Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 1054–1058, February 1997
Mathematics

Using a parity-sensitive sieve to count prime values of a polynomial

JOHN FRIEDLANDER*† AND HENRYK IWANIEC‡

*Scarborough College, University of Toronto, Scarborough, ON, M1C 1A4, Canada; and ‡Department of Mathematics, Rutgers University, New Brunswick, NJ 08903

Communicated by Charles L. Fefferman, Princeton University, Princeton, NJ, November 25, 1996 (received for review November 11, 1996)

ABSTRACT **It is expected that any irreducible polynomial with integer coefficients assumes infinitely many prime values provided that it satisfies some obvious local conditions. Moreover, it is expected that the frequency of these primes obeys a simple asymptotic law. This has however been proven for only a few special classes of polynomials. In the most famous unsolved cases the sequence of values is "thin" in the sense that it contains fewer than N^{θ} integers up to N for some constant $\theta < 1$. Quite generally it seems to be difficult to show the infinitude of primes in a given thin integer sequence and there is no polynomial for which this has hitherto been done. The polynomial $x^2 + y^4$ is an example of such a thin sequence; here, specifically, $\theta = 3/4$. We report here the development of new methods that rigorously demonstrate the asymptotic formula in the case of this polynomial and that are applicable to an infinite class of polynomials to which this one belongs. The proof is based partly on a new sieve method that breaks the well-known parity problem of sieve theory and partly on a careful harmonic analysis of the special properties of biquadratic polynomial sequences.**

The prime numbers that can be written in the form $a^2 + b^2$ were characterized more than 300 years ago by Fermat. It is quite easy to see that no prime of the form $4m + 3$ can be a sum of two squares, and Fermat proved the much more difficult result that every prime of the form $4m + 1$ can be so written. In the eighteenth and nineteenth centuries, mainly due to the efforts of Lagrange and Gauss, this result was found to be a special case of a more general phenomenon: Given any irreducible binary quadratic form $\varphi(a, b) = \alpha a^2 + \beta ab + \gamma b^2$, the primes represented by φ are characterized by congruence and class group conditions. This fact made it possible, following the nineteenth century breakthroughs on prime counting by Dirichlet, Hadamard, and Vallée-Poussin, to give asymptotic formulae for the number of primes up to x, which are represented by such a form. Apart from a minority of φ that fail to satisfy some local condition and hence cannot represent more than one prime, one finds that a positive density of all primes are represented by such a form.

For more general polynomials one cannot expect such a simple characterization; nevertheless, one may quite generally formulate expected asymptotic formulae for the frequency of primes represented. Success in proving these has however been limited; even proving the representability of infinitely many primes seems no easier. In the case of two variables the result is known for general quadratic polynomials, as given by Iwaniec (1). For polynomials in one variable the problem is harder still and only the case of linear polynomials, that is arithmetic progressions, is settled thanks to Dirichlet.

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "*advertisement*" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

0027-8424/97/941054-5$2.00/0
PNAS is available online at **http://www.pnas.org**.

Here we describe new methods that prove that there are infinitely many primes of the form $a^2 + b^4$ and give the asymptotic formula, the first such results for any thin polynomial sequence.

THEOREM 1. *We have, with* Λ *the von Mangoldt function,*

$$\sum_{\substack{a>0\ b>0\\ a^2+b^4\le x}}\sum \Lambda(a^2 + b^4) = 4\pi^{-1}\kappa x^{3/4}\left\{1 + O\left(\frac{\log\log x}{\log x}\right)\right\},$$

where $\kappa = \int_0^1(1 - t^4)^{1/2}dt$.

We remark that by comparing this with the well-known asymptotic formula for the case of $a^2 + b^2$ (change $x^{3/4}$ to x and t^4 to t^2), we see that the "probability" of an integer $a^2 + b^2$ being prime is the same when we are told that b is a square as it is when we are told that b is not a square.

The proof of *Theorem 1* is based on a sieve method. In its classical format the sieve is unable to detect primes for a very basic reason known as the parity problem. In the case where the sequence is close to positive density and has extremely good regularity properties the sieve very barely fails, whereas in the case of a thin sequence like the one we consider the failure is by a wider margin. The former case was analyzed very precisely by the asymptotic sieve of Bombieri (2). By adding an additional axiom to those already present, we are able to modify Bombieri's sieve to the point that we can produce asymptotic formulae for primes even in thin sequences.

Having this sieve at hand, there remains the still more difficult problem of proving that the sequence of integers $a^2 + b^4$ satisfies the additional axiom. This occupies the greater part of the work and incidentally gives rise to a number of results of independent interest.

The Sieve

Given a general sequence $\mathcal{A} = (a_n)$ of nonnegative reals, we should like to evaluate asymptotically the sum

$$S(x) = \sum_{n\le x} a_n\Lambda(n). \qquad [1]$$

In the case of our application we have a_n being the number of representations of $n = a^2 + b^4$. Thus, we want to allow the sequence $\mathcal{A}$ to be quite thin. Setting

$$A(x) = \sum_{n\le x} a_n \qquad [2]$$

we make the very mild assumption

$$A(x) \ll A(\sqrt{x})(\log x)^2. \qquad [3]$$

Inserting in Eq. **1** the formula $\Lambda(n) = \sum_{d|n}\lambda_d$ we obtain, after an interchange of order,

†To whom reprint requests should be addressed.

$$S(x) = \sum_{d \le x} \lambda_d A_d(x), \qquad [4]$$

where $\lambda_d = -\mu(d)\log d$. This reduces the problem to a sufficiently precise evaluation of the sums

$$A_d(x) = \sum_{\substack{n \le x \\ n \equiv 0 \pmod d}} a_n. \qquad [5]$$

We assume that, for some nice function g, $A_d(x)$ is closely approximated by $g(d)A(x)$, say

$$A_d(x) = g(d)A(x) + r_d(x), \qquad [6]$$

where $r_d(x)$ is small. This last vague statement must be made more precise in several respects. There are a number of standard ways to do this and we do not attempt to choose a minimal set of axioms. We assume that, uniformly in $d \le x^{1/3}$ we have

$$A_d(x) \ll g(d)A(x). \qquad [7]$$

The function g is assumed to have a number of properties [think of $g(d) = d^{-1}$ as the prototypical example]. We assume g is multiplicative with $0 \le g(p) < 1$ for all primes p, that

$$g(d) \ll d^{-1}\tau(d)^B, \qquad [8]$$

for some constant B, where τ is the divisor function, that for $y \ge 2$,

$$\sum_{d \le y} \mu^2(d)g(d) = c_1 \log y + c_0 + O((\log y)^{-8}) \qquad [9]$$

for some constants $c_1 > 0$ and c_0, and finally that, for $y \ge 2$,

$$\sum_{d \le y} \mu(d)g(d) \ll (\log y)^{-8}. \qquad [10]$$

All of the above axioms are easy to verify for a great many sequences A to which the sieve has been applied and, in particular, to the sequence we consider here. In our case one has $g(p) = \frac{1}{p} + (\chi(p)/p)(1 - \frac{1}{p})$, where χ is the Dirichlet character of conductor 4.

About the remainder terms r_d we assume

$$\sum_{d \le D} \mu^2(d)|r_d(t)| \le A(x)(\log x)^{-1996} \qquad [\mathbf{R}]$$

for all $t \le x$, with some $D = D(x)$ such that $x^{2/3} < D(x) < x$. This assumption, or something very much like it, is the final and pivotal assumption of classical sieve theory. In contrast to the earlier assumptions, this one is much more important and usually more difficult to verify. In the case of our application the assumption **[R]** was recently proven by Fouvry and Iwaniec (3) with $D = x^{3/4-\varepsilon}$, for every $\varepsilon > 0$. It was this surprising and best-possible result that gave us the courage to attempt this project.

The additional assumption that gives the asymptotic for primes is an estimate for bilinear forms. We assume

$$\sum_m \left| \sum_{\substack{N < n \le 2N \\ mn \le x}} \gamma(n)\mu(mn)a_{mn} \right| \le A(x)(\log x)^{-1996} \qquad [\mathbf{B}]$$

for every N with

$$\Delta^{-1}\sqrt{D} < N < \delta^{-1}\sqrt{x},$$

for some $\delta = \delta(x) \ge 2$ and $\Delta = \Delta(x) \ge 2$, and where

$$\gamma(n) = \gamma(n, C) = \sum_{d|n, d \le C} \mu(d).$$

This is required for every C with $1 \le C \le xD^{-1}$.

THEOREM 2. *If the* a_n *are supported on squarefree integers, then under the above assumptions*

$$\sum_{p \le x} a_p \log p = HA(x)\left\{1 + O\left(\frac{\log \delta(x)}{\log \Delta(x)}\right)\right\},$$

where $H = \Pi_p(1 - g(p))(1 - \frac{1}{p})^{-1}$ *and the implied constant depends only on the function g.*

We remark that by modifying slightly the assumptions we can remove the requirement that a_n be supported on squarefree integers.

For the proof of Theorem 2 we decompose the function Λ by means of a combinatorial identity. Such identities have been used before by many people including Vinogradov, Linnik, Vaughan, and Heath-Brown. In our case, we choose a parameter z and can write, for $n > z$, $\Lambda(n)$ essentially as a sum of several sub-sums, the most difficult and important of which are of the type $\Sigma_{de|n}\mu(d)\Lambda(e)$, where d and e are either both small or both large. Inserting this into the formula (Eq. **1**), we get a decomposition of that sum. It is not hard to see that the pieces where d and e are small can be handled by **[R]**, roughly when their product is less than D, and that these give the main term in *Theorem 2*. If one assumed **[R]** held to a sufficiently high level D this would take care of matters since the remaining case of d, e both large would not happen often, or at all, since $de \mid n$ and $n \le x$. This would however require an unrealistically strong assumption and the resulting theorem would be without application. Any more realistic assumption about D necessitates a more careful treatment and even then still leaves uncovered the contributions where one of d, e come from a mid-sized range. These however can be estimated by the bilinear form occurring in the assumption **[B]**. The presence of δ and Δ in this assumption is necessary to avoid making it unreasonably strict.

There are a number of technical details we have not yet mentioned. The most essential is the following: In dealing with the contribution where d, e are both large it is difficult to keep control of a certain cancellation coming from the Möbius function and this necessitates attaching sieve weights ϱ_n to a_n right from the beginning. This device was used by Bombieri (2) serve the analogous function of allowing one to assume **[R]** only up to a realistic level.

The Bilinear Form

The various assumptions of the previous section, other than **[R]** and **[B]**, are easily verified for our sequence and **[R]** was demonstrated with $D = x^{3/4-\varepsilon}$ in ref. 3. Our remaining task is to prove that **[B]** holds for all N with

$$x^{1/4+\varepsilon} < N < x^{1/2}(\log x)^{-A}.$$

This is actually stronger than needed for *Theorem 1*. It would suffice in this lower bound to cover the range $N > x^\alpha$ for some $\alpha < 3/8$.

The double sum occurring in **[B]** is easily transformed into sums of the form

$$\sum\sum_{(m,n)=1} \alpha_m \beta_n a_{mn},$$

where $\beta_n = \gamma_n \mu(n)$, α_m replaces the absolute value, and where it is convenient for technical reasons to break up the ranges for m, n into subintervals and restrict to integers free from small prime factors. To attack the above double sum we have little choice but to rid ourselves of the set of coefficients α_m by

Cauchy's inequality but to do so at once would be too costly. It is more natural and also more efficient to first write this in terms of Gaussian integers obtaining by the unique factorization in that ring

$$a_{mn} = \tfrac{1}{4} \sum_{|w|^2=m} \sum_{|z|^2=n} \mathfrak{q}(\mathrm{Re}\ \bar{w}z),$$

where w, z run through $\mathbb{Z}[i]$, the factor $1/4$ takes account of the units and $\mathfrak{q}$ is the characteristic function of the squares. Now applying Cauchy's inequality, introducing a smooth majorant $f(w)$, and squaring out, we are led to the problem of bounding the sum

$$\sum_{(z_1,z_2)=1} \sum \beta_{z_1}\bar{\beta}_{z_2}\mathscr{C}(z_1, z_2) \qquad \textbf{[11]}$$

with

$$\mathscr{C}(z_1, z_2) = \sum_w f(w)\mathfrak{q}(\mathrm{Re}\ \bar{w}z_1)\mathfrak{q}(\mathrm{Re}\ \bar{w}z_2),$$

where $\beta_z = \beta_{|z|^2}$ and the condition $(z_1, z_2) = 1$ can be introduced with acceptable error because β lives on integers without small prime factors. We may also, by a splitting argument, restrict z_1, z_2 to a small (polar coordinate) box.

The Error Term

We give in this section a type of Fourier expansion for the sum of Eq. **11** and then bound all but one term in this expansion. The remaining "main" term is arithmetic in nature and does reduce in size due to the oscillation of sign in the sequence β. The treatment of this main term, which is much more difficult, we defer to future sections.

The problem of obtaining an asymptotic formula for $\mathscr{C}(z_1, z_2)$ reduces to the counting of lattice points inside the "biquadratic ellipse"

$$t_1^4 - 2\gamma t_1^2 t_2^2 + t_2^4 = x$$

for fixed γ, $0 < \gamma < 1$. We put

$$\Delta = \Delta(z_1, z_2) = \mathrm{Im}\bar{z}_1 z_2,$$

and $\mathrm{Re}\ \bar{w}z_1 = b_1^2$, $\mathrm{Re}\ \bar{w}z_2 = b_2^2$. These determine w by the equation $i\Delta w = b_1^2 z_2 - b_2^2 z_1$. As w ranges over $\mathbb{Z}[i]$, this equation is equivalent to a congruence modulo $|\Delta|$ and we have

$$\mathscr{C}(z_1, z_2) = \sum_{b_1^2 z_2 \equiv b_2^2 z_1 \pmod{|\Delta|}} \sum f((b_1^2 z_2 - b_2^2 z_1)/\Delta). \qquad \textbf{[12]}$$

Since $|\Delta|$ may be very large there are few lattice points relative to the volume and the problem may be expected to be difficult.

An application of the Poisson summation formula transforms Eq. **12** into

$$|z_1 z_2|^{-1/2} \sum_{h_1} \sum_{h_2} G(h_1, h_2) F(h_1|\Delta z_2|^{-1/2}, h_2|\Delta z_1|^{-1/2}),$$

where $G(h_1, h_2)$ is the sum

$$|\Delta|^{-1} \sum_{\alpha_1^2 z_2 \equiv \alpha_2^2 z_1 (\mathrm{mod}|\Delta|)} \sum e((\alpha_1 h_1 + \alpha_2 h_2)|\Delta|^{-1}) \qquad \textbf{[13]}$$

and $F(u_1, u_2)$ is the integral

$$\int\int f\left(\frac{z_2}{|z_2|}t_1^2 - \frac{z_1}{|z_1|}t_2^2\right) e(u_1 t_1 + u_2 t_2) dt_1\, dt_2. \qquad \textbf{[14]}$$

The main term comes from $h_1 = h_2 = 0$. The integral F turns out not to be a difficult problem. In the case of $F(0, 0)$ it may be explicitly evaluated and for the other (error) terms it suffices to input a bound that is derived by repeated partial integration, together with a crude bound for G in terms of the divisor function $\tau(\Delta)$; however, the fact that the divisor function is occasionally fairly large forces us to bound this error only on average over z_1, z_2. Thus, we don't quite solve the lattice point problem, but solving it in this average sense suffices for our main concern. The final result is that the sum of Eq. **11** is, apart from an admissible error, given by the main term

$$\frac{2\hat{f}(0)}{|\Delta_0|\sqrt{N}} \log\left(\frac{2N}{|\Delta_0|}\right) T(\beta),$$

where

$$T(\beta) = \sum_{(z_1,z_2)=1} \sum \beta_{z_1}\bar{\beta}_{z_2} G(0,0).$$

Here we have used the fact that with z_1, z_2 confined inside a small box we can treat Δ as though it may be replaced by a constant Δ_0.

Reduction of the Main Term

Our next task is to simplify and transform the sum $T(\beta)$ in the main term. This requires us to penetrate the arithmetic nature of the sum $G(0, 0)$ from Eq. **13**. The latter is closely related to $\varrho(z_2/z_1; \Delta)$, where $\varrho(z; \Delta)$ counts the number of solutions in rational residue classes of $\omega^2 \equiv z (\mathrm{mod}\ |\Delta|)$ (actually we need to also consider ϱ to moduli dividing Δ to take care of a technical problem involving coprimality). The number ϱ is, as is well known, expressible as a sum of the Jacobi symbol over the divisors d of Δ. Following Dirichlet we separate these divisors into two sets $d < \sqrt{|\Delta|}$ and $d \geq \sqrt{|\Delta|}$, and transform the latter into their complementary divisors $d \to |\Delta|/d$. The first set gives rise to sums of the shape

$$\sum_{(z_1,z_2)=1} \sum \beta_{z_1}\bar{\beta}_{z_2} \sum_{\substack{d|\Delta \\ d < \sqrt{|\Delta|}}} \left(\frac{r_1 r_2}{d}\right),$$

whereas, after some manipulation, the latter give sums

$$\sum_{(z_1,z_2)=1} \sum \beta_{z_1}\bar{\beta}_{z_2}\left(\frac{s_1}{r_1}\right)\left(\frac{s_2}{r_2}\right) \sum_{\substack{d|\Delta \\ d \leq \sqrt{|\Delta|}}} \left(\frac{r_1 r_2}{d}\right).$$

Here, for $j = 1, 2$, we write $z_j = r_j + is_j$, r odd, s even, and in case of even integers d, the 2 part is ignored in the Jacobi symbol. In reducing to these sums (and later in estimating them) all of the basic properties of the Jacobi symbol, multiplicativity, periodicity, and quadratic reciprocity, are used in an essential fashion.

We split into segments $D < d \leq 2D$, detect the condition $d\,|\Delta$ by additive characters, interchange the order of summation, and apply Cauchy's inequality. This leads to the problem of giving nontrivial bounds for various D for the sum

$$S_I = \sum_{D<d\leq 2D} \sum_{a\ (\mathrm{mod}\ d)} \left| \sum_{\bar{r}s \equiv a\ (\mathrm{mod}\ d)} \sum \beta_z \left(\frac{r}{d}\right)\right|^2 \qquad \textbf{[15]}$$

and also for the sum

$$S_{II} = \sum_{D<d\leq 2D} \sum_{a\ (\mathrm{mod}\ d)} \left| \sum_{\bar{r}s \equiv a\ (\mathrm{mod}\ d)} \sum \beta_z \left(\frac{s}{r}\right)\left(\frac{r}{d}\right)\right|^2, \qquad \textbf{[16]}$$

where $z = r + is$ with s even, r odd, $R < r \leq 2R$, $S < s \leq 2S$.

Twisted Sums Over Arithmetic Progressions

In case the range D for the modulus is neither too small nor too large we are able to obtain results where the coefficients β are replaced by arbitrary complex numbers α_{rs}. This means in particular that, for such D, the sums S_I, S_{II} may be treated simultaneously, since the Jacobi symbol (s/r) may be incorporated into β_z and here we name the resulting sum $S(D)$.

In the event that the α_{rs} factorized and the symbol (r/d) were absent this would be a result of Barban type and would follow from the large sieve. Now however new ideas are required.

We proceed in three steps. In the first place, using duality, Poisson summation, and a number of elementary but nontrivial arguments one obtains a bound which covers the range $(\log RS)^A < D < (RS)^{1/2-\varepsilon}$. At the second stage one replaces, in the sum $S(D)$, the congruence $r_1s_2 \equiv s_1r_2 (\mathrm{mod}\ d)$ by the equation $r_1s_2 - r_2s_1 = dm$ and then makes the change of variable $d \to m$. If the modulus d of the old congruence is in the range $(RS)^{1/2+\varepsilon} < d < RS(\log RS)^{-A}$, then the new modulus m is in the range treated in the first step. This idea was first used in the context of Barban–Davenport–Halberstam Theorems by Hooley but of course appears already in Dirichlet's work on the divisor problem.

The first two steps leave uncovered a middle range $(RS)^{1/2-\varepsilon} < D < (RS)^{1/2+\varepsilon}$. Because $(r/dp^2) = (r/d)$ for all primes p not dividing r, it turns out to be possible for any $P \geq 2$ to bound $S(D)$ in terms of $S(DP^2)$ by averaging over the primes in the dyadic interval $P < p \leq 2P$. Now, if D is in the middle range, we may, by choosing P appropriately, place DP^2 in the range of larger moduli covered by the result of step two.

Combining these results we obtain for each of S_I and S_{II} a bound, which, as opposed to the trivial bound, saves an amount $(\log RS)^A$, A arbitrary, throughout the whole range

$$(\log RS)^{B(A)} < D < RS(\log RS)^{-B(A)},$$

and saves quite a bit more when D is not too close to the boundary of this region. Of course, because of the Dirichlet involution and the fact that we treat general coefficients, we do not really need to cover the range $D > (RS)^{1/2+\varepsilon}$. This would not however allow us to skip any of the three steps in the argument.

Siegel–Walfisz

We still need to treat the small moduli where $D < (\log RS)^B$, B arbitrary. Now the two cases S_I, S_{II} need very different treatments and in both cases the special shape of the coefficient β is heavily used. In the case of S_I the cancellation comes from the sign changes of the Möbius function, which is embedded into β and we are able to succeed, even for each individual d, by giving a Siegel–Walfisz Theorem in the Gaussian domain. The fundamentals of such a result are due to Hecke and to Siegel, although we need to do some work to get the result in a form that is applicable to the problem at hand. Grossencharacters enter naturally at this point and as a result of taking them into account our final results on primes $a^2 + b^4$ demonstrate also their uniform distribution in sectors in the Gaussian plane.

Jacobi–Twisted Sums

Our final chore, and rather an interesting one, is the treatment of the small moduli $D < (\log RS)^B$ in the case of sums S_{II}. Recall that these were originally the large moduli before application of the Dirichlet involution. As in the previous case, the special shape of the coefficients is crucial, although now our cancellation will come not from the Möbius function but instead from the oscillation in sign coming from the Jacobi symbol.

We say the Gaussian integer $z = r + is$ is primary if s is even and r is congruent to $s + 1$ modulo four. The product $z = z_1z_2$ of primary numbers is primary. The symbol $[z]$ defined by $[z] = i^{(r-1)/2}(s/|r|)$ for primary z enjoys the multiplicativity property

$$[z_1z_2] = \varepsilon[z_1][z_2]\left(\frac{\mathrm{Re}\, z_1z_2}{|z_2|^2}\right), \qquad \textbf{[17]}$$

where $\varepsilon = \pm 1$ depends only on the quadrants in which z_1, z_2, and z_1z_2 are located. This follows from some manipulations, which again make use of all of the basic properties of the Jacobi symbol, and in particular the law of quadratic reciprocity.

In dealing with the sum S_{II} for small moduli we shall, as in the case of S_I, be able to treat individual d. Thus, referring to the definition of Eq. **16** and incorporating the factor (r/d) into the β, we are left to estimate sums $\sum_z \beta_z[z]$. Because of its resemblance to the Möbius function we are able to decompose β in much the same fashion as we did with Λ in the treatment of the sieve. This reduces the problem to bounding linear forms $\sum_z [wz]$ and bilinear forms $\sum\sum_{wz} \alpha_w\gamma_z[wz]$, where in both cases the variables are constrained by their product being required to belong to a given box. The multiplicativity property of Eq. **17** is basic for the study of such sums. There are a number of alternative treatments. In the case of the linear forms we are able to neglect the summation in all but one variable and reduce the problem to the estimation of the sum of the Jacobi symbol over an interval to which we apply the Polya–Vinogradov inequality. The estimate of Burgess could be used here to improve the result, but this is not necessary for the final goal. For the bilinear forms it is also possible to reduce the problem to a similar one variable sum and here it would suffice to apply the Burgess bound. There is however another method that is more elementary yet, because it takes advantage of a second variable, also gives stronger results.

Combining these bounds we complete the proof of the final step to the main theorem. Because the function Λ can also be decomposed in essentially the same fashion as β (in fact, more simply), we get the following by-product of the work in this section. Define $\lambda(n) = \sum\sum_{r^2+s^2=n} (s/r)$, where r is odd and positive and s is even. Then for some absolute constant $\eta > 0$, for example $\eta = 1/77$, we have

$$\sum_{p \leq x} \lambda(p) \ll x^{1-\eta}. \qquad \textbf{[18]}$$

Discussion

As indicated earlier the methods yield incidentally the uniform distribution of the Gaussian primes $a + ib^2$ in sectors and for that matter within any region having a reasonable boundary. One also obtains the expected distribution on restricting the variables a and b to residue classes having moduli either fixed or growing less quickly than some power of $\log x$.

It seems certain that the methods extend to cover the case of the prime values of $\varphi(a, b^2)$ for any binary quadratic form φ. We have not checked this in detail. One should certainly expect some complications regarding composition of forms in case of nontrivial class group.

A more interesting extension would be the proof of the asymptotic formula, or even a lower bound of the expected order for primes of the form $a^2 + b^6$. The arguments herein carry over to a considerable extent, provided that quadratic reciprocity is replaced by cubic reciprocity. One has, thanks again to the work of Fouvry and Iwaniec (3), the level $D(x) = x^{2/3-\varepsilon}$ in **[R]**. Although also best-possible, this is smaller than before. Thus, one faces more effort in the combinatorics to

avoid the restriction $D > x^{2/3}$ in the sieve part and, of greater significance, one has to settle for lesser results in bounding the sums occurring in the bilinear form **[B]**.

In the event that one can produce primes $a^2 + b^6$ then this would have an interesting application to elliptic curves, since it is morally certain that trivial modifications would allow treatment of the polynomial $27a^2 + b^6$, which is the negative of the discriminant of the elliptic curve $y^2 = 4x^3 + b^2x + a$. One would thus deduce the existence of infinitely many elliptic curves over $\mathbb{Q}$ having prime discriminant. Here we would not get the expected magnitude for the number of such curves since we are not able to directly touch the polynomial $x^2 + y^3$. After all, three is not an even number!

Although the proofs of our results are rather lengthy and complicated we are able to avoid much of the high-powered technology frequently used in modern analytic number theory such as the bounds of Weil and Deligne. We also do not appeal to the theory of automorphic functions although experts will, in several places, detect it bubbling just beneath the surface.

J.F. is supported in part by Natural Sciences and Engineering Research Council (Canada) Grant A5123. H.I. is supported in part by National Science Foundation Grant DMS-9500797.

1. Iwaniec, H. (1973) *Acta Arith.* **24,** 435–459.
2. Bombieri, E. (1976) *Mem. Acad. Naz. Dei XL* **1/2,** 243–269.
3. Fouvry, E. & Iwaniec, H. (1997) *Acta Arith.*, in press.
4. Hecke, E. (1920) *Math. Z.* **6,** 11–51.