SQUAREFREE VALUES OF MULTIVARIABLE POLYNOMIALS

BJORN POONEN

Abstract. Given $f \in \mathbf{Z}[x_1, \dots, x_n]$, we compute the density of $x \in \mathbf{Z}^n$ such that $f(x)$ is squarefree, assuming the abc conjecture. Given $f, g \in \mathbf{Z}[x_1, \dots, x_n]$, we compute unconditionally the density of $x \in \mathbf{Z}^n$ such that $\gcd(f(x), g(x)) = 1$. Function field analogues of both results are proved unconditionally. Finally, assuming the abc conjecture, given $f \in \mathbf{Z}[x]$, we estimate the size of the image of $f(\{1, 2, \dots, n\})$ in $\left(\mathbf{Q}^*/\mathbf{Q}^{*2}\right) \cup \{0\}$.

1. Introduction

An integer n is called *squarefree* if for all prime numbers p we have $p^2 \nmid n$ (that is, p^2 does not divide n). Heuristically, one expects that if one chooses a positive integer n "at random," then for each prime p, the "probability" that $p^2 \nmid n$ equals $1 - p^{-2}$; and the assumption that these probabilities are "independent" leads to the guess that the density of squarefree positive integers equals

$$\prod_{\text{prime } p} (1 - p^{-2}) = \zeta(2)^{-1} = 6/\pi^2,$$

where $\zeta(s)$ is the Riemann zeta function, defined by

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{\text{prime } p} (1 - p^{-s})^{-1}$$

for $\operatorname{Re} s > 1$. One can formulate this guess precisely by defining the density of a set of positive integers S as

$$\mu(S) := \lim_{B \to \infty} \frac{\#(S \cap [1, B])}{B}.$$

In fact, the guess can be proved by simple sieve techniques [HW79, §18.6].

Now suppose that $f(x)$ is a polynomial with integer coefficients, and let S be the set of positive integers n for which $f(n)$ is squarefree. This time one guesses that the density of S equals $\prod_{\text{prime } p}(1 - c_p/p^2)$ where c_p equals the number of integers $n \in [0, p^2 - 1]$ for which $p^2 \mid f(n)$. When $\deg f \leq 2$, a simple sieve again shows that the guess is correct. When $\deg f = 3$, a more complicated argument is needed (see [Hoo67], or, for an improved error term, Chapter 4 of [Hoo76]). For general f with $\deg f \geq 4$, it is unknown whether the heuristic conjecture is correct, but A. Granville [Gra98] showed that it follows from the abc conjecture. (Recall that the abc conjecture is the statement that for any $\epsilon > 0$, there exists a constant $C = C(\epsilon) > 0$ such that if a, b, c are coprime positive integers satisfying

---

Date: September 28, 2003 (revised slightly after publication).

2000 *Mathematics Subject Classification.* Primary 11C08.

This research was supported by NSF grant DMS-9801104 and a Packard Fellowship. Part of the research was done while the author was enjoying the hospitality of the Université de Paris-Sud. This article has been published in *Duke Math. J.* **118** (2003), no. 2, 353–373.

$a+b=c$, then $c < C(\prod_{p|abc} p)^{1+\epsilon}$.) Granville used the abc conjecture in conjunction with Belyi's Theorem, to bound the number of polynomial values divisible by the square of a large prime. He also proved a conditional result for homogeneous polynomials in two variables, extending some earlier results along these lines, such as [Gre92]. (See [Gra98] for more references; some of these earlier results were unconditional in low degree cases.)

In this paper we generalize Granville's results to arbitrary polynomials over $\mathbf{Z}$ in many variables, still assuming the abc conjecture. The proof proceeds by reduction to the one-variable case, and the abc conjecture is required only because it is used by Granville; it is not required for the reduction. Such a fibering argument was used also in [GM91]. One defect of our proof is that it appears not to work for the most natural generalization of density in the multivariable case: see Section 2 and the remark following the proof of Lemma 6.2 for more details. An application of our result is towards estimating, given a regular quasiprojective scheme X over $\mathbf{Z}$, what fraction of hypersurface sections of X are regular. (See [Poo02].)

If $\mathbf{F}_q$ is a finite field of characteristic p, we prove an analogue for polynomials over $\mathbf{F}_q[t]$ unconditionally, using a completely different proof, exploiting the fact that $\mathbf{F}_q[t]$ has an $\mathbf{F}_q[t^p]$-linear derivation. One application of this result, suggested by A. J. de Jong [dJ02, §4.22], is to counting elliptic curves with squarefree discriminant: see Section 3. The case of squarefree values of a separable irreducible one-variable polynomial over $\mathbf{F}_q[t]$ (or more generally k^{th}-power-free values for polynomials over the ring of regular functions on any affine curve over $\mathbf{F}_q$) was proved earlier by K. Ramsay [Ram92][1] using a lemma of N. Elkies involving a derivation. In Section 8, we sketch a generalization of our result to multivariable polynomials over such rings of regular functions.

A related problem asks, given relatively prime polynomials $f(x_1,\dots,x_n)$ and $g(x_1,\dots,x_n)$ over $\mathbf{Z}$, what is the density of n-tuples of positive integers for which the values of f and g are relatively prime? Again there is a heuristic guess, and it was proved in [Eke91] that this guess is correct. We generalize by using a stronger definition of density (involving boxes of arbitrary dimensions, instead of only equal dimensions as considered in [Eke91]) and by simultaneously proving the function field analogue. The generalizations are needed to prove the corresponding results about squarefree values.

Finally, we confirm a guess made in [Gra98], namely that for a nonzero polynomial $f(x) \in \mathbf{Z}[x]$, the size of the image of $\{f(1), f(2), \dots, f(B)\}$ in $(\mathbf{Q}^*/\mathbf{Q}^{*2}) \cup \{0\}$ is $c_f B + o(B)$ as $B \to \infty$, for some constant c_f depending on f. Moreover, we find an explicit formula for c_f. In particular, $c_f = 1$ if f is squarefree of degree ≥ 2.

2. Definition of density

In Sections 2 through 7, A denotes $\mathbf{Z}$ or $\mathbf{F}_q[t]$ for some prime power $q = p^e$. Let K denote the fraction field of A. For nonzero $a \in A$ define $|a| := \#(A/a)$, and define $|0| = 0$. If $\mathfrak{p}$ is a nonzero prime of A, let $|\mathfrak{p}| := \#(A/\mathfrak{p})$. Define

$$\mathrm{Box} = \mathrm{Box}(B_1,\dots,B_n) = \begin{cases} \{\, (a_1,\dots,a_n) \in \mathbf{Z}^n : 0 < a_i \leq B_i \text{ for all } i \,\} & \text{if } A = \mathbf{Z}, \\ \{\, (a_1,\dots,a_n) \in A^n : |a_i| \leq B_i \text{ for all } i \,\} & \text{if } A = \mathbf{F}_q[t]. \end{cases}$$

[1] The formula for the density in Theorem 1 of [Ram92] should read $Z = \prod_{v \notin S} \left(1 - \rho(kv)/\|v\|^k\right)$. The proof there is correct, but the statement is unfortunately misprinted, with $\rho(v)$ in place of $\rho(kv)$.

For $\mathcal{S} \subseteq A^n$, define

$$\mu(\mathcal{S}) := \lim_{B_1,\ldots,B_n\to\infty} \frac{\#(\mathcal{S}\cap \text{Box})}{\#\text{Box}},$$

and define $\overline{\mu}(\mathcal{S})$ and $\underline{\mu}(\mathcal{S})$ similarly using lim sup and lim inf in place of lim. If a subset $\mathcal{S} \subseteq \mathbf{Z}^n$ and its 2^n reflections in the coordinate hyperplanes have a common density in this strong sense, then we can estimate $\#(\mathcal{S}\cap R)/\#R$ for regions R of many other shapes. For instance, if R_B is the ball of radius B centered at the origin, then $\#(\mathcal{S}\cap R_B)/\#R_B \to \mu(\mathcal{S})$ as $B\to\infty$, since R_B can be approximated by a Boolean combination of k boxes and their reflections, with an error of at most $\epsilon_k B^n$ lattice points for B large relative to k, where $\epsilon_k \to 0$ as $k\to\infty$.

In some of our results we can prove that the density exists only in a weaker sense. Define

$$\overline{\mu}_n(\mathcal{S}) := \limsup_{B_1,\ldots,B_{n-1}\to\infty}\ \limsup_{B_n\to\infty} \frac{\#(\mathcal{S}\cap \text{Box})}{\#\text{Box}}.$$

This has the effect of considering only boxes in which the n^{th} dimension is large relative to the others. Define $\underline{\mu}_n(\mathcal{S})$ similarly. If $\overline{\mu}_n(\mathcal{S}) = \underline{\mu}_n(\mathcal{S})$, define $\mu_n(\mathcal{S})$ as the common value. Also define

$$\overline{\mu}_{\text{weak}}(\mathcal{S}) := \max_{\sigma}\ \limsup_{B_{\sigma(1)}\to\infty}\cdots\limsup_{B_{\sigma(n)}\to\infty} \frac{\#(\mathcal{S}\cap \text{Box})}{\#\text{Box}},$$

where σ ranges over permutations of $\{1,2,\ldots,n\}$. This definition in effect considers only boxes whose dimensions can be ordered so that each is very large relative to the previous dimensions. Define $\underline{\mu}_{\text{weak}}(\mathcal{S})$ similarly, and define $\mu_{\text{weak}}(\mathcal{S})$ if $\overline{\mu}_{\text{weak}}(\mathcal{S}) = \underline{\mu}_{\text{weak}}(\mathcal{S})$.

3. Theorems

Throughout this paper, p represents a prime number. In particular, in a sum or product indexed by p, it is assumed that p runs through only primes. Similarly, $\mathfrak{p}$ represents a nonzero prime of A.

Theorem 3.1 (Relatively prime values). *Let $f, g \in A[x_1,\ldots,x_n]$ be polynomials that are relatively prime as elements of $K[x_1,\ldots,x_n]$. Let*

$$\mathcal{R}_{f,g} := \{\, a\in A^n : \gcd(f(a),g(a)) = 1 \,\}.$$

Then $\mu(\mathcal{R}_{f,g}) = \prod_{\mathfrak{p}}(1-c_{\mathfrak{p}}/|\mathfrak{p}|^n)$, where $\mathfrak{p}$ ranges over all nonzero primes of A, and $c_{\mathfrak{p}}$ is the number of $x\in(A/\mathfrak{p})^n$ satisfying $f(x) = g(x) = 0$ in $A/\mathfrak{p}$.

The assumptions and conclusions for the squarefree value theorem differ slightly in the $\mathbf{Z}$ and $\mathbf{F}_q[t]$ cases, so we separate them into Theorem 3.2 and Theorem 3.4.

Theorem 3.2 (Squarefree values over $\mathbf{Z}$). *Assume the abc conjecture. Let $f \in \mathbf{Z}[x_1,\ldots,x_n]$ be a polynomial that is squarefree as an element of $\mathbf{Q}[x_1,\ldots,x_n]$, and suppose that x_n appears in each irreducible factor of f. Let*

$$\mathcal{S}_f := \{\, a\in \mathbf{Z}^n : f(a) \text{ is squarefree} \,\}.$$

For each prime p, let c_p be the number of $x\in(\mathbf{Z}/p^2)^n$ satisfying $f(x) = 0$ in $\mathbf{Z}/p^2$. Then $\mu_n(\mathcal{S}_f) = \prod_p(1-c_p/p^{2n})$.

If the degree of x_n in each irreducible factor of f in Theorem 3.2 is ≤ 3, then it is unnecessary to assume the abc conjecture, because the proof reduces to the case of one-variable polynomials of degree ≤ 3, for which an unconditional result is known [Hoo67].

The $n = 1$ case of Theorem 3.2 differs slightly from Theorem 1 in [Gra98] in that the latter computes the density of squarefree values of $f(x)/m$ where m is a particular positive integer dividing all values of f. Such results can be proved in the multivariable case just as easily as Theorem 3.2; the key to all such results is Lemma 6.2.

Corollary 3.3. *Let notation and assumptions be as in Theorem 3.2 but without the restriction that x_n appears in f. Then $\mu_{\mathrm{weak}}(\mathcal{S}_f) = \prod_p (1 - c_p/p^{2n})$.*

Corollary 3.3 for $f(x_1, \ldots, x_n)$ follows from Theorem 3.2 applied to $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all permutations σ, since in the definition of μ_{weak} we may discard each lim sup corresponding to a variable that does not appear.

Theorem 3.4 (Squarefree values over $\mathbf{F}_q[t]$). *Let $A = \mathbf{F}_q[t]$. Let $f \in A[x_1, \ldots, x_n]$ be a polynomial that is squarefree as an element of $K[x_1, \ldots, x_n]$. Let*

$$\mathcal{S}_f := \{\, a \in A^n : f(a) \text{ is squarefree} \,\}.$$

For each nonzero prime $\mathfrak{p} \subseteq A$, let $c_{\mathfrak{p}}$ be the number of $x \in (A/\mathfrak{p}^2)^n$ satisfying $f(x) = 0$ in $A/\mathfrak{p}^2$. Then $\mu(\mathcal{S}_f) = \prod_{\mathfrak{p}} (1 - c_{\mathfrak{p}}/|\mathfrak{p}|^{2n})$.

Remark. Note in particular that Theorem 3.4 proves a result for μ instead of only for μ_n.

Suppose $\gcd(q, 6) = 1$. One application of Theorem 3.4 is to computing asymptotics for the weighted number R_d of isomorphism classes of elliptic curves (E, O) over $\mathbf{F}_q[t]$ with squarefree discriminant, as $d \to \infty$ for fixed q [dJ02, §4.22]. "Weighted" means that each isomorphism class receives the weight $1/\#\operatorname{Aut}(E, O)$ instead of 1. This number R_d is closely connected to the density of $(A, B) \in \mathbf{F}_q[t]^2$ such that the discriminant $\Delta = -16(4A^3 + 27B^2)$ of $y^2 = x^3 + Ax + B$ is squarefree, except that one works with homogeneous polynomials $A \in H^0(\mathbf{P}^1, \mathcal{O}(4d))$ and $B \in H^0(\mathbf{P}^1, \mathcal{O}(6d))$, so that the density has a factor corresponding to the point at infinity on $\mathbf{P}^1$ in addition to the affine points. A calculation shows that the density of such (A, B) having a double zero at a particular closed point $\mathfrak{p}$ of $\mathbf{P}^1 = \mathbf{P}^1_{\mathbf{F}_q}$ is $(2|\mathfrak{p}|^2 - |\mathfrak{p}|)/|\mathfrak{p}|^4$, where $|\mathfrak{p}|$ denotes the size of the residue field of $\mathfrak{p}$; from this and our methods we obtain

$$\lim_{d \to \infty} \frac{R_d}{q^{10d+1}} = \frac{q}{q-1} \prod_{\mathfrak{p} \in \mathbf{P}^1} \left(1 - \frac{2|\mathfrak{p}|^2 - |\mathfrak{p}|}{|\mathfrak{p}|^4} \right),$$

and the number γ_q of [dJ02, §4.22] equals

$$\gamma_q = \frac{q^3}{(q-1)^2(q+1)} \prod_{\mathfrak{p} \in \mathbf{P}^1} \left(1 - \frac{2|\mathfrak{p}|^2 - |\mathfrak{p}|}{|\mathfrak{p}|^4} \right).$$

Remark. Since $-16(4A^3 + 27B^2)$ has degree only 2 in B, it is possible to obtain the result of the previous paragraph by arguments simpler than those needed for the proof of Theorem 3.4 in general. (This was pointed out to me by de Jong.)

For a generalization of Theorem 3.4 to other rings of functions, see Section 8. Analogues where "squarefree" is replaced by "k^{th}-power-free" follow immediately from the same arguments once one has Lemma 6.2 (or the corresponding function field result).

Theorem 3.5 (Values in $\mathbf{Q}^*/\mathbf{Q}^{*2}$). *Let $f(x) \in \mathbf{Z}[x]$ be a nonzero polynomial. Write $f(x) = cg(x)^2h(x)$ where $c \in \mathbf{Z}$, $g(x) \in \mathbf{Z}[x]$, and $h(x)$ is a squarefree polynomial in $\mathbf{Z}[x]$ whose coefficients have gcd 1. If $\deg h > 3$, assume the abc conjecture. Then the image of $\{f(1), f(2), \ldots, f(B)\}$ in $(\mathbf{Q}^*/\mathbf{Q}^{*2}) \cup \{0\}$ has size $c_f B + o(B)$ for some constant $c_f \in [0, 1]$. If $\deg h = 0$, then $c_f = 0$. If $\deg h \geq 2$, then $c_f = 1$. If $\deg h = 1$, say $h(x) = ax + b$, then*

$$c_f = \frac{6}{\pi^2}\left(\sum_{r=0}^{|a|-1} \delta_r\right)\prod_{p|a}(1-p^{-2})^{-1} \quad \in \frac{1}{\pi^2}\mathbf{Q},$$

where $\delta_r := 1/m^2$ if m is the smallest positive integer satisfying $m^2 r \equiv b \pmod{a}$, or $\delta_r := 0$ if no such m exists.

Assuming the abc conjecture, Granville [Gra98, Corollary 2] proved that the size of the image in Theorem 3.5 was *at least* some positive constant times B (when $f(x)$ has no repeated roots), and guessed that the size should be asymptotic to a constant times B, as our Theorem 3.5 shows. An essentially equivalent version of Theorem 3.5 has been independently proved by P. Cutter, A. Granville, and T. Tucker (Theorems 1A, 1B, and 1C of [CGT03]), using a similar proof. They also prove a few related results not considered here.

It is natural to ask, as Granville has also done, what the multivariable analogue of Theorem 3.5 should be. Here we formulate a precise question along these lines:

Question 3.6. Suppose $f \in \mathbf{Z}[x_1, \ldots, x_n]$ is nonconstant and squarefree as an element of $\mathbf{Q}[x_1, \ldots, x_n]$. For $B \geq 1$, let $S_B = f(\{1, 2, \ldots, B\}^n) \subset \mathbf{Z}$, and let T_B be the image of S_B in $(\mathbf{Q}^*/\mathbf{Q}^{*2}) \cup \{0\}$. Does $\#T_B/\#S_B$ tend to a positive limit as $B \to \infty$?

We do not have enough evidence to conjecture an answer. But even if the answer is yes, it is not clear that we would understand the asymptotic size of T_B, because even the problem of estimating $\#S_B$ seems very difficult.

4. Zero values

The following lemma is well-known. We include a proof mainly because it is a toy version of some of the reductions used later on.

Lemma 4.1. *Let $f \in A[x_1, \ldots, x_n]$ be a nonzero polynomial. Let $\mathcal{Z} = \{\, a \in A^n : f(a) = 0 \,\}$. Then $\mu(\mathcal{Z}) = 0$.*

Proof. We use induction on n. The base case $n = 0$ is trivial, so suppose $n \geq 1$. Let $f_1 \in A[x_1, \ldots, x_{n-1}]$ be the leading coefficient of f when f is viewed as a polynomial in x_n. Let δ be the x_n-degree of f. Now $\mathcal{Z} \subseteq \mathcal{Z}_1 \cup \mathcal{Z}_2$ where

$$\mathcal{Z}_1 := \{\, a \in A^n : f_1(a) = 0 \,\},$$
$$\mathcal{Z}_2 := \{\, a \in A^n : f_1(a) \neq 0 \text{ and } f(a) = 0 \,\}.$$

By the inductive hypothesis, $\mu(\mathcal{Z}_1) = 0$. For each $(a_1, \ldots, a_{n-1}) \in A^{n-1}$, there are at most δ values $a_n \in A$ for which $(a_1, \ldots, a_{n-1}, a_n) \in \mathcal{Z}_2$. Thus $\mu(\mathcal{Z}_2) = 0$, by definition of μ. Hence $\mu(\mathcal{Z}) = 0$, as desired. $\square$

5. Relatively prime values

The bulk of the work in proving Theorem 3.1 is in the following.

Lemma 5.1. *Let $f, g \in A[x_1, \ldots, x_n]$ be polynomials that are relatively prime as elements of $K[x_1, \ldots, x_n]$. Let*

$$\mathcal{Q}_{f,g,M} := \{\, a \in A^n : \exists \mathfrak{p} \text{ such that } |\mathfrak{p}| \geq M \text{ and } \mathfrak{p} \mid f(a), g(a) \,\}.$$

Then $\lim_{M\to\infty} \overline{\mu}(\mathcal{Q}_{f,g,M}) = 0$.

Proof. Since we are interested only in $\mathfrak{p}$ with $|\mathfrak{p}|$ large, we may divide f and g by any factors in A that they have, in order to assume that f and g are relatively prime as elements of $A[x_1, \ldots, x_n]$.

The proof will be by induction on n. The case $n = 0$ is trivial, so assume $n \geq 1$. We need to bound the size of $Q := \mathcal{Q}_{f,g,M} \cap \text{Box}$, whenever the "dimensions" B_i of Box are su☐ciently large. Without loss of generality, $M \leq B_1 \leq B_2 \leq \cdots \leq B_n$. Set $B_0 = M$ and $B_{n+1} = \infty$. Let $f_1, g_1 \in A[x_1, \ldots, x_{n-1}]$ be the leading coe☐cients of f and g when f and g are viewed as polynomials in x_n.

Case 1. One of the polynomials, say g, is a polynomial in $x_1, \ldots, x_{n-1}$ only.

In this case, we use an inner induction on δ, where δ is the x_n-degree of f. The base case $\delta = 0$ is handled by the outer inductive hypothesis, so from now on assume $\delta > 0$. We may reduce to the case that f and g are irreducible. If $g \mid f_1$, then we can subtract a multiple of g from f to lower its x_n-degree δ, without changing $\mathcal{Q}_{f,g,M}$ or the relative primality of f and g, so the result follows from the inner inductive hypothesis. Hence we may assume $g \nmid f_1$. Since g is irreducible, f_1 and g are relatively prime in $A[x_1, \ldots, x_{n-1}]$.

Now $Q = \bigcup_{s=0}^{n} Q_s$, where

$$Q_s := \{\, a \in \text{Box} : \exists \mathfrak{p} \text{ such that } B_s \leq |\mathfrak{p}| < B_{s+1} \text{ and } \mathfrak{p} \mid f(a), g(a) \,\},$$

so it su☐ces to show that given $0 \leq s \leq n$, the ratio $\#Q_s/\#\text{Box}$ can be made arbitrarily small by choosing the B_i su☐ciently large.

Suppose we fix s with $0 \leq s < n$. (We will bound Q_n later.) Let X be the subscheme of $\mathbf{A}^n_A$ defined by $f = g = 0$. Since f and g are relatively prime, X has codimension at least 2 in $\mathbf{A}^n_A$. Let $\pi : \mathbf{A}^n_A \to \mathbf{A}^s_A$ be the projection onto the first s coordinates. Let Y_i be the (constructible) set of $y \in \mathbf{A}^s_A$ such that the fiber $X_y := X \cap \pi^{-1}(y)$ has codimension i in $\pi^{-1}(y) \simeq \mathbf{A}^{n-s}_{\kappa(y)}$. (Here $\kappa(y)$ denotes the residue field of y.) Since X has codimension at least 2 in $\mathbf{A}^n_A$, it follows from Theorem 15.1(i) of [Mat89] that the subset Y_i has codimension at least $2 - i$ in $\mathbf{A}^s_A$. In particular, we can choose a nonzero $h \in A[x_1, \ldots, x_s]$ vanishing on Y_1. Also we can find relatively prime $j_1, j_2 \in A[x_1, \ldots, x_s]$ vanishing on Y_0 as follows: choose any nonzero j_1 vanishing on Y_0; if $I(Y_0)$ is not contained in the union of the minimal primes over (j_1), then any $j_2 \in I(Y_0)$ outside those primes will be relatively prime to j_1; if $I(Y_0)$ is contained in that union, then Proposition 1.11(i) of [AM69] implies that $I(Y_0)$ is contained in some minimal prime over (j_1), but such a prime has codimension 1, contradicting the fact that Y_0 has codimension at least 2. Define $Y_{\geq 2} := \bigcup_{i \geq 2} Y_i$.

Given $a = (a_1, \ldots, a_n) \in A^n$ and a nonzero prime $\mathfrak{p}$ of A, let $a_\mathfrak{p} = (a_1, \ldots, a_n)_\mathfrak{p}$ denote the closed point in $\mathbf{A}^n_{A/\mathfrak{p}}$ whose coordinates are $a_1, \ldots, a_n$. Thus

$$Q_s = \{\, a \in \text{Box} : \exists \mathfrak{p} \text{ such that } B_s \leq |\mathfrak{p}| < B_{s+1} \text{ and } a_\mathfrak{p} \in X \,\}.$$

Let $Z := \{ a \in \text{Box} : h(a_1, \ldots, a_s) = 0 \}$. Define

$$R_{\geq 2} := \{ a \in \text{Box} : \ \exists \mathfrak{p} \text{ such that } B_s \leq |\mathfrak{p}| < B_{s+1},\ a_{\mathfrak{p}} \in X, \text{ and } (a_1, \ldots, a_s)_{\mathfrak{p}} \in Y_{\geq 2} \},$$

and define R_1 and R_0 similarly, using Y_1 and Y_0, respectively, in place of $Y_{\geq 2}$.

Then $Q_s \subseteq Z \cup R_{\geq 2} \cup (R_1 - Z) \cup R_0$. By Lemma 4.1, $\#Z/\#\text{Box}$ can be made arbitrarily small by choosing the B_i sufficiently large.

Next consider $R_{\geq 2}$. It suffices to show that for $(a_1, \ldots, a_s) \in \text{Box}(B_1, \ldots, B_s)$, the fraction of $(a_{s+1}, \ldots, a_n)$ in $\text{Box}(B_{s+1}, \ldots, B_n)$ for which there exists a prime $\mathfrak{p}$ with $B_s \leq |\mathfrak{p}| < B_{s+1}$, $a_{\mathfrak{p}} \in X$, and $(a_1, \ldots, a_s)_{\mathfrak{p}} \in Y_{\geq 2}$ is small when B_s is large. Fix $(a_1, \ldots, a_s) \in \text{Box}(B_1, \ldots, B_s)$. If $\mathfrak{p}$ is a prime with $B_s \leq |\mathfrak{p}| < B_{s+1}$ and $y := (a_1, \ldots, a_s)_{\mathfrak{p}}$ lies in $Y_{\geq 2}$, then X_y has codimension at least 2 in $\mathbf{A}^{n-s}_{A/\mathfrak{p}}$, so

$$\#X_y(A/\mathfrak{p}) = O(|\mathfrak{p}|^{n-s-2}) = O((\#(A/\mathfrak{p})^{n-s})/|\mathfrak{p}|^2).$$

Moreover, the implied constant can be made uniform in y, since the X_y are fibers in an algebraic family. Since $|\mathfrak{p}| < B_{s+1}$, the reductions modulo $\mathfrak{p}$ of the $(a_{s+1}, \ldots, a_n) \in \text{Box}(B_{s+1}, \ldots, B_n)$ are almost uniformly distributed in $(A/\mathfrak{p})^{n-s}$: to be precise, each residue class in $(A/\mathfrak{p})^{n-s}$ is represented by a fraction at most $O(\#(A/\mathfrak{p})^{-(n-s)})$ of these $(a_{s+1}, \ldots, a_n)$, where the implied constant depends only on n. Hence the fraction of $(a_{s+1}, \ldots, a_n) \in \text{Box}(B_{s+1}, \ldots, B_n)$ satisfying $(a_1, \ldots, a_n)_{\mathfrak{p}} \in X_y$ is $O(1/|\mathfrak{p}|^2)$, and summing over all $\mathfrak{p}$ with $B_s \leq |\mathfrak{p}| < B_{s+1}$ still yields a fraction that can be made arbitrarily small by taking B_s large, since $\sum_{\mathfrak{p}} 1/|\mathfrak{p}|^2$ converges.

We now adapt the previous paragraph to bound $\#(R_1 - Z)$. Suppose $(a_1, \ldots, a_s) \in \text{Box}(B_1, \ldots, B_s)$ and $h(a_1, \ldots, a_s) \neq 0$. Let η be the total degree of h. Then $|h(a_1, \ldots, a_s)| = O(B_s^{\eta})$, where the constant implied by the O depends only on h, not on the a_i or B_i. Thus, provided that B_s is large, $h(a_1, \ldots, a_s)$ can be divisible by at most η primes $\mathfrak{p}$ satisfying $B_s \leq |\mathfrak{p}| < B_{s+1}$. Hence $(a_1, \ldots, a_s)_{\mathfrak{p}} \in Y_1$ for at most η primes $\mathfrak{p}$ satisfying $B_s \leq |\mathfrak{p}| < B_{s+1}$. By definition of Y_1, if $y = (a_1, \ldots, a_s)_{\mathfrak{p}}$ for such $\mathfrak{p}$, then X_y has codimension at least 1 in $\mathbf{A}^{n-s}_{A/\mathfrak{p}}$, so $\#X_y(A/\mathfrak{p}) = O((\#(A/\mathfrak{p})^{n-s})/|\mathfrak{p}|)$, where the implied constant is independent of y. The reductions modulo $\mathfrak{p}$ of the $(a_{s+1}, \ldots, a_n) \in \text{Box}(B_{s+1}, \ldots, B_n)$ are again almost uniformly distributed in $(A/\mathfrak{p})^{n-s}$. Hence the fraction of $(a_{s+1}, \ldots, a_n)$ in $\text{Box}(B_{s+1}, \ldots, B_n)$ whose reduction modulo $\mathfrak{p}$ lies in X_y is $O(1/|\mathfrak{p}|)$. Summing over at most η possible primes $\mathfrak{p}$ with $|\mathfrak{p}| \geq B_s$ still yields a fraction that can be made arbitrarily small by taking B_s large.

Finally we consider R_0. Since $s < n$, the outer inductive hypothesis applied to j_1 and j_2 implies that $\#R_0/\#\text{Box}$ can be made arbitrarily small by taking the B_i large.

To finish Case 1, we need to bound Q_n. We have $Q_n \subseteq S_0 \cup S \cup S'$, where

$$S_0 := \{ a \in \text{Box} : g(a_1, \ldots, a_{n-1}) = 0 \},$$
$$S := \{ a \in \text{Box} : \exists \mathfrak{p} \text{ such that } |\mathfrak{p}| \geq B_n \text{ and } \mathfrak{p} \mid f_1(a), g(a) \}$$
$$S' := \{ a \in \text{Box} : g(a_1, \ldots, a_{n-1}) \neq 0 \text{ and } \exists \mathfrak{p} \text{ such that } |\mathfrak{p}| \geq B_n,\ \mathfrak{p} \mid f(a), g(a) \text{ and } \mathfrak{p} \nmid f_1(a) \}.$$

Lemma 4.1 bounds $\#S_0/\#\text{Box}$. The outer inductive hypothesis applied to f_1 and g bounds $\#S/\#\text{Box}$.

It remains to bound $\#S'$. For $(a_1, \ldots, a_{n-1}) \in \text{Box}(B_1, \ldots, B_{n-1})$ such that $g(a_1, \ldots, a_{n-1}) \neq 0$, we will show that the fraction of $a_n \in \text{Box}(B_n)$ such that there exists $\mathfrak{p}$ with $|\mathfrak{p}| \geq B_n$, $\mathfrak{p} \mid f(a), g(a)$ and $\mathfrak{p} \nmid f_1(a)$ is small. We use a method similar to that used to bound R_1. Let γ denote the total degree of g. If B_n is sufficiently large (depending only on g), then given $(a_1, \ldots, a_{n-1})$, there are at most γ primes $\mathfrak{p}$ dividing $g(a)$ with $|\mathfrak{p}| \geq B_n$. For each such $\mathfrak{p}$, if moreover $\mathfrak{p} \nmid f_1(a)$, then the polynomial $f(a_1, \dots, a_{n-1}, x_n) \bmod \mathfrak{p}$ in $(A/\mathfrak{p})[x_n]$ is of degree δ, and has at most δ roots in $A/\mathfrak{p}$. For each such root, there are at most $O(1)$ elements of $\operatorname{Box}(B_n)$ reducing to it modulo $\mathfrak{p}$, since $|\mathfrak{p}| \geq B_n$. Thus given $(a_1, \dots, a_{n-1})$, there are at most $\gamma\delta \cdot O(1) = O(1)$ values of $a_n \in \operatorname{Box}(B_n)$ for which $(a_1, \dots, a_n) \in S'$. Thus $\#S'/\#\operatorname{Box}$ can be made small by choosing B_n large.

Case 2. The x_n-degree of f and g are both positive.

Let $R \in A[x_1, \dots, x_{n-1}]$ be the resultant of f and g with respect to x_n. Since f and g are relatively prime, R is nonzero. Since f_1, g_1, and R are all nonzero and do not involve x_n, none of them are multiples of f or g. Since f and g are irreducible, each of f_1, g_1, and R must be relatively prime to each of f and g. Moreover, if $\mathfrak{p}$ is a prime dividing $f(a)$ and $g(a)$, and if the leading coefficients $f_1(a)$ and $g_1(a)$ are nonzero modulo $\mathfrak{p}$, then by a well known property of the resultant, $\mathfrak{p} \mid R(a)$. Hence

$$\begin{aligned}\{\, a \in \operatorname{Box} : \mathfrak{p} \mid f(a), g(a) \,\} \subseteq \{\, a \in \operatorname{Box} : \mathfrak{p} \mid f_1(a), g(a) \,\}&\\ \cup \{\, a \in \operatorname{Box} : \mathfrak{p} \mid f(a), g_1(a) \,\}&\\ \cup \{\, a \in \operatorname{Box} : \mathfrak{p} \mid f(a), R(a) \,\}&.\end{aligned}$$

Taking the union over all $\mathfrak{p}$ with $|\mathfrak{p}| \geq M$ and applying Case 1 to f_1, g, to f, g_1, and to f, R completes the proof. $\square$

Proof of Theorem 3.1. Let P_M denote the set of nonzero primes $\mathfrak{p}$ of A such that $|\mathfrak{p}| < M$. Approximate $\mathcal{R}_{f,g}$ by

$$\mathcal{R}_{f,g,M} := \{\, a \in A^n : \ f(a) \text{ and } g(a) \text{ are not both divisible by any prime } \mathfrak{p} \in P_M \,\}.$$

Define the ideal I as the product of all $\mathfrak{p}$ in P_M. Then $\mathcal{R}_{f,g,M}$ is a union of cosets of the subgroup $I^n \subset A^n$. (Here I^n is the cartesian product.) Hence $\mu(\mathcal{R}_{f,g,M})$ is the fraction of residue classes in $(A/I)^n$ in which for all $\mathfrak{p} \in P_M$, at least one of $f(a)$ and $g(a)$ is nonzero modulo $\mathfrak{p}$. Applying the Chinese Remainder Theorem shows that $\mu(\mathcal{R}_{f,g,M}) = \prod_{\mathfrak{p} \in P_M}(1 - c_{\mathfrak{p}}/|\mathfrak{p}|^n)$. By Lemma 5.1,

$$\mu(\mathcal{R}_{f,g}) = \lim_{M \to \infty} \mu(\mathcal{R}_{f,g,M}) = \prod_{\mathfrak{p}} (1 - c_{\mathfrak{p}}/|\mathfrak{p}|^n).$$

Since f and g are relatively prime as elements of $K[x_1, \dots, x_n]$, there exists a nonzero $u \in A$ such that $f = g = 0$ defines a subscheme of $\mathbf{A}^n_{A[1/u]}$ of codimension at least 2. Thus $c_{\mathfrak{p}} = O(|\mathfrak{p}|^{n-2})$ as $|\mathfrak{p}| \to \infty$, and the product converges. $\square$

6. Squarefree values of polynomials over $\mathbf{Z}$

If $f \in A[x_1, \dots, x_n]$, and $M \geq 1$, define

$$\mathcal{T}_{f,M} := \{\, a \in A^n : \exists \mathfrak{p} \text{ with } |\mathfrak{p}| \geq M \text{ such that } \mathfrak{p}^2 \mid f(a) \,\}.$$

For the rest of this section, we take $A = \mathbf{Z}$. The following is a variant of Theorem 1 of [Gra98], and has the same proof.

Lemma 6.1. *Assume the abc conjecture. Suppose that $f \in \mathbf{Z}[x]$ is squarefree as a polynomial in $\mathbf{Q}[x]$. For each prime $p \geq M$, let c_p be the number of $x \in \mathbf{Z}/p^2$ satisfying $f(x) = 0$ in $\mathbf{Z}/p^2$. Then $1 - \mu(\mathcal{T}_{f,M}) = \prod_{p \geq M}(1 - c_p/p^2)$.*

We are now ready to prove the analogue of Lemma 5.1 for squarefree values of multivariable polynomials over $\mathbf{Z}$:

Lemma 6.2. *Assume the abc conjecture. Suppose that $f \in \mathbb{Z}[x_1,\dots,x_n]$ is squarefree as a polynomial in $\mathbb{Q}[x_1,\dots,x_n]$, and suppose that x_n appears in each irreducible factor of $f(x)$. Then $\lim_{M\to\infty} \overline{\mu}_n(\mathcal{T}_{f,M}) = 0$.*

Proof. Factors of f lying in $\mathbb{Z}$ are irrelevant as $M \to \infty$, so we may assume that f is squarefree as a polynomial in $\mathbb{Z}[x_1,\dots,x_n]$. If f factors as a product of two relatively prime polynomials g and h, then the result for f follows from the result for g and h together with Lemma 5.1 applied to g,h. Hence we may reduce to the case where f is irreducible in $\mathbb{Z}[x_1,\dots,x_n]$.

Let $\Delta \in \mathbb{Z}[x_1,\dots,x_{n-1}]$ and $\delta \geq 1$ be the discriminant and degree, respectively, of f considered as a polynomial in x_n. Given $B_1,\dots,B_n$, let $Q := \mathcal{T}_{f,M} \cap \mathrm{Box}$. We need to show that if the B_i are sufficiently large, and B_n is sufficiently large relative to the other B_i, then $\#Q/\#\mathrm{Box}$ is small.

The fraction of $(a_1,\dots,a_{n-1})$ in $\mathrm{Box}_{n-1} := \mathrm{Box}(B_1,\dots,B_{n-1})$ at which Δ vanishes is negligible, by Lemma 4.1. Since f is irreducible, when f is viewed as a polynomial in x_n, its coefficients (in $\mathbb{Z}[x_1,\dots,x_{n-1}]$) are relatively prime (not necessarily pairwise). In particular, the common zero locus of these coefficients has codimension at least 2 in $\mathbb{A}^{n-1}_{\mathbb{Q}}$, hence is contained in the subvariety defined by $\tilde{f} = \tilde{g} = 0$ for two relatively prime elements $\tilde{f},\tilde{g} \in \mathbb{Z}[x_1,\dots,x_{n-1}]$. Thus Lemma 5.1 implies that the fraction of $(a_1,\dots,a_{n-1}) \in \mathrm{Box}_{n-1}$ such that there exists a prime $p \geq M$ such that the image of $f(a_1,\dots,a_{n-1},x_n)$ in $\mathbb{F}_p[x_n]$ is zero is negligible, when M is large.

It remains to bound $\#(Q \cap (Q' \times [1,B_n]))/\#\mathrm{Box}$, where Q' is the set of $(a_1,\dots,a_{n-1}) \in \mathrm{Box}_{n-1}$ such that

- $\Delta(a_1,\dots,a_{n-1}) \neq 0$, and
- there is no prime $p \geq M$ such that the image of $f(a_1,\dots,a_{n-1},x_n)$ in $\mathbb{F}_p[x_n]$ is zero.

By the first condition, Lemma 6.1 applies to $f(a_1,\dots,a_{n-1},x_n) \in \mathbb{Z}[x_n]$ for each $(a_1,\dots,a_{n-1}) \in Q'$. Letting B_n tend to infinity while $B_1,\dots,B_{n-1}$ are fixed, we find that it suffices to bound

$$\frac{1}{\#\mathrm{Box}} \sum_{(a_1,\dots,a_{n-1})\in Q'} B_n \left(1 - \prod_{p\geq M}\left(1 - \frac{c_p(a_1,\dots,a_{n-1})}{p^2}\right)\right), \tag{1}$$

where $c_p(a_1,\dots,a_{n-1})$ is the number of $x_n \in \mathbb{Z}/p^2$ such that $f(a_1,\dots,a_{n-1},x_n) = 0$ in $\mathbb{Z}/p^2$. The inequality $1-\alpha\beta \leq (1-\alpha) + (1-\beta)$ holds for $\alpha,\beta \in [0,1]$; applying this with

$$\alpha := \prod_{\substack{p\geq M\\ p\nmid\Delta(a_1,\dots,a_{n-1})}} \left(1 - \frac{c_p(a_1,\dots,a_{n-1})}{p^2}\right), \qquad \beta := \prod_{\substack{p\geq M\\ p\mid\Delta(a_1,\dots,a_{n-1})}} \left(1 - \frac{c_p(a_1,\dots,a_{n-1})}{p^2}\right)$$

and using

$$1-\alpha \leq \sum_{\substack{p\geq M\\ p\nmid\Delta(a_1,\dots,a_{n-1})}} \frac{c_p(a_1,\dots,a_{n-1})}{p^2}$$

bounds (1) by $s_1 + s_2$ where

$$s_1 := \frac{1}{\#\mathrm{Box}} \sum_{(a_1,\dots,a_{n-1})\in Q'} B_n \sum_{\substack{p\ge M\\ p\nmid\Delta(a_1,\dots,a_{n-1})}} \frac{c_p(a_1,\dots,a_{n-1})}{p^2},$$

$$s_2 := \frac{1}{\#\mathrm{Box}} \sum_{(a_1,\dots,a_{n-1})\in Q'} B_n \left(1 - \prod_{\substack{p\ge M\\ p\mid\Delta(a_1,\dots,a_{n-1})}} \left(1-\frac{c_p(a_1,\dots,a_{n-1})}{p^2}\right)\right).$$

When $(a_1,\dots,a_{n-1}) \in Q'$ and $p \nmid \Delta(a_1,\dots,a_{n-1})$, Hensel's Lemma implies $c_p(a_1,\dots,a_{n-1}) \le \delta$, while $B_n \# Q' \le \#\mathrm{Box}$, so $s_1 \le \sum_{p\ge M} \delta/p^2$, which is negligible as $M \to \infty$. When $(a_1,\dots,a_{n-1}) \in Q'$ and $p \mid \Delta(a_1,\dots,a_{n-1})$, the image of $f(a_1,\dots,a_{n-1},x_n)$ in $\mathbf{F}_p[x_n]$ has at most δ zeros in $\mathbf{F}_p$; so $c_p(a_1,\dots,a_{n-1}) \le \delta p$, and

$$s_2 \le \frac{1}{\#\mathrm{Box}} \sum_{(a_1,\dots,a_{n-1})\in Q'} B_n \left(1 - \prod_{\substack{p\ge M\\ p\mid\Delta(a_1,\dots,a_{n-1})}} \left(1-\frac{\delta}{p}\right)\right). \tag{2}$$

Let $\Phi(x_n) = \prod_{j=1}^{\delta}(x_n - j)$. We may assume $M \ge \delta$; then

$$1 - \prod_{\substack{p\ge M\\ p\mid\Delta(a_1,\dots,a_{n-1})}} \left(1-\frac{\delta}{p}\right)$$

equals the density of

$$\{\, x_n \in \mathbf{Z} : \ \exists p \ge M \text{ such that } p \mid \Delta(a_1,\dots,a_{n-1}), \Phi(x_n) \,\}.$$

Hence, as $B_n \to \infty$ for fixed $M, B_1, \dots, B_{n-1}$, the right hand side of (2) has the same limit as

$$\frac{\#\left((Q' \times [1, B_n]) \cap \mathcal{Q}_{\Delta(x_1,\dots,x_{n-1}),\Phi(x_n),M}\right)}{\#\mathrm{Box}}.$$

The latter is negligible, by Lemma 5.1. □

Remark. It seems difficult to improve Lemma 6.2 to obtain a result for the more natural definition of density, $\overline{\mu}$ instead of $\overline{\mu}_n$. This would require a version of Granville's one-variable result that is uniform in the coefficients of the polynomial. Granville's proof uses Belyi functions, however, whose degrees vary wildly with the coefficients.

Proof of Theorem 3.2. Approximate $\mathcal{S}_f$ by

$$\mathcal{S}_{f,M} := \{\, a \in \mathbf{Z}^n : \ f(a) \text{ is not divisible by } p^2 \text{ for any prime } p < M \,\}.$$

Then $\mathcal{S}_{f,M}$ is a union of cosets of $(I\mathbf{Z})^n$ where $I = \prod_{p<M} p^2$. The Chinese Remainder Theorem implies $\mu_n(\mathcal{S}_{f,M}) = \prod_{\mathfrak{p}\in P_M}(1 - c_p/p^{2n})$. By Lemma 6.2,

$$\mu_n(\mathcal{S}_f) = \lim_{M\to\infty} \mu_n(\mathcal{S}_{f,M}) = \prod_p (1 - c_p/p^{2n}).$$

Finally, we show that the product converges (instead of diverging to 0) by showing that $c_p = O(p^{2n-2})$. (The value of the product could still be zero if some factor were zero.) Let X be the subscheme of $\mathbf{A}^n_{\mathbf{Z}}$ defined by $f = 0$. Since the field $\mathbf{Q}$ is perfect, the nonsmooth locus of $X \times \mathbf{Q} \to \operatorname{Spec} \mathbf{Q}$ has codimension at least 2 in $\mathbf{A}^n_{\mathbf{Q}}$. It follows that for sufficiently large p, the nonsmooth locus Y_p of $X \times \mathbf{F}_p \to \operatorname{Spec} \mathbf{F}_p$ has codimension at least 2 in $\mathbf{A}^n_{\mathbf{F}_p}$, so $\#Y_p(\mathbf{F}_p) = O(p^{n-2})$. Each point in $Y_p(\mathbf{F}_p)$ can be lifted to an n-tuple in $(\mathbf{Z}/p^2)^n$ in p^n ways. On the other hand, $\#(X_p - Y_p)(\mathbf{F}_p) = O(p^{n-1})$ but the nonvanishing of some derivative modulo p at a point in $(X_p - Y_p)(\mathbf{F}_p)$ implies that such a point lifts to at most p^{n-1} solutions to $f(x) = 0$ in $(\mathbf{Z}/p^2)^n$. Thus $c_p = p^n O(p^{n-2}) + p^{n-1} O(p^{n-1}) = O(p^{2n-2})$. □

7. Squarefree values of polynomials over $\mathbf{F}_q[t]$

Throughout this section, $A = \mathbf{F}_q[t]$ where $q = p^e$. Our goal is to prove Theorem 3.4. We begin by stating the analogue of Lemma 6.2.

Lemma 7.1. *Suppose that $f \in A[x_1, \dots, x_n]$ is squarefree as a polynomial in $K[x_1, \dots, x_n]$. Then $\lim_{M\to\infty} \overline{\mu}(\mathcal{T}_{f,M}) = 0$.*

Before beginning the proof of Lemma 7.1, we state and prove two results that will be needed in its proof.

Lemma 7.2. *If $f \in K[x_1, \dots, x_n]$ is squarefree, then*

$$F := f\left(y_0^p + t y_1^p + \cdots + t^{p-1} y_{p-1}^p, x_2, x_3, \dots, x_n\right) \in K[y_0, \dots, y_{p-1}, x_2, \dots, x_n]$$

is squarefree.

Proof. We work in $B := K^{1/p}[y_0, \dots, y_{p-1}, x_2, \dots, x_n]$, where $K^{1/p} = \mathbf{F}_q(t^{1/p})$. Define $u := y_0 + t^{1/p} y_1 + \cdots + t^{(p-1)/p} y_{p-1}$.

We first show that $K^{1/p}[u] \cap K[y_0, \dots, y_{p-1}] = K[u^p]$. Suppose $g = \sum \alpha_i u^i \in K^{1/p}[u] \cap K[y_0, \dots, y_{p-1}]$. The coefficient of y_0^i in g is α_i, so $\alpha_i \in K$ for all i. The coefficient of $y_0^{i-1} y_1$ in g is $i t^{1/p} \alpha_i$; this too is in K, so for all i, either $p \mid i$ or $\alpha_i = 0$. Thus $g \in K[u^p]$, as desired.

It follows that

$$K^{1/p}[u, x_2, \dots, x_n] \cap K[y_0, \dots, y_{p-1}, x_2, \dots, x_n] = K[u^p, x_2, \dots, x_n]. \tag{3}$$

Suppose that $G^2 \mid F$ for some $G \in K[y_0, \dots, y_{p-1}, x_2, \dots, x_n] - K$. Then $G^2 \mid F$ in B. If we view B as a polynomial ring over $K^{1/p}$ in algebraically independent indeterminates $u, y_1, \dots, y_{p-1}, x_2, \dots, x_n$ (by eliminating y_0), then $F = f(u^p, x_2, \dots, x_n)$ does not involve $y_1, \dots, y_{p-1}$, so $G \in K^{1/p}[u, x_2, \dots, x_n]$ too. By (3), $G \in K[u^p, x_2, \dots, x_n]$. If we write $G = g(u^p, x_2, \dots, x_n)$ where $g \in K[x_1, \dots, x_n]$, then $g^2 \mid f$ and $g \notin K$, contradicting the assumption that f is squarefree in $K[x_1, \dots, x_n]$. □

Lemma 7.3. *Suppose $f \in K[x_1^p, \dots, x_n^p]$ is squarefree as an element of $K[x_1, \dots, x_n]$. Then f and $\partial f/\partial t$ are relatively prime as elements of $K[x_1, \dots, x_n]$.*

Proof. The gcd g of f and $\partial f/\partial t$ in $K[x_1^p, \dots, x_n^p]$ equals their gcd in $K[x_1, \dots, x_n]$. We may multiply g by an element of K^* to assume that some coefficient of g equals 1. Write $f = gh$. Since f is squarefree, g and h are relatively prime in $K[x_1, \dots, x_n]$. But g divides $\frac{\partial f}{\partial t} = g\frac{\partial h}{\partial t} + h\frac{\partial g}{\partial t}$, so g divides $\partial g/\partial t$. The total degree of $\partial g/\partial t$ is less than or equal to that of g, so $\partial g/\partial t = cg$ for some $c \in K$. Then each coefficient γ of g satisfies $\partial\gamma/\partial t = c\gamma$. One of these coefficients is 1, so $c = 0$. Thus each coefficient γ is in K^p, so $g = G^p$ for some $G \in K[x_1, \dots, x_n]$. But $g \mid f$, and f is squarefree, so $g \in K$. Hence f and $\partial f/\partial t$ are relatively prime. □

Proof of Lemma 7.1. We may assume that f is squarefree as an element of $A[x_1, \ldots, x_n]$. Define

$$F := f\left(\sum_{j=0}^{p-1} t^j y_{1j}^p, \ldots, \sum_{j=0}^{p-1} t^j y_{nj}^p\right) \in K[\ldots, y_{ij}, \ldots]$$

By n applications of Lemma 7.2, F is squarefree. Let $B_{ij} = (B_i/|t^j|)^{1/p}$. As each y_{ij} ranges through elements of A satisfying $|y_{ij}| \le B_{ij}$, the n-tuples

$$\left(\sum_{j=0}^{p-1} t^j y_{1j}^p, \ldots, \sum_{j=0}^{p-1} t^j y_{nj}^p\right)$$

exhaust the elements of Box, with each element appearing once. Hence Lemma 7.1 for f follows from Lemma 7.1 for F.

Evaluation of F at an element $a \in A^{np}$ commutes with formal application of $\partial/\partial t$, since $F \in K[\ldots, y_{ij}^p, \ldots]$. Thus, for a prime $\mathfrak{p}$ of A, we have $\mathfrak{p}^2 \mid F(a)$ if and only if $\mathfrak{p}$ divides $F(a)$ and $(\partial F/\partial t)(a)$. Hence Lemma 7.1 for F follows from Lemma 5.1 for F and $\partial F/\partial t$, which are relatively prime by Lemma 7.3. □

Proof of Theorem 3.4. We mimic the proof of Theorem 3.2 at the end of Section 6, using Lemma 7.1 in place of Lemma 6.2. But the last paragraph of that proof, proving $c_p = O(p^{2n-2})$ to obtain convergence of the infinite product, does not carry over, since it uses the fact that $\mathbf{Q}$ is perfect to obtain generic smoothness, and $\mathbf{F}_q(t)$ is not perfect.

Therefore we prove $c_{\mathfrak{p}} = O(|\mathfrak{p}|^{2n-2})$ by a different method. The fraction $c_{\mathfrak{p}}/|\mathfrak{p}|^{2n}$ is unchanged when we replace the $c_{\mathfrak{p}}$ and n for the original f by the corresponding values for the F defined in the beginning of the proof of Lemma 7.1. This fraction for F is bounded by the fraction of $\bar{a} \in (A/\mathfrak{p})^{np}$ such that F and $\partial F/\partial t$ vanish mod $\mathfrak{p}$ at $\bar{a}$. By Lemma 7.3, F and $\partial F/\partial t$ are relatively prime in $K[\ldots, y_{ij}, \ldots]$, so they define a subscheme of codimension at least 2 in $\mathbf{A}_K^{np}$, and the desired bound follows, just as in the last two sentences of Section 5. □

8. Squarefree values of polynomials over other rings of functions

Let S be a finite nonempty set of closed points of a smooth, projective, geometrically integral curve X over $\mathbf{F}_q$. Define the affine curve $U := X \setminus S$, and let A be the ring of regular functions on U. Thus A is the set of S-integers of the function field K of X. An element $a \in A$ is called squarefree if the ideal (a) of A is a product of distinct primes of A. Let Div_S denote the set of effective divisors on X with support contained in S. If $D \in \operatorname{Div}_S$, then the $\mathbf{F}_q$-subspace $L(D) := \{ f \in K^* : (f) + D \ge 0 \} \cup \{0\}$ of K is contained in A. Let $\ell(D) = \dim_{\mathbf{F}_q} L(D)$. Define the density $\mu(\mathcal{S})$ of a subset $\mathcal{S} \subseteq A^n$ as the limit of $\#(\mathcal{S} \cap \text{Box})/\#\text{Box}$ as Box runs through $L(D_1) \times \cdots \times L(D_n)$, where $D_i \in \operatorname{Div}_S$ and $\min_i \deg D_i \to \infty$. The following theorem generalizes Theorem 1 in [Ram92]; we state it only for squarefree values, but as mentioned already in Section 3 the lemmas used in its proof will yield the analogous result for k^{th}-power-free values.

Theorem 8.1 (Squarefree values over rings of functions). *With notation as above, let $f \in A[x_1, \ldots, x_n]$ be a polynomial that is squarefree as an element of $K[x_1, \ldots, x_n]$. Let*

$$\mathcal{S}_f := \{ a \in A^n : f(a) \text{ is squarefree} \}.$$

For each nonzero prime $\mathfrak{p} \subseteq A$, let $c_\mathfrak{p}$ be the number of $x \in (A/\mathfrak{p}^2)^n$ satisfying $f(x) = 0$ in $A/\mathfrak{p}^2$. Then $\mu(\mathcal{S}_f) = \prod_\mathfrak{p}(1 - c_\mathfrak{p}/|\mathfrak{p}|^{2n})$, where $|\mathfrak{p}| := \#(A/\mathfrak{p})$.

Sketch of proof of Theorem 8.1. Most of the proof follows the proofs of Theorems 3.1 and 3.4, so we will comment only on the differences.

First we prove the analogue of Lemma 5.1. Enlarging S only makes this analogue harder to prove, since there are more boxes to consider, while the primes $\mathfrak{p}$ involved are the same once M exceeds $|\mathfrak{p}|$ for every new $\mathfrak{p}$ thrown into S. Thus we may assume that A is a principal ideal domain. Let g be the genus of X. Given Box = $L(D_1) \times \cdots \times L(D_n)$, let $B_i = \deg D_i - (2g - 2)$. We may assume $\deg D_1 \leq \cdots \leq \deg D_n$. Replace the definition of Q_s in the proof of Lemma 5.1 by

$$Q_s := \{\, a \in \text{Box} : \exists \mathfrak{p} \text{ such that } B_s \leq \deg \mathfrak{p} < B_{s+1} \text{ and } \mathfrak{p} \mid f(a), g(a) \,\}.$$

Replace the argument "Since $|\mathfrak{p}| < B_{s+1}$, the reductions modulo $\mathfrak{p}$ of the $(a_{s+1}, \ldots, a_n) \in \text{Box}(B_{s+1}, \ldots, B_n)$ are almost uniformly distributed in $(A/\mathfrak{p})^{n-s}$" by "By Riemann-Roch, if D is a divisor with $\deg D - \deg \mathfrak{p} > 2g-2$, then $\ell(D) - \ell(D - \mathfrak{p}) = \deg \mathfrak{p}$; hence the $\mathbf{F}_q$-linear reduction map

$$L(D_{s+1}) \times \cdots \times L(D_n) \to (A/\mathfrak{p})^{n-s}$$

is surjective for $\deg \mathfrak{p} < B_{s+1}$." Replace the estimate "$|h(a_1, \ldots, a_s)| = O(B_s^\eta)$" by

> "$\deg h(a_1, \ldots, a_s) = O(\deg D_s) = O(B_s)$ where the implied constants depend on h and the genus g, but not on the a_i or D_i"

to bound the number of primes $\mathfrak{p}$ with $\deg \mathfrak{p} \geq B_s$ dividing $h(a_1, \ldots, a_s)$. The rest of the proof of Lemma 5.1 goes as before.

Next we prove the analogue of Lemma 7.1. Choose any $t \in A - A^p$, and note that Lemmas 7.2 and 7.3 go through without change; in fact, we can generalize Lemma 7.2 by replacing the form $y_0^p + ty_1^p + \cdots + t^{p-1}y_{p-1}^p$ by $t_1y_1^p + t_2y_2^p + \cdots + t_my^m$ for any $t_1, \ldots, t_m \in A$ provided that $t_i/t_j \notin K^p$ for some i, j.

We claim that there exist $t_1, \ldots, t_m \in A$ such that for every $D \in \text{Div}_S$ and every $a \in L(D)$, it is possible to write $a = t_1a_1^p + \cdots + t_ma_m^p$ with $a_i \in A$ such that $t_ia_i^p \in L(D)$ for each i. More precisely, we claim that if E is the divisor $(p + 1)(2g + 5)\sum_{\mathfrak{p}\in S} \mathfrak{p}$, then the choice $\{t_1, \ldots, t_m\} := L(E)$ works. To prove this, it suffices to show, given $D \in \text{Div}_S$ and $a \in L(D) - L(E)$, that one can adjust a by an element of the form $t_ia_i^p$ in $L(D)$ to obtain an element in $L(D - \mathfrak{p})$ for some $\mathfrak{p}$ in the support of D; then iterate. If $a \in L(D) - L(E)$, then for some $\mathfrak{p} \in S$, a has a pole of order greater than $(p + 1)(2g + 5)$ at $\mathfrak{p}$. If $n \geq 2g + 4$, Riemann-Roch shows that $\ell(n\mathfrak{p}) - \ell((n-1)\mathfrak{p}) = \deg \mathfrak{p}$; in particular there exists a function in A having a pole of order n with prescribed leading coefficient at $\mathfrak{p}$, and no other poles. Since every integer greater than $(p+1)(2g+5)$ is expressible as $i + pj$ with $2g + 4 \leq i < 2g + 4 + p$ and $j \geq 2g + 4$, we can find functions $t \in L(i\mathfrak{p})$ and $\alpha \in L(j\mathfrak{p})$ such that $t\alpha^p$ and a have the same order of pole at $\mathfrak{p}$, and the same leading coefficient. Then $t \in L(E)$ and $t\alpha^p \in L(D)$, so this proves the claim.

By the previous paragraph, for each $D \in \text{Div}_S$, we have a surjection

$$\begin{aligned} L(D_1) \times \cdots \times L(D_r) &\to L(D) \\ (a_1, \ldots, a_r) &\mapsto t_{i_1}a_1^p + \cdots + t_{i_r}a_r^p \end{aligned}$$

for some subset $\{i_1, \ldots, i_r\} \subseteq \{1, 2, \ldots, m\}$ and for some $D_i \in \text{Div}_S$ depending on D. If $\deg D$ is sufficiently large, then $L(D)$ contains nonzero functions with ratio outside K^p, so some t_{i_α}/t_{i_β} lies outside K^p. Thus in proving the analogue of Lemma 7.1, we may reduce the result for f to the result for each F in the finite set of polynomials of the form

$$F := f\left(\sum_{j\in S_1} t_j y_{1j}^p, \dots, \sum_{j\in S_n} t_j y_{nj}^p\right) \in K[\dots, y_{ij}, \dots]$$

for all possible subsets $S_1, \dots, S_n \subseteq \{1, 2, \dots, m\}$ such that each subset contains i, j with $t_i/t_j \notin K^p$.

Choose $b \in A$ such that $b\frac{\partial}{\partial t}$ is a nonzero derivation $A \to A$. Then the analogue of Lemma 7.1 for an F as above follows from the analogue of Lemma 5.1 applied to F and $b\partial F/\partial t$.

To complete the proof of Theorem 8.1, it remains to prove $c_{\mathfrak{p}} = O(|\mathfrak{p}|^{2n-2})$, to obtain convergence of the infinite product. This follows as in the proof of Theorem 3.4 at the end of Section 7, except that the fraction $c_{\mathfrak{p}}/|\mathfrak{p}|^{2n}$ for f is now bounded by a *sum* of the analogous fractions for several different polynomials F. Each of the latter fractions is bounded by $O(1/|\mathfrak{p}|^2)$, and the number of polynomials F is $O(1)$, independent of $\mathfrak{p}$, so $c_{\mathfrak{p}}/|\mathfrak{p}|^{2n} = O(1/|\mathfrak{p}|^2)$, as desired. □

9. The image of the values in $\mathbf{Q}^*/\mathbf{Q}^{*2}$

This section is devoted to the proof of Theorem 3.5.

Lemma 9.1. *Suppose that $f(x) \in \mathbf{Z}[x]$ is squarefree as an element of $\mathbf{Q}[x]$, and that* $\deg f \geq 2$. *Fix $q \in \mathbf{Q}^*$ such that $q \neq 1$. Then the number of solutions (m, n) to $f(m) = qf(n)$ satisfying $1 \leq m, n \leq B$ is $o(B)$ as $B \to \infty$.*

Proof. Since $f(m)$ has constant sign for large positive m, the result is trivial if $q < 0$. Therefore assume $q > 0$.

Theorem 2 in Chapter 13 of [Ser97] implies that the number of such solutions on each irreducible component of the curve $f(m) - qf(n) = 0$ in the (m, n)-plane over $\mathbf{Q}$ is $O(B^{1/2} \log B)$ unless some component is a line. If there is a line, it cannot be of the form $n = \alpha$ for any $\alpha \in \mathbf{Q}$, so it would have an equation $m = \alpha n + \beta$ for some $\alpha, \beta \in \mathbf{Q}$. Then $f(\alpha n + \beta) - qf(n) = 0$ as polynomials in $\mathbf{Q}[n]$. Equating leading coefficients shows that $\alpha \neq 1$. Choose $\gamma \in \mathbf{Q}$ so that $\alpha\gamma + \beta = \gamma$. Then the polynomial $F(x) := f(x + \gamma)$ satisfies $F(\alpha x) - qF(x) = 0$. Since $q > 0$ and $q \neq 1$, there is at most one integer d such that $\alpha^d = q$. Thus F is a monomial of degree d, and $f(n) = c(n - \gamma)^d$ for some $c \in \mathbf{Q}$. Since $\deg f \geq 2$, this contradicts the assumption that f is squarefree. □

We now begin the proof of Theorem 3.5. We easily reduce to the case where $f(x) = h(x)$, that is, where the coefficients of f have gcd 1, and f is squarefree in $\mathbf{Z}[x]$. Also we may assume that the leading coefficient of f is positive. The $\deg f = 0$ case is trivial.

Proof of Theorem 3.5 in the case $\deg f = 1$. Write $f(x) = ax + b$. Changing b by a multiple of a changes the sequence of values only in finitely many terms, so we may assume $0 < b \leq a$. Given $r, N \in \mathbf{Z}_{\geq 0}$, let $S(r \bmod a, N)$ denote the set of positive squarefree integers $\leq N$ that are congruent to r modulo a. Identify each element of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ with a squarefree integer representative.

We claim that the image of $\{f(1), f(2), \dots, f(B)\}$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ is the disjoint union of $S(r \bmod a, \delta_r(aB + b))$ as r ranges from 0 to $a - 1$. Let m be as in the definition of δ_r, when it exists. If $s \in S(r \bmod a, \delta_r(aB + b))$, then $\delta_r > 0$, so the integer m in the definition of δ_r exists; then $m^2 s \equiv m^2 r \equiv b \pmod{a}$ and $m^2 s \leq m^2 \delta_r(aB+b) = aB+b$, so $m^2 s \in \{f(1), f(2), \ldots, f(B)\}$, and hence s is in the image. Conversely, suppose that the squarefree integer s represents the image of $f(n)$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ for some $n \in \{1, 2, \ldots, B\}$. Thus $f(n) = \bar{m}^2 s$ for some $\bar{m}$. Let $r \in [0, a)$ be such that $r \equiv s \pmod{a}$. Then $\bar{m}^2 r \equiv \bar{m}^2 s = an + b \equiv b \pmod{a}$, so the m in the definition of δ_r exists, and $m \leq \bar{m}$. Now $s = f(n)/\bar{m}^2 \leq (aB+b)/m^2 = \delta_r(aB+b)$, so $s \in S(r \bmod a, \delta_r(aB+b))$. This proves the claim.

When $\gcd(a, r) = 1$, the density of squarefree values of $ax + r$ equals

$$\prod_{p \nmid a} \left(1 - p^{-2}\right) = \frac{6}{\pi^2} \prod_{p|a} \left(1 - p^{-2}\right)^{-1},$$

so

$$\#S(r \bmod a, N) = \left(\frac{6}{\pi^2} \prod_{p|a} \left(1 - p^{-2}\right)^{-1} + o(1)\right)(N/a)$$

as $N \to \infty$. The result follows upon setting $N = \delta_r(aB+b) \sim \delta_r aB$ for each $r \in [0, a)$ for which $\delta_r \neq 0$ (such r are necessarily prime to a), and summing over r. $\square$

Proof of Theorem 3.5 in the case $\deg f \geq 2$. Replacing $f(x)$ by $f(x+n)$ for some n, we may assume that $0 < f(1) < f(2) < \cdots$. It suffices to show, given $\epsilon > 0$, that for sufficiently large B, the image of $\{f(1), \ldots, f(B)\}$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ has size at least $(1-\epsilon)B$. For a positive integer n, let $\mathfrak{s}(n)$ denote the largest positive integer m such that $m^2 \mid n$. Define

$$S_m = \{\, n \in \{1, 2, \ldots, B\} : \mathfrak{s}(f(n)) = m \,\}.$$

By Lemma 6.1, the density of the set of integers n such that $\mathfrak{s}(f(n))$ is divisible by a prime $p > M$ tends to zero as $M \to \infty$. Also, for each fixed prime ℓ, the set of integers n such that $\ell^m \mid \mathfrak{s}(f(n))$ tends to zero as $m \to \infty$, because the number of $n \in \mathbf{Z}/\ell^{2m}$ such that $f(n) = 0$ in $\mathbf{Z}/\ell^{2m}$ is $O(1)$ as $m \to \infty$, since f is squarefree. Hence $\mu(\{\, n \in \mathbf{Z} : \mathfrak{s}(f(n)) \geq M \,\}) \to 0$ as $M \to \infty$. In particular, if M is sufficiently large, then $\#(S_1 \cup \cdots \cup S_{M-1}) > (1 - \epsilon/2)B$ for large B.

Now f maps each S_i injectively into $\mathbf{Q}^*/\mathbf{Q}^{*2}$. For $1 \leq i < j < M$, the intersection of the images of $f(S_i)$ and $f(S_j)$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ has size $o(B)$ as $B \to \infty$ by Lemma 9.1. Thus the image of $\{f(1), f(2), \ldots, f(B)\}$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ has size at least $(1-\epsilon/2)B - \binom{M-1}{2} o(B) > (1-\epsilon)B$, if B is sufficiently large relative to M. $\square$

Acknowledgements

I thank Johan de Jong and Ofer Gabber for independently suggesting that I try to use ideas from [Poo02] to compute the density of squarefree values in the $\mathbf{F}_q[t]$ case. I thank Brian Conrad for pointing out some errors in an earlier draft, and the referee for helpful suggestions. Finally, I thank Pamela Cutter, Andrew Granville, and Tom Tucker for sharing their preprint with me.

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[CGT03] Pamela Cutter, Andrew Granville, and Thomas J. Tucker, *The number of fields generated by the square root of values of a given polynomial*, Canad. Math. Bull. **46** (2003), no. 1, 71–79.

[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.

[Eke91] Torsten Ekedahl, *An infinite version of the Chinese remainder theorem*, Comment. Math. Univ. St. Paul. **40** (1991), no. 1, 53–59.

[GM91] Fernando Gouvêa and Barry Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.

[Gra98] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices (1998), no. 19, 991–1009.

[Gre92] George Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) **43** (1992), no. 169, 45–65.

[Hoo67] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.

[Hoo76] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge, 1976, Cambridge Tracts in Mathematics, No. 70.

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[Mat89] Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid.

[Poo02] Bjorn Poonen, *Bertini theorems over finite fields*, 2002, `arXiv:math.AG/0204002`.

[Ram92] Keith Ramsay, *Square-free values of polynomials in one variable over function fields*, Internat. Math. Res. Notices (1992), no. 4, 97–102.

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`