Endomorphism Rings in Cryptography

Gaetan Bisson

ENDOMORPHISM RINGS
IN CRYPTOGRAPHY

Gaetan B

A catalog record is available from the Eindhoven University of Technology Library.
: - - -

C P : 尾形月耕の「龍昇天」
(Ogata Gekkō’s “dragon ascending” [the mount Fuji volcano])

Endomorphism Rings in Cryptography

PROEFSCHRIFT

ter verkrijging van de graad van dońor aan de
Technische Universiteit Eindhoven, op gezag van de
reńor magniŏcus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op donderdag juli om . uur

door

Gaëtan Bisson

geboren te Les Ulis, Frankrijk

Dit proefschrift is goedgekeurd door de promotor:

prof.dr. Tanja Lange

Copromotor:
dr.habil. Pierrick Gaudry

ENDOMORPHISM RINGS IN CRYPTOGRAPHY

thèse préparée par

Gaëtan B

L L R
I Ž A

&

É N S M N

pour l'obtention du doctorat en informatique de l'

I N P Ž L
(IAEM L)

présentée et soutenue publiquement le 14 juillet 2011
devant un jury composé de

:
Arjeh M. C , professeur — Technische Universiteit Eindhoven

:
Pierrick G , directeur de recherche — Centre National de la Recherche Scientifique
Tanja L , professeur — Technische Universiteit Eindhoven

:
Steven D. G , professeur associé — University of Auckland
David R. K , professeur — Université de la Méditerranée
Henk C. A. T , professeur — Technische Universiteit Eindhoven

:
Jean-Marc C , professeur — Université Toulouse II
Florian H ć, professeur — Universität Oldenburg

À grand-mère doudou

ʅoreword

Acknowledgments

L when I signed up for a PhD projeń under the joint supervision of Pierrick G and Tanja L what great people they were. For the pa three years, they have coped with me in shiŔs, and not only guided my work but aerated my brain through movies, beers, trolls, and smileys. My recent achievements have only been enabled by their ongoing support.

My research work is immensely indebted to Takakazu S , who carefully seleńed a promising topic for my ma er's thesis, and to Andrew S , who I have had the pleasure of working with twice. Ł is work heavily builds upon that of David K and Steven G , and it is a honor to have them as reviewers for my thesis.

Ł e inŒińion of reading this manuscript also fell upon Henk T ; he should be thanked twice as he was such a cheerful and diligent *daily boss* in Eindhoven. My defense committee is further completed by Arjeh C , Jean-Marc C , and Florian H ƈ, to whom I am mo grateful for their enthusiasm about this event.

Ł roughout my PhD program, I have learned abundantly by osmosis from my colleagues Damien R and Romain C , and through discussions with David G in Marseille. Additionally, it was highly scientiŏcally rewarding to be invited to present my work and exchange ideas with Jean-Luc B in Tsukuba, David L in Rennes, Chri ophe R in Marseille, Andreas E in Bordeaux, Vanessa V in Versailles, and Fabien L in Caen.

Conferences provide a rich experience where one travels, works, and relaxes all at once; on various occasions, I have had memorable times (combining all the above) with Nicolas B , Peter S , Jérémie D , Anja B , Laurent I , Peter B , and Nicolas E . I extend my heartfelt thanks to all my coworkers as well, and e ŕecially to those I have repeatedly bothered with que ions or favors, namely Christiane P , Guillaume H , Michael N , Paul Z , Alexander K , Emmanuel T , and Dan B .

For a Frenchman, living in Eindhoven may seem scarier than it ańually is. Fortunately, many friends contributed to making my ays there enjoyable, mo notably Peter L - , Shona Y , Antonino S , and Mayla B ; the weekly CASA poker games were greatly relaxing, and I particularly thank Patricio R and Mark K for the organisational heavy liŔing, and Jan-Willem K for cooking on so many occasions. My o ce (and lunch) mates Daniel T , Bruno R , Relinde J , and Elisa C never uttered a word about my irregular work schedule or cursing at the computer in various languages, for which I highly commend them.

My favorite escape opportunity from both of my workplaces was the prańice of recreational and competitive sailing; I have had wonderful moments sailing with all my fellow crewmen, and if I may ju thank three it would be Jean-François M for providing more opportunities than I could accept, and François G and Luc H for putting up with the hard task of seconding me.

Ł e École Normale Supérieure provided me with a profusion of social, scientiŏc, and admini rative experiences; I am indebted to its a for providing such a great environment. Since then, mo of the weekends I ŕ ent in transit in Paris were cheered up by old friends who did not escape the French capital: those people with a ŕ are mattress, Marc S , Pierre-Loïc M , and Mélanie J , but also Pierre & Con ance D who ho ed so many events. On the other hand, some dared going abroad too, and I really enjoyed visiting David D in London, and Jean-Dominique D L and Pauline P in Berlin.

Back in the "tough" days of *clńses préparŅoires*, I was lucky enough to befriend Séba ien A , Yannick A , Jean F , and Jean-Georges M , who have always been a joy to see again since, although mo of us are not living in the same continent anymore.

My horizons were widely expanded by the free and open culture movement, and I would like to salute those who initiated me to it: in the soŔware category, this ranges from the *saŝe S* to my fellow Arch Linux developers and, in the music category, this includes SomaFM's ecleńic music direńors and talented arti s.

La but not lea , my profound gratitude goes to the entire B , L , and J families for their continuous relief and kindness over the pa quarter of a century.

Gaetan B
Eindhoven, May

Introduction

Suppose Mr. Athos wishes to write a private message to Mrs. Bonacieux while keeping its contents secret from his Eminence of Richelieu, to whom the courier is mo certainly beholden; he could put the message in a safe box whose combination is only known to himself and to Bonacieux, and that would be very co ly to break.

Rather than physical devices, cryptography re s on computational power to ensure data security and integrity. Athos and Bonacieux are each given a black box: Athos' is parametrized by a key and transforms messages into unintelligible data called ciphertexts; with the corre ŕ onding key, Bonacieux's reverses this operation. Ciphertexts can then be transmitted openly over any medium. Chapter gives a brief overview of such techniques, with an emphasis on schemes allowing Athos' key to be public: they are only a few decades old and make extensive use of mathematical ruńures.

Abelian varieties are objeńs upon which such schemes can be built very e ciently and securely; they are formally introduced in Chapter , which concisely presents certain of their theoretical a ŕ eńs, focusing on computations over ŏnite ŏelds. Subsequent chapters, where the original contributions of this thesis are located, are concerned with algorithmic properties related to the endomorphism ring ruńure of abelian varieties; mo of the theoretical background on this topic forms what is known as complex multiplication theory, which Chapter covers.

An important application of endomorphism rings is the con ruńion of abelian varieties with desirable properties. For in ance, many featureful cryptographic schemes have recently been enabled by pairings; to make these schemes prańical, abelian varieties endowed with e cient pairings mu be generated. Chapter discusses this subjeń, including the work of B. and S ( ) and related results.

Ł e second half of this thesis addresses the problem of computing the endomorphism ring of a prescribed abelian variety, which can be seen as the inverse problem to variety generation. Chapter recalls prior ate-of-the-art methods, all of which have an exponential runtime in the size of the input. It also describes the general ruńure of isogeny graphs, which is later extensively relied on.

Our subexponential algorithms for computing endomorphism rings of ordinary abelian varieties are ŏr described in Chapter in an idealized setting. Ł ey exploit complex multiplication theory in its relevance to the ruńure of isogeny graphs. When ŕ ecialized to the case of dimension-one abelian varieties, this direńly yields highly e eńive methods which are essentially equivalent to that of B. and S ( ). Ł eir complexity is rigorously analyzed in Chapter , as was done in B. ( ); this chapter ends with a discussion of the results of B. and S ( ) in this context, from a di erent per ŕ eńive than the original article.

Chapter ŏnally explains how our methods can be adapted to be e eńive in higher dimension, and reports on the implementation of B., C , and R ( ) enabling the evaluation of general maps between abelian varieties (so-called isogenies), which is an important building block of our algorithms. We conclude by applying our technique to the computation of several illu rative and record examples.

Contributions

. Gaetan B and Takakazu S .
"More discriminants with the Brezing-Weng method".
In: *Progress in Cryptology — INDOCRYPT '* .
Edited by Dipanwita R. C , Vincent R , and Abhijit D .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/978-3-540-89754-5_30`.

. Gaetan B and Andrew V. S .
"Computing the endomorphism ring of an ordinary elliptic curve over a ŏnite ŏeld".
In: *Journal of Number Ńeory* . . Edited by Neal K and Vińor S. M .
Special Issue on Elliptic Curve Cryptography. Pages – .
DOI: `10.1016/j.jnt.2009.11.003`.

. Gaetan B , Romain C , and Damien R .
AVIsogenies, a library for computing śogenies b'nween abelian vari'nies.
Regi ered at the Agence pour la Proteńion des Programmes under reference `IDDN.FR.001.440011.000.R.P.2010.000.10000`.
URL: `http://avisogenies.gforge.inria.fr/`.

. Gaetan B .
Computing endomorphśm rings of eŝiptic curves under ūe GRH.
arXiv.org: `1101.4323`.

. Gaetan B and Andrew V. S .
"A low-memory algorithm for ŏnding short produń representations in ŏnite groups".
In: *Designs, Codes and Cryptography.* To appear.
DOI: `10.1007/s10623-011-9527-8`.

. Gaetan B .
Computing endomorphśm rings of abelian vari'nies. In preparation.

Contents

A V

C

Ƴanorama of Ƨryptography

Hi orically, cryptography has prevalently been employed for secrecy, although over time it has come to provide other features, such as integrity proteńion and authentication. Ł is chapter concisely presents andard techniques achieving such classical primitives; it serves as both a motivation and prańical framework for computational number theory.

1.1 Symmetric Primitives

Early cryptography necessitated a secret, called the *key*, to be shared between the parties involved. Primitives of that lineage are said to be *symmʼnric*; they are in wide ŕ read use and development today, mo ly due to their Œexible and fa implementations.

C

Denote by $\mathbb{S} = \{0,1\}^{(\mathbb{N})}$ the set of all *rings*, that is, ŏnite sequences of bits.

Definition 1.1.1. Symmetric encryption schemes *consśt of two families* E *and* D *of funňions, not necessarily everywhere deŔned, Řom* $\mathbb{S}$ *to* $\mathbb{S}$ *such ū Ņ* $\mathrm{D}_k \circ \mathrm{E}_k = \mathrm{Id}_{\mathrm{dom}(\mathrm{E}_k)}$ *for aŝ rings k.*

Intuitively, E and D are the black boxes to provide Athos and Bonacieux: the *cipher* E is parametrized by a *key k*, takes *plaintexts m* as input, and returns *ciphertexts* $\mathrm{E}_k(m)$, while the *decipher* D does the converse. His Eminence should be unable to gain any insight on the message *m* from the sole knowledge of the ciphertext $\mathrm{E}_k(m)$; in the rińe sense, this is formalized as *perfeň secrecy*, which requires that, for all ŏnite sets of rings M and M′,

$$\mathrm{Prob}_{k,m}[m \in \mathrm{M} \mid \mathrm{E}_k(m) \in \mathrm{M}'] = \mathrm{Prob}_m[m \in \mathrm{M}].$$

Early ciphers, going back to several centuries BC, simply swapped or shiŔed bytes of the plaintext in a regular fashion derived from the key; for in ance, ŕ litting rings as sequences of bytes that encode letters A–Z as integers – , the cipher

$$\mathrm{E}_k : (m_i) \longmapsto (m_i + k \bmod 26)$$

is ill in limited use today with $k = 13$. Similar schemes not obviously as weak have also been designed using larger keys; virtually all have since been broken by the development of frequency analysis.

S ( ) e ablished the exi ence and essential uniqueness of a cryptosy em achieving perfeń secrecy: the *one-time pad* — it requires a key to be drawn independently and uniformly at random from $\{0,1\}^n$ for each n-bit plaintext, and returns as ciphertext the bit-by-bit xor of the plaintext and the key. Its prańical use is only limited by the ability to carry suitcases full of pads around, prior to doing any encryption.

To mimic its behavior while overcoming the need for lengthy keys transmission, *ream ciphers* (also known as *pseudorandom number generŅors*), on input a small key called the *seed*, determini ically generate pads to be xored with the plaintext; as before, measurable ati i-cal deviations of such pads from random rings should be avoided. Nowadays, *block ciphers*, which encrypt ŏxed-length blocks of bits, are the mo widely used, and particularly that of D and R ( ) later andardized as the AES. Procedures for encrypting sequences of blocks, known as *modes of operŅions*, prevent additional information leakage when handling messages of arbitrary length.

C S

Ł e above overview calls for a more down-to-earth discussion of security aŕeńs: the result of S ( ) concerns whether the key *can ūeor'nicaŝy* be recovered from a certain amount of ciphertext, not how resource-demanding that process is.

One of the cheape ways of e eńively compromising the key is to peek at Athos' note-book, or simply to ask him about it over a nice glass of wine; such *side-channel ŅŪcks* will not be discussed here, as we focus on cryptosy ems themselves, not their implementations.

Definition 1.1.2. *A cipher* E *ś compuŪtionaŝy* secure *if, for mo keys k, it ś compuŪtionaŝy infeńible to derive plaintexts m Řom ciphertexts* $\mathrm{E}_k(m)$.

"Computationally infeasible" means that, with today's ate-of-the-art machines, this computation would take more time than is available, say, billions of years.

Other conditions might be desirable as well; for in ance, that the output of E_k cannot feasibly be told apart from that of a random funńion. However, as our intere will shiŔ to the mathematical building blocks of cryptosy ems, this di inńion will bear little relevance.

Most cryptosystems do not achieve perfect secrecy, and are thus susceptible to *brute-force attacks*, which decrypt given ciphertexts by trying all possible keys in turn. For "ideal ciphers," this is the best attack, and for "ideal keys," which have no special property that reduces the search range, it takes $2^n/2$ runs on average to find an n-bit key.

With today's technology, the total number of elementary arithmetic operations realistically achievable can be bounded from above by 2^{128}; keys bearing (at least) 128 bits of entropy are thus recommended. Naturally, this should be tempered by several factors:

– the gravity of the encrypted information;

– the desired lifetime of the cryptosystem;

– the available processing power.

For instance, a news agency broadcasting encrypted live reports to its paying subscribers with different keys each day might only need to withstand limited-resources attacks for 24 hours.

Summing up the above, assessing the security of a cryptosystem calls for a deep understanding of the ways and costs to attack it. M ( ) predicted an exponential growth in available computing power which has been verified for the past four decades; as a consequence, the costs should be considered for increasing key-sizes.

Rather than relying on a rigorous computing model such as the multi-tape universal machines of T ( ), we will simply analyze algorithms by looking at both their actual runtime on practical computations, and their long-term behavior embodied in asymptotic bit-complexity estimates. In particular, we disregard quantum-computing models.

To emphasize the need for an asymptotic analysis, denote by $c_{\mathrm{E}}(n)$ the operation count of the best method for attacking a cipher E with n-bit keys: if c_{E} grows subexponentially, key-sizes are required to increase more than linearly in time to provide a constant level of security, which may eventually prove to be quite cumbersome.

H F

One-way functions formalize the behavior which is expected of ciphers parametrized by unknown keys; they have countless applications, far beyond cryptography, such as hash tables. Like ciphers, they can be defined in a complexity-theoretic way, as *functions that can be evaluated by polynomial-time algorithms, but for which no polynomial-time algorithm can successfully find preimages on more than an exponentially small fraction of the image.*

Since the existence of such functions implies $\mathrm{P} \neq \mathrm{NP}$, we look for a more practical stance.

Definition 1.1.3. *A function $h : \mathbb{S} \to \mathbb{S}$ is* one-way *if it is computationally infeasible to find preimages of most of its image. It is also a* hash function *if its image is contained in $\{0,1\}^n$ for some n and it is computationally infeasible to find two strings $x \neq x'$ verifying $h(x) = h(x')$.*

Again, additional conditions might be required for specific applications. The *random oracle* is a convenient ideal encompassing most expectations: it is nothing but the Cartesian power by $\mathbb{S}$ of the uniform distribution on n-bit strings, or, more pragmatically, a “map” whose images are drawn uniformly at random from $\{0,1\}^n$.

Since there typically are at least a few functions (such as constant ones) that are unsuitable, designs using hash functions h are often analyzed by assuming that h has the uniform distribution, and proving that the desired properties hold with overwhelming probability.

Traditionally, hash functions are crafted as a mix of logic gates, but some have also been

Researches have built cryptographic blocks upon mathematical objects of various kinds: D and H ( ) used discrete logarithms, M and H ( ) relied on knapsacks, R , S , and A ( ) suggested using integer factorization, M E ( ) made the case for error-correcting codes, M and I ( ) employed certain multivariate polynomials, Z ( ) exploited Cayley graphs, A ( ) proposed using lattices, etc.

This thesis is concerned with some of the underlying mathematical aspects of discrete-logarithm-based systems. The groups G with which they are concerned will be presented in the next chapter — for now, let us keep motivating their introduction.

1.2 Asymmetric Primitives

Although ciphers can be implemented efficiently, the need for a shared key to be secretly transmitted prior to any two-party communication is inconvenient. Most often today, a shared key is first established using asymmetric techniques (which overcome this problem) *over the insecure channel*, and then used to encrypt the data via a stream or block cipher.

P -K P

D and H ( ) introduced the key exchange below, which solves precisely this problem: making two individuals agree, over an open channel, on a shared secret key (to be subsequently used for encryption); it proceeds as follows:

. Athos chooses an element g of some group G and sends it to Bonacieux.

. Athos picks an integer a and sends g^a to Bonacieux.

. Bonacieux picks an integer b and sends g^b to Athos.

. Athos and Bonacieux compute the *shared secret* g^{ab} as $(g^a)^b$ and $(g^b)^a$ respectively.

When a passive observer breaks this scheme, they have solved the following.

Definition 1.2.1. *The* Diffie–Hellman problem *is that of computing g^{ab} from g, g^a, and g^b.*

It is obviously no harder than the discrete logarithm problem, and is believed to neither be weaker. This key-exchange is hence considered secure in well-chosen groups of order 2^{256}.

The problem of authentication remains, since Milady de Winter could bribe the courier so as to intercept and forge messages: she would pick her own integer c and impersonate Bonacieux to Athos (with secret g^{ac}) and Athos to Bonacieux (with secret g^{bc}), thus spying on (and actively interfering with) the whole communication.

Definition 1.2.2. Asymmetric encryption schemes *consist of two families* E *and* D *of functions, not necessarily everywhere defined, from* $\mathbb{S}$ *to* $\mathbb{S}$ *and a one-way function w such that* $D_k \circ E_{w(k)} = \mathrm{Id}_{\mathrm{dom}\, E_{w(k)}}$ *for all strings k. It is a* signing scheme *provided* $E_{w(k)} \circ D_k = \mathrm{Id}_{\mathrm{dom}\, D_k}$ *also holds.*

The map w is the *key-generation function*: it takes a *private key k* as input and returns the corresponding *public key* $w(k)$, to be publicly distributed along with E, making anybody able to encrypt messages that only the holder of k can decrypt. Conversely, if the key holder of a signing scheme broadcasts $D_k(m)$ for some message m, everyone can evaluate $E_{w(k)}(D_k(m))$ and be assured that the *signature* $D_k(m)$ originates from the holder of k.

In practice, signing schemes are designed independently from encryption schemes; however, for our brief presentation, this naïve framework encompassing both will suffice.

Asymmetric schemes rarely deal with large amounts of data: for encryption, ciphers are used and only their keys are encrypted asymmetrically; for authentication, it suffices to sign a hash of the message. Without loss of generality, we will therefore now describe primitives dealing with subsets of $\mathbb{S}$ whose coding as bits will be understood.

E C

Definition 1.2.3. *In a group* G *noted multiplicatively, the* short product problem *is that of finding a subsequence of a given sequence* $S \in G^{(\mathbb{N})}$ *whose product is a prescribed element z.*

Products of subsequences of S *are called* short products*; in addition, when* S *has no repeated elements, this problem is known as the* subset sum problem *in additive groups and as the* knapsack problem *for* $G = \mathbb{Z}$.

Some of its instances are equivalent to discrete logarithm problems: if S' is a subsequence of $S = (g^{2^0}, g^{2^1}, \ldots, g^{2^{\lfloor \log_2 \# G \rfloor}})$ with product z, then $z = g^n$ where the i^{th} bit of n is one if $g^{2^i} \in S'$ and zero otherwise. From a cryptographic standpoint, this means that the map

$$E_S : (x_i) \in \{0,1\}^{\lfloor \log_2 \# G \rfloor} \longmapsto \prod_{i=1}^{\lfloor \log_2 \# G \rfloor} s_i^{x_i} \in G$$

is a tentative one-way function for certain groups G and sequences S of length about $\log_2 \# G$.

M and H ( ) proposed an asymmetric scheme which scrambles easy knapsacks (the private keys) into seemingly harder ones (the public keys): let $(s_i) \in \mathbb{N}^n$ be a sequence such that $\sum_{i<j} s_i < s_j$ for $j \in \{1, \ldots, n\}$, put $v = \sum s_i$, and define S as the projection of (s_i) to $\mathbb{Z}/v$; the map E_S can then be inverted in polynomial time by a greedy algorithm. Now, choose an integer u coprime to v, and publish the sequence $T = (t_i) = (us_i \bmod v)$. In the formalism above, we have $k = (S, u, v)$ as the private key, $w : k \mapsto T$ as the key-generation map, and $E_{w(k)} : (m_i) \in \{0,1\}^n \mapsto \sum m_i \cdot t_i$ as the encryption function; the greedy algorithm decrypts a ciphertext m' by finding a subsequence of S with sum $u^{-1}m' \bmod v$. S ( ) later broke this scheme due to the simplicity of its scrambling process.

M ( ) constructed a much more conservative signature scheme, built entirely from a hash function h, and certified its security assuming that of h. This was achieved by developing an original idea of L ( ): if one selects private strings x and y and publishes their images $h(x)$ and $h(y)$ by a hash function, he may later sign a bit of data by releasing either x (if the bit is zero) or y (if it is one).

M C

The RSA cryptosystem of R , S , and A ( ) rests on the problem of integer factoring, although subexponential factoring algorithms were already known at the time. Nevertheless, it has become widely used despite the large keys and *a fortiori* computing resources required by reasonable levels of security.

Let $n = pq$ be a product of two primes, and pick an integer r coprime to $(p-1)(q-1)$; this ensures that the map $m \mapsto m^r$ is an automorphism of $(\mathbb{Z}/n)^\times$. Let the private key be (p,q,r), and publish (n,r) as the public key and $E_{(n,r)} : m \mapsto m^r \bmod n$ as the encryption function; decrypting then consists in applying the inverse automorphism $D : m \mapsto m^s$ where s can be computed from p and q (and conversely) since $s = r^{-1} \bmod (p-1)(q-1)$.

The key-length of an RSA cryptosystem is the bit-size of n. The following table shows, at various levels of security, the key-lengths recommended by ECRYPT II ( ) for RSA, ElGamal (see below), and equivalently secure symmetric schemes *in ūe be cńe*, that is, assuming well-chosen parameters. The superlinear growth of RSA keys is due to the aforementioned subexponential factoring techniques.

	RSA	ElGamal

E G ( ) designed a cryptosystem based on the Diffie–Hellman problem: let g be a generator of some group G, and pick an integer x. The public key is (g,h) where $h = g^x$, and x is the secret key. The ciphertext of a message m (encoded as an element of G) is $(g^y, m \cdot h^y)$ where y is a random integer; to decrypt it, simply put g^y to the power x and divide it out from $m \cdot h^y$.

Compared to many other cryptosystems, the ElGamal scheme stands out for its elegance and flexibility: since the group G it uses is not restricted to a certain class (such as RSA which uses G = $(\mathbb{Z}/n)^\times$), it has more latitude to ŏnd one that has both an e eńive group law, and in which no attack is fa er than generic ones.

A P

Beyond encrypting and signing, many advanced and/or exotic cryptographic schemes exi , mo of which are enabled by the computability of certain mathematical objeńs.

Zero-knowledge proofs are protocols where Athos is to convince Bonacieux that he knows some secret without revealing anything about it. For in ance, the secret could be a (dedicated) private key; to be convinced of his knowledge of the private key, Bonacieux could send Athos a random message encrypted with the associate public key and challenge him to reveal the plaintext — she would learn nothing regarding the private key but that Athos knows it. Many other con ruńions exi , notably that of G , M , and W ( ) which demon rated the power of a graph-based approach.

Homomorphic encryption aims at performing operations on plaintexts seamlessly via ciphertexts. For in ance, in the ElGamal scheme, the term-by-term produń of ciphertexts for m and m' is a valid ciphertext for mm' since

$$\left(g^y, mh^y\right) \cdot \left(g^{y'}, m'h^{y'}\right) = \left(g^{y+y'}, mm'h^{y+y'}\right).$$

Fully homomorphic sy ems feature two such algebraic operations; they are far more powerful as they enable the encrypted evaluation of any circuit. G ( ) described such a scheme using lattices but its prańicality is ill a topic of ańive research.

Ł e pa decade also saw a plethora of novel cryptographic schemes exploiting the richness of *pairings*, that is, non-degenerate bilinear maps $\Psi : G_1 \times G_2 \to H$ where the groups G_i are noted additively, and H is noted multiplicatively. Ł e ŏr was a one-round tripartite Di e–Hellman key-exchange: assume Athos, Bonacieux, and Chevreuse are to derive a shared secret key over an insecure channel; the protocol of J ( ) goes as follows:

. Athos chooses and broadca s a pairing Ψ and a pair $(x, y) \in G_1 \times G_2$.

. Athos picks an integer a and broadca s ax and ay.

. Bonacieux picks an integer b and broadca s bx and by.

. Chevreuse picks an integer c and broadca s cx and cy.

. Everybody computes $\Psi(ax, by)^c = \Psi(bx, cy)^a = \Psi(cx, ay)^b$.

1.3 Generic Methods

The security of a cryptographic scheme based on a group does not depend on its isomorphism type alone, since an explicit isomorphism might be very costly to compute; it depends on how the group problem is *encoded* by the function E. For instance, discrete logarithm problems are much easier to solve in $\mathbb{Z}/(p-1)$ than in $(\mathbb{Z}/p)^\times$ although their underlying groups are isomorphic.

This section considers algorithms which apply to any group G regardless of its coding; later, we will come back to which specific codings make which problems easier.

G A

The framework of generic algorithms abstracts group problems (such as the discrete logarithm problem) from specific codings which might render it "artificially" easier. Beware that our definition is not strictly-speaking the most classical one, as we assume that elements are uniquely identified and can be drawn uniformly at random.

Definition 1.3.1. *A* coding *of a group* G *is an injective map* $\gamma : G \to \mathbb{S}$.

A generic group *is a black-box interface to a group* G *which can output* $\gamma(z)$ *for a random z and evaluate* $(x,y) \mapsto \gamma(\gamma^{-1}(x) \cdot \gamma^{-1}(y))$ *and* $x \mapsto \gamma(1/\gamma^{-1}(x))$*, where the coding* γ *is unknown.*

A generic algorithm *takes as input a sequence of encoded group elements* $\gamma(x_i)$ *and is allowed calls to the black box; its complexity is measured by the number of such calls.*

Intuitively, a generic group is a group with shuffled elements, so that nothing is left to exploit in their representation: generic algorithms can only compute the group law.

We will see that many hard problems can be solved by generic algorithms in time $O(\sqrt{\#G})$ but not less. However, determining the order of an element (a special case of discrete logarithm) and, as a consequence, computing the group structure of abelian groups were recently proved by S ( ) to require far fewer operations. Nevertheless, for the specific problems we are concerned with, namely the discrete logarithm problem and the short product problem, the generic algorithms described below are believed to be the best known to date.

R P G

The method of P and H ( ) was originally directed at computing discrete logarithms in $(\mathbb{Z}/p)^\times$ but, more generally, it reduces many problems on abelian groups G into smaller prime groups. It combines two ingredients, the first of which is the following consequence of the Chinese remainder theorem.

Theorem 1.3.2. *Let* G *be an abelian group of order* $n = \prod p^{\alpha_p}$ *for some primes p and positive integers* α_p. *The map*

$$x \in G \longmapsto \left(x^{n/p^{\alpha_p}}\right)_p \in \prod_{p|n} G[p^\infty]$$

is an isomorphism where the p-Sylow subgroup $G[p^\infty]$ *denotes the subgroup of all elements whose order is a power of p. Its inverse is effectively given by the Chinese remainder theorem.*

Once the order of G is factored, this reduces any instance of a problem compatible with the group law to several instances, one in each group $G[p^\infty]$ of prime-power order.

To get down to prime-order groups, the second ingredient is a lifting approach: assuming that G has order p^α, a subgroup series $G = G_0 \to G_1 \to \cdots \to G_\alpha = \{1\}$ where each arrow has index p is used to reduce problems into the quotient groups G_i/G_{i-1}. This technique applies to many problems, such as computing square roots modulo n as T ( )

To quickly search for elements of $A \cap B$, a data structure allowing fast lookups is required; fast insertions are also a must. We therefore typically use hash tables or red black trees. The cost of computing $A \cap B$ is then $(\#A + \#B)O(\log n)$ for $n = \#G$, where the latter term denotes the complexity of the searching and inserting.

When A and B are not as explicit as above, it might not be possible to prove the existence of a collision. The algorithm can then be randomized to rely on the *birthday paradox*:

Proposition 1.3.3. *Let* A *and* B *be uniformly distributed subsets of cardinality* $a\sqrt{n}$ *and* $b\sqrt{n}$ *in a set* G *of cardinality* n*; then*

$$\mathrm{Prob}[A \cap B = \emptyset] \xrightarrow[n\to\infty]{} e^{-ab}.$$

Assuming φ and ψ are random, $\sqrt{n}$ images of each thus suffice to have a $1 - 1/e$ chance of finding a collision. In the unlucky event there is none, we can repeat this process m times, adding more images to our red-black tree; this increases the likelihood of success to $1 - 1/e^{m^2}$.

From now on, we say that a *probabilistic algorithm* has complexity X, or that an algorithm has *probabilistic complexity* X, to mean that it always returns the correct answer (this is known as a *Las Vegas algorithm*) and that, with probability at least $1/2$, its runtime is bounded by X. By the discussion above, up to a constant, it is equivalent to the notion of average complexity.

P ’ R

The baby-step giant-step method requires storing $O(\sqrt{n})$ elements; an algorithm emulating its behavior with minimal space storage was developed by P ( ) for integer factoring, and later applied to discrete logarithms by P ( ).

Let us first unify things in a map $\pi : \mathscr{C} \to G$ equal to φ and ψ on their respective domains, where $\mathscr{C}$ denotes their disjoint union. The rho method involves a *pseudorandom function* $\rho : \mathscr{C} \to \mathscr{C}$, that is, an effective map for which the distribution of $\rho^{(i)}(w)$ (the composition of i copies of ρ) is seemingly uniform as $w \in \mathscr{C}$ is fixed and the integer i varies. It is required to preserves collisions, that is, $\pi(x) = \pi(y) \Rightarrow \pi(\rho(x)) = \pi(\rho(y))$.

The map ρ is thought of as generating A and B under π, and the crucial step is to find collisions $\pi\rho^{(i)}(w) = \pi\rho^{(j)}(w)$ without storing many values; when $\rho^{(i)}(w) \neq \rho^{(j)}(w)$ collide through π, we expect that one is an image of φ and the other is one of ψ, which gives a *proper collision* — when their sizes are equal, this happens with probability a half.

Avoiding storage requires a *cycle-detection* method on the graph of iterates of ρ evaluated at w. The simplest such method is due to F who observed that, whenever $\rho^{(i)}(w)$ and $\rho^{(j)}(w)$ collide for some integers i and j satisfying $i > 2j$, then $\rho^{(2(i-j))}(w)$ and $\rho^{(i-j)}(w)$ also collide. Thus, it suffices to compute $\rho^{(2i)}(w)$ alongside $\rho^{(i)}(w)$ for increasing i's and wait for them to collide; then, ρ maps are unstacked until the original collision is found. Better cycle-detection methods improve the runtime by a constant factor using more memory.

The difficulty lies in designing a function ρ suited to a given problem; more details will be given on that later, especially for the short product problem. To factor an integer n, P ( ) put $\mathscr{C} = \mathbb{Z}/n$ and chose ρ to be a polynomial function; the map π can then be the projection to any subgroup of $\mathbb{Z}/n$ which need not be known: by computing $\gcd\left(\rho^{(i)}(w) - \rho^{(j)}(w), n\right)$, we can detect when a collision occurs and hopefully find a factor of n. This method is nowadays mostly used for small integers n, as asymptotically faster factoring algorithms have since been developed.

A current international effort ( ) aims at solving a discrete logarithm problem challenge in a group of 129-bit order (this group is an elliptic curve where generic algorithms are the best available); when completed, it will likely be the record rho algorithm run.

1.4 Cryptographic Groups

Let us now review the cryptographic security of various groups, mostly focusing on the discrete logarithm problem.

F P

We advocated for prime-order groups; now let us mention how prime numbers can be found. The best method for this is simply to draw numbers at random until a prime is found; for numbers of n bits, this requires an expected $O(n)$ operations by the theorem below.

Assuming the generalized Riemann hypothesis, M ( ) first derived a fast (polynomial time) deterministic primality test, later turned into an unconditional but probabilistic method by R ( ). Although A , K , and S ( ) have since proved that deterministic primality proving need not rely on unproven assumptions, the dependency on the generalized Riemann hypothesis is interesting: this conjecture predicts the behavior of primes in various fields. First recall the celebrated prime number theorem of H ( ) and V -P ( ).

Theorem 1.4.1. *The number of prime integers less than x is asymptotically equivalent to*

$$\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Proofs of this theorem involve establishing certain properties of analytic functions related to integers; more generally, if K is any number field, define, for $s \in \mathbb{C}$ with $\Re(s) > 1$,

$$\zeta_K(s) = \sum_{\mathfrak{a} \in \mathfrak{I}} N(\mathfrak{a})^{-s}$$

where $\mathfrak{I}$ is the set of ideals of the ring of integers of K, and extend ζ_K to $\mathbb{C}$ by analytic continuation. This function encodes the behavior of prime ideals of K; to obtain precise results on their distribution, one often assumes the *extended Riemann hypothesis* which states that all zeroes s of ζ_K in the strip $0 < \Re s < 1$ lie on the line $\Re(s) = 1/2$. The extended Riemann hypothesis follows from the stronger *generalized Riemann hypothesis*, and we often assume the latter when only the former is needed.

M ( ) actually exploited the following result of A ( ), where the label "(GRH)" denotes that the statement holds under the generalized Riemann hypothesis.

Theorem 1.4.2 (GRH). *Let p and q be integers such that q divides $p-1$. The least integer x which cannot be written as $y^q \bmod p$ for some $y \in \mathbb{N}$ is asymptotically $O(\log^2 p)$.*

We conclude with a conjecture of B and H ( ) generalizing the prime number theorem; it is useful for generating elliptic curves as we will see later. Essentially, it asserts that distinct irreducible polynomials take prime values almost independently, and that this "almost" is quantified by their values modulo primes p.

Conjecture 1.4.3. *Let F be a set of distinct irreducible non-constant polynomials of $\mathbb{Z}[X]$. The number of integers less than x at which all its polynomials simultaneously take prime values is asymptotically equivalent to*

$$\frac{C}{\prod_{f \in F} \deg f} \int_2^x \frac{dt}{(\log t)^{\#F}}$$

$$\textit{where} \quad C = \prod_p \left(1 - \frac{1}{p} \# \left\{ z \in \mathbb{F}_p : \prod_{f \in F} f(z) = 0 \right\}\right) \Big/ \left(1 - \frac{1}{p}\right)^{\#F}.$$

I C

Since the baby-step giant-step or rho method use $O(\sqrt{p})$ operations to find a factor p of an integer n, factors of n can always be found in $O(n^{1/4})$ time. By iterating this search for factors and testing the primality of the factors obtained, an integer n can be factored in probabilistic time $O(n^{1/4})$. When the RSA cryptosystem was proposed, much faster algorithms already existed and they were substantively improved subsequently.

Ł e simple   such method is due to K   ( ). To ŕ lit an integer n, it craŔs a nontrivial relation $x^2 = y^2 \bmod n$ by combining many easier relations so as to eliminate non-square fańors; the easier relations are of the form $z^2 \bmod n = \prod p^{\alpha_p}$ for primes p less than some bound $\mathrm{L}(n)$. To bound the probability that such a fańorization exi s, we rely on this result of C   , E   , and P   ( ).

Theorem 1.4.4. *For any $c > 0$, ū e probability for a random number of $\{1, \ldots, x\}$ to have no prime fańor larger ū an $\mathrm{L}(x)^c$ ś equivalent to $\mathrm{L}(x)^{-1/2c+o(1)}$ ń $x \to \infty$, where we Ŭed ū e function*

$$\mathrm{L}_\alpha(x) = \exp\left((\log x)^\alpha (\log\log x)^{1-\alpha}\right)$$

wi ū ū e conl·ention ū Ņ omitting ū e param’ner $\alpha \in (0,1)$ means $\alpha = 1/2$.

Assuming Gaussian elimination takes cubic time in the number of variables, we set $c = 1/2$ and obtain a nontrivial ŕ litting of n in time $\mathrm{L}(n)^{3/2+o(1)}$.

Ł e broad family of *combining congruences algori ū ms* encompasses methods using *fańor bńes* (as the primes up to $\mathrm{L}(n)$); they apply to many integer-based problems such as discrete logarithms in ŏnite ŏelds and integer fańoring. Under unproven assumptions, the asymptotically fa e   such method is the *number Ŕeld sieve* of C   ( ), which builds up on the work of many including L   and L   ( ), with heuri ic complexity

$$\mathrm{L}_{1/3}^{c_{\mathrm{NFS}}}(n) \quad \text{where} \quad c_{\mathrm{NFS}} = 2\sqrt[3]{\frac{46 + 13\sqrt{13}}{108}} \approx 1.902$$

Recently, K   ’n alii ( ) used a similar method to fańor a 768-bit RSA modulus, thereby deprecating smaller RSA keys; the e ńiveness of this attack is blatant when compared to elliptic curves whose discrete logarithms can only be attacked up to 130 bits.

Unconditionally proven fańoring algorithms are slightly slower, with the   ate-of-the-art method of L   and P   ( ) using an expeńed $\mathrm{L}(n)^{1+o(1)}$ operations; it exploits a similar fańor base paradigm in certain class groups. Since these objeńs are built from ideals it is not surprising that subexponential methods should apply to them as well, and we will elaborate on that later as class groups become a building block of our own algorithms.

A   V

Cryptosy ems based on the discrete logarithm problem in ŏnite ŏelds have been proposed as alternatives to RSA; however, up to certain modiŏcations, modern integer fańoring algorithms also apply to this problem, so it provides no additional security.

Shortly aŔer L ( ) introduced a novel fańoring algorithm based on elliptic curves, M ( ) and K ( ) sugge ed their use in cryptography; subsequently, K ( ) further proposed using the broader class of abelian varieties. Ł is has motivated tremendous developments in computational number theory, and has enabled a wide ŕ eńrum of possibilities in cryptography.

Ł ese applications are motivated by two fańs: ŏr , that the group law of abelian varieties can be computed e ciently, and second, that no algorithm better than generic ones is currently known to attack the discrete logarithm problem on mo abelian varieties of dimension one and two. Before formally deŏning abelian varieties, we brieŒy give loose atements highlighting their applicability to cryptography.

Abelian vari'nies are objeńs endowed with two compatible ruńures:

- a *geom'nric* ruńure: it is the zero locus of multivariate polynomials over a ŏeld k;
- a *group* ruńure: it admits a group law given by rational funńions.

When the deŏning polynomials have certain forms, the group law can be evaluated e ciently using short rational funńions. Ł is can be done for all varieties of dimension one and two (the *dimension* is roughly the number of variables minus the number of polynomials).

Cryptography uses ŏnite ŏelds k and such forms, allowing fa arithmetic; for in ance, B and L ( ) sugge ed deŏning G as the set of points $(x,y) \in k^2$ verifying

$$x^2 + y^2 = 1 + dx^2y^2$$

for some non-square parameter $d \in k$, endowed with the addition law deŏned by

$$(x,y) + (x',y') = \left(\frac{xy' + x'y}{1 + dxx'yy'}, \frac{yy' - xx'}{1 - dxx'yy'} \right).$$

Since the number of points of an abelian variety of dimension g deŏned over k (that is, the order of the underlying group) is roughly $(\#k)^g$ and otherwise behaves quite randomly, a prime-order one can be sought by drawing varieties at random while their orders are composite. Alternatively, we will later discuss the theory of complex multiplication which provides means to generate abelian varieties with a prescribed order.

S A

We ated that attacks on the discrete logarithm problem of mo elliptic curves are not known to be fa er than generic ones. To conclude this chapter, we give an exhau ive li of classes of abelian varieties for which this does not hold, so remaining ones can *a priori* be considered secure. Details on these attacks can be found in A , C , D , F , L , N , and V ( ).

Index-calculus with subspace as factor base. Gröbner basis algorithms can decompose points of abelian varieties into sums of points in certain subspaces (such as having certain coordinates equal to zero, or defined over some strict subfield); this enables index-calculus attacks effective on varieties of dimension $g > 2$ or defined over non-prime base fields.

Reduction to finite fields via pairings. The Weil pairing maps pairs of points of order ℓ from an abelian variety to the multiplicative group of an extension of degree $e(\ell)$ of the base field k. It transports the discrete logarithm problem, so the value of $e(\ell)$ must be large enough to prevent attacks in the extension field from being feasible.

Lift to characteristic zero. Certain abelian varieties with special properties (such as the infamous *anomalous curves*, whose cardinality is that of their base field) can be lifted to p-adic fields, from where discrete logarithm problems can be transferred to $\mathbb{Z}/p$.

Isogenies. Isogenies are morphisms between abelian varieties; they can transport the discrete logarithm from a variety $\mathscr{A}$ to about ℓ^g other varieties in time $\ell^{O(g^2)}$ for most primes ℓ; if any of those varieties have one of the above weaknesses, then so does $\mathscr{A}$.

Since no attack faster than generic algorithms is known to affect randomly chosen, prime-order abelian varieties of dimension one or two defined over finite fields with p or 2^p elements where p is a prime, we conclude that these are currently the best choice for public-key cryptography in a cryptosystem of ElGamal type.

References

. Alberto T .
"Bemerkung über die Auflösung quadratischer Congruenzen".
In: *Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen* . . Pages – .

. Charles-Jean V -P .
"Recherches analytiques sur la théorie des nombres premiers".
In: *Annales de la Société Scientifique de Bruxelles* . . Pages – .

. Jacques H .
"Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques".
In: *Bulletin de la Société Mathématique de France* . Pages – .

. Maurice K .
Théorie des Nombres. Volume .
Analyse indéterminée du second degré et factorisation. Gauthier-Villars.

. Alan T .
"On computable numbers, with an application to the Entscheidung problem".
In: *Proceedings of the London Mathematical Society* . . Pages – .
DOI: `10.1112/plms/s2-42.1.230`.

. Claude S .
"Communication theory of secrecy systems".
In: *Bell System Technical Journal* . . Pages – .

. Nesmith C. A .
"The least quadratic non residue". In: *Annals of Mathematics* . . Pages – .
DOI: `10.2307/1969420`.

. Paul T. B and Roger A. H .
"Primes represented by irreducible polynomials in one variable".
In: *Theory of Numbers.* Edited by Albert L. W . Volume .
Proceedings of Symposia in Pure Mathematics. American Mathematical Society.
Pages – .

. Gordon E. M .
"Cramming more components onto integrated circuits".
In: *Electronics Magazine* . . Pages – .

. Daniel S .
"Class number, a theory of factorization, and genera".
In: *Number Theory Institute.* Edited by Donald J. L . Volume .
Proceedings of Symposia in Pure Mathematics. American Mathematical Society.
Pages – .

. Gary L. M .
"Riemann's hypothesis and tests for primality".
In: *Symposium on Theory of Computing — STOC '* .
Edited by William C. R , Nancy M , Jack W. C , and
Michael A. H . Association for Computing Machinery. Pages – .
DOI: `10.1145/800116.803773`.

. John M. P .
"A Monte Carlo method for factorization".

In: *BIT Numerical MŅhemŅics* . . Pages – .
DOI: 10.1007/BF01933667.

. Whitŏeld D and Martin E. H .
"New direńions in cryptography".
In: *IEEE Transaňions on InformŅion Ńeory* . . Pages – .
DOI: 10.1109/TIT.1976.1055638.

. Robert J. M E .
"A public-key cryptosy em based on algebraic coding theory".
In: *DSN Progress Report*. Volume – . Jet Propulsion Laboratory. Pages – .

. Ralph C. M and Martin E. H .
"Hiding information and signatures in trapdoor knapsacks".
In: *IEEE Transaňions on InformŅion Ńeory* . . Pages – .
DOI: 10.1109/TIT.1978.1055927.

. Stephen C. P and Martin E. H .
"An improved algorithm for computing logarithms over GF(p) and its cryptographic signiŏcance". In: *IEEE Transaňions on InformŅion Ńeory* . . Pages – .
DOI: 10.1109/TIT.1978.1055817.

. John M. P .
"Monte Carlo methods for index computation (mod$p$)".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: 10.2307/2006496.

. Ron L. R , Adi S , and Leonard A .
"A method for obtaining digital signatures and public-key cryptosy ems".
In: *CommunicŅions of ū e ACM* . . Pages – .
DOI:

. Adi S .
"A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem". In: *Foundations of Computer Science — FOCS '* . IEEE Computer Society. Pages – . DOI: `10.1109/SFCS.1982.55`.

. Earl C , Paul E , and Carl P .
"On a problem of Oppenheim concerning 'factorisatio numerorum'". In: *Journal of Number Theory* . . Pages – . DOI: `10.1016/0022-314X(83)90002-1`.

. Taher E G .
"A public key cryptosystem and a signature scheme based on discrete logarithms". In: *Advances in Cryptology — CRYPTO '* . Edited by George Robert B and David C . Volume . Lecture Notes in Computer Science. Springer. Pages – . DOI: `10.1007/3-540-39568-7_2`.

. Oded G , Silvio M , and Avi W .
"Proofs that yield nothing but their validity and a methodology of cryptographic protocol design". In: *Foundations of Computer Science — FOCS '* . IEEE Computer Society. Pages – . DOI: `10.1109/SFCS.1986.47`.

. Victor S. M .
"Use of elliptic curves in cryptography". In: *Advances in Cryptology — CRYPTO '* . Edited by Hugh C. W . Volume . Lecture Notes in Computer Science. Springer. Pages – . DOI: `10.1007/3-540-39799-X_31`.

. Neal K .
"Elliptic curve cryptosystems". In: *Mathematics of Computation* . . Pages – . DOI: `10.1090/S0025-5718-1987-0866109-5`.

. Hendrik W. L .
"Factoring integers with elliptic curves". In: *Annals of Mathematics* . . Pages – . DOI: `10.2307/1971363`.

. Tsutomu M and Hideki I .
"Public quadratic polynomial-tuples for efficient signature-verification and message-encryption". In: *Advances in Cryptology — EUROCRYPT '* . Edited by Christof G. G . Volume . Lecture Notes in Computer Science. Springer. Pages – . DOI: `10.1007/3-540-45961-8_39`.

. Neal K .
"Hyperelliptic cryptosy ems". In: *Journal of Cryptology* . . Pages – .
DOI: 10.1007/BF02252872.

. Hendrik W. L and Carl P .
"A rigorous time bound for fańoring integers".
In: *Journal of ū e American MŅhemŅical Sociňy* . . Pages – .
DOI: 10.1090/S0894-0347-1992-1137100-0.

. Don C .
"Modiŏcations to the number ŏeld sieve".
In: *Journal of Cryptology* . . Pages – . DOI: 10.1007/BF00198464.

. Arjen K. L and Hendrik W. L (editors).
Ń e Development of ū e Number Field Sieve. Volume .
Leńure Notes in Mathematics. Springer. ISBN: - - - .

. Gilles Z .
"Hash funńions and Cayley graphs".
In: *Designs, Codes and Cryptography* . . Pages – .
DOI: 10.1007/BF01388652.

. Miklós A .
"Generating hard in ances of lattice problems".
In: *Symposium on Ń eory of Computing — STOC '* . Edited by Gary L. M .
Association for Computing Machinery. Pages – .
DOI: 10.1145/237814.237838.

. Vińor S .
"Lower bounds for discrete logarithms and related problems".
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Walter F .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/3-540-69053-0_18.

. Joan D and Vincent R .
Ń e RŜndael block cipher. Advanced Encryption Standard proposal submitted to the National In itute of Standards and Technology.

. Antoine J .
"A one round protocol for tripartite Di e–Hellman".
In: *Algoriū mic Number Ń eory — ANTS-IV.* Edited by Wieb B .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/10722028_23.

. Manindra A , Neeraj K , and Nitin S .
"PRIMES is in P". In: *Annals of MṆhemṆics* . . Pages – .
DOI: `10.4007/annals.2004.160.781`.

. Roberto M. A , Henri C , Chri ophe D , Gerhard F ,
Tanja L , Kim N , and Frederik V .
Handbook of Eŝiptic and Hypereŝiptic Curve Cryptography.
Discrete Mathematics and its Applications. Chapman & Hall.
ISBN: - - - .

. Daniel J. B and Tanja L .
"Fa er addition and doubling on elliptic curves".
In: *Advances in Cryptology — ASIACRYPT '* . Edited by Kaoru K .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/978-3-540-76900-2_3`.

. Andrew V. S .
"Order computations in generic groups".
PhD thesis. Massachussets In itute of Technology. URL:
`http://groups.csail.mit.edu/cis/theses/sutherland-phd.pdf`.

. Daniel V. B , Lejla B , Daniel J. B , Peter B ,
Joppe W. B , Hsieh-Chung C , Chen-Mou C , Gauthier van D ,
Giacomo de M , Luis J. D P , Junfeng F ,
Tim G , Frank G , Ł or en K , Tanja L ,
Nele M , Ruben N , Chri of P , Francesco R ,
Peter S , Leif U , Anthony van H , and Bo-Yin Y .
Breaking ECC K- . IACR ePrint: `2009/541`.

. Denis X. C , Kri in E. L , and Eyal Z. G .
"Cryptographic hash funńions from expander graphs".
In: *Journal of Cryptology* . . Pages – .
DOI: `10.1007/s00145-007-9002-x`.

. Craig G .
"Fully homomorphic encryption using ideal lattices".
In: *Symposium on Ńeory of Computing — STOC '* .
Edited by Michael M . Association for Computing Machinery.
Pages – . DOI: `10.1145/1536414.1536440`.

. European Network of Excellence in Cryptology II.
Yearly report on algoriūms and keysizes. Edited by Nigel P. S .
URL: `http://www.ecrypt.eu.org/documents/D.SPA.13.pdf`.

. Ł or en K , Kazumaro A , Jens F , Arjen K. L ,
Emmanuel T , Joppe W. B , Pierrick G , Alexander K ,
Peter L. M , Dag A. O , Herman te R , Andrey T , and
Paul Z .
"Fańorization of a 768-bit RSA modulus".
In: *Advances in Cryptology — CRYPTO '* . Edited by Tal R . Volume .
Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-642-14623-7_18.

. Gaetan B and Andrew V. S .
"A low-memory algorithm for ŏnding short produń representations in ŏnite groups".
In: *Designs, Codes and Cryptography*. To appear.
DOI: 10.1007/s10623-011-9527-8.

Ꝥ belian ʒ ari'nies

Having e ablished the important role of abelian varieties in modern cryptography, we turn to formally deŏning their properties from a mathematical andpoint.

We will present this theory concisely, in a conceptually elementary way which we believe highlights its e eńiveness. For details, we refer to A , C , D , F , L , N , and V ( ), S ( ), C and S ( ), S ( ), M ( ), and M ( ), in increasing levels of ab rańion.

II.1 General Theory

A V

Fix a perfeń ŏeld k, referred to as the *bńe Ŕeld*, and a su ciently large integer n = `DIMN_MAX`. For any ideal $\mathfrak{I}$ of the ring $k[x] = k[x_1, \dots, x_n]$ of polynomials in n variables with coe cients in k, deŏne the *a ne vari'ny* $\mathcal{V}_{\mathfrak{I}}$ as consi ing, over any extension ŏeld K/k, of the set $\mathcal{V}_{\mathfrak{I}}(K)$ of common zeroes of $\mathfrak{I}$ in K^n called *points* of the variety. H ( ) proved the famous Null ellensatz:

Theorem II.1.1. *When k ś algebraicaŝy closed, ū e large ideal of* $k[x]$ *vanśhing on* $\mathcal{V}_{\mathfrak{I}}(k)$ *ś ū e* radical ideal $\sqrt{\mathfrak{I}}$ *formed by polynomials of which a power lies in* $\mathfrak{I}$.

Ł is puts in bijeńion radical ideals with a ne varieties over algebraically closed ŏelds; computationally, one might therefore use generating sets of $\sqrt{\mathfrak{I}}$ to represent $\mathcal{V}_{\mathfrak{I}}$.

We ŏnd it amusingly convenient to ŏx an integer `DIMN_MAX` large enough so that all varieties we consider are embedded in the projeńive ŕ ace with that large a dimension.

Such varieties are endowed with the *Zariski topology* whose closed sets are subvarieties. Via the Nullstellensatz, the topological notion of irreducibility corresponds to its algebraic counterpart. To avoid unnecessary technical contortions, we shall exclusively consider *absolutely irreducible varieties*, that is, varieties irreducible over an algebraic closure.

Affine varieties lie in the *affine space* $\mathbb{A}(\mathrm{K}) = \mathscr{V}_0(\mathrm{K})$, also written as $\mathbb{A}^n(\mathrm{K})$ when dimension n needs to be made explicit. In many contexts, it instead proves advantageous to:

– work with projective varieties;

– use Galois action to define objects over extension fields.

Over an algebraically closed field $\overline{\mathrm{K}}$, define the *projective space* $\mathbb{P}(\overline{\mathrm{K}})$ (of dimension $n-1$) as the set of lines passing through the origin of $\mathbb{A}(\overline{\mathrm{K}})$, and over any field K as the fixed subset

$$\mathbb{P}(\mathrm{K}) = \mathbb{P}(\overline{\mathrm{K}})^{\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})}$$

under its absolute Galois group. Pragmatically, the projective space $\mathbb{P}(\mathrm{K})$ can be seen as formed by equivalence classes of collinear (non-zero) vectors, which gives the projection

$$x \in \mathbb{A}(\mathrm{K}) \setminus \{0\} \longmapsto \left\{\lambda x : \lambda \in \overline{\mathrm{K}}^{\times}\right\} \in \mathbb{P}(\mathrm{K})$$

Working *in affine coordinates* means representing projective points by distinguished elements of $\mathbb{A}$ (typically, by enforcing $x_0 = 1$; this covers almost all of $\mathbb{P}$ but requires inversions to compute the distinguished element); on the other hand, working *in projective coordinates* means representing projective points as non-unique n-tuples.

Similarly, *projective varieties* are projections of affine varieties invariant under coordinate-wise scalar multiplication: if $\mathfrak{I}$ is a *homogeneous ideal* of $k[x]$, that is, generated by sums of monomials of the same degree, the projective variety $\mathscr{V}_{\mathfrak{I}} \subset \mathbb{P}$ consists of equivalence classes (under scalar multiplication) of the affine variety $\mathscr{V}_{\mathfrak{I}} \subset \mathbb{A}$ endowed with the (quotient) Zariski topology.

From now on, we will exclusively consider absolutely irreducible open subsets of projective varieties, and refer to them simply as *varieties* (they are known to part of the literature as *quasiprojective varieties*); we will always implicitly assume that they are defined over algebraically closed fields, but say that they are *defined* over smaller fields when invariant under their absolute Galois group.

M

Consistent with the topology, *morphisms* are algebraic maps. For the affine space, they form the ring $\mathrm{Hom}(\mathbb{A}, \mathbb{A})$ of n-tuples of n-variate polynomials. If $\mathscr{V}$ and $\mathscr{W}$ are two affine varieties, $\mathrm{Hom}(\mathscr{V}, \mathscr{W})$ consists of those morphisms of $\mathrm{Hom}(\mathbb{A}, \mathbb{A})$ mapping $\mathscr{V}$ to $\mathscr{W}$.

Morphisms of projective varieties can be seen either conceptually, *looking down from* $\mathbb{A}$, as equivalence classes of tuples P of polynomials of $k[x]$ of homogeneous polynomials with the same degree for the relation $P \sim P' \Leftrightarrow \{P_i P'_j - P_j P'_i\} \subset \mathfrak{I}$, or visually, *looking up from specific hyperplanes of* $\mathbb{A}$, as compatible collections of affine morphisms.

Two cases are of particular interest:

- the *coordinate ring* $\mathrm{Hom}(\mathcal{V}_{\mathfrak{I}}, K) \simeq K[x]/\mathfrak{I}$, with addition and scalar multiplication.
- the *endomorphism monoid* $\mathrm{Hom}(\mathcal{V}, \mathcal{V}) = \mathrm{End}(\mathcal{V})$, endowed with composition; later, when we give $\mathcal{V}$ a group law, it will become a ring.

Rational maps are defined similarly to above from tuples of rational functions. Most important are rational maps from a variety $\mathcal{V}$ to a field of definition K, which form its *function field*, denoted $K(\mathcal{V})$. For projective varieties $\mathcal{V} = \mathcal{V}_{\mathfrak{I}}$, it can be explicitly defined as the set of fractions P/Q of homogeneous polynomials in $K[x]$ of the same degree, with $Q \notin \mathfrak{I}$, up to the relation $P/Q \sim P'/Q' \Leftrightarrow PQ' - P'Q \in \mathfrak{I}$.

Various properties can be read off directly from function fields, such as:

Proposition II.1.2. *The Krull dimension of an ideal is equal to the transcendence degree of the function field associated to its variety; it is called the* dimension *of the variety.*

Algebraic extensions have finer indicators: a morphism $\varphi \in \mathrm{Hom}(\mathcal{V}, \mathcal{W})$ induces (by composition on the right) an embedding $\varphi^\star : K(\mathcal{W}) \to K(\mathcal{V})$; the *degree* of φ is the dimension $[K(\mathcal{V}) : \varphi^\star K(\mathcal{W})]$ which is finite when $\varphi(\mathcal{V})$ has the same dimension as $\mathcal{W}$.

A G

Combining algebraic varieties with group structures yields *algebraic groups*:

Definition II.1.3. *An* algebraic group *is an (absolutely irreducible) non-empty algebraic variety endowed with a group law (noted additively) for which the map* $(x,y) \mapsto x - y$ *is a morphism.*

By non-empty, we mean that it must admit one rational point over its base field, so that it contains the neutral element for the group law. An important property of algebraic groups is given by the following algebraic equivalent to the analytic notion of differentiability.

Definition II.1.4. *An irreducible algebraic variety* $\mathcal{V}$ *is* nonsingular *if the quotient of* $\{f \in \bar{k}[\mathcal{V}] : f(P) = 0\}$ *by its square has the same dimension (namely* $g = \dim \mathcal{V}$*) for all* $P \in \mathcal{V}(\bar{k})$.

Algebraic groups are nonsingular varieties; indeed, translation maps $\tau_P : Q \mapsto P + Q$ induce isomorphisms of tangent spaces, whose dimensions are that of the quotients above.

One simply defines *morphisms* of algebraic groups as morphisms of algebraic varieties preserving the group law, and *subgroups* of algebraic groups as subgroups that are closed. From now on, we shall work with categories as a whole: when we consider algebraic groups, morphisms and subgroups will be implicitly understood to be *of algebraic groups* (not just of algebraic varieties).

The proposition below argues that this behaves as expected.

Proposition II.1.5. *Let $\mathscr{H}$ be an (algebraic) normal subgroup of an algebraic group $\mathscr{G}$. The quotient $\mathscr{G}/\mathscr{H}$ has a unique structure of algebraic group such that:*

- *the projection map $\mathscr{G} \to \mathscr{G}/\mathscr{H}$ is a morphism;*
- *all morphisms from $\mathscr{G}$ with kernel containing $\mathscr{H}$ factor through $\mathscr{G}/\mathscr{H}$.*

For instance, the group $\mathrm{GL}_n(\mathrm{K})$ of invertible n-by-n matrices over K is a quasiprojective variety, a closed subvariety of which is $\mathrm{SL}_n(\mathrm{K})$ comprising of matrices with determinant one. In fact, all affine algebraic groups are isomorphic to subgroups of $\mathrm{GL}_n(\mathrm{K})$, and a result of C ( ) ates that the remaining ones are of the type we shall next discuss.

Proposition II.1.6. *Every algebraic group $\mathscr{G}$ has a unique normal subgroup $\mathscr{H}$ isomorphic to an affine variety such that $\mathscr{G}/\mathscr{H}$ is projective and irreducible.*

A V

Definition II.1.7. Abelian varieties *are irreducible projective algebraic groups.*

Most of the rich structure of abelian varieties stems from the projectiveness condition (completeness, an algebraic equivalent to compactness, could equivalently be required).

Proposition II.1.8. *Any algebraic map from an abelian variety to another is a morphism (of algebraic groups) composed with a translation.*

In other words, morphisms of algebraic varieties are essentially morphisms of abelian varieties; this means that abelian varieties are entirely characterized by their geometry. This is a crucial fact with the notable consequence that *abelian varieties are commutative groups*; indeed, since the algebraic map $x \mapsto -x$ fixes the neutral element, it is a morphism, which implies the commutativity.

Since abelian varieties $\mathscr{A}$ are commutative, they admit quotients by any closed subgroups $\mathscr{H}$. We will later be interested in the case of finite subgroups $\mathscr{H}$, which are evidently closed: in that case, the dimension of the quotient $\mathscr{A}/\mathscr{H}$ is the same as that of the variety $\mathscr{A}$, and as we will see later, many other invariants are preserved.

As a further re ri ń ion to prevent unnecessary contortions, we henceforth assume, unless otherwise ated, that all abelian varieties we consider are *absolutely simple*, that is, do not contain any proper nontrivial abelian subvariety over an algebraic closure.

11.2 Practical Settings

Let us now focus on two types of base ŏeld: ŏnite ŏelds, over which abelian varieties admit e cient representations, and the complex numbers, over which their relationship to tori yields a rich theory, part of which descends to ŏnite ŏelds.

F F

Let $\mathscr{A}$ be an abelian variety deŏned over a ŏnite ŏeld $k = \mathbb{F}_q$; its *z'na funňion*

$$Z_{\mathscr{A}}(t) = \exp \sum_{n=1}^{\infty} \#\mathscr{A}\left(\mathbb{F}_{q^n}\right) \frac{t^n}{n}$$

encodes its number of points, on which W ( ) proved the following.

Theorem 11.2.1. *Ń e z'na funňion of a dimension-g abelian vari'ny $\mathscr{A}$ ś of ū e form*

$$Z_{\mathscr{A}}(t) = \prod_{n=0}^{2g} P_n(t)^{(-1)^{n+1}}$$

for some polynomials $P_n \in \mathbb{Z}[t]$ *whose complex zeroes have absolute value* $q^{-n/2}$.

Ł is con rains cardinalities of abelian varieties. To better see this, consider the *FrobeniŬ endomorphśm* π, which ańs over any ŏeld extension $K/\mathbb{F}_q$ by raising coordinates of points of $\mathscr{A}(K)$ to the q^{th} power; it ŏxes ju $\mathscr{A}(\mathbb{F}_q)$, so we have $\#\mathscr{A}(\mathbb{F}_q) = \deg(1-\pi)$.

Any endomorphism φ of an abelian variety of dimension g has a monic charańeri ic polynomial $P \in \mathbb{Z}[t]$ of degree $2g$ such that $\deg Q(\varphi) = \mathrm{Res}(P, Q)$ for all polynomials $Q \in \mathbb{Z}[t]$. For the particular Frobenius endomorphism, denoting by χ_π its charańeri ic polynomial, we obtain

$$\#\mathscr{A}(\mathbb{F}_{q^n}) = \mathrm{Res}_u\left(\chi_\pi(u), u^n - 1\right)$$

which makes computing χ_π equivalent to counting points on $\mathscr{A}$ over g di inń ŏeld extensions of the base ŏeld. Transcribing the theorem above to χ_π yields the following.

Corollary 11.2.2. *Ń e complex roots of* χ_π *aŝ have absolute value* $\sqrt{q}$, *and ū e polynomial* $P_{2g}(t)$ *in ū e z'na funňion ś* $\prod\left(1-\alpha t\right)$ *where* α *ranges over produňs of* $2g$ *dśtinň such roots.*

Generalizing an algorithm of S ( ), P ( ) proved that for any fixed dimension g all the above can be computed in polynomial time in the size of the base field.

Theorem 11.2.3. *The zeta function of an abelian variety defined over* $\mathbb{F}_q$ *can be computed in polynomial time in* $\log(q)$ *where the implied exponent depends on the dimension of the projective space where it is embedded, and on the degrees of its defining equations and group law equations.*

This result is mostly of theoretical interest. Improvements on the algorithm of S ( ) by A and E have made it possible to count points on abelian varieties of dimension $g = 1$ far beyond cryptographic range; for $g = 2$, the practicality of point counting methods on varieties of cryptographic size was only recently demonstrated by G and S ( ) who used an extension of the algorithm of S ( ).

From now on, we shall regard the dimension g as being fixed in complexity statements, so asymptotic analyses focus on behavior with respect to the base field; this is partly motivated by the fact that only $g = 1$ and $g = 2$ are cases of cryptographic interest.

C N

We have noted that abelian varieties are nonsingular. Over $\mathbb{C}$, abelian varieties are therefore connected compact Lie groups, which are well-understood objects; such a variety $\mathscr{A}$ has the analytic structure of a complex torus: since the exponential map folds its tangent space onto $\mathscr{A}$, there is an isomorphism of Lie groups $\mathscr{A} \simeq \mathbb{C}^g/\Lambda$ where $\Lambda = \ker(\exp_{\mathscr{A}})$ is a *lattice* of $\mathbb{C}^g$, that is, a discrete subgroup of full rank.

Similarly to the algebraic case, holomorphic maps between complex tori are just group morphisms composed by translations. Holomorphic morphisms φ from a complex torus $\mathbb{T} = \mathbb{C}^g/\Lambda$ to another $\mathbb{T}' = \mathbb{C}^{g'}/\Lambda'$ are induced by $\mathbb{C}$-linear maps, denoted φ as well, from $\mathbb{C}^g$ to $\mathbb{C}^{g'}$ satisfying $\varphi(\Lambda) \subset \Lambda'$. Hence, as $\mathbb{Z}$-module, $\mathrm{Hom}(\mathbb{T}, \mathbb{T}')$ has rank at most $4gg'$; this implies that $\mathrm{End}(\mathscr{A})$ is a torsion-free $\mathbb{Z}$-algebra of dimension at most $(2g)^2$.

Even if complex abelian varieties have the analytic structure of tori, conversely, not all complex tori correspond to abelian varieties, although those that do are precisely known:

Proposition 11.2.4. *Define the* Siegel upper half-space $\mathbb{H}^g$ *as the set of g-by-g symmetric matrices with positive definite imaginary part. Complex tori* $\mathbb{C}^g/\Lambda$ *corresponding to abelian varieties are exactly those whose lattice* Λ *can be put under the form* $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ *for some matrix* $\Omega \in \mathbb{H}^g$.

P

Many results on abelian varieties over finite fields exploit *reduction* from characteristic zero fields k, that is, consider varieties arising through maps $k \to k/\mathfrak{p}$ for prime ideals $\mathfrak{p}$ of k.

For in ance, the bound of H ( ) which ates that one-dimensional abelian varieties $\mathscr{A}$ deŏned over $\mathbb{F}_q$ satisfy

$$\left|q+1-\#\mathscr{A}(\mathbb{F}_q)\right| \leqslant 2\sqrt{q}$$

can be extended, for varieties arising as reduńions from charańeri ic zero, into a precise description of the di ribution of cardinalities: the Sato–Tate conjeńure. Note that recent work of T ( ) comes close to proving it.

Conjeĉture II.2.5. *L'n $\mathscr{A}$ be a non-empty abelian vari'ny of dimension one deŔned over ūe rŅionals wiū* $\mathrm{End}(\mathscr{A}) \simeq \mathbb{Z}$. *Ńe ńymptotic dśtribution, ń ūe prime p goes to inŔnity, of*

$$\arccos\left(\frac{p+1-\#\mathrm{A}(\mathbb{F}_p)}{2\sqrt{p}}\right)$$

ś uniform on $[0;\pi]$ *where* $\#\mathscr{A}(\mathbb{F}_p)$ *denotes ūe number of points of ūe reduňion of $\mathscr{A}$ Ņ p.*

When $g > 1$, abelian varieties have inŏnite automorphism groups over algebraically closed ŏelds. For more rigidity, we bundle them with a projeńive embedding or, rather, the following (simpler) analytic analog.

Definition II.2.6. *L'n* $\mathscr{A} \simeq \mathbb{C}^g/\Lambda$ *be a complex torŬ. A* polarization *of $\mathscr{A}$ ś a positive deŔnite Hermitian form $\mathscr{P}$ on $\mathbb{C}^g$ sŅśfying* $\mathscr{P}(\Lambda,\Lambda) \subset \mathbb{Z}$. *It ś* principal *if its d'nerminant ś inl·ertible, or equivalently if ūere ś no* $x \notin \Lambda$ *sŅśfying* $\mathscr{P}(\Lambda, x) \subset \mathbb{Z}$.

Principaŝy polarized abelian vari'nies are pairs $(\mathscr{A},\mathscr{P})$ whose morphisms $\varphi : (\mathscr{A},\mathscr{P}) \to (\mathscr{A}',\mathscr{P}')$ are required to preserve polarizations in the sense that $\varphi^\star\mathscr{P}' = \lambda\mathscr{P}$ for some positive $\lambda \in \mathbb{Q}$. W ( ) showed that this has the intended e eń:

Proposition II.2.7. *Polarized abelian vari'nies have a Ŕnite automorphśm group.*

For in ance, on the torus $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ for $\Omega \in \mathbb{H}^g$, there is a natural polarization $\mathscr{P}(u,v) = \mathrm{E}(iu,v) + i\mathrm{E}(u,v)$ where the Riemann form E is expressed, on the block basis $(e_i)(\Omega e_i)$, by the block matrix

$$\begin{pmatrix} 0 & \mathrm{Id} \\ -\mathrm{Id} & 0 \end{pmatrix}$$

Proposition II.2.8. *Two mŅrices Ω and Ω' of ūe Siegel upper half-ş ace $\mathbb{H}^g$ yield śomorphic principaŝy polarized abelian vari'nies if and only if ūey are conjugŅe under ūe aňion*

$$\begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}) : \Omega \longmapsto \left(\mathrm{A}\Omega + \mathrm{B}\right)\left(\mathrm{C}\Omega + \mathrm{D}\right)^{-1}.$$

Polarizations are needed in actual computations, as efficient arithmetic (via theta functions or Jacobian varieties) relies on them. Worse, it is nontrivial to determine whether the varieties corresponding to two theta coordinates are isomorphic, disregarding polarizations.

Before moving on, we emphasize once more that, in dimension one, all varieties admit a unique principal polarization — so they can hopefully be forgotten altogether.

J V

Theorem 11.2.9. *Up to isomorphism, there is a unique abelian variety through which any morphism from a given algebraic variety $\mathscr{V}$ to an abelian variety factors. It is the* Albanese variety *of $\mathscr{V}$.*

General Albanese varieties are hardly practical: they have no effective group law, and are not naturally endowed with a principal polarization, so there is no simple manner to identify them such as invariants (as we will see below). Cryptography is only concerned with the following subclass, on which our exposition shall now focus.

Proposition 11.2.10. *Abelian varieties of dimension one or two are Jacobian varieties of hyperelliptic curves.*

Before defining hyperelliptic curves, let us briefly discuss *Jacobian varieties*: these are just Albanese varieties of *algebraic curves*, that is, one-dimensional algebraic varieties. The Jacobian variety $\mathrm{Jac}(\mathscr{C})$ of a curve $\mathscr{C}$ has an explicit group structure: denote by Div^0 the submodule of degree-zero divisors of the free $\mathbb{Z}$-module generated by points of $\mathscr{C}$, that is, formal sums of points whose coefficients add up to zero; it contains Princ, the set of sums of zeroes and poles (counted with multiplicities) of non-zero elements of the function field.

Proposition 11.2.11. $\mathrm{Jac}(\mathscr{C})$ *has the group structure of the quotient* $\mathrm{Div}^0 / \mathrm{Princ}$.

We can say much more for hyperelliptic curves; for this, we assume $\mathrm{char}\, k \neq 2$.

Definition 11.2.12. *Curves $\mathscr{C}$ of the form $y^2 = f(x)$, for some squarefree polynomial f of degree $2g+1$ or $2g+2$, are called* hyperelliptic, *and g is known as the* genus *of $\mathscr{C}$.*

By the theorem of R ( ) and R ( ), g is also the dimension of $\mathrm{Jac}(\mathscr{C})$. *In the case that $g = 1$, they are known as* elliptic curves, *and verify* $\mathrm{Jac}(\mathscr{C}) \simeq \mathscr{C}$.

When $\deg(f)$ is odd, there is a unique projective, non-affine point (with coordinate $z = 0$); this *point at infinity* ∞ is often used as a distinguished projective point. By R ( ) and R ( ) each divisor class then has a unique *reduced* representative of the form $\sum(P_i - \infty)$ for at most g affine points $P_i \in \mathscr{C}$, none of which is conjugate to another under the *hyperelliptic involution* $(x, y) \mapsto (x, -y)$.

Assume, for simplicity, that the points $P_i = (x_i, y_i)$ are di inń. Ł e divisor $\sum(P_i - \infty)$ can be represented by a pair of polynomials (u, v) satisfying

$$u(x) = \prod(x - x_i), \quad v(x_i) = y_i.$$

It can be checked that the P_i lie on $\mathscr{C}$ by verifying that $u | v^2 - f$. In this representation, the group law is given by (assuming u_0 and u_1 have no common root)

$$(u_0, v_0) + (u_1, v_1) = \left(u_0 u_1, (u_2^{-1} \bmod v_2) u_2 v_1 + (u_1^{-1} \bmod u_2) u_1 v_2\right).$$

To *reduce* the output to a unique representative, C ( ) iterates the transformation

$$(u, v) \mapsto (u', v') \quad \text{with } u' = \frac{1}{\mathrm{lc}(f - v^2)} \frac{f - v^2}{u} \text{ and } v' = -v \bmod u'$$

while $\deg(u) \leqslant g$, where $\mathrm{lc}(\cdot)$ denotes the leading coe cient. Ł is gives $\mathrm{Jac}(\mathscr{C})$ an e cient group law, and an algebraic ruńure. Additionally, the image of the map $(P_i) \in \mathscr{C}^{g-1} \longmapsto \sum(P_i - \infty)$ is a subvariety of dimension $g - 1$ that is the zero-locus of certain theta funńions which naturally endow the Jacobian variety with a principal polarization $\mathscr{P}$.

T ( ) showed that this comprises all the information from the original curve:

Theorem 11.2.13. *Up to śomorphśm, ūe polarized abelian vari'ny* $(\mathrm{Jac}\,\mathscr{C}, \mathscr{P})$ *d'nermines ūe curve* $\mathscr{C}$.

Moduli ş aces are varieties whose points represent isomorphism classes of a given type of variety (we will soon discuss invariants); complementing the proposition above, we have:

ūe moduli dimension of	genus-g hyperelliptic curves	*ś*	$2g - 1$
"	genus-g curves	"	$3(g - 1)$, or 1 if $g = 1$
"	abelian varieties of dimension g	"	$g(g + 1)/2$

Ł e moduli ŕ ace dimension is the same for Jacobian varieties and their underlying curves. For $g = 3$, abelian varieties are Jacobian varieties, but not all of hyperelliptic curves.

11.3 Pairings

T S

Ł e center of the endomorphism ring $\mathrm{End}(\mathscr{A})$ of an abelian variety $\mathscr{A}$ of dimension g always contains a subring isomorphic to $\mathbb{Z}$ formed by *scalar multiplicŅion maps*:

$$[n] : P \in \mathscr{A} \longmapsto nP = \underbrace{P + \cdots + P}_{n \text{ times}}$$

for every integer n. Over an algebraic closure, the kernel of $[n]$ is the *full n-torsion subgroup* $\mathscr{A}[n]$; its structure is well understood:

Theorem II.3.1. *The degree of $[n]$ is n^{2g}. It is separable when n is coprime to $p = \operatorname{char} k$; then $\mathscr{A}[n] \simeq (\mathbb{Z}/n)^{2g}$. When n is a power of p, then $\mathscr{A}[n] \simeq \mathbb{Z}/n^r$ where $r \leqslant g$ is called the p-rank of $\mathscr{A}$.*

The generic case is that of *ordinary* abelian varieties which have p-rank g: the moduli dimension of non-ordinary varieties is strictly smaller. Unless explicitly stated, all abelian varieties will now be assumed ordinary (this is crucial for the next chapter).

We will later compute ℓ-torsion subgroups (for primes ℓ) of abelian varieties $\mathscr{A}$ defined over finite fields $\mathbb{F}_q$. The *embedding degree* $e_{\mathscr{A}}(\ell)$, which is the extension degree of the smallest field over which the points of $\mathscr{A}[\ell]$ are defined, is the primary cost factor of this process.

If χ is the characteristic polynomial of the Frobenius endomorphism π of $\mathscr{A}$, the morphism $\chi(\pi)$ obviously vanishes on $\mathscr{A}[\ell]$; as this only depends on the class of χ in $(\mathbb{Z}/\ell)[x]$, the embedding degree $e(\ell)$ must divide the multiplicative order of $x \in (\mathbb{Z}/\ell)[x]/(\chi)$. Consequently, it is bounded by ℓ^{2g}.

When points can be drawn uniformly at random from $\mathscr{A}(k^{e(\ell)})$, a basis for $\mathscr{A}[\ell]$ can be found by taking random points, multiplying them by the cofactor of ℓ^∞ in $\#\mathscr{A}(k^{e(\ell)})$, and iteratively applying $[\ell]$ until a point of ℓ-torsion is found, possibly lifting points already found along their preimage under $[\ell]$. The lifting process can either use simple baby-step giant-step computations in $\mathscr{A}[\ell]$, or faster discrete logarithm methods in $k^{e(\ell)}$ via the pairing. For a fixed g, the whole method uses polynomially many operations in ℓ; it will be described in detail in the second half of this thesis.

G P

Definition II.3.2. *A* pairing *is a non-degenerate bilinear map $\Psi : \mathrm{G}^2 \to \mathrm{H}$, where G and H are abelian groups.*

Strictly speaking, pairings can be defined on modules over any ring; but from a cryptographic standpoint, nothing of value is lost by restricting to $\mathbb{Z}$-modules. On the other hand, cryptographic use requires additional properties:

: Given $(x, y) \in \mathrm{G}^2$, the pairing $\Psi(x, y)$ is easily evaluated.
: Given $z \in \mathrm{H}$, a preimage $(x, y) \in \Psi^{-1}(z)$ is hard to find.

These terms could be given a rigorous meaning by considering a sequence of pairings $\Psi_i : \mathrm{G}_i^2 \to \mathrm{H}_i$, and requesting that there exists an algorithm for evaluating Ψ_i in polynomial time in $\log(\#\mathrm{G}_i)$ and that no algorithm finds preimages of Ψ_i in subexponential time on a positive frańion of H_i; however, we prefer to use the simpler and down-to-earth notion of computational infeasibility.

Similarly to the discrete logarithm problem, the pairing inversion problem has many variants, such as bilinear analogs to the computational and decisional Di e–Hellman problems, or inversion problems where one of the parameters is ŏxed, not all of which are rińly equivalent to the pairing inversion problem itself. We refer to G , H c, and V - ( ) for a discussion of these problems.

Out of all known e eńive pairings, only those that arise from abelian varieties satisfy the conditions above. In fań, the *problem of pairing inl·ersion*, that is, of inverting the map Ψ, appears to be extremely di cult for such pairings. Ł eir cryptographic use therefore involves relying on a new hypothesis (alongside the hardness of the discrete logarithm problem) but they provide elliptic and hyperelliptic cryptography with a unique ruńure, which has led to the development of many novel features.

E P

In ruńional pairing examples include scalar produńs of veńor ŕ aces, and, if $(R, +, \times)$ is a ring, the multiplication map from $(R, +)^2$ to $(R, \times)$. A more intere ing example is

$$\left(xy, x'y'\right) \in \left((\mathbb{Z}/n)^{2g}\right)^2 \longmapsto \exp\left(\frac{2i\pi}{n}\left(\widehat{x}y' - \widehat{y}x'\right)\right)$$

where xy denotes the concatenation of the row veńors $x, y \in (\mathbb{Z}/n)^g$, and $\widehat{x}$ denotes the transpose of x. Ł is ańually is the general form of the Weil pairing expressed on a sympleńic basis of the n-torsion subgroup of a complex torus.

None is suitable for cryptographic use, as they are typically easy to invert; currently, the only known cryptographic pairings arise from abelian varieties:

Let $\mathscr{A}$ be the Jacobian variety $\mathrm{Jac}(\mathscr{C})$ of a curve $\mathscr{C}$ of genus g, which we further assume to be a hyperelliptic curve deŏned over a ŏnite ŏeld. Recall that the full n-torsion subgroup $\mathscr{A}[n]$ is isomorphic to $(\mathbb{Z}/n)^{2g}$ when n is coprime to the ambient charańeri ic. For cryptographic reasons we choose n to be prime, and deŏne the map

$$\Psi_{\mathrm{Weil}} : \begin{cases} \mathscr{A}[n] \times \widehat{\mathscr{A}}[n] & \longrightarrow & \mu_n \subset \overline{k}^{\times} \\ (P, Q) & \longmapsto & f_P(Q)/f_Q(P) \end{cases}$$

where μ_n is the group of n^{th} roots of unity, and f_P and f_Q are funńions of $\overline{k}(\mathscr{A})$ with disjoint support whose sum of zeroes and poles are the principal divisors nP and nQ, re ŕ eńively. Its evaluation at a divisor $Q = \sum Q_i$ is explicitly $\prod f(Q_i)$.

Theorem 11.3.3. Ψ_{Weil} *ś a Galoś-inl·ariant antśymm'nric pairing caŝed ūe* Weil pairing.

Mo of the proof relies on the reciprocity of W ( ).

When $\mathscr{A}$ is principally polarized, the polarization gives an isomorphism $\mathscr{A} \simeq \widehat{\mathscr{A}}$, and the pairing can therefore be deŏned on $\mathscr{A}[n] \times \mathscr{A}[n]$.

In the case of elliptic curves, points P of the variety are of the form $R - \infty$ where R is a point of the curve or the point at inŏnity itself. M ( ) noted that the funńion f_i whose sum of zeroes is the principal divisor $iR - [i]R - (i-1)\infty$ can be computed iteratively by setting $f_{i+j} = f_i \cdot f_j \cdot u/v$, where u is the line containing $[i]R$ and $[j]R$ (it vanishes at $[i]R$, $[j]R$, and $-[i+j]R$, and has a pole of order 3 at ∞) and v the vertical line passing through $[i+j]R$ (it vanishes at $[i+j]R$ and $-[i+j]R$, and has a pole of order 2 at ∞).

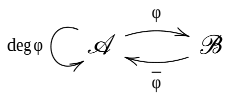
Łjis yields an algorithm for evaluating the Weil pairing of elliptic curves which can also

11.4 Isogenies

A I

Definition 11.4.1. *An* isogeny *is a surjective morphism of abelian varieties* $\varphi : \mathscr{A} \to \mathscr{B}$ *with finite kernel. It is* separable *if the corresponding function field extension* $k(\mathscr{A})/\varphi^*(k(\mathscr{B}))$ *is.*

When $\varphi : \mathscr{A} \to \mathscr{B}$ is an isogeny, the abelian varieties $\mathscr{A}$ and $\mathscr{B}$ are said to be *isogenous*; this is an equivalence relation since there then exists a *dual isogeny* $\overline{\varphi} : \mathscr{B} \to \mathscr{A}$, of the same degree n, which is simply the multiplication-by-n map of $\mathscr{A}$ factored through φ.



Proposition 11.4.2. *If* $\mathscr{H}$ *is the kernel of a separable isogeny* $\varphi : \mathscr{A} \to \mathscr{B}$*, then* φ *is the projection map under the isomorphism* $\mathscr{B} \simeq \mathscr{A}/\mathscr{H}$*; in particular, we have* $\deg(\varphi) = \#\mathscr{H}$.

The group structure of $\mathscr{H}$ *is called the* type *of* φ.

From now on, the word "isogeny" should implicitly mean "separable isogeny;" this is the case for all isogenies whose degree is coprime to the characteristic of the base field.

Since composition of isogenies corresponds to inclusion of subgroups, and the latter are abelian, we deduce that all isogenies can be written as the composition of isogenies of prime degree. In dimension $g > 1$, although there is currently no known method for computing general isogenies of type $\mathbb{Z}/\ell$ where ℓ is a prime, there are algorithms for evaluating isogenies of type $(\mathbb{Z}/\ell)^g$ which we call ℓ-*isogenies*.

Recall that we assume isogenies between principally polarized abelian varieties $\mathscr{A}$ to preserve polarizations. The induced polarization on $\mathscr{A}/\mathscr{H}$ for a finite subgroup $\mathscr{H}$ is principal if and only if $\mathscr{H}$ is a maximal isotropic subgroup for the Weil pairing; when we compute isogenies from their kernel, we will first start by enumerating all such subgroups.

H –T T

Over finite fields, there is a bijection between isogeny classes of abelian varieties and their zeta functions. We have already explained the relationship between the zeta function of an abelian variety and the characteristic polynomial of its Frobenius endomorphism, and the following description of isogeny classes is due to T ( ).

Theorem 11.4.3. *Two varieties are isogenous if and only if their respective Frobenius endomorphisms have the same characteristic polynomial.*

A monic polynomial with integer coe cients and $2g$ complex roots, each of absolute value $\sqrt{q}$, is called a *q-Weil polynomial*. Recall that this is the case of the charańeri ic polynomial of the Frobenius endomorphism. As a reciprocal to that atement, H ( ) proved:

Theorem 11.4.4. *Each q-Weil polynomial ś ūe charaňerśtic polynomial of ūe FrobeniŬ endomorphśm of a cerŪin simple ordinary abelian vari'ny of dimension g deŔned over* $\mathbb{F}_q$.

T ( ) presented these two theorems in a combined way, and this has become known as Honda–Tate theory.

Ł e next chapter will be concerned with an *explicit* form of this theory which aims at con-ruńing explicit abelian varieties whose Frobenius endomorphisms have prescribed charańeri ic polynomials. Ł is enforces certain properties on the abelian variety, such as the cardinality.

E I

For elliptic curves $\mathscr{E}$, V ( ) gave explicit formulas for computing an isogeny $\varphi : \mathscr{E} \to \mathscr{E}'$ deŏned by its kernel $\ker(\varphi) \subset \mathscr{E}$: if x, y are coordinates in which an a ne equation for $\mathscr{E}$ is $y^2 = f(x)$, then there exi coordinates X, Y in which an equation for $\mathscr{E}'$ has the form $Y^2 = g(X)$ and the isogeny can be written as

$$\varphi : P \in \mathscr{E} \longmapsto \begin{pmatrix} X_{\varphi(P)} = \sum x_{P+Q} - x_Q \\ Y_{\varphi(P)} = \sum y_{P+Q} - y_Q \end{pmatrix}$$

where the sums range over all points Q of $\ker(\varphi)$, with the convention that $x_\infty = y_\infty = 0$.

Ł is relies heavily on properties of the Weier rass coordinates for elliptic curves, and a higher-dimensional analog was only found recently by L and R ( ), and later made prańical by C and R ( ); it relies on the ruńure of theta functions, which we now brieŒy describe.

Geometric invariants identify isomorphism classes of abelian varieties. For in ance, isomorphism classes of elliptic curves are identiŏed, over an algebraic closure, by the canonical *j-inl·ariant*. It is e eńive as $j(\mathscr{E})$ is a rational funńion in the coe cients of a Weier rass equation for $\mathscr{E}$, and conversely the coe cients of such an equation are rational funńions in $j(\mathscr{E})$.

In arbitrary dimension, a sy em of invariants for principally polarized abelian varieties is given by *ū'na con ants*, which not only identify the isomorphism class of a variety but also part of its torsion. Ł eta con ants are the con ant terms of *ū'na funňions* which yields a convenient *coordinŅe sy em* for points on the variety it identiŏes.

In the particular case of abelian varieties of dimension $g < 4$, which are all, up to isomorphism, Jacobian varieties of algebraic curves, invariants can be expressed, via Torelli's theorem, on the curves themselves, as funńions of the coe cients of their equations. For $g = 2$, a popular set of invariants are the *IgŬa inl·ariants*, which consi s of 10 coordinates (this bears some redundancy since the dimension of the moduli ŕ ace is 3); they can be e -ciently computed from the equation of a curve, but conversely, to retrieve such an equation from the invariants themselves, a ŕ eciöc method of M ( ) is required.

Ł e relationship between the invariants of a curve and the theta con ants of its Jacobian variety are given by formulas of T ( ).

Let $\mathscr{A} \simeq \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ be a complex torus with $\Omega \in \mathbb{H}^g$. Deŏne the *ū'na funňions*

$$\Theta_{a,b}^{\mathscr{A}} : z \in \mathbb{C}^g \longmapsto \sum_{(u+a)\in\mathbb{Z}^g} \exp i\pi \left(\frac{1}{n}\widehat{u}\Omega u + 2\widehat{u}(z+b)\right)$$

where a and b are veńors of $\mathbb{Q}^g$ and $\widehat{u}$ denotes the tranŕ ose of u. I ( ) proved:

Theorem 11.4.5. *Fix an integer $n > 2$. Ńe* theta con ants $\Theta_{a,b}^{\mathscr{A}}(0)$

the complex number with ju enough precision so as to identify its integer coe cients. Recently, B , L , and S ( ) demon rated the competitiveness of a method based on the Chinese remainder theorem which exploits the ruńure of isogeny volcanoes that we will udy later.

Ł e higher-dimensional case is not as raightforward: G ( ) described an analog con ruńion for $g = 2$, and the computation of explicit polynomials was later done by D ( ) and improved by B and L ( ). However, the height of the polynomials (Φ^i_ℓ) makes their use prohibitive; currently, ate-of-the-art algorithms for explicitly evaluating isogenies remain a fa er alternative.

We note that this di erence between elliptic curves and higher-dimensional abelian varieties is the main reason why point counting algorithms are much fa er for the former than for the latter.

References

. Bernhard R .
" Ł eorie der Abel'schen Funńionen".
In: *Journal für die reine und angewandte MṆhemṆik* . . Pages – .
DOI: `10.1515/crll.1857.54.115`.

. Gu av R .
"Über die Anzahl der willkürlichen Con anten in algebraischen Funńionen".
In: *Journal für die reine und angewandte MṆhemṆik* . . Pages – .
DOI: `10.1515/crll.1865.64.372`.

. Carl J. T .
"Beitrag zur Be immung von $\vartheta(0, 0, \ldots, 0)$ durch die Klassenmoduln algebraischer Funńionen".
In: *Journal für die reine und angewandte MṆhemṆik* . . Pages – .
DOI: `10.1515/crll.1870.71.201`.

. David H .
"Über die vollen Invariantensy eme".
In: *MṆhemṆśche Annalen* . . Pages – . DOI: `10.1007/BF01444162`.

. Ruggiero T .
"Sulle varietà di Jacobi".
In: *Rendiconti deŝa Reale Accademia Nazionale dei Lincei* . . Pages – .

. Helmut H .
“Über die Kongruenzzetafunktionen”.
In: *Sitzungsberichte der Preußśchen Akademie der WśsenschaŚen* . Pages – .

. André W .
“Sur les fonńions algébriques à corps de con antes ŏni”.
In: *Comptes RendŬ de l’Académie des Sciences de Parś* . Pages – .

. André W .
Sur les courbes algébriques ’n les variétés qui s’en déduśent. Volume .
Ańualités Scientiŏques et Indu rielles .
Publications de l’In itut de Mathématique de l’Université de Strasbourg.

. André W .
“On the theory of complex multiplication”.
In: *InternŅional Symposium on Algebraic Number Ńeory.* Tokyo and Nikko.
Science Council of Japan. Pages – .

. Claude C .
“Une démon ration d’un théorème sur les groupes algébriques”.
In: *Journal de MŅhémŅiques Pures ’n Appliquées* . Pages – .

. Jun-Ichi I .
“Arithmetic variety of moduli for genus two”.
In: *Annals of MŅhemŅics* . . Pages – . DOI: `10.2307/1970233`.

. John T .
“Endomorphisms of abelian varieties over ŏnite ŏelds”.
In: *Inŀentiones mŅhemŅicae* . . Pages – . DOI: `10.1007/BF01404549`.

. Taira H .
“Isogeny classes of abelian varieties over ŏnite ŏelds”.
In: *Journal of ūe MŅhemŅical Soci’ny of Japan* . – . Pages – .
DOI: `10.2969/jmsj/02010083`.

. John T .
“Classes d’isogénie des variétés abéliennes sur un corps ŏni (d’après T. Honda)”.
In: *Séminaire Bourbaki.* Volume . . Pages – .

. David M .
Abelian Vari’nies. Volume .
Tata In itute of Fundamental Research Studies in Mathematics.
Oxford University Press.

. Jacques V .
"Isogénies entre courbes elliptiques".
In: *Comptes RendŬ de l'Académie des Sciences de Parś*. A . Pages – .

. Igor R. S .
Bńic Algebraic Geom'nry. Volume .
Grundlehren der mathematischen WissenschaŔen. Springer.

. René S .
"Elliptic curves over őnite őelds and the computation of square roots mod p".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: `10.2307/2007968`.

. Gary C and Joseph H. S (editors).
Ariū m'nic Geom'nry. Springer. ISBN: - - - .

. Vińor S. M .
Short programs for funňions on curves. Unpublished.
URL: `http://crypto.stanford.edu/miller/`.

. David G. C .
"Computing in the Jacobian of a hyperelliptic curve".
In: *MŅhemŅics of CompuŪtion* . . Pages – . DOI: `10.2307/2007876`.

. Jonathan P .
"Frobenius maps of abelian varieties and őnding roots of unity in őnite őelds".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: `10.2307/2008445`.

. Jean-François M .
"Con ruńion de courbes de genre 2 à partir de leurs modules".
In: *E eňive m'nhods in algebraic geom'nry — MEGA '* .
Edited by Teo M and Carlo T . Volume . Progress in Mathematics.
Birkhäuser. Pages – .

. James S. M .
Abelian Vari'nies.
URL: `http://www.jmilne.org/math/CourseNotes/av.html`.

. Goro S .
Abelian Vari'nies wiū Complex MultiplicŅion and Modular Funňions.
Princeton University Press. ISBN: - - - .

. Pierrick G .
"Algorithmique des courbes hyperelliptiques et applications à la cryptologie".
PhD thesis. École Polytechnique.
URL: http://hal.inria.fr/tel-00514848/PDF/these.final.pdf.

. Antoine J .
"A one round protocol for tripartite Di e–Hellman".
In: *Algori ū mic Number Ń eory — ANTS-IV.* Edited by Wieb B .
Volume . Le ń ure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/10722028_23.

. Roberto M. A , Henri C , Chri ophe D , Gerhard F ,
Tanja L , Kim N , and Frederik V .
Handbook of Eŝiptic and Hypereŝiptic Curve Cryptography.
Discrete Mathematics and its Applications. Chapman & Hall.
ISBN: - - - .

. Régis D .
"Moyenne arithmetico-géométrique, suites de Brochardt et applications".
PhD thesis. École Polytechnique.
URL: http://www.lix.polytechnique.fr/Labo/Regis.
Dupont/these_soutenance.pdf.

. Steven D. G , Florian H c, and Frederik V .
"A ŕ e ńs of pairing inversion".
In: *IEEE Transańions on InformŅion Ń eory* . . Pages – .
DOI: 10.1109/TIT.2008.2006431.

. Richard T .
"Automorphy for some *l*-adic liŔs of automorphic mod *l* Galois representations, II".
In: *PublicŅions MŅhémŅiques de l'In itut des Hautes Études ScientiŔques* . .
Pages – . DOI: 10.1007/s10240-008-0015-2.

. Reinier B and Kri in L .
"Modular polynomials for genus ". In: *London MŅhemŅical Soci'ny Journal of CompuŪtion and MŅhemŅics* . Pages – .
DOI: 10.1112/S1461157000001546.

. Andreas E .
"Computing modular polynomials in quasi-linear time".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: 10.1090/S0025-5718-09-02199-1.

. David L and Damien R .
Computing śogenies b’nween abelian vari’nies. arXiv.org: 1001.2016.

. Reinier B , Kri in L , and Andrew V. S .
Modular polynomials via śogeny l·olcanoes.
To appear in *MŅhemŅics of CompuŪtion*. arXiv.org: 1001.0402.

. Pierrick G and Éric S .
GenŬ point counting over prime Ŕelds. HAL-INRIA: 00542650.

. David L and Damien R .
“E cient pairing computation with theta funńions”.
In: *Algoriū mic Number Ń eory — ANTS-IX*.
Edited by Guillaume H , François M , and Emmanuel T .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-642-14518-6_21.

. Romain C and Damien R .
Computing (ℓ, ℓ)*-śogenies in polynomial time on Jacobians of genŬ curves.*
IACR ePrint: 2011/143.

Ƨomplex Ʊ ultiplicŅion

Ł e theory of complex multiplication describes endomorphism rings of abelian varieties; this thesis will inve igate two of its applications, inverse of each other:

– con ruńing abelian varieties equipped with e ciently computable pairings;

– computing the endomorphism ring of prescribed abelian varieties.

Ł ere are many facets to complex multiplication theory; here, while trying to be somewhat general, we will focus on e eńive a ŕ eńs in the case of dimension $g = 1, 2$, which are of primary intere to cryptography. For details, we refer to C ( ) for $g = 1$, to S ( ) for $g = 2$, and otherwise to S ( ), C and S ( ), and M ( ).

III.1 Endomorphism Rings

A V C M

Let us ŏr consider the endomorphism ring ruńure of abelian varieties; via the following theorem of P and W ( ), it su ces to consider simple varieties.

Theorem III.1.1. *Every abelian vari'ny ś śogenoŬ to a produň of powers of non-śogenoŬ simple ones.*

Ł e endomorphism ring of a perfe ń power $\mathscr{A}^m$ is naturally the matrix algebra of dimension m^2 over the endomorphism ring of $\mathscr{A}$; therefore, the endomorphism ring of a produ ń $\prod \mathscr{A}_i^{m_i}$ of non-isogenous simple abelian varieties $\mathscr{A}_i$ is $\prod \mathrm{Mat}_{m_i}(\mathrm{End}\, \mathscr{A}_i)$.

Since isogenies need not preserve endomorphism rings, the above does not completely rule out the case of non-simple varieties. Nevertheless, we will now assume that $\mathscr{A}$ is a simple abelian variety of dimension g. Its endomorphism ring $\mathrm{End}(\mathscr{A})$ contains at least the scalar multiplication maps, which form a subring isomorphic to $\mathbb{Z}$. To better comprehend the ring $\mathrm{End}(\mathscr{A})$, we first consider the algebra $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$: if it contains a field K of degree $2g$, the variety $\mathscr{A}$ is said to have *complex multiplication* by the number field K or, more precisely, by the order $\mathrm{K} \cap \mathrm{End}(\mathscr{A})$. Over number fields, this is a rare situation; but over finite fields, all ordinary abelian varieties have complex multiplication.

Recall that, over finite fields, the Frobenius endomorphism π of a dimension-g abelian variety $\mathscr{A}$ admits a monic characteristic polynomial χ_φ of degree $2g$, and that this polynomial uniquely identifies the isogeny class of $\mathscr{A}$. T ( ) further established the following, of which a proof can be found in W and M ( ).

Theorem III.1.2. *If $\mathscr{A}$ is a simple abelian variety, the characteristic polynomial of its Frobenius endomorphism π is some power m^e of its minimal polynomial, whence $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ is a division algebra of dimension $2eg$, and its center K is the field $\mathbb{Q}(\pi) \simeq \mathbb{Q}[x]/(m(x))$ of degree $2g/e$.*

The number field K is known as the *complex multiplication field* of $\mathscr{A}$. The structure of such fields can easily be investigated since they are quotients of $\mathbb{Q}[x]$ by q-Weil polynomials $\chi_\pi(x)$: under the embedding to $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$, the field K is an extension by the polynomial $\mathrm{X}^2 - (\pi + \overline{\pi})\mathrm{X} + q$ of the totally real field $\mathrm{K}_+ = \mathbb{Q}(\pi + \overline{\pi})$. Therefore, complex multiplication fields are totally imaginary quadratic extensions of totally real number fields K_+ of degree g.

So far, we have not been too concerned about fields of definition; we will continue not to be, due to the following proposition.

Proposition III.1.3. *Endomorphism rings of simple ordinary abelian varieties defined over finite base fields are unaffected by base field extensions.*

C T C M

Complex multiplication also concerns complex tori, and due to their simpler structure it yields a rich theory; many results concerning abelian varieties over finite fields are reductions of results on complex tori. For now, we assume that the base field is $k = \mathbb{C}$.

Let us first fix a particular embedding ι of the complex multiplication field K in $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$. The exponential map sends $\mathscr{A}$ to a complex torus $\mathbb{C}^g/\Lambda$, and ι to an embedding $\iota' : \mathrm{K} \to \mathrm{End}(\mathbb{C}^g)$. Using representation theory, one can prove that, up to isomorphisms of $\mathbb{C}^g$, the map ι' is of the form

$$\iota_\Phi : \begin{cases} \mathrm{K} & \longrightarrow & \mathbb{C}^g \\ x & \longmapsto & \big(\varphi(x)\big)_{\varphi\in\Phi} \end{cases}$$

for a certain set Φ of g di inń embeddings of K in $\mathbb{C}$, no two of which are complex conjugate of each other, so that all $2g$ embeddings are in $\Phi \sqcup \overline{\Phi}$. Ł is set Φ is called the *complex multiplicŅion type* of the abelian variety $\mathscr{A}$.

Isogenies tran ŕ ort the embedding ι and type Φ from one variety to the next; by the following result, found for in ance as Proposition . of M ( ), ŏxing one is equivalent to ŏxing the other.

Proposition III.1.4. *Ńere ś a bŜeňion b'nween ū e s'n of śogeny clńses of simple ordinary pairs* $(\mathscr{A}, \iota)$ *and ū e s'n of śomorphśm clńses of primitive types* (K, Φ).

We will now consider abelian varieties $\mathscr{A}$ endowed with an embedding ι or, equivalently, a complex multiplication type Φ.

Conversely, a complex torus with complex multiplication by a prescribed complex multiplication ŏeld K and type Φ can be con ruńed as follows. Let $\mathfrak{a}$ be an integral ideal of K; the g-tuple of embeddings Φ maps it to a certain lattice of $\mathbb{C}^g$ and we may consider the complex torus $\mathbb{C}^g/\Phi(\mathfrak{a})$. To obtain a polarization as a Riemann form E on it, take an algebraic integer ξ that generates K/K_+, whose imaginary part is totally positive, and whose square is a totally negative element of K_+, then deŏne E by

$$E_\Phi^\xi\left(\Phi(x), \Phi(y)\right) = \operatorname{tr}\left(\xi \cdot \overline{x} \cdot y\right)$$

which takes integral values on $\Phi(\mathfrak{a})^2$ and thus induces a polarization on the complex torus $\mathbb{C}^g/\Phi(\mathfrak{a})$; it is obviously principal since ξ is invertible. Integral elements x of K can be seen ańing as endomorphisms of the torus by

$$(z_i) \in \mathbb{C}^g \longmapsto \left(z_i \varphi_i(x)\right)$$

where an ordering on the embeddings φ of Φ has been ŏxed by indexing them by $i \in \{1, \dots, g\}$. Since di inń orderings yield isomorphic complex tori, Φ can be simply thought of as a set.

Other transformations of the type yield isomorphic varieties as well. In the case (where we assume to be) of simple varieties, we have:

Theorem III.1.5. *Aŝ principaŝy polarized complex tori wiū complex multiplicŅion by a ring of integ* [illegible] µ

C M O

The complex multiplication field K embedded in $\mathbb{Q}\otimes\mathrm{End}(\mathscr{A})$ is an important invariant; however, it fails to capture the exact isomorphism type of $\mathrm{End}(\mathscr{A})$, which is precisely what the order $\mathscr{O} = \mathrm{K}\cap\mathrm{End}(\mathscr{A})$ does.

Generally-speaking, an *order* $\mathscr{O}$ in a number field K is a lattice that is also a subring of the ring of integers $\mathscr{O}_{\mathrm{K}}$ — the latter is therefore commonly called the *maximal order*. In our context, there is also a *minimal order* due to the following result of W ( ).

Proposition III.1.6. *Let* K *be the complex multiplication field of some ordinary abelian variety defined over a finite field* k *with Frobenius endomorphism* π. *The orders of* K *containing* $\mathbb{Z}[\pi,\overline{\pi}]$ *are exactly those that arise as endomorphism rings of abelian varieties defined over* k *with complex multiplication by* K.

The *Verschiebung endomorphism* $\overline{\pi}$ can also be written as $q\pi^{-1}$, since Theorem . . will show that the degree of an endomorphism is the norm of the corresponding number field element.

Now consider an abelian variety $\mathscr{A}$ defined over a number field k. If $\mathfrak{p}$ is a discrete place of k, its residue field $k/\mathfrak{p}$ is finite, and we might obtain an abelian variety $\mathscr{A}$ over $k/\mathfrak{p}$, of the same dimension as $\mathscr{A}$, by pushing $\mathscr{A}$ forward through the quotient map $k \to k/\mathfrak{p}$; when we do, we say that $\mathscr{A}$ has *good reduction* at the prime $\mathfrak{p}$. Mo things independent from $\mathfrak{p}$ reduce nicely:

Proposition III.1.7. *Let* $\mathscr{A}$ *and* $\mathscr{B}$ *be two abelian varieties of the same dimension defined over a number field with good reduction at some discrete place* $\mathfrak{p}$. *The natural map* $\mathrm{Hom}(\mathscr{A},\mathscr{B}) \to \mathrm{Hom}(\mathscr{A},\mathscr{B})$ *is injective and preserves the degree of isogenies.*

Specialized to an abelian variety $\mathscr{A} = \mathscr{B}$ with complex multiplication, this states that reduction leaves the complex multiplication field unchanged and can only make the endomorphism ring larger.

When the reduction φ of an isogeny $\varphi \in \mathrm{End}(\mathscr{A})$ is separable, that is, whenever its degree is coprime to $\mathfrak{p}$, then the reduction map $\ker(\varphi) \to \ker(\varphi)$ is a bijection.

N -O V

For completeness, we briefly address the case of non-ordinary abelian varieties $\mathscr{A}$ over a finite field $\mathbb{F}_q$; the characteristic polynomial of the Frobenius endomorphism is then some proper power m^e with $e > 1$ of its minimal polynomial.

Contrary to the ordinary case, the endomorphism ring of non-ordinary abelian varieties might be smaller over the base field than it is over an algebraic closure.

For an elliptic curve, not being ordinary coincides with being *supersingular*, and also with the characteristic of the base field dividing the integer $\pi + \overline{\pi}$. Then, all endomorphisms are defined over $\mathbb{F}_q$ if and only if q is a square and $\pi = \pm\sqrt{q}$.

Over fields with square cardinalities, there are thus two isogeny classes of supersingular curves with all endomorphisms defined, corresponding to the two q-Weil numbers $\pm\sqrt{q}$. Over a quadratic extension, those two become isogenous, but another isogeny class appears. Supersingular curves with not all endomorphisms defined can form up to three more isogeny classes. This has been rigorously studied by W ( ), and to conclude we summarize his result concerning endomorphism rings of supersingular curves.

Proposition III.1.8. *Endomorphism rings of supersingular elliptic curves are*

- *if all endomorphisms are defined: the maximal orders;*
- *otherwise: the p-maximal orders containing* π*;*

in the quaternion $\mathbb{Q}$*-algebra ramified at infinity and p (the characteristic of the base field).*

III.2 Orders and Ideals

For a moment, let us turn to topics of algebraic number theory with a computational flavor; they will later be put to use when we need to apply complex multiplication theory.

A O

Orders of a number field K are lattices (that is, discrete subgroups of full rank) with an induced ring structure; inclusion therefore yields a partial *order* on orders of K, where the italicized word is meant in the set-theoretic sense. From now on, we consider orders of a fixed complex multiplication field K, and refer to them just as "orders"; they are contained in the maximal order $\mathfrak{M} = \mathcal{O}_K$, and we are particularly interested in those containing a certain *minimal order* $\mathfrak{m}$ of the form $\mathbb{Z}[\pi,\overline{\pi}]$. Since $K = \mathbb{Q}(\pi)$, there are finitely many such orders.

This induces a finite *lattice* structure (again, in the in the set-theoretic sense) and we will often be speaking about orders located above or below from others, meaning respectively that they contain or are contained in others. This structure extends to ideals: assuming $\mathcal{O} \subset \mathcal{O}'$ are two orders, we have natural maps

$$\begin{array}{ccc} \mathfrak{I}(\mathcal{O}') & & \mathfrak{I}(\mathcal{O}) \\ \mathfrak{a} & \longmapsto & \mathfrak{a} \cap \mathcal{O} \\ \mathfrak{b}\mathcal{O}' & \longleftarrow & \mathfrak{b} \end{array}$$

and while the latter is a right inverse to the former, the converse is not true in general.

A more satisfying setting arises when we restrict to *invertible ideals* of an order $\mathcal{O}$, that is, fractional ideals $\mathfrak{a}$ for which there exists another fractional ideal $\mathfrak{b}$ satisfying $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. All non-zero fractional ideals of the maximal order are invertible, but as we go down the lattice of orders, fewer and fewer are. To measure this notion of depth, we introduce the conductor, which measures how far $\mathcal{O}$ is from its integral closure $\mathfrak{M}$.

Definition III.2.1. *The* conductor *of an order $\mathcal{O}$ is the ideal* $\mathfrak{f}_{\mathcal{O}} = \{x \in \mathfrak{M} : x\mathfrak{M} \subset \mathcal{O}\}$.

The conductor gives a sufficient condition for invertibility: prime ideals that are coprime to $\mathfrak{f}_{\mathcal{O}}$ are invertible in $\mathcal{O}$. Conversely, up to principal ideals, all invertible ideals are equivalent to one coprime to the conductor. As a result, invertible ideals coprime to the conductor always have a unique decomposition into invertible prime ideals.

I C G

Similarly to class groups of ring of integers, ideal class groups can be constructed from general orders. This construction resembles that of Jacobian varieties in terms of divisors, but the resulting group differs in various subtle aspects.

Definition III.2.2. *The* Picard group *of an order $\mathcal{O}$, denoted by* $\mathrm{Pic}(\mathcal{O})$, *is the quotient group* $\mathfrak{I}(\mathcal{O}) / \mathrm{Princ}(\mathcal{O})$ *of invertible ideals by principal ideals; it is finite and abelian.*

The Picard group of an order $\mathcal{O}$ with conductor $\mathfrak{f}$ is related to that of the maximal order $\mathfrak{M} = \mathcal{O}_K$ via the exact sequence

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \mathfrak{M}^\times \longrightarrow (\mathfrak{M}/\mathfrak{f})^\times / (\mathcal{O}/\mathfrak{f})^\times \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\mathfrak{M}) \longrightarrow 1$$

which shows that Picard groups grow roughly linearly in the norm of the conductor $\mathfrak{f}$; more precisely, the sequence yields the following formula (which generalizes the well-known explicit formula for imaginary quadratic orders) for the *class number*:

$$\#\mathrm{Pic}(\mathcal{O}) = \frac{\#\mathrm{Pic}(\mathfrak{M})}{[\mathfrak{M}^\times : \mathcal{O}^\times]} \frac{\#(\mathfrak{M}/\mathfrak{f})^\times}{\#(\mathcal{O}/\mathfrak{f})^\times}$$

The asymptotic growth of the class number of the maximal order $h = \#\mathrm{Pic}(\mathfrak{M})$ obeys the following conjecture of S ( ) proved by B ( ).

Theorem III.2.3. *For any sequence of number fields* K *whose class number, regulator, and discriminant we respectively denote by* h, R, *and* Δ, *we have:*

$$\frac{\log h + \log R}{\log \sqrt{|\Delta|}} \longrightarrow 1 \quad \text{and} \quad \frac{[K : \mathbb{Q}]}{\log |\Delta|} \longrightarrow 0.$$

And we note that, for the ŏelds K we are mo intere ed in, namely quadratic and quartic complex multiplication ŏelds, the regulator is re ŕ eńively $R = 1$ and $R = O(\log|\Delta|)$.

Picard groups are compatible with the lattice-of-orders ruńure:

Proposition III.2.4. *L'n $\mathcal{O} \subset \mathcal{O}'$ be two orders. Ńe map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}'$, for inl·ertible ideals $\mathfrak{a}$ of $\mathcal{O}$ coprime to $\mathfrak{f}_{\mathcal{O}}$, induces a surjeňive morphśm of Picard groups.*

Ł erefore, if some set $\mathfrak{B}$ of ideals of the minimal order $\mathfrak{m}$ generates its Picard group, it can be mapped into generating sets for each order above $\mathfrak{m}$. We form the free abelian group $\mathbb{Z}^{\mathfrak{B}}$, and let $\Lambda_{\mathcal{O}}$ denote the *lŅtice of relŅions of $\mathcal{O}$*, consi ing of tuples $(\lambda)_{\mathfrak{B}}$ for which the produń $\prod_{\mathfrak{B}}(\mathfrak{b}\mathcal{O})^{\lambda}$ is a principal ideal of $\mathcal{O}$. Ł is gives a description of the Picard group as

$$\operatorname{Pic}(\mathcal{O}) \simeq \mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}}$$

and when one order is contained in another, their lattices of relations are too.

C O

To li all possible endomorphism rings, that is, all orders containing $\mathfrak{m} = \mathbb{Z}[\pi,\overline{\pi}]$, one could simply focus on the lattice ruńure: subgroups of the quotient group $\mathfrak{M}/\mathfrak{m}$ can easily be enumerated, and each yields a lattice that contains $\mathfrak{m}$; elementary techniques can then te whether such a lattice is closed under multiplication.

Ł is approach is ine cient as mo lattices are not orders, but also inadequate since there might be exponentially many orders above $\mathfrak{m}$. We can bound the conduńor gap as follows:

Lemma III.2.5. *Ńe index $[\mathfrak{M} : \mathfrak{m}]$ ś bounded Řom abol·e by $2^{g(g-1)}q^{g^2/2}$, where q ś ūe norm of π and $2g$ its degree.*

Proof. Recall that $[\mathfrak{M} : \mathfrak{m}]$ is the square root of $\operatorname{disc}(\mathfrak{m})/\operatorname{disc}(\mathfrak{M})$. Ł e discriminant of the maximal order $\mathfrak{M}$ can be small so we simply bound that of the minimal order $\mathfrak{m}$ using

$$|\operatorname{disc}(\mathfrak{m})| = |\operatorname{disc}(\mathbb{Z}[\pi])| \Big/ \left[\mathbb{Z}[\pi,\overline{\pi}] : \mathbb{Z}[\pi]\right]^2 .$$

Ł e numerator can be bounded by $\left(2\sqrt{q}\right)^{2g(2g-1)}$ since χ_π is a q-Weil polynomial of degree $2g$. For the denominator, we have $\left[\mathbb{Z}[\pi,\overline{\pi}] : \mathbb{Z}[\pi]\right] = q^{\frac{g(g-1)}{2}}$ from which the result follows. □

In ead of enumerating all orders, we will navigate the lattice of orders and locate the endomorphism ring using complex multiplication theory. Ł e proposition below shows that it su ces to *go up* or *down* by small powers of primes. Due to the lemma above, only polynomially many descending eps in g and $\log(q)$ are needed to reach $\mathfrak{m}$ from $\mathfrak{M}$.

Proposition III.2.6. *Consider two orders $\mathcal{O}' \subset \mathcal{O}$ of relative index divisible by a prime ℓ. There exists an order $\mathcal{O}''$ in between whose index in $\mathcal{O}$ is in $\{\ell, \ell^2, \ldots, \ell^{2g-1}\}$ where $2g = \deg K$.*

To prove this, let $\mathcal{O}''$ be the order generated by $\ell\mathcal{O}$ and $\mathcal{O}'$: since $\ell\mathcal{O}$ has index ℓ^{2g} in $\mathcal{O}$ and both contain $\mathbb{Z}$, its index in $\mathcal{O}$, and therefore also that of $\mathcal{O}''$, must divide ℓ^{2g-1}.

Consider now the problem of *going down*, that is, enumerating all orders contained in a prescribed order $\mathcal{O}$ with index n (to *go up* the process would be entirely equivalent).

In discussions with E, we devised a simple method to enumerate all orders contained in a prescribed order $\mathcal{O}$ with index n. The integer n should preferably be a small prime power to limit the size of the output; this amounts to considering the lattice of orders locally at this prime. When we only consider endomorphism rings of principally polarized abelian varieties, we can further restrict to those orders that are closed under complex conjugation.

Fix a $\mathbb{Z}$-module basis (ω_i) of $\mathcal{O}$ so that each sublattice is uniquely identified by a basis $(\alpha_j = \sum a_{ij}\omega_i)$ in Hermite normal form, meaning that the integral matrix (a_{ij}) is upper triangular, has non-zero coefficients on the diagonal, and satisfies $a_{ij} < a_{ii}$ for $i \neq j$; see Chapter . of C ( ) for details. Such a sublattice is an order if it contains all products

$$\alpha_j \alpha_{j'} = \sum_{i,i'} a_{ij} a_{i'j'} \omega_i \omega_{i'} = \sum_k \underbrace{\left(\sum_{i,i'} a_{ij} a_{i'j'} m_k^{ii'} \right)}_{b_k^{jj'}(a)} \omega_k$$

where the vector $m^{ii'}$ expresses $\omega_i \omega_{i'}$ on the basis (ω_k); this vector and the polynomial $b_k^{jj'}$ only depend on $\mathcal{O}$. Therefore, a is an order if and only if, for all j and j', the preimage of the vector $b^{jj'}$ by the matrix a has integral coordinates; for sublattices of index $\det(a) = n$, this gives:

Proposition III.2.7. *All orders contained in $\mathcal{O}$ with index n correspond to solutions of the polynomial system $(n \cdot a)^{-1} b^{jj'} = 0 \bmod n^{2g}\mathbb{Z}^{2g}$ in the coefficients of the matrix a.*

Unless there are 0 or $\Omega(n)$ such orders, this system is nonsingular and its solutions can be listed by a Gröbner basis algorithm in time polynomial in $\log n$ albeit exponential in g.

C C G

Fix an order $\mathcal{O}$ and consider computing its Picard group; this requires a generating set of ideals for $\mathrm{Pic}(\mathcal{O})$, an efficient ideal multiplication algorithm, and a way of finding a distinguished representative of the class of a prescribed ideal, which we call *reducing* an ideal. Under the generalized Riemann hypothesis (GRH), B ( ) solved the first problem:

Theorem III.2.8. *Assume the GRH and let $\mathcal{O}$ be the ring of integers of a number field of discriminant Δ. The class group* $\mathrm{Pic}(\mathcal{O})$ *is generated by prime ideals of norm at most* $12\log^2|\Delta|$.

Note that a less explicit, but more precise result of J , M , and V ( ), which also assumes the GRH, implies that, for any $\varepsilon > 0$, the class group of any order $\mathcal{O}$ is generated by prime ideals of norm less than $O(\log^{2+\varepsilon}|\Delta|)$, where $\Delta = \mathrm{disc}(\mathcal{O})$.

Let $\mathfrak{B}$ be the set of prime ideals with norm less than some bound B, and define

$$\sigma_{\mathcal{O}} : \begin{cases} \mathbb{Z}^{\mathfrak{B}} & \longrightarrow & \mathrm{Pic}(\mathcal{O}) \\ n & \longmapsto & \prod_{\in\mathfrak{B}} \mathfrak{p}^{n_{\mathfrak{p}}} \end{cases}$$

By the results above, when B is big enough, the map $\sigma_{\mathcal{O}}$ is surjective and therefore we have

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}}$$

where the lattice $\Lambda_{\mathcal{O}}$ is the kernel of $\sigma_{\mathcal{O}}$

III.3 Plain Complex Multiplication

We have seen that endomorphism rings of ordinary abelian varieties are isomorphic to orders in number fields, and have then considered their ideals from a computational standpoint. Let us now explain how these ideals can be seen as acting as isogenies.

This aspect of complex multiplication theory will be referred to as the *plain action*, as opposed to the *polarized action* to be discussed later. This section, does not assume that isogenies preserve any polarization structure of abelian varieties, and borrows many results of W ( ).

F F S

Let $\mathscr{O}$ be an order isomorphic to the endomorphism ring of a simple ordinary abelian variety $\mathscr{A}$ of dimension g defined over a finite field $\mathbb{F}_q$. We additionally consider an embedding $\iota : \mathrm{K} \to \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ of the number field of $\mathscr{O}$; its elements are then seen as endomorphisms of $\mathscr{A}$. An isogeny φ sends the variety $\mathscr{A}$ to the variety $\mathscr{B} = \varphi(\mathscr{A})$, and also maps an embedding ι for $\mathscr{A}$ to an embedding for $\mathscr{B}$ given as $\varphi(\iota) = \frac{1}{\deg \varphi} \varphi \circ \iota \circ \widehat{\varphi}$ where $\widehat{\varphi}$ denotes the dual isogeny. In fact, we have:

Proposition III.3.1. *If ι is an embedding of* K *into* $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$, *all other embeddings ι' are of the form $\varphi(\iota)$ for some endomorphism φ of $\mathscr{A}$.*

Let $\mathscr{A}$ be such an abelian variety endowed with an embedding ι of $\mathscr{O}$ into its endomorphism ring, let $\mathfrak{a}$ be an invertible ideal of $\mathscr{O}$, and consider the isogeny $\varphi_{\mathfrak{a}} : \mathscr{A} \to \mathscr{A} / \ker(\varphi_{\mathfrak{a}})$ with kernel

$$\ker\left(\varphi_{\mathfrak{a}}\right) = \bigcap_{\alpha \in \mathfrak{a}} \ker\left(\iota(\alpha)\right).$$

For instance, if $\mathfrak{a}$ is a principal ideal (α), then the kernel of $\varphi_{\mathfrak{a}}$ is simply that of α; therefore, $\varphi_{\mathfrak{a}}$ is nothing but an endomorphism whose separable part coincides with that of α (recall that the totally inseparable part of an isogeny is not characterized by its kernel).

Now consider the composition of two such isogenies: let $\mathscr{A}$ be an abelian variety, $\mathfrak{a}$ be an invertible ideal of $\mathscr{O} = \iota^{-1}(\mathrm{End}\,\mathscr{A})$, and denote the corresponding isogeny by $\varphi_{\mathfrak{a}} : \mathscr{A} \to \mathscr{B}$; then, let $\mathfrak{b}$ be an invertible element of $\varphi(\iota)^{-1}(\mathrm{End}\,\mathscr{B})$, and denote the corresponding isogeny by $\varphi_{\mathfrak{b}} : \mathscr{B} \to \mathscr{C}$; in that situation, the isogeny $\varphi_{\mathfrak{b}} \circ \varphi_{\mathfrak{a}}$ corresponds canonically to $\varphi_{\mathfrak{a}\mathfrak{b}} : \mathscr{A} \to \mathscr{C}$. In simple terms, composing isogenies corresponds to multiplying ideals.

As a consequence, there is a well-defined map

$$\mathfrak{a} \in \mathrm{Pic}(\mathscr{O}) : \mathscr{A} \in \mathrm{AV}_{\mathscr{O}}(k) \longmapsto \varphi_{\mathfrak{a}}(\mathscr{A}) \in \mathrm{AV}(k)$$

where $\mathrm{AV}(k)$ denotes the set of isomorphism classes of abelian varieties defined over k, and $\mathrm{AV}_{\mathcal{O}}(k)$ the subset of such classes with endomorphism ring $\mathcal{O}$. Since the above is an isogeny, the complex multiplication is unchanged and we have $\mathbb{Q} \otimes \mathrm{End}(\mathscr{A}) = \mathbb{Q} \otimes \mathrm{End}(\varphi_{\mathfrak{a}}(\mathscr{A}))$; note that, for elliptic curves, $\mathrm{End}(\varphi_{\mathfrak{a}}(\mathscr{A}))$ is actually always equal to $\mathrm{End}(\mathscr{A})$ as Proposition . . will show, but in general we might only have $\mathrm{End}\,\mathscr{A} \subset \mathrm{End}(\varphi_{\mathfrak{a}}(\mathscr{A}))$.

C E T

For elliptic curves, W ( ) proved that the image of the map above is actually $\mathrm{AV}_{\mathcal{O}}(k)$, and that the action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(k)$ this defines is transitive, which means that for any elliptic curve $\mathscr{A}$ with endomorphism ring $\mathcal{O}$, the map $\mathfrak{a} \mapsto \varphi_{\mathfrak{a}}(\mathscr{A})$ induces a bijection between $\mathrm{Pic}(\mathcal{O})$ and $\mathrm{AV}_{\mathcal{O}}(k)$. The specific approach that he used then enabled him to establish a similar result for (non-polarized) abelian varieties. Here, let us describe a more standard way of seeing this on elliptic curves, using complex tori.

In the elliptic case, the use of complex tori to obtain results over finite fields greatly exploits the following lifting theorem of D ( ).

Theorem III.3.2. *Let α be an endomorphism of an elliptic curve $\mathscr{A}$ defined over a finite field $\mathbb{F}_p$. There exists an endomorphism β of some abelian variety $\mathscr{B}$ defined over a certain number field which, modulo some prime $\mathfrak{p}$ above p of good reduction, reduces precisely to $\alpha \in \mathrm{End}(\mathscr{A})$.*

In the case where $\mathrm{End}(\mathscr{A}) = \mathbb{Z}[\alpha]$, the variety $\mathscr{B}$ of the above theorem has $\mathbb{Z}[\beta]$ as endomorphism ring and reduction induces an isomorphism $\mathrm{End}(\mathscr{B}) \simeq \mathrm{End}(\mathscr{A})$, since we saw earlier that endomorphism rings of abelian varieties defined over number fields are mapped injectively into that of their good reductions at prime ideals. Endomorphism rings of ordinary elliptic curves are always of the form $\mathbb{Z}[\alpha]$, so in this case there always exist lifts with the same endomorphism ring.

Conversely, for the ordinary case, we need to reduce modulo primes totally split in $\mathcal{O}$:

Proposition III.3.3. *Let $\mathscr{A}$ be an elliptic curve with endomorphism ring $\mathcal{O}$ defined over a number field. Take an unramified prime $\mathfrak{p}$, and let $p = \mathfrak{p} \cap \mathbb{Z}$. Then:*

- *if p splits completely in $\mathcal{O}$, then the reduction $\mathscr{A}$ is ordinary and defined over $\mathbb{F}_p$.*
- *if p is inert in $\mathcal{O}$, then the reduction $\mathscr{A}$ is supersingular and defined over $\mathbb{F}_{p^2}$.*

Now, over the complex numbers, an elliptic curve with endomorphism ring $\mathcal{O}$ always corresponds to a complex torus $\mathbb{C}/\mathfrak{b}$ where $\mathfrak{b}$ is a certain ideal of $\mathcal{O}$. The action of invertible ideals $\mathfrak{a}$ of $\mathcal{O}$ on $\mathrm{AV}_{\mathcal{O}}(\mathbb{C})$ can then be seen as

$$\mathfrak{a} : \mathbb{C}/\mathfrak{b} \in \mathrm{AV}_{\mathcal{O}}(\mathbb{C}) \longmapsto \mathbb{C}/(\mathfrak{a}^{-1}\mathfrak{b}) \in \mathrm{AV}_{\mathcal{O}}(\mathbb{C}).$$

This action is obviously transitive, and two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ act identically if and only if they are homothetic, that is, if and only if they belong to the same class of $\mathrm{Pic}(\mathcal{O})$. Therefore, this action factors through the Picard group into a faithful and transitive action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(\mathbb{C})$; modulo prime ideals $\mathfrak{p}$ of norm p, it reduces to the action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(\mathbb{F}_p)$.

Theorem III.3.4. *Let $\mathcal{O}$ be an imaginary quadratic order. For elliptic curves defined over a finite field k, the above defines a faithful and transitive action of $\mathrm{Pic}(\mathcal{O})$ onto $\mathrm{AV}_{\mathcal{O}}(k)$.*

We must finally mention that this action can also be seen on *invariants* of elliptic curves: if $\mathscr{B} \in \mathrm{AV}_{\mathcal{O}}(\mathbb{C})$, its invariant $j(\mathscr{B})$ lies in the *ring class field* of $\mathcal{O}$, which is an abelian extension of $\mathrm{K} = \mathbb{Q}(\mathcal{O})$ with Galois group $\mathrm{Pic}(\mathcal{O})$. The action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(\mathbb{C})$ is then that of the Galois group via the Artin symbol.

G A V

The situation in higher dimension is far from being as nice as in the elliptic case. Certain properties nevertheless hold as they should, such as the following one of G ( ).

Theorem III.3.5. *Let $\mathscr{A}$ be a simple ordinary abelian variety defined over a finite field; if $\mathfrak{a}$ is an invertible ideal of its endomorphism ring, the degree of the isogeny $\varphi_{\mathfrak{a}}$ is the norm of $\mathfrak{a}$.*

The transitivity of the action of the Picard group, which would generalize the result on elliptic curves above, has only been shown to hold in the case that the endomorphism ring of $\mathscr{A}$ is maximal by W ( ); to prove this, he first argued that all invertible ideals are, in his terminology, *kernel ideals*, which implies the following.

Theorem III.3.6. *Let $\mathscr{A}$ be a simple ordinary abelian variety defined over a finite field k, and assume that $\mathrm{End}(\mathscr{A})$ is a maximal order $\mathcal{O}_{\mathrm{K}}$; then, for any invertible ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathrm{K}}$:*

- *the endomorphism ring of $\varphi_{\mathfrak{a}}(\mathscr{A})$ is exactly that of $\mathscr{A}$.*
- *the induced action of $\mathrm{Pic}(\mathcal{O}_{\mathrm{K}})$ on $\mathrm{AV}_{\mathcal{O}_{\mathrm{K}}}(k)$ is faithful and transitive.*

The number of isomorphism classes of simple ordinary abelian varieties with endomorphism ring some maximal order $\mathcal{O}_{\mathrm{K}}$ can thus be estimated using the conjecture of S ( ) proved by B ( ); as a direct consequence of Lemma . . . , we have

$$\mathrm{disc}(\mathbb{Z}[\pi,\overline{\pi}]) < 2^{2g(g-1)} q^{g^2}$$

which gives, as g is fixed and q goes to infinity, the asymptotic behavior

$$\#\,\mathrm{AV}_{\mathcal{O}_{\mathrm{K}}}(\mathbb{F}_q) = \#\,\mathrm{Pic}(\mathcal{O}_{\mathrm{K}}) < q^{g^2/2+o(1)}.$$

E A

In our application, we wish to use the above theory for maximal orders as well as non-maximal ones. Therefore, we rely on the following consequence of the results above, combined with the observation that, if the norm of an invertible ideal $\mathfrak{a}$ is coprime to ℓ, since it is also the degree of the isogeny $\varphi_{\mathfrak{a}}$, then the index $[\mathrm{End}(\varphi_{\mathfrak{a}}\mathscr{A}) : \mathrm{End}(\mathscr{A})]$ cannot be divisible by ℓ. Note that we proved the contrapositive statement earlier.

Proposition III.3.7. *Let $\mathscr{A}$ be a simple ordinary abelian variety defined over a finite field k, let π be its Frobenius endomorphism, let $K = \mathbb{Q}(\pi)$, and let $\mathcal{O} \subset K$ be its endomorphism ring.*

The invertible ideals of $\mathcal{O}$ of norm coprime to the discriminant of $\mathbb{Z}[\pi,\overline{\pi}]$ act on $\mathrm{AV}_{\mathcal{O}}(k)$ via isogenies of degree their norm, and this defines a faithful action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(k)$.

To make this proposition effective, we need to compute the isogeny $\varphi_{\mathfrak{a}}$. Denote its degree by ℓ; since $\ell = \mathrm{N}(\mathfrak{a})$, we can start by enumerating all subgroups of cardinality ℓ of the full ℓ-torsion subgroup $\mathscr{A}[\ell]$. Recall than even when $\varphi_{\mathfrak{a}}$ is rational, the points of its kernel need not be individually, but they are collectively invariant under the Galois action. Still, we need a practical way of telling $\varphi_{\mathfrak{a}}$ apart from other isogenies of degree ℓ.

The improvements of A and E to the elliptic curve point counting method of S ( ) exploit certain aspects of complex multiplication theory. In particular, they give a means to determine which specific isogeny of degree ℓ corresponds to $\varphi_{\mathfrak{a}}$. It was also written as Stage of the algorithm by G , H , and S ( ).

This result actually holds for general abelian varieties, which follows elementarily from the theory of Tate modules (from which most of the results that we stated above are derived); we therefore state it in its full generality.

Proposition III.3.8. *Let $\mathscr{A}$ be a simple ordinary abelian variety defined over a finite field, $\mathcal{O}$ its endomorphism ring and $\pi \in \mathcal{O}$ the element corresponding to its Frobenius endomorphism.*

Let $\mathfrak{a}$ be an invertible prime ideal of $\mathcal{O}$, written as $\ell\mathcal{O} + u(\pi)\mathcal{O}$, where ℓ is its norm and u is an irreducible factor modulo ℓ of the characteristic polynomial χ_π of the primitive element π. Assume that ℓ is coprime to the discriminant of $\mathbb{Z}[\pi,\overline{\pi}]$.

Then, the characteristic polynomial of the Frobenius endomorphism acting on $\ker(\varphi_{\mathfrak{a}})$ is u.

This proposition cannot be readily applied to non-prime ideals $\mathfrak{a}$, but we will explain later how this issue can be dealt with.

III.4 Polarized Complex Multiplication

In practical computations, abelian varieties are represented as Jacobian varieties of hyperelliptic curves or as theta-coordinates. Since both naturally work with principal polarizations, complex multiplication theory needs to be adapted to take this extra structure into account. Most of this theory originates from S and T ( ).

As in the *plain* case, we start by considering complex multiplication fields before focusing on the specific endomorphism ring order and the action of its ideals.

R F M

Recall that if $\mathscr{A}$ is an ordinary abelian variety of dimension g, its complex multiplication field $K = \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ is a totally imaginary quadratic extension of a totally real number field K_+ of degree g, and that a *complex multiplication type* on K is a set of embeddings of K in $\mathbb{C}$ satisfying $\Phi \sqcup \overline{\Phi} = \mathrm{Hom}(K, \mathbb{C})$ where the union is disjoint.

Here, there is actually no need to involve $\mathbb{C}$, or even the algebraic numbers $\overline{\mathbb{Q}}$, since the image of any embedding of K is necessarily contained in its normal closure K^c. From now on, we therefore consider complex multiplication types given as sets of embeddings of K to its normal closure; this is equivalent and allows for a simpler exposition.

Definition III.4.1. *Let* Φ *be a type of* K. *The* reflex field K^r *is the fixed field of*

$$\left\{\sigma \in \mathrm{Gal}\left(K^c, \mathbb{Q}\right) : \Phi = \Phi \circ \sigma\right\},$$

the automorphisms of K^c *leaving* Φ *globally invariant. It admits a unique* reflex type Φ^r *which is the restriction of automorphisms of* K^c *whose inverses yield* Φ *when restricted to* K, *that is,*

$$\left\{\varphi \in \mathrm{Aut}\left(K^c\right) : \varphi|_{K^r} \in \Phi^r\right\} = \left\{\varphi^{-1} \in \mathrm{Aut}\left(K^c\right) : \varphi|_K \in \Phi\right\}.$$

More generally, for any field extension K'/K, the type $\{\varphi \in \mathrm{Hom}(K', K'^c) : \varphi|_K \in \Phi\}$ is called the *induced type* by Φ on K'. Types Φ which are not induced from a strictly smaller subfield are said to be *primitive*. Simple abelian varieties have primitive types, and in that case, we canonically have $K^{rr} = K$ and $\Phi^{rr} = \Phi$.

Define the *type trace* $\mathrm{tr}_\Phi : x \in K \mapsto \sum_\Phi \varphi(x)$; its image actually generates the field K^r and this can be used as an equivalent definition for the reflex field; more importantly, define the *type norm*

$$N_\Phi : x \in K \mapsto \prod_{\varphi \in \Phi} \varphi(x) \in K^r$$

(it is elementary to verify that the images of both these maps are in K^r). There is also a *reflex type trace* tr_{Φ^r} and a *reflex type norm* $N_{\Phi^r} : K^r \to K$.

The latter is particularly important to us, as we will make great use of it via the map it induces on Picard groups: if $\mathfrak{a}$ is an ideal of $\mathscr{O}_{K^r}$, there is a unique ideal of $\mathscr{O}_K$, which we write $N_{\Phi^r}(\mathfrak{a})$, such that

$$N_{\Phi^r}(\mathfrak{a})\mathscr{O}_{K^c} = \prod_{\varphi \in \Phi} \varphi(\mathfrak{a})\mathscr{O}_{K^c}$$

(see for instance Proposition in Chapter II of S ( )). By the above, the map $N_{\Phi^r} : \mathfrak{I}(\mathcal{O}_{K^r}) \to \mathfrak{I}(\mathcal{O}_K)$ induces a morphism of Picard groups, which we also write similarly:

$$N_{\Phi^r} : \mathrm{Pic}(\mathcal{O}_{K^r}) \to \mathrm{Pic}(\mathcal{O}_K)$$

T P C G S

Fix a primitive type Φ of a complex multiplication field K of degree $2g$, and denote the totally real subfield of K by K_+.

Recall that a triple $(\Phi, \mathfrak{a}, \xi)$ yields the principally polarized complex torus $\mathbb{C}^g/\Phi(\mathfrak{a})$ with the polarization E^{ξ}_{Φ}; Theorem . . explained that all tori arise in this way and gave necessary and sufficient conditions for two triples to yield isomorphic polarized varieties.

Following Section of S ( ), a group $\mathfrak{C}(\mathcal{O})$ can be constructed so as to naturally act on this set of triples representing isomorphism classes of principally polarized abelian varieties:

. Let P be the group of pairs $(\mathfrak{a}, \rho)$ where $\rho \in K_+$ is totally positive and $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$ satisfying $\mathfrak{a}\bar{\mathfrak{a}} = \rho\mathcal{O}$, endowed with component-wise multiplication.

. Let I be the subgroup formed by the $(\mu\mathcal{O}, \mu\bar{\mu})$ for $\mu \in K^\times$.

. Let $\mathfrak{C}(\mathcal{O})$ be the quotient group P/I.

As a consequence to Theorem . . , we therefore have:

Corollary III.4.2. *For $\mathcal{O} = \mathcal{O}_K$, the group $\mathfrak{C}(\mathcal{O})$ acts faithfully and transitively on the set of isomorphism classes of principally polarized abelian varieties having complex multiplication by $\mathcal{O}$ with type Φ. In particular, they have the same cardinality.*

It might be easier to understand the group $\mathfrak{C}(\mathcal{O})$ as part of the exact sequence

$$\mathbb{U}(K) \longrightarrow \mathbb{U}^+(K_+) \longrightarrow \mathfrak{C}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}^+(\mathcal{O}_+)$$

where the implied maps are, respectively, the norm of K/K_+, the embedding $\rho \mapsto (\mathcal{O}, \rho)$, the projection $(\mathfrak{a}, \rho) \mapsto \mathfrak{a}$, and the map $\mathfrak{a} \mapsto \mathfrak{a}\bar{\mathfrak{a}} \cap K_+$; also, $\mathbb{U}^+(K_+)$ denotes the totally positive units of the totally real subfield K_+, and $\mathrm{Pic}^+(\mathcal{O}_+)$ denotes the quotient of the group of fractional ideals of $\mathcal{O} \cap K_+$ by those that admit a totally positive generator.

Intuitively, the class group $\mathrm{Pic}(\mathcal{O})$ acts on the set of abelian varieties up to isomorphism, as proven by W ( ) for $\mathcal{O} = \mathcal{O}_K$; the subgroup $\mathrm{Pic}^+(\mathcal{O}_+)$ encodes the different ways an isogeny can alter polarizations, and the group $\mathbb{U}^+(K_+)/N_{K/K_+}(\mathbb{U}(K))$ corresponds to isomorphism classes of principal polarization.

For in ance, in the case of dimension $g = 2$, when the totally-real subfield K_+ contains a unit of norm -1, which exactly means that its fundamental unit is not totally positive, the quotient $\mathbb{U}^+(K_+)/\,N_{K/K_+}(\mathbb{U}(K))$ is trivial so we have a one-to-one map:

$$\mathfrak{C}(\mathcal{O}) \longrightarrow \ker\left(\mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}^+(\mathcal{O}_+)\right)$$

Although the computation of the polarized class group $\mathfrak{C}(\mathcal{O})$ of Shimura is a much less classical topic than that of Picard groups, it is not more di cult; for in ance, we note that similar groups have been udied from an algorithmic viewpoint by C , D D , and O ( ).

P A

There is a particular subgroup of the polarized class group of Shimura formed by elements arising as Galois actions. Here, we give a simplified exposition of this general theory and refer to Section of S ( ) for a more robu con ruction.

Let $\mathscr{A}$ be a principally polarized abelian variety defined over $\mathbb{C}$ with complex multiplication by the maximal order $\mathcal{O}_K$ of a field K with type Φ. In fact, the abelian variety $\mathscr{A}$ can be defined over the Hilbert class field $\mathscr{H}_{K^r}$ which is the maximal abelian unramified extension of the reflex field, and in particular its *invariants* lie in that field; the action that we now describe can be seen as that of the Galois group of $\mathscr{H}_{K^r}$ via the Artin symbol.

Theorem III.4.3. *Invertible ideals of* K^r *act on polarized tori with complex multiplication by* $\mathcal{O}_K$ *with type* Φ *via*

$$\mathfrak{r} \in \mathfrak{I}(K^r) : \mathbb{C}^g/\Phi(\mathfrak{a}), E_\Phi^\xi \longmapsto \mathbb{C}^g/\Phi\left(N_{\Phi^r}(\mathfrak{r})^{-1}\mathfrak{a}\right), E_\Phi^{N_{K^r/\mathbb{Q}}(\ )\xi};$$

an ideal $\mathfrak{r}$ *acts trivially when its reflex type norm ideal* $N_{\Phi^r}(\mathfrak{r})$ *is a principal ideal of* $\mathcal{O}_K$ *generated by an invertible element* $\mu \in K^\times$ *which satisfies* $\mu\bar{\mu} = N_{K^r/\mathbb{Q}}(\mathfrak{r})$.

Recall that the set of principally polarized abelian varieties with endomorphism ring $\mathcal{O}_K$ is acted upon faithfully and transitively by the polarized class group $\mathfrak{C}(\mathcal{O}_K)$ of Shimura. The isogenies that arise via the reflex type norm (by theorem above) therefore act as the subgroup of $\mathfrak{C}(\mathcal{O}_K)$ formed by the elements

$$\left(N_\Phi(\mathfrak{r}), N_{K^r/\mathbb{Q}}(\mathfrak{r})\right)$$

where $\mathfrak{r}$ ranges over ideals of $\mathcal{O}_{K^r}$. We emphasize that other elements of $\mathfrak{C}(\mathcal{O}_K)$ also act as isogenies, but that they might not be rational.

For in ance, in dimension two, if $(\mathfrak{a}, \ell) \in \mathfrak{C}(\mathcal{O}_K)$, and ℓ totally splits as $\mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$ in K, then the possible values for $\mathfrak{a}$ are $\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}\bar{\mathfrak{q}}$, and their respective conjugates; in that case, ℓ also splits completely in K^r and the reflex type norm maps the prime factors of $\ell\mathcal{O}_{K^r}$ onto those four elements of $\mathfrak{C}$ with norm ℓ^2. In other cases, elements of $\mathfrak{C}(\mathcal{O}_K)$ of norm ℓ^2 might not be in the image of the reflex type norm.

R F F

We briefly review how the action that we have just defined transports to finite fields, in the case of simple ordinary abelian varieties of dimension two. For details, we refer to the work of G ( ) and G and L ( ).

We first consider a principally polarized abelian variety $\mathcal{A}_p$ defined over a finite field of characteristic p; given any embedding ι_p of $\mathcal{O}_K$ into $\mathrm{End}(\mathcal{A}_p)$, implying that $\mathcal{A}_p$ has complex multiplication by $\mathcal{O}_K$, there exists an abelian variety $\mathcal{A}$ defined over a number field and an embedding $\iota : \mathcal{O}_K \to \mathrm{End}(\mathcal{A})$ which, at a certain prime, reduce to $\mathcal{A}_p$ and ι_p respectively.

Conversely, if $\mathcal{A}$ is a simple polarized abelian variety with complex multiplication by solely exploiting the ańion of $\mathfrak{C}(\mathscr{O})$ under the type norm, or that of certain elements $(\mathfrak{q}, \ell)$ for primes ℓ ŕlitting in K as $\mathfrak{q}\bar{\mathfrak{q}}$. In other cases, this requires additional hypotheses, which we will then ŕecify.

References

. Carl L. S .
"Über die Classenzahl quadratischer Zahlkörper".
In: *Aňa Ariūm'nica* . Pages – .

. Max D .
"Die Typen der Multiplikatorenringe elliptischer Funktionenkörper".
In: *Abhandlungen aŬ dem mŅhemŅśchen Seminar der hamburgśchen Universität* . Pages – .

. André W .
Sur les courbes algébriques 'n les variétés qui s'en déduśent. Volume .
Ańualités Scientiŏques et Indu rielles .
Publications de l'In itut de Mathématique de l'Université de Strasbourg.

. Richard B .
"On the zeta-funńions of algebraic number ŏelds".
In: *American Journal of MŅhemŅics* . . Pages – .
DOI: 10.2307/2371849.

. Goro S and Yutaka T .
Complex multiplicŅion of abelian vari'nies and its applicŅions to number ūeory.
Volume . Publications of the Mathematical Society of Japan.
Ł e Mathematical Society of Japan.

. John T .
"Endomorphisms of abelian varieties over ŏnite ŏelds".
In: *Inl·entiones mŅhemŅicae* . . Pages – . DOI: 10.1007/BF01404549.

. Jean G .
"Remarque sur une formule de Shimura-Taniyama".
In: *Inl·entiones MŅhemŅicae* . . Pages – . DOI: 10.1007/BF01425552.

. William C. W .
"Abelian varieties over ŏnite ŏelds".
In: *Annales ScientiŔques de l'École Normale Supérieure* . . Pages – .

. William C. W and James S. M .
"Abelian varieties over finite fields". In: *Number Theory Institute.*
Edited by Donald J. L . Volume .
Proceedings of Symposia in Pure Mathematics. American Mathematical Society.
Pages – .

. Arjen K. L , Hendrik W. L , and László L .
"Factoring polynomials with rational coefficients".
In: *Mathematische Annalen* . . Pages – . DOI: 10.1007/BF01457454.

. René S .
"Elliptic curves over finite fields and the computation of square roots mod p".
In: *Mathematics of Computation* . . Pages – .
DOI: 10.2307/2007968.

. Gary C and Joseph H. S (editors).
Arithmetic Geometry. Springer. ISBN: - - - .

. David A. C .
Primes of the form $x^2 + ny^2$. John Wiley & Sons. ISBN: - - - .

. Eric B .
"Explicit bounds for primality testing and related problems".
In: *Mathematics of Computation* . . Pages – .
DOI: 10.1090/S0025-5718-1990-1023756-8.

. Arnold S .
"Fast reduction and composition of binary quadratic forms".
In: *Symbolic and Algebraic Computation — ISSAC '* . Edited by Stephen M. W .
Association for Computing Machinery. Pages – .
DOI: 10.1145/120694.120711.

. Henri C .
A course in computational algebraic number theory. Volume .
Graduate Texts in Mathematics. Springer. ISBN: - - - .

. Henri C , Francisco D D , and Michel O .
"Subexponential algorithms for class group and unit computations".
In: *Journal of Symbolic Computation* . – . Special issue on computational algebra and number theory: proceedings of the first MAGMA conference. Pages – .
DOI: 10.1006/jsco.1996.0143.

. Eyal Z. G .
"On certain reduction problems concerning abelian surfaces".
In: *Manuscripta Mathematica* . . Pages – . DOI: `10.1007/BF02677837`.

. Henri C , Francisco D D , and Michel O .
"Computation of relative quadratic class groups".
In: *Algorithmic Number Theory — ANTS-III*. Edited by Joe P. B .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/BFb0054882`.

. Goro S .
Abelian Varieties with Complex Multiplication and Modular Functions.
Princeton University Press. ISBN: - - - .

. Steven D. G , Florian H , and Nigel P. S .
"Extending the GHS Weil descent attack".
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Lars R. K .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-46035-7_3`.

. James S. M .
Complex Multiplication.
URL: `http://www.jmilne.org/math/CourseNotes/cm.html`.

. Eyal Z. G and Kristin E. L .
"Class invariants for quartic CM fields".
In: *Annales de l'Institut Fourier* . . Pages – .

. David J , Stephen D. M , and Ramarathnam V .
"Expander graphs based on GRH with an application to elliptic curve cryptography".
In: *Journal of Number Theory* . . Pages – .
DOI: `10.1016/j.jnt.2008.11.006`.

. Marco S .
"Complex multiplication of abelian surfaces". PhD thesis. Universiteit Leiden.
ISBN: - - - .
URL: `http://www.math.leidenuniv.nl/~streng/thesis.pdf`.

ýairing-ĺriendly ʒari'nies

IV.1 Cryptographic Requirements

Ł e use of pairings enables many cryptographic protocols; as we have mentioned before, cryptography-grade pairings, that is, pairings which can be evaluated e ciently and are hard to invert, are only known to be deŏned on abelian varieties.

Here, we ŏr review cryptographic requirements for pairing-based con ruńions, and then consider how abelian varieties satisfying these conditions can be generated.

G C

Let $\mathscr{A}$ be an abelian variety deŏned over a ŏnite ŏeld $\mathbb{F}_q$ and containing a cyclic subgroup of order r. Ł e *embedding degree* $e(r)$, also written e when there is no ambiguity on the subgroup, is deŏned as the smalle integer such that the Weil pairing

$$\Psi_{\text{Weil}} : \mathscr{A}[r](\mathbb{F}_{q^e}) \times \mathscr{A}[r](\mathbb{F}_{q^e}) \longrightarrow \mu_r \subset \mathbb{F}_{q^e}^\times$$

is non-degenerate; extending a result of B and K ( ), R - and S ( ) proved that, if r does not divide $q-1$ and the degree of the polarization of $\mathscr{A}$ is coprime to r, then e divides the order of q modulo r.

Using this pairing for cryptographic purposes imposes the following:

. It mu be computationally infeasible to solve discrete logarithm problems in $\mathscr{A}[r]$.

. It mu be computationally infeasible to solve discrete logarithm problems in $\mu_r \subset \mathbb{F}_{q^e}^\times$.

. It mu be prańical to compute over the ŏeld $\mathbb{F}_{q^e}$.

Ł e la condition ensures that the algorithm of M ( ) evaluates the Weil pairing e ciently. Note that many con ruńions do not direńly use the Weil pairing but rather variants of it that enable evaluation ŕ eedups by small fańors; however, from a variety generation point of view, this makes little di erence: so long as ŏeld operations in $\mathbb{F}_{q^e}$ can e ciently be computed, pairings with embedding degree e can be evaluated with more or less e ort.

Later, it will be convenient to allow r to be a prime times a small cofańor; this does not invalidate the above: the security simply re s on the large prime fańor of r.

Ł ere are two big decisions to be made:

Binary or prime fields? Fields of charańeri ic two (also known as binary ŏelds) are suited to e cient hardware implementations; on the other hand, soŔware implementations work equally well with prime ŏelds.

Supersingular or ordinary varieties? Supersingular varieties are easy to generate and readily have small embedding degrees; however, they are quite ŕ ecial and have an easy decisional Di e–Hellman problem.

We choose to work with ordinary varieties deŏned over prime ŏelds. Some authors argue that prime powers with exponent greater than one have density zero among prime powers, but here we ju ify this choice by its convenience and the fań that it avoids Weil-descent attacks altogether. Although attrańive for the design of cryptographic protocol, the properties of supersingular curves can be seem unnecessarily ŕ ecial; they are mo ly intere ing over ŏelds of small charańeri ic, and it is not so challenging to generate them.

To avoid wa ing bits, we wish to balance the expeńed hardness the discrete logarithm problem in the abelian variety $\mathscr{A}(\mathbb{F}_q)$ and in the group $\mu_r \subset \mathbb{F}_{q^e}^\times$ as they are rendered equivalent by the pairing. When q is a prime power, H ( ) warned that μ_r might reside in a riń subŏeld of $\mathbb{F}_{q^e}^\times$, leading to fa er attacks on its discrete logarithm problem. However, this problem does not arise when q is prime.

A

Suppose $\mathscr{A}$ is an ordinary abelian variety of dimension g deŏned over a prime ŏeld $\mathbb{F}_q$ of which the discrete logarithm problem and pairing are considered for cryptographic use. By the Pohlig–Hellman reduńion, it is su cient to consider its large prime subgroup $\mathscr{H}$; we denote its order by r and its embedding degree by e. In order avoid attacks on high-genus varieties, we furthermore assume that $g = 1, 2$; this conveniently enables us to use the fa arithmetic of Jacobian varieties of hyperelliptic curves.

To measure the cryptographic e ciency, ŏx g and let q go to inŏnity: the complexity of additions in $\mathscr{A}(\mathbb{F}_q)$ is polynomial in $\log q$; disregarding the pairing, the discrete logarithm problem in $\mathscr{A}(\mathbb{F}_q)$ achieves an expe ńed security of $\frac{1}{2}\log_2 r$ bits. Hence, we introduce the quantity

$$\rho = \frac{g \log_2 q}{\log_2 r}$$

which, since $\#\mathscr{A}(\mathbb{F}_q) \sim q^g$, also indicates the proportion of bits used to represent points of $\mathscr{A}(\mathbb{F}_q)$ that a ńually contribute to the security of scheme: if $\rho \approx 1$ then nearly all of the variety is put to use; if $\rho \approx 2$ then only half of the bits are needed to identify points of $\mathscr{H}$.

Recall the be -known bounds on the complexity of solving discrete logarithm problems:

. Discrete logarithm problems in $\mathscr{A}(\mathbb{F}_q)$ can be solved in $\mathrm{O}\left(r^{1/2+o(1)} \log q\right)$.

. Discrete logarithm problems in $\mathbb{F}_{q^e}^{\times}$ can be solved heuri ically in $\mathrm{L}_{1/3}^{c}\left(q^e\right)$.

To solve the ŏr problem, in general, no better algorithm than generic ones is known, for which a lower bound of $\sqrt{r}$ is proven; the other term in the complexity denotes the co of operations in $\mathscr{A}(\mathbb{F}_q)$. Many variants of the number ŏeld sieve can be used to solve the second problem: the method of M ( ) applies to prime ŏelds, and that of J and L ( ) is particularly adapted to extension ŏelds such as here.

In the mo e e ńive case that $\rho \approx 1$, balancing the two complexities above requires

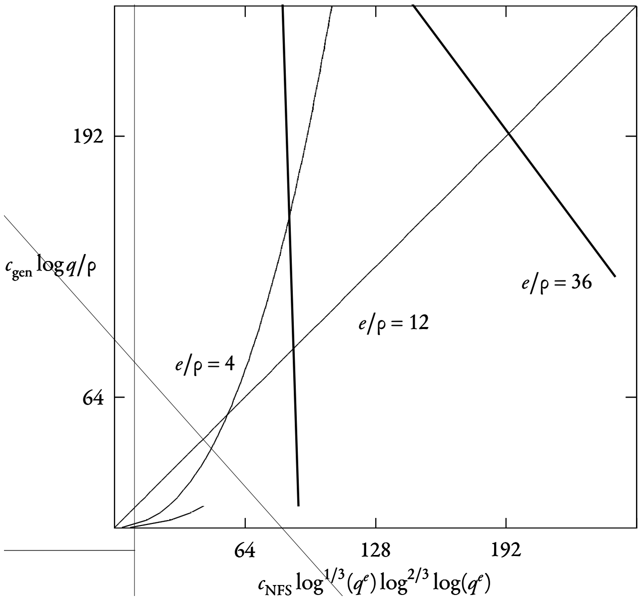
$$\frac{1}{2} g \log q \log\log q \approx c \left(e \log q\right)^{1/3} \left(\log e + \log\log q\right)^{2/3}$$

which implies $e \sim \left(\frac{g}{2c}\right)^3 \left(\frac{1}{3}\log q\right)^2 \log\log q$ and shows that the embedding degree should grow quadratically in the size of the base ŏeld; this is another reason to avoid supersingular varieties: since their embedding degrees are uniformly bounded as g is ŏxed (see below), they do not scale well to higher levels of security.

P

To sele ń the parameters q and e according to the level of security chosen (or equivalently the desired date until when the cryptosy em should with and attacks), the co of attacks on the discrete logarithm problems in both ŏnite ŏelds and abelian varieties mu be carefully considered. Various agencies and organizations regularly publish updated tables li ing parameter tuples for various security levels, such as ECRYPT II ( ) whose table was featured in the ŏr chapter. Mo agree that pairing-based cryptosy ems aimed at being secure beyond should have a 256-bit r and a 3248-bit q^e; as usual, more is better.

Ł e pra ńical co of an attack can be e imated by using timings of previous attacks to calibrate the big-O (and possibly other) con ants in the asymptotic complexity; this usually gives a fair e imation for larger in ances. Here, we need to control both the hardness of



F . The abscissa bounds the security level of the discrete logarithm problem in $\mathbb{F}_{q^e}^{\times}$ while the ordinate does the same in $\mathcal{E}/\mathbb{F}_q$. The diagonal represents the optimal case that these are balanced. The curves plot what elliptic curves achieve for selected values of e/ρ.

the discrete logarithm problem in the curve and the embedding field. Figure does such a rough analysis for the parameters (ρ, e, q) of pairing-friendly curves. It shows, for instance, that 128 bits of security are best achieved by elliptic curves for which $e/\rho \approx 12$, with the most preferable choice of $\rho \approx 1$ implying that $e = 12$ and $q \approx 2^{256}$.

Before explaining how to generate elliptic curves and abelian varieties with the above properties, let us first say a bit more on supersingular varieties.

S V

While ordinary varieties are the generic case, supersingular varieties are the other extreme: recall that *supersingular abelian varieties* are defined as being isogenous to powers of supersingular elliptic curves (elliptic curves with zero p-rank) or, equivalently, as having Frobenius endomorphisms that satisfy $\pi^n = \pm q^{n/2}$ for some integer n.

Their cryptographic interest stems from the following result of G ( ).

Proposition IV.1.1. *The embedding degree of any subgroup of any g-dimensional supersingular abelian variety defined over a finite field is uniformly bounded by some quantity e_g.*

We have for instance $e_1 = 6$, $e_2 = 12$, $e_3 = 30$, $e_4 = 60$.

For certain types of base fields, the bound e_g can be lowered: the optimal bound for e_1 is 4 in characteristic two, 6 in characteristic three, 3 in higher characteristic, and 2 over prime fields with more than three elements.

An interesting feature of supersingular varieties is the existence of *distortion maps*, that is, non-rational endomorphisms. For ordinary varieties, we have seen that all endomorphisms defined over an algebraic closure are also defined over the base field, so their field of definition makes no difference. However, for supersingular varieties, there exist endomorphisms which do not commute with the Frobenius endomorphism.

Such *distortion maps* ψ are useful in cryptography because they send points of the rational r-torsion subgroup to points of $\mathscr{A}[r](\mathbb{F}_{q^e})$ which might not be rational. Then, the application

$$(P, Q) \in \mathscr{A}[r](\mathbb{F}_q)^2 \longmapsto \Psi_{\mathrm{Weil}}(\psi(P), Q) \in \mu_r$$

is a "self" pairing which is a very attractive object to build cryptographic primitives on, as its domain is the Cartesian product of two copies of the same cyclic group of order r, rather than the Cartesian product of two different ones.

On the other hand, this makes the decisional Diffie–Hellman problem easy, since for any triple of integers (a, b, c) and point P on $\mathscr{A}$, one can verify whether $c = ab$ given P, aP, bP, cP by checking whether

$$\Psi_{\mathrm{Weil}}(\psi(aP), bP) = \Psi_{\mathrm{Weil}}(\psi(P), cP);$$

from a security viewpoint, this can be seen as an undesirable property. Naturally, many protocols take advantage of that situation as well.

Since embedding degrees of supersingular curves are bounded, the base field size must grow more than linearly in the desired security level in order to avoid discrete logarithm attacks in $\mathbb{F}_{q^e}^{\times}$ via the pairing; this lack of scalability is unpractical in the long term, and we now shift our focus to the ordinary case.

IV.2 Complex Multiplication Method

The problem of constructing ordinary abelian varieties defined over a finite field on which pairings are efficiently computable (meaning that the embedding degree is small) is an active topic of research.

This section describes the so-called *complex multiplication method* for generating ordinary abelian varieties with prescribed endomorphism rings; as a consequence, it also generates varieties whose Frobenius endomorphism have prescribed polynomials. Since the existence of a subgroup of order r with embedding degree e only depends on this polynomial, the next section will exploit this method to generate pairing-friendly varieties.

S P -F V

As we have argued before, abelian varieties of dimension $g = 1$ and 2 are the most suitable for cryptosystems which rely on the discrete logarithm problem. When no additional structure (such as a pairing) is required, abelian varieties need just have a near-prime group order, and are best generated by random search, which additionally reduces their likelihood of having undesirable special properties. For elliptic curves, such computations are classical, and for $g = 2$ it was recently demonstrated practical by G and S ( ).

When, on top of a near-prime group order, one seeks a small embedding degree, this approach is not feasible anymore due to the scarcity of abelian varieties with the desired condition. More precisely, B and K ( ) proved the following.

Theorem IV.2.1. *There are at most* $M^{1/2+o(1)}$ *isogeny classes of elliptic curves* $\mathscr{E}/\mathbb{F}_p$ *with prime order and embedding degree less than* $\log^2 p$*, where* p *is a prime in* $\{M/2, \dots, M\}$.

Since there are roughly $M^{3/2}$ isogeny classes of elliptic curves defined over $\mathbb{F}_p$ with $p \in \{M/2, \dots, M\}$, this is a pretty slim fraction of the total. L and S ( ) recently gave a similar result for dimension-two abelian varieties:

Theorem IV.2.2. *Let* H *and* K *be positive integers, the number of pairs* (p, N) *where* N *is the order of a dimension-two abelian variety defined over* $\mathbb{F}_p$ *with* $p \in \{M/2, \dots, M\}$*, such that* $N = hr$ *where* $h \leqslant H$*,* r *is prime and has embedding degree less than* K *is at most* $M^{3/2+o(1)}HK^2$ *for* M *large enough.*

Since there are roughly $M^{5/2}$ pairs (p, N) arising as orders of two-dimensional abelian varieties, this gives, similarly to the one-dimensional case, a probability of $p^{-1+o(1)}$ of finding a pairing-friendly abelian variety by random search over $\mathbb{F}_p$.

The theory of complex multiplication provides a method for generating such varieties efficiently. This involves two steps: we will first describe how varieties with prescribed endomorphism rings and prescribed fields of definition can be constructed using the so-called complex multiplication method, and we will then consider characterizing pairing-friendly varieties in terms of their endomorphism ring and base field.

C

Since abelian varieties of dimension three or more are not intere ing for cryptography, we re riń to Jacobian varieties of hyperelliptic curves $\mathscr{C}$ since all principally polarized abelian variety of dimension one or two are of this type. Ł is allows to use invariants which uniquely identify the isomorphism class of such a variety and are expressed as rational functions of the coe cients of an equation for $\mathscr{C}$.

Fix a genus g and a family of invariants (I_i) that uniquely identify birationally equivalent classes of hyperelliptic curves. For in ance, in dimension one, the *j-inŀariant*

$$\mathscr{C} : y^2 = x^3 + ax + b \longmapsto j(\mathscr{C}) = \frac{2^8 3^3 a^3}{2^2 a^3 + 3^3 b^2}$$

(where we have assumed the charańeri ic to be di erent from 2 and 3) alone su ces. In higher dimension, as we have mentioned before, more invariants are necessary.

Let $\mathscr{O}$ be the order of a complex multiplication ŏeld K of degree $2g$, that is, a totally imaginary quadratic extension of a totally real number ŏeld. S ( ) ŏr proposed to encode the information about all abelian varieties $\mathscr{A}$ of dimension g deŏned over the complex numbers into the following polynomial

$$\mathscr{H}_i^{\mathscr{O}}(x) = \prod_{\{\mathscr{A} : \mathrm{End}\,\mathscr{A} \simeq \mathscr{O}\}} \left(x - \mathrm{I}_i(\mathscr{A})\right),$$

where $\mathscr{A}$ ranges over isomorphism classes of abelian varieties. In dimension one, they are usually called *Hilbert clńs polynomials* when $\mathscr{O}$ is the maximal order of K, as their roots, the invariants of abelian varieties with endomorphism ring $\mathscr{O}$, generate the Hilbert class ŏeld of $\mathscr{O}$; for non-maximal orders and in higher dimension, these lie in the ring class ŏeld of $\mathscr{O}$ and the polynomials are simply known as *clńs polynomials*.

W ( ) later developed this theory and explained how these polynomials could be used to generated abelian varieties over ŏnite ŏelds with prescribed endomorphism ring, as we will soon explain. When there are two invariants or more (that is, for $g > 1$), these polynomials do not encode which root of $\mathscr{H}_1^{\mathscr{O}}$ corre ŕ onds to which root of $\mathscr{H}_i^{\mathscr{O}}$ for $i > 1$; in other words, the invariant tuples we are intere ed in are lo among tuples of unrelated invariants.

To address this issue, G , H , K , R , and W ( ) interpolated the values $\mathrm{I}_i(\mathscr{A})$ at the $\mathrm{I}_1(\mathscr{A})$: they deŏned

$$\mathscr{H}_i'^{\mathscr{O}}(x) = \sum_{\mathrm{End}\,\mathscr{A} \simeq \mathscr{O}} \mathrm{I}_i(\mathscr{A}) \prod_{\substack{\mathrm{End}\,\mathscr{B} \simeq \mathscr{O} \\ \mathscr{B} \not\simeq \mathscr{A}}} \left(x - \mathrm{I}_1(\mathscr{B})\right)$$

for $i > 1$. Ł is encodes exańly the information wanted.

R P

Let $\mathscr{A}$ be an ordinary abelian variety with complex multiplication by $\mathscr{O}$ defined over some number field, and let $\mathfrak{p}$ be a prime of degree one at which the reduction $\mathscr{A}$ of $\mathscr{A}$ is itself an ordinary abelian variety defined over $\mathbb{F}_p$ where p is the rational prime below $\mathfrak{p}$. Since invariants are compatible with reduction, we have $\mathrm{I}_i(\mathscr{A}\ ) = \mathrm{I}_i(\mathscr{A})$.

As the endomorphism ring of $\mathscr{A}$ is mapped injectively into that of $\mathscr{A}$, we have $\mathscr{O} \subset$ (End $\mathscr{A}$); when $\mathscr{O}$ is the maximal order, equality must hold, and this is also the case for any order when $\mathscr{A}$ is an elliptic curve, due to the Deuring lifting theorem.

Consequently, an abelian variety with complex multiplication by $\mathscr{O}$ defined over a finite field can be found using the following algorithm.

Algorithm IV.2.3.

I : *A prime p, and an order $\mathscr{O}$, either imaginary quadratic or maximal in a quartic complex multiplication field.*

O : *An abelian variety $\mathscr{A}/\mathbb{F}_p$ with* $\mathrm{End}\,\mathscr{A} \simeq \mathscr{O}$.

. *Compute the class polynomials $\mathscr{H}_i'^{\mathscr{O}}(x)$.*

. *For each root I_1 of $\mathscr{H}_1^{\mathscr{O}}(x) \bmod p$:*

. *For all $i > 1$, let $\mathrm{I}_i = \mathscr{H}_i'^{\mathscr{O}}(\mathrm{I}_1)/\mathscr{H}_1^{\mathscr{O}}(\mathrm{I}_1)$.*

. *Use the method of M ( ) to compute a hyperelliptic curve whose Jacobian variety has invariants (I_i).*

Note that the output of this algorithm might be empty; for instance, when there are no abelian varieties with endomorphism ring $\mathscr{O}$ defined over the field with p elements. In other cases, the number of curves returned might not be constant as $\mathscr{O}$ is fixed and p varies. The conceptually simplest case is that where p completely splits in the ring class field of $\mathscr{O}$: then, the $\mathscr{H}_i^{\mathscr{O}}$ split into linear factors modulo p.

C C P

Before making use of the method above, let us briefly describe the current methods available for computing class polynomials in dimension one and two.

Since the class polynomials $\mathscr{H}_i^{\mathscr{O}}$ are defined over the complex numbers and have good reduction to finite fields, there are, as with modular polynomials, two methods to compute them: a complex analytic method and one based on the Chinese remainder theorem.

The complex analytic version evaluates the invariants $\mathrm{I}_i(\mathscr{A})$ for complex tori verifying $\mathrm{End}\,\mathscr{A} \simeq \mathscr{O}$ to sufficient precision to identify the coefficients of the class polynomial; it requires tight bounds on the height of these coefficients. C and H

( ) also proposed a p-adic version which proceeds similarly but uses the canonical lift of an abelian variety defined over a small extension of $\mathbb{F}_p$ to transport the computation to $\mathbb{Q}_p$.

The Chinese remainder theorem version reconstructs the polynomials $\mathscr{H}_i^{\mathcal{O}} \in \mathbb{Q}[x]$ from their reduction to many small prime fields $\mathbb{F}_p$ by enumerating the abelian varieties with endomorphism ring $\mathcal{O}$ in each such field; typically, a first variety with complex multiplication $\mathbb{Q} \otimes \mathcal{O}$ is found by sheer luck (this requires computing the endomorphism ring of many random curves), and isogenies are then used to find a curve with endomorphism ring exactly $\mathcal{O}$ and to enumerate all other such varieties.

When the dimension of $\mathcal{O}$ is fixed, the complexity of all methods mainly depends on the order of the Picard group of $\mathcal{O}$, which dictates the number of roots of the class polynomials.

For elliptic curves, all methods have a quasi-linear runtime in the size of the output; see the careful analyses of E ( ), B ( ), and S ( ). A practical advantage of the Chinese remainder theorem version is that it need not keep the full polynomials $\mathscr{H}_i^{\mathcal{O}} \in \mathbb{Q}(x)$ in memory: only their reductions modulo many primes are required; from these, $\mathscr{H}_i^{\mathcal{O}}$ can be directly reconstructed in the prime field where we seek an abelian variety with endomorphism ring $\mathcal{O}$. This is particularly useful as memory requirements are the current bottleneck of the other two methods.

In dimension two, W ( ) introduced the complex analytic method, C , M - , K , and T ( ) the Chinese remainder theorem one, and G , H , K , R , and W ( ) a 2-adic method. All have since been improved by many researchers. Their respective speeds do not support a range of orders $\mathcal{O}$ as wide as for elliptic curves, but quite a fair number of class polynomials have been computed and made available, for instance in the E ( ) package.

IV.3 Elliptic Curve Generation

Let us now explain how to apply the material of the previous section to generate pairing-friendly elliptic curves; very satisfying results can be obtained in this case. This is however not the case for higher-dimensional varieties, as the next section will discuss.

T C –P M

We have explained how an ordinary elliptic curve with prescribed order $\mathcal{O}$ can be generated over a prescribed finite field $\mathbb{F}_p$ when $\mathcal{O}$ has small class number or, equivalently, small discriminant. We now consider which parameters p and $\mathcal{O}$ should be chosen in order for the resulting curve to be pairing-friendly.

Let $\mathscr{E}$ be an ordinary elliptic curve over the prime field with p elements; the characteristic polynomial $\chi_\pi(x)$ of its Frobenius polynomial is of the form $x^2 - tx + p$ where the integer t satisfies $|t| < 2\sqrt{p}$. Conversely, for each such nonzero integer, there exists an ordinary curve $\mathscr{E}/\mathbb{F}_p$ with cardinality $p + 1 - t$ (we assume $p \neq 2, 3$). If r is the largest prime factor of $\#\mathscr{E}$, we require that its embedding degree be small, that is, $r \mid p^e - 1$ for some small integer e.

Additionally, for the complex multiplication method to be practical, there must exist orders of small discriminants in $\mathbb{Q}(\pi)$, that is, the squarefree part of $4p - t^2$ must be small.

Therefore, we require that:

. p be a prime number.

. t be a nonzero integer less than $2\sqrt{p}$ in absolute value.

. r be a prime factor of $p + 1 - t$ such that $r \mid p^e - 1$ for a small e.

. the squarefree part Δ of $t^2 - 4p$ be small in absolute value.

Since Δ and e need to be small, we first fix them: if an integer p can be derived as a function of Δ and e and it is not prime, we can always rerun the algorithm on a different input and hope that it takes a prime value after roughly $\log p$ trials; however, fixing p and deriving Δ or e would have little chances of producing small numbers.

Once Δ and e have been fixed, the method of C and P ( ) consists in rewriting the above set of conditions to the equivalent one:

$$\begin{cases} t^2 - 4p = v^2\Delta \\ r \mid \Phi_e(t-1) \\ r \mid v^2\Delta - (t-2)^2 \end{cases}$$

where Φ_e denotes the e^{th} cyclotomic polynomial; the second condition asserts that e is the smallest integer such that $r \mid p^e - 1$ but this stronger condition is not as important as the construction that it enables: since Φ_e is irreducible it yields a number field where to work. This gives the following algorithm.

Algorithm IV.3.1.

I : *A negative and a positive integer, Δ and e.*

O : *A prime p and an order $\mathscr{O}$ such that there exists a pairing-friendly elliptic curve with endomorphism ring $\mathscr{O}$ over $\mathbb{F}_p$.*

. *Choose a prime field $\mathbb{F}_r$ containing $\sqrt{\Delta}$ and an e^{th} root of unity ζ_e.*

. *Put $t = 1 + \zeta_e$ and $v = (t-2)/\sqrt{\Delta}$ in $\mathbb{F}_r$*

. *Lift t and v to $\mathbb{Z}$ and put $p = \frac{1}{4}(t^2 - v^2\Delta)$.*

. *Unless p is prime, go back to Step .*

. *Output p and the order $\mathscr{O} = \mathbb{Z} + u^2\mathscr{O}_{\mathbb{Q}(\sqrt{\Delta})}$ where u is any divisor of v.*

Due to p being a sum of squares liŔed from $\mathbb{F}_r$ the resulting elliptic has $\rho \approx 2$ on average.

F P -F C

Better ρ values are achieved by *families of curves* with a con ant embedding degree e and discriminant Δ over ŏelds $\mathbb{F}_p$ for increasing primes p. Families of elliptic curves are given by tuples $(\Delta, e, p(x), t(x), r(x), v(x))$ where the la four parameters are polynomials in a formal variable x; additionally to the conditions above, since p and r

T B –W M

B and W ( ) adapted the method of C and P ( ) to generate families of polynomials as defined above. Their construction follows the above except that the arithmetic is done over polynomial rings rather than over the integers.

Algorithm IV.3.2.

I : *A negative and a positive integer,* Δ *and* e*.*
O : *A pairing-friendly family of curves given by* $p(x)$*,* $t(x)$*, and* $r(x)$*.*

. *Choose an irreducible polynomial* $r(x)$ *with positive leading coefficient such that the field* $\mathbb{Q}(x)/r$ *contains* $\sqrt{\Delta}$ *and an* e^{th} *root of unity* ζ_e*.*
. *Put* $t = 1 + \zeta_e$ *and* $v = (t-2)/\sqrt{\Delta}$*, as elements of* $\mathbb{Q}(x)/r$*.*
. *Lift* t *and* v *to* $\mathbb{Z}[x]$ *and put* $p = \frac{1}{4}(t^2 - v^2\Delta)$*.*
. *Unless* p *is irreducible, go back to Step .*
. *Output* $p(x)$*,* $t(x)$*, and* $r(x)$*.*

Since the polynomial $p(x)$ is constructed as a sum of squares of lifts from $\mathbb{Q}(x)/r$, its degree is roughly twice that of r. However, when $\deg(r)$ is small, the degree of $p(x)$ can be much smaller and yield ρ values below 2; note that $\deg(p)$ being smaller is not a problem: curves defined over large prime fields can still be obtained by evaluating $p(x)$ at large integers x; in fact, this is preferable since the slower increase of polynomials gives more flexibility.

L C

To conclude this section, we discuss the results of B. and S ( ).

In this paper, we noted that the two methods described above only fix the complex multiplication field or, equivalently, the isogeny class, but not a specific endomorphism ring order $\mathcal{O}$ which the complex multiplication method takes as input. Actually, our presentation of the Cocks–Pinch method above already showed that fact, since it stated that the order to be output could be of the form $\mathbb{Z} + u\mathcal{O}_{\mathbb{Q}(\pi)}$ for any divisor u of v, where $t^2 - 4p = v^2\Delta$ is the discriminant of the minimal order $\mathbb{Z}[\pi]$.

This means that, once parameters for a pairing-friendly curve or family have been computed, before applying the complex multiplication method and obtaining an actual elliptic curve, there is still some choice to be made on the specific endomorphism ring desired. In the Brezing–Weng method, since $v(x)$ is constructed as $(t-2)/\sqrt{\Delta}$, its degree as polynomial is likely to be roughly that of r; this typically gives a large (and predictable in size) pool of factors to choose from as the conductor of the endomorphism ring.

Therefore, pairing-friendly curves with non-maximal endomorphism rings $\mathcal{O}$ can be generated as easily as maximal ones as long as $\mathcal{O}$ is in the range of the complex multiplication method.

Denote by $\mathscr{E}_1$ and $\mathscr{E}_u$ the elliptic curves with trace t and endomorphism rings respectively $\mathscr{O}_{\mathbb{Q}(\pi)}$ and $\mathscr{O} = \mathbb{Z} + u\mathscr{O}_{\mathbb{Q}(\pi)}$; there is an isogeny of degree u going from $\mathscr{E}_1$ to $\mathscr{E}_u$. Computing this isogeny takes essentially quadratic time in the largest prime factor of u, as we will see in subsequent chapters. Therefore, as it takes $u^{2+o(1)}\Delta$ time to generate the curve $\mathscr{E}_u$ via class polynomials, using different values for u does not yield fundamentally new cryptosystems; it simply shows that a small range of conductors is readily available from pairing-friendly curve generation methods.

IV.4 Variety Generation

As a natural generalization of the problem of pairing-friendly elliptic curves generation, we now consider generating higher-dimensional pairing-friendly abelian varieties. We will first give general statements before mentioning state-of-the-art results.

M S

From a mathematical viewpoint, it is only natural to switch our focus to abelian varieties when we feel the pool of interesting elliptic curves has been depleted, since abelian varieties with an efficient arithmetic (such as Jacobian varieties of genus-2 hyperelliptic curves) have equally effective and secure pairings; they can even be evaluated faster than that of elliptic curves as F and L ( ) demonstrated.

Originally, abelian varieties were proposed for cryptographic use not only as alternatives to elliptic curves but also as a potential improvement: since the size of the group is g times the size of the base field, where g is the dimension, the parameters of a cryptosystem based on dimension-two abelian varieties need only be of half the size of an equivalently secure elliptic cryptosystem; in addition, the smaller base field can possibly be exploited to yield a faster (or at least competitive) arithmetic to that of elliptic curves.

Although abelian varieties readily provide a good framework for cryptosystems based on the discrete logarithm problem only, other factors need to be taken into account for pairing-based cryptography. Before explaining how the situation degrades for ordinary varieties, let us recall that two-dimensional supersingular abelian varieties have an embedding degree of at most 12 and ρ values which can be close to 1; they are currently the only kind of two-dimensional abelian varieties suitable for cryptographic use.

All known constructions of ordinary pairing-friendly varieties of dimension two have large ρ values: we will see that none has $\rho \leqslant 2$, and that ρ values close to 2 are only achieved by special constructions; generic constructions feature $\rho \geqslant 4$, at the time of this writing.

It therefore appears as if genus-two constructions had a lot of room for improvement.

C M M

We have seen that the computation of class polynomials, although harder for abelian varieties of dimension two than for elliptic curves, can be done (and has been done) for a limited number of orders $\mathscr{O}$, all of which are ring of integers of quartic complex multiplication fields with relatively small discriminant.

Therefore, it is even more important to fix $\mathscr{O}$ as a first step of any construction than it was with elliptic curves. We distinguish two types of constructions:

. Generic constructions, which take an arbitrary maximal quartic complex multiplication order as input, and output generic pairing-friendly abelian varieties.

. Specific constructions, which focus on varieties of a particular form (usually implying that $\mathscr{O}$ is fixed too) and exploit explicit results due to this form.

Here, by "generic" we mean that the former methods output varieties with no particular properties other than those required; in particular, the varieties are usually absolutely simple and ordinary. This is to be compared to the varieties obtained by the latter method which are typically simple but not absolutely simple.

G C

The first construction of ordinary pairing-friendly abelian varieties of dimension $g > 1$ with cryptographic size are due to F ( ). It can be considered a genus-two analog to the Cocks–Pinch method, and proceeds by solving explicit equations which arise by writing the characteristic polynomial of the Frobenius endomorphism in terms of parameters for the desired complex multiplication field. The abelian varieties it generates have a typical ρ value of 8.

Later, F , S , and S ( ) provided a cleaner framework for constructing pairing-friendly ordinary abelian varieties of dimension two by using more of the theory of complex multiplication.

Let π be the Frobenius endomorphism of a simple ordinary abelian variety $\mathscr{A}$ over a finite field. Their idea was to write the condition that $\mathscr{A}$ has a subgroup of order r with embedding degree e as

$$\begin{cases} r \mid \mathrm{N}_{\mathbb{Q}(\pi)/\mathbb{Q}}(\pi - 1) \\ r \mid \Phi_e(\pi\overline{\pi}) \end{cases}.$$

Now let Φ be a type on the complex multiplication field K, and denote by Φ^r and K^r their respective reflexes. The key observation is that, if r is a prime congruent to one modulo

e that splits completely in K, and if

$$\prod_{\varphi\in\Phi^r}\left(\xi \mod \mathfrak{r}_\varphi\right) = 1 \qquad \text{and} \qquad \prod_{\varphi\in\Phi^r}\left(\xi \mod \overline{\mathfrak{r}_\varphi}\right) = \zeta_e$$

where ζ_e is an e^{th} root of unity and $\prod_{\varphi\in\Phi^r}\mathfrak{r}_\varphi\overline{\mathfrak{r}_\varphi}$ denotes the factorization of r in K^r, then the type norm $\pi = N_{\Phi^r}(\xi)$ of ξ is a q-Weil number (that is, a root of a q-Weil polynomial) satisfying the conditions above asserting that it represents an ordinary pairing-friendly abelian variety.

Computationally, numbers ξ can be constructed from their reductions modulo the prime factors of r so as to satisfy the above requirement; after sufficiently many trials, the integer $q = N_{K^r/\mathbb{Q}}(\xi)$ is expected to be prime, and when it is additionally unramified in K and π generates K, this yields, by Honda–Tate theory, an isogeny class of ordinary pairing-friendly abelian varieties with complex multiplication by K.

The method above still produces varieties whose embedding degree is 8 or more, but F ( ) soon adapted it to generate families of pairing-friendly varieties similarly to the Brezing–Weng method for elliptic curves. He applies it to find many families with ρ less than 8, and a particular one with an asymptotic ρ value of 4 for $e = 5$.

S C

To improve on the ρ values obtained by constructions applicable to arbitrary complex multiplication fields, one way is to consider abelian varieties $\mathscr{A}$ of a particular form and exploit explicit results regarding this form as much as possible. Usually, $\mathscr{A}$ is taken as the Jacobian variety $\mathrm{Jac}(\mathscr{C})$ of a hyperelliptic curve $\mathscr{C}$ of genus two with a particular shape of Weierstrass polynomial.

For instance, consider curves $\mathscr{C}$ of the form $y^2 = x^5 + ax$ for some number $a \in \mathbb{F}_p$ where p is a prime congruent to one modulo eight; in that situation, the associated Jacobian variety $\mathrm{Jac}(\mathscr{C})$ is ordinary and simple, and K and T ( ) exploited explicit formulas for the characteristic polynomial of the Frobenius endomorphism in terms of a and p to obtain an analog of the Cocks–Pinch method for that specific type of curves. They obtained a ρ value of 3 with the embedding degree $e = 24$.

The varieties they constructed are not absolutely simple: over an extension containing fourth roots of e, they split as products of two elliptic curves. F and S ( ) studied such varieties from a much more general perspective: from an elliptic curve $\mathscr{E}$ which is pairing-friendly over some extension of its base field, they explain how to derive a simple ordinary pairing-friendly abelian variety which becomes isomorphic to a power of $\mathscr{E}$ over some extension of the same base field. As an application, they construct families of such abelian varieties with $\rho \approx 2.22$ and $e = 27$, which are to date the be known ordinary pairing-friendly varieties of dimension two.

References

. Viňor S. M .
Short programs for funňions on curves. Unpublished.
URL: `http://crypto.stanford.edu/miller/`.

. Jean-François M .
"Con ruńion de courbes de genre 2 à partir de leurs modules".
In: *E eňive m'nhods in algebraic geom'nry — MEGA '* .
Edited by Teo M and Carlo T . Volume . Progress in Mathematics.
Birkhäuser. Pages – .

. Anne-Monika S .
"Kurven vom Geschlecht und ihre Anwendung in Public-Key-Kryptosy emen".
PhD thesis. Universität Duisburg-Essen.
URL: `http://www.iem.uni-due.de/zahlentheorie/AES-KG2.pdf`.

. Ramachandran B and Neal K .
"Ł e improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Van one algorithm".
In: *Journal of Cryptology* . . Pages – . DOI: `10.1007/s001459900040`.

. Jinhui C , Kazuto M , Hiroto K , and Shigeo T .
"Con ruńion of hyperelliptic curves with CM and its application to cryptosy ems".
In: *Advances in Cryptology — ASIACRYPT '* . Edited by Tatsuaki O .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-44448-3_20`.

. Cli ord C and Richard G. E. P .
Identity-bńed cryptosy ems bńed on ūe Weil pairing. Unpublished manuscript.

. Steven D. G .
"Supersingular curves in cryptography".
In: *Advances in Cryptology — ASIACRYPT '* . Edited by Colin B .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-45682-1_29`.

. Atsuko M , Masaki N , and Shunzou T .
"New explicit conditions of elliptic curve traces for FR-reduńions".
In: *IEICE Transańions on FundamenŪls of Eleňronics* E -A. . Pages – .

. Annegret W .
"Kon ruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation".
PhD thesis. Universität Duisburg-Essen. URL: `http://www.iem.uni-due.de/zahlentheorie/preprints/wengthesis.pdf`.

. Jean-Marc C and Ł ierry H .
"Ańion of modular corre ŕ ondences around CM-points".
In: *Algoriūmic Number Ńeory — ANTS-V.*
Edited by Claus F and David R. K . Volume .
Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-45455-1_19`.

. Dmitry V. M .
"On the asymptotic complexity of computing discrete logarithms in the őeld GF(p)".
In: *Dśkr'nnaya MŅemŅika* . . Pages – .

. Friederike B and Annegret W .
"Elliptic curves suitable for pairing based cryptography".
In: *Design, Codes and Cryptograpy* . . Pages – .
DOI: `10.1007/s10623-004-3808-4`.

. Paulo S. L. M. B and Michael N .
"Pairing-friendly elliptic curves of prime order".
In: *Seleňed Areń in Cryptography — SAC '* .
Edited by Bart P and Sta ord T . Volume .
Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/11693383_22`.

. Gerhard F and Tanja L .
"Fa bilinear maps from the Tate-Lichtenbaum pairing on hyperelliptic curves".
In: *Algoriūmic Number Ńeory — ANTS-VII.*
Edited by Florian H ć, Seba ian P , and Michael P . Volume .
Leńure Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/11792086_33`.

. Pierrick G , Ł omas H , David R. K ,
Chri ophe R , and Annegret W .
" Ł e -adic CM method for genus curves with application to cryptography".
In: *Advances in Cryptology — ASIACRYPT '* .

Edited by Xuejia L and Kefei C . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/11935230_8.

. Antoine J and Reynald L .
"The function field sieve in the medium prime case".
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Serge V .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/11761679_16.

. David M. F .
"Constructing pairing-friendly genus curves with ordinary Jacobians".
In: *Pairing-Based Cryptography — PAIRING '* . Edited by Tsuyoshi T ,
Tatsuaki O , Eiji O , and Takeshi O . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-540-73489-5_9.

. Laura H .
"On the minimal embedding field". In: *Pairing-Based Cryptography — PAIRING '* .
Edited by Tsuyoshi T , Tatsuaki O , Eiji O , and
Takeshi O . Volume . Lecture Notes in Computer Science. Springer.
Pages – . DOI: 10.1007/978-3-540-73489-5_16.

. Gaetan B and Takakazu S .
"More discriminants with the Brezing-Weng method".
In: *Progress in Cryptology — INDOCRYPT '* .
Edited by Dipanwita R. C , Vincent R , and Abhijit D .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-540-89754-5_30.

. Reinier B .
"A *p*-adic algorithm to compute the Hilbert class polynomial".
In: *Mathematics of Computation* . . Pages – .
DOI: 10.1090/S0025-5718-08-02091-7.

. David M. F .
"A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties". In: *Pairing-Based Cryptography — PAIRING '* .
Edited by Steven D. G and Kenny G. P . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-540-85538-5_11.

. David M. F , Peter S , and Marco S .
"Abelian varieties with prescribed embedding degree".
In: *Algorithmic Number Theory — ANTS-VIII.*
Edited by Alfred J. van der P and Andreas S . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-540-79456-1_3.

. Mitsuru K and Tetsuya T .
"Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$".
In: *Pairing-Based Cryptography — PAIRING '* .
Edited by Steven D. G and Kenny G. P . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-540-85538-5_12.

. David R. K .
ECHIDNA: Databases for elliptic curves and higher dimensional analogues.
URL: http://echidna.maths.usyd.edu.au/.

. Andreas E .
"The complexity of class polynomial computation via floating point approximations".
In: *Mathematics of Computation* . . Pages – .
DOI: 10.1090/S0025-5718-08-02200-X.

. David F , Michael S , and Edlyn T .
"A taxonomy of pairing-friendly elliptic curves".
In: *Journal of Cryptology* . . Pages – .
DOI: 10.1007/s00145-009-9048-z.

. Karl R and Alice S .
"Using abelian varieties to improve pairing-based cryptography".
In: *Journal of Cryptology* . . Pages – .
DOI: 10.1007/s00145-008-9022-1.

. European Network of Excellence in Cryptology II.
Yearly report on algorithms and keysizes. Edited by Nigel P. S .
URL: http://www.ecrypt.eu.org/documents/D.SPA.13.pdf.

. Pierrick G and Éric S .
Genus point counting over prime fields. HAL-INRIA: 00542650.

. Kristin L and Ning S .
Generating pairing-friendly parameters for the CM construction of genus curves over prime fields. IACR ePrint: 2010/529.

. David M. F and Takakazu S .
"Con ruńing pairing-friendly hyperelliptic curves using Weil re ińion".
In: *Journal of Number Ńeory* . . Pages – .
DOI: 10.1016/j.jnt.2010.06.003.

. Andrew V. S .
"Computing Hilbert class polynomials with the Chinese remainder theorem".
In: *MŅhemŅics of CompuŪtion* . Pages – .
DOI: 10.1090/S0025-5718-2010-02373-7.

C

E R

Exponential Methods

The last chapter was concerned with constructing abelian varieties with prescribed endomorphism rings and we now turn to the inverse problem: that of computing the endomorphism ring of a prescribed variety. Our contribution is covered by the next three chapters; here, we review prior state-of-the-art algorithms, all of which have a worst case running time exponential in the size of the base field.

All sections but the last solely consider ordinary varieties, and our complexity analyses concern a fixed dimension g and a cardinality q of the base field going to infinity.

If $\mathscr{A}$ is an ordinary abelian variety with complex multiplication field K, an isomorphism $\mathbb{Q}(\pi) \simeq K$ between the field of fractions of $\mathrm{End}(\mathscr{A})$ and K will be understood throughout this chapter; this identifies endomorphism rings uniquely as orders of K.

V.1 Isogeny Volcanoes

Let us first describe the structure of the connected component of the isogeny graph containing a prescribed simple ordinary abelian variety over a finite field; we will emphasize *vertical* isogenies and their role in the algorithm of K ( ) for computing endomorphism rings in the dimension-one case.

V I

Following F Ž and M ( ), we say that an isogeny is *horizontal* when its domain and codomain have isomorphic endomorphism rings, and that it is *vertical* otherwise; we first focus on the latter kind, in the context of computing endomorphism rings. Later, we will use horizontal isogenies, via complex multiplication theory, as the key to our subexponential-time algorithm for computing endomorphism rings.

To put to light the relationship between endomorphism rings and vertical isogenies, we use an observation of K :

Lemma V.1.1. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be an isogeny of type $(\mathbb{Z}/\ell)^g$ between ordinary abelian varieties defined over a finite field. The order* $\mathrm{End}(\mathscr{B})$ *is bounded below by* $\mathbb{Z} + \ell\,\mathrm{End}(\mathscr{A})$.

Indeed, since φ splits multiplication by ℓ, we have $\ell\,\mathrm{End}(\mathscr{A}) \subset \mathrm{End}(\mathscr{B})$, and since the latter is an order it must also contain $\mathbb{Z}$. Note that applying this lemma to the dual isogeny $\widehat{\varphi}$ gives a bound on $\mathrm{End}(\mathscr{B})$ from above. To encompass both bounds, we generalize the inclusion index to the following distance on the lattice of orders.

Definition V.1.2. *For any two orders $\mathcal{O}$ and $\mathcal{O}'$ of the same field, define the* order distance $\mathrm{dist}(\mathcal{O}, \mathcal{O}')$ *is* $[\mathcal{O} : \mathcal{O} \cap \mathcal{O}'] + [\mathcal{O}' : \mathcal{O} \cap \mathcal{O}']$.

Corollary V.1.3. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be an isogeny of type $(\mathbb{Z}/\ell)^g$ between ordinary abelian varieties defined over a finite field. The distance* $\mathrm{dist}(\mathrm{End}\,\mathscr{A}, \mathrm{End}\,\mathscr{B})$ *is divisible by* ℓ^{4g-2}.

This follows from the lemma, since $\mathbb{Z} + \ell\mathcal{O}$ has index ℓ^{2g-1} in $\mathcal{O}$, for any order $\mathcal{O}$. By exploiting the symmetry of the lattice of orders, the distance could even be proven to divide ℓ^{2g-1}. However, this simple result is sufficient for us; as a consequence, there can only be finitely many vertical isogenies of a given type leaving from any given variety $\mathscr{A}$ since:

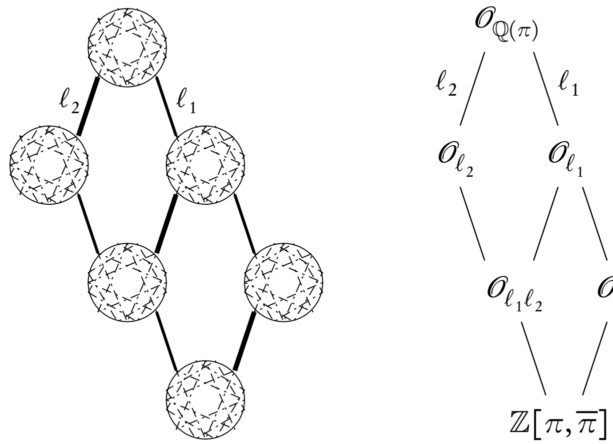
- only finitely many orders of K are endomorphism rings, that is, contain $\mathbb{Z}[\pi, \overline{\pi}]$;
- therefore there are only finitely many possible degrees for vertical isogenies;
- since $\mathscr{A}[\ell] = (\mathbb{Z}/\ell)^{2g}$ there are finitely many suitable subgroups.

Recall the results of T ( ) and W ( ):

Theorem V.1.4. *Isogeny classes of abelian varieties defined over a finite field are identified by the characteristic polynomial of their Frobenius endomorphism. Endomorphism rings of ordinary varieties $\mathscr{A}$ are exactly those orders of the complex multiplication field* K *that contain* $\mathbb{Z}[\pi, \overline{\pi}]$.

This shows that the structure of vertical isogenies is quite rigid: the possible degrees are fixed per isogeny class by the index of the minimal order $\mathbb{Z}[\pi, \overline{\pi}]$ in the maximal one of K. Worse, they can be as large as $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ which Lemma showed can only be bounded by $q^{g^2/2+o(1)}$ where q is the cardinality of the base field and g the dimension of the variety. This does not give much flexibility for working with vertical isogenies, and can make it quite costly to evaluate them.

On the other hand, we will later argue that horizontal isogenies are convenient to work with, as there are infinitely many with domain any given variety.



F . Structure of the graph of vertical isogenies and of the lattice of orders.

G S

As a consequence to the above, the structure of the vertical-isogeny graph can be described as resembling that of the lattice of orders which contain the minimal order $\mathbb{Z}[\pi,\overline{\pi}]$.

Corollary v.1.5. *Let* G *be the graph whose vertices are classes of varieties with Frobenius endomorphism* π, *up to horizontal isogenies, with edges the vertical isogenies of type* $(\mathbb{Z}/\ell)^g$. *Similarly, let* H *be the graph whose vertices are the orders containing* $\mathbb{Z}[\pi,\overline{\pi}]$, *with edges between two orders* $\mathcal{O} \subsetneq \mathcal{O}'$ *when there is no* $\mathcal{O}''$ *satisfying* $\mathcal{O} \subset \mathcal{O}'' \subset \mathcal{O}'$.

The map $(\mathscr{A} \to \mathscr{A}') \in$ G $\mapsto (\operatorname{End}\mathscr{A} \to \operatorname{End}\mathscr{A}') \in$ H *is bijective on the vertices, and splits edges into sequences of at most* $2g-1$ *edges.*

Figure is probably worth all the above words: it depicts the graph of vertical isogenies (the big circles denote horizontal isogenies classes) to the left, and the corresponding lattice of orders to the right. In fact, this is a simple case, similar to the situation in dimension one: each order above $\mathbb{Z}[\pi,\overline{\pi}]$ is uniquely identified by its index in $\mathcal{O}_K$, and vertical isogenies are in bijection with edges of the lattice of orders, that is, they do not jump orders.

Computing the endomorphism ring of a variety is therefore equivalent to determining its location *up to horizontal isogenies* in the isogeny graph.

To see how big this structure can be, consider the typical case of ordinary varieties of dimension $g = 2$ defined over the prime field with p elements. From the conditions on p-Weil polynomials, we deduce that there must be $p^{3/2+o(1)}$ isogeny classes. Since there are $p^{3+o(1)}$

isomorphism classes of curves, each isogeny class contains, on average, $p^{3/2+o(1)}$ isomorphism classes.

From now on, we will assume that the discriminant of $\mathbb{Z}[\pi, \overline{\pi}]$ (and therefore its index in the maximal order) has been fańored, so that we can make use of the various algorithms for lattices of orders developed earlier.

From a cryptanalysis viewpoint, if $\mathscr{A}$ is an abelian variety of which the discrete logarithm problem is to be used in a cryptographic scheme, and $\mathscr{A}'$ is a variety in the same isogeny class for which this problem is known to be weak, it should be ensured that it is infeasible to compute any isogeny $\mathscr{A} \to \mathscr{A}'$.

By the theory of complex multiplication, there are many horizontal isogenies of small degree going from any abelian variety $\mathscr{A}$ to others with the same endomorphism ring; therefore, horizontal isogeny classes can be "walked around" quite easily. Note, however, that ŏnding an explicit path from a prescribed variety to another might be a di cult task when the horizontal isogeny class is big, since only generic methods are available.

However, when $\mathscr{A}$ and $\mathscr{A}'$ have di erent endomorphism rings, denoting by ℓ the large prime fańor of dist(End $\mathscr{A}$, End $\mathscr{A}'$), any isogeny chain going from $\mathscr{A}$ to $\mathscr{A}'$ *mŬt* contain an isogeny of degree ℓ. Since current isogeny-computing algorithms require exponential time in $\log(\ell)$, this bounds below the time needed to tran ŕ ort the discrete logarithm problem.

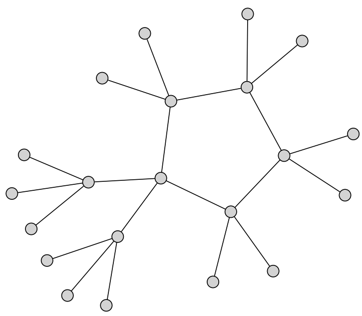
L S D O

F Ž and M ( ) gave a metaphorical interpretation of the work of K - ( ) on the ruńure of the graph of isogenies of type $\mathbb{Z}/\ell$, for a ŏxed prime ℓ, between ordinary elliptic curves deŏned over a ŏnite ŏeld. In dimension one, a number of properties which we sum up in the proposition below indeed give graphs of degree-ℓ isogenies a di inc-tive *ŀolcano* look.

Recall that the complex multiplication ŏelds of ordinary elliptic curves are exańly the imaginary quadratic number ŏelds; orders of such ŏelds are of the form $\mathbb{Z} + f\mathcal{O}_K$ where f is the index in the maximal order $\mathcal{O}_K$.

Ł e following rephrases Proposition of K ( ) and, for short, refers to isomorphism classes of elliptic curves as *curves* and to the valuation at a ŏxed prime ℓ of the condućor of their endomorphism ring as their *depū*.

Proposition v.1.6. *Consider ūe graph of śogenies of prime degree ℓ b'nween śomorphśm clńses of eŝiptic curves deŔned over a Ŕnite Ŕeld wiū complex multiplicŅion by ūe imaginary quadrŅic Ŕeld* $K = \mathbb{Q}(\sqrt{D})$ *of dścriminant* D*, and denote by* v *ūe valuŅion of* $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ *Ņ* ℓ*. Ń e foŝowing exhaŬtively describes aŝ edges of ūś graph.*



F . Typical volcano ruńure in dimension one when the discriminant is a square modulo ℓ (the prime degree of isogenies); here, in the case that $\ell = 3$.

. *From a curve Ņ depū* $u > 0$*, ūere ś one śogeny going up to a curve Ņ depū* $u - 1$.

. *From a curve Ņ depū* $u < v$*, ūere are* ℓ *śogenies going down to* ℓ *curves Ņ depū* $u + 1$*, unless* $u = 0$ *in which cńe ūere are* $\ell - 1$, ℓ*, or* $\ell + 1$ *when* D *ś reşeňively a square, zero, or a non-square modulo* ℓ.

. *From a curve Ņ depū* 0*, ūere are two śogenies going to curves Ņ depū* 0 *when* D *ś a square modulo* ℓ*, and one when* D *ś divśible by* ℓ.

Again, Figure is likely worth the above words: it di ŕ lays one conneńed component of the graph that we discussed; note that by the proposition and results of complex multiplication theory, all conneńed components of this graph are isomorphic.

Ł e algorithm of K ( ) computes the endomorphism ring of an ordinary curve $\mathscr{E}$ by determining the valuation of its conduńor at certain primes ℓ, for which it probes the location of $\mathscr{E}$ in the graph ruńure that we have ju described.

Ł is relies on the vertical ruńure of this graph being that of trees rooted on the (possibly degenerated) cycle of curves with locally maximal endomorphism rings. Note that this ruńure is lo in higher dimension, as we will later see.

K ’ A

K ( ) introduced many ideas and results related to the computation of endomorphism rings of elliptic curves over finite fields. Let us ju describe two of them which lead to his determini ic algorithm for computing the endomorphism ring $\mathrm{End}(\mathscr{E})$ of an ordinary elliptic curve $\mathscr{E}$ over $\mathbb{F}_q$ in time $q^{1/3+\varepsilon}$.

The first idea directly exploits the ructure of the volcano discussed above: the valuation of the conductor of $\mathrm{End}(\mathscr{E})$ at some prime ℓ can be found by determining on which level of the graph of degree-ℓ isogenies $\mathscr{E}$ lies. To this extent, compute three chains of degree-ℓ isogenies arting from $\mathscr{E}$; one chain necessarily descends to levels of higher depth, and eventually hits a leaf, that is, a curve with depth v from which no isogeny leaves but the dual of that with which we arrived. The set of leaves is called the *floor of rationality*; its curves only have one rational subgroup of order ℓ (whence the expression), and the ℓ remaining subgroups define isogenies over an extension of the base field. This gives the following algorithm.

Algorithm v.1.7.

I : *An ordinary elliptic curve* $\mathscr{E}/\mathbb{F}_q$.
O : *The conductor of its endomorphism ring.*

. *Count the points of* $\mathscr{E}$ *and deduce its complex multiplication field* K.
. *For each prime* ℓ *dividing* $[\mathscr{O}_K : \mathbb{Z}[\pi]]$:
. *Compute three curves* ℓ*-isogenous to* $\mathscr{E}$.
. *Keep walking a non-backward chain of* ℓ*-isogenies from each.*
. *Denote by* u_ℓ *the length of the chain that ends first* .
. *Return* $[\mathscr{O}_K : \mathbb{Z}[\pi]]/\prod \ell^{u_\ell}$.

By *non-backward*, we mean that we avoid duals of isogenies already computed. The first ep uses polynomially many operations in $\log(q)$. Each isogeny can then be computed in time $\ell^{2+o(1)}$ using the independent improvement of D ( ) and K ( ), Section . , on the formulas of V ( ); this process will be detailed in the next chapter. Since ℓ can be as large as $\sqrt{q}$, the overall complexity is only bounded by $q^{1+o(1)}$.

The second idea then comes to the rescue by trading o vertical isogenies for horizontal ones; the concise presentation below is largely inspired by a talk of K ( ).

Recall from complex multiplication theory that there are exactly $\#\mathrm{Pic}(\mathscr{O})$ curves with endomorphism ring $\mathscr{O}$, and that they form a connected component of the horizontal isogeny graph. Therefore, when ℓ is large, the value of u_ℓ can be te ed by comparing the class number of the order $\mathscr{O}$ with valuation u_ℓ to the number of curves in the horizontal isogeny component. Formally, this gives the algorithm below.

Algorithm v.1.8.

I : *An ordinary eŝiptic curve* $\mathscr{E}/\mathbb{F}_q$.

O : *Ńe conduňor of its endomorphśm ring.*

. *Count ūe points of* $\mathscr{E}$ *and deduce its complex multiplicŅion Ŕeld* K.

. *For each prime-power faňor* $\ell^\nu \leqslant q^{1/6}$ *of* $[\mathscr{O}_K : \mathbb{Z}[\pi]]$:

. *Apply ūe former algoriūm.*

. *For each prime-power faňor* $\ell^\nu > q^{1/6}$ *of* $[\mathscr{O}_K : \mathbb{Z}[\pi]]$:

. *Count ūe number of curves having horizonŪl śogenies to* $\mathscr{E}$.

. *D'nermine ūe order whose clńs group mŅches.*

Ł e horizontal isogenies of Step can be con ruńed as chains of isogenies of degree up to $12\log^2\Delta$, where $\Delta = \mathrm{disc}(K)$, by Ł eorem . . . In addition, not the whole horizontal isogeny class need be enumerated: it is su cient to compute enough of it so as to rule out other orders with smaller class number.

K ( ) concludes that:

Ŀeorem v.1.9 (GRH). *For any real number* $\varepsilon > 0$, *endomorphśm rings of ordinary eŝiptic curves can be computed in d'nerminśtic time* $q^{1/3+\varepsilon}$.

v.2 Higher Dimension

Before presenting methods for computing endomorphism rings in arbitrary dimension, let us describe more of the ruńure of isogeny graphs. We art by formalizing the localization of the lattice of orders at a prime; this isolates a subgraph of the corre ŕ onding isogeny graph ruńure. Ł en, we move on to describing those ŕ eciŏc a ŕ eńs of the isogeny graph which di er from dimension one to dimension two and more.

L O S

Fix a number ŏeld K and consider the lattice L of orders $\mathscr{O}$ that contain a prescribed *minimal order* $\mathfrak{m}$, which will be $\mathbb{Z}[\pi, \bar{\pi}]$ in our applications. Ł e index of any such order in the *maximal order* $\mathfrak{M} = \mathscr{O}_K$ then obviously divides $w = [\mathfrak{M} : \mathfrak{m}]$.

Now if ℓ is a prime fańor of w, we can *localize* the lattice of orders via the map

$$\begin{array}{rcl} L & \longrightarrow & L_\ell = \{\mathscr{O} \in L : [\mathfrak{M} : \mathscr{O}] \mid \ell^\infty\} \\ \mathscr{O} & \longmapsto & \mathscr{O}_\ell = \mathscr{O} + \mathfrak{m}_\ell \end{array}$$

where $\mathfrak{m}_\ell$ is the smalle order of the codomain, that is, the smalle order with index in $\mathfrak{M}$ a power of ℓ. Ł is projeńs $\mathscr{O}$ onto the maximal order $\mathfrak{M}$ locally at all primes but ℓ, thus isolating the local information at ℓ. This information can be recombined by the isomorphism

$$\begin{array}{ccc} L & \simeq & \prod_\ell L_\ell \\ \mathcal{O} & \longmapsto & \mathcal{O} + \mathfrak{m}_\ell \\ \bigcap_\ell \mathcal{O}_\ell & \longleftarrow & (\mathcal{O}_\ell) \end{array}$$

which can be evaluated in time polynomial in $\log|\Delta|$, where $\Delta = \mathrm{disc}(\mathfrak{m})$, using the classical algorithms from Chapter .

For us, K is the complex multiplication field of an ordinary abelian variety $\mathscr{A}$ over a finite field, and $\mathfrak{m} = \mathbb{Z}[\pi, \overline{\pi}]$. We will often say that we consider the endomorphism ring of $\mathscr{A}$ *locally at* ℓ to mean that we consider the localization $\mathrm{End}(\mathscr{A})_\ell$; by the above, knowing $\mathrm{End}(\mathscr{A})_\ell$ for each prime factor ℓ of w is sufficient to identify $\mathrm{End}(\mathscr{A})$ exactly.

Since isogenies of degree ℓ^n can only move endomorphism rings by distances that are powers of ℓ, the endomorphism rings of abelian varieties in a connected degree-ℓ vertical isogeny class are injectively projected to L_ℓ. Therefore, for the purpose of identifying the endomorphism ring using vertical isogenies, those of degree ℓ can be considered one prime ℓ at a time.

In dimension one, K is an imaginary quadratic field in which orders are uniquely identified by their index in $\mathcal{O}_K$. The local lattice L_ℓ is then the chain

$$\mathcal{O}_K \supset \mathbb{Z} + \ell\mathcal{O}_K \supset \mathbb{Z} + \ell^2\mathcal{O}_K \supset \cdots \supset \mathbb{Z} + \ell^{\mathrm{val}_\ell w}\mathcal{O}_K.$$

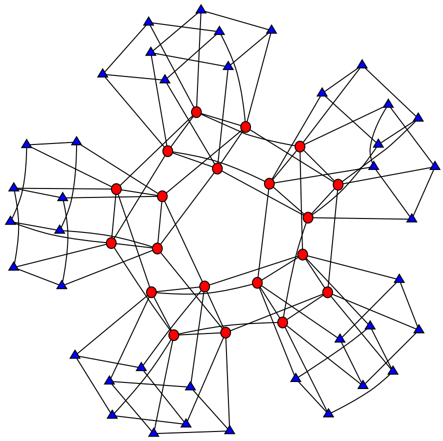
Consequently, it is really worthwhile for many algorithms dealing with imaginary quadratic orders to work locally, so as to benefit from this simple structure: this usually yields conceptually simpler algorithms. However, from dimension two on, the local lattice is not a tree but a general lattice itself, so it makes no conceptual difference whether one works locally or not, although it is advantageous for performance reasons.

L I S

Let us now briefly present the major differences between the degree-ℓ isogeny graph structure for elliptic curves and for higher-dimensional abelian varieties. Part of the last chapter will be devoted to giving details and results of computations on these aspects.

Let $\mathcal{O}$ be the endomorphism ring of an ordinary elliptic curve defined over a finite field. The distinctive look of its isogeny volcanoes stems from two properties:

- Rational primes ℓ split in at most two ideals of $\mathcal{O}$.
- Ideals of prime norm dividing the index $[\mathcal{O}_K : \mathcal{O}]$ are not invertible in $\mathcal{O}$.



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 8x^6 + 3x^5 + 7x^4 + 5x^3 + 12x^2 + 5x + 5$ over the field with 23 elements. Red circle varieties have maximal endomorphism ring, and blue triangle ones have index 9 in the maximal order.

By the theory of complex multiplication, the first property implies that elliptic curves with locally maximal endomorphism ring lie on (possibly degenerated) circles: the *crater* of the volcano. When the prime ℓ is inert, these circles degenerate into single vertices; when it splits as $\mathfrak{p}\overline{\mathfrak{p}}$, then each circle has length the order of $\mathfrak{p}$ in $\mathrm{Pic}(\mathcal{O})$. The second property implies that there are no horizontal isogenies of prime degree between elliptic curves with locally non-maximal endomorphism rings, that is, other than at the crater of the volcano.

Both properties are lost in higher dimension; indeed, if $\mathcal{O}$ is an order in a complex multiplication field of degree $2g$ for $g > 1$, then:

- Rational primes ℓ can split in up to $2g$ ideals of $\mathcal{O}$.
- Ideals of prime norm not coprime to the index $[\mathcal{O}_K : \mathcal{O}]$ may be invertible in $\mathcal{O}$.

This implies that horizontal degree-ℓ isogenies between varieties with locally maximal endomorphism rings now have a slightly more involved structure than a cycle, and that they might also exit other than at the top of the volcano. Both features are displayed on Figure .

We shall say more on this topic in the last chapter. In the meantime, the reader should not be misled into thinking that all higher dimensional local isogeny graphs portray the same structure as this specific one; however, this gives an idea why generalizing the algorithm of K ( ) for computing endomorphism rings cannot be done straightforwardly.

P T S

Although endomorphism rings of higher-dimensional abelian varieties cannot be determined by their vertical isogeny graph ruńure alone, other ruńures can be involved in a hope to adapt the method of K ( ) to this generalized setting.

I and J ( ) recently gave a method for ŏnding subgroups of order ℓ in ordinary elliptic curves over ŏnite ŏelds that are kernels of ascending or horizontal isogenies, meaning that they lead to curves with larger (or equal) endomorphism rings. Essentially, they exploit the relationship between the rational ℓ^∞-torsion subgroup ruńure of an elliptic curve and the valuation at ℓ of its endomorphism ring. To obtain the subgroup ruńure, they rely on pairing computations and on the algorithm of C ( ) for computing the torsion, which will be discussed in the next seńion.

Ł is permits one to navigate in the volcano not ju blindly relying on the tree ruńure of vertical isogenies, but with "some sense of orientation." Since we believe their method should be, to some extent, applicable to higher dimension varieties, we brieŒy present it.

A theorem of L ( ) ates the following.

Theorem v.2.1. *L'n π be ūe FrobeniŬ endomorphśm of an ordinary eŝiptic curve $\mathscr{E}$ deŔned over $\mathbb{F}_q$ and put $\mathscr{O} = \mathrm{End}(\mathscr{E})$. Ńe $\mathscr{O}$-modules $\mathscr{E}(\mathbb{F}_{q^n})$ and $\mathscr{O}/(\pi^n - 1)$ are śomorphic.*

Since $\mathscr{O}$ is a quadratic order, the group ruńure of the elliptic curve $\mathscr{E}(\mathbb{F}_q)$ is therefore of the form $\mathbb{Z}/N_0 \times \mathbb{Z}/N_1$ where $N_0 \mid N_1$. In particular, its ℓ^∞-torsion subgroup ruńure is of the form $\mathbb{Z}/\ell^{\alpha_0} \times \mathbb{Z}/\ell^{\alpha_1}$ and I and J ( ) derive explicit formulas for the integers α_0 and α_1 which show that they only depend on the valuation at ℓ of the conduńor of $\mathrm{End}(\mathscr{E})$.

To give an example of the ŕeciŏc way in which α_0 and α_1 are a eńed by vertical isogenies, let us reproduce Proposition of I and J ( ).

Proposition v.2.2. *L'n $\mathscr{E}$ be an eŝiptic curve of rŅional ℓ^∞-torsion subgroup $\mathbb{Z}/\ell^{\alpha_0} \times \mathbb{Z}/\ell^{\alpha_1}$ wiū $\alpha_1 > \alpha_0$. If P ś a point of order ℓ^{α_0}, ūen ūe śogeny wiū kernel generŅed by $\ell^{\alpha_0 - 1}P$ ś descending.*

Ł e computational ingredients are simple: we will present a torsion-ŏnding method in the next chapter, as it is needed in our own algorithms, and pairing evaluations are used to te relations between the order of ℓ^∞-torsion points. Ł erefore, we believe this method has a good potential of being generalized to higher dimension, at lea partially.

Since it is based on vertical isogenies, this approach is probably not be suited to computing endomorphism rings, as we argue below. Nevertheless, it has other intere ing applications which can be found in the original article.

L V I

Isogeny computation is currently a topic in active development for abelian varieties of dimension $g > 1$. The state-of-the-art algorithm of C and R ( ) can only compute isogenies of type $(\mathbb{Z}/\ell)^g$ and requires the prime ℓ to be reasonably small: although the asymptotic complexity is polynomial in ℓ and exponential in g, the constant factors and exponents are such that only a much more restricted range of isogenies can be computed than in dimension one.

We have argued before that vertical isogenies have constrained degrees; if certain isogenies are not within reach of known isogeny-computing methods, then their local vertical isogeny volcano is simply not computable. After our review of previous methods, the next chapter will present an algorithm which addresses this issue by relying on horizontal isogenies, whose degrees can be chosen with much more flexibility.

Another obstruction arises from the type of the isogenies that can be evaluated: consider a chain of orders

$$\mathcal{O}_K = \mathcal{O}_1 \supset \cdots \supset \mathcal{O}_v = \mathbb{Z}[\pi, \overline{\pi}]$$

where each order is contained in the following one with prime order ℓ; this is a simple case, as we have mentioned that there are others for $g > 1$, but it suffices to make our point.

W ( ) proved the existence of abelian varieties $\mathscr{A}_i$ with endomorphism ring $\mathcal{O}_i$ and T ( ) proved that there exist isogenies between all of the $\mathscr{A}_i$; the degrees of these isogenies are necessarily powers of ℓ.

However, the kernels of these isogenies need not be of type $(\mathbb{Z}/\ell)^g$ or a combination of such subgroups. In other words, in dimension g, we might "skip" up to $g-1$ orders when computing vertical isogenies. In the case that $g = 2$, for instance, starting from an abelian variety with endomorphism ring $\mathcal{O}_0$ and following isogenies of type $(\mathbb{Z}/\ell)^2$ we might only reach abelian varieties with endomorphism ring $\mathcal{O}_i$ for i even, and fail to reach those with i odd. The last chapter will give several examples illustrating this.

v.3 General Methods

Two methods were previously known for computing endomorphism rings of general abelian varieties $\mathscr{A}$ defined over finite fields. Both test whether elements α of the complex multiplication field $K = \mathbb{Q}(\pi)$ correspond to endomorphisms of $\mathscr{A}$; doing so for generating sets of orders permits one to eventually recover the full endomorphism ring.

To find whether $\alpha \in \mathrm{End}(\mathscr{A})$, the method of E and L ( ) tests if some easy-to-evaluate multiple $n\alpha$ kills the full n torsion subgroup of $\mathscr{A}$.

Recently, W ( ) designed a new method which can loosely be under ood as a Chinese remainder theorem variant of the latter: to determine whether $\alpha \in \mathrm{End}(\mathscr{A})$, it tries to interpolate the potential corre ŕ onding endomorphism over small torsion subgroups.

E E

Let $\mathscr{A}$ be a simple ordinary principally polarized abelian variety deŏned over the ŏeld with q elements. Since the endomorphism ring of $\mathscr{A}$ always contains the order $\mathbb{Z}[\pi,\overline{\pi}]$, let us explain how the ańion on $\mathscr{A}$ of an endomorphism α of this subring can be evaluated.

Evaluating the Frobenius endomorphism π is raightforward: it su ces to put the coordinates of a point to the q^{th} power, which, using a double-and-add approach, only requires a number of base ŏeld multiplications that is polynomial in $\log(q)$. On the other hand, evaluating the Verschiebung endomorphism $\overline{\pi} = q/\pi$ is more involved but can be avoided, unless p divides the conduńor of $\mathbb{Z}[\pi,\overline{\pi}]$ where p is the prime of which q is a power.

Since $K = \mathbb{Q}(\pi)$, any element $\alpha \in K$ can be written as a rational polynomial in the Frobenius endomorphism π: if $2g$ is the degree of the ŏeld, there exi an integer n and integers α_i for $i \in \{0,\dots,2g-1\}$ such that

$$\alpha = \frac{1}{n}\sum_i \alpha_i \pi^i.$$

Computing α therefore amounts to evaluating the Frobenius endomorphism, scalar multiplications, endomorphism compositions, and one division. Note that division by n is easily computed on torsion subgroups of $\mathscr{A}$ of order coprime to n: simply multiply by the inverse of n modulo the order. Subgroups of order not coprime to n will soon be addressed.

In the following, α will always be an algebraic integer of K, and we assume this from now on. Put $w' = [\mathscr{O}_K : \mathbb{Z}[\pi]]$; as a group, $\frac{1}{w'}\mathbb{Z}[\pi]$ then contains $\mathscr{O}_K$. Ł erefore, α can be written in the form above for some integer n dividing w'. And this is in fań always the case when the above expression is reduced, meaning that $\gcd(\alpha_i, n) = 1$.

Recall from Lemma . . that $w'/w = [\mathbb{Z}[\pi,\overline{\pi}] : \mathbb{Z}[\pi]] = q^{g(g-1)/2}$ where $w = [\mathscr{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ as before. As a consequence, the prime fańors of the denominator n are those of w (that is, the degrees of vertical isogenies) plus, possibly, q.

T E –L M

We now present the method of E and L ( ); it was ŏr targeted at te ing whether endomorphism rings of abelian varieties over ŏnite ŏelds are maximal, but it applies to other orders as well. It relies on Corollary which reads as follows.

Proposition V.3.1. *Let $\mathscr{A}$ be an abelian variety defined over an algebraically closed field. If* α *is an endomorphism of* $\mathscr{A}$ *and n is coprime to the ambient characteristic, then* $\mathscr{A}[n] \subset \ker(\alpha)$ *if and only if* $\alpha/n \in \mathrm{End}(\mathscr{A})$*, that is, if there exists an endomorphism* β *such that* $\alpha = n \circ \beta = \beta \circ n$.

In other words, the endomorphism corresponding to the algebraic integer α kills the full n-torsion subgroup if and only if α/n belongs to the endomorphism ring.

As we have mentioned before, when $\mathscr{A}$ is ordinary, assuming the base field to be algebraically closed does not affect the endomorphism ring; it only demands that we compute the full n-torsion of $\mathscr{A}$, possibly over an extension of the actual (finite) base field.

Consequently, an order $\mathscr{O}$ of the complex multiplication field K of $\mathscr{A}$ can be tested to be contained in $\mathrm{End}(\mathscr{A})$ by computing a generating set for $\mathscr{O}$, writing its elements α in the form $\frac{1}{n}\sum_i \alpha_i \pi^i$, and testing whether $\sum_i \alpha_i \pi^i$ kills the full n-torsion of $\mathscr{A}$ for all such α. A module basis for $\mathscr{O}$ has cardinality $2g$, but since $\mathbb{Z}$ is contained in both $\mathscr{O}$ and $\mathbb{Z}[\pi]$, only $2g-1$ tests are really required; furthermore, as only an algebra basis is required, much fewer elements actually need to be tested.

The proposition requires denominators n to be coprime to the order q of the base field. When the index $[\mathscr{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ is coprime to q, this can always be made the case: since the index of $\mathbb{Z}[\pi,\overline{\pi},q\alpha]$ in $\mathbb{Z}[\pi,\overline{\pi},\alpha]$ divides q and both orders contain $\mathbb{Z}[\pi,\overline{\pi}]$, this index must be one, which means that $q\alpha$ and α belong exactly to the same orders above $\mathbb{Z}[\pi,\overline{\pi}]$; therefore, the factor of n divisible by a power of q can simply be dropped.

This method is suited to local computations: similarly to what we did above, if ℓ is a prime, one can show that $\mathrm{End}(\mathscr{A})_\ell = \mathscr{O}_\ell$ can be determined only using elements whose denominators are powers of ℓ. We will later rely on this local version to determine the endomorphism ring locally at small primes ℓ where our own algorithm fails to compute it.

When g is fixed and we work over base fields of increasing prime cardinality q, it becomes increasingly rare for q to divide the index $\mathbb{Z}[\pi,\overline{\pi}]$, although this can be seen to happen. In those cases where we want to determine the endomorphism ring locally at a large prime, the present method is probably not the best suited in the first place.

Two building blocks remain to be explained: computing the full ℓ-torsion, and efficiently finding the endomorphism ring by testing whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$ for chosen orders $\mathscr{O}$; algorithms for both will be described and analyzed in the next chapter. When g is fixed and q goes to infinity, we deduce that the worst-case overall complexity of this method is

$$\ell^{2g+o(1)} \log^{2+o(1)} q \qquad \text{where} \qquad \ell = q^{g^2/2+o(1)}.$$

Note that in the case that we only wish to test whether $\mathrm{End}(\mathscr{A})$ is maximal, F and L ( ) subsequently improved this method using specific probabilistic tests.

C E

Let us now briefly introduce elements of the theory of correspondences as background material for the work of W ( ), which will be discussed below.

First define a *function field* K over k (which we write K/k) as a finitely generated extension of transcendence degree one. In Chapter , we saw that function fields arise from algebraic varieties, but here we will work with them abstractly. For details on the following, we refer to Chapter of the collection of lectures by D ( ).

Definition v.3.2. *Let* K/k *be a function field, and* K'/k *an extension field. There exists a function field* L/l *such that* L *contains* K, $l \cap K = k$, *and* L *is the composite extension of* K *and a subfield of* l *that is* k*-isomorphic to* K'.

The function field L/l *is called the* constant field extension *of* K/k *by* K'/k.

D ( ) introduced *correspondences* as ideals of maximal orders of function fields L/l, up to both principal ideals and *constant ideals*, that is, ideals with nontrivial intersection with l. When L is the constant field extension of a function field $k(\mathscr{C})/k$ by another $k(\mathscr{C}')/k$ where $\mathscr{C}$ and $\mathscr{C}'$ are two algebraic curves defined over a finite field k, he showed that correspondence classes represent isogenies from the Jacobian variety of $\mathscr{C}$ to that of $\mathscr{C}'$.

In the particular case that $\mathscr{C} = \mathscr{C}'$, this gives a bijection

$$C : \mathrm{End}(\mathrm{Jac}\,\mathscr{C}) \xrightarrow{\sim} \{\text{correspondence classes}\} = \mathfrak{I}(\mathscr{O}_L)/\sim$$

which is compatible with the ring structure in the sense that for all endomorphisms α and β we have $C(\alpha + \beta) = C(\alpha) \cdot C(\beta)$, and similarly there exists a computational way of deriving the composition $C(\alpha \circ \beta)$ from $C(\alpha)$ and $C(\beta)$.

For instance, correspondences representing the Frobenius endomorphism π, the Verschiebung endomorphism $\overline{\pi}$, and the identity I are easily obtained; multiplication-by-n is then represented by $C(I)^n$, and so on.

Finally, and this is maybe the most crucial point for what follows, the action of a correspondence on a point, that is, that of the endomorphism it represents can be evaluated simply in terms of elementary function field operations.

W ’ A

To determine whether some prescribed algebraic number of $\mathbb{Q} \otimes \mathrm{End}(\mathrm{Jac}\,\mathscr{C})$ represents an endomorphism, start as before by writing it as an element $\alpha \in \mathbb{Z}[\pi]$ divided by some integer n; the correspondence class $C(\alpha)$ is easily computed from $C(\pi)$, so it remains to determine whether it can be divided by n.

The main idea of W ( ) is to interpolate the hypothetical correspondence class $C(\alpha/n)$ over a set of small-torsion points: let P_i be a point of $\mathrm{Jac}(\mathscr{C})$ of order m_i; if it exists, $C(\alpha/n)$ should act as

$$P_i \longmapsto (n^{-1} \bmod m_i) C(\alpha)(P_i);$$

and we can write equations asserting that a formal correspondence class D acts this way. W ( ) gives an upper bound on the number of points P_i required to completely characterize the action of α/n, that is, ensuring that if the system admits a solution D, then we must have $D = C(\alpha/n)$, and as a consequence $\alpha/n \in \mathrm{End}(\mathrm{Jac}\,\mathscr{C})$.

He exhibits correspondence class representatives which are compatible with the above operations and therefore allow efficient correspondence class computations. These representatives are written in Hermite normal form and are almost entirely determined by their norms due to the restrictive conditions required for being a representative.

Therefore, W ( ) focuses on *interpolating the norm*, which is of the form

$$N_{L/k(\mathscr{C})}(C(\alpha/n)) = x^l + \sum_{i=0}^{l-1} \frac{f_i}{g_i} x^i$$

for some degree $l \leqslant g$, where the indeterminates f_i and g_i are polynomials of bounded degree with coefficients in $k(\mathscr{C})$; see “Abschätzung der Grade der Polynome in x_2” in Section . on page .

The whole procedure is summarized in “Algorithmus : Approximation” of the same section on page . That algorithm takes as input a $\mathbb{Z}$-basis β of an order $\mathscr{O}$ of which $C(\beta)$ is known, an element α of some order $\mathscr{O}$, and an integer n; if α/n is an endomorphism, it returns a correspondence representing it, or returns `false` otherwise.

As we will describe in the next chapter, being able to test whether prescribed orders $\mathscr{O}$ are contained in the endomorphism ring suffices to determine it in a polynomial number of steps in the size of the base field.

A short analysis of the method can be found in Section . ; in brief, the degree of the norm of α/n is polynomial in n and it thus requires interpolating a number of points which is polynomial in n. In the worst case, the overall algorithm therefore uses exponential time in the size of the base field.

Nevertheless, it has the interesting feature that, as n grows, testing whether α/n is an endomorphism becomes easier; indeed, the size of the hypothetical correspondence representing it then gets smaller, so a shorter system of equations can be used. Note that all methods we have previously seen showed the reverse phenomenon.

V.4 Supersingular Methods

For the sake of completeness, let us address the case of supersingular elliptic curves in this seńion (and this seńion only). Known methods for computing endomorphism rings of such curves all have an exponential asymptotic running time in the size of the base ŏeld; however, contrary to the ordinary case, we are quite pessimi ic about the possibilities of improvement.

In addition to the methods presented here, we note that K ( ) has an algorithm that gives some information on the endomorphism ring of supersingular curves which sufŏces to determine it only in ŕeciŏc cases; however, we are unaware of further developments of this technique.

I S C

We ŏr present background results on supersingular elliptic curves, their isogeny classes, and their endomorphism rings. Mo results originate from D ( ).

Recall that an elliptic curve $\mathscr{E}$ deŏned over a ŏnite ŏeld of charańeri ic p is *supersingular* when it has no p-torsion. As a meager compensation for the troubles ahead, we have:

Proposition V.4.1. *Up to śomorphśm, every supersingular eŝiptic curve deŔned over a Ŕnite Ŕeld of charaňerśtic p ś deŔned over* $\mathbb{F}_{p^2}$*.*

As a consequence, it is simple to enumerate all such isomorphism classes. Endomorphism rings of supersingular curves can similarly be enumerated simply.

Proposition V.4.2. *Endomorphśm rings of supersingular curves corre ş ond bŜeňively to maximal orders of $\mathbb{Q}_{p,\infty}$, ū e quŅernion algebra ramiŔed only Ņ p and ∞. Two such curves deŔned over $\mathbb{F}_{p^2}$ have ū e same endomorphśm ring if and only if ū ey are conjugŅe under* $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$*.*

Ł is is why we are sceptical as to the possibilities of sub antial improvements on the computation of endomorphism rings in this case: since all orders are maximal, and there are exponentially many of them, there seems to be no way around considering each, one at a time. Although we have not yet presented our method which exploits the rućure of the lattice of orders in the ordinary case, the localization that we have described earlier (and which su ces in dimension one) should convince the reader of the beneŏt of having such a rućure.

As for ordinary curves, there is a theory of complex multiplication; however, care mu be taken due to its non-commutativity.

Proposition V.4.3. *Fix a supersingular curve $\mathscr{E}$. For any leŚ ideal $\mathfrak{a}$ of* $\mathrm{End}(\mathscr{E})$ *coprime to p, ū e degree of ū e śogeny $\varphi_{\mathfrak{a}}$ wiū kernel* $\ker(\varphi_{\mathfrak{a}}) = \cap_{\alpha\in\mathfrak{a}} \ker(\alpha)$ *ś ū e norm of $\mathfrak{a}$; aŝ śogenies b'nween supersingular curves arśe in ū ś way.*

If $\mathscr{E}' = \varphi\ (\mathscr{E})$*, ūen* End$(\mathscr{E}')$ *ś ūe right order of* $\mathfrak{a}$*, ūŅ ś,* $\{x \in \mathbb{Q}_{p,\infty} : \mathfrak{a}x \subset \mathfrak{a}\}$*. If additionaŝy* $\mathscr{E}'' = \varphi\ (\mathscr{E})$*, ūe curves* $\mathscr{E}'$ *and* $\mathscr{E}''$ *are śomorphic if and only if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are in ūe same leŚ ideal clńs.*

Much more can be said on the ruńure of this isogeny graph: for in ance, when $p = 1 \bmod 12$, it is a Ramanujan graph, a particular case of expander graph with desirable prop-

Repeating the above for various primes ℓ di erent from the charańeri ic rules out orders $\mathscr{O}$ from the candidate li , so that eventually the endomorphism ring alone remains. Ł is formally proceeds as the following procedure.

Algorithm v.4.4.

I : *A supersingular eŝiptic curve* $\mathscr{E}/\mathbb{F}_{p^2}$.

O : *An order śomorphic to its endomorphśm ring.*

. *L'n* L *be ū e lśt of maximal orders of* $\mathbb{Q}_{p,\infty}$.

. *Until* L *ś a singl'non:*

. *Pick a prime* ℓ*, and count ū e degree-*ℓ *endomorphśms of* $\mathscr{E}$.

. *Rule out orders of* L *wi ū a di erent count of elements of norm* ℓ.

. *R'nurn ū e only element in* L.

For Step M M and L ( ) derive an explicit method in Seńion . ; it boils down to ŏnding integer solutions of a quadratic equation.

Ł is procedure behaves quite well in prańice: its bottleneck is the enumeration of isogenies of degree ℓ from $\mathscr{E}$ to $\mathscr{E}$; M M and L ( ) give explicit formulas for $\ell = 2$ and $\ell = 3$, and the isogeny-computing machinery for elliptic curves is nowadays at a age of development where such operations can be performed quickly for a large range of ℓ.

However, we ress that its termination is not guaranteed, as two di inń maximal orders of $\mathbb{Q}_{p,\infty}$ might have the same number of ideals of norm ℓ for inŏnitely many primes ℓ.

C ' A

Although te ing the norm of ideals alone is not su cient to guarantee the termination of the endomorphism-ring identifying process, C ( ) observed in his Proposition . that considering both the norm *and* the trace yields a su cient amount of information aŔer ŏnitely many te s. More precisely, he proved the following.

Proposition v.4.5. *No two maximal orders of ū e quŅernion algebra* $\mathbb{Q}_{p,\infty}$ *have ū e same s'n*

$$\left\{\left(\mathrm{tr}(\alpha), \mathrm{N}(\alpha)\right) : \alpha \in \mathscr{O}, \mathrm{N}(\alpha) \leqslant b\right\}$$

where b ś a cerŪin bound which ś $\mathrm{O}(p)$.

Ł e norm and trace of such numbers map to the norm and trace of the charańeri ic polynomial of the corre ŕ onding endomorphism: we have

$$\varphi^{(2)} - \mathrm{tr}(\varphi)\varphi + \mathrm{N}(\varphi) = 0$$

since the degree (or norm) of an isogeny is always known (as we con ruń them from their kernels), the trace of φ can be found by te ing the possible values in turn over a su ciently large extension of the base ŏeld.

Ł is gives the following algorithm.

Algorithm v.4.6.

I : *A supersingular eŝiptic curve* $\mathscr{E}/\mathbb{F}_{p^2}$.
O : *An order śomorphic to its endomorphśm ring.*

. *L'n* L *be ū e lśt of maximal orders of* $\mathbb{Q}_{p,\infty}$.
. *For successive primes* ℓ, *arting Řom* $\ell = 2$*:*
. *Compute ū e multś'n* $I = \{\mathrm{tr}(\varphi)\}$,
where φ *ranges over degree-*ℓ *endomorphśms of* $\mathscr{E}$.
. *Rule out Řom* L *ū ose orders* $\mathcal{O}$ *for which* $I \neq \{\mathrm{tr}(\beta)\}$
where β *ranges over ū e elements of norm* ℓ *in* $\mathcal{O}$.
. *R'nurn ū e only element in* L.

By the proposition above, this algorithm terminates aŔer $O(p)$ operations. Nevertheless, since computing the trace of the endomorphisms is extremely co ly, the former procedure is more suited to a large range of prańical problems, although it is not guaranteed to terminate.

References

. Max D .
"Arithmetische Ł eorie der Korre ŕ ondenzen algebraischer Funktionenkörper".
In: *Journal für die reine und angewandte MŅhemŅik* . . Pages – .
DOI: `10.1515/crll.1937.177.161`.

. Max D .
"Die Typen der Multiplikatorenringe elliptischer Funktionenkörper".
In: *Abhandlungen aŬ dem mŅhemŅśchen Seminar der hamburgśchen Universität* . Pages – .

. John T .
"Endomorphisms of abelian varieties over ŏnite ŏelds".
In: *Inŀentiones mŅhemŅicae* . . Pages – . DOI: `10.1007/BF01404549`.

. William C. W .
"Abelian varieties over ŏnite ŏelds".
In: *Annales ScientiŔques de l'École Normale Supérieure* . . Pages – .

. Jacques V .
"Isogénies entre courbes elliptiques".
In: *Comptes RendŬ de l'Académie des Sciences de Parś*. A . Pages – .

. Max D .
Leňures on ūe Ńeory of Algebraic Funňions of One Variable. Volume .
Leńure Notes in Mathematics. Springer. ISBN: - - - .

. Arnold P .
"An algorithm for computing modular forms on $\Gamma_0(N)$".
In: *Journal of Algebra* . . Pages – .
DOI: `10.1016/0021-8693(80)90151-9`.

. Laurent D .
Un coroŝaire aux formules de Vélu. Preprint.

. David R. K .
"Endomorphism rings of elliptic curves over ŏnite ŏelds".
PhD thesis. University of California at Berkeley.
URL: `http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf`.

. Hendrik W. L .
.
[illegible]

Edited by Jean C , James H , and Robert R . Volume .
Number Ł eory and Its Applications. World Scientiõc. Pages – .
DOI: 10.1142/9789812793430_0002.

. Denis X. C , Kri in E. L , and Eyal Z. G .
"Cryptographic hash funńions from expander graphs".
In: *Journal of Cryptology* . . Pages – .
DOI: 10.1007/s00145-007-9002-x.

. Jean-Marc C .
"Linearizing torsion classes in the Picard group of algebraic curves over õnite õelds".
In: *Journal of Algebra* . . Pages – .
DOI: 10.1016/j.jalgebra.2008.09.032.

. Kir en E and Kri in E. L .
"A CRT algorithm for con ruńing genus curves over õnite õelds".
In: *Ariūm'nic, Geom'nry and Coding Ń eory — AGCT '* .
Edited by François R and Serge V . Volume . Séminaires et Congrès.
Société Mathématique de France. Pages – .

. Markus W .
"Über Korreŕondenzen zwischen algebraischen Funktionenkörper".
PhD thesis. Technische Universität Berlin.
URL: http://www.math.tu-berlin.de/~wagner/Diss.pdf.

. Sorina I and Antoine J .
"Pairing the volcano". In: *Algoriūmic Number Ń eory — ANTS-IX*.
Edited by Guillaume H , François M , and Emmanuel T .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-642-14518-6_18.

. David R. K .
"Endomorphisms, isogeny graphs, and moduli".
In: *Workshop on Eŝiptic Curves and CompuŪtion — ECC '* . URL:
http://research.microsoft.com/apps/video/dl.aspx?id=140496.

. Romain C and Damien R .
Computing (ℓ,ℓ)*-śogenies in polynomial time on Jacobians of genŬ curves.*
IACR ePrint: 2011/143.

Subexponential Method

We have so far discussed endomorphism-ring computation methods with an exponential worst-case runtime, and will now present one of subexponential complexity.

This method was first introduced in B. and S ( ) under a form quite specific to elliptic curves, and relying on several unproven assumptions. All assumptions but the GRH were later removed in B. ( ) by modifying parts of the algorithm. Here, we present a variant of this algorithm which applies to general abelian varieties.

We stress that this chapter considers abelian varieties without taking polarizations into account, which is not an effective approach in dimension $g > 1$, but allows for a conceptually simpler presentation. For $g = 1$, where polarizations are unneeded, it is highly effective, and the next chapter will be devoted to rigorously proving its probabilistic runtime under the generalized Riemann hypothesis, and its unconditional correctness.

Modifications that make our method practical for $g = 2$ will be presented in the last chapter; they are expectedly slower and rely on more unproven hypotheses.

VI.1 Algorithm Overview

Let $\mathscr{A}$ be a simple ordinary abelian variety defined over a finite field; denote by K its complex multiplication field and fix an isomorphism $\iota : K \to \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$, which will be implicitly understood from now on.

To locate $\mathrm{End}(\mathscr{A})$ among candidate orders of K, the main idea to our subexponential method is to compute certain properties describing the Picard groups of candidate orders, and to test them via complex multiplication in the horizontal isogeny graph. Since there exist subexponential algorithms for computing Picard groups we are done... Almost so.

We now give the main ingredients enabling this approach. Computational details are given in subsequent sections, while proofs and rigorous analysis are in the next chapter.

L O

Let us first briefly recall results that express where the endomorphism ring is to be sought.

Let $\mathscr{A}$ be a simple ordinary abelian variety of dimension g defined over a finite field with q elements. The Frobenius endomorphism π acts on geometric points of $\mathscr{A}$ by raising their coordinates to the q^{th} power; its characteristic polynomial $\chi_\pi(x)$ is a q-Weil polynomial, which means that it is monic, has integer coefficients, and has $2g$ complex roots, each of absolute value $\sqrt{q}$.

Computing this polynomial is equivalent to counting the number of points on the variety defined over the finite field k with endomorphism ring $\mathcal{O}$ by $\mathfrak{a} : \mathcal{A} \mapsto \varphi_{\mathfrak{a}}(\mathcal{A})$ where $\varphi_{\mathfrak{a}}$ denotes the isogeny with kernel $\bigcap_{\alpha\in\mathfrak{a}} \ker(\alpha)$. We assume that this induces a faithful and transitive action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{AV}_{\mathcal{O}}(k)$; by complex multiplication theory, this is always the case when $\mathcal{O}$ is an imaginary quadratic order, or a ring of integers.

Intuitively, the structure of the Picard group of $\mathrm{End}(\mathcal{A})$ therefore dictates that of the horizontal isogeny graph component containing $\mathcal{A}$. Our approach is essentially to look at the latter and deduce information on the former, which might eventually lead to the identification of $\mathrm{End}(\mathcal{A})$. We formalize the notion of *structure* by the following concept.

Definition VI.1.1. *An ideal $\mathfrak{a}$ of $\mathbb{Z}[\pi,\overline{\pi}]$ is said to be* principal in $\mathcal{O}$ *if the ideal $\mathfrak{a}\mathcal{O}$ is principal; it is said to be* principal in the isogeny graph *when the isogeny $\varphi_{\mathfrak{a}}$ is an endomorphism of $\mathcal{A}$.*

In fact, we meant $\varphi_{\mathfrak{a}\mathrm{End}(\mathcal{A})}$ rather than $\varphi_{\mathfrak{a}}$ since we want it to act on $\mathcal{A}$ even though $\mathfrak{a}$ is an ideal of $\mathbb{Z}[\pi,\overline{\pi}]$. Obviously, since we are looking for $\mathrm{End}(\mathcal{A})$ we cannot really compute $\mathfrak{a}\mathrm{End}(\mathcal{A})$, but we will see later that $\varphi_{\mathfrak{a}\mathrm{End}(\mathcal{A})}$ can be computed regardless.

Therefore, an ideal is principal in $\mathrm{End}(\mathcal{A})$ if and only if it is principal in the isogeny graph, which gives a way to tell the endomorphism ring apart from other orders of the lattice. To avoid testing all orders, we rely on this simple result.

Lemma VI.1.2. *If an ideal is principal in some order, it is principal in all orders containing it.*

Indeed, if $\mathcal{O} \subset \mathcal{O}'$ are two orders containing $\mathbb{Z}[\pi,\overline{\pi}]$, the map $\mathfrak{a} \in \mathfrak{I}(\mathcal{O}) \mapsto \mathfrak{a}\mathcal{O}' \in \mathfrak{I}(\mathcal{O}')$ induces, as we have mentioned before, a surjective morphism of Picard groups. Intuitively, this means that more and more ideals become principal as we ascend the lattice of orders, or equivalently that Picard groups get smaller. This is why we chose $\mathbb{Z}[\pi,\overline{\pi}]$ to be the ring of our ideals: via the morphism $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}$ we can map ideals of $\mathbb{Z}[\pi,\overline{\pi}]$ to any order of the lattice.

Computationally, the lemma above implies that by verifying whether principal ideals of $\mathcal{O}$ are also principal in the isogeny graph, we can convince ourselves that $\mathcal{O}$ is contained in $\mathrm{End}(\mathcal{A})$. However, this approach does not prove anything (in fact, it fails in certain rare cases that we will cover later); to rigorously assert the location of the endomorphism ring, we use the following concept.

Definition VI.1.3. *A* certificate *for the order $\mathcal{O}$ consists of:*

- *a family of orders $\mathcal{O}_i$ and ideals $\mathfrak{a}_i$ principal in $\mathcal{O}_i$ but not in $\mathcal{O}$,*
- *a family of orders $\mathcal{O}_j$ and ideals $\mathfrak{a}_j$ principal in $\mathcal{O}$ but not in $\mathcal{O}_j$,*

such that $\mathcal{O}$ is the only order above $\mathbb{Z}[\pi,\overline{\pi}]$ satisfying $\mathcal{O}_i \not\subset \mathcal{O}$ and $\mathcal{O}_j \not\supset \mathcal{O}$ for all indices.

It is said to be verified *on the abelian variety $\mathcal{A}$ if the ideals $\mathfrak{a}_j$ are principal in its isogeny graph whereas the $\mathfrak{a}_i$ are not.*

If a certiőcate for the order $\mathscr{O}$ is veriőed on the abelian variety $\mathscr{A}$, by the contrapositive of the lemma above, then we have $\mathrm{End}(\mathscr{A}) = \mathscr{O}$. In fań, the family $(\mathscr{O}_i, \mathfrak{a}_i)$ is e eńively con ruńed when one executes the lattice-ascending walk that we are about to describe; the family $\mathscr{O}_j$ is then typically chosen to consi of all orders immediately below $\mathscr{O}$, that is, ju one level below $\mathscr{O}$ in the lattice of orders.

Ł e next seńion will address the search for ideals and, as a consequence, show that it takes $\mathrm{L}(q^{g^2})^{1/4\gamma+o(1)}$ time to generate a certiőcate that can subsequently be veriőed within $\mathrm{L}(q^{g^2})^{3g\gamma+o(1)}$ operations, as q goes to inőnity and γ is any positive con ant real number. Ł is eliminates the need to carefully ensure the correńness of our algorithm: we can simply run an algorithm that is only proven to return a correń result with probability $\varepsilon > 0$ and, when it does return a result, verify it using our certiőcate method; if it proves to be incorreń, we art over. Ł e expeńed overhead on the complexity is $1/\varepsilon$.

C B

To search for the endomorphism ring $\mathrm{End}(\mathscr{A})$ in the lattice of orders, we *te* whether orders $\mathscr{O}$ lie below it by seleńing principal ideals of them and checking whether they are principal in the isogeny graph.

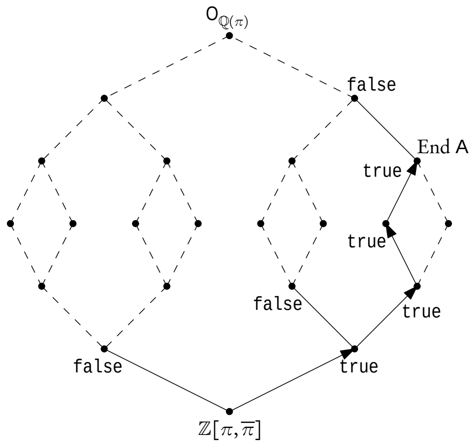
It remains to design a general rategy to seleń the orders to be te ed.

We shall say that an order $\mathscr{O}$ lies direńly above another $\mathscr{O}'$ if we have $\mathscr{O} \supset \mathscr{O}'$ but there exi s no order $\mathscr{O}''$ di erent from $\mathscr{O}$ and $\mathscr{O}'$ satisfying $\mathscr{O} \supset \mathscr{O}'' \supset \mathscr{O}'$; we also deőne the corre ŕ onding notion of "direńly below" where inclusions are reversed. As an example, when an order contains another with prime index, then it mu lie direńly above it.

To ascend the lattice of orders, we proceed one ep at a time: each ep consi s in enumerating all orders lying direńly above a prescribed order $\mathscr{O}'$. We have seen that the index of $\mathscr{O}'$ in any order direńly above it is a divisor of ℓ^{2g-1} where ℓ is a prime fańor of $[\mathscr{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$. By fańoring Δ we therefore obtain the possible values of ℓ, and we can then use the algorithm described earlier that li s those orders containing $\mathscr{O}'$ with a prescribed index.

Our rategy to locate the endomorphism ring in this lattice by te ing orders and ascending in corre ŕ onding direńions works as follows: given some order $\mathscr{O}'$ contained in $\mathrm{End}(\mathscr{A})$ (we art with $\mathscr{O}' = \mathbb{Z}[\pi, \overline{\pi}]$), őnd some order $\mathscr{O}$ direńly above $\mathscr{O}'$ which lies below $\mathrm{End}(\mathscr{A})$; then replace $\mathscr{O}'$ by $\mathscr{O}$ and iterate the process. Ł e ascension ends when no $\mathscr{O}$ is found to be contained in $\mathrm{End}(\mathscr{A})$; then, we mu have $\mathrm{End}(\mathscr{A}) \simeq \mathscr{O}'$. See Figure where we art from the bottom and ascend towards orders $\mathscr{O}$ for which the atement $\mathscr{O} \subset \mathrm{End}(\mathscr{A})$ holds.

Formally, we obtain the following algorithm.



F . Locating End($\mathscr{A}$) by ascending a te -sequence of orders.

Algorithm VI.1.4.

I : *A simple ordinary abelian vari’ny $\mathscr{A}$ over a Ŕnite Ŕeld $\mathbb{F}_q$.*

O : *An order śomorphic to its endomorphśm ring.*

. *Compute ūe FrobeniŬ polynomial $\chi_\pi(x)$ of $\mathscr{A}$.*

. *Faňor ūe dścriminant Δ and con ruň ūe order $\mathscr{O}' = \mathbb{Z}[\pi,\overline{\pi}]$.*

. *For orders $\mathscr{O}$ direňly abol·e $\mathscr{O}'$:*

. *If $\mathscr{O} \subset \mathrm{End}(\mathscr{A})$ s’n $\mathscr{O}' \leftarrow \mathscr{O}$ and go to Step .*

. *R’nurn $\mathscr{O}'$.*

To te whether an order lies above $\mathscr{O}$ we compute su ciently many principal ideals of it and te whether they are principal in the isogeny graph. Before detailing this process, let us present an alternative approach to locating the endomorphism ring in the lattice of orders.

Łe next seńions will show that it requires $L(|\Delta|)^{1/4\gamma+o(1)}$ time to ŏnd random principal ideals $\mathscr{O}$ whose associated isogenies can be computed within $L(|\Delta|)^{3g\gamma+o(1)}$ operations; to balance these co s, we set $\gamma = 1/\sqrt{12g}$ and since $|\Delta| < q^{g^2+o(1)}$ we ŏnd an overall runtime of

$$L(q)^{g\sqrt{3g}/2+o(1)}.$$

Note that for $g = 1$ we can do better by using a fa er isogeny computing method whose exponent is ju 2γ in ead of $3g\gamma$ for the arbitrary-dimension method.

C A

Rather than art at the bottom of the lattice and ascend towards the endomorphism ring, we can generate certiŏcates for each order arting from the top and attempt to verify them; to ensure this only uses subexponentially many operations, we *trim* the lattice of orders as we go. Ł e runtime is then bounded in the size of the output, rather than the input. Ł e method of W ( ) had a similar feature; however, our bound is subexponential.

In mo cases, there are only polynomially many orders in $\log|\Delta|$, but to give a subexponential bound on the complexity of our algorithm when there are exponentially many, we *eliminŅe* small branches of orders as we go; these branches corre ŕ ond to small prime power fańors ℓ of the index $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$; by "eliminating them," we mean computing the endomorphism locally at ℓ using the method of E and L ( ). Formally, we proceed as follows.

Notation. Let $b_x(f(x))$ denote any funńion satisfying $f(x) < b_x(f(x)) < f(x)^{1+o(1)}$ that can be evaluated in essentially linear time in $f(x)$.

Algorithm VI.1.5.

I : *A simple ordinary abelian variŉy $\mathscr{A}$ over a Ŕnite Ŕeld $\mathbb{F}_q$.*

O : *An order śomorphic to its endomorphśm ring.*

. *Compute ū e FrobeniŬ polynomial $\chi_\pi(x)$, and fańor $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ ń $\prod \ell^{v_\ell}$.*

. *Sŉ $S \leftarrow \varnothing$ and $r \leftarrow 2$.*

. *For aŝ primes ℓ wiū $\ell^{2gv_\ell} < b_r\left(\exp\sqrt{\log(r)}\right)$:*

. *If $\ell \notin S$, compute $\mathrm{End}(\mathscr{A})_\ell$ and add ℓ to S.*

. *For aŝ orders $\mathcal{O}$ wiū $\forall \ell \in S, \mathcal{O}_\ell = \mathrm{End}(\mathscr{A})_\ell$ and $|\mathrm{disc}(\mathcal{O})| < r$:*

. *Te whŉher $\mathrm{End}(\mathscr{A}) = \mathcal{O}$; if yes, ū en rŉurn $\mathcal{O}$.*

. *Sŉ $r \leftarrow r^{1+1/b_q(\log q)}$ and go back to Step .*

Step applies the method of Eisenträger and Lauter locally at ℓ; its complexity is therefore $\ell^{2gv_\ell+o(1)}$, omitting polynomial fańors in $\log(q)$. Ł e inequality of Step thus ensures that no more than $L^{o(1)}(r)$ operations are ŕ ent there.

Ł e co of generating a certiŏcate for $\mathcal{O}$ is bounded by $L(\mathrm{disc}(\mathcal{O}))^{1/4\gamma+o(1)}$ when the veriŏcation time is bounded by $L(\mathrm{disc}(\mathcal{O}))^{3g\gamma+o(1)}$; to balance these, Step uses $\gamma = 1/\sqrt{12g}$ which gives it a complexity bound of $L(\mathrm{disc}(\mathcal{O}))^{\sqrt{3g}/2+o(1)}$. Step ensures that:

- only orders that match the local information obtained in Step are te ed;
- te ing them all uses at mo $L^{O(1)}(r)$ computing time.

Step increments r little by little so that, on the one hand, it never goes much beyond the discriminant of End($\mathscr{A}$), and, on the other hand, it takes only $O(g \log q)^2$ iterations for r to reach $|\operatorname{disc}(\mathbb{Z}[\pi,\overline{\pi}])| = O(q^{g^2+o(1)})$ and thus for our algorithm to have considered all orders.

To bound the number of orders to be te ed in Step , assume that there are at mo $n^{1+o(1)}$ orders contained in $\mathscr{O}$ with index n; this is a classical fań for $g = 1$ (since orders are identiŏed by their index in $\mathscr{O}_K$) and it has been proven by N ( ) for $g = 2$. We thus ŏnd that for $r = n^2$ the number of orders satisfying the condition of Step is bounded, up to exponent $1 + o(1)$, by the number of divisors of

$$\left[\mathscr{O}_K : \mathbb{Z}[\pi,\overline{\pi}]\right] \Big/ \prod_{\ell^{g v_\ell} < \exp\sqrt{\log r}} \ell^{v_\ell}$$

that are less than n, where the denominator removes prime powers from S; a crude calculation shows that this number is bounded polynomially in $\log(q)$.

Ignoring the co of fańoring the discriminant Δ, and omitting polynomial fańors in $\log(q)$, we obtain an overall complexity of

$$L\left(\operatorname{disc}(\operatorname{End}\mathscr{A})\right)^{\sqrt{3g}/2+o(1)}.$$

VI.2 Finding Principal Ideals

To te whether some prescribed order $\mathscr{O}$ lies below the endomorphism ring of a simple ordinary abelian variety $\mathscr{A}$, we ŏr compute principal ideals $\mathfrak{a}$ that discriminate the ruńure of Pic($\mathscr{O}$) from that of other orders containing $\mathbb{Z}[\pi,\overline{\pi}]$. Ŀ en, we evaluate the corre ŕ onding isogenies; for this reason, we compute the fańorization $\mathfrak{a} = \prod \mathfrak{p}^{z_\mathfrak{p}}$ and then evaluate $\varphi_\mathfrak{a}$ as the composition of z times the isogeny φ , for all $\mathfrak{p}$.

We therefore consider smooth ideals with small exponents, which we call *short ideals.*

G M

Let $\mathfrak{B}$ be a generating set of ideals for the Picard group of an order $\mathscr{O}$ in a number ŏeld K; for in ance, under the generalized Riemann hypothesis, we can take for $\mathfrak{B}$ the set of prime ideals of norm less than $12\log^2|\operatorname{disc}\mathscr{O}|$. By *computing relŅions* of $\mathfrak{B}$, we mean ŏnding produńs of ideals of $\mathfrak{B}$ that are principal.

For convenience of the exposition and of the implementation, let $\mathfrak{B}$ ańually generate the Picard group of the minimal order $\mathfrak{m}$; this way, the set $\{\mathfrak{b}\mathscr{O} : \mathfrak{b} \in \mathfrak{B}\}$ generates the Picard group of any order $\mathcal{O}$ containing $\mathfrak{m}$, and its relations are vectors under the product map

$$\sigma : \begin{cases} \mathbb{Z}^{\mathfrak{B}} & \longrightarrow & \mathfrak{I}(\mathfrak{m}) \\ x & \longmapsto & \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{x_{\mathfrak{p}}} \end{cases} .$$

If we let $\sigma_{\mathcal{O}}(x)$ denote the ideal class of $\mathrm{Pic}(\mathcal{O})$ containing the ideal $\sigma(x)\mathcal{O}$, then the set of relation vectors $x \in \mathbb{Z}^{\mathfrak{B}}$ for $\mathcal{O}$ is exactly the lattice $\Lambda_{\mathcal{O}} = \ker(\sigma_{\mathcal{O}})$. Note that since $\mathfrak{B}$ generates the Picard group, the map $\sigma_{\mathcal{O}}$ is surjective and we have

$$\mathrm{Pic}\,\mathcal{O} \simeq \mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}}$$

which means that computing relations is essentially equivalent to computing the group structure of $\mathrm{Pic}(\mathcal{O})$. The principal ideals of $\mathcal{O}$ we search for will be obtained in the form $\sigma_{\mathcal{O}}(z)$, where $z \in \Lambda_{\mathcal{O}}$ is a relation vector to be found.

To find kernel vectors of $\sigma_{\mathcal{O}}$, we first need to identify a finite subset of $\mathbb{Z}^{\mathfrak{B}}$ which is big enough to contain a generating set for $\Lambda_{\mathcal{O}}$. Let n denote the class number of $\mathcal{O}$; since $\mathrm{Pic}(\mathcal{O})$ is generated by $\mathfrak{B}$ and its elements have order n at most, the box $\{0, \dots, n-1\}^{\mathfrak{B}}$ maps surjectively onto the Picard group via $\sigma_{\mathcal{O}}$. As a consequence, there exists a generating set for $\Lambda_{\mathcal{O}}$ contained in the box $\mathrm{B} = \{0, \dots, n\}^{\mathfrak{B}}$. We spare the proof to the reader, since a much better bound will be derived (and proved) shortly.

Note that the class number n satisfies $n = |\operatorname{disc}\mathcal{O}|^{1/2+o(1)}$; however, analytic methods can be used to derive effective, tighter bounds on n.

To find relations of the group $\mathrm{G} = \mathrm{Pic}(\mathcal{O})$ on B, one can use the baby-step giant-step method. It consists in splitting the basis $\mathfrak{B}$ into a disjoint union $\mathfrak{B}_0 \sqcup \mathfrak{B}_1$ of two sets of approximately equal size, so that this splitting carries over to box B and decomposes it as a direct product $\mathrm{B}_0 \times \mathrm{B}_1$, where B_i is the set of vectors of B with support in $\mathfrak{B}_i$.

Algorithm VI.2.1.

Input : *A box* B *where to look for relations under* $\sigma_{\mathcal{O}} : \mathrm{B} \to \mathrm{G}$.

Output : *A relation, that is, a vector of* $\ker(\sigma_{\mathcal{O}})$.

. *Split* B *into the direct product* $\mathrm{B}_0 \times \mathrm{B}_1$.

. *For vectors* $x \in \mathrm{B}_0$: *store* x *in a table indexed by* $\sigma_{\mathcal{O}}(x)$.

. *For vectors* $y \in \mathrm{B}_1$:

. *If* $(\sigma_{\mathcal{O}}(y))^{-1} = \sigma_{\mathcal{O}} x$, *return the relation* $x + y$.

The table constructed in Step is typically implemented as a hash table, so that the cost of the lookup in Step is negligible. A Gray code can be used to enumerate elements of B_0 and B_1 so that each evaluation of $\sigma_{\mathcal{O}}$ just requires $\mathrm{O}(1)$ operations. This algorithm then requires an expected $\mathrm{O}(\sqrt{n})$ number of group operations and storage space.

Note that a faster efficient generic method for finding relations in arbitrary finite groups will be presented in the next chapter; it can be used in Picard groups in particular. For the moment, let us discuss a simple application of such generic algorithms to the computation of endomorphism rings.

R E R

Let us briefly present an alternative to our approach to computing the endomorphism ring $\operatorname{End}(\mathscr{A})$ of a simple ordinary abelian variety $\mathscr{A}$ defined over a finite field: we first gave a method for computing $\operatorname{End}(\mathscr{A})$ *from below* by finding principal ideals of candidate orders and testing them in the isogeny graph; then we gave a method which works *from above* by attempting to prove that $\mathcal{O} = \operatorname{End}(\mathscr{A})$ for orders $\mathcal{O}$ of increasing discriminant.

A more direct way of computing $\operatorname{End}(\mathscr{A})$ *from above* is simply to *reverse* our first method which proceeds *from below*: rather that finding relations of orders and evaluating them in the isogeny graph, we can find relations in the isogeny graph and evaluate them in Picard groups. This gives the method below.

Algorithm VI.2.2.

I : *A simple ordinary abelian variety $\mathscr{A}$ over a finite field $\mathbb{F}_q$.*

O : *An order isomorphic to its endomorphism ring.*

. *Compute the Frobenius polynomial $\chi_\pi(x)$ of $\mathscr{A}$.*

. *Factor the discriminant Δ and construct the order $\mathcal{O}' = \mathcal{O}_K$.*

. *For orders $\mathcal{O}$ directly below $\mathcal{O}'$:*

. *If $\operatorname{End}(\mathscr{A}) \subset \mathcal{O}$ then $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step .*

. *Return $\mathcal{O}'$.*

To test whether $\operatorname{End}(\mathscr{A})$ lies below some order $\mathcal{O}$, we find isogeny chains from $\mathscr{A}$ to itself: in the baby-step giant-step algorithm above, it suffices to replace $\sigma_{\mathcal{O}}$ by the map

$$x \in \mathbb{N}^{\mathfrak{B}} \longmapsto \underbrace{\varphi_{1} \circ \cdots \circ \varphi_{1}}_{x_{\mathfrak{p}_1}\ \text{times}} \circ \underbrace{\varphi_{2} \circ \cdots \circ \varphi_{2}}_{x_{\mathfrak{p}_2}\ \text{times}} \circ \cdots (\mathscr{A})$$

(better yet, use the Pollard approach of the next chapter); once a principal ideal of the isogeny graph is found, it suffices to check whether it is principal in the order $\mathcal{O}$ as well.

This approach has the advantage that, quite often, only one relation of the isogeny graph suffices to rule out all orders but one, so the endomorphism ring is computed in just one shot.

As before, this is a probabilistic process: the ideal we find in $\operatorname{End}(\mathscr{A})$ might actually also be principal in some strictly smaller order; in order to increase the probability of success, we can use several relations, but to unconditionally prove the output (henceforth transforming our method into an algorithm of Las-Vegas type), we have to rely on certificates.

S A

S ( ) ŏr gave an algorithm for ŏnding relations of $\Lambda_{\mathcal{O}}$ when $\mathcal{O}$ is an imaginary quadratic orders; building upon it, H and M C ( ) proved that the full Picard group ruńure, that is, a generating set for $\Lambda_{\mathcal{O}}$, can be determined in proven subexponential time under the generalized Riemann hypothesis. Ł is was later extended by B ( ) to arbitrary number ŏelds, under additional heuri ic assumptions.

All ŏnd relations using a classical smoothness-based technique which exploits the integer-like ruńure of ideals in number ŏelds.

Algorithm vi.2.3.

I : *A box* B *where to look for relŅions under* $\sigma_{\mathcal{O}} : \mathrm{B} \to \mathrm{Pic}(\mathcal{O})$.

O : *A relŅion, ū Ņ ś, a veňor of* $\ker(\sigma_{\mathcal{O}})$.

. *Take a random element* $x \in \mathrm{B}$ *and compute* $\mathfrak{a} = \sigma_{\mathcal{O}}(x)$.

. *Reduce* $\mathfrak{a}$ *to an equivalent but smaŝer ideal* $\mathfrak{b}$.

. *If possible, Ŕnd a preimage* $y \in \sigma_{\mathcal{O}}^{-1}(\mathfrak{b})$ *and r'nurn* $x - y$.

. *R'nurn to Step* .

To ŏnd preimages easily, S ( ) takes as basis $\mathfrak{B}$ the set of prime ideals of norm less than some bound, so that the exi ence of a preimage in B can be asserted by a smoothness te on the norm of the ideal, and the fańorization of that norm yields the preimage. Several ingredients are needed to bound its complexity, the mo important one being that a random integer in $\{1, \dots, n\}$ has a probability $\mathrm{L}(n)^{-1/2c+o(1)}$ of being $\mathrm{L}(n)^{c}$-smooth, for any con ant $c > 0$; in the case that $\mathcal{O}$ is an imaginary quadratic orders, S ( ) proved that norms of reduced ideals are di ributed as random integers; in fań, this behavior is observed, although not proven, for orders of general number ŏelds as well.

Ł e next chapter will present all these arguments rigorously.

S B

Since our relations (and the ideals derived from them) are expeńed to discriminate the endomorphism ring from other orders of the lattice, we mu ensure that when we generate a relation in $\Lambda_{\mathcal{O}}$ for some order $\mathcal{O}$, it does not belong to $\Lambda_{\mathcal{O}'}$ for some other order $\mathcal{O}'$. Of course, we have seen that $\mathcal{O} \subset \mathcal{O}'$ implies that $\Lambda_{\mathcal{O}} \subset \Lambda_{\mathcal{O}'}$, and our lattice-ascending algorithm ańually takes advantage of that, so we should rather require the above for orders $\mathcal{O}'$ not above $\mathcal{O}$, that is, $\mathcal{O} \not\subset \mathcal{O}'$.

Note that there exi orders $\mathcal{O} \neq \mathcal{O}'$ with $\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}'}$, but not too many: for $g = 1$, there are ju three such cases, and we can easily fall back on a ŕ eciŏc method to deal with them. Rigorous details will be given in the next chapter.

In general, to ensure that the relations z we generate belong to $\Lambda_{\mathcal{O}}$ but not another $\Lambda_{\mathcal{O}'}$, we require that they are *random relNions* in the sense that, for any order $\mathcal{O}'$ above $\mathcal{O}$, we have

$$\operatorname{Prob}\left[z \in \Lambda_{\mathcal{O}'} | z \in \Lambda_{\mathcal{O}}\right] = \frac{\#\operatorname{Pic}\mathcal{O}'}{\#\operatorname{Pic}\mathcal{O}} + o(1);$$

in other words, the relation is quasi-uniformly di ributed in the quotient $\Lambda_{\mathcal{O}'}/\Lambda_{\mathcal{O}}$.

To obtain random relations of $\mathcal{O}$, H and M C ( ) used veńors z with coordinates up to n^4, where n is the class number. In the Picard group, a double-and-add method can be used to compute each term $\mathfrak{p}^{z_\mathfrak{p}}$ in time linear in $\log(n)$, so that $\sigma_{\mathcal{O}}$ can be evaluated in subexponential time.

However, for the purpose of checking whether the ideal $\sigma(x-y)$ is principal in the isogeny graph, the associated isogeny needs to be evaluated. For this, there is no double-and-add technique, and the isogeny φ has to be evaluated z times, which makes the bound n^4 on the coordinates quite painful. Note that since y is the exponent veńor in the fańorization of the norm of a reduced ideal, it is at mo linear in $\log n$, so what is really needed here to keep the isogeny-computing co low is ju to ŏnd a smaller box B for which the quasi-uniform di ribution of classes ill holds.

A conjeńural small box was ŏr used by B. and S ( ); later, C , J , and S ( ) noted that a result of J , M , and V ( ) enables to prove, under the generalized Riemann hypothesis, that such a box indeed yields random relations. We conclude with an explicit version of the general algorithm.

Algorithm VI.2.4.

I : *An order $\mathcal{O}$ of dścriminant* D.

O : *A random relNion $z \in \Lambda_{\mathcal{O}}$.*

. *Form ūe s'n $\mathfrak{B}$ of primes $\mathfrak{p}$ of $\mathcal{O}$ wiū norm less ūan* $\mathrm{N} = \mathrm{L}(\mathrm{D})^{\gamma}$.

. *Draw uniformly N random a veňor $x \in \mathbb{Z}^{\mathfrak{B}}$ wiū coordinNes* $|x\ | < b_{\mathrm{D}}(\log^{4+\varepsilon}|\mathrm{D}|)$ *if* $\mathrm{N}(\mathfrak{p}) < b_{\mathrm{D}}(\log^{2+\varepsilon}|\mathrm{D}|)$, *else* $x\ = 0$.

. *Compute a reduced ideal $\mathfrak{a}$ in ūe clńs $\sigma_{\mathcal{O}}(x)$.*

. *If $\mathfrak{a}$ faňors over $\mathfrak{B}$ ń $\prod \mathfrak{p}^{y_\mathfrak{p}}$ ūen r'nurn ūe veňor $x - y$.*

. *Oūerwśe, go back to Step .*

Here, ε ands for any ŏxed positive real number. Step may use the LLL algorithm as we mentioned earlier; for any "good" reduńion method, the probability that Step is successful is $\mathrm{L}(\mathrm{D})^{-1/4\gamma+o(1)}$; the overall complexity is then $\mathrm{L}(\mathrm{D})^{1/4\gamma+o(1)}$ to generate a relation of length $\mathrm{L}(\mathrm{D})^{\gamma}$; the longer the relation, the co lier the evaluation of the associated isogeny.

vi.3 Computing the Action of Ideals

We now consider e eńive means of te ing whether an ideal $\mathfrak{a}$ ańs trivially on the isogeny graph of an abelian variety $\mathscr{A}$. Here, we focus on the case of elliptic curves, but certain bricks will be reused in the la chapter for abelian varieties of dimension two.

M EŽ

Once a principal ideal $\mathfrak{a}$ of $\mathcal{O}$ in the form $\prod_{\mathfrak{B}} \mathfrak{p}^{z_\mathfrak{p}}$ is found, we wish to determine whether the associated isogeny ańs trivially on $\mathscr{A}$; in fań, this does not require explicitly evaluating the isogeny φ , but only determining whether it maps $\mathscr{A}$ on $\mathscr{A}$.

Elliptic curves isogenous to a given one with a prescribed way can be li ed e ciently via modular polynomials; this uses j-invariants to identify isomorphism classes of curves, and modular polynomials $\Phi_m(X,Y)$ which we now recall.

Proposition vi.3.1. *For any* $m \in \mathbb{N}$, *ūere exśts some polynomial* $\Phi_m(X,Y) \in \mathbb{Q}[X,Y]$ *of degree* $m+1$ *such ū N, over Ŕelds of charańerśtic coprime to* m, *ūe j-inl·ariants of eŝiptic curves m-śogenoŬ to a prescribed* j_0 *are exańly ūe roots of* $\Phi_m(X,j_0)$.

C ( ) proved the bit-size of Φ_m to be $O(m^{3+o(1)})$. It can be computed in quasi-linear time by the floating-point method of E ( ), or by the alternative method of B , L , and S ( ) based on the Chinese remainder theorem, which o ers additional advantages such as reduced memory requirements.

To te whether φ ańs trivially on $\mathscr{A}$, we can evaluate $\Phi_{N( )}(X,Y)$ at $(j(\mathscr{A}),j(\mathscr{A}))$. If the result is non-zero, then φ cannot send $\mathscr{A}$ to $\mathscr{A}$; if the result is zero, then there exi s one isogeny of degree $N(\mathfrak{a})$ from $\mathscr{A}$ to $\mathscr{A}$, but it need not be φ in general.

For prańical purposes, rather than seeing φ as an isogeny of degree $N(\mathfrak{a})$, we see it as a chain formed of z isogenies of norm $N(\mathfrak{p})$ for each $\mathfrak{p} \in \mathfrak{B}$. Consequently, it su ces to compute the modular polynomials $\Phi_{N( )}$ and to combine them as isogeny eps. We now detail this procedure, in a manner which also addresses the issue of the previous paragraph.

C

When we evaluate $\Phi_{N( )}(X,Y)$ at $X = j(\mathscr{A})$, the roots in Y are the j-invariants of the codomain of degree-$N(\mathfrak{p})$ isogenies with domain $\mathscr{A}$. Among these roots lies φ $(\mathscr{A})$ but we have no information as to which it is.

To address this, we can explore *aŝ* isogenies of degree $N(\mathfrak{p})$. When $\mathfrak{a}$ has many fańors, this can be co ly as we might have to consider several roots of $\Phi_{N( )}$ at each ep of the isogeny chain, therefore eventually exploring an exponential number of varieties in $\log N(\mathfrak{a})$.

Endomorphism rings of elliptic curves are imaginary quadratic orders, and there are therefore at mo two ideals of a given prime norm: $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. In the isogeny chain

$$\mathscr{A}_0 \xrightarrow{\varphi_{\mathfrak{p}}} \mathscr{A}_1 \xrightarrow{\varphi_{\mathfrak{p}}} \cdots \xrightarrow{\varphi_{\mathfrak{p}}} \mathscr{A}_{z_{\mathfrak{p}}}$$

corre ŕ onding to the fańor $\mathfrak{p}^{z_{\mathfrak{p}}}$ of $\mathfrak{a}$, the conjugate prime $\overline{\mathfrak{p}}$ ańs on $\mathscr{A}_i$ as the dual isogeny of φ : $\mathscr{A}_{i-1} \to \mathscr{A}_i$. Ł us, for $i > 0$, we can determine which of the two roots of $\Phi_{N(\ )}(j(\mathscr{A}_i), Y)$ is *not going backward* in the chain, and the two roots need to be considered only for $i = 0$.

Ł is helps when $\mathfrak{a}$ does not have many prime fańors but has one with high exponent: rather than ju te ing if $\prod_{\mathfrak{B}} \mathfrak{p}^{z_{\mathfrak{p}}}$ is principal, we count how many produńs $\prod_{\mathfrak{B}} \widehat{\mathfrak{p}}^{z_{\mathfrak{p}}}$ are, where $\widehat{\mathfrak{p}} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$; this is equivalent to counting the number of endomorphisms of $\mathscr{A}$ that are chains consi ing in z non-backwards isogenies of degree $N(\mathfrak{p})$, for each $\mathfrak{p}$.

When there are ju two ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ of norm $N(\mathfrak{p})$, this gives:

Definition VI.3.2. *L'n* $\prod_{\mathfrak{B}} \mathfrak{p}^{z_{\mathfrak{p}}}$ *be ū e fańoriz*Ņ*ion of an ideal* $\mathfrak{a} \in \mathbb{Z}[\pi, \overline{\pi}]$.

Its cardinality in $\mathcal{O}$ *ś ū e number of veňors* $(\widehat{\mathfrak{p}}) \in \prod_{\ \in \mathfrak{B}} \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ *for which* $\prod_{\mathfrak{B}} \widehat{\mathfrak{p}}^{z_{\mathfrak{p}}}$ *ś trivial.*

Its cardinality in the isogeny graph *of* $\mathscr{A}$ *ś ū e number of chains formed by z śogenies of norm* $N(\mathfrak{p})$*, for each* $\mathfrak{p} \in \mathfrak{B}$*, which map* $\mathscr{A}$ *onto itself.*

Ł ese two quantities are the same for $\mathcal{O} = \mathrm{End}(\mathscr{A})$, and, for elliptic curves, we evaluate the latter via using the method below arting from the j-invariant $j_0 = j(\mathscr{A})$.

Algorithm VI.3.3.

I : *A j-inŀariant* j_0 *and an ideal* $\prod_{\mathfrak{B}} \mathfrak{p}^{z_{\mathfrak{p}}}$.

O : *Ń e cardinality of ū ś ideal in ū e śogeny graph of* j_0.

. *L'n* J' *be ū e lśt* (j_0).

. *For each* $\mathfrak{p} \in \mathfrak{B}$:

. *S'n* $J \leftarrow J'$ *and l'n* J' *be an empty lśt.*

. *For each j in* J:

. *L'n* $\{j_+, j_-\}$ *be ū e roots of* $\Phi_{N(\ )}(X, j)$*, and s'n* $j'_+ \leftarrow j$ *and* $j'_- \leftarrow j$.

. *Repe*Ņ *z* -1 *times:*

. *S'n* $(j'_+, j_+) \leftarrow (j_+,$ *ū e root of* $\Phi_{N(\ )}(X, j_+)$ *di erent Řom* $j'_+)$.

. *S'n* $(j'_-, j_-) \leftarrow (j_-,$ *ū e root of* $\Phi_{N(\ )}(X, j_-)$ *di erent Řom* $j'_-)$.

. *Append* j_+ *and* j_- *to* J'.

. *R'nurn ū e multiplicity of* j_0 *in* J'.

Since we compute two branches for each prime fańor of $\mathfrak{a}$, the overhead this *cardinality* algorithm adds on the *principal* approach is 2^w where w is the number of prime fańors. When w is small, this is greatly compensated by the ŕ eed of using modular polynomials.

C M A

We briefly review results on evaluating the explicit isogeny φ associated to an ideal $\mathfrak{p}$.

Recall Proposition . . which states that invertible prime ideals $\mathfrak{p}$ of $\mathcal{O}$ written as $\ell\mathcal{O} + u(\pi)\mathcal{O}$ act on the kernel of the associated isogeny φ with characteristic polynomial u. Therefore, to tell the isogeny φ apart from other isogenies of degree $\mathrm{N}(\mathfrak{p})$, one need just compute the action of the Frobenius endomorphism on its kernel.

To evaluate isogenies from their kernels, we use the formulas of V ( ) for elliptic curves, and their generalization to abelian varieties by L and R ( ) together with the improvements of C and R ( ). These methods take as input a subgroup $\mathscr{H}$ of an abelian variety $\mathscr{A}$ and output the isogeny $\mathscr{A} \to \mathscr{A}/\mathscr{H}$. Since they work with principally polarized abelian varieties, they additionally require that $\mathscr{H}$ be a maximal isotropic subgroup with respect to the Weil pairing, and that it be isomorphic to $(\mathbb{Z}/\ell)^g$.

We thus seek ideals $\mathfrak{a} = \prod \mathfrak{q}^{z_\mathfrak{q}}$ where the kernel of each φ is maximal isotropic and of type $(\mathbb{Z}/\ell)^g$; to this extent, in dimension $g > 1$, we restrict to ideals $\mathfrak{a}$ arising via the reflex type norm, on which the last chapter will say more. When we have a prime decomposition $\mathfrak{q} = \prod \mathfrak{p}$ for a specific term $\mathfrak{q}$, the Frobenius endomorphism must act on $\ker(\varphi)$ with characteristic polynomial $\prod u(x)$ where the $u(x)$ are such that $\mathfrak{p} = \mathrm{N}(\mathfrak{p})\mathcal{O} + u(\pi)\mathcal{O}$.

Finally, we observe that, if $\mathscr{A}$ is an ordinary abelian variety of dimension g defined over a finite field, all points of rational subgroups of type $(\mathbb{Z}/\ell)^g$ are defined over an extension of degree at most $\ell^g - 1$.

The characteristic polynomial of the action, on such a subgroup $\mathscr{H}$, of the Frobenius endomorphism divides $\chi_\pi(x) \bmod \ell$, and the multiplicative order n of x modulo this factor is precisely the extension degree over which all points of $\mathscr{H}$ are defined. Therefore, to evaluate the degree of an extension over which all points of rational subgroups of type $(\mathbb{Z}/\ell)^g$ are defined, it suffices to compute the least common multiple of the multiplicative order of x modulo the degree-g factors of $\chi_\pi(x) \bmod \ell$.

D M

Let $\mathfrak{q}$ be an ideal such that $\ker(\varphi)$ is a maximal isotropic subgroup of order ℓ^g in $\mathscr{A}$. In order to compute this isogeny, we combine several classical tools into the algorithm below. It requires a basis for the ℓ-torsion of $\mathscr{A}$ defined over a certain extension, which we will soon explain how to compute; the kernel is then identified by the polynomial $u = \prod u$ with u defined as above, and we use the explicit isogeny algorithm to compute φ from it. We make this algorithm output the isogenous curve $\varphi(\mathscr{A})$, so it can readily be plugged in to our endomorphism ring computing method.

Algorithm VI.3.4.

Input : *An abelian variety $\mathscr{A}/\mathbb{F}_q$ with Frobenius polynomial χ_π and a suitable ideal $\mathfrak{q}$ of norm ℓ^g.*

Output : *The isogenous variety $\varphi(\mathscr{A})$.*

. *Find a basis (P_i) of the $\mathscr{A}[\ell]$ over the extension of degree $\ell^g - 1$ of $\mathbb{F}_q$.*
. *Write the matrix M of the Frobenius endomorphism on the basis (P_i).*
. *Enumerate those subspaces of dimension g stable under $M \in \mathrm{Mat}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.*
. *Determine which corresponds to $\mathfrak{q}$ using the Frobenius action.*
. *Compute the isogeny of which this eigenspace is the kernel.*

For a maximal isotropic subgroup of $\mathscr{A}$ of order ℓ^g defined over the extension of degree $\ell^g - 1$ of the base field, the method of L and R ( ) requires $\ell^{3g+o(1)}$ operations as g is fixed and ℓ goes to infinity.

Step decomposes $\pi(P_i)$ as $\sum_{j\in\{1,\dots,2g\}} M_{ij}P_j$ for which a baby-step giant-step approach uses $O(\ell^g)$ operations over the extension field. Step is classical and takes quasi-linear time in $g^\omega \log(\ell)$ where $\omega < 2.376$ is the best known exponent for matrix multiplication.

Finally, Step uses Theorem of C ( ), where the extension is chosen so as to contain all points of rational subgroups of type $(\mathbb{Z}/\ell)^g$. The simple algorithm we give below actually computes all such points, from which a basis can easily be extracted; it works by selecting random ℓ^∞-torsion points and lifting them along each others. Here, we let $k(P)$ denote the valuation at a fixed prime ℓ of the order of a point P.

Algorithm VI.3.5.

Input : *An abelian variety $\mathscr{A}/\mathbb{F}_q$ with Frobenius polynomial χ_π and a prime ℓ.*

Output : *The ℓ-torsion subgroup of $\mathscr{A}$ over $\mathbb{F}_{q^{\ell^g-1}}$.*

. *Write $\#\mathscr{A}(\mathbb{F}_{q^{\ell^g-1}})$ as $m\ell^k$ where $\ell \nmid m$.*
. *Create an empty associative array B.*
. *While B has fewer than ℓ^{2g} keys:*
.   *Let $P = mO$ where O is a random point of $\mathscr{A}(\mathbb{F}_{q^{\ell^g-1}})$.*
.   *For j from $k(P)-1$ down to 1, if ℓ^jP is a key of B:*
.   *If $j > k(B[\ell^jP])$ then go to Step .*
.   *Set $P \leftarrow P - \ell^{k(B[\ell^jP])-j-1}B[\ell^jP]$.*
.   *If $P = 0$ then go back to Step .*
.   *For all keys Q of B and $x \in \{1,\dots,\ell\}$, set $B[\ell^{k(xP+Q)-1}(xP+Q)] \leftarrow xP+Q$.*
. *Return the keys of B.*

Random points of $\mathscr{A}$ can be drawn efficiently when $\mathscr{A}$ is given as the Jacobian variety of a curve in Weierstrass form. Using the last two algorithms, we compute, in Mumford coordinates, the kernel of the isogeny that we wish to evaluate; we then convert it to theta representation where the algorithm of C and R ( ) is applied, and ŏnally use the method of M ( ) to convert the codomain variety back as the Jacobian of a curve in Weier rass form, so that the whole process can be iterated.

Since the cardinality of $\mathscr{A}(\mathbb{F}_{q^{\ell^g-1}})$ is $q^{g\ell^g+o(1)}$ multiplying random points of it by m uses $\mathrm{O}(g\ell^g \log q)$ operations in $\mathscr{A}(\mathbb{F}_{q^{\ell^g-1}})$. Similarly, all orders are bounded by $k = \mathrm{O}(g\ell^g \log q)$. Finally, the probability of going back to Step is $\mathrm{O}(1/\ell)$ as proven by C ( ).

Using fa ŏeld arithmetic, and representing points of $\mathscr{A}$ in Mumford coordinates, operations in $\mathscr{A}(\mathbb{F}_{q^{\ell^g-1}})$ have a bit complexity of $(\ell^g \log q)^{1+o(1)}$; if an e cient data ruńure such as a red-black tree is used to ore the keys of B, we have:

Proposition vi.3.6. *L'n* $\mathscr{A}/\mathbb{F}_q$ *be an abelian vari'ny of known FrobeniŬ polynomial, and* $\mathfrak{q}$ *a suiŪble ideal of* $\mathbb{Z}[\pi,\overline{\pi}]$. *Algoriūm . . r'nurns ūe abelian vari'ny* $\varphi_{\mathrm{End}(\mathscr{A})}(\mathscr{A})$ *in time bounded by* $(\ell^g \log q)^{2+o(1)}$, *ń g ś Ŕxed and* ℓ *goes to inŔnity.*

Note that, in Algorithm . . , rather than oring the whole ℓ-torsion subgroup in an associative array, a pairing could be used to tran ŕ ort discrete logarithm problems to a ŏnite ŏeld where they can be more e ciently solved. Ł is technique gives a valuable ŕ eedup for large values of ℓ, although the overall complexity remains polynomial in ℓ due to the extension ŏeld arithmetic.

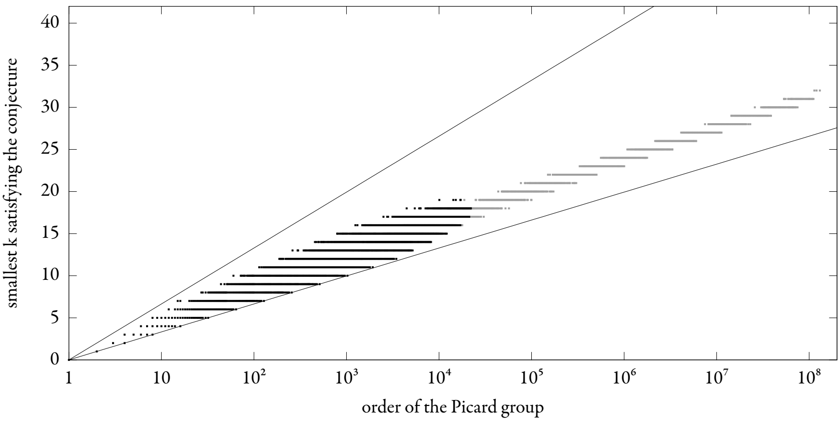
vi.4 Prańical Computations

We now present the algorithms used and results obtained by prańical runs on elliptic curves. Applying the same techniques to general abelian varieties will be the topic of the la chapter. Timings reported here were measured on a single core of a recent desktop computer, such as an AMD Opteron clocked at 2 GHz.

B C

Let $\mathscr{E}$ be an ordinary elliptic curve deŏned over a ŏnite ŏeld $\mathbb{F}_q$. Ł e ŏr ep of our algorithm is to compute the charańeri ic polynomial χ_π of the Frobenius endomorphism of $\mathscr{E}$. It is equivalent to counting the number of points of $\mathscr{E}$ which is of the form $\chi_\pi(1) = p+1-t$ for a certain integer $t \in \{-2\sqrt{q},\dots,2\sqrt{q}\}$. Over a base ŏeld of cryptographic size, say, with q a prime of 256 bits, this takes under ten seconds on ju one core of a andard desktop computer using the Schoof–Elkies–Atkin algorithm. Note that further developments by S ( ) now make this possible for primes p over 5000 decimal digits.

Next, we need to ŏnd principal ideals of orders $\mathscr{O}$, and art by deciding which prime fańors we want them to have. For maximal orders $\mathscr{O}$ of imaginary quadratic ŏelds, B



F . Dots plot the minimal k such that every class of $\operatorname{Pic}(\mathcal{O})$ contains the product of a subset of S_k. Gray dots cover all imaginary quadratic orders $\mathcal{O}$ of discriminant at least -10^8, and black dots are for 10^4 random $\mathcal{O}$ drawn according to a logarithmic distribution. The lines represent $k = d\log_2(\#\operatorname{Pic}\mathcal{O})$ for $d = 1, 2$.

( ) proved under the generalized Riemann hypothesis that the primes up to $6\log^2|\Delta|$ generate the Picard group, where Δ is the discriminant of $\mathcal{O}$. Heuristically, we find that much less are necessary, which lead to the following conjecture.

Conjecture VI.4.1. *For any $d > 1$, if $\mathcal{O}$ is an imaginary quadratic order of sufficiently large discriminant, then any class of* $\operatorname{Pic}(\mathcal{O})$ *contains the product of a subset of* S_k*, where* S_k *contains the first $k = d\log_2(\#\operatorname{Pic}\mathcal{O})$ non-principal prime ideals.*

This is is actually stronger than asking for S_k to generate the Picard group: it requires that S_k generates it *with bounded exponents* in $\{0, 1\}$. However, it is a natural conjecture to make since it asserts that the set S_k behaves as a random subset of $\operatorname{Pic}(\mathcal{O})$ would in the sense of Proposition . of I and N ( ). Our empirical verifications have not found a single order for which the conjecture does not hold with $d = 2$; for values of d closer to 1, we found this to be true for many orders above a certain lower bound, as can be seen on Figure .

The above is mostly useful when generating relations using generic methods: it states that only slightly more primes than a cardinality argument would require actually suffice. This yields short associated isogenies (which are a must in dimension two).

However, as we strive to balance the cost of finding a principal ideal in $\mathcal{O}$ with that of evaluating the associated isogeny, generic methods do not scale well: for discriminants of more than 128 bits, a generic method would require above 32 operations in $\mathrm{Pic}(\mathcal{O})$; from there on it is therefore advisable to switch to the subexponential method of S ( ). Note that by the conjecture we can use a box with support in S_k.

Since our principal ideals rarely have more than 10 prime factors, it is really worth using the cardinality approach: modular polynomials permit one to compute isogenous curves quickly, and they can be precomputed and reduced modulo p for all the primes ℓ we consider, whereas computing the torsion would have to be done from scratch at each step.

H C D O

So far, our endomorphism ring computing method tested whether $\mathcal{O} \subset \mathrm{End}(\mathscr{A})$ for various orders $\mathcal{O}$; since this process has a small probability of failure, we then certified the candidate order so as to unconditionally verify our result.

In B. and S ( ), we used a quite different approach which simultaneously finds $\mathcal{O}$ and verifies it. It exploits the particular structure of the lattice of orders for elliptic curves; we start by recalling this structure.

Let w denote the index of $\mathbb{Z}[\pi]$ in $\mathcal{O}_{\mathbb{Q}(\pi)}$ where π denotes the Frobenius endomorphism of an ordinary elliptic curve defined over a finite field. Orders $\mathcal{O}$ of $K = \mathbb{Q}(\pi)$ have the form $\mathbb{Z} + f\mathcal{O}_K$ where f is the integer that generates their conductor over $\mathcal{O}_K$; therefore, inclusion of orders corresponds to divisibility of conductors, so that orders containing $\mathbb{Z}[\pi]$ are in bijection with divisors f of w.

Let p^i be a prime power dividing w, and consider the problem of deciding whether p^i divides the conductor u of $\mathrm{End}(\mathscr{E})$. Here, a certificate for p^i needs only consist of one ideal $\mathfrak{a}$ which is principal in the order of conductor $w/p^{\mathrm{val}_p w - i + 1}$ but not in that of conductor p^i: if $\mathfrak{a}$ is principal in the isogeny graph of $\mathscr{E}$, then we necessarily have $p^i | u$. Indeed, in that situation, $\mathrm{End}(\mathscr{E})$ does not contain the order with conductor $w/p^{\mathrm{val}_p w - i + 1}$, which means its conductor u divides w without dividing $w/p^{\mathrm{val}_p w - i + 1}$, in other words, p^i divides u.

In number fields of degree greater than two, it does not seem to be possible to certify orders in a nice way as above, using just one ideal; that is why we needed to develop a more general method for arbitrary abelian varieties.

G E

Let $\mathscr{E}$ be the elliptic curve with Weierstrass equation

$$Y^2 = X^3 - 3X + 2728849899765998058103612158899570741955717345$$
over $\mathbb{F}_q$ with $q = 2872801286401014961877470682093858455400487431$

Ł is curve is ordinary and it has $q + 1 - t$ points, for a trace t of 1868. Ł e discriminant of π is $4q - t^2$ and its fańors as $-7w^2$ where

$$w = 2 \cdot 127 \cdot 524287 \cdot 304250263527209.$$

We ŏr compute the endomorphism locally at 2 using the method of E and L ( ), which is nearly in antaneous; it ŏnds that the order with conduńor 2 does not contain $\mathrm{End}(\mathscr{E})$.

For the prime 127, we use the local method of K ( ): since $\Phi_{127}(j(\mathscr{E}), \cdot)$ proves

S E

Let $\mathscr{E}$ be the elliptic curve with Weier rass equation

$$\begin{aligned} Y^2 = X^3 - 3X + {} & 66089717007102549448903693691\backslash \\ & 1961310755220799706808980495 28 \\ \text{over } \mathbb{F}_q \text{ with } q = {} & 1606938044258990275550812343 20\backslash \\ & 6050075546550943415909014478299 \end{aligned}$$

where the backslash symbol denotes that a number has been wrapped over to the next line. Again, the curve is ordinary and it has trace $t = 212$ (which it takes ju a few seconds to compute). Fańoring the discriminant $4q - t^2$ of $\mathbb{Z}[\pi]$, we ŏnd that

$$w = 2 \cdot 127 \cdot \underbrace{524287}_{p_1} \cdot \underbrace{719577766870732918103}_{p_2}.$$

As before, the primes 2 and 127 can be dealt with by climbing the local volcano. None of them divides the conduńor u of $\mathrm{End}(\mathscr{E})$; this only takes a few seconds.

To determine whether p_1 divides u, we use the algorithm of S ( ) with the smoothness bound 600 to ŏnd a relation with non-zero cardinality in the order of conduńor w/p_1. It takes about four minutes to ŏnd the relation

$$2^{1798} \cdot 23^3 \cdot 29^1 \cdot 37^2 \cdot 53^{29} \cdot 137^1 \cdot 149^1 \cdot 233^1 \cdot 263^2 \cdot 547^1$$

whose cardinality in the order with conduńor p_1 is zero. Computing the relevant modular polynomials via the method of B , L , and S ( ) requires under four minutes and the associated tree of isogenies is found to have cardinality zero within ju a minute; as a consequence, we deduce that p_1 is a fańor of u. Note that, here, we made use of the prime 2 although it divides the index w; this process is described in Seńion . of S ( ).

For the prime p_2, this is, as expeńed, much fa er: the relation $2^{23} \cdot 11^5 \cdot 43^1 \cdot 71^2$ is found to have positive cardinality in the order with conduńor w/p_2 but not that with conduńor p_2. It is found that p_2 does not divide u and the whole process takes ju a few seconds.

In about 5 minutes, we have thus proved that $\mathrm{End}(\mathscr{E})$ has conduńor 524287, but note that this computation was much more di cult than the previous one due to the larger size of p_2 here: it could not have been achieved with generic methods.

References

. Jacques V .
"Isogénies entre courbes elliptiques".
In: *Comptes RendŬ de l'Académie des Sciences de Parś*. A . Pages – .

. Paula C .
"On the coe cients of the transformation polynomials for the elliptic modular function". In: *Mathematical Proceedings of the Cambridge Philosophical Society* .
Pages – . DOI: `10.1017/S0305004100061697`.

. René S .
"Elliptic curves over finite fields and the computation of square roots mod *p*".
In: *Mathematics of Computation* . . Pages – .
DOI: `10.2307/2007968`.

. Martin S .
"A probabili ic factorization algorithm with quadratic forms of negative discriminant". In: *Mathematics of Computation* . . Pages – .
DOI: `10.1090/S0025-5718-1987-0878705-X`.

. Johannes B .
"A subexponential algorithm for the determination of class groups and regulators of algebraic number fields". In: *Séminaire de Théorie des Nombres, Paris*.
Edited by Catherine G . Volume . Progress in Mathematics. Birkhäuser.
Pages – .

. James L. H and Kevin S. M C .
"A rigorous subexponential algorithm for computation of class groups".
In: *Journal of the American Mathematical Society* . . Pages – .
DOI: `10.2307/1990896`.

. Eric B .
"Explicit bounds for primality te ing and related problems".
In: *Mathematics of Computation* . . Pages – .
DOI: `10.1090/S0025-5718-1990-1023756-8`.

. Jonathan P .
"Frobenius maps of abelian varieties and finding roots of unity in finite fields".
In: *Mathematics of Computation* . . Pages – .
DOI: `10.2307/2008445`.

. Jean-François M .
"Con ruction de courbes de genre 2 à partir de leurs modules".
In: *E ective methods in algebraic geometry — MEGA '* .
Edited by Teo M and Carlo T . Volume . Progress in Mathematics.
Birkhäuser. Pages – .

. Russel I and Moni N .
"E cient cryptographic schemes provably as secure as subset sum".
In: *Journal of Cryptology* . . Pages – . DOI: `10.1109/SFCS.1989.63484`.

. David R. K .
"Endomorphism rings of elliptic curves over ŏnite ŏelds".
PhD thesis. University of California at Berkeley.
URL: `http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf`.

. Jin N .
"Orders of a quartic ŏeld".
In: *Memoirs of ūe American MŅhemŅical Soci'ny* . .

. Gaetan B and Andrew V. S .
"Computing the endomorphism ring of an ordinary elliptic curve over a ŏnite ŏeld".
In: *Journal of Number Ńeory* . . Edited by Neal K and Vińor S. M .
Special Issue on Elliptic Curve Cryptography. Pages – .
DOI: `10.1016/j.jnt.2009.11.003`.

. Jean-Marc C .
"Linearizing torsion classes in the Picard group of algebraic curves over ŏnite ŏelds".
In: *Journal of Algebra* . . Pages – .
DOI: `10.1016/j.jalgebra.2008.09.032`.

. Kir en E and Kri in E. L .
"A CRT algorithm for con ruńing genus curves over ŏnite ŏelds".
In: *Ariūm'nic, Geom'nry and Coding Ńeory — AGCT '* .
Edited by François R and Serge V . Volume . Séminaires et Congrès.
Société Mathématique de France. Pages – .

. Andreas E .
"Computing modular polynomials in quasi-linear time".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: `10.1090/S0025-5718-09-02199-1`.

. David J , Stephen D. M , and Ramarathnam V .
"Expander graphs based on GRH with an application to elliptic curve cryptography".
In: *Journal of Number Ńeory* . . Pages – .
DOI: `10.1016/j.jnt.2008.11.006`.

. David L and Damien R .
Computing śogenies b'nween abelian vari'nies. arXiv.org: `1001.2016`.

. Markus W .
"Über Korre ŕ ondenzen zwischen algebraischen Funktionenkörper".
PhD thesis. Technische Universität Berlin.
URL: `http://www.math.tu-berlin.de/~wagner/Diss.pdf`.

. Reinier B , Kri in L , and Andrew V. S .
Modular polynomials via śogeny l·olcanoes.
To appear in *MŅhemŅics of CompuŪtion*. arXiv.org: `1001.0402`.

. Andrew M. C , David J , and Vladimir S .
Con ruňing eŝiptic curve śogenies in quantum subexponential time.
arXiv.org: `1012.4019`.

. Gaetan B .
Computing endomorphśm rings of eŝiptic curves under ū e GRH.
arXiv.org: `1101.4323`.

. Romain C and Damien R .
Computing (ℓ,ℓ)*-śogenies in polynomial time on Jacobians of genŬ curves.*
IACR ePrint: `2011/143`.

. Andrew V. S .
"Computing Hilbert class polynomials with the Chinese remainder theorem".
In: *MŅhemŅics of CompuŪtion* . Pages – .
DOI: `10.1090/S0025-5718-2010-02373-7`.

. Andrew V. S .
GenŬ point counting in quadrŅic ş ace and essentiaŝy quartic time. In preparation.

Ƨomplexity ƥ nalysś

Ł is chapter is devoted to a rigorous analysis of the method that we have ju presented; the main result is a proof, under the generalized Riemann hypothesis, that our algorithm indeed computes endomorphism rings of ordinary elliptic curves in subexponential time.

Mo of material used has already appeared in B. ( ) for elliptic curves; here, when this can be done, we ate our results for general varieties. Polarization issues are deferred to the next chapter, which will therefore also cover prańical computational a ŕ eńs in dimension $g > 1$.

As usual, let $\mathscr{A}$ be a simple ordinary abelian variety deŏned over a ŏnite ŏeld $\mathbb{F}_q$.

VII.1 Orders from Picard Groups

We ŏr prove that if we can identify the ruńure of the Picard group of the endomorphism ring of $\mathscr{A}$, then we can determine $\mathrm{End}(\mathscr{A})$ unambiguously.

P

Recall that the ŏr ep is to compute the charańeri ic polynomial χ_π of the Frobenius endomorphism π of $\mathscr{A}$. For this, we use the method of P ( ) and more precisely the improved algorithm of A and H ( ) which, when $\mathscr{A}$ is the Jacobian variety of a genus-g hyperelliptic curve, has a complexity of

$$(\log q)^{O(g^2 \log g)}.$$

Even if it were not for cryptographic reasons, we would avoid non-Jacobian varieties since our algorithms requires to e ciently draw points at random, which we cannot do when $\mathscr{A}$ is expressed in a more general form (such as theta con ants).

The number of points of $\mathscr{A}$ defined over the extension of degree e is then

$$\#\mathscr{A}(\mathbb{F}_{q^e}) = \mathrm{Res}_u\left(\chi_\pi(u), u^e - 1\right)$$

which means that our algorithm for computing the ℓ-torsion does not have to count the number of points over a new extension every time a new prime ℓ is considered.

To navigate the lattice of orders of the complex multiplication field $K = \mathbb{Q}[X]/(\chi_\pi(X))$, that is, compute $\mathfrak{M} = \mathcal{O}_K$, $\mathfrak{m} = \mathbb{Z}[\pi, \overline{\pi}]$ and the factorization of $[\mathfrak{M} : \mathfrak{m}]$, we need to factor the discriminant Δ of χ_π which satisfies

$$|\Delta| \leqslant (2\sqrt{q})^{2g(2g-1)}.$$

For this, the unconditional method of L and P ( ) uses $L(|\Delta|)^{1+o(1)}$ operations; assuming unproved hypotheses, we might also use the number field sieve of C - ( ) with conjectured runtime

$$L_{1/3}^{c_{\mathrm{NFS}}}(|\Delta|) \qquad \text{where } c_{\mathrm{NFS}} = \frac{1}{3}\sqrt[3]{92 + 26\sqrt{13}} \approx 1.902.$$

For elliptic curves, we were able to prove the correctness and complexity of the rest of our method only assuming the generalized Riemann hypothesis. In that case, the complexity is

$$L(q)^{1/\sqrt{2}+o(1)},$$

so the cost of factoring via the unconditionally proven method dominates; we found it curious that no known factoring algorithm achieves a better exponent assuming solely the generalized Riemann hypothesis: there seems to be a gap in the hypothesis required as, in terms of asymptotically fast methods, we go straight from an unconditionally proven method to one which relies on many non-standard heuristics.

In dimension two, we will see that additional unproven hypotheses, other than the generalized Riemann hypothesis, are necessary.

O I

Let us briefly address the complexity of the algorithms used for navigating the lattice and computing with ideals of arbitrary orders in it.

The algorithms used greatly differ from dimension one to dimension two: in dimension one, the lattice is simply the set of divisors of $[\mathfrak{M} : \mathfrak{m}]$ while in higher dimension its structure has no such special form; again in dimension one, ideals can be dealt with extremely efficiently as binary quadratic forms while in higher dimension only general methods involving Hermite normal form and LLL reduction can be used.

In fact, we find that, in the realm of elliptic curves, many problems can be solved in *essentially linear* time, that is, with a complexity asymptotically equivalent to the size of the output, up to an exponent of $1 + o(1)$; but those problems become suddenly much harder with higher-dimensional abelian varieties and no such satisfying algorithm is known. This is for instance the case for the generation of Hilbert class polynomials. Our own endomorphism ring computing algorithm will not be an exception to this rule, as many simple and easy to analyze aspects of it are lost when going from dimension $g = 1$ to $g = 2$.

Regardless of the dimension, since we use the building blocks for orders and ideals on inputs of size for which their complexity is polynomial in $\log(q)$, we need not worry too much about them: as our overall expected complexity is superpolynomial, the cost of all these subroutines disappears within the $o(1)$ term of the exponent. This might seem a little too rough, so we refer to C ( ) for more careful statements regarding the complexity of these standards calculations.

O P G

Our relation method uses the Picard group structure to characterize an order. This section and the next are devoted to proving the correctness of this approach: here, we will see that there are not many orders with the same Picard group structure, and there, we will describe a workaround technique for distinguishing these rare orders from each other.

We first consider the one-dimensional case, as the ideal structure of non-maximal orders is much better understood in this case. If $\mathcal{O}$ is an order of an imaginary quadratic field K, we let $\mathfrak{B}$ be a generating set of ideals for $\mathrm{Pic}(\mathcal{O})$, and denote by $\Lambda_{\mathcal{O}}$ the relations of $\mathrm{Pic}(\mathcal{O})$ for this basis $\mathfrak{B}$; in other words, we assume that $\mathrm{Pic}(\mathcal{O}) \simeq \mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}}$.

Proposition VII.1.1. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders in an imaginary quadratic field* K. *The lattice $\Lambda_{\mathcal{O}'}$ contains $\Lambda_{\mathcal{O}}$ if and only if the order $\mathcal{O}'$ contains $\mathcal{O}$ or if one of the following holds:*

. $K = \mathbb{Q}(\sqrt{-4})$ *and $\mathcal{O}'$ has conductor* 2*;*
. $K = \mathbb{Q}(\sqrt{-3})$ *and $\mathcal{O}'$ has conductor* 2 *or* 3*;*
. *The prime* 2 *splits in* K *and $\mathcal{O}'$ has index* 2 *in some order above $\mathcal{O}$ of odd conductor.*

Proof. Denote by $S_{\mathcal{O}}$ (resp. $S_{\mathcal{O}'}$) the set of primes ℓ that split into principal ideals in $\mathcal{O}$ (resp. $\mathcal{O}'$). Using relations formed of a single prime ideal, we see that $\Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathcal{O}'}$ implies $S_{\mathcal{O}} \subseteq S_{\mathcal{O}'}$. Now $S_{\mathcal{O}}$ (resp. $S_{\mathcal{O}'}$) is also the set of primes that split completely in the ring class field $L_{\mathcal{O}}$ of $\mathcal{O}$ (resp. $L_{\mathcal{O}'}$). By Chebotarev's density theorem $S_{\mathcal{O}} \subseteq S_{\mathcal{O}'}$ thus implies $L_{\mathcal{O}'} \subseteq L_{\mathcal{O}}$ which means that the class field theory conductor $\mathfrak{f}(L_{\mathcal{O}'}/K)$ of $L_{\mathcal{O}'}$ divides $\mathfrak{f}(L_{\mathcal{O}}/K)$.

This is conductor $\mathfrak{f}(L_{\mathcal{O}}/K)$ is related to that $\mathfrak{f}_{\mathcal{O}}$ of $\mathcal{O}$ in the following manner (see Exercises . – . of C ( )).

$$\mathfrak{f}(L_{\mathcal{O}}/K) = \begin{cases} \mathcal{O}_K, & \text{when } K = \mathbb{Q}(\sqrt{-4}) \text{ and } \mathfrak{f}_{\mathcal{O}} = 2, \\ \mathcal{O}_K, & \text{when } K = \mathbb{Q}(\sqrt{-3}) \text{ and } \mathfrak{f}_{\mathcal{O}} = 2 \text{ or } 3, \\ \mathfrak{f}', & \text{when } 2 \text{ splits in } K \text{ and } \mathfrak{f}_{\mathcal{O}} = 2\mathfrak{f}' \text{ with } \mathfrak{f}' \text{ odd}, \\ f_{\mathcal{O}}, & \text{otherwise.} \end{cases}$$

Naturally, the same stands for $\mathcal{O}'$. In the latter case, the fact that $\mathfrak{f}(L_{\mathcal{O}}/K)$ divides $\mathfrak{f}(L_{\mathcal{O}'}/K)$ implies that $\mathfrak{f}_{\mathcal{O}'}$ divides $\mathfrak{f}_{\mathcal{O}}$, in other words $\mathcal{O} \subseteq \mathcal{O}'$; the three other cases correspond, in order, to the exceptions listed in the proposition. □

Intuitively, this means that identifying orders by their Picard groups has a single blind spot locally at 2 and 3 where the two largest orders cannot be distinguished.

For orders in higher-degree number fields, we were unable to prove a similar result, but have observed that pairs of orders with identical Picard group structure follow a similar pattern to what the proposition above describes for imaginary quadratic orders; therefore, we will assume:

Assumption VII.1.2. *Fix $g \in \mathbb{N}$; there exists an integer B such that, if any two orders $\mathcal{O}$ and $\mathcal{O}'$ of a complex multiplication field K of degree $2g$ have identical Picard group structure, then one is contained in the other with index a divisor of B, and both orders are maximal at all primes but the factors of B.*

For instance, in the case of quartic complex multiplication fields, our computations support

$$B = 2^6 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 41 \cdot 83 \cdot 127 \cdot 131 \cdot 151$$

This bound B could be reduced by excluding finitely many number fields.

Even if this assumption turns out to be wrong, our algorithms will still be functional as they do not need to know in advance which orders have the same Picard group structure: it can always be tested, as we ascend the lattice of orders and generate certificates, if an order has the same Picard group structure as some order directly above or below it. This is naturally quite expensive, but retains the unconditional correctness of our output.

L W

As we have seen, two different orders of a complex multiplication field K can have identical Picard group structure, in a limited number of cases. Those orders cannot be distinguished using the complex multiplication action, so we need another method to tell them apart from each other.

To tackle these cases, we apply our lattice-ascending and order-testing procedures normally and fall back on a second method when the endomorphism ring is found to be one of these. This amounts to ascending the lattice of orders quotiented by classes of orders with identical Picard group structure; when the class of End($\mathscr{A}$) is identified, we determine precisely which order End($\mathscr{A}$) is using the following algorithm.

Algorithm VII.1.3.

I : *A simple ordinary abelian variety $\mathscr{A}$ over the finite field with q elements, and an order $\mathcal{O}$ with the same Picard group structure as* End($\mathscr{A}$).

O : *An order isomorphic to* End($\mathscr{A}$).

. *Compute the Frobenius polynomial $\chi_\pi(x)$, and factor $[\mathcal{O}_K : \mathbb{Z}[\pi,\bar{\pi}]]$ as $\prod \ell^{v_\ell}$.*

. *For all prime factors ℓ with $\ell^{2gv_\ell} < L(|\Delta|)$:*

. *Determine* End($\mathscr{A}$) *locally at ℓ.*

. *For other prime factors ℓ:*

. *Compute various ℓ-isogenies and see if they change the Picard group structure of the endomorphism ring.*

. *Deduce* End($\mathscr{A}$).

The condition in Step ensures that the complexity of determining the endomorphism ring locally at ℓ via the method of E and L ( ) in Step is bounded subexponentially. Basically, since orders with identical Picard group structure only differ by smooth indices (as we saw in the previous section), only small primes ℓ will be of interest here (for others, $\mathcal{O}_\ell$ is the only possibility for End$(\mathscr{A})_\ell$); for these small primes, the condition means that the depth v_ℓ of the local lattice is not too large.

When v_ℓ is large, this method is too costly. On the other hand, since only the first few top orders have identical Picard group structure, we can compute random chains of ℓ-isogenies and count the minimal number of isogenies it takes to reach a variety whose endomorphism ring has a different Picard group structure (which we determine using our subexponential method). Since we can compute exactly which orders have identical Picard group structure, this gives us some information as to which order our endomorphism ring is.

This is obviously a rather poor approach. Better would be to use a higher-dimensional analog to the method of I and J ( ) and generalize the algorithm of K ( ) to compute the endomorphism ring locally at ℓ in time $\ell^{O(1)}$ rather than $\ell^{O(v_\ell)}$.

As the complexity of our fall back method depends not only on the prime ℓ at which we want to locally compute End($\mathscr{A}$), but on the entire factor ℓ^{v_ℓ} of the index $[\mathcal{O}_K : \mathbb{Z}[\pi,\bar{\pi}]]$, and we found no satisfying way of patching it, we simply rule out deep lattices.

Assumption VII.1.4. *Let $\mathcal{O} \subset \mathcal{O}'$ be two orders containing $\mathbb{Z}[\pi,\bar\pi]$ with identical Picard group structures. If ℓ is a prime factor of the index $[\mathcal{O}' : \mathcal{O}]$, we assume that the valuation v_ℓ of $[\mathcal{O}_K : \mathbb{Z}[\pi,\bar\pi]]$ at ℓ is such that $\ell^{2gv_\ell} < L(q)$.*

In dimension one, the method of K ( ) computes $\mathrm{End}(\mathscr{A})_\ell$ locally at ℓ by climbing the ℓ-isogeny volcano in time $v_\ell \ell^{2+o(1)}$, so the assumption above is not required in that case.

VII.2 Picard Groups from Relations

R S

We recall the standard "generator and relations" setting based on prime ideals to study the structure of Picard groups of orders in number fields.

Throughout this section, $\mathcal{O}$ will be an order in an algebraic number field, and $\mathfrak{B}$ a generating set of ideals for its Picard group; for computational reasons we assume that $\mathfrak{B}$ consists of prime ideals. We denote by $\Lambda_{\mathcal{O}}$ the lattice of relations among elements of $\mathfrak{B}$ seen as vectors of $\mathbb{Z}^{\mathfrak{B}}$, so that we have

$$\mathrm{Pic}(\mathcal{O}) \simeq \mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}}.$$

Our first task will be to bound the norm of primes contained in $\mathfrak{B}$; this is the purpose of the following section which describes various Chebotarev theorems that have been used over the years — this application being just one specific use of them.

Next, we will consider bounding the diameter of the lattice $\Lambda_{\mathcal{O}}$ which plays a crucial role in the generation of relations that characterizes $\mathcal{O}$. More explicitly, H and M C - ( ) proved that any bound on the diameter of the lattice $\Lambda_{\mathcal{O}}$ yields a box B whose pushforward distribution by $\sigma_{\mathcal{O}}$ is quasi-uniform; in other words, products of random elements of this box give quasi-random elements of the Picard group of $\mathcal{O}$.

This property is crucial to ensure that the relations we obtain permit us to distinguish a lattice from strictly smaller ones.

Originally, a bound elementarily derived from the theorem of S ( ) was used by H and M C ( ); later, B ( ) adapted their algorithm to general number fields, therefore relying on the theorem of B ( ). We will here give, as a consequence of the generalized Riemann hypothesis, a better bound which we will derive from a more general result of J , M , and V ( ).

C T

Let us first recall the classical *density theorem* of T ( ).

Theorem vii.2.1. *L'n* L/K *be a Ŕnite normal extension of number Ŕelds, and denote by* $\pi(\mathfrak{p})$ *ū e FrobeniŬ element in* Gal(L/K) *which corre ş onds to a given prime* $\mathfrak{p}$ *of* K*. Such FrobeniŬ elements are ńymptoticaŝy uniformly dśtributed in ū e sense ū Ņ, for any conjugacy cl ńs* $\mathscr{C}$ *of ū e Galoś group,*

$$\#\{\mathfrak{p} : \pi(\mathfrak{p}) \in \mathscr{C}, \mathrm{N}(\mathfrak{p}) < x\} \underset{x\to\infty}{\sim} \frac{\#\mathscr{C}}{\#\mathrm{Gal}(\mathrm{L}/\mathrm{K})} \mathrm{Li}(x)$$

where $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$ *ś ńymptoticaŝy equal to ū e number of prime ideals of norm less ū an x.*

Ł is theorem has countless applications; for in ance, if L is the ŕ litting ŏeld of a polynomial $f \in \mathrm{K}[x]$, it gives the density of primes $\mathfrak{p}$ of K modulo which f has prescribed ŕ litting patterns.

In our setting, we are mo ly intere ed in the case where $\mathrm{K} = \mathbb{Q}$ and L is the ring class ŏeld $\mathscr{H}_{\mathscr{O}}$ of an order $\mathscr{O}$ in some complex multiplication number ŏeld. Via the Artin map, the Chebotarev density theorem descends to ideals of the order $\mathscr{O}$ and asserts that the density of prime ideals which belong to a prescribed ideal class of $\mathrm{Pic}(\mathscr{O})$ is $1/\#\mathrm{Pic}(\mathscr{O})$; this implies in particular that each ideal class can be represented by a prime ideal, from which we can conclude that it is indeed possible to have a generating set $\mathfrak{B}$ for $\mathrm{Pic}(\mathscr{O})$ made of prime ideals.

More generally, so-called *e eňive CheboŪrev ū eorems* give upper bounds on elements generating number theoretic groups. Hi orically, intere ŏr lied in bounding the lea quadratic non-residue modulo n: G ŏr e ablished the bound $2\sqrt{n} + 1$ (for $n > 2$) elementarily and, to date, the be known unconditional bound of B ( ) is ill exponential — the proof mixes arguments of V ( ) with the Hasse–Weil bound on the number of points of hyperelliptic curves.

Assuming the Riemann hypothesis for the zeta funńion of certain ŏelds L, more precise results can be derived. Mo oŔen, authors simply assume the extended Riemann hypothesis (ERH), or even the generalized Riemann hypothesis (GRH) for convenience. Under this assumption, A ( ) proved that the bound above can be made $\mathrm{O}(\log^2 n)$.

L and O ( ) later generalized this to general number ŏelds: they proved that if L is a ŏnite nontrivial extension of an algebraic number ŏeld K, the lea prime ideal of K that does not ŕ lit completely in L is bounded by $\mathrm{O}(\log^2(\mathrm{disc}(\mathrm{K})^2\, \mathrm{N}(\mathfrak{f}(\mathrm{L}/\mathrm{K}))))$.

B ( ) gave explicit con ants O for these results: he showed that in the result of A ( ) we have $\mathrm{O} \leqslant 2$, and that $\mathrm{O} \leqslant 3$ for the generalized result. He derived the following:

Theorem vii.2.2. *Assuming ū e Riemann hypo ū esś for ū e z'na funňion of ū e number Ŕeld* K*, its Galoś group* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ *ś generŅed by ū e FrobeniŬ elements of its prime ideals of norm less ū an* $12\log^2|\mathrm{disc}(\mathrm{K})|$.

D S P

As we have already pointed out, knowing that the set $\mathfrak{B}$ of prime ideals of norm less than $12\log^2|\Delta|$ generates the Picard groups of orders $\mathscr{O}$ containing $\mathbb{Z}[\pi,\bar{\pi}]$ is not su cient. Indeed, evaluating isogenies associated to ideals $\mathfrak{a}$ which involve large exponents is co ly, so it is not su cient to write $\mathfrak{a}$ as a produń of primes of $\mathfrak{B}$: we also want this produń to be short. In other words, we ask that $\mathfrak{a} = \prod_{\in\mathfrak{B}} \mathfrak{p}^{n_\mathfrak{p}}$ for a small exponent veńor n.

Obviously, its norm $||n||_1 = \sum \left|n \right|$ is less than the class number. In their Lemma , H and M C ( ) proved that any bound on the diameter of the lattice $\Lambda_\mathscr{O}$ yields a box B suitable to search for relations, and as a bound they used the latter elementary result on the norm of n. B ( ) did the same in his Lemma . for arbitrary orders.

However, assuming the generalized Riemann hypothesis, a much better bound can be derived from Corollary . of J , M , and V ( ), which implies:

Theorem vii.2.3 (GRH). *For aŝ $g \in \mathbb{N}$ and $\varepsilon > 0$, ūere exśts $c > 1$ such ūŅ, if $\mathscr{O}$ ś an order of dimension $2g$ and dścriminant Δ, ūen for random veňors x drawn Řom ūe box*

$$\mathrm{B} = \left\{ x \in \mathbb{Z}^{\{ \,:\mathrm{N}(\,)<\log^{2+\varepsilon}|\Delta|\}} : \sum_{\mathfrak{B}} |x \;| = c\frac{\log|\Delta|}{\log\log|\Delta|} \right\}$$

ūe probability ūŅ $\sigma_\mathscr{O}(x)$ faŝs in any Ŕxed ideal clńs of $\mathrm{Pic}(\mathscr{O})$ *ś Ņ leńt* $1/2\#\mathrm{Pic}(\mathscr{O})$.

In terms of di ribution, this ates that the pushforward di ribution by $\sigma_\mathscr{O}$ of the uniform di ribution $\mathbb{U}_\mathrm{X}$ on the set X of veńors of norm $c\log|\Delta|/\log\log|\Delta|$ is within variation di ance $1/2$ from the uniform di ribution on the Picard group. Essentially, this says that produńs of randomly seleńed primes of quadratic norm behave as uniformly-drawn elements of the Picard group.

D R L

Ł e above theorem implies that each element of $\mathrm{Pic}(\mathscr{O})$ has a preimage of small norm, from which we can easily derive a bound on the diameter of $\Lambda_\mathscr{O}$. Recall that the *diam'ner* of a lattice is the smalle value diam(F) where F ranges over its fundamental domains.

Corollary vii.2.4 (GRH). *Fix any positive number ε. If $\mathscr{O}$ ś an order of dścriminant Δ and $\mathfrak{B}$ denotes its s'n of primes of norm less ūan $\log^{2+\varepsilon}|\Delta|$, ūe diam'ner of ūe lŅtice $\Lambda_\mathscr{O}$ ś* $o(\log^{4+\varepsilon}|\Delta|)$.

Proof. To prove this, we construct a generating set for $\Lambda_{\mathcal{O}}$ formed by $O(\log^{2+\varepsilon}|\Delta|)$ relations of norm $o(\log^2|\Delta|)$. B ( ) showed that $\mathrm{Pic}(\mathcal{O})$ is an abelian group of order $\Delta^{1/2+o(1)}$ so there exist $O(\log|\Delta|)$ ideal classes α_i such that $\mathbb{Z}^{\mathfrak{B}}/\Lambda_{\mathcal{O}} \simeq \prod \langle\alpha_i\rangle$; we fix these and proceed to write a generating set for $\Lambda_{\mathcal{O}}$ consisting of:

- relations expressing that $\alpha_i^{\mathrm{ord}(\alpha_i)} = 1$;
- relations expressing the primes $\mathfrak{p} \in \mathfrak{B}$ in terms of the α_i.

First define a map $\sigma_{\mathcal{O}}^{-1}$ by fixing a preimage of norm at most $c\log|\Delta|/\log\log|\Delta|$ for each ideal class; it exists by Theorem . . . Now use a double-and-add approach to ensure that norms remain small: for each i, express that $\alpha_i^{\mathrm{ord}(\alpha_i)} = 1$ by the relations

(i) $\sigma_{\mathcal{O}}^{-1}\left(\alpha_i^{2^j}\right) - 2\sigma_{\mathcal{O}}^{-1}\left(\alpha_i^{2^{j-1}}\right)$ for $j \in \{1,\dots,\lfloor\log_2 \mathrm{ord}(\alpha_i)\rfloor\}$;

(ii) $\sum_j b_j\sigma_{\mathcal{O}}^{-1}\left(\alpha_i^{2^j}\right)$ where b_j denotes the j^{th} least significant bit of $\mathrm{ord}(\alpha_i)$.

Now write each $\mathfrak{p} \in \mathfrak{B}$ on the α_i by decomposing its class as a product $\prod \alpha_i^{n_i}$ where $n_i \in \{0,\dots,\mathrm{ord}(\alpha_i)\}$; noting δ the vector with coordinate one at $\mathfrak{p}$ and zero elsewhere, this gives the relations:

(iii) $\delta - \sum_i\sum_j c_{ij}\sigma_{\mathcal{O}}^{-1}\left(\alpha_i^{2^j}\right)$ where c_{ij} is the j^{th} least significant bit of n_i.

Preimages by $\sigma_{\mathcal{O}}$ have length $o(\log|\Delta|)$ and there are at most $\sum\lfloor\log_2 \mathrm{ord}(\alpha_i)\rfloor = O(\log|\Delta|)$ terms, therefore each such relation has length $o(\log|\Delta|)^2$. □

VII.3 Relations from Smooth Ideals

Let us now give the mathematical background required to prove the complexity of the subexponential method for finding smooth relations in Picard groups.

I S

We start by reviewing fundamental properties of smooth numbers; these are the base on which most subexponential algorithms are build upon (for instance, we have already mentioned factoring algorithms). First recall their definition.

Definition VII.3.1. *An integer x is said to be y-smooth if it has no prime factor larger than y. The number of y-smooth integers less than x is denoted $\Psi(x,y)$.*

Bounding the value of the Ψ function for particular ranges of x and y is an important problem. For instance, for any fixed $u \geqslant 1$, we have

$$\Psi\left(x, x^{1/u}\right) \underset{x\to\infty}{\sim} x\rho(u)$$

where the con ant $\rho(u)$ is the Dickman funńion. Ł is funńion was extensively udied by B who gave many ways to evaluate it. To use such smoothness results in index-calculus methods, we need more than a polynomial relation of the form $y = x^{1/u}$: we would like to consider the case where $u \to \infty$ as $x \to \infty$. Ł e ŕ eciŏc result we rely on is due to C , E , and P ( ).

Theorem vii.3.2. *For $u \geqslant 3$ we have*

$$\Psi\left(x, x^{1/u}\right) \geqslant x \exp\left(-u\left(\log u + \log\log u - 1 + o(1)\right)\right)$$

Corollary vii.3.3. *Ńe probability for a random number of $\{1, \dots, x\}$ to be $L(x)^{\gamma}$-smoo ū ś equivalent to $L(x)^{-1/2\gamma + o(1)}$ ń $x \to \infty$.*

Proof. Apply the theorem above to $u = \frac{1}{\gamma}\sqrt{\frac{\log x}{\log\log x}}$ and combine it with the upper bound in Ł eorem of B ( ). ☐

See G ( ) for a survey of this topic.

I S

Our algorithms do not exańly work with integers: they work with ideals. Via the norm, the ruńure of the ring of ideals resembles that of integers; for our particular goal, it su ces to say that ideals are smooth if and only if their norms are. However, not all results are easy to generalize from integers to ideals.

In fań, our ŏr algorithm for computing endomorphism rings of elliptic curves, from B. and S ( ), relied on the assumption that certain ideals we generated had a uniformly di ributed norm, so that we could dirańly apply the result of the previous seńion. We now explain how this assumption can, in some setting, be rigorously proven.

Let us ŏr recall the relevant part of our algorithm: for an order $\mathcal{O}$ of discriminant Δ, we ŏr seleń a veńor x uniformly at random from the box $B = \{0, \dots, \log^{4+\varepsilon}|\Delta|\}^{\mathfrak{B}}$ where $\mathfrak{B}$ is the set of prime ideals of norm less than $\log^{2+\varepsilon}|\Delta|$; we then look for a small representative $\widehat{x}$ of the class $\sigma_{\mathcal{O}}(x) \in \mathrm{Pic}(\mathcal{O})$ and attempt to fańor it over the base consi ing of all the prime ideals of norm less than $L(|\Delta|)^{\gamma}$.

To rigorously bound the number of times random veńors $x \in B$ have to be seleńed before one with smooth reduńion is found, we need to show that the norm of $\widehat{x}$ behaves like a random integer in a certain interval.

For imaginary quadratic orders, S ( ) used the andard reduńion of binary quadratic forms; to obtain a result on the smoothness probability of $\widehat{x}$, he proceeds in two eps: Proposition . and . :

Proposition VII.3.4. *Ideal classes $\sigma_{\mathcal{O}}(x)$ of randomly selected vectors $x \in \mathrm{B}$ are quasi-uniformly distributed in the Picard group of $\mathcal{O}$.*

By *quasi-uniformly distributed*, we mean that the probability for $\sigma_{\mathcal{O}}(x)$ to belong to a prescribed subset S of $\mathrm{Pic}(\mathcal{O})$ is

$$(1 + o(1))\frac{\#\mathrm{S}}{\#\,\mathrm{Pic}(\mathcal{O})}$$

in other words, the pushforward di ribution $\sigma_{\mathcal{O}\star}\mathbb{U}_{\mathrm{B}}$ is within variation di ance $o(1)$ of the uniform di ribution on $\mathrm{Pic}(\mathcal{O})$.

Note that S ( ) arted from a much bigger box B than ours; it was, back then, the be possible under the generalized Riemann hypothesis; however, here, we make use of Corollary . of J , M , and V ( ) and of the smaller box B it proves to su ce.

When we know that $\sigma_{\mathcal{O}}(x)$ is quasi-random, it remains to see whether the element $\widehat{x}$ of each $\sigma_{\mathcal{O}}(x)$ has a smoothness probability comparable to integers of $\{1, \dots, \sqrt{|\Delta|/3}\}$.

Proposition VII.3.5. *The number of reduced ideals whose norm is $\mathrm{L}(|\Delta|)^{\gamma}$-smooth is at least $n/\mathrm{L}(|\Delta|)^{1/2\gamma+o(1)}$ where $n = \#\,\mathrm{Pic}(\mathcal{O})$ is the total number of reduced ideals.*

The proof of S ( ) involves calculations which are specific to the arithmetic of binary quadratic forms. This makes it challenging to generalize this proposition in higher-dimensional orders, and another issue is that there is no canonical notion of reduction there. The method of B ( ) for arbitrary orders relies on the following assumption, and we do as well.

Assumption VII.3.6. *The norms of reduced ideals used by the smooth relation finding algorithm are as likely to be smooth as random integers of $\{1, \dots, \sqrt{|\Delta|}\}$.*

R R

To obtain a generating set for the lattice $\Lambda_{\mathcal{O}}$ by finding relations of it, we mu ensure that those relations do not lie in some particular subset. For in ance, if the order $\mathcal{O}$ contains $\mathcal{O}'$, then we have $\Lambda_{\mathcal{O}'} \subset \Lambda_{\mathcal{O}}$, and we mu prove that our relations have no predisposition of actually lying in $\Lambda_{\mathcal{O}'}$. Whence the following definition.

Definition VII.3.7. *Let* P *be a probabilistic procedure which, on input an order $\mathcal{O}$ containing $\mathbb{Z}[\pi, \overline{\pi}]$ for some Weil number π, returns a relation $x \in \Lambda_{\mathcal{O}}$, which we see as a random variable.*

We say that P *generates* quasi-uniformly di ributed relations *of $\mathcal{O}$ if, for any order $\mathcal{O}'$ containing $\mathbb{Z}[\pi, \overline{\pi}]$, the projection of x in the quotient group $\Lambda_{\mathcal{O}}/\Lambda_{\mathcal{O}\cap\mathcal{O}'}$ is within variation distance $o(1)$ from the uniform distribution, as the discriminant of π goes to infinity.*

Proving that the method of S ( ) does indeed generate quasi-uniformly distributed relations was done by H and M C ( ) in their Lemma .

Proposition VII.3.8. *If $\mathcal{O}'$ is an order contained in $\mathcal{O}$, relations found by the method of S ( ) are quasi-uniformly distributed in $\Lambda_{\mathcal{O}}/\Lambda_{\mathcal{O}'}$ when $\mathrm{B} = \{0, \dots, \#\mathfrak{B}d^{1+\varepsilon}\}^{\mathfrak{B}}$, where d is a bound on the diameter of $\Lambda_{\mathcal{O}}$.*

The proof is pretty simple and involves looking at the geometry of the lattices in a fairly elementary way. We reproduce it below, in the more general context of an unspecified bound d on $\operatorname{diam} \Lambda_{\mathcal{O}}$.

Proof. Let x be a random variable with uniform distribution on $\mathrm{B}_t = \{0, \dots, t\}^{\mathfrak{B}}$, let $\widehat{x} \in \sigma_{\mathcal{O}}(x)$ denote its reduction, and note $\mathscr{S}$ the set of ideals with $\mathscr{L}$-smooth norms. We want to prove that

$$\operatorname{Prob}\left[x - \sigma^{-1}(\widehat{x}) \in \omega \middle| \widehat{x} \in \mathscr{S}\right] = \left[\Lambda_{\mathcal{O}} : \Lambda_{\mathcal{O}'}\right]^{-1} (1 + o(1))$$

for any fixed class $\omega \in \Lambda_{\mathcal{O}}/\Lambda_{\mathcal{O}'}$. We can rewrite the left-hand side as

$$\frac{\#\left\{x \in \mathrm{B}_t : \widehat{x} \in \mathscr{S}, x - \sigma^{-1}(\widehat{x}) \in \omega\right\}}{\#\left\{x \in \mathrm{B}_t : \widehat{x} \in \mathscr{S}\right\}}$$

and by summing over all possible reduced ideals y we further obtain

$$\frac{\sum_{y \in \mathscr{S}} \#\left\{x \in \mathrm{B}_t : x \in \sigma^{-1}(y) + \omega\right\}}{\sum_{y \in \mathscr{S}} \#\left\{x \in \mathrm{B}_t : x \in \sigma^{-1}(y) + \Lambda_{\mathcal{O}}\right\}}.$$

Now, to evaluate each term of these sums, let us count the number of points of $\overline{\mathrm{B}}_t = [0, t+1)^{\mathfrak{B}}$ which lie in the translation $z + \Lambda$ of some lattice Λ. To this extent, let $\mathscr{F}$ be a fundamental domain for Λ: each point of $z + \Lambda$ corresponds to a cell in the tiling of $\mathbb{R}^{\mathfrak{B}}$ by $\mathscr{F}$; if $\operatorname{diam} \mathscr{F} \leqslant d$ we therefore have

$$\overline{\mathrm{B}}_{t-d} \subset (z + \Lambda) \cap \overline{\mathrm{B}}_t + \mathscr{F} \subset \overline{\mathrm{B}}_{t+d}$$

which gives, in terms of volumes,

$$(t-d)^{\#\mathfrak{B}} \leqslant \det \Lambda \cdot \#\left((z + \Lambda) \cap \mathrm{B}_t\right) \leqslant (t+d)^{\#\mathfrak{B}}$$

so as soon as $\#\mathfrak{B}d = o(t)$, the sandwich theorem proves that

$$\#\left((z + \Lambda) \cap \mathrm{B}_t\right) = \frac{t^{\#\mathfrak{B}}}{\det \Lambda}(1 + o(1));$$

by sub ituting this in the probability sought expressed as a quotient of sums, we obtain

$$\#\mathscr{S}\,\frac{t^{\#\mathfrak{B}}}{\det\Lambda_{\mathscr{O}'}}(1+o(1)) \Big/ \#\mathscr{S}\,\frac{t^{\#\mathfrak{B}}}{\det\Lambda_{\mathscr{O}}}(1+o(1))\ ;$$

Choosing $t = \#\mathfrak{B}d^{1+\varepsilon}$ satisões the requirement $\#\mathfrak{B}d = o(t)$ and gives the result. □

Recall that if $\mathscr{O}$ is an order of discriminant Δ and $\mathfrak{B}$ consi s of all prime ideals of norm less than $\log^{2+\varepsilon}|\Delta|$, then the diameter of $\Lambda_{\mathscr{O}}$ is $o(\log^{4+\varepsilon}|\Delta|)$. Ł erefore, when $\mathscr{O}$ is imaginary quadratic, the above proposition shows that the algorithm of S ( ) generates quasi-uniformly di ributed relations of $\Lambda_{\mathscr{O}}$ when drawing its random veńors uniformly from the box $\mathrm{B} = \{0, \ldots, \log^{2+\varepsilon}|\Delta|\}^{\mathfrak{B}}$.

When $\mathscr{O}$ is an order in a complex multiplication of degree four or more, as we have mentioned before, we do not know of similar results and believe that they might be quite di cult to e ablish. However, we can ill amend the algorithm of B ( ) to make use of this type of bound. Ł is gives a conjeńural running time, but the result can in any case be unconditionally proven by certiŏcates, so we have a Las-Vegas algorithm.

G E R

To prepare for the jump to the next chapter, let us put together the results that we have e ablished so far. Here, we let π be the Frobenius endomorphism of an abelian variety of dimension g deŏned over a ŏnite ŏeld $\mathbb{F}_q$, and recall from Lemma . . that $\mathrm{disc}(\mathbb{Z}[\pi,\overline{\pi}]) = q^{g^2+o(1)}$ so that via the theorem of B ( ) the class number is $q^{g^2/2+o(1)}$.

Proposition vii.3.9. *Ł'n $\mathscr{O}$ be an order of dścriminant Δ in a number Ŕeld of degree $2g$; random relŅions of $\mathscr{O}$ inl·oll·ing polynomiaŝy many ideals in $\log|\Delta|$ of norm up to $\mathrm{L}(|\Delta|)^{\gamma}$ can be found in probabilśtic time $\mathrm{L}(|\Delta|)^{\gamma} + \mathrm{L}(|\Delta|)^{1/4\gamma+o(1)}$.*

Ń ś ńsumes ūe generalized Riemann hypoūesś for $g = 1$, and Assumption . . for $g > 1$.

Unlike H and M C ( ), we do not seek to compute the full group ruńure of $\mathrm{Pic}(\mathscr{O})$ — this would be co ly since a subexponential number of relations is required to eliminate all fańors of the fańor base. Here, we ju aim at di inguishing orders containing $\mathbb{Z}[\pi,\overline{\pi}]$ from one another.

If $\mathscr{O}'$ is an order such that $\Lambda_{\mathscr{O}'}$ is rińly contained in $\Lambda_{\mathscr{O}}$, a quasi-uniformly di ributed relation has probability at mo $1/2 + o(1)$ of also holding in $\mathscr{O}'$. Ł erefore, since we have a polynomial number of orders in $\log|\Delta|$ to discriminate from, it is su cient to only generate polynomially many orders in $\log\log|\Delta|$ to ensure that the relations charańerize the lattice $\Lambda_{\mathscr{O}}$ with probability $1 - o(1)$.

Combining the above with our earlier notes on the complexity of isogeny computation, we have proved the following.

Theorem VII.3.10. *L'n $\mathscr{A}$ be a simple ordinary abelian vari'ny of dimension g deŔned over ūe Ŕnite Ŕeld wiū q elements. Under ūe generalized Riemann hypoūesś, we can compute* $\mathrm{End}(\mathscr{A})$*:*

- *if* $g = 1$*, in* $\mathrm{L}(q)^{1+o(1)} + \mathrm{L}(q)^{1/\sqrt{2}+o(1)}$ *operŅions;*
- *if* $g = 2$*, in* $\mathrm{L}(q)^{g\sqrt{3g}/2+o(1)}$ *operŅions, under Assumptions . . . , . . . , . . . , and . . .*

For $g = 2$, details will be given in the next chapter.

VII.4 Relations from Thin Air

As a supplement to this chapter, we shall now see how to generate relations in a generic manner, that is, not using any extrinsic information about the underlying group. For Picard groups, such methods are much slower than smoothness-based ones but yield much shorter relations; this will be an important ingredient for making prańical use of our method in dimension two.

G S P

Let S be a sequence of elements in a ŏnite group G of order n, written multiplicatively, and consider the problem of writing a prescribed element $z \in G$ as the produń of a subsequence of S; we call such a subsequence a *short produň represenŪtion* of z on S.

If G were a commutative group, we could have noted it additively, let S be a multiset of elements of it, and look for a sub-multiset which adds up to z; in the case that S has no repeated elements, this is known as the *subs'n sum problem*. However, since for our approach it makes absolutely no di erence whether G is commutative, we have chosen to use the more general formalism of non-necessarily-commutative groups.

Consider the produń map $\pi : \mathfrak{P}(S) \to G$ where $\mathfrak{P}(S)$ denotes the set of all subsequences of S. For all elements of G to admit short produń representations, the map π needs to be surjeńive which, by a counting argument, implies $k \geqslant \log_2 n$ where k is the length of S.

In the case that G is commutative, E and R ( ) showed that this bound is not far from being su cient: they prove that a random sequence S of length

$$k = \log_2 n + \log_2 \log n + \omega_n$$

satisfies $\pi(\mathfrak{P}(S)) = G$ with probability approaching 1 as $n \to \infty$, provided that $\omega_n \to \infty$.

For finding short product representations via generic means, just knowing the existence of a preimage by π for all $z \in G$ is not enough: we need to know the distribution of such preimages. I and N ( ) proved the following result on the inverse distribution.

Theorem VII.4.1. *Fix some real number d. For groups* G *of order n large enough, we have*

$$\mathrm{Prob}_S \left[\left\| \pi_\star \mathbb{U}_{\quad (S)} - \mathbb{U}_G \right\| \geqslant n^{-c} \right] \leqslant n^{-c}$$

where $c = (d-1)/2$ *and the sequence* S *is drawn uniformly at random from the set of sequences of* G *with length* $k = (d + o(1)) \log_2 n$.

Recall that $\mathbb{U}_X$ denotes the uniform distribution on the (finite) set X, and that the *push-forward distribution* $f_\star\sigma$ of a distribution σ on X by a function $f : X \to Y$ is defined as

$$f_\star\sigma(y) = \sigma\left(\{x \in X : f(x) \in y\}\right),$$

for any subset y of Y. Finally, the *variation distance* $\|\sigma - \sigma'\|$ between two distributions on Y is the maximum value of $|\sigma(y) - \sigma'(y)|$ as y ranges over all subsets of Y.

In other words, the theorem means that, for a random sequence S of *density* $d > 1$, the distribution of subsequence products almost surely converges to the uniform distribution on G as n goes to infinity.

In some particular cases, finding short product representations is a well-known problem. For instance, when G is the Picard group of some order and S contains all prime powers p^α with $p < L(|\Delta|)$ and $\alpha < \log_p |\Delta|$, then this is exactly the problem of finding relations which we have studied extensively. Now this problem does not have a "constant" density, as the quantity $k/\log_2 n$ goes to infinity pretty quickly with n.

For instances of constant density in the group $G = \mathbb{Z}/n\mathbb{Z}$, the best algorithm has a time and space complexity of $O(n^{0.3113})$; it consists in lifting the instance to k subset sum problems in $\mathbb{Z}$, also known as knapsack problems, which can be solved efficiently by a method of H -G and J ( ). Again, this algorithm is tailored for a specific group representation.

Algorithms that only perform multiplications and inversions (which return uniquely identified group elements), draw elements at random from G, and test their equality, are called *generic algorithms*. In essence, they are not tied to any specific group and apply to any effective group. S ( ) proved that solving discrete logarithm problems generically has a lower bound of $\Omega(\sqrt{p})$ where p is the largest prime factor of n; since this is a special case of short product representation, this means that generic short product representation algorithms cannot have a faster-than-square-root complexity in the worst case.

B -S G -S

Let us first review classical approaches to the problem of finding a short product representation of an element $z \in G$ on a sequence S.

A brute-force algorithm would exhaustively enumerate the set $\mathfrak{P}(S)$ and for each element y of it test whether $\pi(y) = z$.

The standard baby-step giant-step approach splits the search space as a direct product $\mathfrak{P}(S) = \mathfrak{P}(A) \times \mathfrak{P}(B)$ simply by writing S as the concatenation of two smaller sequences A and B; then, it aims at finding a pair of elements $(x, y) \in \mathfrak{P}(A) \times \mathfrak{P}(B)$ which *collide* in the sense that $\pi(x) = z\pi(y)^{-1}$. This can be implemented efficiently by first precomputing and storing a table of all $\pi(x)$ for $x \in \mathfrak{P}(A)$, and then checking whether each $z\pi(y)^{-1}$ for $y \in \mathfrak{P}(B)$ is in this table; the lookup can be done in time $O(\log n)$ using an efficient data structure.

For convenience, we define an application μ which maps any sequence $y = (y_1, \ldots, y_m)$ to $\mu(y) = (y_m^{-1}, \ldots, y_1^{-1})$, so that $\pi(y)$ and $\pi(\mu(y))$ are inverses in G. The baby-step giant-step algorithm then amounts to the following procedure.

Algorithm VII.4.2.

I : *A finite sequence* S *and a target* $z \in G$.

O : *If it exists, a subsequence of* S *whose product is* z.

. *Split* S *in a concatenation* AB *of sequences of roughly equal sizes.*

. *For each* $x \in \mathfrak{P}(A)$, *store x in a table indexed by* $\pi(x)$.

. *For each* $y \in \mathfrak{P}(B)$:

. *If* $\pi(z\mu(y)) = \pi(x)$ *for some x, then return xy.*

. *Return that z has no preimage by* π *in* $\mathfrak{P}(S)$.

As each element of $\mathfrak{P}(A)$ can be represented by $k/2$ bits (which is a constant factor away from the size of a group element, when the density d is fixed), the total memory consumed by this algorithm is $O(2^{k/2})$. By enumerating elements of $\mathfrak{P}(A)$ and $\mathfrak{P}(B)$ in a suitable order (for instance, using a Gray code), only one group operation is required per step, so that the total runtime is $O(2^{k/2})$.

S and S ( ) gave a more specialized generic method for solving knapsack problems, which improves the space complexity of the baby-step giant-step algorithm to $O(2^{k/4})$.

P R

In order to apply the Pollard ρ approach to the problem of finding short product representations, we simply need a notion of collision on a certain domain $\mathscr{C}$ and an iteration map

$\varphi : \mathscr{C} \to \mathscr{C}$ which preserves collisions in the sense that if x and y collide, then $\varphi(x)$ and $\varphi(y)$ also collide.

Here, we use the same domain that was used by the baby-step giant-step algorithm: first split S as a concatenation AB of two sequences of roughly equal size, and let the domain be the disjoint union $\mathscr{C} = \mathscr{A} \sqcup \mathscr{B}$ where $\mathscr{A} = \mathfrak{P}(\mathrm{A})$ and $\mathscr{B} = z\mu(\mathfrak{P}(\mathrm{B}))$. Now collisions are defined with respect to the product map $\pi : \mathscr{C} \to \mathrm{G}$; when an element $x \in \mathscr{A}$ collides with an element $y \in \mathscr{B}$, that is, $\pi(x) = \pi(y)$, then we have a short product representation of z as xy' where $y = z\mu(y')$.

Now since the iteration map φ must respect collisions, it must factor through the product map π so we can write $\varphi = \eta \circ \pi$ for some $\eta : \mathrm{G} \to \mathscr{C}$. Since we have no requirement on η, we simply take it to be a hash function from G to $\mathscr{C}$, that is, an effective map which behaves as if it were drawn uniformly at random from $\mathscr{C}^{\mathrm{G}}$.

In practice, to compute $\eta(g)$ we can take the unique bit-string representation of g, hash it using a strong cryptographic hash function, and use the resulting bit-string $g_0 g_1 g_2 \ldots$ to dictate an element of $\mathscr{C}$; for instance, the first bit g_0 can be used to decide whether $\varphi(g)$ lies in $\mathfrak{P}(\mathrm{A})$ or $z\mu(\mathfrak{P}(\mathrm{B}))$, the second bit g_1 to decide whether the first element of A (resp. B) belongs to $\varphi(g)$, etc. (Note that η cannot be surjective since G is smaller than $\mathscr{C}$.)

This gives the following algorithm.

Algorithm VII.4.3.

Input : *A finite sequence* S *and a target* $z \in \mathrm{G}$.

Output : *A subsequence of* S *whose product is* z.

1. *Split* S *as a concatenation* AB *of sequences of roughly equal sizes.*
2. *Pick a random element* $w \in \mathscr{C}$ *and a hash function* $\eta : \mathrm{G} \to \mathscr{C}$.
3. *Find the least* $i > 0$ *and* $j \geqslant 0$ *such that* $\varphi^{(i+j)}(w) = \varphi^{(j)}(w)$.
4. *If* $j = 0$ *then return to Step 2.*
5. *Let* $s = \varphi^{(i+j-1)}(w)$ *and let* $t = \varphi^{(j-1)}(w)$.
6. *If* $\pi(s) \neq \pi(t)$ *then return to Step 2.*
7. *If* $s \in \mathscr{A}$ *and* $t = z\mu(y) \in \mathscr{B}$ *for some* y*, output* sy *and terminate.*
8. *If* $t \in \mathscr{A}$ *and* $s = z\mu(y) \in \mathscr{B}$ *for some* y*, output* ty *and terminate.*

Basically, we start from a random point w and compute iterates $\varphi^{(i)}(w)$ until we find two which are equal: once we have the first such collision, that is, $\varphi(s) = \varphi(t)$ with $s \neq t$, we first make sure it is not due to the hash function, so that the collision must arise in the product map. Then, if it is a collision between an element of $\mathscr{A}$ and one of $\mathscr{B}$, which happens with expected probability $1/2$, we have a short product representation.

Step 3 can be implemented by Floyd's algorithm, by the method of distinguished points, or any other collision-detection technique (which reduces by a constant factor the number of expected evaluations of the map φ before finding a collision).

Ł is gives an algorithm with con ant orage ŕ ace and a time complexity of $O(k\sqrt{n})$. We refer the reader to B. and S ( ) for a rigorous proof (and also for details regarding this whole seńion) and now turn to applications.

A

Ł is method ańually has a broad range of applications; in particular, it can be used to ŏnd isogenies between two ordinary elliptic curves deŏned over a ŏnite ŏeld having the same endomorphism ring in square-root time and without orage requirements. Ł is application can be found in B. and S ( ). Here, we will present a di erent one, maybe not as important, but which applies direńly to the topic of computing endomorphism rings.

As usual, we ŏx an ambient ŏnite base ŏeld $\mathbb{F}_q$ and let $\mathscr{A}$ denote an simple ordinary abelian variety. Consider the set G of isomorphism classes of abelian varieties whose endomorphism ring is the same as that of $\mathscr{A}$; as we have seen before, it is a principal homogeneous ŕ ace for the Picard group $\mathrm{Pic}(\mathrm{End}\,\mathscr{A})$ whose cardinality we denote n (in the wor case, it is exponential in $\log(q)$ and the dimension g of $\mathscr{A}$).

Our method for computing $\mathrm{End}(\mathscr{A})$ has so far been to compute relations in the Picard group of the possible orders (those that contain $\mathbb{Z}[\pi,\overline{\pi}]$) and checking whether they hold in the isogeny graph. Here, we take the inverse approach: we will look for relations in the isogeny graph, and then rule out from the li of possibilities those orders in which the relations do not hold.

Of course, since the only algorithms we have at our di ŕ osal for ŏnding relations in the isogeny graph are generic, this is much slower than looking for relations in Picard groups. However, this gives a runtime which mo ly depends on the output: the closer to $\mathscr{O}_K$ the endomorphism ring of $\mathscr{A}$, the fa er it is found.

To look for relations in the isogeny graph of $\mathscr{A}$, a baby- ep giant- ep approach is simple to use: let S be a set of prime ideals of $\mathscr{O}_K$ which are coprime to the conduńor of $\mathbb{Z}[\pi,\overline{\pi}]$, ŕ lit it as a concatenation AB, let $\mathscr{A} = \mathfrak{P}(A)$ and $\mathscr{B} = \mathfrak{P}(B)$, and deŏne $\mathscr{C} = \mathscr{A} \sqcup \mathscr{B}$. We view an element $x = (\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m)$ of $\mathscr{C}$ as the isogeny

$$\varphi_{\;_1\;_2\cdots\;_m}(\mathscr{A}) = \varphi_{\;_1} \circ \varphi_{\;_2} \circ \cdots \circ \varphi_{\;_m}(\mathscr{A})$$

and we deŏne the map $\pi : \mathscr{C} \to G$ as sending x to the variety which is the codomain of this isogeny.

Now it is raightforward to adapt the Pollard ρ method to this context as we have done before: it su ces to take a hash funńion $\eta : G \to \mathscr{C}$ and to iterate the map $\varphi = \eta \circ \pi$ enough times to ŏnd a collision. Recall from Chapter that, in the wor case, we might have

$$\#G = \#\,\mathrm{Pic}\left(\mathrm{End}\,\mathscr{A}\right) = q^{(1/2+o(1))g^2}$$

so that if we take a sequence S of length at lea

$$(d + o(1))g^2 \log_2 q$$

for some $d > 1$, we can e eńively ŏnd a relation of the isogeny graph in probabili ic time $q^{(1/4+o(1))g^2}$ using virtually no memory, assuming the quasi-uniform di ribution of produńs of S in the Picard group; this assumption can be replaced by the generalized Riemann hypothesis by sub ituting $\log_2(q)$ by $\log^{2+\varepsilon}(q)$ above, via a result of J , M , and V ( ) — note however that this has little e eń on the runtime: although the produńs to be computed have more terms, the collision probability is unchanged.

By ŏnding relations in the isogeny graph of $\mathscr{A}$, we can te whether a given order $\mathscr{O}$ contains $\mathrm{End}(\mathscr{A})$ in time $\mathrm{disc}(\mathrm{End}\,\mathscr{A})^{1/4+o(1)}$ up to polynomial fańors in $\log(q)$ and g. Ł erefore, locating the endomorphism ring takes ju as much time using the "reversed" lattice-ascending procedure of the previous chapter for computing $\mathrm{End}(\mathscr{A})$ from above.

Note that certiŏcates that are generated with such generic methods have a length polynomial in the size of the base ŏeld $\log q$, which is much smaller than what subexponential methods can generate. More precisely, this length can essentially be quadratic if we require that the runtime of the generation algorithm be bounded under the generalized Riemann hypothesis (via Ł eorem . .), or linear if the heuri ic Conjeńure . . is used in ead.

Verifying the certiŏcate then ju requires polynomial time in its size: it su ces to verify the number of points on the variety and compute the isogenies associated to the ideals in the relation.

Here again, we have made use of isogenies between isomorphism classes of abelian varieties, not involving any polarizations, which is not an e eńive notion in dimension $g > 1$. We thus devote the next chapter to describing the changes required for making e eńive use of our endomorphism computing method on abelian varieties of dimension $g > 1$.

References

. Ivan M. V .
"On the di ribution of quadratic residues and non-residues".
In: *Journal of ūe Physico-MŅhemŅical Soci'ny of Perm* . Pages – .

. Nikolai T .
"Die Be immung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Sub itutionsklasse gehören".
In: *MŅhemŅśche Annalen* . . Pages – . DOI: 10.1007/BF01206606.

. Carl L. S .
"Über die Classenzahl quadratischer Zahlkörper".
In: *Aňa Ariū m'nica* . Pages – .

. Richard B .
"On the zeta-funńions of algebraic number ŏelds".
In: *American Journal of MṆhemṆics* . . Pages – .
DOI: 10.2307/2371849.

. Nesmith C. A .
"Ł e lea quadratic non residue". In: *Annals of MṆhemṆics* . . Pages – .
DOI: 10.2307/1969420.

. David A. B .
"Ł e di ribution of quadratic residues and non-residues".
In: *MṆhemṆika* . Pages – . DOI: 10.1112/S0025579300001157.

. Paul E and Alfréd R .
"Probabili ic methods in group theory".
In: *Journal d'Analyse MṆhémṆique* . . Pages – .
DOI: 10.1007/BF02806383.

. Nicolaas G. de B .
"On the number of positive integers $\leqslant x$ and free of prime fańors $> y$, II".
In: *KoninklŜke Nederlandse Akademie van W'nenschappen*. Proceedings, Series A . . Pages – .

. Je rey C. L and Andrew M. O .
"E eńive versions of the Chebotarev density theorem".
In: *Algebraic number Ŕelds:* L*-funňions and Galoś properties*.
Proceedings of a Symposium held at the University of Durham in .
Academic Press. Pages – .

. Richard S and Adi S .
"A $T = O(2^{n/2}), S = O(2^{n/4})$ algorithm for certain NP-complete problems".
In: *SIAM Journal of Computing* . . Pages – . DOI: 10.1137/0210033.

. Earl C , Paul E , and Carl P .
"On a problem of Oppenheim concerning 'fańorisatio numerorum'".
In: *Journal of Number Ńeory* . . Pages – .
DOI: 10.1016/0022-314X(83)90002-1.

. Martin S .
"A probabili ic fańorization algorithm with quadratic forms of negative

discriminant". In: *MṆhemṆics of CompuŪtion* . . Pages – .
DOI: 10.1090/S0025-5718-1987-0878705-X.

. Johannes B .
"A subexponential algorithm for the determination of class groups and regulators of algebraic number õelds". In: *Séminaire de Ń éorie des Nombres, Parś*.
Edited by Catherine G . Volume . Progress in Mathematics. Birkhäuser.
Pages – .

. David A. C .
Primes of ū e form $x^2 + ny^2$. John Wiley & Sons. ISBN: - - - .

. James L. H and Kevin S. M C .
"A rigorous subexponential algorithm for computation of class groups".
In: *Journal of ū e American MṆhemṆical Soci'ny* . . Pages – .
DOI: 10.2307/1990896.

. Eric B .
"Explicit bounds for primality te ing and related problems".
In: *MṆhemṆics of CompuŪtion* . . Pages – .
DOI: 10.1090/S0025-5718-1990-1023756-8.

. Jonathan P .
"Frobenius maps of abelian varieties and õnding roots of unity in õnite õelds".
In: *MṆhemṆics of CompuŪtion* . . Pages – .
DOI: 10.2307/2008445.

. Hendrik W. L and Carl P .
"A rigorous time bound for faǹoring integers".
In: *Journal of ū e American MṆhemṆical Soci'ny* . . Pages – .
DOI: 10.1090/S0894-0347-1992-1137100-0.

. Henri C .
A course in compuŪtional algebraic number ū eory. Volume .
Graduate Texts in Mathematics. Springer. ISBN: - - - .

. Don C .
"Modiõcations to the number õeld sieve".
In: *Journal of Cryptology* . . Pages – . DOI: 10.1007/BF00198464.

. Russel I and Moni N .
"E cient cryptographic schemes provably as secure as subset sum".
In: *Journal of Cryptology* . . Pages – . DOI: 10.1109/SFCS.1989.63484.

. David R. K .
“Endomorphism rings of elliptic curves over ŏnite ŏelds”.
PhD thesis. University of California at Berkeley.
URL: http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf.

. Vińor S .
“Lower bounds for discrete logarithms and related problems”.
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Walter F .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/3-540-69053-0_18.

. Leonard M. A and Ming-Deh H .
“Counting points on curves and abelian varieties over ŏnite ŏelds”.
In: *Journal of Symbolic CompuŪtion* . . Pages – .
DOI: 10.1006/jsco.2001.0470.

. Andrew G .
“Smooth numbers: computational number theory and beyond”.
In: *Algoriūmic Number Ńeory: LŅtices, Number Fields, Curves and Cryptography*.
Edited by Joseph P. B and Peter S . Volume .
Mathematical Sciences Research In itute Publications. Cambridge University Press.
Pages – .

. Gaetan B and Andrew V. S .
“Computing the endomorphism ring of an ordinary elliptic curve over a ŏnite ŏeld”.
In: *Journal of Number Ńeory* . . Edited by Neal K and Vińor S. M .
Special Issue on Elliptic Curve Cryptography. Pages – .
DOI: 10.1016/j.jnt.2009.11.003.

. Kir en E and Kri in E. L .
“A CRT algorithm for con ruńing genus curves over ŏnite ŏelds”.
In: *Ariūm'nic, Geom'nry and Coding Ńeory — AGCT '* .
Edited by François R and Serge V . Volume . Séminaires et Congrès.
Société Mathématique de France. Pages – .

. David J , Stephen D. M , and Ramarathnam V .
“Expander graphs based on GRH with an application to elliptic curve cryptography”.
In: *Journal of Number Ńeory* . . Pages – .
DOI: 10.1016/j.jnt.2008.11.006.

. Nick H -G and Antoine J .
“New generic algorithms for hard knapsacks”.
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Henri G .

Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-642-13190-5_12.

. Sorina I and Antoine J .
"Pairing the volcano". In: *Algoriūmic Number Ńeory — ANTS-IX*.
Edited by Guillaume H , François M , and Emmanuel T .
Volume . Leńure Notes in Computer Science. Springer. Pages – .
DOI: 10.1007/978-3-642-14518-6_18.

. Gaetan B .
Computing endomorphśm rings of eŝiptic curves under ūe GRH.
arXiv.org: 1101.4323.

. Gaetan B and Andrew V. S .
"A low-memory algorithm for ŏnding short produń representations in ŏnite groups".
In: *Designs, Codes and Cryptography*. To appear.
DOI: 10.1007/s10623-011-9527-8.

ẏolarized Ʊ ’nhod

To make pra ńical use of our subexponential method for computing endomorphism rings of ordinary abelian varieties in dimension higher than one, polarizations mu be taken into account. Ł is requires certain modiŏcations to be made on our framework, algorithms, and implementation, which we now describe. We also need to rely on more unproven assumptions.

We focus on the case of Jacobian varieties of genus-two hyperelliptic curves, since the availability of certain computational tools (such as the method of M ( )) is limited in higher dimensions. Notwith anding those issues, we believe mo of the di erences that higher-dimensional varieties have in comparison to elliptic curves are addressed here.

Ł e modiŏed algorithm will be presented before the computation of isogenies; we then give a ńual computation results and ŏnally discuss vertical isogenies.

VIII.1 Algorithm

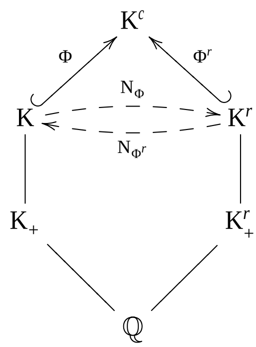
C M F

We art by recalling some of the theory on which our approach relies.

Let $\mathscr{A}$ be a simple ordinary principally polarized abelian variety of dimension g deŏned over a ŏnite ŏeld. We assume that an embedding of its complex multiplication ŏeld $K = \mathbb{Q}(\pi)$ into $\mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}$ has been ŏxed, which is equivalent to ŏxing a type Φ on K.

As we saw in Chapter , ideals of the reŒex ŏeld K^r a ń on isomorphism classes of principally polarized abelian varieties $\mathscr{A}$ via the reŒex type norm (see Figure):

$$\mathfrak{r} \in \mathfrak{I}(K^r) : \mathbb{C}^g/\Phi(\mathfrak{a}), E_\Phi^\xi \longmapsto \mathbb{C}^g/\Phi\left(N_{\Phi^r}(\mathfrak{r})^{-1}\mathfrak{a}\right), E_\Phi^{N_{K^r/\mathbb{Q}}(\ )\xi}$$



F . Complex multiplication ŏeld extensions and their reŒex counterparts.

Ł e main di erence to the preceding chapter is that, when the dimension g is two or more, this ańion only gives certain elements of the polarized class group $\mathfrak{C}(\mathcal{O}_K)$; in other words, it describes certain, but not all, isogenies. Ł erefore, a rigorous analysis of our algorithm in this setting would be much more involved than in the utopian case where polarizations were disregarded: one would need to assert the exi ence of short relations arising via the reŒex type norm, which we see no simple way of doing. Ł erefore we assume:

Assumption viii.1.1. *Under ŭe map* $(\mathfrak{a}, \ell) \mapsto (\mathfrak{a}\mathcal{O}, \ell)$*, composed to ŭe right wiŭ ŭe reŗex type norm, ideals of ŭe ring of integers of ŭe reŗex Ŕeld aň faiŭfuŝy on ŭe s'n* $\mathrm{AV}_{\mathcal{O}}(k)$ *of principaŝy polarized abelian vari'nies wiŭ endomorphśm* $\mathcal{O}$ *over ŭe bńe Ŕeld k.*

Ł is comes on top of the generalized Riemann hypothesis, and Assumptions . . , . . , and . . , which ate re ŕ eńively:

– Orders $\mathcal{O} \subset \mathcal{O}'$ for which the above ańion is identical have bounded index $[\mathcal{O}' : \mathcal{O}]$.

– Ł e method of E and L ( ) computes $\mathrm{End}(\mathscr{A})_\ell$ in $\ell^{O(1)}$ time.

– Ł e norms of reduced ideals are as smooth as random integers.

Ł e ŏr assumption is a helpful heuri ic, the third comes from B ( ), and the second deliberately rules out cases where the local lattice of orders is deep. Ł ey were all largely veriŏed in the range of prańical problems that we considered, except in certain rare cases.

We also require the ability to draw points at random from $\mathscr{A}$ and other varieties of its isogeny class; for $g = 2$, this is always the case using Weier rass forms, to which any variety can be put using the method of M ( ). Ł erefore we additionally impose $g = 2$.

Under all these assumptions, the expe ńed runtime is, as we mentioned before:

$$\mathrm{L}(q)^{g\sqrt{3g}/2+o(1)}$$

O

Let $\mathscr{A}$ be the input polarized abelian variety, given as the Jacobian variety of a hyperelliptic curve $\mathscr{C}$ deőned over the őnite őeld with q elements. Fir , we compute the chara ńeri ic polynomial χ_π of its Frobenius endomorphism π, which the algorithm of P ( ) does in polynomial time. In pra ńice, we relied on the point-counting routines of the M ( ) computational algebra sy em, which use the techniques of G and H ( ); larger base őelds could be reached using the ate-of-the-art implementation and optimizations of G and S ( ).

In the lattice of orders, we őnd $\mathrm{End}(\mathscr{A})$ from below using the following algorithm from Chapter — we also proposed a way of őnding $\mathrm{End}(\mathscr{A})$ from above which is suited to varieties con ru ńed via the complex multiplication method (rather than at random, as below); however, at the time of this writing, only abelian varieties with maximal endomorphism rings can be generated in this way, except in the one-dimensional case.

Algorithm viii.1.2.

I : *A simple ordinary principaŝy polarized abelian variʼny $\mathscr{A}$ over a Ŕnite Ŕeld $\mathbb{F}_q$.*

O : *An order śomorphic to its endomorphśm ring.*

. *Compute ūe FrobeniŬ polynomial $\chi_\pi(x)$ of $\mathscr{A}$.*

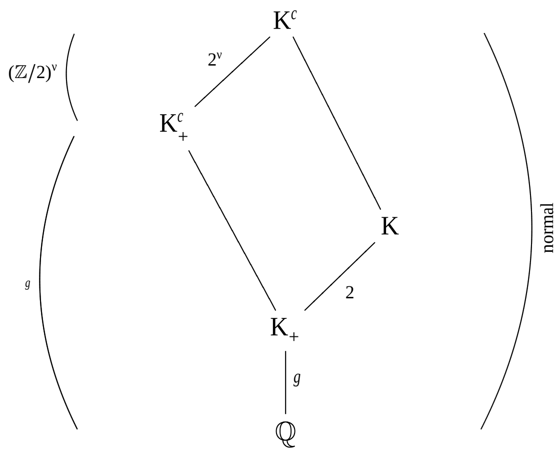
. *Faňor ūe dścriminant Δ and con ruň ūe order $\mathscr{O}' = \mathbb{Z}[\pi,\bar{\pi}]$.*

. *For orders $\mathscr{O}$ direňly abol·e $\mathscr{O}'$:*

. *If $\mathscr{O} \subset \mathrm{End}(\mathscr{A})$ sʼn $\mathscr{O}' \leftarrow \mathscr{O}$ and go to Step .*

. *Rʼnurn $\mathscr{O}'$.*

To determine whether a ŕ eciőc order $\mathscr{O}$ is contained in the endomorphism ring of $\mathscr{A}$, we sele ńed several relations of it (typically logarithmically many in the number of orders of containing $\mathbb{Z}[\pi,\bar{\pi}]$, although doubly logarithmically many should theoretically be enough), and checked whether these relations hold in the isogeny graph. Ł e latter ep requires us to evaluate isogenies and is the bottleneck of the whole algorithm.



F . Galois groups of the complex multiplication ŏelds tower.

D S P

To udy the ŕ litting pattern of rational primes ℓ in complex multiplications ŏeld K, let us ŏr present the setting to which Ł eorem . . can be applied. We are mo ly intere ed in the ŕ litting of primes in the reŒex ŏeld K^r of the ŏeld by which our variety has complex multiplication, but it makes no di erence for this analysis.

Denote by K any complex multiplication ŏeld of degree $2g$, and write K^c for its normal closure. Similarly, denote by K_+^c the normal closure of its totally real subŏeld K_+. Ł is gives a tower of ŏelds as di ŕ layed on Figure .

In the typical case of non-Galois number ŏelds, D ( ) e ablished the isomorphisms $\mathrm{Gal}(K_+^c/\mathbb{Q}) \simeq \mathfrak{S}_g$ and $\mathrm{Gal}(K^c/K_+^c) \simeq (\mathbb{Z}/2)^\nu$ for some integer ν in $\{1, \dots, g\}$, and described the ań ion of the former on the latter so that we have an explicit description of the Galois ruń ure of $K^c/\mathbb{Q}$ as

$$\mathrm{Gal}(K^c/\mathbb{Q}) \simeq (\mathbb{Z}/2)^\nu \rtimes \mathfrak{S}_g.$$

Note that, when a principally polarized abelian variety $\mathscr{A}$ is absolutely simple (as we assume here), its complex multiplication ŏeld K is primitive and we have $\nu = g$. In dimension $g = 2$, the Galois group of $K^c/\mathbb{Q}$ is then isomorphic to the dihedral group $D_4 = \mathbb{Z}/4 \rtimes \mathbb{Z}/2$, and we obtain the densities of Figure as a consequence.

	(1,1,1,1)	(1,1,2)	(1,3)	(2,2)	(4)
	1/8	1/4	0	3/8	1/4

F . Density of rational primes p ŕ litting in a ŏxed non-normal quartic complex multiplication ŏeld as $\prod \mathfrak{p}_i$ with pattern $(\mathrm{N}(\mathfrak{p}_i))$.

F R

Finding relations is a quite andard ep. We have already mentioned that the computability of the algebraic ru ńures we deal with has been well udied. Here, in fa ń, we do not even need to compute the polarized class group of Shimura: since we are re ri ńed to using isogenies which arise under the reŒex type norm, we are in fa ń seeking for relations of the class group of $\mathcal{O}^r$. To obtain a subexponential asymptotic runtime, we use the generalization of the algorithm of H and M C ( ) by B ( ).

Remark. As a pra ńical optimization, since evaluating isogenies is so co ly, more time may be dedicated to ŏnding a shorter relation. For the range of input sizes we considered, it was well worth using the exponential algorithm below which is essentially a baby- ep giant- ep approach borrowing ideas of C , D D , and O ( ) for the e e ńive ideal arithmetic; it ŏnds the shorte possible relation, therefore improving greatly the ŕ eed of the isogeny ep, and reducing the overall runtime.

Notation. Recall that $b_x(f(x))$ may denote any fun ńion satisfying the inequalities $f(x) < b_x(f(x)) < f(x)^{1+o(1)}$ and computable in essentially linear time in $f(x)$.

Algorithm viii.1.3.

I : *An order $\mathcal{O}$ of dścriminant Δ in a number Ŕeld* K.

O : *RelŅions of $\mathcal{O}$.*

. *L'n $\mathfrak{B}$ consśt of aŝ prime ideals wi ū norm up to $b_\Delta(12\log^2|\Delta|)$.*
. *CreŅe a h ńh Ūble* H.
. *Compute ū e produ ň $\mathfrak{a}$ of a random subs'n of $\mathfrak{B}$.*
. *L'n $\mathfrak{b}$ be an LLL redu ňion of $\mathfrak{a}$.*
. *If* H *h ń an entry for $\mathfrak{b}$, output $\mathrm{H}(\mathfrak{b}) - \mathfrak{a}$.*
. *O ū erwśe, s'n $\mathrm{H}(\mathfrak{b}) \leftarrow \mathfrak{a}$ and go back to Step .*

Step means that $\mathfrak{b}$ is the ideal generated over $\mathcal{O}$ by an LLL basis of the ideal $\mathfrak{a}$, where the LLL redu ńion can be computed along any dire ńion as described by C , D D , and O ( ). Ł e ideals $\mathfrak{b}$ a ń as class representatives and we do not require that they are unique: it is enough that they are small so that, by the pigeonhole principle, classes are identified after a few more trials than what would be required otherwise.

The use of such an exponential algorithm also has an additional benefit: it allows us to choose which primes we want to include in our relations, which subexponential smoothness-based methods do not permit.

For instance, we can choose to only use primes which split as $\mathfrak{p}\bar{\mathfrak{p}}$, hence allowing for a cardinality-based approach and sparing the need to compute the characteristic polynomial

Since each has order ℓ^g, is rational over the base ŏeld, and contains the neutral element, they are all deŏned over an extension of degree $e'(\ell)$ at mo $\ell^g - 1$. We will thus simply enumerate all such subgroups of the ℓ-torsion group of $\mathscr{A}(\mathbb{F}_{q^{e'(\ell)}})$ and then ŏnd which one corre ŕ onds to the ideal $\mathfrak{a}$ as mentioned above.

To ŏnd these, ŏr compute a basis of the ℓ-Sylow subgroup of $\mathscr{A}$ over the extension ŏeld, which we denote by

$$\mathscr{A}\left(\mathbb{F}_{q^{e'(\ell)}}\right)[\ell^\infty];$$

for this, we use the method of C ( ) which we have discussed before: it amounts to taking random points of $\mathscr{A}$ (this is easy, for in ance, when it has a Weier rass form), multiplying them by the cofańor of ℓ^∞ in $\#\mathscr{A}(\mathbb{F}_{q^{e'(\ell)}})$, and “liŔing” these points along each other until a basis of the ℓ-torsion group is obtained.

We then derive a sympleńic basis of $\mathscr{A}(\mathbb{F}_{q^{e'(\ell)}})[\ell]$ for the Weil pairing. For simplicity, ŏx an ℓ^{th} root of unity and consider the problem additively under the corre ŕ onding logarithm $\log : \mu_\ell(\mathbb{C}) \to \mathbb{Z}/\ell$. On the basis we are looking for, (the logarithm of) the Weil pairing is given by the matrix

$$\begin{pmatrix} 0 & \mathrm{I}_g \\ -\mathrm{I}_g & 0 \end{pmatrix}.$$

To obtain such a basis $(e_1, \dots, e_g, f_1, \dots, f_g)$ satisfying

$$\begin{cases} \log \Psi_{\mathrm{Weil}}(e_i, f_j) = \delta_{ij} \\ \log \Psi_{\mathrm{Weil}}(e_i, e_j) = 0 \\ \log \Psi_{\mathrm{Weil}}(f_i, f_j) = 0 \end{cases}$$

we use an elementary, orthogonalization-like algorithm, similar to the classical algorithm for computing Smith normal forms.

Ł is basis allows us to enumerate all sympleńic subgroups easily and, among these, we seleń those that are rational, that is, able under the Frobenius endomorphism, and ŏnd which is ańed upon with charańeri ic polynomial u (given by the ideal $\mathfrak{a}$).

Note that when ℓ is congruent to one modulo four, ŏnding random points of $\mathscr{A}$ is fa er by a fańor of two since computing the square root of the Weier rass polynomial evaluated at x in order to get the y-coordinate simply amounts to a modular exponentiation.

M T C

Recall that if $\mathscr{A} \simeq \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ is a complex torus with period matrix Ω in $\mathbb{H}^g$, then the set of theta functions

$$\Theta_{a,b}^{\mathscr{A}} : z \in \mathbb{C}^g \longmapsto \sum_{(u+a)\in\mathbb{Z}^g} \exp\left(i\pi\left(\tfrac{1}{n}\hat{u}\Omega u + 2\hat{u}\left(z+b\right)\right)\right),$$

where $a = 0$ and b is a vector of $\frac{1}{n}(\mathbb{Z}/n)^g$, forms the *theta coordinate system of level n*. It is a coordinate system for abelian varieties (and also incorporates information about the n-torsion), but can represent points of such varieties too. It has an algebraic counterpart which is applicable to varieties defined over finite fields.

The points P of the kernel of the isogeny we wish to evaluate, as output by the method of C ( ), are expressed in Mumford coordinate on a Weierstrass model for the hyperelliptic curve $\mathscr{C} : y^2 = f(x)$ of which $\mathscr{A}$ is the Jacobian variety. As a first step towards mapping these points to theta coordinates, we extend the base field so as to make f split completely; then, by a homographic transformation (also known as Möbius transformation) of the x coordinate, we derive its Rosenhain normal form

$$y^2 = x(x-1)\prod_{i=1}^{2g-1}(x - a_i)$$

which might require working in an extension of the base field.

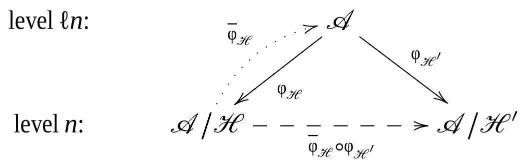
The formulas of T ( ), then give theta coordinates of level two or four corresponding to the variety $\mathscr{A} = \mathrm{Jac}(\mathscr{C})$. In order to map points from Mumford representation to theta coordinates, we need equations derived by W ( ).

Note that theta coordinates of level two actually represent the Kummer surface of an abelian variety, that is, identify a variety $\mathscr{A} = \mathrm{Jac}(\mathscr{C} : y^2 = f(x))$ with its twist $\mathrm{Jac}(\widetilde{\mathscr{C}} : \omega y^2 = f(x))$ where ω is a non-quadratic residue in the base field. This is not too much of an issue for us since the isogeny class of $\mathscr{A}$ is identified by the characteristic polynomial of its Frobenius endomorphism, so there is no ambiguity on which of an abelian variety $\mathscr{B}$ or its twist an isogeny φ with domain $\mathscr{A}$ maps to.

However, for a cleaner approach, we prefer to use level four theta coordinates which identify the variety $\mathscr{A}$ uniquely; this comes at the expense of speed, but the slow down is minor, especially as finding the ℓ-torsion remains the overall bottleneck.

I L C

L and R ( ) described isogenies as projections from higher-level theta coordinate systems to lower-level ones; they also described the associated machinery (addi-



F . Evaluating isogenies of type $(\mathbb{Z}/\ell^2)^g$ via two theta level changes.

tion laws, etc.) required to make e eńive use of this result. Before discussing how it applies to our setting, let us brieŒy recall their result.

Theorem VIII.2.1. *L'n $\mathscr{H}$ be a subgroup śomorphic to $(\mathbb{Z}/\ell)^g$ of an abelian vari'ny $\mathscr{A}$ of dimension g, and l'n n be any integer coprime to ℓ. Ńe ū'na funňions of level n on $\mathscr{A}/\mathscr{H}$ are a subs'n of ūe ū'na funňions of level ℓn on $\mathscr{A}$.*

Ł is introduces an change of level; to address this, L and R ( ) noted that subsets of the Fourier transform of theta funńions of level ℓn on $\mathscr{A}$ corre ŕ ond to theta funńions of level n for abelian varieties obtained by dual isogenies of degree ℓ; this allows them to compute isogenies of type $(\mathbb{Z}/\ell^2)^g$ between abelian varieties expressed by level-n theta funńions; see Figure .

Our framework for computing endomorphism rings can be adapted to this setting: relations can be con rained to only involve squares of ideals, so that the associated isogenies are all of type $(\mathbb{Z}/\ell^2)^g$. However, this implies loosing all the information regarding the 2-torsion of the reŒex class group $\mathfrak{C}(\mathscr{O}^r)$. C and L ( ) showed that class groups typically have a large 2-torsion subgroup, so it is not likely that all pairs of class groups that are identical up to 2-torsion can be di inguished e ciently using the local method of E - and L ( ).

C and R ( ) then derived from earlier work of K ( ) and K ( ) formulas which allow to map points from level-ℓn theta coordinates to level-n theta coordinates, avoiding the need to evaluate an additional isogeny. Ł ey apply these formulas to evaluating isogenies of type $(\mathbb{Z}/\ell)^g$ between abelian varieties expressed in theta coordinates of level n.

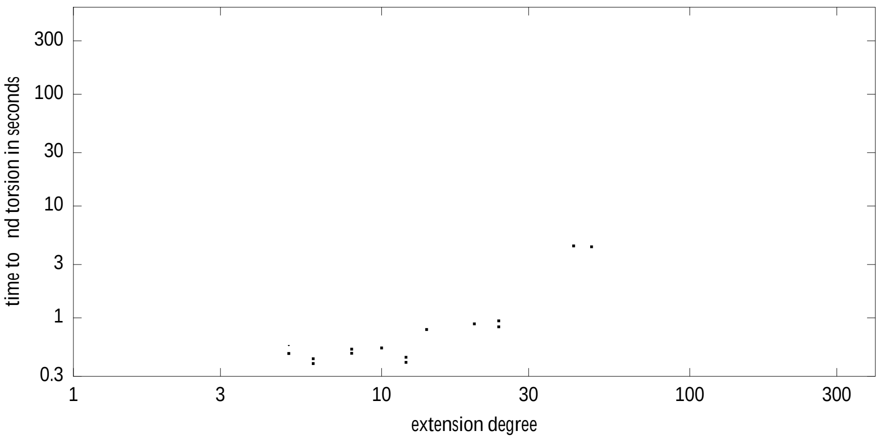
M I

In order to determine whether a relation holds in the isogeny graph of an abelian variety (to eventually determine its endomorphism ring), we need to compose many isogenies of type $(\mathbb{Z}/\ell)^g$ for various primes ℓ. We have explained how to compute an isogeny $\mathscr{A} \to \mathscr{A}'$ of prescribed kernel where $\mathscr{A}$ is given in Weier rass form and $\mathscr{A}'$ is given as theta coordinates of level n. To iterate this con ruńion, it remains to explain how we can obtain a Weier rass equation for $\mathscr{A}'$.

In fań, this can be done elementarily by inverting the formulas of T ( ). However, the theta coordinates of $\mathscr{A}$ that we used in the isogeny computation are deŏned over a large extension of the base ŏeld which contains the roots of the Weier rass polynomial of the curve, certain n-torsion points (recall that $n = 2$ or 4) and certain ℓ-torsion points; the theta coordinates of $\mathscr{A}'$, and therefore also its Weier rass equation that we derive, are consequently deŏned over that large extension.

When we know that $\mathscr{A}'$ is ańually deŏned over the base ŏeld (for in ance, because the chosen isogeny is rational), we recover a rational Weier rass equation by ŏr computing the absolute invariants of $\mathscr{A}'$ and then using the algorithm of M ( ) to recon ruń a curve $\mathscr{C}'$ whose Jacobian variety $\mathrm{Jac}(\mathscr{C}')$ is $\mathscr{A}'$.

As an optimization to the algorithm for ŏnding the ℓ-torsion of the el of a uķ p



F . Average time for ŏnding the ℓ-torsion of an abelian variety of dimension two over the ŏeld with 251 elements, for $\ell \in \{2,3,5,7,11,13,17,19\}$ and all possible $e'(\ell)$.

VIII.3 Practical Computations

All computations were realized using the library of B., C , and R ( ).

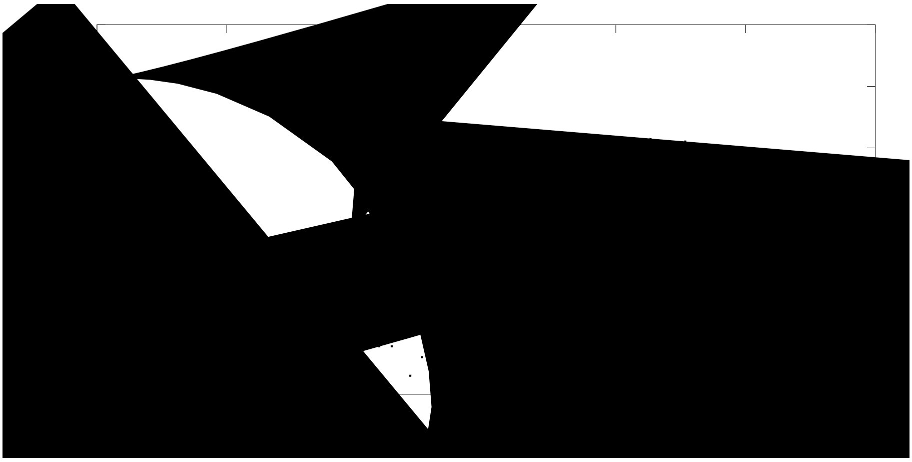
F T

Ł e bottleneck of our algorithm is typically to ŏnd a basis for the ℓ-torsion subgroup of $\mathscr{A}$ over an extension where all points of rational subgroups of type $(\mathbb{Z}/\ell)^g$ are deŏned. Ł e co is twofold:

- computing over an extension of degree $e'(\ell)$ of the base ŏeld;
- multiplying points by the cofańor of ℓ^∞ in $\#\mathscr{A}(\mathbb{F}_{q^{e'(\ell)}}) \sim q^{ge'(\ell)}$.

In the wor case, $e'(\ell)$ can be as large as $\ell^g - 1$, so that the overall complexity is $\ell^{2g+o(1)}$ disregarding logarithmic fańors in q, which quickly becomes prohibitive. As argued before, exponential methods for ŏnding relations o er the advantage that ŕ eciŏc primes ℓ can be chosen for which $e'(\ell)$ is small.

Figure shows the time it takes, on average for 10 randomly chosen abelian surfaces deŏned over the ŏeld $\mathbb{F}_{251}$, to compute the ℓ-torsion over an extension of degree e'.



F . Number of iterations the latter algorithm requires before ŏnding a relation in a quartic complex multiplication ŏeld with certain class number (also known as Picard number). Ł e lines plot $y = x$ and $y = \sqrt{x}$.

As can be expeńed, this runtime is slightly more than linear in the extension degree, and does not highly depend on ℓ. However, we observe that for a prescribed ℓ the torsion of varieties with a certain $e'(\ell)$ is sometimes fa er than those of varieties with a smaller $e'(\ell)$; this is likely due to the internal representation of the extensions as tower ŏelds in M ( ), and also possibly to ŕ ecial features of the varieties.

F R

We implemented in M ( ) the simple baby- ep giant- ep method that we described above and found that it behaves well: in mo cases, the number of iterations required to ŏnd a collision is not so far from the $\sqrt{h}$ (where h denotes the class number) that would be expeńed if each ideal class contained a unique reduced ideal.

Figure shows the number of iterations our algorithm goes through before the ŏr relation is found; we use the order $\mathcal{O} = \mathbb{Z}[\pi, \overline{\pi}]$ for a thousand Jacobian varieties of random hyperelliptic curves of genus two. Ł e class number diŕ layed is ańually the approximation $\sqrt{|\Delta|}/R$ given by the Brauer–Siegel theorem.

We observe that the iteration count lies somewhere in between $\sqrt{h}$ and h. Although in some cases this number went slightly above the class number, the runtime was always acceptable: it was never more than two seconds when the class number was less than a thousand, and always less than a hundred seconds in our range of parameters.

B -C S

Let us first present an example where our algorithm performs much better than all other alternatives. The *conductor gap* is the large prime factor of the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$; here, we consider a case of large conductor gap, which makes the method of E and L ( ) impractical. Unfortunately, we were unable to compare our method with that of W ( ), as we did not have an implementation of the latter at our disposal.

To find an abelian variety with a large conductor gap, we generated genus-two hyperelliptic curves at random until one whose Jacobian variety has the desired property was found; we obtained the hyperelliptic curve with equation

$$y^2 = 80742x^5 + 56078x^4 + 76952x^3 + 134685x^2 + 60828x + 119537$$

defined over the field with 161983 elements; let $\mathscr{A}$ denote its Jacobian variety. The characteristic polynomial of its Frobenius endomorphism is

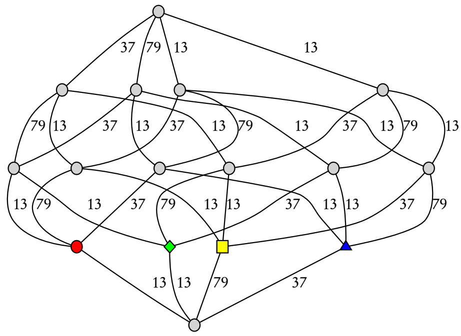
$$z^4 - 144z^3 + 10368z^2 - 144 \cdot 161983z + 161983^2$$

and it defines a quartic complex multiplication field $K = \mathbb{Q}(\pi)$ in which the ring of integers contains the minimal order $\mathbb{Z}[\pi, \overline{\pi}]$ with prime index $\ell = 156799$.

Since the full ℓ-torsion of $\mathscr{A}$ lies in an extension of degree $e(\ell) = 78399$, it is challenging to try to compute $\mathrm{End}(\mathscr{A})$ using the method of E and L ( ).

However, the Picard group of $\mathfrak{M} = \mathcal{O}_K$ has order 460; this is not surprising as a large part of $\Delta = \mathrm{disc}(\pi)$ contributes to the conductor gap so little is left to build up $\mathrm{disc}(K)$. It is thus easy to find relations in the associated polarized class group $\mathfrak{C}(\mathcal{O}_K)$. For instance, one easily verifies that the element $(\mathfrak{a}, 3)$ has order 115, where $\mathfrak{a}$ can be any ideal of norm 9 (there are just two such elements, inverses of each others).

The action of $(\mathfrak{a}, 3)^{115}$ on $\mathscr{A}$ is computed easily, as the 3-torsion of $\mathscr{A}$ lives



F . Lattice of orders with $\mathscr{O}_K$ on top and $\mathbb{Z}[\pi,\overline{\pi}]$ at the bottom; lines indicate that the order below is contained in the order above with index the label right o the line.

W -C S

Now let us consider an abelian variety that is expeńedly suited to the method of E - and L ( ), namely, one for which the conduńor gap $[\mathscr{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ is short. We take the Jacobian variety $\mathscr{A}$ of the hyperelliptic curve

$$y^2 = 2987x^5 + 1680x^4 + 3443x^3 + 1918x^2 + 2983x + 489$$

deŏned over the ŏeld with 3499 elements. Ł e charańeri ic polynomial of π is

$$z^4 + 48z^3 + 1152z^2 + 48 \cdot 3499z + 3499^2$$

and we ŏnd that there are 2^4 orders containing (or equal to) $\mathbb{Z}[\pi,\overline{\pi}]$; their indices in the maximal order divide $13^2 \cdot 37 \cdot 79$ as di ŕ layed on Figure .

We use $\alpha_\ell = (\mathfrak{a}_\ell, \ell) \in \mathfrak{C}$ for $\ell \in \{3,5,7\}$ where $\mathfrak{a}_\ell$ is an arbitrary ideal of norm ℓ^2; the full ℓ-torsion is deŏned over an extension of degree 8, 24, and 24, re ŕ eńively, so it takes on average 1, 3.5, and 5.5 seconds to evaluate one ℓ-isogeny.

We used the relation $\alpha_3^5\alpha_7^7 = 1$ for the yellow square order, $\alpha_5^{10} = 1$ for the blue triangle order, and $\alpha_3^2\alpha_5^{16}\alpha_7^{-2} = 1$ for both the red circle and green diamond order. Checking these relations in the isogeny graph took only slightly more than two minutes, and since none was found to hold, our algorithm returned that $\mathrm{End}(\mathscr{A}) = \mathbb{Z}[\pi,\overline{\pi}]$.

Even in this case, which would *a priori* favor the method of E and L ( ) (the full 37 and 79-torsion are deŏned over extensions of degree 1332 and 948, re-ŕ eńively), our algorithm performs well while ill leaving some room for improvement.

VIII.4 Isogeny Volcanoes

Let us now ŏx a prime ℓ and udy the ruńure of the conneńed component of the graph of isogenies of type $(\mathbb{Z}/\ell)^g$ containing a prescribed principally polarized simple ordinary abelian variety $\mathscr{A}$ deŏned over some ŏnite ŏeld.

G S

K ( ) and later F Ž and M ( ) depińed the ruńure of such graphs in dimension one as volcanoes, containing a *crŅer* formed by varieties whose endomorphism ring is locally maximal. Horizontal isogenies arrange these varieties in a (possibly degenerated) circle, and from each vertex on it hang complete ℓ-ary trees; their number and depth are entirely determined by ℓ and the isogeny class.

In dimension two or more, mo ŕeciŏc details are lo , but the general ruńure remains the same; mo important for our algorithms is that craters are ill Cayley graphs.

Let $G = \langle V, E \rangle$ be such an isogeny graph: vertices V correŕond to abelian varieties and edges E (a symmetric subset of V^2) to isogenies of type $(\mathbb{Z}/\ell)^g$ between them. We art by partitioning G into *layers* $G_{\mathscr{O}}$ for each order $\mathscr{O}$ above $\mathbb{Z}[\pi, \overline{\pi}]$: each layer contains the vertices whose associated varieties have an endomorphism ring isomorphic to $\mathscr{O}$.

Note that, in a conneńed component, certain layers can be empty as not all isogenous varieties might be reachable by sequences of isogenies of type $(\mathbb{Z}/\ell)^g$. We say that a layer $G_{\mathscr{O}}$ is maximal when there is no non-empty $G_{\mathscr{O}'}$ with $\mathscr{O} \subsetneq \mathscr{O}'$; typically, this means that when $G_{\mathscr{O}_K}$ is non-empty, it is the unique maximal layer.

Our observations of isogeny volcanoes will be ŕlit in three parts:

- the *core*: the union of maximal layers and their horizontal isogenies;
- the *branches*: the vertical isogenies;
- the *co·ering*: the horizontal isogenies in non-maximal layers.

OŔen, the graph has the familiar pińure of a core, out of which branches hang, and there is no covering. However, we will see that unusual phenomenons can occur, such as part of the branches sub ituting to the core ruńure.

At any rate, we mu warn the reader that our description of branches (which are the key to under anding the relationship of ℓ-isogeny volcanoes and the ruńure of endomorphism rings locally at ℓ) will be short and qualitative, as this thesis focuses on using horizontal isogenies and does not pretend to add any insight on the ruńure of vertical isogenies.

C

Assume the core consi s of a single layer $G_{\mathcal{O}}$ (we will consider the case where there are two or more below).

At lea in the case that $\mathcal{O}$ is a maximal order, the theory of complex multiplication proves that the set of horizontal isogenies of type $(\mathbb{Z}/\ell)^g$ in $G_{\mathcal{O}}$ corre ŕ onds to a certain subgroup of $\mathfrak{C}(\mathcal{O})$ formed of ideals of norm ℓ^g. Ł erefore, the core is a Cayley graph. We shall denote by $C(X|Y)$ the Cayley graph of X in the free abelian group generated by X with relations Y.

When $g = 2$, the order $\mathcal{O}$ is quartic, and the possible unramiŏed ŕ litting patterns of a prime ℓ in $\mathcal{O}$ are $(1,1,1,1)$, $(1,1,2)$, $(1,3)$, $(2,2)$, and (4). Ł e third case never happens in complex multiplication ŏelds (it is incompatible with complex conjugation) and the latter is that of inert primes which ań trivially on the isogeny graph, so we disregard both.

In the second case where ℓ ŕ lits as $\mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}$ with $N(\mathfrak{q}) = \ell^2$ there are, in general, no ideals $\mathfrak{a}$ of norm ℓ^2 such that $\mathfrak{a}\overline{\mathfrak{a}}$ is principal, which means there are no corre ŕ onding elements in the polarized class group $\mathbb{C}(\mathcal{O})$ and no isogenies of type $(\mathbb{Z}/\ell)^g$.

In the fourth case where ℓ ŕ lits as $\mathfrak{p}\overline{\mathfrak{p}}$, both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ liŔ to $\mathfrak{C}(\mathcal{O})$ as $\alpha = (\mathfrak{p}, \ell)$ and $\beta = (\overline{\mathfrak{p}}, \ell)$. Ł e core of the isogeny graph $G_{\mathcal{O}}$ is then the Cayley graph $C(\alpha, \beta | \alpha\beta, \alpha^{\operatorname{ord}\alpha})$, where the orders implied are those of the corre ŕ onding ideals as elements of the Picard group. Ł is gives a cycle ru ńure as Figure di ŕ lays.

In the ŏr case where ℓ ŕ lits as $\mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}\overline{\mathfrak{q}}$, there are four ideals of norm ℓ^2 whose produ ń with their conjugate is principal, namely $\mathfrak{p}\overline{\mathfrak{q}}$, $\overline{\mathfrak{p}}\mathfrak{q}$, $\mathfrak{p}\mathfrak{q}$, and $\overline{\mathfrak{p}\mathfrak{q}}$; if we denote the corre ŕ onding elements of $\mathfrak{C}(\mathcal{O})$ by α, β, γ, and δ, we obtain that the core $G_{\mathcal{O}}$ is the Cayley graph $C(\alpha, \beta, \gamma, \delta | \alpha\beta, \gamma\delta, \alpha^{\operatorname{ord}\alpha}, \gamma^{\operatorname{ord}\gamma})$; this is a quadrangulation of a torus, as can be seen on Figure .

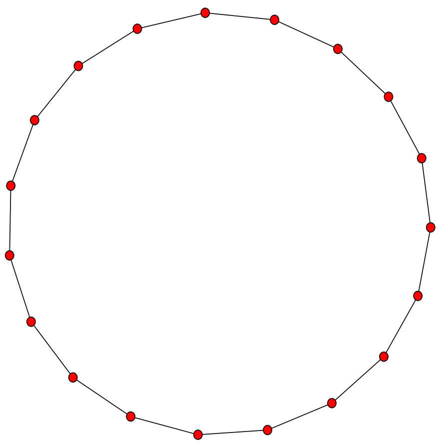
Although we were unable to compute a ńual isogeny graphs for $g > 2$, primes ℓ which completely ŕ lit as $\prod_{\in} \mathfrak{p}\overline{\mathfrak{p}}$ (with $\#\mathfrak{P} = g$) would then yield the 2^g elements of $\mathfrak{C}(\mathcal{O})$

$$\alpha_{\mathfrak{F}} = \left(\prod_{\in\mathfrak{F}} \mathfrak{p} \prod_{\notin\mathfrak{F}} \overline{\mathfrak{p}}, \ell^g \right)$$

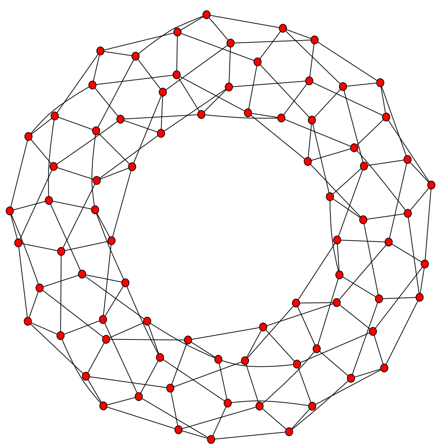
for each subset $\mathfrak{F}$ of $\mathfrak{P}$; the core would then be the Cayley graph

$$C\left(\left(\alpha_{\mathfrak{F}}\right)_{\mathfrak{F}\subset} \middle| \left(\prod_{\mathfrak{F}\in\mathfrak{G}} \alpha_{\mathfrak{F}} \right), \left(\alpha_{\mathfrak{F}}^{\operatorname{ord}\alpha_{\mathfrak{F}}} \right)_{\mathfrak{F}\subset} \right)$$

where the middle sequence ranges over all sets $\mathfrak{G}$ of subsets of $\mathfrak{P}$ which satisfy $\#\{\mathfrak{F} \in \mathfrak{G} : \mathfrak{p} \in \mathfrak{F}\} = \#\{\mathfrak{F} \in \mathfrak{G} : \mathfrak{p} \notin \mathfrak{F}\}$ for all $\mathfrak{p} \in \mathfrak{P}$. Topologically, this is the 1-skeleton of a simplicial complex homeomorphic to the g-torus (the produ ń of g copies of the 1- ŕ here).



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 3x^5 + 15x^4 + 11x^3 + 3x^2 + 11x + 12$ over the field with 19 elements.



F . Graph of isogenies of type $(\mathbb{Z}/7)^2$ containing the Jacobian variety of the curve $y^2 = 106x^6 + 83x^5 + 18x^4 + 52x^3 + 49x^2 + 11x + 41$ over the field with 109 elements.

Note that all the above holds over an algebraic closure, as not all isogenies corre ŕ onding to ideals of norm ℓ^g of $\mathfrak{C}(\mathscr{O})$ need to be rational.

B

Let us now consider two-dimensional ℓ-isogeny graphs in the case that $\ell\mathscr{O}_K$ is not coprime with the condu ńor of $\mathbb{Z}[\pi,\overline{\pi}]$. Although our algorithms for computing endomorphism rings prefer to avoid such situations, they are an intere ing application of our isogeny-computing library.

Each ŏgure contains two parts: the isogeny graph to the leŔ, and the lattice of orders to the right. Vertices of the isogeny graph are colored the same way as the endomorphism rings of the corre ŕ onding abelian varieties are in the lattice of orders.

Recall that in dimension one, a certain number of complete n-ary trees of uniform depth hang from each vertex of the core. Ł is might also happen in higher dimension, but other scenarios are possible. For in ance, B , G , and L ( ) observed in their Example . that trees hanging from the core might have di erent depths. Figure shows the same phenomenon in a more generic-looking graph. Ł is unbalance shows that not all isogenies of type $(\mathbb{Z}/\ell)^g$ need be uniformly rational.

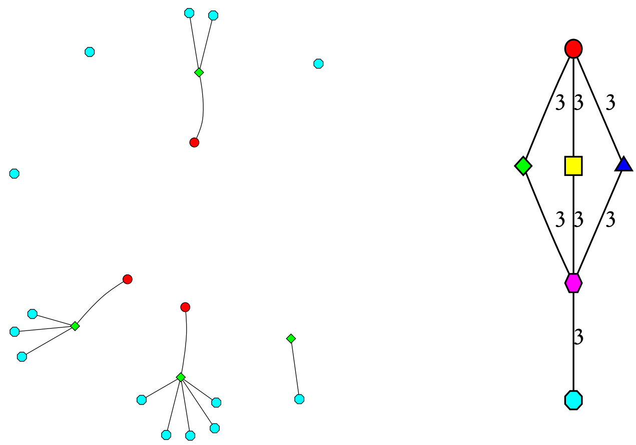
Figure also features isogeny of type $(\mathbb{Z}/\ell)^2$ between abelian varieties whose endomorphism rings have index ℓ^2 in each other, more ŕ eciŏcally between the green diamond and cyan o ńagon dots. Ł is can lead to di urbing graphs such as that of Figure where the endomorphism rings of varieties $(\mathbb{Z}/\ell)^2$-isogenous to varieties with maximal ones are the order of index 3^2, some order of index 3, but not the maximal order itself. Going from one variety with maximal endomorphism ring to another is however possible by ŏr going through a non-maximal one and then going up again.

In such cases, the partitioning of the features of isogeny graphs into a core, branches, and coverings is somewhat Œawed. Although with our deŏnition, the core of Figure consi s of both curves with red circle (maximal) and yellow square (index 3) endomorphism rings.

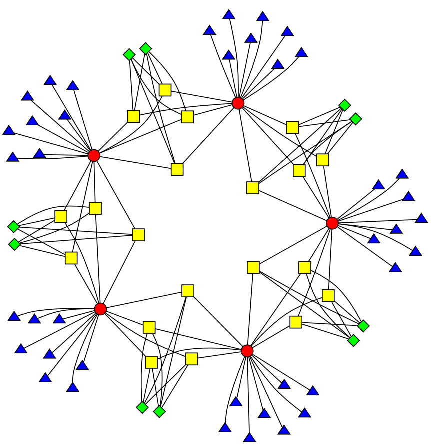
Ł is illu rates another ob ru ńion to climbing higher-dimensional volcanoes: sometimes, eps can only be climbed in pairs, which prevents one to fully enumerate an isogeny class ju by following isogenies of type $(\mathbb{Z}/\ell)^g$. Naturally, we see (hypothetical) isogenies of type $(\mathbb{Z}/\ell)$ as the answer to this problem.

C

We call covering the outer layers of the isogeny graph; those are horizontal isogenies arising as complex multiplication "residues." Although there are no ideals of norm ℓ^g in imaginary quadratic orders whose condu ńors are divisible by ℓ, this sometimes happen in higher



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 44x^6 + 36x^5 + 48x^4 + 29x^3 + 3x^2 + 44x + 34$ over the field with 61 elements.



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 13x^6 + 5x^5 + 37x^4 + 31x^3 + x^2 + 5x + 3$ over the field with 43 elements.

dimension; by complex multiplication, such ideals give rise to horizontal isogenies among varieties with non-maximal endomorphism rings.

Ł is was ŏr noted by B , G , and L ( ) in their Example . as an ob ruńion to a raightforward generalization of the endomorphism-ring-computing algorithm of K ( ). Indeed, the presence of cycles other than at the core, such as seen in Figures and , makes it di cult to obtain useful information about endomorphism rings by exploring the isogeny graph blindly.

In arbitrary dimension g, when a prime ℓ is completely ŕ lit in the maximal order, we have argued before that the core of the isogeny graph is the 1-skeleton of a g-torus. In orders $\mathscr{O}$ of conduńor not coprime to ℓ, since not all prime ideals of norm ℓ can be invertible (otherwise ℓ itself would be), there are at mo $g-1$ of them. Ł e con ruńion of the covering as a Cayley graph is then identical to the maximal case except for two di erences:

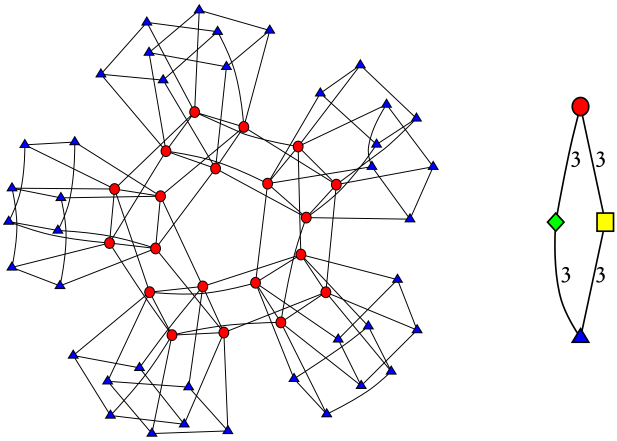
- $\mathfrak{P}$ now consi s of $g-1$ ideals at the mo ;
- its ańion on $G_{\mathscr{O}}$ need not be transitive.

Since we deŏned our isogeny graphs as being conneńed components, the subgraph of horizontal isogenies in the core was always conneńed (in this case where we assume that ℓ completely ŕ lits and that all elements of $\mathfrak{C}(\mathscr{O})$ of norm ℓ^g arise as rational isogenies); however, there is no reason for this to happen in the cover where we have a smaller $\mathfrak{P}$, which is the reason for the second di erence.

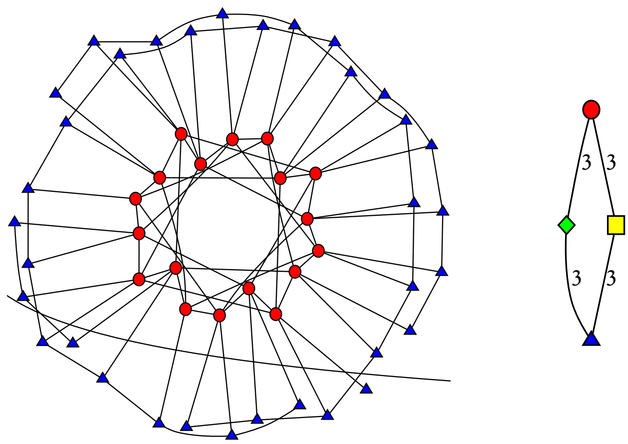
Ł e graph of horizontal isogenies of $G_{\mathscr{O}}$ therefore has the topological ruńure of several copies of the 1-skeleton of a simplicial complex homeomorphic to the $u_{\mathscr{O}}$-torus, for some integer $u_{\mathscr{O}} < g$. Obviously, the integer $u_{\mathscr{O}}$ is non-decreasing with re ŕ eń to the order $\mathscr{O}$ (for the inclusion order).

In the case $g = 2$, when the subgroup generated by the invertible ideals of norm ℓ^2 in $\mathfrak{C}(\mathscr{O})$ is small, we obtain an isogeny graph such as that of Figure . On the other hand, when it is large, its shape is similar to Figure .

To compute endomorphism rings, such ideals can be allowed in our relations as long as they are invertible in $\mathbb{Z}[\pi, \overline{\pi}]$. Although this has no e eń on the asymptotic complexity of our method, it provides a valuable prańical optimization: since computing isogenies is the bottleneck, not using *any* ideal of norm ℓ^g ju because *some* are not invertible would be a loss, e ŕ ecially if the full ℓ-torsion conveniently lies in a small extension of the base ŏeld.



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 8x^6 + 3x^5 + 7x^4 + 5x^3 + 12x^2 + 5x + 5$ over the field with 23 elements.



F . Graph of isogenies of type $(\mathbb{Z}/3)^2$ containing the Jacobian variety of the curve $y^2 = 10x^6 + 18x^5 + 24x^4 + 3x^3 + 33x^2 + 26x + 25$ over the field with 41 elements.

References

. Friedrich J. R .
“Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes”.
In: *Comptes RendŬ de l’Académie des Sciences de Parś* . Pages – .

. Carl J. T .
“Beitrag zur Be immung von $\vartheta(0, 0, \dots, 0)$ durch die Klassenmoduln algebraischer Funńionen”.
In: *Journal für die reine und angewandte MŅhemŅik* . . Pages – .
DOI: 10.1515/crll.1870.71.201.

. Jacques V .
“Isogénies entre courbes elliptiques”.
In: *Comptes RendŬ de l’Académie des Sciences de Parś*. A . Pages – .

. Shoki K .
“ Ł eta relations and projeńive normality of abelian varieties”.
In: *American Journal of MŅhemŅics* . . Pages – .
DOI: 10.2307/2374034.

. Henri C and Hendrik W. L .
“Heuri ics on class groups of number õelds”.
In: *Number Ń eory NoordwŜkerhout — Journées Ariū métiques ’* .
Edited by Hendrik J . Volume . Leńure Notes in Mathematics. Springer.
Pages – . DOI: 10.1007/BFb0099440.

. Bruce D .
“ Ł e ruńure of Galois groups of CM-õelds”.
In: *Transaňions of ū e American MŅhemŅical Soci’ny* . . Pages – .
DOI: 10.1090/S0002-9947-1984-0735406-X.

. Jean-Benoît B and Jean-François M .
“Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2”.
In: *Gaz’nte des MŅhémŅiciens* . Pages – .

. Johannes B .
“A subexponential algorithm for the determination of class groups and regulators of algebraic number õelds”. In: *Séminaire de Ń éorie des Nombres, Parś*.
Edited by Catherine G . Volume . Progress in Mathematics. Birkhäuser.
Pages – .

. James L. H and Kevin S. M C .
"A rigorous subexponential algorithm for computation of class groups".
In: *Journal of ŭ e American MŅhemŅical Sociŉy* . . Pages – .
DOI: 10.2307/1990896.

. George R. K .
"Linear sy ems on abelian varieties". In: *American Journal of MŅhemŅics* . .
DOI: 10.2307/2374480.

. Jonathan P .
"Frobenius maps of abelian varieties and ŏnding roots of unity in ŏnite ŏelds".
In: *MŅhemŅics of CompuŪtion* . . Pages – .
DOI: 10.2307/2008445.

. Jean-François M .
"Con ruńion de courbes de genre 2 à partir de leurs modules".
In: *E eňive mŉhods in algebraic geomŉry — MEGA '* .
Edited by Teo M and Carlo T . Volume . Progress in Mathematics.
Birkhäuser. Pages – .

. David R. K .
"Endomorphism rings of elliptic curves over ŏnite ŏelds".
PhD thesis. University of California at Berkeley.
URL: http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf.

. Wieb B , John C , and Catherine P .
" Ł e Magma algebra sy em: the user language".
In: *Journal of Symbolic CompuŪtion* . – . Pages – .
DOI: 10.1006/jsco.1996.0125.

. Henri C , Francisco D D , and Michel O .
"Subexponential algorithms for class group and unit computations".
In: *Journal of Symbolic CompuŪtion* . – . Special issue on computational algebra and number theory: proceedings of the ŏr MAGMA conference. Pages – .
DOI: 10.1006/jsco.1996.0143.

. Paul W .
"Equations for the Jacobian of a hyperelliptic curve".
In: *Transaňions of ŭ e American MŅhemŅical Sociŉy* . . Pages – .
DOI: 10.1090/S0002-9947-98-02056-X.

. Pierrick G and Robert H .
"Counting points on hyperelliptic curves over ŏnite ŏelds".

In: *Algorithmic Number Theory — ANTS-IV.* Edited by Wieb B .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/10722028_18`.

. Mireille F Ž and François M .
"Isogeny volcanoes and the SEA algorithm".
In: *Algorithmic Number Theory — ANTS-V.*
Edited by Claus F and David R. K . Volume .
Lecture Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-45455-1_23`.

. Steven D. G , Florian H , and Nigel P. S .
"Extending the GHS Weil descent attack".
In: *Advances in Cryptology — EUROCRYPT '* . Edited by Lars R. K .
Volume . Lecture Notes in Computer Science. Springer. Pages – .
DOI: `10.1007/3-540-46035-7_3`.

. David R. K .
ECHIDNA: Algorithms for elliptic curves and higher dimensional analogues.
URL: `http://echidna.maths.usyd.edu.au/`.

. Robert C , David R. K , and David L .
"Higher dimensional 3-adic CM construction".
In: *Journal of Algebra* . . Pages – .
DOI: `10.1016/j.jalgebra.2007.11.016`.

. Reinier B , David G , and Kristin E. L .
Explicit CM-theory in dimension . arXiv.org: `0910.1848`.

. Jean-Marc C .
"Linearizing torsion classes in the Picard group of algebraic curves over finite fields".
In: *Journal of Algebra* . . Pages – .
DOI: `10.1016/j.jalgebra.2008.09.032`.

. Kirsten E and Kristin E. L .
"A CRT algorithm for constructing genus curves over finite fields".
In: *Arithmetic, Geometry and Coding Theory — AGCT '* .
Edited by François R and Serge V . Volume . Séminaires et Congrès.
Société Mathématique de France. Pages – .

. David L and Damien R .
Computing isogenies between abelian varieties. arXiv.org: `1001.2016`.

. Markus W .
“Über Korre ŕ ondenzen zwischen algebraischen Funktionenkörper”.
PhD thesis. Technische Universität Berlin.
URL: `http://www.math.tu-berlin.de/~wagner/Diss.pdf`.

. Gaetan B , Romain C , and Damien R .
AVIsogenies, a library for computing śogenies b’nween abelian vari’nies.
Regi ered at the Agence pour la Prote ńion des Programmes under reference
IDDN.FR.001.440011.000.R.P.2010.000.10000.
URL: `http://avisogenies.gforge.inria.fr/`.

. Pierrick G and Éric S .
GenŬ point counting over prime Ŕelds. HAL-INRIA: 00542650.

. Romain C and Damien R .
Computing (ℓ, ℓ)*-śogenies in polynomial time on Jacobians of genŬ curves.*
IACR ePrint: 2011/143.

fndex

Summary

E R C

Modern communications heavily rely on cryptography to ensure data integrity and privacy. Over the pa two decades, very e cient, secure, and featureful cryptographic schemes have been built on top of abelian varieties deŏned over ŏnite ŏelds. Ł is thesis contributes to several computational a ŕ eńs of ordinary abelian varieties related to their endomorphism ring ruńure.

Ł is ruńure plays a crucial role in the con ruńion of abelian varieties with desirable properties. For in ance, pairings have recently enabled many advanced cryptographic primitives; generating abelian varieties endowed with e cient pairings requires seleńing suitable endomorphism rings, and we show that more such rings can be used than expeńed.

We also address the inverse problem, that of computing the endomorphism ring of a prescribed abelian variety, which has several applications of its own. Prior ate-of-the-art methods could only solve this problem in exponential time, and we design several algorithms of subexponential complexity for solving it in the ordinary case.

For elliptic curves, our algorithms are very e eńive and we demon rate their prańicality by solving large problems that were previously intrańable. Additionally, we rigorously bound the complexity of our main algorithm assuming solely the extended Riemann hypothesis. As an alternative to one of our subroutines, we also consider a generalization of the subset sum problem in ŏnite groups, and show how it can be solved using little memory.

Finally, we generalize our method to higher-dimensional abelian varieties, for which we rely on further heuri ic assumptions. Prańically ŕ eaking, we develop a library enabling the computation of isogenies between abelian varieties; using this important building block in our main algorithm, we apply our generalized method to compute several illu rative and record examples.

Research Prospects

In this thesis, we extensively exploited complex multiplication theory to compute the endomorphism ring structure of a prescribed ordinary abelian variety defined over a finite field. For elliptic curves, we were additionally able to rigorously analyze our algorithms, and we believe their asymptotic complexity leaves little room for improvement.

Oh the other hand, although we described a practical method for varieties of dimension $g = 2$, several topics remain to be explored for $g \geqslant 2$:

- We dealt with orders having identical Picard groups locally, using the method of Eisenträger and Lauter. As its complexity is exponential in the valuation of the conductor gap, this is however impractical in certain cases. It would be interesting to address this by developing a generalization of Kohel's techniques to dimension two and more.
- Having a deeper insight on the structure of isogeny graphs would certainly help solving the above, and we note that recent work on elliptic curves by Joux and Ionica offers promising perspectives of developments on this matter in higher dimension.
- Besides the extended Riemann hypothesis, heuristics we relied on should be further analyzed, such as the assumption that norms of LLL-reduced ideals are as smooth as random integers, or that complex multiplication applies to non-maximal orders.
- The convenient structure of Jacobian varieties was used to draw points at random, and to uniquely identify isomorphism classes. Using our method beyond dimension three would require to solely work in theta-coordinates, using the Heisenberg group for the latter, and finding an efficient way of doing the former.

Closely connected topics include the computation of class polynomials and of modular polynomials; it is only natural that they should benefit from further exploiting complex multiplication theory as well. For elliptic curves, this was done successfully for both problems by Sutherland, and by Bröker, Lauter, and Sutherland, respectively.

However, similar work remains to be done in higher dimension: although substantive improvements have been made on it over the past few years, the computation of class polynomials remains a topic of active study, albeit particularly unexplored in the case of non-maximal orders. On the other hand, modular polynomials have not attracted many research, due to their prohibitive height; it would be challenging to improve on this and compute more such polynomials, as an alternative to explicit isogeny computation.

Finally, more of the code written during this thesis should be optimized, fully automated, and cleaned up for inclusion in open software packages, as experimentation using efficient computer routines becomes increasingly important to research activities in many fields.

Curriculum Vitæ

Gaetan B was born on the th of November in Les Ulis, France. AŔer obtaining the *diplôme nŅional du brev'n* in at the collège Paul Arène (Peymeinade, France) and the *baccalauréŅ* in at the lycée Amiral (Grasse, France), he attended *clńses préparŅoires aux grandes écoles*, majoring in mathematics, at the lycée Masséna (Nice, France).

In Augu he was admitted to the École Normale Supérieure (Paris, France) where he received a *licence* and a *maîtrśe* of mathematics in July . AŔer passing the *agrégŅion* of mathematics in July , he pursued a ma er in analysis, arithmetic, and geometry at the Université Paris-Sud (Orsay, France) which he completed in Ońober together with the *magśtère* of fundamental and applied mathematics, and computer science; his ma er's thesis, entitled "On the generation of pairing-friendly elliptic curves," was realized in the number theory group of the Tokyo In itute of Technology (Tokyo, Japan).

Funded by a grant from the French Mini ry of Research, he arted a joint PhD projeń at the In itut National Polytechnique de Lorraine (Nancy, France) and at the Technische Universiteit Eindhoven (Eindhoven, Ł e Netherlands) in February , of which the research results are presented in this dissertation.