Canad. Math. Bull. Vol. **46** (1), 2003 pp. 71–79

The Number of Fields Generated by the Square Root of Values of a Given Polynomial

Pamela Cutter, Andrew Granville, and Thomas J. Tucker

Abstract. The *abc*-conjecture is applied to various questions involving the number of distinct fields $\mathbb{Q}\big(\sqrt{f(n)}\big)$, as we vary over integers n.

1 Introduction

We first investigate the following problem:

Conjecture 1 *Suppose that $f(x) \in \mathbb{Z}[x]$ has degree ≥ 2 and no repeated roots. Then there are $\sim N$ distinct quadratic fields amongst*

$$\mathbb{Q}\big(\sqrt{f(1)}\big), \mathbb{Q}\big(\sqrt{f(2)}\big), \mathbb{Q}\big(\sqrt{f(3)}\big), \dots, \mathbb{Q}\big(\sqrt{f(N)}\big). \tag{1.1}$$

Conjecture 1 is actually untrue for linear polynomials. Indeed an elementary argument gives:

Theorem 1A *Let $f(x) = ax + b$ with integers $0 \leq b < a < N$ and $\gcd(a, b) = 1$. There are*

$$\left(\frac{6}{\pi^2}\prod_{p\mid a}\Big(1-\frac{1}{p^2}\Big)^{-1}c(a)\right)N + O(\sqrt{aN}\log a)$$

distinct quadratic fields amongst those in (1.1) where $c(a) = \sum_{m\in M_a} 1/m^2$ and M_a is the set of integers m, coprime to a, such that there is no $l < m$ with $l^2 \equiv m^2 \pmod{a}$.

By further elementary arguments one can prove conjecture 1 for quadratic polynomials:

Theorem 1B *Suppose that $f(x) \in \mathbb{Z}[x]$ has degree 2 and no repeated roots. Then there are $N + O(N/\log N)$ distinct quadratic fields amongst*

$$\mathbb{Q}\big(\sqrt{f(1)}\big), \mathbb{Q}\big(\sqrt{f(2)}\big), \mathbb{Q}\big(\sqrt{f(3)}\big), \dots, \mathbb{Q}\big(\sqrt{f(N)}\big).$$

For higher degree polynomials we have proved the conjecture assuming the *abc*-conjecture, using several of the ideas from [3]:

Received by the editors March 26, 2001; revised August 20, 2001.
The second author is supported, in part, by the National Science Foundation.
AMS subject classification: 11N32, 11D41.

***The abc-conjecture* (Oesterlé, Masser, Szpiro)** *Fix $\varepsilon > 0$. If a, b, c are coprime positive integers satisfying $a + b = c$ then*

$$c \ll_\varepsilon N(a,b,c)^{1+\varepsilon}, \tag{1.2}$$

where $N(a,b,c)$ is the product of the distinct primes dividing abc.

A special case of Theorem 1 in [3] states that if we assume the *abc*-conjecture then for $f(x) \in \mathbb{Z}[x]$ without repeated roots with $\gcd\{f(n) : n \in \mathbb{Z}\} = 1$, there exists a constant $c_f > 0$ such that there are $\sim c_f N$ positive integers $n \le N$ for which $f(n)$ is squarefree. (Note that this result can be proved unconditionally if f has degree ≤ 2 using the sieve of Eratosthenes; and was proved unconditionally by Hooley [5] for f of degree 3 by deeper arguments. Perhaps it might be possible to use the techniques of [5] to prove Conjecture 1 for degree 3 polynomials unconditionally).

The main result in this paper is that Conjecture 1 follows from the *abc*-conjecture (a weaker consequence of the *abc*-conjecture was given in Corollary 2 of [3]).

Theorem 1C *If the abc-conjecture is true then Conjecture 1 is also true.*

A key component in the proof of Theorem 1C is the following result (which may be of independent interest) on integral points on $f(x) - cf(y)$, which is proved using Siegel's Theorem.

Theorem 2 *Suppose that $f(x) \in \mathbb{Z}[x]$ has at least three distinct roots. For any fixed $c > 1$ there are at most finitely many integral points (a,b) on the curve $f(x) - cf(y) = 0$.*

A harder though perhaps more important problem is to determine, for a given $f(x) \in \mathbb{Z}[x]$ without repeated roots, an estimate for $A_f(D)$, the number of squarefree integers $d \le D$ such that there exists some integer n with $f(n) = dm^2$ for some integer m. From Theorem 1C we deduce that $A_f(D) \gg D^{1/\deg(f)}$ if the *abc*-conjecture holds. To get an upper bound we use Corollary 1 from [3] (which is deduced from (26) of Elkies' paper [2]):

Lemma 1 *Assume that the abc-conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Then*

$$\prod_{\text{primes } p \mid f(n)} p \gg |n|^{\deg(f)-1-o(1)}.$$

Now, note that in the above case

$$\Big(\prod_{\text{primes } p \mid f(n)} p\Big)^2 = \Big(\prod_{\text{primes } p \mid dm} p\Big)^2 \le (dm)^2 = |df(n)| \ll D|n|^{\deg(f)},$$

and combining this with Lemma 1 shows that that $|n| \ll D^{1/(\deg(f)-2)+o(1)}$. Recalling the definition of the quantity $A_f(D)$ given above, we have now proved:

Theorem 3A *Assume the abc-conjecture. Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Then*

$$D^{1/\deg(f)} \ll A_f(D) \ll D^{1/(\deg(f)-2)+o(1)}.$$

In particular $A_f(D) \ll D^{1/2+o(1)}$ if $\deg(f) \ge 4$.

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

In fact we believe that $A_f(D) = D^{1/\deg(f)+o(1)}$ if $\deg(f) \neq 2$, and we will give a heuristic to justify this for $\deg(f) \geq 3$ in Section 7. For linear polynomials we prove the following, in Section 6.

Theorem 3B *If $f(x) = ax + b$ with $(a, b) = 1$ then*

$$A_f(D) \sim 2^{\alpha(a)} \times \frac{6}{\pi^2} D \prod_{p|a} \frac{p}{2(p+1)},$$

where $\alpha(a)$ equals -1 if $8|a$, equals 0 if $4|a$ but not 8, and equals 1 if 4 does not divide a.

For quadratic polynomials we believe that $A_f(D) = D^{1+o(1)}$ (which might be provable). More precisely we believe that if f is reducible then $A_f(D) \sim c_f D$, and if f is irreducible then $A_f(D) \sim c_f D/\sqrt{\log D}$ for some constants $c_f > 0$. It is easy to see that such a dichotomy exists from the following examples:

Example 1 Consider $f(x) = x^2 - 1$. Then $f(x) = dm^2$ precisely when $x^2 - dm^2 = 1$; in other words, when we have a solution to Pell's equation. Pell's equation always has an integer solution, so $A_f(D) \sim (6/\pi^2)D$.

Example 2 Consider $f(x) = x^2 - 3$. Then $f(x) = dm^2$ is equivalent to $x^2 - dm^2 = 3$; that is, 3 is represented by the principal binary quadratic form of discriminant $4d$. Now 3 is represented by a binary quadratic form of discriminant $4d$ if and only if d is a square mod 3, so that $d \equiv 0$ or $1 \pmod 3$. If that is the case then 3 is represented by a binary quadratic form from the principal genus, of discriminant $4d$, if and only if 3 is a square mod p for every prime p dividing d, so that $p = 3$ or $p \equiv \pm 1 \pmod{12}$. In other words we have $d \equiv 0$ or $1 \pmod 3$, with no prime factors congruent to $\pm 5 \pmod{12}$: By the fundamental lemma of the sieve [4] there are $\asymp D/\sqrt{\log D}$ such integers $d \leq D$. For such d we know that 3 is represented by some form from the principal genus, but it is a relatively deep problem to determine which form(s). However, Cohen and Lenstra conjectured that there is just one class of quadratic forms in each genus for over 75% of real quadratic discriminants, and we expect this to be true for the restricted class of discriminants considered here. Thus we surmise that $A_{x^2-3}(D) \approx D/\sqrt{\log D}$, and a more detailed analysis of the Cohen-Lenstra heuristic leads to the guess that $A_{x^2-3}(D) \sim D/\sqrt{\log D}$.

2 Algebraic Preliminaries

Lemma 2.1 *Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Then there exists a constant $B = B_f$ such that for all prime powers q, there are no more than B values of $a \pmod q$ for which $f(a) \equiv 0 \pmod q$.*

Proof Let K be the splitting field for f over $\mathbb{Q}$, let $\mathcal{P}$ be a prime in K lying over a prime p with ramification index e and with $\mathrm{N}\mathcal{P} = p^g$, let $\alpha_1, \dots, \alpha_n$ be the roots of f, and let p^r be the highest power of p dividing the leading coefficient of f. We

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

will show that for any $m \geq 0$, the number values of $a \pmod{p^m}$ for which $f(a) \equiv 0 \pmod{p^m}$ is at most

$$B_{f,p} := \max_{\mathcal{P}|p} \sum_{i=1}^{n} p^{g(er+v_{\mathcal{P},i})}$$

where $v_{\mathcal{P},i} = \sum_{k\neq i} v_{\mathcal{P}}(\alpha_k - \alpha_i)$. If p does not divide the discriminant D_f of f then $r = 0$ and each $v_{\mathcal{P},i} = 0$, so that $B_{f,p} \leq n$. Therefore $B_f := \max\{n, \max_{p|D_f} B_{f,p}\}$.

Suppose $f(a) \equiv 0 \pmod{p^m}$. Select i such that $v_{\mathcal{P}}(a-\alpha_i) = \max_k\big(v_{\mathcal{P}}(a-\alpha_k)\big)$, so that $v_{\mathcal{P}}(\alpha_i - \alpha_k) \geq \min\big(v_{\mathcal{P}}(a-\alpha_k), v_{\mathcal{P}}(a-\alpha_i)\big) = v_{\mathcal{P}}(a-\alpha_k)$. Therefore

$$em \leq v_{\mathcal{P}}\big(f(a)\big) = er + \sum_k v_{\mathcal{P}}(a-\alpha_k) \leq er + v_{\mathcal{P}}(a-\alpha_i) + \sum_{k\neq i} v_{\mathcal{P}}(\alpha_i - \alpha_k).$$

In other words, $v_{\mathcal{P}}(a-\alpha_i) \geq em - er - v_{\mathcal{P},i}$, so that there are at most $(N\mathcal{P})^{er+v_{\mathcal{P},i}}$ such values of $a \pmod{p^m}$. Summing over i then finishes the proof.

By the Chinese Remainder Theorem we immediately deduce:

Corollary 2.2 *Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Then there exists a constant $B = B_f$ such that there are no more than $B^{\omega(d)}$ values of $a \pmod{d}$ for which $f(a) \equiv 0 \pmod{d}$, where $\omega(d)$ denotes the number of distinct prime factors of d.*

We will now prove a couple lemmas about the nonexistence of various types of low degree factors for certain $f(x) \in \bar{\mathbb{Q}}[x]$.

Lemma 2.3 *Suppose that $f(x) \in \bar{\mathbb{Q}}[x]$ has at least two distinct roots. If c is neither zero nor a root of unity then $f(x) - cf(y)$ has no linear factor in $\bar{\mathbb{Q}}[x, y]$.*

Proof If $f(x)-cf(y)$ has a linear factor $x-ay-b$, with a, b in $\bar{\mathbb{Q}}$, then the linear map $L(y) = ay + b$ has the property that $f\big(L(y)\big) = cf(y)$. This implies that L permutes the roots of f, which means that some power L^k of L fixes all the roots of f. Since there are at least two distinct roots, L^k must be the identity, but this is impossible since then $f(y) = f\big(L^k(y)\big) = c^k f(y)$ and c is not a root of unity.

Lemma 2.4 *Suppose that $f(x) \in \bar{\mathbb{Q}}[x]$ has at least three distinct roots. If c is neither zero nor a root of unity then $f(x) - cf(y)$ has no quadratic factor of the form $x^2 - ay^2 + 2dx + ey + h \in \bar{\mathbb{Q}}[x, y]$.*

Proof Let $g(x) = f(x-d)$ so that $g(x)-cg(y)$ has a factor of the form $x^2-ay^2+\ell y+q$ over $\bar{\mathbb{Q}}$. Define $P(x, y)$ by

$$(x^2 - ay^2 + \ell y + q)P(x, y) = g(x) - cg(y),$$

and let $P_k(x, y)$ be the degree k part of $P(x, y)$. Assuming without loss of generality that g is monic of degree n, we find that $x^2 - ay^2$ divides $x^n - cy^n$ so that n is even,

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

say $2m$, and $c = a^m$, giving $P_{2m-2}(x, y) = (x^{2m} - a^m y^{2m})/(x^2 - ay^2)$. The degree $2m - 1$ terms in the equation above then give

$$(x^2 - ay^2)P_{2m-3}(x, y) + \ell y \frac{(x^{2m} - a^m y^{2m})}{(x^2 - ay^2)} = u(x^{2m-1} - a^m y^{2m-1})$$

for some integer u. Replacing x to $-x$ and subtracting, gives

$$(x^2 - ay^2)\big(P_{2m-3}(x, y) - P_{2m-3}(-x, y)\big) = 2ux^{2m-1},$$

so that $x^2 - ay^2$ divides $2ux^{2m-1}$, which can only happen if $u = 0$. But then $x^2 - ay^2$ divides $-\ell y P_{2m-2}(x, y)$, which can only happen if $\ell = 0$.

We have proved that our quadratic factor must be of the form $x^2 - ay^2 + q$. In fact each $P_{2j-1}(x, y) = 0$ for, if not, select the largest j for which $P_{2j-1}(x, y) \neq 0$ and then $(x^2 - ay^2)P_{2j-1}(x, y) = v(x^{2j+1} - a^m y^{2j+1})$, which is impossible. We deduce that $g(x) - a^m g(y)$ has no terms of odd degree, so that $g(x)$ can be written as $G(x^2)$ for some $G(t) \in \bar{\mathbb{Q}}[t]$. Letting $X = x^2$ and $Y = y^2$, we deduce that $X - aY + q$ is a factor of $G(X) - a^m G(Y)$, and so G has no more than one distinct root by Lemma 2.3. But then g, and so f, can have no more than two distinct roots, contradicting the hypothesis.

Remark It is plausible, following the two previous results, that $f(x) - cf(y)$ has no factor of degree $\leq k$ when c is not a root of unity, and f has more than k distinct roots. However we do not see how to generalize the proofs above.

3 Integer Points on $f(x) - cf(y)$

We will use the following famous theorem due to Siegel, often referred to as Siegel's theorem, in what follows. This will involve introducing the idea of points at infinity, which we now explain. Let $h(x, y)$ be a polynomial in two variables. We will denote the highest degree part of $h(x, y)$ (which is obtained by homogenizing $h(x, y)$ and then setting the homogenizing variable to 0) as $\bar{h}(x, y)$. The linear factors of $\bar{h}(x, y)$ correspond to the points at infinity for the curve $h(x, y) = 0$.

Siegel's Theorem (see [6], or Section 2 of [1] for a contemporary account) *Let $h(x, y)$ be an absolutely irreducible polynomial with coefficients in a number field. If the curve $h(x, y) = 0$ has more than two distinct $\bar{\mathbb{Q}}$-points at infinity, then there are at most finitely many integer points (a, b) on the curve $h(x, y) = 0$.*

Using this we can proceed to the proof of Theorem 2:

Proof of Theorem 2 Suppose $f(x) - cf(y)$ factors over $\bar{\mathbb{Q}}$ into absolutely irreducible factors as $\prod_{i=1}^{r} h_i(x, y)$, each of which has degree ≥ 2 by Lemma 2.3. We will show that each curve $h_i(x, y) = 0$ has at most finitely many integer points.

Since $\prod_{i=1}^{r} \bar{h}_i(x, y) = x^n - cy^n$, and $x^n - cy^n$ has distinct roots, each $\bar{h}_i(x, y)$ has $\deg h_i$ distinct linear factors and so $h_i(x, y) = 0$ has $\deg h_i$ distinct points at infinity. Therefore, by Siegel's theorem (as stated above) we deduce that there are at most finitely many integral points on $h_i(x, y) = 0$ whenever $\deg h_i \geq 3$.

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

We are left with the case where $\deg h_i = 2$. We may assume that $h_i(x, y) = 0$ can be written with rational coefficients, else $h_i(x, y) = 0$ has at most finitely many rational solutions (corresponding to its intersection with its conjugate curves). Now $\bar{h}_i(x, y)$ divides $x^n - cy^n = \prod_{\xi^n=1}(x - \xi\alpha y)$, where α is the positive real n-th root of c, so that $\bar{h}_i(x, y) = (x - \xi_1\alpha y)(x - \xi_2\alpha y)$, for two distinct n-th roots of unity, ξ_1, ξ_2:

- If ξ_1 is real then ξ_2 is real, since $h_i(x, y)$ is real, and thus, since they are distinct real roots of unity, they must be 1 and -1. Therefore $\bar{h}_i(x, y) = x^2 - ay^2$ where a is rational, which is impossible by Lemma 2.4.
- If $\xi_1 = \xi$ is not real then $\xi_2 = \bar{\xi}$, since $h_i(x, y)$ is real. Moreover, the coefficients $\alpha(\xi + \bar{\xi})$ and α^2 are rational, and so $\xi^2 + \bar{\xi}^2 = \big(\alpha(\xi + \bar{\xi})\big)^2/\alpha^2 - 2$ is rational. Therefore ξ^2 generates a field of degree at most two over the rationals, so that ξ^2 is a primitive k-th root unity where $k = 1, 2, 3, 4$ or 6. Now $k = 1$ is impossible as ξ is not real, the case $k = 2$ gives $\bar{h}_i(x, y) = x^2 - ay^2$ for some rational a, which is impossible by Lemma 2.4. The cases $k = 3, 4, 6$ give $\bar{h}_i(x, y) = x^2 - 2bax y + 4ba^2y^2$ for $b = 1, 2, 3$, respectively, where a is rational. Making the change of variables $x = X + aby$ we find that $h_i(x, y) = X^2 + Ay^2 + cX + dy + e$ where $A = b(4 - b)a^2$ is a positive rational number. By further changes of variables to remove the linear terms, and scaling up to make solutions integers, we find that integer points on $h_i(x, y) = 0$ correspond to integer points (u, v) on an ellipse of the form $u^2 + Av^2 = N$; evidently $|u| \le \sqrt{N}$ and $v \le \sqrt{N/A}$ so there are finitely many.

4 Large Squares Dividing $f(n)$

Fix an $\epsilon > 0$ and a sufficiently large integer $y \le N^{1/3}$. We will show that if N is sufficiently large then

$$\#\{n \le N : m^2 | f(n) \text{ for some } m > y\} \le \epsilon N, \tag{4.1}$$

unconditionally if $\deg(f) \le 2$, and assuming the *abc*-conjecture otherwise.

It follows immediately from Theorem 8 of [3] and the discussion preceding it, that if we assume that the *abc*-conjecture is true, then for any fixed $c > 0$ there are $o(N)$ integers $n \le N$ such that $f(n)$ is divisible by the square of a prime $> cN$. Of course if $f(x)$ has degree 1 or 2, then $|f(n)| \ll N^2$ for all $n \le N$, so that $f(n)$ cannot be divisible by the square of a prime $\gg N$.

The number of integers $n \le N$ for which $f(n)$ is divisible by the square of some prime in the range $y < p < cN$ is, using Lemma 2.1,

$$\le \sum_{y<p<cN} B_f\Big(\frac{N}{p^2} + 1\Big) \ll \frac{N}{y} + \frac{N}{\log N}.$$

Finally we must consider those n for which $f(n)$ is divisible by the square of some integer $m > y$, all of whose prime factors are $\le y$. For each n we select the smallest such m and we claim that this is $\le y^2$: for if not select any prime factor p of m so that $p \le y$ and let $M := m/p$ which is $> y^2/y = y$ and such that M^2 divides m^2 which

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

divides $f(n)$, contradicting the minimality of m. Thus using Corollary 2.2, and since $\omega(m) \ll \log m/\log\log m$ so that $B_f^{\omega(m)} = m^{o(1)}$, we have that the number of such n is

$$\leq \sum_{y<m\leq y^2} B_f^{\omega(m)}\Big(\frac{N}{m^2}+1\Big) \ll y^{o(1)}(N/y+y^2) \ll N/y^{1-o(1)}.$$

The result (4.1) follows from combining the last three paragraphs, so long as y was chosen sufficiently large.

5 Proof of Theorems 1B and 1C

We want to determine the number of distinct squarefree integers d for which there exists some integer $n \leq N$ such that $f(n) = dm^2$ for some integer m. Evidently there are no more than N such values of d. To get a lower bound we remove all cases where $m > y$ (where y is as defined in section 4), as well as all those d for which there is more than one such pair m, n with $m \leq y$ and $n \leq N$. In other words, using (4.1), our quantity is

$$\geq (1-\epsilon)N - \sum_{m_1,m_2\leq y} \#\{n_1 \neq n_2 \leq N : f(n_1)/m_1^2 = f(n_2)/m_2^2 \text{ is squarefree}\}.$$

Note that if $m_1 = m_2$ then we are asking for solutions to $f(n_1) = f(n_2)$ with $n_1 \neq n_2$. However for any non-constant polynomial, $|f(n)|$ is monotone increasing for n sufficiently large, so there are at most finitely many such pairs n_1, n_2. Otherwise, assuming without loss of generality that $m_1 > m_2$, each pair (n_1, n_2) gives rise to an integer point on the curve

$$f(x) - cf(z) = 0$$

with $c = (m_1/m_2)^2 > 1$. By Theorem 2 there are $\ll_{c,f} 1$ such points when $\deg(f) \geq 3$. Therefore for fixed but large y,

$$\sum_{m_1,m_2\leq y} \#\{n_1 \neq n_2 \leq N : f(n_1)/m_1^2 = f(n_2)/m_2^2 \text{ is squarefree}\} \ll 1,$$

which completes the proof of Theorem 1C for $\deg(f) \geq 3$.

When $\deg(f) = 2$ we can get more uniform bounds. In that case if $f(x) = ax^2 + bx + c$, we can complete the square to get $4af(x) = X^2 + \Delta$, where $X = 2ax + b$ and $\Delta = -(b^2 - 4ac)$. Then, if we fix positive integers $m_1, m_2 \leq y$, take an integral solution (n_1, n_2) to $f(n_1)/m_1^2 = f(n_2)/m_2^2$, and let $r_j = 2an_j + b$, we obtain an integral solution (r_1, r_2) to

$$(m_2r_1 - m_1r_2)(m_2r_1 + m_1r_2) = \Delta(m_1^2 - m_2^2).$$

This has $\tau\big(\Delta(m_1^2 - m_2^2)\big) = y^{o(1)}$ solutions, where $\tau(.)$ is the number of divisors of an integer. Theorem 1B then follows from the proof in Section 4 with $y = \log^2 N$.

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

6 Linear Polynomials

Proof of Theorem 1A We wish to find the number of squarefree integers d for which there exists an integer m such that $dm^2 = an + b$ for some $n \le N$. For those $d \equiv q \pmod a$, we select m to be the smallest positive integer for which $qm^2 \equiv b \pmod a$ if such an m exists. Thus we need to determine

$$\sum_{m \in M_a} \#\{\text{squarefree } d \le (aN+b)/m^2 : d \equiv b/m^2 \pmod a\}.$$

By elementary sieve theory we have that the number of squarefree integers $d \equiv q \pmod a$, when $(a,q) = 1$, is, writing $d = ar + q$,

$$\begin{aligned}\sum_{r \le x} \sum_{g^2 \mid ar+q} \mu(g) &= \sum_{g \le \sqrt{ax+q}} \mu(g) \#\{r \le x : g^2 \mid ar+q\} \\ &= \sum_{g \le \sqrt{ax+q}, (g,a)=1} \mu(g)\big(x/g^2 + O(1)\big) \\ &= x \prod_{p \nmid a} \Big(1 - \frac{1}{p^2}\Big) + O(\sqrt{ax}).\end{aligned}$$

Summing up over $m \in M_a$ gives the result.

Proof of Theorem 3B If $f(x)$ is a linear polynomial, say $ax + b$ with $(a,b) = 1$, then we are interested in the proportion of squarefree integers $d \le D$ for which there exists some integer m such that $dm^2 \equiv b \pmod a$. In other words d belongs to one of a certain set of congruence classes mod a; the number of such congruence classes being $\phi(a)/2^{w(a)}$ where $w(a)$ denotes the number of distinct odd prime factors of a, plus 2 if 8 divides a, or plus 1 if 4 divides a but not 8. By the estimate in the proof of Theorem 1A each of these arithmetic progressions contains $(D/a)\prod_{p \nmid a}(1 - 1/p^2) + O(\sqrt{D})$ such integers $d \le D$, and so we obtain the result.

7 Heuristic

The argument preceding Lemma 1 in the introduction tells us that if $f(n) = dm^2$ with $d \le D$ then $|n| \ll D^{1/(\deg(f)-2)+o(1)}$, assuming the *abc*-conjecture. If $|n| \ll D^{1/\deg(f)}$ then $|f(n)| \asymp |n|^{\deg(f)} \le D$, so that $d \le D$. Therefore we need to explore further for $D^{1/\deg(f)} \ll |n| \le D^{1/(\deg(f)-2)+o(1)}$. For $N = cD^{1/\deg(f)}2^j$ with $j = 0, 1, 2, \dots, J$ we consider $N < |n| < 2N$, so that $|f(n)| \asymp N^{\deg(f)}$. Then $m^2 = |f(n)|/d \gg N^{\deg(f)}/D$, and obviously $m^2 \ll N^{\deg(f)}$. Now there are $\le B_f^{\omega(m)}$ values of $n \pmod{m^2}$, for which $f(n) \equiv 0 \pmod{m^2}$ by Corollary 2.2. Therefore the number of such $N < |n| < 2N$ is $\le B_f^{\omega(m)}(2N/m^2 + 1)$. For the heuristic assume the term "1" is irrelevant at least on average, and recall that $B_f^{\omega(m)} \ll N^{o(1)}$. Therefore $\#\{n \le N : m^2 \mid f(n) \text{ for some } m \in M\} \ll \sum_{m \in M} N^{1+o(1)}/m^2 \ll \sqrt{D}/N^{\deg(f)/2-1-o(1)}$, where

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press

M is the interval $N^{\deg(f)/2}/D^{1/2} \ll m \ll N^{\deg(f)/2}$. Summing over all such N we get $\ll D^{1/\deg(f)+o(1)}$, for $\deg(f) \geq 3$, as required.

Added in proof: In March 2002, we received a preprint by Bjorn Poonen, "Squarefree values of multivariable polynomials", in which he proves our Theorems 1A, 1B, 1C; his proofs are slightly different from the ones in this paper.

References

[1] E. Bombieri, *Effective Diophantine Approximation on* $\mathbb{G}_m$. Ann. Scuola Norm. Pisa Cl. Sci (4) **20**(1993), 61–89.
[2] N. Elkies, *ABC implies Mordell.* Internat. Math. Res. Notices **7**(1991), 99–109.
[3] A. Granville, *ABC means we can count squarefrees.* Internat. Math. Res. Notices **19**(1998), 991–1009.
[4] H. Halberstam and H.-E. Richert, *Sieve Methods.* Academic Press, London-New York-San Francisco, 1974.
[5] C. Hooley, *On the power free values of polynomials.* Mathematika **14**(1967), 21–26.
[6] C. L. Siegel, *Über einege Anwendungen diophantischer Approximaten.* Abh. Preuss. Akad. Wiss. Phys. Math. Kl. **1**(1929), 209–266.

Department of Mathematics
University of Georgia
Athens, Georgia 30602
USA
email: pcutter@kzoo.edu
andrew@math.uga.edu
ttucker@math.uga.edu

https://doi.org/10.4153/CMB-2003-007-0 Published online by Cambridge University Press