JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 4, Number 1, January 1991

THE SQUARE-FREE SIEVE AND THE RANK OF ELLIPTIC CURVES

F. GOUVÊA AND B. MAZUR

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$. A celebrated theorem of Mordell asserts that $E(\mathbb{Q})$, the (abelian) group of rational points of E, is finitely generated. By the *rank* of E we mean the rank of $E(\mathbb{Q})$. Thus the rank of E is positive if and only if E possesses an infinity of rational points. Relatively few general qualitative assertions can be made about the rank as E varies.

How large can the rank get? Although we expect that there are elliptic curves over $\mathbb{Q}$ with arbitrarily high ranks, this is presently unknown.

What is the average size of the rank? Recently Brumer and McGuinness have reported on their study of 310,716 elliptic curves of prime conductor less than 10^8 where they have found that 20.06% of those curves have even rank ≥ 2. (Cf. [BM]; also see forthcoming work of Brumer where, subject to a number of standard conjectures, he shows that 2.3 is an upper bound for the *average rank* for all elliptic curves over $\mathbb{Q}$ ordered in terms of their Faltings height.)

What is the behavior of the rank over the family of twists of a given elliptic curve? Here, one has three natural kinds of families of twists:

(1) *Quadratic twists.* One can take any elliptic curve and systematically twist it by all quadratic characters (this is the type of family of elliptic curves we are concerned with in this paper). Specifically, if E is an elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $Y^2 = X^3 + A \cdot X + B$, and D is any square-free integer, the (quadratic) twist of E by D, E_D, is given by the equation $D \cdot Y^2 = X^3 + A \cdot X + B$. Put $\mathcal{R}_E(D) := \operatorname{rank}(E_D)$. Goldfeld has conjectured [Go] that the average value (suitably defined) of $\mathcal{R}_E$ is $\frac{1}{2}$. *Conditional upon some standard conjectures* (made explicit below; see Theorem 2), we find lower bounds for the number of times $\mathcal{R}_E$ is ≥ 2. Specifically for a fixed elliptic curve $E_{/\mathbb{Q}}$ and any $\varepsilon > 0$, we prove the (*conditional*) result that for sufficiently large real numbers x, there are at least $x^{1/2-\varepsilon}$ square-free integers D with $|D| \leq x$ such that $\mathcal{R}_E(D)$ is ≥ 2 (and is even).

(2) *Cubic and quartic twists.* One can also take an elliptic curve over $\mathbb{Q}$ with j-invariant 0, and twist it by all cubic characters; or one can take an elliptic curve with j-invariant 1728 and twist by quartic characters. In [ZK] data is

Received by the editors June 9, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 11N35.

accumulated for the family of elliptic curves with j-invariant 0, twisted by all cubic characters. Specifically the family $X^3 + Y^3 = T$ is studied, where T varies through cube-free natural numbers. The data in [ZK] suggests that about 23.3% of the curves (obtained by specializing T in the above equation) that have even rank, have rank ≥ 2. More specifically, the L-function of the specialized curves for square-free positive integers $T \leq 70{,}000$ is examined. It is found that among those instances where the sign of the functional equation of the L-function is $+$, 23.3% of these L-functions vanish at the central point $s = 1$, and these 23.3% are surprisingly evenly distributed.

What can be said about the variation of analytic *rank for a family of elliptic curves obtained from a given modular elliptic curve by twisting by quadratic characters?* If the elliptic curve E is a modular elliptic curve, i.e., if it is parametrized by a cuspidal newform f of weight 2 on $\Gamma_0(C)$ for some positive integer C, then a consequence of the classical conjecture of Birch and Swinnerton-Dyer is that $\mathscr{R}_E(D)$ is the order of vanishing at $s = 1$ of the L-function attached to $f \otimes \chi_D$, where χ_D is the quadratic Dirichlet character attached to the field $\mathbb{Q}(\sqrt{D})$. Let us refer to this order of vanishing as the *analytic rank* of E_D and denote it $\mathscr{R}_f(D)$. Of course, conjecturally, we have $\mathscr{R}_f(D) = \mathscr{R}_E(D)$. But for the analytic rank we obtain the following *unconditional* result:

Theorem 1. *Let E be a modular elliptic curve over $\mathbb{Q}$. For fixed $\varepsilon > 0$, $x^{1/2-\varepsilon}$ is a lower bound for*

$$\sharp\{\textit{square-free } D;\ |D| \leq x;\ \textit{analytic rank } (E_D) \textit{ is } \geq 2 \textit{ and even}\}$$

for sufficiently large real numbers x.

Questions and remarks. (1) Can one hope for a purely analytic proof of the above theorem?

(2) We hardly expect that the statement of Theorem 1 is best possible. Although the technique we use to prove Theorem 1 does not seem to give any exponent larger than $\frac{1}{2} - \varepsilon$, it is conceivable that the statement holds with the exponent $\frac{1}{2} - \varepsilon$ replaced by something on the order of $\frac{3}{4} - \varepsilon$.

For a numerical example, one can cite [ZK] in which the (modular) elliptic curve $Y^2 = X^3 - X$, i.e., the curve connected to the congruence number problem, is examined, along with its quadratic twists E_D, for D a square-free integer, $D \equiv 1 \bmod 16$, and $D < 500{,}000$. The data accumulated in [ZK] would be consistent with a larger exponent (a straight regression based on the table published in [ZK] suggests, for example, that for this E the statement of Theorem 1 might remain true if the exponent $\frac{1}{2} - \varepsilon$ is replaced by some number on the order of $0.88\ldots$, but more numerical work would be necessary to come up with a firm figure).

(3) It is convenient to have a succinct vocabulary to discuss the exponents arising in Theorem 1. So for $s(x)$ any real-valued function, let us say that ϑ is an *exponent* for the function s if for any $\varepsilon > 0$ there is a real number x_ε

such that $x^{\vartheta-\varepsilon} < s(x)$ for $x \geq x_\varepsilon$. In these terms, then, Theorem 1 guarantees that $\frac{1}{2}$ is an *exponent* for the function $\mathcal{S}_f(x) = \sharp\{D$ square-free, $|D| \leq x$, $\mathcal{R}_f(D) \geq 2$, and $\mathcal{R}_f(D)$ is even$\}$.

(4) We think that it may be of interest to pursue analogues of the above result in broader contexts. Specifically,

(a) *Higher orders of vanishing.* Are there positive *exponents* measuring the quantity of twists of E with prescribed analytic or arithmetic ranks other than ranks 0, 1, and 2?[1]

(b) *Broader classes of modular forms f.* Let C and k be positive integers with k even. Let f be a cuspidal newform on $\Gamma_0(C)$, i.e., with trivial nebentypus character, with weight k, and with Fourier expansion at ∞ given by $\sum a_n q^n$ where $q = e^{2\pi i z}$. The summation is taken over all $n \geq 1$, the coefficients a_i are in $\mathbb{C}$, and f is assumed normalized, so that $a_1 = 1$. If χ is a Dirichlet character, let $L(f, \chi, s)$ denote the entire function which is the analytic continuation of the Dirichlet series $\sum a_n \chi(n) n^{-s}$. What can be said about the behavior of the function

$$D \mapsto \mathcal{R}_f(D) := \text{order of vanishing at } s = k/2 \text{ of } L(f, \chi_D, s),$$

where χ_D is the quadratic Dirichlet character attached to the field $\mathbb{Q}(\sqrt{D})$?

Let $\mathcal{S}_f(x)$ denote the cardinality of the set of D's that are square-free, of absolute value $\leq x$, and such that the order of vanishing at the central point, $\mathcal{R}_f(D)$, of the L-function $L(f, \chi_D, s)$ is an even number ≥ 2.

Is it the case that if f is a cuspidal newform of weight 2 whose field of Fourier coefficients is of degree ≤ 3 over $\mathbb{Q}$, then the exponent for $\mathcal{S}_f$ is > 0? If f is a cuspidal newform of weight 4 with Fourier coefficients in $\mathbb{Z}$, is its exponent positive? Do all the other cuspidal newforms of even weight have exponent 0? Questions like these that concern $\mathcal{R}_f$ and $\mathcal{S}_f$ are closely related to lacunarity questions for modular forms of half-integral weight: by the work of Shimura [Sh] and Waldspurger [W], one knows that, for fixed cuspidal newform f, the values $L(f, \chi_D, k/2)$ (suitably normalized) for varying D can be obtained as the squares of certain Fourier coefficients $c_f(D)$ of a modular form $\tilde{f}$ of weight $(k+1)/2$. For a detailed discussion of the modular form related to the congruence number problem (studied numerically in [ZK]) consult [T] and [Ko].

Remarks on the parity of $\mathcal{R}_f(D)$. If f is a cuspidal newform of conductor C and of even weight, the *parity* of $\mathcal{R}_f(D)$ is given by a simple rule in general (cf. [MTT]) which for square-free integers D relatively prime to $2C$ can be stated as follows. If $D \neq 1$ is such an integer, then $\mathcal{R}_f(D)$ and $\mathcal{R}_f(1)$ have the same parity if and only if $\chi_D(-C) = 1$, where χ_D is the quadratic Dirichlet character attached to the field $\mathbb{Q}(\sqrt{D})$.

[1] J.-F. Mestre, for example, has some ideas that may lead to results concerning an exponent for the number of square-free D with $|D| \leq x$ such that E_D has odd analytic rank $r \geq 3$.

Therefore, combining the conjectures of Taniyama–Weil and Birch–Swinnerton–Dyer we have that (conjecturally) for E any elliptic curve over $\mathbb{Q}$ the parity of $\mathscr{R}_E(D)$, for D a square-free integer relatively prime to twice the conductor of E, depends only upon congruence conditions on D. For the purpose of understanding the mechanism of our paper, let us isolate the (conjectural) statement about parity, which is the only implication of the Taniyama–Weil and Birch–Swinnerton–Dyer conjectures that is of relevance to our proof:

Parity Conjecture. *Let E be an elliptic curve over $\mathbb{Q}$, and let D be a square-free integer relatively prime to twice the conductor C of E. Then $\mathscr{R}_E(1) \equiv \mathscr{R}_E(D)$ mod 2 (i.e., the ranks of E and of E_D have the same parity) if and only if $\chi_D(-C) = 1$, where χ_D is the quadratic Dirichlet character belonging to the field $\mathbb{Q}(\sqrt{D})$.*

We prove the following result:

Theorem 2. *Let E be an elliptic curve over $\mathbb{Q}$. If the Parity Conjecture holds, then for fixed $\varepsilon > 0$, $x^{1/2-\varepsilon}$ is a lower bound for the function*

$$\mathscr{S}_E(x) := \sharp\{\textit{square-free } D;\ |D| \leq x;\ \operatorname{rank}(E_D) \textit{ is } \geq 2 \textit{ and even}\}$$

for sufficiently large real numbers x. In other words, $\frac{1}{2}$ is an exponent for $\mathscr{S}_E$.

Our proofs of Theorems 1 and 2 make use of the arithmetic of elliptic curves and a technique of Hooley's, using Gallagher's version of the large sieve[2]. We adapted Hooley's techniques (which were fashioned to treat polynomials in one variable), to make them applicable to *homogeneous* polynomials in two variables all of whose irreducible factors over $\mathbb{Q}$ have degree ≤ 3. After submitting our paper for publication in this journal we learned from Hooley that George Greaves (see the preprint [Gr]) had been developing a method (also an elaboration of Hooley's original technique), which directly treats homogeneous two-variable polynomials with irreducible factors of degree ≤ 6. Moreover, Greaves's proof, which depends upon the fact that binary forms are more evenly distributed in residue classes modulo p^2 than are their counterparts in one variable, is shorter than ours, and yields a better error term than ours when the irreducible factors have degree ≤ 3.[3] It, therefore, might have made sense

[2] Some weaker versions of these theorems are significantly easier to prove. For example, if one restricts attention to elliptic curves E that possess a rational point of order 2, then one need not deal with irreducible factors of degree 3 in Proposition 4, which is the hard case. In this restricted case one obtains a slightly improved error term. Also, if one wishes merely to prove that the exponent is $\geq \frac{1}{3}$, then one can make do with Hooley's original one-variable sieve dealing only with *integral* points $(u, 1)$ in §2 below.

[3] Advances in this area are proceeding rapidly: Mr. Keith Ramsay, a graduate student at Harvard has informed us that, building upon Greaves's idea, he has succeeded in improving Greaves's error term to $O(x^2/(\log x)^{1/2})$ in the case of irreducible binary forms of the sixth degree. Also, one of us has generalized the results of this paper to obtain positive exponent theorems over general number fields (see the preprint [Gou]). Also, see forthcoming work of Jaap Top and Cameron Stewart that applies Greaves's result for sextic binary forms to obtain further positive exponent theorems for $\mathscr{R}_E(D)$ independent of the parity conjecture (but with exponents $< \frac{1}{2}$).

to revise our paper, deleting our treatment of the square-free sieve and referring to Greaves for that proof. But since Greaves's paper [Gr] depends, at a number of points, on the exposition in our paper, on various Lemmas in our paper, on our notation, etc., the question of exactly which deletions we can logically make is something of a game of pick-up-sticks. To keep the exposition smooth and self-contained we have retained, intact, our original proof.[4]

We are very pleased to have been able to use the occasion of writing this paper as grounds for initiating a number of conversations that were interesting and helpful to us; we warmly thank A. Brumer, P. Diaconis, N. Elkies, M. Hakosalo, M.-F. Mestre, A. Odlyzko, J.-P. Serre, and D. Zagier. Diane Meuser generously worked out a calculation in Igusa's theory for us. We are most grateful for that, and hope that we have done justice to her careful exposition in our transcription of it (Lemma 2 of §5). We are thankful to Christopher Hooley for his detailed letter to us, which informed us of Greaves's work.

2. The square-free counting method

We begin by a description of our proof of Theorem 2.

Let $Y^2 = X^3 + AX + B$ be a Weierstrass equation for an elliptic curve E of conductor C, and form the homogeneous quartic equation $F(U, V) = V \cdot f(U, V)$, where

$$f(U, V) := U^3 + AUV^2 + BV^3.$$

Now for any pair of integers (u, v), if $F(u, v)$ is a *square-free integer* put $D = F(u, v)$. Of course, $(X, Y) = (u/v, 1/v^2)$ is a rational point on E_D. It is an easy consequence of a result of Shafarevitch that there are only a finite number of pairs (u, v) for which the rational point $(u/v, 1/v^2)$ is a torsion point on E_D. Explicitly,

Proposition 1. *If E is an elliptic curve over $\mathbb{Q}$, then there are only a finite number of square-free integers D such that the twisted elliptic curve E_D has a torsion point of order > 2.*

Proof. To say that a twist E_D has the property that its Mordell–Weil group contains an element of order p is equivalent to saying that there is a point $(X, Y\sqrt{D})$ on E of order p, with $X, Y \in \mathbb{Q}$. In particular, the cyclic subgroup in E generated by this point is rational over $\mathbb{Q}$, and division by this group yields a rational isogeny of E of degree p. A sufficient condition, therefore, for the prime number p *not* to occur as the order of any element in any or the Mordell–Weil groups $E_D(\mathbb{Q})$ is that E not admit an isogeny of degree p rational over $\mathbb{Q}$. Now any given elliptic curve over $\mathbb{Q}$ admits $\mathbb{Q}$-rational p-isogenies for only a finite number of primes p. Because by Shafarevitch's theorem [III], there are only a finite number of isomorphism classes of elliptic curves over a given number field that are isogenous (over that number field)

[4] Despite the fact that our result has a worse error term than Greaves's, our strategy of obtaining it via fibering might be of independent interest.

to a given elliptic curve. In particular, if there is an infinity of $\mathbb{Q}$-rational p-isogenies with domain E, then the corresponding range elliptic curves represent only a finite number of distinct isormorphism classes over $\mathbb{Q}$. Consequently, one easily deduces the existence of a $\mathbb{Q}$-rational endomorphism (with nontrivial cyclic kernel) of one of the range elliptic curves. But this is a contradiction in that any $\mathbb{Q}$-rational endomorphism of any elliptic curve over $\mathbb{Q}$ is given by multiplication by an integer.

We have reduced our task to showing that for *each* odd prime number p (and also for the integer 4) there are only a finite number of square-free integers D such that $E_D(\mathbb{Q})$ contains an element of order p (or of order 4). But this is quite immediate: If p is a prime number, call ρ_p the natural representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-division points of E so that up to conjugation we may view ρ_p as a homomorphism

$$\rho_p\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbf{F}_p).$$

If p is an odd prime, then $\rho_p \otimes \chi_D$ can contain the identity representation for at most *two* square-free values of D. A similar statement takes care of the case of 4-torsion, concluding the proof of our Proposition.

Remark. The $\mathbb{Q}$-rational isogenies of prime degree (for elliptic curves over $\mathbb{Q}$) have, in fact, been classified [M] and therefore, much finer information than the qualitative assertion in Proposition 1 is available, if needed. For example, it follows from [M] that there is an integer B (and a small integer, at that!) such that for *any* elliptic curve E over $\mathbb{Q}$, there are at most B distinct square-free integers D such that the torsion subgroup of $E_D(\mathbb{Q})$ contains elements of order > 2. Are there analogous *uniform* upper bounds valid for elliptic curves and their quadratic twists over number fields other than $\mathbb{Q}$? For information about isogenies of elliptic curves over general number fields see [Se].

By the Parity Conjecture, if (u, v) is such that D is relatively prime to $2C$, and if u and v are in the appropriate congruence classes modulo $4C$, then the parity of the rank of E_D is even. Let Z be a real number, and let $\mathscr{T}_E(Z)$ refer to the set of all pairs (u, v) with $0 < u$, $v < Z$, such that

(a) the pair (u, v) lies in the appropriate congruence classes modulo $4C$, referred to above;

(b) the point $(X, Y) = (u/v, 1/v^2)$ is not a torsion point on E_D where $D = F(u, v)$;

(c) the value $D = F(u, v)$ is a square-free integer.

We assume that the Parity Conjecture holds. Then, if $(u, v) \in \mathscr{T}_E(Z)$, $\mathscr{R}_E(D)$ is even and since it is > 0, it is ≥ 2. It then follows that there is a positive constant λ depending only upon $f(U, V)$ such that if we set $Z = \lambda \cdot x^{1/4}$, the mapping $(u, v) \mapsto D = F(u, v)$ sends $\mathscr{T}_E(\lambda \cdot x^{1/4})$ to $\mathscr{S}_E(x)$. A technique of Hooley's (or rather, an adaptation of his technique to our situation) enables one to show (as follows immediately from Proposition 6 of §10) that there is a positive constant c such that the cardinality of $\mathscr{T}_E(\lambda \cdot x^{1/4})$ is greater than $c \cdot x^{1/2}$. To prove Theorem 2, then, it suffices to show that the fibers of the mapping

$$(*) \qquad \begin{gathered} \mathscr{T}_E(\lambda \cdot x^{1/4}) \to \mathscr{S}_E(x) \\ (u, v) \mapsto D = v \cdot f(u, v) \end{gathered}$$

have cardinality bounded above by $o(x^{\delta})$ for any $\delta > 0$.

For a given D, consider the (u, v) solving the equation $D = v \cdot f(u, v)$. Clearly, if v is specified then there can be at most three distinct u's verifying this equation. Moreover, v is a divisor of D. Thus the cardinality of any fiber is bounded above by $3 \cdot d(D)$ where $d(D)$ is the number of positive divisors of d. Since $D \leq x$, the well-known inequality $d(x) = o(x^{\delta})$ [HW, 18.1, Theorem 315] allows us to conclude the proof of Theorem 2. □

As for Theorem 1, let f be a cuspidal newform of weight 2 with Fourier coefficients in $\mathbb{Z}$, and let E be the (modular) elliptic curve it parametrizes. For a real number x, consider the set $\text{Image}(\mathscr{T}_E(\lambda \cdot x^{1/4})) \subset \mathscr{S}_E(x)$ that we have just constructed. We know two things: (1) If D is in the image of $\mathscr{T}_E(\lambda \cdot x^{1/4}) \to \mathscr{S}_E(x)$, then the sign of the functional equation satisfied by the entire function $L(f, \chi_D, s)$ is $+$, and (2) (by the argument we have just given) the rank of E_D is ≥ 1 (since we have a point of infinite order in $E_D(\mathbb{Q})$). But, by the recent work of Kolyvagin [K1, K2], supplemented by either the main result in [BFH] or [MM], if $L(f, \chi_D, 1)$ were nonzero, the rank of E_D would be 0. Consequently, $\mathscr{R}_f(D)$ is even and > 0. Hence the cardinality of $\text{Image}(\mathscr{T}_E(\lambda \cdot x^{1/4}))$ is $\leq S_f(x)$ and the same estimate coming from the square-free sieve establishes Theorem 1. □

3. THE SQUARE-FREE SIEVE

A classical theorem due to Gegenbauer, proved in 1885 (cf. [HW, 18.6]), asserts that the number of square-free positive integers $\leq x$ is $(6/\pi^2) \cdot x + O(\sqrt{x})$. The more general problem of estimating the number of l-power-free values $f(n)$ of a polynomial f of one variable of degree d has a large literature, at least when $l \geq d - 1$ (see the discussion of it in [H, Chapter 4]). The case where $l = d - 1$ is significantly harder than the case $l \geq d$. Hooley (loc. cit.) treats $l = d - 1$ by a method combining what he calls the "simple asymptotic sieve" and Gallagher's form of the "large sieve." We are particularly interested in $l = 2$, $d = 3$, i.e., we wish to estimate the number of square-free values of cubic polynomials. We shall refer to Hooley's method in this case as the "square-free sieve" method. Hooley proves that if $f(u)$ is a cubic polynomial with coefficients in $\mathbb{Z}$, the number of positive integers n not exceeding x such that $f(n)$ is square-free is $A \cdot x + O\{x \cdot \log^{-1/2}(x)\}$ where A is a nonnegative constant given explicitly as an infinite product, and which does not vanish provided that $f(x)$ is not divisible by the square of a nonunit in $\mathbb{Z}[x]$. Hooley, in fact, treats explicitly only the case where f is irreducible, for if it is reducible, the argument is much easier, and gives a better error term, namely $O\{x \cdot \log^{-1}(x)\}$.

For our application to elliptic curves, however, we need to estimate square-free values of polynomials of two variables. Specifically, we deal with a homogeneous cubic form in two variables, $f(u, v)$ and we estimate the number of pairs of integers (a, b) both between 0 and x such that $b \cdot f(a, b)$ is square-free. Homogeneity of the form f is strongly used. The format of our treatment is to follow Hooley's proof very closely. We even reduce our most delicate error estimate, via a fibering argument , to a one-variable situation handled by Hooley. We show that the constants obtained from Hooley's argument that are independent of the fiber. We then return to our two-variable situation and derive the two-variable error estimate that we need. Our argument, with no change, treats the case of square-free homogeneous forms in two variables with no square factors, and such that all irreducible factors have degree ≤ 3. We formulate our results in that setting.

4. The main terms and the error terms

Now let $F(u, v)$ be a nontrivial homogeneous polynomial of degree d with coefficients in $\mathbb{Z}$. After an appropriate linear change of variables ($u \mapsto \alpha u+\beta v$; $v \mapsto \gamma u+\delta v$ for $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$) we may (and do) suppose that the coefficients of u^d and of v^d are nonzero. Call these coefficients l and m, respectively. Write $F(u, v) = l \cdot \prod(u-\vartheta_i v)$ where the ϑ_i are algebraic numbers ($i = 1, \dots, d = \text{degree}(F)$). Let $\Delta = \Delta(F)$ denote the absolute value of the quantity $ml^{2d-1}\prod(\vartheta_i - \vartheta_j)$, the product being taken over all pairs of distinct indices $i, j = 1, \dots, d$. Thus Δ (essentially the discriminant of the form F) is a nonnegative integer, nonzero if and only if F has no square factors. We suppose that F has no square factors.

Suppose, further, that all of the irreducible factors of F are of degree ≤ 3. We fix a modulus $M \geq 1$ and two integers a_0 and b_0, both relatively prime to M. We want to study how often $F(a, b)$ is square-free, when we restrict a and b to be congruent to a_0 and b_0 modulo M, respectively.

Define $N(x)$ as the number of pairs of integers (a, b) satisfying $0 \leq a, b \leq x$, $a \equiv a_0 \pmod M$, $b \equiv b_0 \pmod M$ such that $F(a, b)$ is square-free. We define the principal term:

> $N'(x) =$ the number of pairs of integers (a, b) with $0 \leq a, b \leq x$, $a \equiv a_0 \pmod M$, and $b \equiv b_0 \pmod M$ such that $F(a, b)$ is not divisible by the square of any prime less than or equal to $\xi = (1/3)\log x$,

and the error terms E_i for $i = 0, \dots, t$. Put:

> $E_0(x) =$ the number of pairs of integers (a, b) with $0 \leq a, b \leq x$ such that a and b are both divisible by some prime greater than ξ.

Write $F(u, v) = \prod f_i(u, v)$ where $f_i(u, v)$ are irreducible homogeneous forms with coefficients in $\mathbb{Z}$, $i = 1, \dots, t$ and set

> $E_i(x) =$ the number of pairs of integers (a, b) with $0 \leq a, b \leq x$ such that $f_i(a, b)$ is divisible by the square of some prime greater than ξ for $i = 1, \dots, t$.

Put $E(x) = \sum_{i=0}^{t} E_i(x)$.

Proposition 2. *For x sufficiently large, we have*:

$$N'(x) - E(x) \leq N(x) \leq N'(x).$$

Proof. The inequality asserted in Proposition 2 is valid for all x such that $\xi > \Delta = \Delta(F)$. This comes directly from the observation that if x is such that $\xi > \Delta$ and (a, b) is a pair of integers contributing to $N'(x) - N(x)$, i.e., if $0 \leq a, b \leq x$, $a \equiv a_0 \pmod{M}$, $b \equiv b_0 \pmod{M}$ and there is a prime number $p > \xi$ such that p^2 divides $F(a, b)$, then since p cannot divide Δ, either p divides both a and b or p^2 divides $f_i(a, b)$ for some $i = 1, \dots, t$. □

Comments. We will write Proposition 2 in the form

$$N(x) = N'(x) + O(E(x))$$

to emphasize that $N'(x)$ supplies us with the dominant term, and $E(x)$ with the error term (this is why we do not bother with congruence conditions in the definition of the E_i). Heuristically we view ξ as giving us a notion of *small prime* relative to x and, in effect, we show that the square-free condition is well approximated by the condition that the number not be divisible by the square of any small prime. The choice of $\xi = (1/3)\log x$ is not crucial but we will make use of the fact that if l is square-free and all prime factors of l are less than or equal to ξ, then

$$l \leq \prod_{p<\xi} p \leq e^{2\xi} \leq x^{2/3}.$$

(One can take ξ to be any fixed monotonically increasing function of x, which is $\geq \log^{1/2}(x)$, such that $e^{2\xi} \leq x^{\tau}$ for some real number $\tau < 1$.)

5. Counting points modulo m

In this section we suppose given a homogeneous form $F(u, v)$ of degree d, with coefficients in $\mathbb{Z}$, with no square factors. We do not assume that all its irreducible factors are of degree ≤ 3. We also suppose given congruence data $(a_0, b_0) \bmod M$.

Attached to this data we shall define a multiplicative function

$$\rho = \rho_{\{F\,;(a_0, b_0) \bmod M\}}$$

taking values in nonnegative integers as follows:

> Put $\rho(1) = 1$, and for an integer $m \geq 2$ define $\rho(m)$ to be the number of solutions, noncongruent modulo m, of the equation $F(a, b) \equiv 0 \bmod m$, in integers (a, b), satisfying the auxiliary conditions $a \equiv a_0 \pmod{M}$ and $b \equiv b_0 \pmod{M}$.

Note that if $\gcd(m, M) = 1$, the auxiliary congruence conditions do not affect the value of $\rho(m)$; if $\gcd(m, M) = \delta$, the congruence conditions eliminate all but m^2/δ^2 congruence classes. It is convenient, in this case to make the following further definition:

Definition. If $\gcd(m, M) = \delta$, we define $r(m) = \delta^2\rho(m)$.

Lemma 1. (1) *The functions* ρ *and* r *are multiplicative, i.e., if* $\gcd(m, n) = 1$, *then* $\rho(mn) = \rho(m)\rho(n)$ *and* $r(mn) = r(m)r(n)$.

(2) *Let* $\rho_1(p)$ *denote the number of solutions* mod p *of* $F(x, 1) \equiv 0 \bmod p$. *Let* p *be a prime number that does not divide* Δ. *Then, for* $\nu \geq 1$,

$$\rho(p^\nu) \leq p^{2[\nu-\nu/d]} + \rho_1(p) \cdot \sum_{\lambda=0}^{\langle \nu/d \rangle} \varphi(p^{\nu+(d-2)\lambda}),$$

where φ *is Euler's phi-function, and* $[c]$ *(resp.,* $\langle c \rangle$*) denotes the largest integer* $\leq c$ *(resp.,* $< c$*). If* p *does not divide* $M \cdot \Delta$, *then the inequality above is an equality.*

Proof. Assertion (1) follows from the Chinese Remainder Theorem. As for assertion (2), let us show the *equality* when p does not divide $M \cdot \Delta$, the full statement then following from the fact that the ρ attached to F and congruence conditions mod M is $\leq$ the ρ attached to the same F and no congruence conditions.

Since p does not divide Δ, and therefore it divides neither the coefficients of the u^d-term nor of the v^d-term in $F(u, v)$, one sees that

(i) if the pair of integers (a, b) is a solution of $F(a, b) \equiv 0 \bmod p^\nu$ and either $\operatorname{ord}_p(a)$ or $\operatorname{ord}_p(b)$ is $< \nu/d$, then we have equality $\operatorname{ord}_p(a) = \operatorname{ord}_p(b)$. Call the common value, in this situation, the ord of the solution (a, b).

(ii) any pair (a, b) of integers with $\operatorname{ord}_p(a) \geq \nu/d$ and $\operatorname{ord}_p(b) \geq \nu/d$ is a solution of $F(a, b) \equiv 0 \bmod p^\nu$. Call such a solution a *solution of high divisibility.*

The proof of the formula in (2) in the case where p does not divide $M \cdot \Delta$ is then a direct count, where the term $p^{2[\nu-\nu/d]}$ is the number of solutions of high divisibility and the term $\rho_1(p) \cdot \varphi(p^{\nu+(d-2)\lambda})$ is the number of solutions of $\operatorname{ord} = \lambda$ for $\lambda < \nu/d$. □

In a recent letter to us, Diane Meuser provided us with the proof the following lemma, which, as she explained, comes fairly directly from Igusa's techniques (specifically, [I, Chapter III, §3.5]).

Lemma 2 (Meuser, Igusa). *The generating function*

$$R(T) = \sum_{\nu=0}^{\infty} \rho(p^\nu) \cdot T^\nu$$

is a rational function with at worst simple poles at $T = p^{-1}$, *and at* $T = \zeta \cdot p^{-2+2/d}$ *where* ζ *runs through all* d*th roots of unity. The power series above converges in the open disk about* $T = 0$ *of radius* $1/p^{2-2/d}$.

Proof. First note that the statement of our lemma follows immediately from Lemma 1 if p does not divide $M\Delta$, for $R(T)$ is then

$$\sum_{\nu=0}^{\infty} p^{2[\nu-\nu/d]}T^{\nu} + \rho_1(p)(p-1)\sum_{\lambda=0}^{\infty}\sum_{\nu=d\lambda+1}^{\infty} p^{\nu-1+(d-2)\lambda}T^{\nu},$$

which can be directly calculated to be the rational function

$$P(T)/(1-pT)(1-p^{2d-2}T^{d}),$$

where

$$P(T)=1+(1+\rho_1(p)(p-1))T+\sum_{j=2}^{d-1}p^{2j-2}(1-p^{3})T^{j}-p^{2d+1}T^{d}.$$

We now treat the general case. Let $\mathscr{X}$ be the complement of the zero-locus of $F(u,v)$ in $\mathbb{A}^2=\mathbb{Z}_p\times\mathbb{Z}_p$, viewed as p-adic manifold. Let $|\ |$ denote normalized absolute value (i.e., $|p|=1/p$) and consider Igusa's zeta function given by the singular integral

$$Z(t)=\int_{\mathscr{X}}|F(u,v)|^{s}\cdot|du\,dv|,$$

where $t=p^{-s}$. Then the connection between $Z(t)$ and $R(T)$ is easily calculated to be

$$(p^2T-1)\cdot R(T)=p^2T\cdot Z(p^2T)-1$$

(see [I, §3.5, p. 97]). It follows from a quite general result (see loc. cit. §3.1) that $Z(t)$ is a rational function of t, and hence so is $R(T)$. Since $Z(1)=1$, it follows further that the poles of $R(T)$, with multiplicity, are precisely the poles of $Z(p^2T)$, taken as a function of T.

The lemma will then follow if we show that

$$Z(t)=\frac{P(t)}{(p-t)(p^2-t^d)},$$

where $P(t)$ is a polynomial. Consider the quadratic transformation with center $(0,0)\in\mathbb{A}^2$,

$$\begin{tikzcd} \mathscr{Y} \arrow[d, "h"'] & \subset \mathbb{A}^2\times\mathbb{P}^1 \\ \mathbb{A}^2, & \end{tikzcd}$$

where $\mathbb{A}^2\times\mathbb{P}^1$ is coordinatized by $\{(u,v);(w_1:w_2)\}$, $\mathscr{Y}$ is the locus

$$u\cdot w_2-v\cdot w_1=0,$$

and h is the restriction of the projection homomorphism. We may write our singular integral as

$$Z(t)=\int_{\mathscr{Y}}|F\circ h|^{s}\cdot h^{*}|du\,dv|.$$

Now $\mathscr{Y}$ can be covered by two affine neighborhoods $\mathscr{Y}_1$, $\mathscr{Y}_2$ corresponding to $w_1 \neq 0$ and to $w_2 \neq 0$ respectively. On $\mathscr{Y}_1$ we may take $u_1 = u$, $v_1 = w_2/w_1$ as coordinates, and identify $\mathscr{Y}_1$ with $\mathbb{Z}_p \times \mathbb{Z}_p$ via (u_1, v_1). We now consider the integral

$$Z_1(t) = \int_{\mathscr{Y}_1} |F \circ h|^s \cdot h^*|du\,dv|,$$

and note that if we express the above integral over $\mathscr{Y}_1$ as a sum of integrals over a disjoint union of small open sets covering $\mathscr{Y}_1$, the contribution to the poles of $Z_1(t)$ come from open sets about the zeros of $F(u, v) = u_1^d \cdot F(1, v_1)$, i.e., about the points $(u_1 = 0, \tilde{v}_1)$ where $\tilde{v}_1 \in \mathbb{Z}_p$ is a zero of $F(1, v_1)$. Fix such a point $(0, \tilde{v}_1)$. Since $F(1, v_1)$ has no multiple roots we may find a small neighborhood $\mathscr{N}$ of $0 \in \mathbb{Z}_p$ such that $(\partial F/\partial v_1)(1, v_1)$ is nonzero and constant for $v_1 \in \mathscr{N}$. Letting $z := F(1, v_1)v_1 \in \mathscr{N}$, we may view $z : \mathscr{N} \cong \mathscr{O} \subset \mathbb{Z}_p$ as a new coordinate for $\mathscr{N}$, where $\mathscr{O}$ is the image of $\mathscr{N}$ under z in $\mathbb{Z}_p$. Taking our open subset of $\mathscr{Y}_1$ to be $\mathbb{Z}_p \times \mathscr{N}$, parametrized by the variables (u_1, z), the contribution to the integral $Z_1(t)$ coming from this open set is easily computed to be

$$c \cdot \iint_{\mathbb{Z}_p \times \mathscr{O}} |u_1|^{ds+1} \cdot |z|^s \cdot |du_1|\,|dz|,$$

which splits into a product of two simple integrals that contribute to denominators $(1 - p^{-2}t^d)$ and $(1 - p^{-1}t)$, respectively. An identical argument for the contribution to the integral coming from $\mathscr{Y}_2$ concludes the proof of our lemma. □

Lemma 3. (1) *If p^ν ranges through all prime powers, then $\rho(p^\nu) = O(p^{\nu(2-2/d)})$ and $r(p^\nu) = O(p^{\nu(2-2/d)})$;*

(2) *If m ranges through square-free integers, we have: $\rho(m^2) = O(m^2 \cdot d_k(m))$ for $k = d + 1$, where $d_k(m)$ denotes the number of ways in which m can be written as a product of k factors.*

Proof. (1) The inequality in (2) of Lemma 1 gives us what we wish for the set of all p^ν where p is any prime number not dividing Δ and ν any integer ≥ 1. This leaves us the finite set of primes dividing Δ with which to contend. If we show that $\rho(p^\nu) = O(p^{(\nu(2-2/d)})$ for all $\nu \geq 1$ and for each such prime number separately, then part (1) of our lemma will be proved. But this estimate is precisely what comes from the conclusion of Lemma 2, i.e., the convergence of the power series $R(T)$ in the open disk of radius $1/p^{2-2/d}$ about $T = 0$.

(2) This follows directly by applying the inequality (2) of Lemma 1 to obtain an upper bound for $\rho(p^2)$ for all prime numbers p not dividing Δ, noting that $\rho_1(p) \leq d$. □

6. Averaging estimates of rational points mod m

If w is any real (or complex) number, and n a positive integer, let $\sigma_w(n)$ denote the sum of the wth powers of the positive divisors of n. Then $\sigma_w(n)$ is a multiplicative function.

Proposition 3. *Let w be a negative real number. Suppose that $F(u, v)$ is an irreducible homogeneous form of degree d over $\mathbb{Z}$, and that $(a_0, b_0) \bmod M$ are congruence conditions. Let*

$$\rho = \rho_{F, \{a_0, b_0 \bmod M\}}.$$

Then

$$\sum_{1 \le m \le x} \sigma_w(m) \cdot \rho(m)/m = O(x),$$

where the summation is taken over all positive integers $m \le x$.

Proof. We begin with a short discussion of *prime-power functions* h which, by definition, are real-valued functions on the set of all prime powers $p^\nu \mapsto h(p^\nu)$ (p ranges through all prime numbers and $\nu > 0$). A prime-power function h extends (multiplicatively) to a unique multiplicative function, which we denote $\tilde{h}$. By the *Dirichlet series associated to* h, we mean

$$H(s) = \sum_{m \ge 1} \tilde{h}(m) \cdot m^{-s}.$$

Say that a prime-power function h is *negligible* if there are positive constants $c > 1$, $\sigma < 1$, and $A > 0$ such that

$$\left| \log\left\{ 1 + \sum_{\nu \ge 1} |h(p^\nu)| \cdot p^{-\nu s} \right\} \right| \le A p^{-c}$$

for all real $s \ge \sigma$ and all prime numbers p.

The following useful sufficient criterion for negligibility is easily proved:

Lemma 4. *Let h be a prime-power function such that there is a positive number δ, a positive integer μ, and a real number $b < 1 - 1/\mu$ for which*

(a) *there is a positive number A such that for all $j < \mu$, and all prime numbers p, we have $|h(p^j)| \le A p^{j-1-\delta}$;*
(b) *for all prime-powers p^ν we have $h(p^\nu) = O(p^{\nu \cdot b})$.*

Then h is negligible.

Proof. Straightforward. □

Lemma 5. *A finite linear combination of negligible prime-power functions is negligible. If h is a negligible prime-power function, then the abscissa of absolute convergence of its associated Dirichlet series is < 1.*

Proof. Straightforward. □

Lemma 6. *Let h be a nonnegative real-valued prime-power function with the property that if $\tilde{h}$ is its associated multiplicative function then $\sum_{m\le x}\tilde{h}(m) = O(x)$.*

Let ε be any negligible prime-power function, and let $\psi = h + \varepsilon$. Let $\tilde{\psi}$ denote the multiplicative function associated to ψ.

Then $\sum_{m\le x}\tilde{\psi}(m) = O(x)$.

Proof. Say that a positive integer d is a *clean* divisor of m if it is a divisor of m which is relatively prime to m/d. We have that $\tilde{\psi}(m) = \sum \tilde{h}(d)\cdot\tilde{\varepsilon}(m/d)$, where d ranges through all clean divisors of m. So

$$\sum_{m\le x}\tilde{\psi}(m) = \sum_{m\le x}\sum_{d \text{ clean divisor}}\{\tilde{h}(m/d)\cdot\tilde{\varepsilon}(d)\}$$
$$= \sum_{d\le x}\tilde{\varepsilon}(d)\cdot\left\{\sum_{\substack{n\le x/d\\(n,d)=1}}\tilde{h}(n)\right\}.$$

Since $\tilde{h}$ is nonnegative, we have

$$\left|\sum_{m\le x}\tilde{\psi}(m)\right| \le \sum_{d\le x}|\tilde{\varepsilon}(d)|\cdot\left\{\sum_{n\le x/d}\tilde{h}(n)\right\}$$
$$\le O\left\{x\cdot\sum_{d\le x}|\tilde{\varepsilon}(d)|/d\right\}.$$

But by Lemma 5, $\sum|\tilde{\varepsilon}(d)|/d$ converges, giving Lemma 6. □

The key point to the proof of our Proposition (as in, e.g., [E, pp. 14, 15]) is to compare the prime-power function $t(p^\nu) := \sigma_w(p^\nu)\cdot\rho(p^\nu)/p^\nu$ with the prime-power function $t_K(p^\nu)$ whose associated Dirichlet series is the Dedekind zeta function of the field K of degree d over $\mathbb{Q}$ that is obtained by adjoining a root of the polynomial $F(u, 1)$. Specifically, we prove the key lemma below.

Lemma 7. *The prime-power function $t - t_K$ is negligible.*

The proof of our proposition follows directly: Using the fact that the Dedekind zeta-function of K has $\sigma = 1$ as abscissa of absolute convergence, and has a meromorphic continuation to the entire complex plane with its only pole for $\mathrm{Re}(s) > 0$ a simple pole at $s = 1$, the (nonnegative) multiplicative function $\tilde{t}_K$ satisfies the hypothesis on $\tilde{h}$ in Lemma 6. Therefore $\tilde{t}$ satisfies the conclusion of Lemma 6.

Proof of Lemma 7. Consider the following list of prime-power functions:

$$\alpha(p^\nu) = t(p^\nu) = \sigma_w(p^\nu)\cdot\rho(p^\nu)/p^\nu \quad \text{if } p \text{ divides } M\cdot\Delta,$$
$$= 0 \quad \text{if } p \text{ does not divide } M\cdot\Delta.$$

$$\beta(p^\nu) = \sigma_w(p^\nu)\cdot p^{2[\nu-\nu/d]-\nu} \quad \text{if } p \text{ does not divide } M\cdot\Delta,$$
$$= 0 \quad \text{if } p \text{ divides } M\cdot\Delta.$$

$$\gamma(p^\nu) = \sigma_w(p^\nu)\cdot\rho_1(p)\cdot\sum_{\lambda=0}^{\langle\nu/d\rangle}\varphi(p^{\nu+(d-2)\lambda})\cdot p^{-\nu} \quad \text{if } p \text{ does not divide } M\cdot\Delta,$$
$$= 0 \text{ if } p \text{ divides } M\cdot\Delta.$$

Since $\alpha+\beta+\gamma-t_K = t-t_K$, to prove the key lemma we prove that α, β, and $\gamma-t_K$ are each negligible. We use our criterion for negligibility (Lemma 4). Note that (under the hypothesis that w is less than 0) $\sigma_w(p^\nu)$ is universally bounded from above (by $1/(1-2^w)$) and therefore, that factor does not affect our calculations to determine whether the criteria of Lemma 4 are met.

As for α, since $\alpha(p^\nu) = 0$ unless p lies in a certain finite set, we see that the criteria of Lemma 4 are met if for any positive real number δ and any positive integer μ criterion (a) of Lemma 4 is satisfied. Take $\mu = d$. Then, taking $b = 1-2/d$, (b) of Lemma 4 is also satisfied, as is seen using assertion (1) of Lemma 3.

As for β, take $\delta = 1$, $\mu = d$, and $b = 1-2/d$.

Now for γ, let γ_1 denote the prime-power function defined by the rule: $\gamma_1(p) = \rho_1(p)$ for all prime numbers p not dividing $M\cdot\Delta$, and $\gamma_1(p^\nu) = 0$ if $\nu \geq 2$, or if p divides $M\cdot\Delta$. Let $\gamma' = \gamma-\gamma_1$. Another straightforward calculation shows that γ' satisfies our criteria for negligibility (conditions (a) and (b) of Lemma 3) where we may take $\delta = 1$, $\mu = d$, and $b = 1-2/d$. It remains then, to show that $t' = t_K - \gamma_1$ is negligible. But for p not dividing $M\cdot\Delta$, $\rho_1(p)$, i.e., the number of solutions of $F(u, 1) \equiv 0 \bmod p$, is the number of primes of the field K of norm p, i.e., is equal to $t_K(p)$. Thus, for p not dividing $M\cdot\Delta$, $t'(p^\nu) = 0$ if $\nu = 1$ and $= t_K(p^\nu)$ if $\nu \geq 2$. Standard calculations (compare [E, pp. 14, 15]) give that t' is negligible. □

Corollary. $\sum_{m\leq x}\sigma_{-1/2}(m)\cdot\rho(m)/m = O(x)$.

7. The density estimate

We suppose, as in §4, that $F(u, v)$ is a homogeneous form with coefficients in $\mathbb{Z}$, possesses no square factors, and is such that all of its irreducible factors are of degree ≤ 3.

Lemma 8. *Let*

$$A = (1/M^2)\prod_p(1-r(p^2)/p^4).$$

Then as $x \to \infty$,

$$N'(x) = Ax^2 + O(x^2/\log x).$$

Proof. For any positive integer n, put $N_n(a_0, b_0 \bmod M; x) =$ the number of pairs of integers (a, b) with $0 \le a, b \le x$, such that $F(a, b)$ is divisible by n, and such that (a, b) satisfies the auxiliary conditions $a \equiv a_0 \pmod M$ and $b \equiv b_0 \pmod M$. If $M = 1$, i.e., if we have set no auxiliary conditions, we abbreviate the notation $N_n(a_0, b_0 \bmod M; x)$ to $N_n(x)$.

Now let l range over 1 and the square-free numbers all of whose prime divisors are less than or equal to ξ. For each l, let $\delta(l) = \gcd(l^2, M)$. Then we have

$$N_{l^2}(a_0, b_0 \bmod M; x) = \rho(l^2)\{\delta(l)^2 x^2/l^4 M^2 + O(x/l^2)\}.$$

(For each fixed congruence class modulo l^2 of solutions of $F(u, v) \equiv 0 \bmod l^2$ satisfying the congruence condition, count the number of representatives in the square $0 \le a, b \le x$.) Then by the inclusion-exclusion principle,

$$\begin{aligned}
N'(x) &= (1/M^2)\sum_l \mu(l)\rho(l^2)(x^2\delta(l)^2/l^4 + O(x/l^2)) \\
&= (x^2/M^2)\sum_l \mu(l)\rho(l^2)\delta(l)^2/l^4 + O\Big(x \sum_{l \le x^{1/3}} \rho(l^2)/l^2\Big) \\
&= (x^2/M^2)\sum_l \mu(l)r(l^2)/l^4 + O\Big(x \sum_{l \le x^{1/3}} \rho(l^2)/l^2\Big) \\
&= (x^2/M^2)\prod_{p<\xi}(1 - r(p^2)/p^4) + O\Big(x \cdot \sum_{l \le x^{1/3}} d_k(l)\Big) \\
&\qquad\qquad [\text{by Lemma 3 (2), where } k = \text{degree } F + 1] \\
&= (x^2/M^2)\prod(1 - r(p^2)/p^4) + O(x^2/\xi \log \xi) + O(x \cdot x^{1/3} \log^{k-1} x) \\
&= (x^2/M^2)\prod(1 - r(p^2)/p^4) + O(x^2/\log x),
\end{aligned}$$

as desired. □

It remains to estimate the various error terms; $E_0(x)$ and $E_i(x)$ for an index i such that f_i is of degree one are easy:

Lemma 9. *We have $E_i(x) = O(x^2/\log x)$ if $i = 0$, or if $i \ge 1$ and f_i is of degree one.*

Proof. If $i = 0$, we just count elements in congruence classes:

$$\begin{aligned}
E_0(x) &\le \sum_{p>\xi}(x^2/p^2 + O(x/p)) \\
&= O(x^2/\xi \log \xi) = O(x^2/\log x).
\end{aligned}$$

Now let $i \ge 1$ be an index such that $f_i(u, v) = \lambda u + \mu v$, for $\lambda, \mu \in \mathbb{Z}$. We suppose that x is sufficiently large so that $\xi > \Delta$, and therefore no prime number $p > \xi$ divides both λ and μ. For any such p we estimate the number of (a, b) with $0 \le a, b \le x$ such that $\lambda a + \mu b \equiv 0 \bmod p^2$ as being

$x^2/p^2 + O(x/p)$ and exactly the same calculation as for $E_0(x)$ obtains the same bound. □

8. The principal error estimate

We now consider the estimates for $E_i(x)$ when f_i is of degree ≤ 3, the main part of the proof being when it is of degree 3.

Proposition 4. *If f_i is of degree ≤ 2, then*

$$E_i(x) = O\{x^2 \cdot \log^{-1}(x)\},$$

while if f_i is of degree 3, then

$$E_i(x) = O\{x^2 \cdot \log^{-1/2}(x)\}.^5$$

Proof. The case of degree one having been taken care of in Lemma 4, let $f = f_i$ be an irreducible factor of degree 2 or 3. Note that we may now ignore the congruence restrictions completely. We begin by setting $\eta = c \cdot x$ if the degree of f is 2 (where c is a positive constant chosen sufficiently large to insure that $N_{p^2}(x)$ vanishes for prime numbers $p > \eta$ and large values of x) and setting $\eta = x \log^{1/2} x$ if the degree of f is 3. We have

$$E_1(x) \leq \sum_{\xi<p<\eta} N_{p^2}(x) + \sum_{p>\eta} N_{p^2}(x).$$

Lemma 10. $\sum_{\xi<p<\eta} N_{p^2}(x) = O(x^2/\log x)$ *in case the degree of f equals 2 and* $\sum_{\xi<p<\eta} N_{p^2}(x) = O(x^2/\log^{1/2} x)$ *in case degree $f = 3$.*

Proof. By Lemma 1, we have $\rho(p^2) = O(p^2)$; then

$$\begin{aligned}\sum_{\xi<p<\eta} N_{p^2}(x) &= \sum_{\xi<p<\eta} \rho(p^2)(x^2/p^4 + O(x/p^2)) \\ &= O\Big(x^2 \sum_{\xi<p<\eta} 1/p^2\Big) + O\Big(x \cdot \sum_{\xi<p<\eta} \rho(p^2)/p^2\Big) \\ &= O(x^2/\xi \log \xi) + O(x\pi(\eta)) \\ &= O(x^2/\log x) + O(x\eta/\log \eta).\end{aligned}$$

This gives the desired estimates. □

It remains to estimate $P(x) = \sum_{p>\eta} N_{p^2}(x)$.

When f is of degree 2 we have that for large enough x, $N_{p^2}(x) = 0$, if $p > \eta$ in view of our choice of η. This gives the estimate for f of degree 2. From now on, we suppose that f is of degree 3. We estimate $P(x)$ by a fibering argument, reducing our question to a similar estimate for one-variable polynomials dealt with in [H, Chapter 4, §3].

[5] This error term has been improved; see the note at the end of this section.

For each $b \leq x$, let $f_b(u)$ denote the cubic polynomial $f(u, b)$. Let $\Upsilon(b, m)$ denote the number of integers a in the range $0 \leq a \leq x$ such that $f_b(a) = m \cdot p^2$ where p is a prime number $> \eta$. Thus, our $\Upsilon(b, m)$ is simply Hooley's $\Upsilon(m)$ for the polynomial f_b. Now Hooley produces an estimate for $\Upsilon(m)$ (cf. [H, §3, Formula (132)]) which, when expressed for the polynomial f_b, gives

$$\Upsilon(b, m) = O_b\{(x/m)^{1/2}\sigma_{-1/2}(m)\rho_b(m)\},$$

where $\sigma_{-1/2}(m)$ is the sum of the reciprocals of the square roots of positive divisors of m, $\rho_b(m)$ is the number of (incongruent) roots of the congruence $f_b(a) \equiv 0 \bmod m$, and the subscript b on O indicates that, a priori, the implicit constant depends upon the polynomial, i.e., depends upon b. The key observation for us is that this constant may be taken to be independent of b. Explicitly,

Lemma 11. *There is a constant C such that*

$$\Upsilon(b, m) \leq C \cdot \{(x/m)^{1/2} \cdot \sigma_{-1/2}(m) \cdot \rho_b(m)\}$$

for all integers m, $b \geq 0$.

Proof. Let m and b be positive integers, and let q be a prime number which does not divide m. Set $S_b(m, q) =$ the number of (incongruent) solutions (u, w) of the congruence $f_b(u) \equiv m \cdot w^2 \bmod q$, where w is not congruent to $0 \bmod q$.

Sublemma. *There is a constant C_1 such that for all b, m, and q as above, we have:*

$$|S_b(m, q) - q| < C_1 \cdot q^{1/2}.$$

Proof. We use the fact that $f_b(u)$ is a cubic polynomial in u, such that the coefficient of the u^3-term is a nonzero integer independent of b, and we recall that m is a unit mod q. Since the left-hand side of the inequality to be proved is bounded by $q^2 - q$ for any q, it suffices to prove the sublemma under the added restriction that q does not divide 6 times the coefficient of the u^3-term. Then if $f_b(u) \equiv 0 \bmod q$ has no multiple roots, then the well-known inequality for rational points on elliptic curves over finite fields allows us to bound the left-hand side appropriately. If $f_b(u) \equiv 0 \bmod q$ has multiple roots we can compute directly that $S_b(m, q) = q - 1$. □

We now follow [H, §3] in the special case where $r = 3$, and $f = f_b$ to obtain the estimate (132) of loc. cit. noting that the explicit polynomial f_b enters in only two (closely related) places, namely in the setting of a lower bound (called A_4 in [H]) such that for all prime numbers $q > A_4 = A_4(f_b)$ we have that $S_b(m, q) > q^{1/2}$ and in the determination of the constant C_1 of our sublemma. But, by the sublemma, C_1 is independent of b, and consequently so is A_4. This concludes the proof of Lemma 11. □

Now let c' be a constant such that $|f_i(a, b)| < c' \cdot x^3$, for all $0 < a, b < x$ and for large x. Let $\kappa = c' \cdot x/\log x$.

We return to our study of $P(x)$, which is immediately seen to be equal to

$$P(x) = \sum_{0 \le b \le x} \left\{ \sum_{0 \le m \le \kappa} \Upsilon(b, m) \right\}.$$

Reversing the order of summation, we have

$$P(x) = \sum_{0 \le m \le \kappa} \left\{ \sum_{0 \le b \le x} \Upsilon(b, m) \right\}.$$

But as b ranges through all integers between 0 and x, it can go through any given congruence class mod m at most x/m times, giving

$$P(x) \le \sum_{0 \le m \le \kappa} (x/m) \cdot \left\{ \sum_{0 \le b \le m-1} \Upsilon(b, m) \right\},$$

and by Lemma 11,

$$\begin{aligned} P(x) &\le \sum_{0 \le m \le \kappa} (x/m) \cdot \left\{ C \cdot (x/m)^{1/2} \cdot \sigma_{-1/2}(m) \cdot \sum_{0 \le b \le m-1} \rho_b(m) \right\} \\ &\le C \cdot x^{3/2} \cdot \sum_{0 \le m \le \kappa} (m^{-1/2}) \cdot \sigma_{-1/2}(m) \cdot \{\rho(m)/m\} \end{aligned}$$

which by partial summation and the Corollary of §5, is

$$O\{x^{3/2} \cdot \kappa^{1/2}\} = O\{x^2 \cdot \log^{-1/2}(x)\}. \quad \square$$

Putting all these estimates together gives:

Theorem 3. *Let $F(u, v)$ be a homogeneous polynomial with coefficients in $\mathbb{Z}$ without square factors such that all of its irreducible factors are of degree ≤ 3. Let M be an integer, and let a_0 and b_0 be integers relatively prime to M. Finally, let $N(x)$ denote the number of pairs of integers (a, b) satisfying $0 \le a, b \le x$, $a \equiv a_0 \pmod{M}$, and $b \equiv b_0 \pmod{M}$ for which $F(a, b)$ is square-free. Then, as $x \to \infty$, we have*

$$N(x) = Ax^2 + O(x^2/\log^{1/2} x).$$

Here the constant A is given by

$$A = (1/M^2) \prod_p (1 - r(p^2)/p^4),$$

where $\rho(p^2)$ denotes the number of noncongruent solutions of $F(u, v) \equiv 0$ mod p^2 *and $r(p^2)$ is defined to be $(\gcd(p^2, M))^2 \rho(p^2)$.*

Note. As discussed in the introduction, the reader is referred to Greaves's preprint [Gr] for improvements of the above theorem, giving what are currently the strongest results known concerning square-free values of binary forms. Specifically Greaves's method can handle binary forms whose irreducible factors over $\mathbb{Z}$ have degree ≤ 6, and In the case where the irreducible factors have degree ≤ 3, he has a better error term than ours, namely $O(x^2/\log x)$.

9. Nonvanishing criteria for the constant A

For our applications we must have a criterion for when the constant A in Theorem 3 does not vanish. Set $A_p = (1 - r(p^2)/p^4)$.

Proposition 5. (1) *The constant A is zero if and only if $A_p = 0$ for some prime number p.*

(2) *A_p vanishes if p^2 divides all the coefficients of $F(u, v)$.*

(3) *Suppose, now, that p^2 does not divide all the coefficients of $f(u, v)$, and that p divides M. Then a necessary and sufficient condition for A_p to vanish is that either* (i) *or* (ii) *below hold.*

(i) *p^2 divides M and we have restricted to a congruence class, which is a solution of $F(u, v) \equiv 0 \bmod p^2$.*

(ii) *p divides M, $M \not\equiv 0 \bmod p^2$, and we have restricted to a congruence class (a_0, b_0), which represents a singular point of the scheme $F(u, v) \equiv 0 \bmod p$.*

(4) *Suppose, now, that p^2 does not divide all the coefficients of $F(u, v)$, and that p does not divide M. Then A_p is nonzero if $p > \text{degree}(F)$.*

(5) *Suppose that $f(u, v)$ is a homogeneous form of degree 3 and set $F(u, v) = v \cdot f(u, v)$. Suppose further that p does not divide all the coefficients of $F(u, v)$ and that p does not divide M. Then A_p is nonzero.*

Proof. (1) Since $r(p^2) = O(p^2)$, the infinite product A is zero if and only if one of the factors $(1 - r(p^2)/p^4)$ vanishes, i.e., if and only if there is a prime number p such that $r(p^2) = p^4$.

(2) Evident.

(3) If M is divisible by p^2, clearly (i) holds if and only if $\rho(p^2) = 1$, i.e., if and only if $r(p^2) = p^4$. If M is divisible by p and not by p^2, then (ii) holds if and only if

$$(\partial F/\partial u)(a_0, b_0) \equiv (\partial F/\partial v)(a_0, b_0) \equiv 0 \mod p,$$

which happens if and only if $(a_0 + p \cdot \lambda, b_0 + p \cdot \mu)$ is a solution of $F(u, v) \equiv 0 \bmod p^2$ for any λ, μ, i.e., $\rho(p^2) = p^2$ or, equivalently, $r(p^2) = p^4$.

(4) If M is not divisible by p, $r(p^2) = \rho(p^2) = p^4$ if and only if all pairs of integers (a, b) are solutions of $F(u, v) \equiv 0 \bmod p^2$. In particular, all pairs

(a, b) yield solutions of $F(u, v) \equiv 0 \bmod p$. But then if $F(u, v)$ is not identically zero mod p, a simple consideration of degrees tells us that this can only happen (i.e., $\rho(p^2) = p^4$) if $p \leq \text{degree}(F)$.

(5) Just write out $F(u, v) = (A \cdot u^3 + Bu^2 \cdot v + C \cdot u \cdot v^2 + D \cdot v^3) \cdot v$. Using the hypotheses on the prime number p, a direct calculation gives congruence conditions on the coefficients A, B, C, D guaranteeing that $F(u, v)$ is identically zero mod p. Note, by the way, that the only primes not covered already by (4) above are $p = 2$ and 3. □

10. Application to elliptic curves

Let M be a positive integer. Any elliptic curve over $\mathbb{Q}$ can be given a model of the form $Y^2 = X^3 + A \cdot X + B$ where A, B are in $\mathbb{Z}$, and are divisible by M, as can immediately be seen by starting with a model as above without the divisibility condition, making the substitution $(X, Y) \mapsto (X/M^2, Y/M^3)$, and then clearing denominators. If $E/\mathbb{Q}$ is an elliptic curve of conductor C, set $M = 12 \cdot C$ and give E a model as above. Now set $f(u, v) = u^3 + A \cdot u \cdot v^2 + B \cdot v^3$ and $F(u, v) = v \cdot f(u, v)$. If a, $b \in \mathbb{Z}$, then $F(a, b) \equiv b \cdot a^3 \bmod M$. By the sign of a pair of congruence classes $(a_0, b_0) \bmod M$, for a_0, b_0 relatively prime to M, we mean the value $\chi_D(-C)$ for any square-free integer $D \equiv b_0 \cdot a_0^3 \bmod M$, where χ_D is the quadratic Dirichlet character attached to the field $\mathbb{Q}(\sqrt{D})$. Quadratic reciprocity guarantees that this value is in fact determined by $D \bmod 4C$, and hence mod M. Given any C (≥ 11 is all we need) there are pairs (a_0, b_0) of congruence classes mod $M = 12C$ of either sign.

Now let f be a cuspidal newform on $\Gamma_0(C)$ of weight 2 with Fourier coefficients in $\mathbb{Z}$ and let $E/\mathbb{Q}$ be the (modular) elliptic curve that f parametrizes. Give E a Weierstrass model as above with $M = 12C$. Choose a pair of congruence classes $(a_0, b_0) \bmod M$ as above, with sign equal to the sign in the functional equation of the L-function $L(f, s)$.

Proposition 6. *Let x be a real number, and keep notation as above. Let $\mathcal{N}(x)$ be the cardinality of the set of pairs of positive integers $(a, b) \equiv (a_0, b_0) \bmod M$ such that $a \leq x$, $b \leq x$, and $F(a, b)$ is square-free. Then*

$$\mathcal{N}(x) = A \cdot x^2 + O\{x^2 \cdot \log^{-1/2}(x)\}$$

where A is a positive constant.

Proof. By Theorem 3 of §8 we have such an estimate with a constant A that might vanish, a priori. We now refer to Proposition 5 of §9 and we shall check that for each prime number p, A_p does not vanish, and therefore by (1) of that Proposition, neither does A.

Since the coefficient of u^3 in $f(u, v)$ is 1, we are not in case (2) of that proposition. For the same reason, by (4), if p does not divide M, then A_p is nonzero. Suppose now that p does divide M. We must show that we are in neither of the cases (i) or (ii) of (3). But this is immediate since we have chosen our pair (a_0, b_0) so that $F(a_0, b_0)$ is a unit modulo M, and hence not a zero of $F(u, v) \equiv 0 \bmod p$. □

Remark. The above proposition is what is needed for Theorem 1 in §1. To get Theorem 2, we use the same proposition, only applied to the appropriate data; namely, E is the elliptic curve given in the statement of Theorem 2, C is its (arithmetic) conductor, and (a_0, b_0) is a pair of congruence classes mod M, relatively prime to M, with sign taken to be $+$ if the rank of E is even and $-$ if it is odd.

References

[BM] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (NS) **23** (1990), 375–382.

[BFH] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543–618.

[E] O. Erdös, *The sum* $\Sigma d\{f(k)\}$, J. London Math. Soc. **27** (1952), 7–15.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979) (M. B. Nathanson, ed.), Lecture Notes in Math., vol. 751, Springer-Verlag, Berlin, New York, and Heidelberg, 1979, pp. 108–118.

[Gou] F. Gouvêa, *The square-free sieve over number fields*, preprint, 1990.

[Gr] G. Greaves, *Power-free values of binary forms*, preprint, Cardiff, 1990.

[H] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Univ. Press **70** (1976).

[HW] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, 1979.

[I] J.-I. Igusa, *Lectures on forms of higher degree*, Tata Inst. of Fund. Research, 1978.

[K1] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, vol. 11, a collection of articles written in honor of the 60th birthday of Alexander Grothendieck (P. Cartier et al., eds.), Progr. Math. **87** (1990), 435–483.

[K2] ——, *Finiteness of* $E(Q)$ *and* $Ш_{E/Q}$ *for a subclass of Weil curves*, Math USSR-Izv. **32** (3) (1989), 523–541. (English Transl.)

[Ko] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math., vol. 97, Springer-Verlag, 1984.

[M] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[MM] M. R. Murty and K. V. Murty, *Mean values of derivatives of modular L-series*, preprint, 1988.

[Se] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440–481.

[Ш] I. Shafarevitch, *Algebraic number fields*, Proc. Internat. Congress, Stockholm, 1962, pp. 163–176; Amer. Math. Soc. Transl. Ser. 2, vol. 31, pp. 25–39.

[T] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

[W] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. **60** (1981), 375–484.

[ZK] D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51–60.

Department of Mathematics and Statistics, Queens University, Kingston, Ontario K7L 3N6, Canada
E-mail address: gouvea@heac.mast.QueensU.Ca

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, Massachusetts 02138
E-mail address: mazur@zariski.harvard.edu