MOST ODD DEGREE HYPERELLIPTIC CURVES HAVE ONLY ONE RATIONAL POINT

BJORN POONEN AND MICHAEL STOLL

In memory of Robert F. Coleman, who pioneered the effective approach to Chabauty's method

ABSTRACT. Consider the smooth projective models C of curves $y^2 = f(x)$ with $f(x) \in \mathbb{Z}[x]$ monic and separable of degree $2g+1$. We prove that for $g \geq 3$, a positive fraction of these have only one rational point, the point at infinity. We prove a lower bound on this fraction that tends to 1 as $g \to \infty$. Finally, we show that $C(\mathbb{Q})$ can be algorithmically computed for such a fraction of the curves. The method can be summarized as follows: using p-adic analysis and an idea of McCallum, we develop a reformulation of Chabauty's method that shows that certain computable conditions imply $\#C(\mathbb{Q}) = 1$; on the other hand, using further p-adic analysis, the theory of arithmetic surfaces, a new result on torsion points on hyperelliptic curves, and crucially the Bhargava–Gross theorems on the average number and equidistribution of nonzero 2-Selmer group elements, we prove that these conditions are often satisfied for $p = 2$.

1. INTRODUCTION

In 1983, Faltings proved that if C is a curve of genus $g > 1$ over $\mathbb{Q}$, then $C(\mathbb{Q})$ is finite [Fal83]. Our goal is to study $C(\mathbb{Q})$ as C varies in a family, namely the family $\mathcal{F}_g$ of hyperelliptic curves $y^2 = f(x)$ for $f(x) \in \mathbb{Z}[x]$ monic and separable of degree $2g+1$ for a fixed $g > 1$. Although we write an affine equation, we mean the smooth projective model, which has one point ∞ at infinity since $\deg f$ is odd.

Our main results are:

- For each $g \geq 3$, a positive fraction of the $C \in \mathcal{F}_g$ satisfy $C(\mathbb{Q}) = \{\infty\}$ (Theorem 10.3).
- The fraction tends to 1 exponentially fast as $g \to \infty$ (Theorem 10.6).
- Chabauty's method [Cha41, Col85] at the prime 2 is enough to yield an effective algorithm to determine $C(\mathbb{Q})$ for C in a computable subset whose density is positive for $g \geq 3$ and tends to 1 as $g \to \infty$ (Corollary 10.13).

(See Section 2 for the precise definition of density.) In particular, most monic integral polynomials of large odd degree never yield a square when evaluated on rational numbers. This is the first time that Faltings' theorem has been made effective for a positive fraction of a "large" family of curves with a rational point. Note that the presence of a rational point makes it impossible to use local methods to prove that $C(\mathbb{Q}) = \emptyset$, and generally tends to make the determination of $C(\mathbb{Q})$ more difficult. On the other hand, the fraction is conjectured to be 1 for all $g \geq 2$ (Remark 10.11).

Date: June 15, 2014.
2010 *Mathematics Subject Classification.* Primary 11G30; Secondary 14G25, 14G40, 14K15, 14K20.
Key words and phrases. hyperelliptic curve, rational point, Chabauty's method, Selmer group.
This article has been published in *Annals of Math.* **180** (2014), no. 3, 1137–1166.

Our proofs depend crucially on work of Bhargava and Gross on the average behavior of 2-Selmer groups of hyperelliptic Jacobians [BG13, Theorems 11.1 and 12.4]. Their work was inspired by the connection between pencils of quadrics and hyperelliptic Jacobians (work of Reid [Rei72], Donagi [Don80], and Wang [Wan12]), and by earlier work by Bhargava and Shankar for elliptic curves [BS13], itself preceded by work of de Jong [dJ02] in the function field case (see also [Fou93] and other references listed in [Poo13, Section 2]). Bhargava and Gross deduced corollaries for $C(\mathbb{Q})$ from [BG13, Theorem 11.1]: specifically, they proved that for each $g \geq 2$, there is a positive fraction of $C \in \mathcal{F}_g$ satisfying $\#C(\mathbb{Q}) \leq 3$, and for each $g \geq 3$, the fraction of C satisfying $\#C(\mathbb{Q}) < 20$ is more than $1/2$ [BG13, Corollary 4]. On the other hand, our arguments are essentially disjoint from those in [BG13]: we use [BG13, Theorems 11.1 and 12.4] only as a black box.

To explain how Bhargava and Gross passed from Selmer group information to information on $C(\mathbb{Q})$, and to explain why different ideas are needed to obtain *our* results, we must recall Chabauty's method (see [MP12] or [Sto06] for a more detailed exposition). Let C be a curve over $\mathbb{Q}$ embedded in its Jacobian J. In 1941, Chabauty [Cha41], inspired by an idea of Skolem [Sko34], proved a weak form of what is now Faltings' theorem, namely that if $\operatorname{rk} J(\mathbb{Q}) < g$, then $C(\mathbb{Q})$ is finite. Chabauty's approach was to bound $C(\mathbb{Q})$ by $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ inside $J(\mathbb{Q}_p)$, where $\overline{J(\mathbb{Q})}$ is the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Later, Coleman [Col85] showed how to refine Chabauty's argument to obtain an *explicit* upper bound on $\#C(\mathbb{Q})$, and improved bounds were given in [Sto06]. The latter bounds at odd primes of good reduction were sufficient for Bhargava and Gross to obtain their results for $\#C(\mathbb{Q})$ above.

But it is impossible to reduce the Chabauty upper bound on $\#C(\mathbb{Q})$ to 1 if one knows only the size of the 2-Selmer group (when it does not force $J(\mathbb{Q})$ to be finite), because there is nothing to control the position of $\overline{J(\mathbb{Q})}$ in $J(\mathbb{Q}_p)$. Restricting the family of curves to a subfamily defined by finitely many congruence conditions does not help: such conditions can determine the structure of $J(\mathbb{Q}_p)$, but not the position of $\overline{J(\mathbb{Q})}$ in $J(\mathbb{Q}_p)$, it seems.

To solve this problem, we resurrect an idea of McCallum [McC94], that knowledge of the p-Selmer group $\operatorname{Sel}_p J$ and its map to $J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p)$ can sometimes be used to extract a tiny bit of information on the position of $\overline{J(\mathbb{Q})}$ inside $J(\mathbb{Q}_p)$. McCallum used this idea to study the arithmetic of Fermat curves in 1994, but as far as we know, it has not been used since. Fortunately, the method of Bhargava and Gross yields not only the average size of $\operatorname{Sel}_2 J$, but also *equidistribution* of the images of its nonzero elements in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ as C varies (see Section 8.3 for the meaning of this), even if one imposes finitely many congruence conditions on C. We will prove that this suffices for the application of McCallum's idea: we impose congruence conditions to control the position of $C(\mathbb{Q}_2)$ in $J(\mathbb{Q}_2)$ for C with good reduction at 2, and apply equidistribution to prove that for g large enough (at least 3), at least a small positive fraction of these C have the 2-adic closure $\overline{J(\mathbb{Q})}$ in a favorable position, i.e., intersecting $C(\mathbb{Q}_2)$ in only one point, so that a 2-adic Chabauty argument succeeds in proving $C(\mathbb{Q}) = \{\infty\}$.

To carry out the argument in the previous sentence, we introduce a reformulation of Chabauty's method in which we compute $C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})}$ not in $J(\mathbb{Q}_2)$ directly but only after applying a sequence of maps (see (6.1)). Specifically, we prove that if

$$\operatorname{Sel}_2 J \to V := \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2) + J(\mathbb{Q}_2)_{\text{tors}}} \simeq \mathbb{F}_2^g$$

is injective and the images of certain partially-defined maps

$$\rho \log \colon C(\mathbb{Q}_2) \to J(\mathbb{Q}_2) \overset{\log}{\twoheadrightarrow} \mathbb{Z}_2^g \dashrightarrow \mathbb{P}^{g-1}(\mathbb{Q}_2) \overset{\rho}{\to} \mathbb{P}^{g-1}(\mathbb{F}_2)$$

and

$$\mathrm{Sel}_2 J \to V \simeq \mathbb{F}_2^g \dashrightarrow \mathbb{P}^{g-1}(\mathbb{F}_2)$$

do not meet, then $C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})}$ consists of torsion points of odd order (Proposition 6.2). Next, we exclude nontrivial torsion points by proving that most hyperelliptic curves do not contain any $\mathbb{Q}_2$-rational torsion points except for Weierstrass points (Corollary 8.6): this follows from a new purely geometric statement, that the generic hyperelliptic curve contains no torsion points except Weierstrass points (Theorem 7.1). Because Bhargava and Gross tell us how many nonzero Selmer elements there are and how they are distributed in V, it remains to show that $\rho \log(C(\mathbb{Q}_2))$ is not too large. When $g \geq 3$, this can be arranged for a positive fraction of curves by 2-adic congruence conditions on C since it turns out that $\rho \log(C(\mathbb{Q}_2))$ is locally constant as C varies 2-adically, if we exclude curves with unexpected torsion points (Proposition 8.7).

Remark 1.1. For $g = 2$, it seems consistent with known results that the conditions above on $C(\mathbb{Q}_2)$ and $\mathrm{Sel}_2 J$ fail for 100% of curves: the set $\mathbb{P}^{g-1}(\mathbb{F}_2)$ is just too small. But a *3-adic* version of our argument would work even for $g = 2$, if we knew equidistribution of nonzero 3-Selmer group elements (Remark 10.5).

Now let us sketch how we strengthen the result to obtain a fraction that tends to 1 as $g \to \infty$. We must continue to use the prime 2, because the equidistribution is currently known only for the 2-Selmer group, but now we must also consider C with bad reduction at 2, since the density of curves with good reduction at 2 tends to a number strictly less than 1 as $g \to \infty$. There are earlier studies of Chabauty's method in the bad reduction case, such as [LT02, Section 1], [MP12, Appendix], and [KZB13], but the bounds they produce are not sharp enough for our purposes. In fact, we must deal with curves with arbitrarily bad reduction at 2, and our task is to prove that $\rho \log(C(\mathbb{Q}_2))$ is usually small. Since $\log|_{C(\mathbb{Q}_2)}$ is computed by integrating 1-forms on residue disks, which correspond to the $\mathbb{F}_2$-points in the smooth locus $\mathcal{C}^{\mathrm{smooth}}$ of the minimal proper regular model, it suffices to prove that

(1) the average size of $\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_2)$ is small, and
(2) the image of $\rho \log$ on each residue disk is small.

As for (1), the Ogg–Saito formula [Sai88] together with [Liu94, Proposition 1] bounds the number c of connected components of $\mathcal{C}^{\mathrm{smooth}}_{\mathbb{F}_2}$ in terms of the Deligne discriminant of $\mathcal{C}$, but this discriminant is hard to compute, and it is not known whether c can be bounded in terms of the usual discriminant of the polynomial $f(x)$: the best results in this direction we know are those in [Liu96, Section 9]. So instead we analyze the random variable $\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_2)$ by explicitly blowing up non-regular $\mathbb{F}_2$-points until we have an approximation to $\mathcal{C}$; this leads to a recursive analysis of a Bienaymé–Galton–Watson-like process (Lemma 9.5). The result (Theorem 9.1) is that the average of $\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_2)$ is at most 3.

As for (2), this amounts to bounding the image of an analytic curve in $\mathbb{P}^{g-1}(\mathbb{Q}_2)$ under the reduction map to $\mathbb{P}^{g-1}(\mathbb{F}_2)$. We do not know of results in the literature on this kind of nonarchimedean analysis problem, though it is reminiscent of tropical geometry. To handle it, we apply the p-adic Weierstrass preparation theorem to replace the power series defining the analytic curve by polynomials, and hence reduce to the case of an algebraic rational curve.

We reinterpret the map $\mathbb{P}^1_{\mathbb{Q}_2} \to \mathbb{P}^{g-1}_{\mathbb{Q}_2}$ defining this curve as a rational map $\mathbb{P}^1_{\mathbb{Z}_2} \dashrightarrow \mathbb{P}^{g-1}_{\mathbb{Z}_2}$, whose indeterminacy at $\mathbb{F}_2$-points we resolve, the upshot being that our image can be bounded in terms of the complexity of a tree of rational curves over $\mathbb{F}_2$ (see Section 3).

Many of our arguments work also at primes p other than 2, so we work in this more general context when possible. On the other hand, the Bhargava–Gross equidistribution theorem is known only for 2-Selmer elements, so the final results for higher p must remain conditional for the time being.

Remark 1.2. Independently of the present paper, Bhargava [Bha13] has proved that in the family of all not-necessarily-monic *even*-degree genus g hyperelliptic curves over $\mathbb{Q}$, the density of those that have no rational points is $1 - o(2^{-g})$ as $g \to \infty$. Although the statement is similar to that of our Theorem 10.6, and relies on average behavior of 2-Selmer elements, his proof is otherwise completely different: it does not need an equidistribution theorem or Chabauty's method, because there are more methods available for proving the nonexistence of rational points than for determining the rational points when one exists. Specifically, his proof controls the average size of the "fake 2-Selmer set" of the curve, in effect showing that for most curves, all the relevant finite étale covers fail to have local points.

Remark 1.3. For the family of *monic* even-degree genus g hyperelliptic curves over $\mathbb{Q}$, Shankar and Wang [SW14] have adapted the method of [BG13] to prove analogous theorems on the average size and equidistribution of 2-Selmer groups, and then have adapted the method of the present paper to prove that the density of such curves that have only the two rational points at infinity is at least $1 - (48g + 120)2^{-g}$. Just as the presence of one rational point makes it more difficult to control the set of all rational points, the presence of two rational points means that their argument must be more complicated than ours in certain places.

2. Notation

For any field k, let $\overline{k}$ be an algebraic closure.

We fix a prime p. As usual, we define $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and its fraction field $\mathbb{Q}_p := \operatorname{Frac} \mathbb{Z}_p$. More generally for any place v of $\mathbb{Q}$, let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ at v. Let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$, let $\mathcal{O}_{\mathbb{C}_p}$ be its valuation ring, and let D_1 be the open unit disk in $\mathbb{C}_p$. Let v_p be the p-adic valuation on $\mathbb{C}_p$, normalized so that $v_p(p) = 1$.

We fix $g \in \mathbb{Z}_{\geq 1}$. For a field k, let $\mathbb{P}$ be the usual map $k^g \setminus \{\mathbf{0}\} \to \mathbb{P}^{g-1}(k)$. We write ρ for the reduction map $\mathbb{P}^{g-1}(\mathbb{Q}_p) = \mathbb{P}^{g-1}(\mathbb{Z}_p) \to \mathbb{P}^{g-1}(\mathbb{F}_p)$ or for the composition $\mathbb{Q}_p^g \setminus \{\mathbf{0}\} \xrightarrow{\mathbb{P}} \mathbb{P}^{g-1}(\mathbb{Q}_p) \xrightarrow{\rho} \mathbb{P}^{g-1}(\mathbb{F}_p)$. If T is a subset of a set S, and f is a function defined only on T, then $f(S)$ means $f(T)$; for example, we may write $\rho(\mathbb{Q}_p^g) = \mathbb{P}^{g-1}(\mathbb{F}_p)$.

A variety is a separated scheme X of finite type over a field, and X is called nice if it is smooth, projective, and geometrically integral. If X and T are S-schemes, define $X_T := X \times_S T$; in this context we sometimes write R instead of $\operatorname{Spec} R$. Given a ring R, and $f \in R[x]$ of degree $2g + 1$, by the standard compactification of $y^2 = f(x)$ we mean the R-scheme $\operatorname{Proj} R[x, y, z]/(y^2 - z^{2g+2} f(x/z))$ where $\deg x = \deg z = 1$ and $\deg y = g + 1$; it can be covered by two affine patches, one isomorphic to $y^2 = f(x)$ and the other to $y^2 = x^{2g+2} f(1/x)$. For any domain R of characteristic not 2, denote by $\mathcal{F}_g(R)$ the set of all nice genus g curves (over $\operatorname{Frac} R$) arising as the standard compactification of

$$y^2 = x^{2g+1} + a_1 x^{2g} + a_2 x^{2g-1} + \cdots + a_{2g} x + a_{2g+1}$$

for some $a_1, a_2, \dots, a_{2g+1} \in R$. This can be identified with R^{2g+1} minus the zero set of the discriminant of the polynomial in x in the equation above. We set $\mathcal{F}_g := \mathcal{F}_g(\mathbb{Z})$.

Essentially following [BG13], for $C \in \mathcal{F}_g$ corresponding to $(a_1, \dots, a_{2g+1})$, define the height of C as

$$H(C) := \max\bigl\{|a_1|, |a_2|^{1/2}, \dots, |a_{2g}|^{1/2g}, |a_{2g+1}|^{1/(2g+1)}\bigr\}.$$

(Actually, [BG13] required $a_1 = 0$, but this makes little difference: see Remark 8.11. Also, their height is the $2g(2g+1)$-th power of what we have written.) We set

$$\mathcal{F}_{g,X} := \{C \in \mathcal{F}_g : H(C) < X\}.$$

The density of a subset $S \subseteq \mathcal{F}_g$ is

$$\mu(S) := \lim_{X\to\infty} \#(S \cap \mathcal{F}_{g,X})/\#\mathcal{F}_{g,X},$$

if the limit exists. Define lower density and upper density by replacing lim by lim inf or lim sup, respectively. If $S \subseteq T \subseteq \mathcal{F}_g$ and $\mu(T) > 0$, the relative density of S in T is $\mu(S)/\mu(T)$, if $\mu(S)$ exists; similarly define relative lower density and relative upper density. If $f\colon \mathcal{F}_g \to \mathbb{R}$ is a function, then we say that f has average α on $\mathcal{F}_g$ if

$$\lim_{X\to\infty} \frac{\sum_{C\in\mathcal{F}_{g,X}} f(C)}{\#\mathcal{F}_{g,X}} = \alpha.$$

We say that the average of f is at most α if the lim sup is at most α. Similarly define the average of a function on an infinite subset of $\mathcal{F}_g$.

Restrict the normalized Haar measure on $\mathbb{Z}_p^{2g+1}$ to obtain a probability measure on $\mathcal{F}_g(\mathbb{Z}_p)$. Let $\mathbf{P}(S)$ be the probability of an event S. For a random variable X defined on $\mathcal{F}_g(\mathbb{Z}_p)$, let $\mathbf{E}X$ denote its average. If X is a random variable defined only on a positive-measure subset S of $\mathcal{F}_g(\mathbb{Z}_p)$, then $\mathbf{E}X$ denotes the average of X conditioned on the event S.

3. Images of curves under reduction

3.1. **Algebraic curves.** By the degree of a morphism $\phi\colon C \to \mathbb{P}^{g-1}$, where C is a nice curve, we mean $\deg \phi^*\mathscr{O}(1)$. If $f_1, \dots, f_g$ are single-variable polynomials of degree at most n, not all zero, then the rational map $(f_1 : \cdots : f_g)\colon \mathbb{A}^1 \dashrightarrow \mathbb{P}^{g-1}$ extends to a morphism $\mathbb{P}^1 \to \mathbb{P}^{g-1}$ of degree at most n.

Proposition 3.1. *Let $\phi\colon \mathbb{P}^1_{\mathbb{Q}_p} \to \mathbb{P}^{g-1}_{\mathbb{Q}_p}$ be of degree n. Then $\#\rho\bigl(\phi(\mathbb{P}^1(\mathbb{Q}_p))\bigr) \le np + 1$.*

If ϕ has good reduction (i.e., extends to a morphism $\mathbb{P}^1_{\mathbb{Z}_p} \to \mathbb{P}^{g-1}_{\mathbb{Z}_p}$), then $\rho(\phi(\mathbb{P}^1(\mathbb{Q}_p)))$ is contained in $\phi(\mathbb{P}^1(\mathbb{F}_p))$, which has size at most $p+1$. In the general case, we will blow up $\mathbb{P}^1_{\mathbb{Z}_p}$ to resolve the indeterminacy, and control the resulting increase in the number of $\mathbb{F}_p$-points on the source.

Proof of Proposition 3.1. After iteratively blowing up $\mathbb{F}_p$-points on $\mathbb{P}^1_{\mathbb{Z}_p}$, we obtain a proper regular $\mathbb{Z}_p$-scheme S' such that ϕ extends to a rational map $\phi'\colon S' \dashrightarrow \mathbb{P}^{g-1}_{\mathbb{Z}_p}$ defined at all $\mathbb{F}_p$-points of S'. If we also blow up closed points of higher degree, we obtain S'' such that ϕ extends to a *morphism* $\phi''\colon S'' \to \mathbb{P}^{g-1}_{\mathbb{Z}_p}$, as in [Lic68, II.D, Proposition 4.2]. Then $\mathbb{P}^1(\mathbb{Q}_p) = S''(\mathbb{Z}_p) = S'(\mathbb{Z}_p)$, so $\rho(\phi(\mathbb{P}^1(\mathbb{Q}_p))) = \rho(\phi'(S'(\mathbb{Z}_p))) \subseteq \phi'(S'(\mathbb{F}_p))$.

The construction of S' shows that $S'_{\mathbb{F}_p}$ is a strict normal crossings divisor whose components are copies of $\mathbb{P}^1_{\mathbb{F}_p}$ meeting at $\mathbb{F}_p$-points. Name these components $S'_1, S'_2, \dots$ in the order that

they were produced by the blowing up, starting with S'_1 being the strict transform of $\mathbb{P}^1_{\mathbb{F}_p}$. Since $\deg \phi''^*_{\mathbb{F}_p} \mathscr{O}(1) = \deg \phi^* \mathscr{O}(1) = n$, the morphism ϕ'' is non-constant on at most n components of $S''_{\mathbb{F}_p}$, so ϕ' is non-constant on at most n of the sets $S'_i(\mathbb{F}_p)$. Let $\Sigma_0 = \{P\}$ for some $P \in S'_1(\mathbb{F}_p)$, and for $i \geq 1$, let $\Sigma_i := \bigcup_{j=1}^{i} S'_j(\mathbb{F}_p)$. We have $\#\phi'(\Sigma_0) = 1$. Incrementing i increases $\#\phi'(\Sigma_i)$ by 0 if ϕ' is constant on $S'_{i+1}(\mathbb{F}_p)$ and by at most p otherwise, since one of the $p+1$ points of $S'_{i+1}(\mathbb{F}_p)$ was already in Σ_i. Thus $\#\phi'(\Sigma_i)$ increases at most n times, by at most p each time, starting from 1. Hence $\#\phi'(S'(\mathbb{F}_p)) \leq np + 1$. □

Remark 3.2. For each (n, p), the bound in Proposition 3.1 is sharp: for any $g > n$, define ϕ by taking $f_j(t) := p^{j(j-1)} t^{j-1}$ for $1 \leq j \leq n+1$, and $f_j(t) := 0$ for $n+1 < j \leq g$; then $\rho(\phi(\mathbb{P}^1(\mathbb{Q}_p)))$ is a chain of n lines in $\mathbb{P}^{g-1}(\mathbb{F}_p)$.

Remark 3.3. The proof of Proposition 3.1 suggests a down-to-earth algorithm for computing $\rho(\phi(\mathbb{P}^1(\mathbb{Q}_p)))$. Namely, one iteratively subdivides $\mathbb{P}^1(\mathbb{Q}_p)$ into disks until $\rho \circ \phi$ is constant on each.

3.2. **Analytic curves.** Recall the notation $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}_p$, and D_1 from Section 2.

Definition 3.4. Let $\mathbf{w} = (w_1, w_2, \ldots, w_g) \in \mathbb{C}_p[\![t]\!]^g - \{\mathbf{0}\}$. Let $w_{j,n}$ be the coefficient of t^n in w_j. Define the Newton polygon $\mathrm{NP}(\mathbf{w})$ as the lower convex hull of the set

$$\left\{ \left(n, v_p(w_{j,n})\right) : 1 \leq j \leq g,\ n \geq 0 \right\}.$$

Suppose that the minimum of the y-coordinates of the vertices of $\mathrm{NP}(\mathbf{w})$ is attained; then for the vertices attaining this minimum, let $n_{\mathbf{w}}$ and $N_{\mathbf{w}}$ be the minimum and maximum x-coordinates if they exist (the maximum might not exist). When $\mathbf{w}$ consists of a single w, we also write $\mathrm{NP}(w)$, n_w, N_w.

Remark 3.5. The Newton polygon $\mathrm{NP}(\mathbf{w})$ depends only on the $\mathbb{Z}_p$-span of the w_i.

Remark 3.6. Let $\mathbf{w} \in \mathbb{Q}_p[\![t]\!]^g - \{\mathbf{0}\}$. Let R be the valuation ring of an unramified extension of $\mathbb{Q}_p$. If $\lambda_1, \ldots, \lambda_g \in R$ have $\mathbb{F}_p$-independent images in R/pR, then

$$\mathrm{NP}(\mathbf{w}) = \mathrm{NP}(\lambda_1 w_1 + \cdots + \lambda_g w_g).$$

Remark 3.7. For $w \in \mathbb{C}_p[\![t]\!] - \{0\}$ for which n_w is defined, the theory of Newton polygons [Kob84, Corollary on p. 106] implies that $n_w = \#$ (zeros of w on D_1); we write $\#(\ )$ instead of $\#\{\ \}$ to indicate that we are counting zeros with multiplicity.

Following [Sto06, Section 6], for $n \geq 0$, define

$$\delta(p, n) := \max\{d \geq 0 : v_p(n+1) + d \leq v_p(n+d+1)\}.$$

Proposition 3.8. *Suppose that $\mathbf{w} \in \mathbb{Q}_p[\![t]\!]^g \setminus \{\mathbf{0}\}$ has p-adically bounded coefficients. Let $\boldsymbol{\ell} \in \mathbb{Q}_p[\![t]\!]^g$ be such that $d\boldsymbol{\ell}/dt = \mathbf{w}$. Then $\#\rho(\boldsymbol{\ell}(p\mathbb{Z}_p)) \leq p\big(n_{\mathbf{w}} + 1 + \delta(p, n_{\mathbf{w}})\big) + 1$.*

Proof. Let $\mathbf{L}(t) := \boldsymbol{\ell}(pt)$. The lattice point responsible for the value of $N_{\mathbf{L}}$ is a vertex of $\mathrm{NP}(L_j)$ for some j. We ensure that it is a vertex of $\mathrm{NP}(L_i)$ for *every* i by adding w_j to each w_i for which this does not yet hold (this has the effect of applying a linear change of variable to the codomain $\mathbb{P}^{g-1}(\mathbb{F}_p)$ of $\rho \circ \boldsymbol{\ell}$, but does not change the size of the image). By the p-adic Weierstrass preparation theorem (see [Kob84, p. 105, Theorem 14] and its proof), $L_i = f_i u_i$ for some $f_i \in \mathbb{Q}_p[t]$ of degree $N_{\mathbf{L}}$ and $u_i \in 1 + pt\mathbb{Z}_p[\![t]\!]$ converging on $\mathbb{Z}_p$. Set $\mathbf{f} = (f_1, \ldots, f_g)$. For $\tau \in \mathbb{Z}_p$, we have $u_i(\tau) \in 1 + p\mathbb{Z}_p$, so $\rho(\mathbf{L}(\tau)) = \rho(\mathbf{f}(\tau))$. Hence

$\rho(\boldsymbol{\ell}(p\mathbb{Z}_p)) = \rho(\mathbf{L}(\mathbb{Z}_p)) = \rho(\mathbf{f}(\mathbb{Z}_p))$, which has size at most $pN_{\mathbf{L}}+1$ by Proposition 3.1 applied to the morphism $\mathbb{P}^1 \to \mathbb{P}^{g-1}$ defined by $\mathbf{f}$. Finally, we prove $N_{\mathbf{L}} \leq n_{\mathbf{w}} + 1 + \delta(p, n_{\mathbf{w}})$: by Remark 3.6, we may reduce to the case $g = 1$, with coefficients now in an unramified extension; this case can be deduced easily by considering the slopes of the (now standard) Newton polygon; cf. [Sto06, Proposition 6.3]. □

4. The logarithm map

Let J be an abelian variety over $\mathbb{Q}_p$. Let $T_0 J$ be the tangent space to J at 0. Integrating 1-forms defines an analytic group homomorphism $\log\colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ whose kernel is the torsion subgroup $J(\mathbb{Q}_p)_{\mathrm{tors}}$. Since log is a local diffeomorphism and $J(\mathbb{Q}_p)$ is compact, its kernel $J(\mathbb{Q}_p)_{\mathrm{tors}}$ is finite, and its image will be $\mathbb{Z}_p^g$ for a suitable choice of identification $T_0 J \simeq \mathbb{Q}_p^g$; this identification corresponds to a choice of basis $\omega_1, \dots, \omega_g$ of $\mathrm{H}^0(J, \Omega^1)$, which we now fix. Any commutative extension of $\mathbb{Z}_p^g$ by a finite abelian group is split, even as a topological group, so $J(\mathbb{Q}_p) \simeq \mathbb{Z}_p^g \times J(\mathbb{Q}_p)_{\mathrm{tors}}$. Let $\rho\log$ be the composition

$$J(\mathbb{Q}_p) \overset{\log}{\twoheadrightarrow} \mathbb{Z}_p^g \overset{\rho}{\dashrightarrow} \mathbb{P}^{g-1}(\mathbb{F}_p),$$

defined on $J(\mathbb{Q}_p) \setminus J(\mathbb{Q}_p)_{\mathrm{tors}}$.

5. Image of the curve under the logarithm map

For this section, let C be a nice curve of genus $g \geq 1$ over $\mathbb{Q}_p$ with a $\mathbb{Q}_p$-point ∞. Embed C in its Jacobian J by sending ∞ to 0. Define log as in Section 4. Let $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_p$ be the minimal proper regular model of C.

5.1. Image of one residue disk.

Definition 5.1. A residue disk $D \subseteq C(\mathbb{C}_p)$ is the preimage of a point $P \in \mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)$ under $C(\mathbb{C}_p) = \mathcal{C}(\mathcal{O}_{\mathbb{C}_p}) \to \mathcal{C}(\overline{\mathbb{F}}_p)$; then let $D(\mathbb{Q}_p) := D \cap C(\mathbb{Q}_p)$. A uniformizer for D is a regular function t on an open neighborhood of P in $\mathcal{C}$ such that t reduces to a uniformizer at P on $\mathcal{C}_{\mathbb{F}_p}$.

Every point of $C(\mathbb{Q}_p)$ reduces to a point of $\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)$, so $C(\mathbb{Q}_p)$ is the disjoint union of the open sets $D(\mathbb{Q}_p)$.

Let D be a residue disk with uniformizer t. Then t defines a diffeomorphism $D \to D_1$ identifying $D(\mathbb{Q}_p)$ with $p\mathbb{Z}_p$. The restriction of any $\omega \in \mathrm{H}^0(C, \Omega^1)$ to D corresponds to an analytic 1-form $w(t)\,dt$ on D_1, for some $w \in \mathbb{Q}_p[\![t]\!]$ with bounded coefficients. Applying this to $\omega_i|_C$ defines some w_i. Let $\mathbf{w} := (w_1, \dots, w_g)$ and $n_D := n_{\mathbf{w}}$.

Proposition 5.2. *We have* $\#\rho\log(D(\mathbb{Q}_p)) \leq p\big(n_D + 1 + \delta(p, n_D)\big) + 1$.

Proof. Since log is defined by integrating $(\omega_1, \dots, \omega_g)$, the composition

$$p\mathbb{Z}_p \xrightarrow{\sim} D(\mathbb{Q}_p) \hookrightarrow C(\mathbb{Q}_p) \hookrightarrow J(\mathbb{Q}_p) \xrightarrow{\log} \mathbb{Q}_p^g$$

is some $\boldsymbol{\ell} \in \mathbb{Q}_p[\![t]\!]^g$ with $d\boldsymbol{\ell}/dt = \mathbf{w}$. Then

$$\#\rho\log(D(\mathbb{Q}_p)) = \#\rho(\boldsymbol{\ell}(p\mathbb{Z}_p)) \leq p\big(n_D + 1 + \delta(p, n_D)\big) + 1$$

by Proposition 3.8. □

5.2. **Image of many residue disks.**

Lemma 5.3. *Let $\mathcal{D}$ be the set of residue disks on C. Then $\sum_{D\in\mathcal{D}} n_D \le 2g-2$.*

Proof. Let $\lambda_1,\dots,\lambda_g$ be as in Remark 3.6. Let $\omega = \sum_{i=1}^g \lambda_i\omega_i|_C \in \mathrm{H}^0(C_{\mathbb{C}_p},\Omega^1)$. On a residue disk D with uniformizer t, express ω as $w(t)\,dt$, so $w = \sum_{i=1}^g \lambda_i w_i \in \mathbb{C}_p[\![t]\!]$; then

$$n_D = n_{\mathbf{w}} = n_w = \#\left(\text{zeros of } w \text{ on } D_1\right) = \#\left(\text{zeros of } \omega \text{ on } D\right),$$

by Remark 3.7. Thus

$$\sum_{D\in\mathcal{D}} n_D \le \#\left(\text{zeros of } \omega \text{ on } C(\mathbb{C}_p)\right) = 2g-2. \qquad \square$$

Proposition 5.4. *Let $d := \#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)$. Then*

$$\#\rho\log(C(\mathbb{Q}_p)) \le \begin{cases} 5d+6g-6, & \text{if } p=2,\\ (p+1)d + \dfrac{p^2-p}{p-2}(2g-2), & \text{if } p>2.\end{cases}$$

Proof. Sum the bound of Proposition 5.2 over all D and use Lemma 5.3 to obtain

$$\#\rho\log(C(\mathbb{Q}_p)) \le p(2g-2) + (p+1)d + p\sum_D \delta(p,n_D).$$

If $p=2$, use the bound $\delta(2,n)\le 1+n/2$ (and use Lemma 5.3 again) to conclude. If $p>2$, then $\sum_D \delta(p,n_D) \le \Delta_p(d,2g-2)$, where

$$\Delta_p(d,N) := \max\Big\{\sum_{j=1}^d \delta(p,n_j) : n_j\in\mathbb{Z}_{\ge 0} \text{ and } \sum_{j=1}^d n_j \le N\Big\};$$

use the bound $\Delta_p(d,N)\le N/(p-2)$ of [Sto06, Lemma 6.2]. $\square$

6. Image of the rational points under the logarithm map

We now assume that C is a nice curve of genus $g\ge 1$ over $\mathbb{Q}$ with a $\mathbb{Q}$-point ∞, which we use as base-point for embedding C in its Jacobian J. Taking Galois cohomology of $0\to J[p]\to J\xrightarrow{p} J\to 0$ over $\mathbb{Q}$ and over $\mathbb{Q}_v$ for all places v of $\mathbb{Q}$ yields the rows in the following commutative diagram, where δ now denotes a connecting homomorphism:

$$\begin{array}{ccc} \dfrac{J(\mathbb{Q})}{pJ(\mathbb{Q})} & \xhookrightarrow{\ \delta\ } & \mathrm{H}^1(\mathbb{Q},J[p]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \displaystyle\prod_v \frac{J(\mathbb{Q}_v)}{pJ(\mathbb{Q}_v)} & \xhookrightarrow{\ \delta'\ } & \displaystyle\prod_v \mathrm{H}^1(\mathbb{Q}_v,J[p]). \end{array}$$

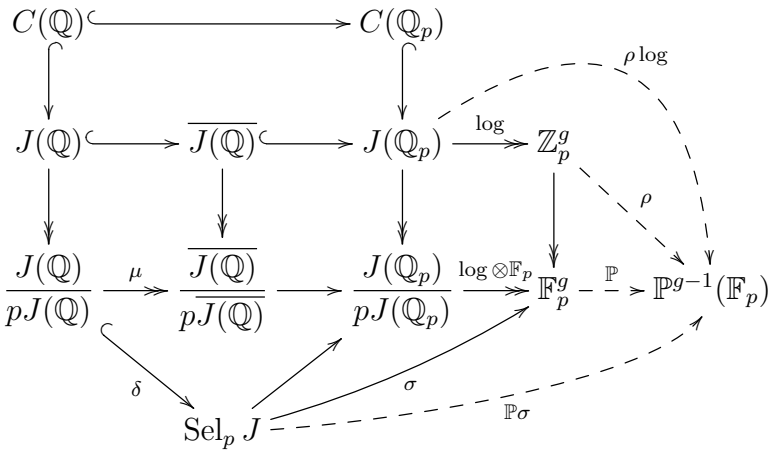
The p-Selmer group of J is defined by

$$\mathrm{Sel}_p J := \{\,\xi\in \mathrm{H}^1(\mathbb{Q},J[p]) : \mathrm{res}(\xi)\in \mathrm{im}(\delta')\,\}.$$

In particular, res restricts to a homomorphism $\mathrm{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p)$. Since the p-adic closure $\overline{J(\mathbb{Q})}$ contains a finite-index closed subgroup that is a free $\mathbb{Z}_p$-module of finite rank,

the natural map $\mu\colon J(\mathbb{Q})/pJ(\mathbb{Q}) \to \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})}$ is surjective. Choose $\log\colon J(\mathbb{Q}_p) \twoheadrightarrow \mathbb{Z}_p^g$ as in Section 4. Then we have a diagram

(6.1)



in which σ and $\mathbb{P}\sigma$ are defined as the compositions, so that the diagram commutes on elements for which the maps are defined.

Let $J(\mathbb{Q}_p)[p']$ be the set of points of finite order prime to p in $J(\mathbb{Q}_p)_{\mathrm{tors}}$. By Section 4, $J(\mathbb{Q}_p) \simeq \mathbb{Z}_p^g \times F$ for a finite abelian group F, so $J(\mathbb{Q}_p)[p']$ is the set of points that are infinitely p-divisible in $J(\mathbb{Q}_p)$.

Proposition 6.2. *If σ is injective and the images $\rho\log(C(\mathbb{Q}_p))$ and $\mathbb{P}\sigma(\mathrm{Sel}_p\, J)$ are disjoint, then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p)[p']$.*

Proof. Suppose that the hypotheses hold. Then $\sigma\delta$ is injective, and (6.1) shows that the surjection μ is an isomorphism and that $\overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \to \mathbb{F}_p^g$ is injective.

Suppose also that the conclusion fails; fix $P \in C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ not in $J(\mathbb{Q}_p)[p']$. Then P is not infinitely p-divisible in $\overline{J(\mathbb{Q})}$, so $P = p^n Q$ for some $n \geq 0$ and some $Q \in \overline{J(\mathbb{Q})}$ outside $p\overline{J(\mathbb{Q})}$. Let $\bar{Q}$ be the image of Q in $\overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})}$. Then $\bar{Q}$ is nonzero, so its image in $\mathbb{F}_p^g$ is nonzero, and $\mathbb{P}\sigma\big(\delta\mu^{-1}(\bar{Q})\big)$ is defined. Tracing through (6.1), we have

$$\mathbb{P}\sigma(\mathrm{Sel}_p\, J) \ni \mathbb{P}\sigma\big(\delta\mu^{-1}(\bar{Q})\big) = \rho\log(Q) = \rho\log(p^n Q) = \rho\log(P) \in \rho\log(C(\mathbb{Q}_p)),$$

contradicting the assumption that $\rho\log(C(\mathbb{Q}_p))$ and $\mathbb{P}\sigma(\mathrm{Sel}_p\, J)$ are disjoint. □

We state the following consequence explicitly, since it may have applications outside the context of this paper.

Corollary 6.3. *Let C be a nice curve of genus $g \geq 1$ over $\mathbb{Q}$ with a rational point $\infty \in C(\mathbb{Q})$. We embed C in its Jacobian J using ∞ as base-point. Let p be a prime number such that in diagram (6.1) σ is injective and the images $\rho\log(C(\mathbb{Q}_p))$ and $\mathbb{P}\sigma(\mathrm{Sel}_p\, J)$ are disjoint. Then $C(\mathbb{Q}) \subseteq J(\mathbb{Q})[p']$.*

Proof. Apply Proposition 6.2 and use that $C(\mathbb{Q}) = C(\mathbb{Q}_p) \cap J(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$. □

Given C, ∞, and a prime p, the hypotheses on p in Corollary 6.3 can be checked explicitly:

- We can compute a regular model $\mathcal{C}$ of C over $\mathbb{Z}_p$, which gives us a covering of $C(\mathbb{Q}_p)$ by residue disks.

- We can compute a basis of the space of regular 1-forms on C and their integrals on a set of representatives of generators of $J(\mathbb{Q}_p)/(pJ(\mathbb{Q}_p) + J(\mathbb{Q}_p)_{\mathrm{tors}})$. This gives us $\log\colon J(\mathbb{Q}_p) \twoheadrightarrow \mathbb{Z}_p^g$.
- We can then compute $\rho\log(C(\mathbb{Q}_p))$ by evaluating $\rho\log$ on each residue disk.
- The p-Selmer group of J can be computed (at least in principle). This computation also provides the map $\mathrm{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p)$.
- By post-composing with $\log \otimes \mathbb{F}_p$, we get σ, so we can check whether σ is injective and we can determine the image of $\mathbb{P}\sigma$.

See also Section 10.3 below.

7. Torsion points on a generic hyperelliptic curve

Theorem 7.1, which we hope is of independent interest, shows that the only torsion points lying on a generic hyperelliptic curve are its Weierstrass points.

Theorem 7.1. *Let C be a generic hyperelliptic curve of genus $g > 1$ over a field k of characteristic 0; i.e., the image of the corresponding morphism from $\operatorname{Spec} k$ to the moduli space over $\mathbb{Q}$ is the generic point. Assume that C has a k-rational Weierstrass point, which is used to embed C in its Jacobian J. Then $C(\overline{k}) \cap J(\overline{k})_{\mathrm{tors}}$ consists of only the Weierstrass points.*

Remark 7.2. See [CEFS13, Theorem 2.3] for a related result concerning torsion points on the theta divisor of a generic hyperelliptic curve.

Before giving the proof in detail, let us explain the strategy. If P is a torsion point of order n on C, then so are all its Galois conjugates. Because of "big monodromy", there are many such Galois conjugates. Taking combinations of these yields a principal divisor associated to a rational function of low degree on C. Such functions are fixed by the hyperelliptic involution, and this will force P to be a Weierstrass point.

Proof. We may assume that C is the curve $y^2 = \prod_{i=1}^{2g+1}(x - a_i)$ over $k := \mathbb{Q}(a_1, \ldots, a_{2g+1})$, where the a_i are indeterminates, and that C is embedded in J using the Weierstrass point ∞. By [A'C79, Theorem 1], the geometric monodromy group contains $\ker(\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}))$. For $n \geq 1$, let I_n be the image of the geometric monodromy group in $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$. Suppose that $n = 2^e m$ where $e \in \mathbb{Z}_{\geq 0}$ and m is odd. Strong approximation [Kne65, Satz 2] for $\mathrm{Sp}_{2g}(\mathbb{Z})$ shows that $I_n = I_{2^e} \times I_m$, where I_{2^e} contains diagonal matrices mapping the first standard basis element of $(\mathbb{Z}/2^e\mathbb{Z})^{2g}$ to any odd multiple, and I_m contains $\mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, which acts transitively on points of exact order m.

Now suppose that $P \in C(\overline{k})$ is a torsion point of exact order n. Then P is the first vector in a $\mathbb{Z}/n\mathbb{Z}$-basis of $J[n]$, say $P, Q, \ldots$. Decompose P as $P_{2^e} + P_m$ where $P_{2^e} \in J[2^e]$ and $P_m \in J[m]$. Decompose Q similarly as $Q_{2^e} + Q_m$. Then we may find elements of I_n mapping $P = P_{2^e} + P_m$ to $R_1 := P_{2^e} + Q_m$, $R_2 := P_{2^e} + 2P_m$, and $R_3 := P_{2^e} + (P_m + Q_m)$. Then $P + R_3 - R_1 - R_2$, viewed as a divisor on $C_{\overline{k}}$, is principal. If $m \geq 3$, then P, R_1, R_2, R_3 are all distinct, so the corresponding rational function is of degree 2, which implies that its divisor is fixed by the hyperelliptic involution, a contradiction. Thus $m = 1$, so $n = 2^e$. If $e \geq 3$, then we may find elements of I_n mapping P to $S_1 := (2^{e-2} + 1)P$, $S_2 := (2 \cdot 2^{e-2} + 1)P$, and $S_3 := (3 \cdot 2^{e-2} + 1)P$, and then the divisor $P + S_1 - S_2 - S_3$ yields a contradiction as before. Thus $e \leq 2$, so $n \leq 4$.

Now $nP - n\infty$ is the divisor of some $h \in \overline{k}[x] + \overline{k}[x]y$. The valuation v at ∞ satisfies $v(x) = -2$ and $v(y) = -(2g+1) < -4$, so $h \in \overline{k}[x]$. Thus the hyperelliptic involution fixes h, so it fixes $nP - n\infty$, so it fixes P. In other words, P is a Weierstrass point. □

Remark 7.3. Our application to 2-adic Chabauty needs to consider only torsion points P of odd order n in Theorem 7.1. There is a simpler proof in this special case: the point $Q := 2P$ is a Galois conjugate of P, and the divisor $Q + \infty - 2P$ is principal.

8. Families of curves and Jacobians

8.1. **Abelian scheme over a p-adic variety.** Let M be a smooth variety over $\mathbb{Q}_p$. Let $\mathscr{J} \to M$ be an abelian scheme. Given $m \in M(\mathbb{Q}_p)$, let $\mathscr{J}_m$ be the fiber, an abelian variety over $\mathbb{Q}_p$. If $\Omega^1_{\mathscr{J}/M}$ is a free $\mathscr{O}_{\mathscr{J}}$-module with basis $\omega_1, \dots, \omega_g$, then fiberwise integration of these 1-forms defines a local diffeomorphism $\mathrm{Log}\colon \mathscr{J}(\mathbb{Q}_p) \to \mathbb{Q}_p^g \times M(\mathbb{Q}_p)$ that is fiberwise the homomorphism log of Section 4.

Definition 8.1. For an open subset $U \subseteq M(\mathbb{Q}_p)$, let $\mathscr{J}(\mathbb{Q}_p)_U$ be its inverse image in $\mathscr{J}(\mathbb{Q}_p)$. By a trivialization of $\mathscr{J}(\mathbb{Q}_p) \to M(\mathbb{Q}_p)$ above U, we mean a diffeomorphism

$$\tau\colon \mathscr{J}(\mathbb{Q}_p)_U \to (\mathbb{Z}_p^g \times F) \times U$$

over U, for some finite abelian group F, such that

- for each $m \in U$, the fiber $\tau_m\colon \mathscr{J}_m(\mathbb{Q}_p) \to \mathbb{Z}_p^g \times F$ is an isomorphism of p-adic Lie groups, and
- after replacing M by a Zariski open subset whose set of $\mathbb{Q}_p$-points still contains U, the composition of τ with the projection to $\mathbb{Z}_p^g \times U$ agrees with a map Log defined as above.

Proposition 8.2. *The base $M(\mathbb{Q}_p)$ can be covered by open subsets U above which $\mathscr{J}(\mathbb{Q}_p) \to M(\mathbb{Q}_p)$ can be trivialized.*

Proof. Since $\mathscr{J} \to M$ is an abelian scheme, $\Omega^1_{\mathscr{J}/M}$ is trivialized on the preimages of some Zariski open sets covering M. Thus we may reduce to the case that $\Omega^1_{\mathscr{J}/M}$ is free. Choose a basis to define Log.

Let $m_0 \in M(\mathbb{Q}_p)$. Change the basis above so that $\mathrm{Log}(\mathscr{J}_{m_0}(\mathbb{Q}_p)) = \mathbb{Z}_p^g$. Since $\mathscr{J}(\mathbb{Q}_p) \to M(\mathbb{Q}_p)$ is a proper and open map, for each compact open subgroup $H \leq \mathbb{Q}_p^g$, the locus of $m \in M(\mathbb{Q}_p)$ such that $\mathrm{Log}(\mathscr{J}_m(\mathbb{Q}_p)) \subseteq H$ is open and closed. The same is true for the locus where $\mathrm{Log}(\mathscr{J}_m(\mathbb{Q}_p))$ *equals* H, because a subgroup of $\mathbb{Q}_p^g$ equals H if and only if it is contained in H and not contained in any of the finitely many maximal subgroups of H. In particular, we can find an open neighborhood U of m_0 in $M(\mathbb{Q}_p)$ such that $\mathrm{Log}(\mathscr{J}(\mathbb{Q}_p)_U) = \mathbb{Z}_p^g \times U$. Since Log is a local diffeomorphism, after shrinking U, we can find analytic sections $s_1, \dots, s_g$ of $\mathscr{J}(\mathbb{Q}_p)_U \to U$ such that $\mathrm{Log}\big(s_i(U)\big) = \{e_i\} \times U$ for each i, with e_i the standard basis vector. Each group $\mathscr{J}_m(\mathbb{Q}_p)$ factors canonically as a finitely generated $\mathbb{Z}_p$-module and a prime-to-p finite group; if we replace each s_i by its projection onto the $\mathbb{Z}_p$-module, fiberwise, then we may define a fiberwise $\mathbb{Z}_p$-module homomorphism $\phi\colon \mathbb{Z}_p^g \times U \to \mathscr{J}(\mathbb{Q}_p)_U$ sending e_i to s_i.

The map from the torsion locus $\mathscr{J}(\mathbb{Q}_p)_{\mathrm{tors}} = \mathrm{Log}^{-1}(\{0\} \times M(\mathbb{Q}_p))$ to $M(\mathbb{Q}_p)$ is proper (since $\mathscr{J}(\mathbb{Q}_p) \to M(\mathbb{Q}_p)$ is proper) and a local diffeomorphism (since Log is), so it is a locally constant family of finite abelian groups over $M(\mathbb{Q}_p)$. Shrink U so that this family is constant,

say equal to F, above U. Thus we obtain a fiberwise homomorphism $\psi\colon F \times U \to \mathscr{J}(\mathbb{Q}_p)_U$. The product of ϕ and ψ (over U) is a fiberwise isomorphism $(\mathbb{Z}_p^g \times F) \times U \to \mathscr{J}(\mathbb{Q}_p)_U$ whose inverse is a trivialization τ above U. □

8.2. **The universal family of hyperelliptic curves.** Recall from Section 2 the notation $\mathcal{F}_g(R)$ for the set of all nice hyperelliptic curves of odd degree and genus g in standard form with coefficients in R. Let $\mathcal{M}$ be the moduli space over $\mathbb{Q}$ such that $\mathcal{M}(k) = \mathcal{F}_g(k)$ for each field extension $k/\mathbb{Q}$; more precisely, $\mathcal{M}$ is the complement of the discriminant locus $\Delta = 0$ in $\mathbb{A}^{2g+1}$. Then $\mathcal{F}_g(\mathbb{Z}_p) = \mathbb{Z}_p^{2g+1} \cap \mathcal{M}(\mathbb{Q}_p)$. Endow $\mathcal{F}_g(\mathbb{Z}_p)$ with the Haar measure from $\mathbb{Z}_p^{2g+1}$. By a congruence class in $\mathcal{F}_g(\mathbb{Z}_p)$, we mean a coset U of $(p^e\mathbb{Z}_p)^{2g+1}$ in $\mathbb{Z}_p^{2g+1}$ with $U \subseteq \mathcal{F}_g(\mathbb{Z}_p)$; for such U, the density of $\mathcal{F}_g \cap U$ equals the measure of U.

Let $\pi\colon \mathscr{C} \to \mathcal{M}$ be the universal curve; π is a smooth proper morphism whose fibers are nice hyperelliptic curves of genus g. Its relative Jacobian is an abelian scheme $\mathscr{J} \to \mathcal{M}$ [BLR90, p. 260, Proposition 4]. Call a congruence class $U \subseteq \mathcal{F}_g(\mathbb{Z}_p)$ trivializing if $\mathscr{J}(\mathbb{Q}_p) \to \mathcal{M}(\mathbb{Q}_p)$ is trivialized above U.

Lemma 8.3. *Any open subset of $\mathcal{F}_g(\mathbb{Z}_p)$ is a disjoint union of trivializing congruence classes.*

Proof. The congruence classes in $\mathcal{F}_g(\mathbb{Z}_p)$ form a basis for its topology. By Proposition 8.2, the same is true for the trivializing congruence classes. Thus any open subset V of $\mathcal{F}_g(\mathbb{Z}_p)$ is a union of trivializing congruence classes U_i. If two congruence classes meet, then one contains the other. Thus V is the disjoint union of the U_i not contained in a larger one. □

Proposition 8.4. *The density of $C \in \mathcal{F}_g$ such that $J(\mathbb{Q})_{\mathrm{tors}} \neq 0$ is zero.*

Proof. By Lemma 8.3, there is a finite disjoint union $\mathcal{U}$ of trivializing congruence classes U such that the measure of $\mathcal{U}$, or equivalently the density of $\mathcal{F}_g \cap \mathcal{U}$, is as close as desired to 1. Thus it suffices to prove the result for the $C \in \mathcal{F}_g$ belonging to one trivializing congruence class U. For such C, the size of $J(\mathbb{Q}_p)_{\mathrm{tors}}$ is constant, say n. The monodromy action does not fix any nonzero torsion point on the geometric generic fiber of $\mathscr{J} \to \mathcal{M}$, so the Hilbert irreducibility theorem shows that the density of such C such that $J(\mathbb{Q})$ has a nonzero point of order dividing n is zero. □

Using the section $\infty\colon \mathcal{M} \to \mathscr{C}$, we identify $\mathscr{C}$ with a closed subscheme of $\mathscr{J}$. Let $\mathscr{W} \hookrightarrow \mathscr{C}$ be the locus of Weierstrass points. Then $\mathscr{W}$ is Zariski open and closed in $\mathscr{J}[2]$. Let Z be the set of $m \in \mathcal{F}_g(\mathbb{Z}_p)$ such that $\mathscr{C}_m(\mathbb{Q}_p) \cap \mathscr{J}_m(\mathbb{Q}_p)_{\mathrm{tors}}$ is *not* contained in $\mathscr{W}_m(\mathbb{Q}_p)$.

Proposition 8.5. *The set Z is closed in $\mathcal{F}_g(\mathbb{Z}_p)$ and is of measure zero.*

Proof. By Lemma 8.3 applied to $\mathcal{F}_g(\mathbb{Z}_p)$, we may restrict attention to a trivializing congruence class U. Let n be the constant value of $\#\mathscr{J}_m(\mathbb{Q}_p)_{\mathrm{tors}}$ for $m \in U$. Let Z' be the image of the $\mathbb{Q}_p$-points under the restriction $\pi_n\colon \mathscr{C} \cap (\mathscr{J}[n] - \mathscr{W}) \to \mathcal{M}$ of π. Then $Z \cap U = Z' \cap U$. Since $\mathscr{C} \to \mathcal{M}$ is proper and $\mathscr{J}[n] \setminus \mathscr{W} \to \mathcal{M}$ is finite étale, the morphism π_n is proper, so Z' is closed. By Theorem 7.1, π_n is not dominant, so Z' is of measure zero. □

Corollary 8.6. *The set of $C \in \mathcal{F}_g$ such that $C(\mathbb{Q}_p) \cap J(\mathbb{Q}_p)_{\mathrm{tors}}$ contains a non-Weierstrass point is of density zero.*

Proof. Apply Lemma 8.3 to $\mathcal{F}_g(\mathbb{Z}_p) \setminus Z$ to show that the complement has density 1. □

Proposition 8.7. *Let U be a trivializing congruence class. Let Z be as in Proposition 8.5. Let $U' := U \setminus Z$. Then $\rho\log(\mathscr{C}_m(\mathbb{Q}_p))$ in $\mathbb{P}^{g-1}(\mathbb{F}_p)$ is locally constant as m varies in U'.*

Proof. We have analytic maps of p-adic manifolds

$$\mathscr{C}(\mathbb{Q}_p)_{U'} \longrightarrow \mathscr{J}(\mathbb{Q}_p)_{U'} \xrightarrow{\text{Log}} \mathbb{Z}_p^g \times U' \longrightarrow \mathbb{Z}_p^g \overset{\mathbb{P}}{\dashrightarrow} \mathbb{P}^{g-1}(\mathbb{Q}_p) \xrightarrow{\rho} \mathbb{P}^{g-1}(\mathbb{F}_p), \tag{8.8}$$

except that the dashed arrow is indeterminate at 0. We resolve the indeterminacy by blowing up the first four manifolds along the inverse image of $0 \in \mathbb{Z}_p^g$. The inverse image in $\mathscr{C}(\mathbb{Q}_p)_{U'}$ is the torsion locus, which by definition of U' equals only $\mathscr{W}(\mathbb{Q}_p)_{U'}$, which is a smooth *divisor* on $\mathscr{C}(\mathbb{Q}_p)_{U'}$. Thus the blow-up of $\mathscr{C}(\mathbb{Q}_p)_{U'}$ is $\mathscr{C}(\mathbb{Q}_p)_{U'}$ itself, so (8.8) extends to a continuous map $e\colon \mathscr{C}(\mathbb{Q}_p)_{U'} \to \mathbb{P}^{g-1}(\mathbb{F}_p)$. The fibers of e are open and closed. So are their images in U' since $\mathscr{C} \to \mathcal{M}$ is smooth and proper. The locus in U' where $e(\mathscr{C}_m(\mathbb{Q}_p))$ equals a given subset of $\mathbb{P}^{g-1}(\mathbb{F}_p)$ is a finite Boolean combination of these images, hence again open and closed. Thus $e(\mathscr{C}_m(\mathbb{Q}_p))$ is locally constant as m varies in U'. Finally, $\rho\log$ is just the restriction of e to a dense open subset of $\mathscr{C}_m(\mathbb{Q}_p)$, and e is locally constant, so $\rho\log(\mathscr{C}_m(\mathbb{Q}_p)) = e(\mathscr{C}_m(\mathbb{Q}_p))$. □

Remark 8.9. The set $\rho\log(\mathscr{C}_m(\mathbb{Q}_p))$ is generally *not* locally constant in a neighborhood of points of Z.

8.3. **Equidistribution of Selmer elements.** Let U be a trivializing congruence class. If $m \in \mathcal{F}_g \cap U$, the trivialization lets us construct the diagram (6.1) for $C := \mathscr{C}_m$ and $J := \mathscr{J}_m$; in particular, we obtain $\sigma\colon \operatorname{Sel}_p J \to \mathbb{F}_p^g$.

For each $g \geq 1$ and prime p, we may now formulate the following equidistribution conjecture, compatible with both the heuristics in [PR12] and the theorems for $p = 2$ in [BG13].

Conjecture $\operatorname{Eq}_g(p)$**.** For any trivializing congruence class U and any $w \in \mathbb{F}_p^g$, the average size of $\{s \in \operatorname{Sel}_p J \setminus \{0\} : \sigma(s) = w\}$ as C varies in $\mathcal{F}_g \cap U$ is p^{1-g}.

Theorem 8.10. *For each $g \geq 1$, $\operatorname{Eq}_g(2)$ holds.*

Proof. By [BG13, Theorem 11.1] (adapted as in Remark 8.11 below), the average size of $\operatorname{Sel}_2 J \setminus \{0\}$ for $C \in \mathcal{F}_g \cap U$ is 2. The trivialization identifies each group $J(\mathbb{Q}_2)$ with a fixed group $\mathbb{Z}_2^g \times F$, and [BG13, Theorem 12.4] states that the images of the nonzero Selmer elements under $\operatorname{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \mathbb{F}_2^g \times F/2F$ are equidistributed in $\mathbb{F}_2^g \times F/2F$, so their images under the projection to $\mathbb{F}_2^g$ are equidistributed too. Thus on average there are $2/\#\mathbb{F}_2^g = 2^{1-g}$ nonzero Selmer elements mapping to a given element of $\mathbb{F}_2^g$. □

Remark 8.11. Let $\mathcal{F}_g'$ be the subset of $\mathcal{F}_g$ where $a_1 = 0$, and let $\mathcal{F}_g''$ be the subset of $\mathcal{F}_g'$ where there is no prime p with $p^{2m} \mid a_m$ for all m. The paper [BG13] works not with $\mathcal{F}_g$, but with $\mathcal{F}_g''$. Here we explain how to transfer the equidistribution results from $\mathcal{F}_g''$ to $\mathcal{F}_g$.

First, given subsets

$$B_\infty := [b_2, b_2'] \times \cdots \times [b_{2g+1}, b_{2g+1}'] \subseteq \mathbb{R}^{2g},$$

and B_p a coset of a finite-index subgroup of $\mathbb{Z}_p^{2g}$ for p in some finite set S, call $B := B_\infty \times \prod_{p \in S} B_p$ a box. For $X > 0$, consider the curves in $\mathcal{F}_g'$ whose coefficient tuple satisfies $[a_2/X^2, \ldots, a_{2g+1}/X^{2g+1}] \in B_\infty$ and $(a_2, \ldots, a_{2g}) \in B_p$ for all $p \in S$. The arguments of [BG13] carry over essentially without change to prove equidistribution of Selmer elements for such curves as $X \to \infty$. By taking finite linear combinations, one obtains a variant that counts the same curves but with a weight that is a step function that is finitely piecewise constant on sub-boxes of B. Now if w is any bounded weight function on B such for every $\epsilon > 0$, there is a step function s as above such that $|w - s| \leq \epsilon$ outside a finite union of

sub-boxes that has total measure less than ϵ, then by comparing with s and taking the limit as $\epsilon \to 0$, we can count both curves and Selmer elements weighted according to w. In particular, for nonnegative w bounded below by a positive constant on some sub-box, we can deduce an analogous Selmer equidistribution result.

Let S be a finite set of primes including those dividing $2g+1$. The "complete the $(2g+1)^{\text{st}}$ power and scale" map sending $f(x)$ to $(2g+1)^{2g+1} f((x-a_1)/(2g+1))$ defines a map on coefficient tuples from $[-1,1]^{2g+1} \times \prod_{p \in S} \mathbb{Z}_p^{2g+1}$ into some box B, and the pushforward of the uniform measure is a weight function w as above. The corresponding map from $\mathcal{F}_{g,X}$ to $\mathcal{F}'_g$ has fibers whose size is approximately proportional to w at the corresponding $f \in \mathcal{F}'_g$, normalized, so the limit of the average for $\mathcal{F}_g$ equals the limit of the weighted average for $\mathcal{F}'_g$. (One can also impose finitely many congruence conditions by replacing each $\mathbb{Z}_p^{2g+1}$ by a coset of a finite-index subgroup.)

Remark 8.12. Although $\mathrm{Eq}_g(p)$ is about p-adic equidistribution of p-Selmer elements, one could also ask about v-adic equidistribution of p-Selmer elements for any place v of $\mathbb{Q}$. In fact, [BG13, Theorem 12.4] proves v-adic equidistribution of 2-Selmer elements for all v, and can even handle finitely many v simultaneously.

8.4. **A general density result.**

Proposition 8.13. *Let U be a trivializing congruence class such that the subset $\rho \log(\mathscr{C}_m(\mathbb{Q}_p))$ of $\mathbb{P}^{g-1}(\mathbb{F}_p)$ is constant for $m \in U$, say equal to I. Then, for $C \in \mathcal{F}_g \cap U$ outside a subset of relative upper density at most $(1+\#I)p^{1-g}$, we have:*

(i) *if $p=2$, then $C(\mathbb{Q}) = C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} = \{\infty\}$.*

(ii) *if $p>2$ and $\mathrm{Eq}_g(p)$ holds, then $C(\mathbb{Q}) = \{\infty\}$ and $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ consists of Weierstrass points.*

Proof. By Theorem 8.10, $\mathrm{Eq}_g(2)$ holds; if $p>2$, assume $\mathrm{Eq}_g(p)$. Then for $C \in \mathcal{F}_g \cap U$, the average number of nonzero elements of $\mathrm{Sel}_p J$ mapped by σ to 0 is p^{1-g}, so the relative upper density of C having such a Selmer element is at most p^{1-g}. Similarly, the average number of nonzero elements of $\mathrm{Sel}_p J$ mapped by $\mathbb{P}\sigma$ into I is $(p-1)\#I p^{1-g}$, but each curve with such an element has at least $p-1$ such elements (its nonzero multiples), so the relative upper density of such curves is at most $\#I p^{1-g}$. Together, these have relative upper density at most $(1+\#I)p^{1-g}$, and this is unchanged if we include the density zero sets of Proposition 8.4 and Corollary 8.6.

For the *other* $C \in \mathcal{F}_g \cap U$, Proposition 6.2 states that $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subseteq J(\mathbb{Q}_p)[p']$. Since we excluded the set of Corollary 8.6, $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ consists of Weierstrass points. For $p=2$, these together imply $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = \{\infty\}$. For all p, our exclusion of the set of Proposition 8.4 implies $C(\mathbb{Q}) = \{\infty\}$. □

Remark 8.14. By Lemma 8.3 and Proposition 8.7, there is a disjoint union of sets U satisfying the hypothesis of Proposition 8.13 and having total measure 1.

Remark 8.15. We expect that for $p>2$, there is a positive density of $C \in \mathcal{F}_g$ such that $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is strictly larger than $\{\infty\}$. The reason is that we expect that there is a positive density of C such that C has good reduction at p, there is a Weierstrass point $W \in C(\mathbb{Q}_p) \setminus C(\mathbb{Q})$, and there is a point $P \in J(\mathbb{Q})$ with the same reduction as W. For such curves, $p^n P \to W$ as $n \to \infty$, so $W \in C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$.

9. Average number of residue disks

In this section, we fix $g \geq 1$ and a prime p. For a random $C \in \mathcal{F}_g(\mathbb{Z}_p)$, let $\mathcal{C}$ be its minimal proper regular model. The main goal of this section is the following.

Theorem 9.1. *We have* $\mathbf{E}\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p) \leq p+1$.

Because it is difficult to construct $\mathcal{C}$ explicitly, we construct a model with a weaker property. Call a $\mathbb{Z}_p$-model $\mathcal{D}$ of C decent if $\mathcal{D}$ is proper over $\mathbb{Z}_p$ and the image of $C(\mathbb{Q}_p) = \mathcal{D}(\mathbb{Z}_p) \to \mathcal{D}(\mathbb{F}_p)$ is contained in $\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$.

Lemma 9.2. *If $\mathcal{D}$ is decent, then $\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p) \leq \#\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$.*

Proof. Let $\pi\colon \mathcal{E} \to \mathcal{D}$ be the minimal desingularization of $\mathcal{D}$; this is an isomorphism above $\mathcal{D}^{\mathrm{smooth}}$. Also, if $e \in \mathcal{E}^{\mathrm{smooth}}(\mathbb{F}_p)$, then e is the reduction of a point in $C(\mathbb{Q}_p)$ by Hensel's lemma, and $\mathcal{D}$ is decent, so $\pi(e) \in \mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$. Thus π defines a bijection $\mathcal{E}^{\mathrm{smooth}}(\mathbb{F}_p) \to \mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$. On the other hand, $\mathcal{E} \to \mathcal{C}$ factors as a sequence of blow-ups at closed points [Lic68, II.A, Theorem 1.15], and each blow-up morphism is surjective on $\mathbb{F}_p$-points. □

By Lemma 9.2, to prove Theorem 9.1 it suffices to construct a decent model $\mathcal{D}$ of each $C \in \mathcal{F}_g(\mathbb{Z}_p)$ and to prove $\mathbf{E}\#\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p) \leq p+1$. We use the following recursive algorithm to construct $\mathcal{D}$.

Algorithm `MakeDecentModel`(C).
Input: A curve $C\colon y^2 = f(x)$ in $\mathcal{F}_g(\mathbb{Z}_p)$.

1. Let $\mathcal{D}$ be the standard compactification of $y^2 = f(x)$ over $\mathbb{Z}_p$.
2. Let U be the closed subscheme $y^2 = f(x)$ of $\mathbb{A}^2_{\mathbb{Z}_p}$ with its open immersion into $\mathcal{D}$.
3. Modify $\mathcal{D}$ by running `Fix`(U) below.

Subroutine `Fix`(U).
Input: A closed subscheme $U\colon y^2 = h(x)$ of $\mathbb{A}^2_{\mathbb{Z}_p}$ with an open immersion into $\mathcal{D}$.

1. Replace $\mathcal{D}$ by its blow-up at the set of non-regular $\mathbb{F}_p$-points of U.
2. For each $c \in \{0, 1, \dots, p-1\}$, if $p \mid h'(c)$ and $p^2 \mid h(c)$, then let U_c be $y^2 = p^{-2}h(c+px)$, which is an affine patch of the blown-up $\mathcal{D}$, and run `Fix`(U_c). (These processes for different c may be run independently without interference, since the special fibers of the U_c have disjoint images in $\mathcal{D}$.)

Lemma 9.3. *Algorithm* `MakeDecentModel`(C) *terminates and yields a decent model $\mathcal{D}$ of C.*

Proof. If the recursion reaches nesting depth n (where the initial call to `Fix`(U) is nesting depth 0), then the composition of the changes of variable $x \mapsto c+px$ is of the form $x \mapsto d+p^n x$ for some $d \in \{0, 1, \dots, p^n - 1\}$ such that $p^{-2n} f(d + p^n x) \in \mathbb{Z}_p[x]$, and hence $f(d) \in p^{2n}\mathbb{Z}_p$ and $f'(d) \in p^n\mathbb{Z}_p$. Thus if the nesting is unbounded, compactness yields $d \in \mathbb{Z}_p$ such that $f(d) = f'(d) = 0$, contradicting the definition of $\mathcal{F}_g(\mathbb{Z}_p)$. Hence the algorithm terminates.

Suppose that $P \in C(\mathbb{Q}_p)$. If $x(P) \notin \mathbb{Z}_p$, then P reduces to the smooth point ∞ on the special fiber of $\mathcal{D}$. Otherwise, P belongs to $U(\mathbb{Z}_p)$ for the initial U. Consider the *last* time `Fix`(U) is called with a U such that $P \in U(\mathbb{Z}_p)$. Without loss of generality, make a change of variables $x \mapsto x + c$ to assume that P reduces to a point in $U(\mathbb{F}_p)$ with $x = 0$. Let $a = h(0)$ and $b = h'(0)$.

(1) Suppose $p \nmid b$. Then U is smooth at the $\mathbb{F}_p$-points with $x = 0$ (the x-derivative is nonzero).
(2) Suppose $p \mid b$.
  (a) Suppose $p \nmid a$.
    (i) Suppose $p \neq 2$. Then U is smooth at the $\mathbb{F}_p$-points with $x = 0$ (the y-derivative is nonzero).
    (ii) Suppose $p = 2$. Then U is isomorphic to $y^2 + 2y = (a-1) + bx + \cdots$, and has a unique $\mathbb{F}_2$-point u with $x = 0$.
      (A) If $a \equiv 3 \pmod 4$, then U is regular but not smooth at u, so P could not have existed.
      (B) If $a \equiv 1 \pmod 4$, then U is not regular at u, so u was blown up in Step 1 of `Fix`(U); then P corresponds to a $\mathbb{Z}_2$-point of the affine patch $U'\colon y^2 + y = a' + b'x + \cdots$ of the blow-up obtained by making the change of variable $(x, y) \mapsto (2x, 2y)$ and dividing by 2^2; this entire patch is smooth (the y-derivative is nonvanishing).
  (b) Suppose $p \mid a$ but $p^2 \nmid a$. Then U is regular but not smooth at the unique $\mathbb{F}_p$-point with $x = 0$ (the origin), so P could not have existed.
  (c) Suppose $p^2 \mid a$. Then in Step 2 of `Fix`(U), we would have called `Fix`(U_0) for U_0 such that $P \in U_0(\mathbb{Z}_p)$, contradicting the assumption on U. □

Construct $\mathcal{D}$ by algorithm `MakeDecentModel`. For $n \geq 0$, let $\overline{\mathcal{H}}_n$ be the set of polynomials

$$f(x) := p^{(2g-1)n}x^{2g+1} + p^{(2g-2)n}a_{2g}x^{2g} + \cdots + p^n a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

with $a_0, \ldots, a_{2g} \in \mathbb{Z}_p$, and let $\mathcal{H}_n$ be the (full measure) subset with nonzero discriminant. Identify each $f \in \mathcal{H}_n$ with the standard compactification of $y^2 = f(x)$ over $\mathbb{Q}_p$; for example, $\mathcal{H}_0 \simeq \mathcal{F}_g(\mathbb{Z}_p)$. Let $\overline{\mathcal{S}}_n := \{h \in \overline{\mathcal{H}}_n : p \mid a_1 \text{ and } p^2 \mid a_0\}$; define $\mathcal{S}_n$ similarly. The bijection $\overline{\mathcal{S}}_n \to \overline{\mathcal{H}}_{n+1}$ sending $h(x)$ to $p^{-2}h(px)$ respects addition, so it respects Haar measure (up to normalization). Thus, by induction on n, inside a call to subroutine `Fix`(U) at nesting depth n arising from a sequence of choices $c_1, \ldots, c_n$ in Step 2 of earlier calls, the distribution of h is uniform over $\mathcal{H}_n$. Let X_n be the random variable on $\mathcal{H}_n$ that counts the number of smooth $\mathbb{F}_p$-points of the final $\mathcal{D}$ lying above $\mathbb{F}_p$-points in this U having $x = 0$; if we replaced 0 by any other $c \in \{0, 1, \ldots, p-1\}$, the distribution of values would be the same.

Lemma 9.4. *For $n \geq 0$, the restriction $X_n|_{\mathcal{S}_n}$ is the sum of p random variables, each of which has the same distribution of values on $\mathcal{S}_n$ as X_{n+1} has on $\mathcal{H}_{n+1}$.*

Proof. For $h \in \mathcal{S}_n$, Step 2 of `Fix`(U) leads to $U'\colon y^2 = p^{-2}h(px)$, and the points of $\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$ lying above points in U with $x = 0$ are all those lying above U'. The number of these whose image in U' has a particular x-coordinate in $\mathbb{F}_p$ is distributed like X_{n+1} on $\mathcal{H}_{n+1}$. □

Lemma 9.5. *For $n \geq 0$, we have $\mathbf{E}X_n = 1$.*

Proof. We divide $\mathcal{H}_n$ into subsets corresponding to the cases in the proof of Lemma 9.3. For each case, we compute its probability, and the average contribution to X_n conditioned on being in that case:

Case	Probability	Average contribution to X_n
(1)	$1-p^{-1}$	1
(2)(a)	$p^{-1}-p^{-2}$	1
(2)(b)	$p^{-2}-p^{-3}$	0
(2)(c)	p^{-3}	sum of p copies of X_{n+1}.

Let us explain the entries in the last column. In case (1), the smooth $\mathbb{F}_p$-points of U with $x=0$ correspond to square roots of a uniformly random element of $\mathbb{F}_p$; the expected number of square roots is 1. In case (2)(a) for $p\neq 2$, the contribution is the expected number of square roots of a random element of $\mathbb{F}_p^\times$, which is again 1. In case (2)(a) for $p=2$, in subcase (A) the contribution is 0 (we are counting smooth $\mathbb{F}_p$-points), while in subcase (B) the average contribution is 2 since each point of $\mathbb{A}^2(\mathbb{F}_p)$ has a 1/2 chance of lying in $U'(\mathbb{F}_p)$; thus the overall average contribution in case (2)(a) for $p=2$ is again 1. In case (2)(b), the contribution is 0. Case (2)(c) corresponds to $\mathcal{S}_n$, so we use Lemma 9.4. Moreover, the analysis shows that $X_n\leq 4$ outside of case (2)(c).

The upshot is that X_n is given by a process whose parameters are independent of n; it would be a Bienaymé–Galton–Watson process if the p random variables in Lemma 9.4 were independent (they are generally not). For real $B>4$, the only way that $X_n\geq B$ can hold is if we are in case (2)(c) and one of the p copies of X_{n+1} exceeds B/p; thus $\mathbf{P}(X_n\geq B)\leq p^{-3}p\,\mathbf{P}(X_{n+1}\geq B/p)$. Iterate this k times, where k is the first integer with $B/p^k\leq 4$, to obtain

$$\mathbf{P}(X_n\geq B)\;\leq\; p^{-2k}\,\mathbf{P}(X_{n+k}\geq B/p^k)\;\leq\; p^{-2k}\;=\;O(B^{-2}).$$

Thus the average $\mathbf{E}X_n=\sum_{B=1}^\infty \mathbf{P}(X_n\geq B)$ is finite and bounded independently of n. The table implies that

$$\mathbf{E}X_n=(1-p^{-1})\cdot 1+(p^{-1}-p^{-2})\cdot 1+(p^{-2}-p^{-3})\cdot 0+p^{-3}(p\cdot\mathbf{E}X_{n+1}).$$

By induction on k, we obtain $\mathbf{E}X_n=1-p^{-2k}+p^{-2k}\cdot\mathbf{E}X_{n+k}$. Taking the limit as $k\to\infty$ yields $\mathbf{E}X_n=1$. □

Lemma 9.6. *We have* $\mathbf{E}\#\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)=p+1$.

Proof. First, $\mathcal{D}$ has the smooth $\mathbb{F}_p$-point ∞ on the standard compactification. The other points of $\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)$ lie above the initial U. The average number of these lying above $\mathbb{F}_p$-points in U with $x=c$ is independent of $c\in\mathbb{F}_p$, so it equals its value for $c=0$, which by definition is $\mathbf{E}X_0$, which is 1 by Lemma 9.5. Thus $\mathbf{E}\#\mathcal{D}^{\mathrm{smooth}}(\mathbb{F}_p)=1+\sum_{c\in\mathbb{F}_p}1=p+1$. □

This completes the proof of Theorem 9.1.

Remark 9.7. One can show that there is a positive probability that the morphism $\mathcal{E}\to\mathcal{C}$ in the proof of Lemma 9.2 involves blowing up a smooth $\mathbb{F}_p$-point; thus $\mathbf{E}\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)<p+1$.

Remark 9.8. On the other hand, at least for $p>2$, one can show that a random $C\in\mathcal{F}_g$ *with good reduction* has $\mathbf{E}\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)=p+1$. (This is because all such C arise from a curve in $\mathcal{F}_g$ with discriminant in $\mathbb{Z}_p^\times$ by a substitution $x\mapsto d+p^nx$ for a uniquely determined $n\geq 0$ and $d\in\{0,1,\ldots,p^n-1\}$, and the expected value of $C(\mathbb{F}_p)$ for $C\in\mathcal{F}_g(\mathbb{F}_p)$ is $p+1$, as one sees by grouping each C with its quadratic twist.) Thus one has the counterintuitive fact that on average, curves with bad reduction have fewer smooth $\mathbb{F}_p$-points than curves with good reduction!

Remark 9.9. The argument proving Theorem 9.1 proves $\mathbf{E}\#\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p) \le p+1$ also for the random nice curve over $\mathbb{Q}_p$ given by

$$y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

for $a_0, \ldots, a_{2g+2} \in \mathbb{Z}_p$ such that the discriminant is nonzero.

Corollary 9.10. *For $C \in \mathcal{F}_g(\mathbb{Z}_p)$, the average size of $\rho\log(C(\mathbb{Q}_p))$ is at most*

$$\begin{cases} 6g+9, & \text{if } p=2, \\ \dfrac{p^2-p}{p-2}(2g-2)+(p+1)^2, & \text{if } p>2. \end{cases}$$

Proof. Combine Proposition 5.4 and Theorem 9.1. □

Remark 9.11. Working with residue disks defined in terms of decent models and making use of the fact that $\rho\log\circ\iota = \rho\log$, where ι is the hyperelliptic involution, one could improve this to $3g+9/2$ for $p=2$ and

$$\frac{p^2-p}{p-2}(g-1)+\frac{(p+1)^2}{2}$$

for $p>2$. We omit the details, since they are somewhat technical and yield only a modest improvement in our main results.

10. The main results

10.1. Positive density for $g \ge 3$.

Lemma 10.1. *Let $\mathcal{J}$ be an abelian scheme over $\mathbb{Z}_p$. Define $\log\colon \mathcal{J}(\mathbb{Q}_p) \to \mathbb{Q}_p^g$ by integrating a $\mathbb{Z}_p$-basis of $\mathrm{H}^0(\mathcal{J}, \Omega^1_{\mathcal{J}/\mathbb{Z}_p})$. If $\mathcal{J}(\mathbb{F}_p)[p]=0$ and $\mathcal{J}(\mathbb{Q}_p)[p]=0$, then $\log(\mathcal{J}(\mathbb{Q}_p)) = (p\mathbb{Z}_p)^g$.*

Proof. Let F be the formal group of $\mathcal{J}$ over $\mathbb{Z}_p$. For $e \ge 1$, define

$$K_e := F((p^e\mathbb{Z}_p)^g) = \ker(\mathcal{J}(\mathbb{Z}_p) \to \mathcal{J}(\mathbb{Z}/p^e\mathbb{Z})).$$

Since K_1 is a pro-p-group and $\mathcal{J}(\mathbb{Q}_p)[p]=0$, we have $(K_1)_{\mathrm{tors}}=0$. Thus $\log|_{K_1}$ is injective. Hence for $e \ge 2$,

$$(\log K_{e-1} : \log K_e) = (K_{e-1} : K_e) = ((p^{e-1}\mathbb{Z}_p)^g : (p^e\mathbb{Z}_p)^g) = p^g.$$

Also, $p\log K_{e-1} \subseteq \log K_e$. On the other hand, $\log K_e$ is a compact open subgroup of $\mathbb{Q}_p^g$, and hence a free $\mathbb{Z}_p$-module of rank g. The previous three sentences show that $\log K_{e-1} = p^{-1}\log K_e$.

We prove that $\log K_e = (p^e\mathbb{Z}_p)^g$ for all $e \ge 1$, by reverse induction on e. For large e, we have $\log K_e = (p^e\mathbb{Z}_p)^g$ since the derivative of the composition $(p\mathbb{Z}_p)^g \longrightarrow \mathcal{J}(\mathbb{Q}_p) \xrightarrow{\log} \mathbb{Q}_p^g$ at 0 is invertible over $\mathbb{Z}_p$. The previous paragraph lets us pass from e to $e-1$.

In particular, $\log K_1 = (p\mathbb{Z}_p)^g$. Since $(\mathcal{J}(\mathbb{Q}_p) : K_1) = \#\mathcal{J}(\mathbb{F}_p)$, which is prime to p, we have $\log(\mathcal{J}(\mathbb{Q}_p)) = (p\mathbb{Z}_p)^g$ as well. □

Lemma 10.2. *For each $g>1$, there exists $C \in \mathcal{F}_g \setminus Z$ such that $\#\rho\log(C(\mathbb{Q}_2)) = 1$.*

Proof. Let $C \in \mathcal{F}_g$ be a curve isomorphic to $y^2 + y = x^{2g+1} + x + 1$. Completing the square yields a new equation for C of the form $y^2 = f(x)$. The 2-adic Newton polygon of f is a single line segment from $(0, -2)$ to $(2g + 1, 0)$, which has no interior lattice points, so f is irreducible over $\mathbb{Q}_2$. Elements of $J(\overline{\mathbb{Q}}_2)[2]$ correspond to partitions of the set of zeros of f into two parts, but only the trivial partition is $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-invariant, so $J(\mathbb{Q}_2)[2] = 0$.

The curve C has good reduction at 2. Let $\mathcal{C}$ and $\mathcal{J}$ be the smooth proper models of C and J over $\mathbb{Z}_2$. The hyperelliptic involution of $\mathcal{C}_{\mathbb{F}_2}$ is $(x, y) \mapsto (x, y + 1)$, which fixes only ∞; this implies that $\mathcal{J}(\overline{\mathbb{F}}_2)[2] = 0$, so $\mathcal{J}(\mathbb{F}_2)[2] = 0$. Lemma 10.1 implies that a basis of $\mathrm{H}^0(\mathcal{J}, \Omega^1_{\mathcal{J}/\mathbb{Z}_2})$ defines log such that $\log(J(\mathbb{Q}_2)) = (2\mathbb{Z}_2)^g$. We may divide by 2 if desired to make $\log(J(\mathbb{Q}_2)) = \mathbb{Z}_2^g$, but this will not change the map $\rho \log$.

The change of variable $s := 1/x$ and $t := y/x^{g+1}$ rewrites the equation of $\mathcal{C}$ as

$$t^2 + s^{g+1}t = s^{2g+2} + s^{2g+1} + s,$$

with ∞ corresponding to $(0, 0)$ in the new model. Let

$$\omega_1 := \frac{dt}{-(g+1)s^g t + (2g+2)s^{2g+1} + (2g+1)s^{2g} + 1},$$

the denominator being a partial derivative of the curve equation. Then $\omega_j := s^{j-1}\omega_1$ for $j = 1, \dots, g$ form a basis for $\mathrm{H}^0(\mathcal{C}, \Omega^1_{\mathcal{C}/\mathbb{Z}_2})$. We have $\mathcal{C}(\mathbb{F}_2) = \{\infty\}$, so there is just one residue disk, and t is a uniformizer for it. Expanding in power series in t, we find $s = t^2 + t^{2g+3} + \cdots$, $\omega_1 = (1 + 0t + \cdots)\, dt$, and $\omega_j = (t^{2j-2} + \cdots)\, dt$ for $j = 1, \dots, g$, with all coefficients in $\mathbb{Z}_2$. Integrating yields

$$\boldsymbol{\ell}(t) = (t + 0t^2 + \cdots, t^3/3 + \cdots, \cdots, t^{2g-1}/(2g+1) + \cdots).$$

After removing the common factor of t, for $t \in 2\mathbb{Z}_2$ each summand on the right is in $2\mathbb{Z}_2$ except the initial 1; thus $\rho(\boldsymbol{\ell}(t)) = (1 : 0 : \cdots : 0)$ for all nonzero $t \in 2\mathbb{Z}_2$. Hence $\rho \log(C(\mathbb{Q}_2)) = \{(1 : 0 : \cdots : 0)\}$. The computation shows also that the only zero of log on $C(\mathbb{Q}_2)$ is ∞, so $C(\mathbb{Q}_2) \cap J(\mathbb{Q}_2)_{\mathrm{tors}} = \{\infty\}$, so $C \notin Z$. □

Theorem 10.3. *Fix $g \geq 3$. The lower density of the set of curves $C \in \mathcal{F}_g$ satisfying $C(\mathbb{Q}) = C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} = \{\infty\}$ is positive.*

Proof. Proposition 8.7 yields $U \subseteq \mathcal{F}_g(\mathbb{Z}_p) \setminus Z$ containing the curve of Lemma 10.2 and satisfying the hypothesis of Proposition 8.13. By Proposition 8.13, $C(\mathbb{Q}) = C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} = \{\infty\}$ for $C \in \mathcal{F}_g \cap U$ outside a subset of relative upper density at most $2 \cdot 2^{1-g} < 1$. □

Remark 10.4. The density of U will be rather small, so the lower bound on the lower density of curves with just one rational point we obtain in this way will also be very small.

Remark 10.5. Although Theorem 10.3 says nothing for $g = 2$, $\mathrm{Eq}_2(3)$ would imply that the lower density of the set of $C \in \mathcal{F}_2$ satisfying $C(\mathbb{Q}) = \{\infty\}$ is positive. This implication can be proved by a similar argument, using curves 3-adically close to $y^2 = x^5 - x^3 - 1$.

10.2. **Density tending to 1.**

Theorem 10.6. *Fix $g > 1$. Then the lower density of the set of curves $C \in \mathcal{F}_g$ satisfying $C(\mathbb{Q}) = C(\mathbb{Q}_2) \cap \overline{J(\mathbb{Q})} = \{\infty\}$ is at least $1 - (12g + 20)2^{-g}$.*

Proof. Apply Proposition 8.13 to each congruence class in Remark 8.14, and sum the results by using Corollary 9.10 for $p = 2$: the upper density of curves *not* satisfying the condition is at most $(1 + (6g + 9))\, 2^{1-g} = (12g + 20)2^{-g}$. □

Remark 10.7. We have $1-(12g+20)2^{-g} > 0$ if and only if $g \geq 7$. Also, $1-(12g+20)2^{-g} \to 1$ as $g \to \infty$. Using the refinement given in Remark 9.11, the bound could be improved to $1 - (6g + 11)2^{-g}$, which is positive also for $g = 6$.

Theorem 10.8. *Fix $g > 1$ and an odd prime p. Assume $\mathrm{Eq}_g(p)$. Then the lower density of the set of curves $C \in \mathcal{F}_g$ satisfying $C(\mathbb{Q}) = \{\infty\}$ is at least*

$$1 - \Big(1 + (p+1)^2 + \frac{p^2 - p}{p - 2}(2g - 2)\Big)p^{1-g}.$$

Proof. Repeat the proof of Theorem 10.6, using the bound for odd p in Proposition 5.4. □

Corollary 10.9. *Fix $g \geq 4$. Assume that $\mathrm{Eq}_g(p)$ holds for arbitrarily large primes p. Then the set of curves $C \in \mathcal{F}_g$ satisfying $C(\mathbb{Q}) = \{\infty\}$ has density 1.*

Proof. The lower bound in Theorem 10.8 tends to 1 as $p \to \infty$. □

Remark 10.10. For $g = 3$, the lower bound tends to 0 from below, but using Remark 9.11 to cut the subtracted term essentially in half, we would obtain a limit of $1/2$. Thus if $\mathrm{Eq}_3(p)$ holds for arbitrarily large primes p, then the set of curves $C \in \mathcal{F}_3$ satisfying $C(\mathbb{Q}) = \{\infty\}$ has lower density at least $1/2$.

Remark 10.11. Several authors have presented heuristics or conditional proofs that suggest that in an algebraic family of curves of genus greater than 1, the density of those having rational points other than points that exist generically is 0: see [PV04, Conjecture 2.2], [Poo06], [Gra07, Conjecture 1.3(ii)], and [Sto09, Conjecture 1].

10.3. **Effectivity.** Let $\mathcal{F}_g^{\mathrm{good}}$ be the set of $C \in \mathcal{F}_g$ such that σ is injective, the images $\rho \log(C(\mathbb{Q}_2))$ and $\mathbb{P}\sigma(\mathrm{Sel}_2 J)$ are disjoint, and $C(\mathbb{Q}_2)$ contains no nontrivial torsion point of odd order. Our proof of Theorem 10.3 (resp., Theorem 10.6) can be summarized as follows:

- if $C \in \mathcal{F}_g^{\mathrm{good}}$, then Chabauty's method at the prime 2 proves that $C(\mathbb{Q}) = \{\infty\}$;
- $\mathcal{F}_g^{\mathrm{good}}$ has positive lower density if $g \geq 3$ (resp., density at least $1 - (12g + 20)2^{-g}$ for each $g > 1$).

Theorem 10.12. *There is an algorithm that takes as input an integer $g > 1$ and a curve $C \in \mathcal{F}_g$ and decides whether or not $C \in \mathcal{F}_g^{\mathrm{good}}$.*

Proof. One such algorithm (not an especially efficient one) proceeds as follows. Let $\mathbb{Q}_2'$ be the subfield of $\mathbb{Q}_2$ consisting of elements algebraic over $\mathbb{Q}$. The advantage of $\mathbb{Q}_2'$ over $\mathbb{Q}_2$ from the algorithmic point of view is that an element of $\mathbb{Q}_2'$ can be specified exactly with a finite amount of data. On the other hand, $\mathbb{Q}_2'$ approximates $\mathbb{Q}_2$ well in the sense that $C(\mathbb{Q}_2')$ is dense in $C(\mathbb{Q}_2)$ and $J(\mathbb{Q}_2')$ is dense in $J(\mathbb{Q}_2)$.

First, use [Poo01] to compute the finite set $C(\overline{\mathbb{Q}}) \cap J(\overline{\mathbb{Q}})_{\mathrm{tors}}$. Check each of its points for membership in $C(\mathbb{Q}_2)$ to compute $\mathcal{T} := C(\mathbb{Q}_2) \cap J(\mathbb{Q}_2)_{\mathrm{tors}}$. Since $J(\mathbb{Q}_2)_{\mathrm{tors}} \subseteq J(\mathbb{Q}_2')$, we have $\mathcal{T} \subseteq C(\mathbb{Q}_2')$. If any $T \in \mathcal{T}$ is of odd order greater than 1, then return "no".

Next, use [Sto01] to compute the group $\mathrm{Sel}_2 J$, the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$, and the map between them. Compute $J(\mathbb{Q}_2)_{\mathrm{tors}}$ and its image in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. If the map $\sigma\colon \mathrm{Sel}_2 J \to$

$J(\mathbb{Q}_2)/(2J(\mathbb{Q}_2) + J(\mathbb{Q}_2)_{\mathrm{tors}}) \simeq \mathbb{F}_2^g$ is not injective, then return "no". Otherwise compute $\mathbb{P}\sigma(\mathrm{Sel}_2 J)$.

Finally, we need to compute $\rho\log(C(\mathbb{Q}_2))$. For any $P \in C(\overline{\mathbb{Q}}_2)$ and $\omega \in \mathrm{H}^0(C, \Omega^1)$, one can define the 2-adic integral $\int_\infty^P \omega \in \overline{\mathbb{Q}}_2$ (see [MP12, Section 5.1], for example). For a divisor $D = \sum n_P P \in \operatorname{Div} C_{\overline{\mathbb{Q}}_2}$, define $\int^D \omega := \sum n_P \int_\infty^P \omega$. Given $D \in \operatorname{Div} C_{\mathbb{Q}_2'} \hookrightarrow \operatorname{Div} C_{\overline{\mathbb{Q}}_2}$ and ω as above, the integral $\int^D \omega \in \mathbb{Q}_2$ can be computed to any desired precision by integrating formal power series and using the group law on J (see [MP12, Section 8.3], for example).

Choose degree 0 divisors $D_1, \dots, D_g$ on $C_{\mathbb{Q}_2'}$ representing an $\mathbb{F}_2$-basis for $J(\mathbb{Q}_2)/(2J(\mathbb{Q}_2) + J(\mathbb{Q}_2)_{\mathrm{tors}})$. Choose any $\mathbb{Q}$-basis $\omega_1', \dots, \omega_g'$ for $\mathrm{H}^0(C, \Omega^1)$, say $\omega_j' := x^{j-1}\,dx/y$. Compute the integrals $\int^{D_i} \omega_j' \in \mathbb{Q}_2$ to sufficient precision that we can find a new basis $\omega_1, \dots, \omega_g$ of $\mathrm{H}^0(C, \Omega^1)$ guaranteed to make the matrix $(\int^{D_i} \omega_j)$ lie in $\mathrm{GL}_g(\mathbb{Z}_2)$. This new basis defines a homomorphism log as in Section 4.

For each $T \in \mathcal{T}$, choose a uniformizer t on $C_{\mathbb{Q}_2'}$ at T. For each sufficiently small value of t in $\mathbb{Q}_2$, let P_t be the corresponding point of $C(\mathbb{Q}_2)$ near T. Each coordinate of P_t is a power series in $\mathbb{Q}_2'[[t]]$ that can be calculated in the sense that any desired coefficient can be calculated. The same is true for the power series $\ell_i(t) := \int_\infty^{P_t} \omega_i$ for each i. Each $\ell_i(t)$ vanishes at $t = 0$ since T is torsion, but some ω_i is nonvanishing at T so the $\ell_i(t)$ do not all vanish to order 2. Using Hensel's lemma, we can control the rate of convergence of all these power series in order to compute an explicit open and closed neighborhood of 0 in $\mathbb{Q}_2$ on which $\rho(t^{-1}\ell_1(t), \dots, t^{-1}\ell_g(t))$ converges and is constant. Then $\rho\log$ is constant on the corresponding explicit neighborhood of T in $C(\mathbb{Q}_2)$. Such a neighborhood can be specified explicitly as a fiber of the map $C(\mathbb{Q}_2) = \mathcal{C}(\mathbb{Z}_2) \to \mathcal{C}(\mathbb{Z}/2^e\mathbb{Z})$ for some e, where $\mathcal{C}$ is an explicit proper $\mathbb{Z}_2$-model of C, say the Weierstrass model. Let U be the union of these neighborhoods as T varies; thus we know $\rho\log(U)$.

On $C(\mathbb{Q}_2) \setminus U$, log is bounded away from $\mathbf{0}$. Therefore, for any $P \in C(\mathbb{Q}_2) \setminus U$, the value $\rho\log(P)$ can be computed, and the computation examines only finitely many 2-adic digits of the coefficients of P; in other words, the computation succeeds with the same result for all points in a fiber of $C(\mathbb{Q}_2) = \mathcal{C}(\mathbb{Z}_2) \to \mathcal{C}(\mathbb{Z}/2^e\mathbb{Z})$ for some e. Since $C(\mathbb{Q}_2) \setminus U$ is compact, it can be covered by finitely many such fibers. For $e = 1, 2, \dots$ in turn, attempt to calculate $\rho\log(P)$ for one point P in each nonempty fiber of $C(\mathbb{Q}_2) \setminus U \to \mathcal{C}(\mathbb{Z}/2^e\mathbb{Z})$ using only the precision specified by the image of P in $\mathcal{C}(\mathbb{Z}/2^e\mathbb{Z})$. We may fail for the first few e, but the compactness argument guarantees that eventually a successful e will be found, and then we know $\rho\log(C(\mathbb{Q}_2) \setminus U)$.

Taking the union of $\rho\log(U)$ and $\rho\log(C(\mathbb{Q}_2) \setminus U)$ yields $\rho\log(C(\mathbb{Q}_2))$. Return "yes" or "no" according to whether $\rho\log(C(\mathbb{Q}_2))$ and $\mathbb{P}\sigma(\mathrm{Sel}_2 J)$ are disjoint. □

Corollary 10.13. *There is an algorithm based on Chabauty's method at the prime 2 that succeeds in determining $C(\mathbb{Q})$ for a computable set of curves $C \in \mathcal{F}_g$ of lower density at least the bound in Theorem 10.3 or Theorem 10.6 for any $g \geq 3$.*

Acknowledgements

The idea to combine Chabauty's method with results on the average 2-Selmer group size is due to Manjul Bhargava and Benedict Gross, whom we thank for discussions. In particular, we thank Gross for lingering after giving a lecture to explain the details of their argument

to us; it was only after this that we had the idea that an equidistribution result (also proved by Bhargava and Gross) could be used to refine a 2-adic Chabauty argument enough to reduce the upper bound on $\#C(\mathbb{Q})$ to 1. We thank Alice Guionnet and Scott Sheffield for discussions regarding Lemma 9.5, and Jennifer Park for a discussion regarding Lemma 10.2. The first author thanks the Centre Interfacultaire Bernoulli at EPFL for its hospitality during the period when most of the research for this paper was done; his research was partially supported by the Guggenheim Foundation and National Science Foundation grant DMS-1069236. The second author thanks the German Science Foundation for supporting his research through a grant within the framework of the DFG Priority Programme 1489 *Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory*. He thanks ICERM at Brown University for its hospitality during part of the semester program on *Complex and arithmetic dynamics*.

We also thank the referees for useful comments.

References

[A'C79] Norbert A'Campo, *Tresses, monodromie et le groupe symplectique*, Comment. Math. Helv. **54** (1979), no. 2, 318–327, DOI 10.1007/BF02566275 (French). MR535062 (80m:14006) ↑7

[BG13] Manjul Bhargava and Benedict Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, April 29, 2013. Preprint, `arXiv:1208.1007v2`. ↑1, 1.3, 2, 8.3, 8.3, 8.11, 8.12

[Bha13] Manjul Bhargava, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, August 5, 2013. Preprint, `arXiv:1308.0395v1`. ↑1.2

[BS13] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, December 23, 2013. Preprint, `arXiv:1006.1002v3`, to appear in *Annals of Math.* ↑1

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034) ↑8.2

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484 (3,14d) ↑1

[CEFS13] Alessandro Chiodo, David Eisenbud, Gavril Farkas, and Frank-Olaf Schreyer, *Syzygies of torsion bundles and the geometry of the level ℓ modular variety over $\overline{\mathscr{M}}_g$*, Invent. Math. **194** (2013), no. 1, 73–118, DOI 10.1007/s00222-012-0441-0. Theorem 2.3 is misstated in the journal article, but a correct statement appears in the version at `http://arxiv.org/abs/1205.0661v4` . MR3103256 ↑7.2

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR808103 (87f:11043) ↑1

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Mosc. Math. J. **2** (2002), no. 2, 281–311. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR1944508 (2003m:11080) ↑1

[Don80] Ron Donagi, *Group law on the intersection of two quadrics*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **7** (1980), no. 2, 217–239. MR581142 (82b:14025) ↑1

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German); English transl., *Finiteness theorems for abelian varieties over number fields* (1986), 9–27. Erratum in: Invent. Math. **75** (1984), 381. MR718935 (85g:11026a) ↑1

[Fou93] É. Fouvry, *Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 61–84 (French). MR1263524 (95b:11057) ↑1

[Gra07] Andrew Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Not. IMRN **8** (2007), Art. ID 027, 24, DOI 10.1093/imrn/rnm027. MR2340106 (2008j:11070) ↑10.11

[KZB13] Eric Katz and David Zureick-Brown, *The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, January 25, 2013. Preprint, `arXiv:arXiv:1204.3335v3`. ↑1

[Kne65] Martin Kneser, *Starke Approximation in algebraischen Gruppen. I*, J. Reine Angew. Math. **218** (1965), 190–203 (German). MR0184945 (32 #2416) ↑7

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 (86c:11086) ↑3.7, 3.2

[Lic68] Stephen Lichtenbaum, *Curves over discrete valuation rings*, Amer. J. Math. **90** (1968), 380–405. MR0230724 (37 #6284) ↑3.1, 9

[Liu94] Qing Liu, *Conducteur et discriminant minimal de courbes de genre* 2, Compositio Math. **94** (1994), no. 1, 51–79 (French). MR1302311 (96b:14038) ↑1

[Liu96] ———, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610, DOI 10.1090/S0002-9947-96-01684-4 (French, with English summary). MR1363944 (97h:11062) ↑1

[LT02] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR1892843 (2003d:11088) ↑1

[McC94] William G. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), no. 3, 565–596. MR1282232 (95c:11079) ↑1

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117. ↑1, 1, 10.3

[Poo01] Bjorn Poonen, *Computing torsion points on curves*, Experiment. Math. **10** (2001), no. 3, 449–465. MR1917430 (2003k:11104) ↑10.3

[Poo06] ———, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR2293593 (2008d:11062) ↑10.11

[Poo13] ———, *Average rank of elliptic curves [after Manjul Bhargava and Arul Shankar]*, Astérisque **352** (2013), Exp. No. 1049, viii, 187–204. Séminaire Bourbaki. Vol. 2011/2012. Exposés 1043–1058. MR3087347 ↑1

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483 ↑8.3

[PV04] Bjorn Poonen and José Felipe Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), 2004, pp. 175–184. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz. MR2029869 ↑10.11

[Rei72] Miles Reid, *The complete intersection of two or more quadrics*, 1972. Ph.D. thesis, Trinity College, Cambridge. ↑1

[Sai88] Takeshi Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** (1988), no. 1, 151–173, DOI 10.1215/S0012-7094-88-05706-7. MR952229 (89f:14024) ↑1

[SW14] Arul Shankar and Xiaoheng Wang, *Average size of the 2-Selmer group of Jacobians of monic even hyperelliptic curves*, February 17, 2014. Preprint, `arXiv:1307.3531v2`. ↑1.3

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German). ↑1

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 (2002b:11089) ↑10.3

[Sto06] ———, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661 ↑1, 3.2, 3.2, 5.2

[Sto09] ———, *On the average number of rational points on curves of genus* 2, February 24, 2009. Preprint, `arXiv:0902.4165`. ↑10.11

[Wan12] Xiaoheng Jerry Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, October 29, 2012. Ph.D. thesis, Harvard University. ↑1

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.
E-mail address: Michael.Stoll@uni-bayreuth.de
URL: http://www.mathe2.uni-bayreuth.de/stoll/