MATHEMATICS OF COMPUTATION
Volume 72, Number 241, Pages 499–519
S 0025-5718(02)01418-7
Article electronically published on May 2, 2002

NEW QUADRATIC POLYNOMIALS WITH HIGH DENSITIES OF PRIME VALUES

MICHAEL J. JACOBSON, JR. AND HUGH C. WILLIAMS

ABSTRACT. Hardy and Littlewood's Conjecture F implies that the asymptotic density of prime values of the polynomials $f_A(x) = x^2 + x + A$, $A \in \mathbb{Z}$, is related to the discriminant $\Delta = 1 - 4A$ of $f_A(x)$ via a quantity $C(\Delta)$. The larger $C(\Delta)$ is, the higher the asymptotic density of prime values for any quadratic polynomial of discriminant Δ. A technique of Bach allows one to estimate $C(\Delta)$ accurately for any $\Delta < 0$, given the class number of the imaginary quadratic order with discriminant Δ, and for any $\Delta > 0$ given the class number and regulator of the real quadratic order with discriminant Δ. The Manitoba Scalable Sieve Unit (MSSU) has shown us how to rapidly generate many discriminants Δ for which $C(\Delta)$ is potentially large, and new methods for evaluating class numbers and regulators of quadratic orders allow us to compute accurate estimates of $C(\Delta)$ efficiently, even for values of Δ with as many as 70 decimal digits. Using these methods, we were able to find a number of discriminants for which, under the assumption of the Extended Riemann Hypothesis, $C(\Delta)$ is larger than any previously known examples.

1. INTRODUCTION

Consider the polynomial $f(x) = ax^2 + bx + c$. If $p \mid f(X)$ for some $X \in \mathbb{Z}$, then $\Delta = b^2 - 4ac$, the discriminant of $f(x)$, must be a square modulo p. Thus, if Δ is not a square modulo many primes p, we expect $f(x)$ to take on many prime values asymptotically. Hardy and Littlewood formalized this phenomenon as Conjecture F in [10]. If $\pi_f(n)$ denotes the number of prime values assumed by $f(X)$ for $X = 0, 1, \ldots, n$, then their conjecture can be given as follows:

Conjecture (F). Let $a > 0, b, c$ be integers such that $\gcd(a, b, c) = 1$, $\Delta = b^2 - 4ac$ is not a square and $a+b$, c are not both even. Then there are infinitely many primes of the form $f(x)$, and

$$\pi_f(n) \sim \varepsilon C_f Li(n),$$

where

$$Li(n) = \int_2^n \frac{dx}{\log x},$$

$$\varepsilon = \begin{cases} \frac{1}{2} & \text{when } 2 \nmid a + b, \\ 1 & \text{otherwise,} \end{cases}$$

Received by the editor September 8, 1999 and, in revised form, February 28, 2001.
2000 *Mathematics Subject Classification.* Primary 11R11, 11R29, 11Y40; Secondary 11Y16.
Key words and phrases. Prime-generating quadratic polynomial, quadratic order, class group.

and

$$C_f = \prod_{\substack{p>2 \\ p \mid (a,b)}} \frac{p}{p-1} \prod_{\substack{p>2 \\ p \nmid a}} \left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p-1}\right).$$

The products in the expression for C_f are taken over the primes only, and $\left(\frac{\Delta}{p}\right)$ denotes the Legendre symbol. Note here that εC_f is what really determines the density of prime values assumed by f, since $Li(n)$ is a function of n only. The larger εC_f is, the higher the asymptotic density of prime values for any quadratic polynomial of discriminant Δ.

We restrict ourselves to polynomials of the form $f_A(x) = x^2 + x + A$. If we denote by $P_A(n)$ the number of prime values assumed by $f_A(x)$ for $0 \leq x \leq n$, then for these polynomials we have the following simplified form of Conjecture F:

$$P_A(n) \sim C(\Delta) L_A(n),$$

where

$$L_A(n) = 2 \int_0^n \frac{dx}{\log f_A(x)}$$

and

$$C(\Delta) = \prod_{p \geq 3} 1 - \frac{\left(\frac{\Delta}{p}\right)}{p-1}. \tag{1.1}$$

Here $\Delta = 1 - 4A$.

The most famous example of such a polynomial is certainly Euler's polynomial $f_{41}(x) = x^2 + x + 41$, which is prime for $0 \leq x \leq 39$. To date, no one has found a polynomial of the form $f_A(x)$ that represents distinct primes for more than the first 40 values of x. However, several people including Beeger [3], Lehmer [14], and Fung and Williams [7] have found polynomials which have higher asymptotic densities of prime values. According to Conjecture F, the function $C(\Delta)$ should provide a good indication of likely candidate polynomials. For example, the largest value of $C(\Delta)$ currently known [11] before this work is

$$C(-1359885851421247218 7) = 5.3670819.$$

The corresponding polynomial $x^2 + x + 3399714628553118047$ starts off slower than Euler's polynomial (only 24 primes for $x \leq 100$ compared to 87), but for $x \leq 10^7$ it assumes 2517022 prime values as compared to only 2208197 by Euler's polynomial. Notice that for Euler's polynomial we have $C(-163) = 3.3197732$, so by Conjecture F we expect that it will assume fewer prime values asymptotically than $x^2 + x + 3399714628553118047$.

The purpose of this paper is to describe a new method for accurately computing $C(\Delta)$ for values of $|\Delta|$ up to 70 digits (under the Extended Riemann Hypothesis — ERH) and to provide some new values of Δ for which $C(\Delta)$ is larger than any value previously computed.

2. Estimating $C(\Delta)$

The infinite product representation (1.1) of $C(\Delta)$ converges very slowly; consequently, we need another method to approximate it more rapidly. We used the formula of Fung and Williams [7], which can be derived from (14) and (20) of Shanks [23]. For $\Delta < -4$ they show that

$$C(\Delta) = \frac{c\pi^3\sqrt{|\Delta|}}{90h_\Delta} \cdot \frac{1}{L\left(2, \chi_\Delta\right)} \prod_{\substack{p \mid \Delta \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right),$$

where q denotes a prime such that $\left(\frac{\Delta}{q}\right) = 1$, h_Δ is the ideal class number of the imaginary quadratic order $\mathcal{O}_\Delta$ and

$$c = \begin{cases} \frac{5}{2} & \text{if } \Delta \equiv 1 \pmod 8, \\ \frac{1}{2} & \text{if } \Delta \equiv 5 \pmod 8, \\ \frac{15}{16} & \text{otherwise.} \end{cases}$$

Similarly, one can derive for $\Delta > 0$ [11]

$$C(\Delta) = \frac{c\pi^4\sqrt{\Delta}}{180R_\Delta h_\Delta} \cdot \frac{1}{L\left(2, \chi_\Delta\right)} \prod_{\substack{p \mid \Delta \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right),$$

where as above h_Δ is the class number of the real quadratic order $\mathcal{O}_\Delta$ and R_Δ is the regulator, i.e., the natural logarithm of the fundamental unit of $\mathcal{O}_\Delta$. Thus, in order to approximate $C(\Delta)$ we have to compute the class number (and regulator for $\Delta > 0$) of the quadratic order $\mathcal{O}_\Delta$, factor Δ, and estimate the infinite product

$$P = \frac{1}{L\left(2, \chi_\Delta\right)} \cdot \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right).$$

Also, we note that because

$$-\log \prod_{\substack{p \mid \Delta \\ p \geq A}} \left(1 - p^{-4}\right) \sim \sum_{\substack{p \mid \Delta \\ p \geq A}} p^{-4} = O\left(A^{-4} \log_A |\Delta|\right),$$

it is a simple matter to estimate the value of $\prod_{p \mid \Delta}(1-p^{-4})$ very accurately without having to completely factor Δ. Fortunately, P converges much more quickly than (1.1), and, while we could use the method of [7] to estimate it rapidly, we found that a slight modification of the method of Bach [2] to evaluate $L\left(2, \chi_\Delta\right)$ produced an even faster technique for doing this. We will now briefly sketch this procedure. The notation, unless otherwise stated, is that of [2].

We first let χ be any non-principal character modulo m, and we put

$$B(x, \chi) = \prod_{p < x} \frac{p^2}{p^2 - \chi(p)}, \quad \overline{B}(x, \chi) = \prod_{p \geq x} \frac{p^2}{p^2 - \chi(p)},$$
$$F(x, \chi) = \prod_{q < x} \left(1 - \frac{2}{q(q-1)^2}\right), \quad \overline{F}(x, \chi) = \prod_{q \geq x} \left(1 - \frac{2}{q(q-1)^2}\right),$$

where, as above, the values of p are prime integers and the values of q are odd primes such that $\left(\frac{\Delta}{q}\right) = 1$. It is easy to deduce that

$$|\log \overline{F}(x, \chi)| \leq 3 \sum_{n \geq x} \frac{1}{(n-1)^3} < \frac{2}{x^2} \quad (x > 15). \tag{2.1}$$

By the reasoning in [2], we have

$$\log \overline{B}(x,\chi) = \int_{x^-}^{\infty} \frac{d\Psi(t,\chi)}{t^2 \log t} dt - T(x,\chi), \tag{2.2}$$

where

$$T(x,\chi) = \sum_{\substack{p^k \geq x \\ p < x}} \frac{\chi(p^k)}{kp^{2k}}.$$

The method of the proof of Lemma 5.1 of [2] can be used to establish that

$$|T(x,\chi)| \leq 4C \left[\frac{2}{3x^{3/2} \log x} + \frac{3}{5x^{5/3} \log 2} \right], \tag{2.3}$$

where $C = 1.25506$. Also, if

$$\Psi^1(x,\chi) = \int_0^x \Psi(t,\chi) dt,$$

then under the ERH (Lemma 9.3 of [2]) we know that

$$|\Psi^1(x,\chi)| \leq c(m) x^{3/2} + h(x), \tag{2.4}$$

where

$$c(m) = 2/3 \,(\log m + 5/3)$$

and

$$h(x) = x \log x + (2c(m) + 1)\, x + 3c(m) + 1.$$

If we integrate by parts twice, we get, on the assumption that x is integral,

$$\begin{aligned} \int_{x^-}^{\infty} \frac{d\Psi(t,\chi)}{t^2 \log t} dt = {} & -\frac{\Psi(x-1,\chi)}{x^2 \log x} - \frac{\Psi^1(x,\chi)(2\log x + 1)}{x^3 \log^2 x} \\ & + \int_x^{\infty} \Psi^1(t,\chi) \left(\frac{6 \log^2 t + 5 \log t + 2}{t^4 \log^3 t} \right) dt. \end{aligned} \tag{2.5}$$

We next define, for a given positive integer x,

$$a_i = \frac{(x+i)^2 \log(x+i)}{S(x)},$$

where

$$S(x) = \sum_{i=0}^{x-1} (x+i)^2 \log(x+i).$$

Clearly

$$\sum_{i=1}^{x-1} a_i = 1. \tag{2.6}$$

We now consider

$$E(x,\chi) = \sum_{i=0}^{x-1} a_i \log \overline{B}(x+i,\chi) \tag{2.7}$$

and note that

$$\sum_{i=0}^{x-1} a_i \log B(x+i,\chi) + E(x,\chi) = \log L\,(2,\chi)\,. \tag{2.8}$$

It follows that

$$|\log L\,(2,\chi) - \sum_{i=0}^{x-1} a_i \log B(x+i,\chi)| \le |E(x,\chi)|.$$

We put

(2.9)

$$C^*(Q,\Delta) = w\sqrt{|\Delta|}\prod_{p\,|\,\Delta}\left(1-\frac{1}{p^4}\right)F(Q,\chi_\Delta)\exp\left\{-\sum_{i=0}^{Q-1} a_i \log B(Q+i,\chi_\Delta)\right\},$$

where χ_Δ is the Kronecker symbol $(\Delta/\cdot)$ and

$$w = \begin{cases} c\pi^3/(90h_\Delta) & \text{if } \Delta < 0,\\ c\pi^4/(180R_\Delta h_\Delta) & \text{if } \Delta > 0.\end{cases}$$

We now note that if $k = 5\cdot 10^{-r}$, then

$$\left|\frac{C(\Delta) - C^*(Q,\Delta)}{C(\Delta)}\right| < k$$

when

$$|\log C(\Delta) - \log C^*(Q,\Delta)| < \log(1+k), \tag{2.10}$$

and $C^*(Q,\Delta)$ will approximate $C(\Delta)$ to r figures of accuracy. By (2.8)

$$\log C(\Delta) - \log C^*(Q,\Delta) = \log \overline{F}(Q,\chi_\Delta) - E(Q,\chi_\Delta).$$

Hence, by (2.1),

$$|\log C(\Delta) - \log C^*(Q,\Delta)| \le |E(Q,\chi_\Delta)| + \frac{2}{Q^2} \quad (Q > 15).$$

Thus, we need to be able to bound $E(x,\chi_\Delta)$ in order to find a value for Q such that (2.10) holds.

We note that by (2.2), (2.5), and (2.7), we get

$$\begin{aligned}|E(x,\chi)| \le{}& \left|\sum_{i=0}^{x-1} a_i \frac{\Psi(x+i-1,\chi)}{(x+i)^2\log(x+i)}\right| + \left|\sum_{i=0}^{x-1} a_i \frac{\Psi^1(x+i,\chi)(2\log(x+i)+1)}{(x+i)^3\log^2(x+i)}\right| \\ &+ \left|\sum_{i=0}^{x-1} a_i \int_{x+i}^{\infty}\Psi^1(t,\chi)\frac{6\log^2 t + 5\log t + 2}{t^4\log^3 t}dt\right| + \left|\sum_{i=0}^{x-1} a_i T(x+i,\chi)\right|.\end{aligned}$$

It is easy to see that

$$\begin{aligned} S(x) > U(x) :={}& \int_0^{x-1}(t+x)^2\log(t+x)dt \\ ={}& 1/3\left[(2x-1)^3(\log(2x-1)-1/3) - x^3(\log x - 1/3)\right] \\ >{}& 2x^3\log x \end{aligned} \tag{2.11}$$

when $x > 3000$. Also,

$$\sum_{i=0}^{x-1}(x+i)^{1/2} < \int_0^x (x+t)^{1/2}dt = \lambda x^{3/2}, \tag{2.12}$$

where $\lambda = 2/3(2^{3/2}-1) \approx 1.2189514$. With these observations, (2.4), and (2.6) we get

$$\begin{aligned}\left|\sum_{i=0}^{x-1} a_i \frac{\Psi(x+i-1,\chi)}{(x+i)^2\log(x+i)}\right| &= \frac{1}{S(x)}\left|\sum_{i=0}^{x-1}\Psi(x+i-1,\chi)\right| \\ &< \frac{(1+2^{3/2})c(m)x^{3/2}}{U(x)} + \frac{h(x)+h(2x)}{2x^3\log x}\end{aligned} \tag{2.13}$$

and

$$\begin{aligned}\left|\sum_{i=0}^{x-1} a_i \frac{\Psi^1(x+i,\chi)(2\log(x+i)+1)}{(x+i)^3\log^2(x+i)}\right| &\le \sum_{i=0}^{x-1} a_i \frac{c(m)(x+i)^{3/2}(2\log(x+i)+1)}{(x+i)^3\log^2(x+i)} \\ &\quad + \frac{h(x)(2\log x+1)}{2x^3\log x},\end{aligned}$$

because $h(x)(2\log x+1)/(2x^3\log x)$ is a decreasing function of x. It follows from (2.11), (2.12) and the definition of a_i that

$$\begin{aligned}\left|\sum_{i=0}^{x-1} a_i \frac{\Psi^1(x+i,\chi)(2\log(x+i)+1)}{(x+i)^3\log^2(x+i)}\right| &\le \frac{c(m)}{U(x)}\left(2+\frac{1}{\log x}\right)\lambda x^{3/2} \\ &\quad + \frac{h(x)(2\log x+1)}{2x^3\log x}.\end{aligned} \tag{2.14}$$

It is also easy to deduce from (2.3), (2.6), (2.11), and (2.12) that

$$\left|\sum_{i=0}^{x-1} a_i T(x+i,\chi)\right| \le \frac{8C\lambda x^{3/2}}{3S(x)} + \frac{12C}{(5\log 2)x^{5/3}}. \tag{2.15}$$

We note that by (2.4)

$$\begin{aligned}&\left|\sum_{i=0}^{x-1} a_i \int_{x+i}^{\infty}\Psi^1(t,\chi)\frac{6\log^2 t+5\log t+2}{t^4\log^3 t}dt\right| \\ &\quad \le c(m)\sum_{i=0}^{x-1} a_i\left(\frac{6}{\log(x+i)}+\frac{5}{\log^2(x+i)}+\frac{2}{\log^3(x+i)}\right)\int_{x+i}^{\infty}t^{-5/2}dt \\ &\qquad + \int_x^{\infty}\frac{h(x)}{t^4}\left(\frac{6}{\log t}+\frac{5}{\log^2 t}+\frac{2}{\log^3 t}\right)dt.\end{aligned}$$

Also, by (2.12) we have

$$\begin{aligned}&\sum_{i=0}^{x-1} a_i\left(\frac{6}{\log(x+i)}+\frac{5}{\log^2(x+i)}+\frac{2}{\log^3(x+i)}\right)(x+i)^{-3/2} \\ &\qquad \le \frac{\lambda x^{3/2}}{S(x)}\left(6+\frac{5}{\log x}+\frac{2}{\log^2 x}\right).\end{aligned}$$

TABLE 2.1. Q values for approximating $C(\Delta)$.

$\log_{10}\|\Delta\|$	Q
30	525500
35	576000
40	624500
45	670500
50	715000
55	758000
60	799500
65	839500
70	879000
75	917000

If, after Bach, we define the linear functional T_x on any function f which is positive and non-decreasing but grows sufficiently slowly that $f(x)(1+2\log x)/(x^3 \log x)$ is decreasing, as

$$T_x(f) = \frac{f(x)+f(2x)}{2x^3\log x} + \frac{f(x)(2\log x+1)}{2x^3\log x} + \int_x^\infty \frac{f(t)}{t^4}\left(\frac{6}{\log t} + \frac{5}{\log^2 t} + \frac{2}{\log^3 t}\right) dt,$$

we see by (2.13), (2.14), (2.15) and our results above that

$$|E(x,\chi)| \le \frac{c(m)x^{3/2}}{U(x)}\left(1+2^{3/2}+6\lambda\right) + \frac{13c(m)\lambda}{6x^{3/2}\log^2 x} + \frac{2\lambda c(m)}{3x^{3/2}\log^3 x} + \frac{4C\lambda}{3x^{3/2}\log x} + \frac{12C}{(5\log 2)x^{5/3}} + T_x(h). \tag{2.16}$$

Since (for $\alpha < 3$)

$$T_x(x^\alpha) \le \frac{1}{x^{3-\alpha}\log x}\left[\left(3+2^\alpha+\frac{6}{3-\alpha}\right) + \left(1+\frac{5}{3-\alpha}\right)\frac{1}{\log x} + \frac{2}{3-\alpha}\frac{1}{(\log x)^2}\right],$$

$$T_x(x\log x) \le \frac{1}{x^2}\left[8 + \frac{2\log 2+6}{\log x} + \frac{1}{\log^2 x}\right],$$

it is easy to use (2.16) to find the least value of Q such that

$$|E(Q,\chi_\Delta)| + 2/Q^2 < \log(1+k).$$

Since the dominant term of (2.16) is $O(x^{-3/2}\log m)$, we would expect

$$Q = O\left(10^{2r/3}\left(\log|\Delta|\right)^{2/3}\right).$$

Of course, since the bound on $E(Q,\chi_\Delta)$ and (later) the correctness of h_Δ and R_Δ are all conditional on the truth of the ERH, our approximation of $C(\Delta)$ is as well. In Table 2.1 we list the Q values required to approximate $C(\Delta)$ to 8 significant figures for various sizes of Δ. Naturally, any Q which works for a given size of Δ also works for all smaller values of Δ. We note here that since $\Delta \equiv 1 \pmod 4$ and our values of Δ will be squarefree in the sequel, we may use $m = |\Delta|$. These same properties of Δ are assumed in Table 2.1.

3. Computing the class number and regulator

The majority of the computation time spent in using (2.9) to approximate $C(\Delta)$ is in computing the class number and regulator of the quadratic order $\mathcal{O}_\Delta$. We used the method described in [12] (Algorithm 4.3). The underlying strategy of this algorithm is the same as that of Hafner and McCurley [9] and its variants [6], [4], [1], [5]. Suppose we have computed a factor base $FB = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ consisting of invertible prime ideals such that the equivalence classes of some subset of FB generates the class group Cl_Δ of $\mathcal{O}_\Delta$. For $\vec{v} \in \mathbb{Z}^k$ we define

$$FB^{\vec{v}} = \prod_{i=1}^{k} \mathfrak{p}_i^{v_i},$$

where $\mathfrak{p}_i \in FB$. We call $\vec{v}$ a *relation* if the ideal $FB^{\vec{v}}$ is principal, i.e., $FB^{\vec{v}} \sim \mathcal{O}_\Delta$. The algorithm then produces a generating system $L = \{\vec{v}_1, \dots, \vec{v}_n\}$ of the *relation lattice*

$$\Lambda = \{\vec{v} \in \mathbb{Z}^k \mid FB^{\vec{v}} \sim \mathcal{O}_\Delta\}, \tag{3.1}$$

which is the kernel of the homomorphism

$$\mathbb{Z}^k \to Cl_\Delta, \quad \vec{v} \to FB^{\vec{v}}. \tag{3.2}$$

Since the equivalence classes of the ideals of FB generate the class group, it follows that the homomorphism (3.2) is surjective, and we have

$$Cl_\Delta \cong \mathbb{Z}^k/\Lambda.$$

This implies that Λ is a k-dimensional lattice and its determinant is equal to h_Δ. Also, the *relation matrix* $A = (\vec{v}_1^T, \dots, \vec{v}_n^T)$, the matrix formed by taking the relations $\vec{v}_i$ as columns, has rank k. The diagonal elements which are greater than 1 in S, the Smith normal form of A, are precisely the elementary divisors of Cl_Δ. Thus, in addition to h_Δ, we get the structure of Cl_Δ as a direct product of cyclic subgroups with very little extra effort.

This strategy can easily be extended to compute class groups and regulators of real quadratic orders [4, 1]. In this case, we compute relations of the form $(\vec{v}, \log|\gamma|)$, where $FB^{\vec{v}} = (\gamma)$, i.e., γ generates the principal ideal $FB^{\vec{v}}$. We produce a generating system

$$L' = \{(\vec{v}_1, \log|\gamma_1|), (\vec{v}_2, \log|\gamma_2|), \dots, (\vec{v}_l, \log|\gamma_l|)\}$$

of the extended relation lattice

$$\Lambda' = \{(\vec{v}, \log|\gamma|) \in \mathbb{Z}^k \times \mathbb{R} \mid FB^{\vec{v}} = (\gamma)\}. \tag{3.3}$$

Then, if Λ is the part of Λ' in $\mathbb{Z}^k$, as before we have $Cl_\Delta \cong \mathbb{Z}^k/\Lambda$. Furthermore, it can be shown [4] that $\det(\Lambda') = h_\Delta R_\Delta$, so by computing this determinant we also get the regulator.

The major difference between our approach and that of [9], [6], etc., is in the way the generating system of the relation lattice is produced. The solution employed by contemporary algorithms is to attempt to factor randomly produced ideals over the factor base. We replace this step by a sieve-based strategy similar to that used in the MPQS factoring algorithm [24]. The idea of employing sieving to compute relations in similar contexts was first suggested by Seysen [22], and later by Paulus [20].

In the MPQS, one sieves over quadratic polynomials $F(x) = ax^2 + bx + c$ in order to find certain values of x for which $F(x)$ completely factors over a finite factor base of prime integers. By sieving a polynomial $F(x)$ over an interval, we mean testing each value of X in a given interval as to whether all the prime factors of $F(X)$ are contained in a finite, given set. The observation that $F(X) \equiv F(X+ip) \pmod{p}$ for $i \in \mathbb{Z}$, p prime, allows one to use a sieve to perform this test rather than evaluating every value of $F(x)$ and attempting to factor it.

In our case, we first compute an ideal $\mathfrak{a}$ as a power-product of the prime ideals in our factor base FB, i.e., $\mathfrak{a} = FB^{\vec{e}}$ for some $\vec{e} \in \mathbb{Z}^k$. The vector $\vec{e}$ is sparse with non-zero entries ± 1. In [12], we provide further details on how $\vec{e}$ is selected. Then, we search for integers X and Y such that $f(X,Y) = aX^2 + bXY + cY^2$, the norm form of $\mathfrak{a}$, factors over the norms of the ideals in FB. For each such pair (X,Y), there exists a quadratic number γ such that $\mathfrak{a}/(\gamma) = \mathfrak{b}^{-1}$ splits over the factor base. As shown in [12], we can explicitly compute $\mathfrak{b}$ and its decomposition over FB easily. Since $\mathfrak{a}$ splits over FB by construction, we have that $\mathfrak{a}\mathfrak{b} = (\gamma)$ yields a relation.

The main work in generating relations with the strategy outlined above is finding smooth values of the quadratic polynomial $f(x,y)$. It is certainly possible to sieve $f(x,y)$ in two dimensions. However, most sieve-based factoring algorithms, including the MPQS, work exclusively with univariate quadratic polynomials. Hence, in order to parallel these factoring methods as closely as possible, we also work with the univariate polynomials $F(x) = f(x,1) = ax^2 + bx + c$.

Thus, the problem of finding relations for class group computation is reduced to the same problem as finding relations in the MPQS factoring algorithm. A large amount of effort has been invested in making the MPQS and its variants as efficient as possible, and we make use of as many of these techniques as possible, most notably self-initialization. The use of these sieving methods results in a dramatic increase in performance. See [12] for more details and computational results.

4. Previous results

The example $\Delta = -135988585142124 72187$ and others like it were generated using the MSSU [18, 17], a numerical sieving device capable of searching for solutions to sets of simultaneous linear congruences at the rate of over 4×10^{12} candidates per second. A typical problem solvable by such sieving devices is as follows. A set of moduli is first specified, and then a set of acceptable residues is chosen for each modulus. The sieve then searches for integer solutions $x > L$ for some lower bound L such that x is congruent to any one of the acceptable residues modulo each of the corresponding moduli.

The strategy employed to find values of Δ with large $C(\Delta)$ values was to search for values of $\Delta \equiv 5 \pmod{8}$ for which $\left(\frac{\Delta}{q}\right) = -1$ for all odd primes q less than or equal to some bound p. Clearly this has the effect of maximizing the leading terms in the infinite product representation of $C(\Delta)$. The problem of finding such values of Δ can be formulated as a sieve problem by fixing as moduli 8 and the primes less than or equal to p. For each of these primes q the acceptable residues are the integers x such that $1 \leq x < q$ and x is a quadratic non-residue modulo q. The acceptable residue for 8 is 5, since we want solutions $\Delta \equiv 5 \pmod{8}$. The sieve then searches for integers which are congruent to one of the acceptable residues for each modulus.

Following Lehmer [14], we define the symbol N_p to represent the least positive integer congruent to 3 modulo 8 such that $\left(\frac{-N_p}{q}\right) = -1$ for all odd primes $q \leq p$. Lehmer computed the first table of N_p values for $p \leq 107$. Lehmer, Lehmer, and Shanks extended these computations in [15], Problem III, to values of $p \leq 163$, and Lehmer also computed the next three values up to $p = 181$, but did not publish them. In [11], the MSSU was used to extend these computations further, and values of N_p up to $p = 277$ and least prime solutions of N_p up to $p = 269$ were found. Tables 4.1 and 4.2 are reproduced from [11], and contain all the currently known values of N_p and the least prime solutions of N_p, respectively.

TABLE 4.1. N_p — Least Solutions

p	N_p	h_{-N_p}	$C(-N_p)$
3	19	1	0.94222046
5,7	43	1	1.6297209
11,13	67	1	2.0873308
17, ... ,37	163	1	3.3197732
41,43	77683	22	3.3003388
47	1333963	79	3.8123997
53,59	2404147	107	3.7793704
61	20950603	311	3.8410195
67	36254563	432	3.6365197
71	51599563	487	3.8514289
73,79	96295483	665	3.8528890
83	114148483	692	4.0332358
89, ... ,103	269497867	1044	4.1092157
107	585811843	1536	4.1185705
109,113	52947440683	13909	4.3245257
127	71837718283	15204	4.6097143
131,137	229565917267	29351	4.2679170
139	575528148427	44332	4.4746374
149, ... ,163	1432817816347	70877	4.4163429
167	6778817202523	149460	4.5565681
173	16501779755323	223574	4.7524812
179,181	30059924764123	296475	4.8379057
191,193,197	110587910656507	553436	4.9711959
199	4311527414591923	3791896	4.5293043
211,223	10472407114788067	5798780	4.6162389
227, ... ,241	22261805373620443	8035685	4.8576312
251	132958087830686827	19412108	4.9146545
257	441899002218793387	33684408	5.1635913
263,269	2278509757859388307	77949544	5.0669199
271	5694230275645018963	119705436	5.2163043
277	9828323860172600203	156104956	5.2552050

TABLE 4.2. N_p — Least Prime Solutions

p	N_p	h_{-N_p}	$C(-N_p)$
3	19	1	0.94222046
5,7	43	1	1.6297209
11,13	67	1	2.0873308
17, ... ,37	163	1	3.3197732
41	222643	33	3.7289570
43,47	1333963	79	3.8123997
53,59	2404147	107	3.7793704
61	20950603	311	3.8410195
67,71	51599563	487	3.8514289
73,79	96295483	665	3.8528890
83	146161723	857	3.6832906
89	1408126003	2293	4.2771747
97,101,103	3341091163	3523	4.2878711
107,109,113	52947440683	13909	4.3245257
127	193310265163	26713	4.3024065
131,137	229565917267	29351	4.2679170
139	915809911867	59801	4.1834705
149, ... ,163	1432817816347	70877	4.4163429
167, ... ,181	30059924764123	296475	4.8379057
191	3126717241727227	3201195	4.5685162
193,197,199	8842819893041227	5188215	4.7414735
211,223	13688678408873323	6524653	4.6907580
227, ... ,241	22261805373620443	8035685	4.8576312
251	4908856524312968467	121139393	4.7847955
257,263,269	7961860547428719787	140879803	5.2409110

Similarly, we define the symbol M_p to represent the least positive integer congruent to 5 modulo 8 such that $\left(\frac{M_p}{q}\right) = -1$ for all odd primes $q \leq p$. We would expect, due to Conjecture F, that $|f_A(x)|$ will have a large density of prime values when $A = (1 - M_p)/4$. According to Poletti [21], Beeger was the first to make a table of M_p values; he listed them up to $p = 59$. Lehmer, Lehmer, and Shanks [15], Problem VI, extended this table in 1970 up to $p = 139$, and Lehmer produced one more value for $p = 163$, but did not publish it. The MSSU was used to extend the table further, to $p = 283$ and $p = 263$ for least prime solutions. Tables 4.3 and 4.4, again reproduced from [11], contain all the currently known values of M_p and the least prime solutions of M_p, respectively.

TABLE 4.3. M_p — Least Solutions

p	M_p	R_{M_p}	h_{M_p}	$C(M_p)$
3	5	0.4812	1	1.7733051
5	53	1.9657	1	1.3831458
7,11	173	2.5708	1	2.0427655
13	293	2.8366	1	2.4386997
17	437	3.0422	1	2.7933935

TABLE 4.3. M_p — Least Solutions (continued)

p	M_p	R_{M_p}	h_{M_p}	$C(M_p)$
19,23	9173	12.4722	1	3.1227858
29	24653	5.0562	4	3.1631443
31,37,41	74093	7.2159	5	3.0809338
43	170957	16.9391	3	3.3299831
47,53,59	214037	28.9536	2	3.2704656
61	2004917	48.2972	3	4.0077796
67	44401013	352.5078	2	3.8743032
71	71148173	140.5395	6	4.1026493
73,79	154554077	694.9131	2	3.6684052
83,89,97	163520117	152.1367	9	3.8307572
101,103	261153653	512.3272	3	4.3158954
107,109,113	1728061733	4021.1400	1	4.2447622
127	9447241877	1252.3775	7	4.5541813
131	19553206613	6209.5055	2	4.6250203
137,139	49107823133	18804.6808	1	4.8420287
149, ... ,163	385995595277	27068.0628	2	4.7144914
167	13213747959653	330785.2663	1	4.5147795
173	14506773263237	331149.0061	1	4.7257867
179,181	57824199003317	165998.4596	4	4.7059530
191,193	160909740894437	275610.2629	4	4.7279560
197,199	370095509388197	794079.6472	2	4.9779329
211	1409029796180597	3130386.6897	1	4.9274990
223	4075316253649373	5291574.7242	1	4.9577054
227,229,233	18974003020179917	2737025.3979	4	5.1711431
239,241	224117990614052477	10257518.4583	4	4.7415726
251,257,263	637754768063384837	22908547.7970	3	4.7753226
269, ... ,283	4472988326827347533	14462868.4419	12	5.0085747

TABLE 4.4. M_p — Least Prime Solutions

p	M_p	R_{M_p}	h_{M_p}	$C(M_p)$
3	5	0.48121	1	1.7733051
5	53	1.96572	1	1.3831458
7,11	173	2.57081	1	2.0427655
13	293	2.83665	1	2.4386997
17	2477	6.47234	1	3.1173079
19,23	9173	12.47223	1	3.1227858
29	61613	36.23370	1	2.7929099
31,37,41	74093	7.21597	5	3.0809338
43	170957	16.93918	3	3.3299831
47	360293	68.23691	1	3.6032397
53	679733	92.04349	1	3.6713558
59,61	2004917	48.29722	3	4.0077796
67	69009533	869.69643	1	3.9166092
71	138473837	1369.29769	1	3.5221802

TABLE 4.4. M_p — Least Prime Solutions (continued)

p	M_p	R_{M_p}	h_{M_p}	$C(M_p)$
73	237536213	1725.64096	1	3.6624765
79	384479933	2087.35754	1	3.8534093
83	883597853	3018.26471	1	4.0411818
89, ... ,113	1728061733	4021.14004	1	4.2447622
127	9447241877	1252.37753	7	4.5541813
131,137,139	49107823133	18804.68086	1	4.8420287
149	1843103135837	119080.85359	1	4.6828076
151,157	4316096218013	192239.83257	1	4.4390420
163,167	15021875771117	344898.80858	1	4.6165765
173,179	82409880589277	804942.51462	1	4.6336310
181	326813126363093	1551603.41110	1	4.7874230
191,193	390894884910197	1650908.48845	1	4.9214877
197	1051212848890277	547589.04349	5	4.8659116
199,211,223	4075316253649373	5291574.72421	1	4.9577054
227	274457237558283317	45653225.95687	1	4.7155029
229	443001676907312837	6097479.67224	9	4.9843291
233	599423482887195557	65388978.22854	1	4.8658247
239	614530964726833997	64783176.97206	1	4.9730080
241, ... ,263	637754768063384837	22908547.79705	3	4.7753226

The example $\Delta = -13598858514212472187$ was found by using the MSSU to generate all values of Δ such that $-2\times 10^{19} < \Delta < 10^{19}$, $\Delta \equiv 5 \pmod 8$, and $(\Delta/q) = -1$ for all odd primes $q \leq 199$. By restricting to the primes less than 200 more results were generated than if a larger bound had been used. Furthermore, the sieve runs faster if fewer moduli are used, and thus a larger number of candidates could be tested. For the several thousand numbers that resulted, $C(\Delta)$ was computed using the Shanks heuristic [19, p.283] to calculate the class numbers when $\Delta > 0$, and the technique of the previous section when $\Delta < 0$. The $C(\Delta)$-hichamps for the cases $\Delta < 0$ and $\Delta > 0$ were then selected, i.e., those Δ with the property that their corresponding $C(\Delta)$ value is greater than that of any Δ of smaller magnitude found by the sieve.

$C(\Delta)$ was evaluated correct to 8 figures for all of these $C(\Delta)$-hichamps by using the previously described technique with the class numbers and regulators computed as in [11]. No deviations from the results given by the Shanks heuristic were found. Table 4.5 contains the $C(\Delta)$-hichamps for the negative values of Δ and Table 4.6 contains the $C(\Delta)$-hichamps for the positive values of Δ. The largest $C(\Delta)$ value found by this method is the aforementioned $C(-13598858514212472187) = 5.3670819$.

By using Littlewood's bounds on $L(1, \chi_\Delta)$ [16], it is easy to see [18] that under the ERH

$$C(\Delta) < \{1 + o(1)\} e^{\gamma} \log\log|\Delta|,$$

where γ is Euler's constant. Indeed, if we define

$$r(\Delta) = C(\Delta)/e^{\gamma} \log\log|\Delta|, \tag{4.1}$$

Table 4.5. $C(\Delta)$-hichamps ($\Delta < 0$).

Δ	h_Δ	$r(\Delta)$	$C(\Delta)$
-4311527414591923	3791896	0.70964311	4.5293043
-5513463660887323	4214276	0.72070730	4.6086597
-8842819893041227	5188215	0.73881217	4.7414735
-11779882219755787	5904498	0.74766420	4.8086435
-14363876114143483	6478729	0.75133104	4.8393795
-15326624594334307	6664840	0.75401443	4.8590033
-30462609261723907	9340770	0.75475096	4.8883007
-32779240456803163	9520419	0.76778682	4.9753684
-50792117776428667	11782274	0.76982885	5.0043010
-221328140358231307	24591656	0.76210545	5.0050646
-234391954943494723	24980688	0.77179828	5.0706939
-369885383792662483	31346105	0.77034080	5.0766794
-441899002218793387	33684408	0.78260083	5.1635912
-554395014308976163	37602038	0.78412438	5.1814176
-803608018073876563	45224688	0.78297632	5.1864453
-2038991582966171563	71351592	0.78588177	5.2369507
-2039953459173530587	70825967	0.79181939	5.2765336
-6849319464662435083	128288704	0.79508448	5.3384020
-13598858514212472187	179800672	0.79604287	5.3670819

Table 4.6. $C(\Delta)$-hichamps ($\Delta > 0$).

Δ	h_Δ	R_Δ	$r(\Delta)$	$C(\Delta)$
370095509388197	2	794079.64725	0.79561686	4.9779328
16710980998953317	2	5296924.24250	0.77763395	5.0144216
18974003020179917	4	2737025.39798	0.80118713	5.1711431
587108439330001613	2	30377994.30089	0.78408776	5.1831340
2430946649400343037	4	30781378.01108	0.78019116	5.2048129
3512773592849667053	1	146959147.17623	0.78399584	5.2422843
4927390995446922917	2	86988957.82243	0.78257150	5.2437622

then as Δ increases we would expect that extreme values of the $r(\Delta)$ would tend to approach 1 if the ERH is true. Indeed, it is possible to use a result of Joshi [13] to show unconditionally that for any given positive $\varepsilon < 1$, there exists an infinitude of values of Δ such that $r(\Delta) > (1+\varepsilon)/2$. Thus, the closeness of $r(\Delta)$ to 1 provides an indication of how good our $C(\Delta)$ values are in relation to the size of Δ. We have listed the $r(\Delta)$ values corresponding to the $C(\Delta)$ values in both Table 4.5 and Table 4.6. The largest $r(\Delta)$ value we found was 0.80118713, corresponding to $\Delta = 18974003020179917$.

5. Generating Δ with larger $C(\Delta)$ values

The MSSU and other sieving devices only allow a fixed number of moduli to be used at one time. Furthermore, when many moduli are used solutions can be quite rare. Hence, we used an unpublished idea of Lehmer which he employed to find the

TABLE 5.1. A_p^- and A_p^+ values.

p	A_p^-	A_p^+
257	93	43
277	942	1457
307	8138	1730
331	75586	203909
353	4893645	3261415

20 digit value of Δ with small $L(1, \chi_\Delta)$ that appears in [15, p.439]. Lehmer's idea allows us to find solutions Δ with $\left(\frac{\Delta}{q}\right) = -1$ for all $q \leq p$ while using fewer moduli for the sieve than would otherwise be required. To this end, we examined negative discriminants of the form

$$\Delta = -(A_p^- + B_p X)$$

and positive discriminants of the form

$$\Delta = A_p^+ + B_p X,$$

where

$$B_p = \prod_{\substack{q \geq 233 \\ q \text{ prime}}}^{p} q$$

and $\left(\frac{-A_p^-}{q}\right) = \left(\frac{A_p^+}{q}\right) = -1$ for all primes q ($233 \leq q \leq p$). We used five different values of p ranging from 257 to 353, and the least non-square values of A_p^- and A_p^+ for each $p \in \{257, 277, 307, 331, 353\}$, which are given in Table 5.1. Our values of B_p, A_p^-, and A_p^+ were selected so that we could generate solutions with approximately 30, 40, 50, 60, and 70 decimal digits, respectively.

For the case $\Delta = -(A_p^- + B_p X) < 0$, we ran five separate sieve jobs corresponding to each of the five pairs (A_p^-, B_p), $p \in \{257, 277, 307, 331, 353\}$. We employed the MSSU to sieve on values of $X > 0$ using as moduli 8 and primes $q_1, q_2, \ldots, q_m$ with $q_m \leq 229$. For each q_i, the acceptable residues were the values of x such that $0 \leq x < q_i$ and $\left(\frac{-(A_p^- + B_p x)}{q_i}\right) = -1$. The observation that if $\left(\frac{y}{q}\right) = -1$ then $x \equiv (y + A_p^-)(-B_p)^{-1} \pmod{q}$ satisfies $\left(\frac{-(A_p^- + B_p x)}{q}\right) = -1$ allows one to easily determine all the acceptable residues for any given modulus q. In order to ensure that $-(A_p^- + B_p X) \equiv 5 \pmod{8}$ we use $x \equiv (5 + A_p^-)(-B_p)^{-1} \pmod{8}$ as the single acceptable residue for the modulus 8. Thus, each solution X found by the sieve which is congruent to one of the acceptable residues modulo 8 and every odd prime $q_i \leq 229$ yields a value of $\Delta = -(A_p^- + B_p X)$ such that $\left(\frac{\Delta}{q}\right) = -1$ for all odd primes q less than or equal to 257, 277, 307, 331, and 353, for each of the five pairs (A_p^-, B_p). Notice that in order to find these Δ values we need only sieve with primes less than or equal to 229.

We ran another five sieve jobs for the cases $\Delta = (A_p^+ + B_p X) > 0$ corresponding to the five pairs (A_p^+, B_p), $p \in \{257, 277, 307, 331, 353\}$. Again, we used as moduli 8 and the odd primes $q_i \leq 229$. The single acceptable residue for 8 is $(5 - A_p^+)(B_p)^{-1} \bmod 8$, and the residues for each odd modulus q are given by $(y - A_p^+)(B_p)^{-1} \bmod q$ for each $0 \leq y < q$ such that $\left(\frac{y}{q}\right) = -1$. Similarly, we obtained solutions $\Delta = A_p^+ + B_p X$

TABLE 5.2. X values yielding $\Delta = -(A_p^- + B_pX)$ with large $C(\Delta)$.

	Composite Δ		Prime Δ	
p	X	n_p	X	n_p
257	466615859130369190	30	450663765848215486	30
277	370813410258174265	40	216364723669119361	39
307	47981058088400465	49	177458814519025865	49
331	180678079710346857	59	395114060043264249	60
353	628306272374561842	70	22664467457614162	69

TABLE 5.3. X values yielding $\Delta = A_p^+ + B_pX$ with large $C(\Delta)$.

	Composite Δ		Prime Δ	
p	X	n_p	X	n_p
257	396312611459525290	30	218767904524491586	30
277	697769695386840996	40	482626651962422460	40
307	639546162945216939	50	762810077127556299	50
331	390861540221680416	60	435543163377951528	60

such that $\left(\frac{\Delta}{q}\right) = -1$ for all odd primes q less than or equal to 257, 277, 307, 331, and 353, for each of the five pairs (A_p^+, B_p), again sieving only with the primes less than or equal to 229.

For each of the ten sieve jobs, we recorded the first 40 solutions X and computed an estimate of $C(\Delta)$ from (1.1) using only the odd primes less than 300000. The composite and prime solutions with the largest $C(\Delta)$ estimates for each pair (A_p^-, B_p) and (A_p^+, B_p) were selected, and their corresponding $C(\Delta)$ values were approximated to 8 significant digits using (2.9). The values of X yielding the best negative composite and prime solutions are listed in Table 5.2, and those yielding the best positive composite and prime solutions in Table 5.3. In these tables, as well as all subsequent tables, n_p denotes the number of decimal digits of the corresponding $|\Delta|$.

In Table 5.4 and 5.5 we present the class numbers, $r(\Delta)$ values, and $C(\Delta)$ approximations for composite and prime $\Delta = -(A_p^- + B_pX)$, respectively. Tables 5.6 and 5.7 contain the corresponding values for those $\Delta = A_p^+ + B_pX$, together with the regulators of the quadratic orders $\mathcal{O}_\Delta$. Unfortunately, we have not yet been able to compute h_Δ and R_Δ for the 70-digit positive values of Δ corresponding to $p = 353$, and hence we do not give $C(\Delta)$ values for these two discriminants.

TABLE 5.4. $C(\Delta)$ values for $\Delta = -(A_p^- + B_pX)$.

p	h_Δ	$r(\Delta)$	$C(\Delta)$
257	31732649150720	0.69697563	5.24106505
277	1976760608074606524	0.68146521	5.46609410
307	61214787639146593755232	0.64025219	5.37024150
331	11759774715020356643576929686	0.62718279	5.48239469
353	2665657958662748945432048763520638	0.59889664	5.41351382

TABLE 5.5. $C(\Delta)$ values for prime $\Delta = -(A_p^- + B_pX)$.

p	h_Δ	$r(\Delta)$	$C(\Delta)$
257	32205652661741	0.67490844	5.07451231
277	1616387968869310119	0.63738276	5.10571428
307	1216769866630410363955593	0.61788587	5.19553338
331	1864424811361812456660398865	0.58425088	5.11311211
353	508563922487050052185191214201329	0.59868248	5.38920304

TABLE 5.6. $C(\Delta)$ values for $\Delta = A_p^+ + B_pX$.

p	h_Δ	R_Δ	$r(\Delta)$	$C(\Delta)$
257	2	22720556233553.76096	0.70502465	5.29857981
277	32	136748579504713684.06545	0.66227548	5.32039776
307	200	1756711054276061939500.58651	0.63660975	5.36584646
331	2	13733001618386164806256150133.05014	0.61969493	5.42321540

TABLE 5.7. $C(\Delta)$ values for prime $\Delta = A_p^+ + B_pX$.

p	h_Δ	R_Δ	$r(\Delta)$	$C(\Delta)$
257	23	1486019958907.89109	0.69782143	5.23353756
277	1	3524266116230524920.39910	0.68457204	5.49456617
307	1	388454242975025771000236.31306	0.62860736	5.30013214
331	3	10083301848416825689407861674.34216	0.59383948	5.19778395

TABLE 5.8. Run times for $\Delta = -(A_p^- + B_pX)$.

	Composite Δ			Prime Δ		
p	n_p	t_h	t_{ver}	n_p	t_h	t_{ver}
257	30	19.35 s	44.26 s	30	18.79 s	44.27 s
277	40	2.81 m	4.12 m	39	2.77 m	4.40 m
307	49	23.45 m	1.58 h	49	26.34 m	2.29 h
331	59	8.62 h	9.15 h	60	8.26 h	8.51 h
353	70	6.47 d	1.18 s	69	5.29 d	0.55 s

We made use of Jacobson's technique [12] to evaluate h_Δ and R_Δ for these large values of Δ. The computations were carried out on a 296 MHz SUN UltraSPARC-II processor with 1024 MB of main memory using C++ routines based on the LiDIA computer algebra library [8]. The CPU time required for these computations ranged from about 19 seconds to about 6.5 days. In order to guarantee the correctness of our results under the ERH, we also performed the verification described in [12, Ch.3] for each of the ten discriminants. The time required for this additional computation ranged from about 26 seconds to 9 hours. The run-times in CPU seconds (s), minutes (m), hours (h), or days (d) for all Δ considered above are contained in Tables 5.8 and 5.9. By t_h we denote the CPU time required to compute the class

TABLE 5.9. Run times for $\Delta = A_p^+ + B_p X$.

	Composite Δ			Prime Δ		
p	n_p	t_{Cl}	t_{ver}	n_p	t_{Cl}	t_{ver}
257	30	38.95 s	30.48 s	30	41.42 s	25.65 s
277	40	7.75 m	3.50 m	40	10.02 m	3.17 m
307	50	1.78 h	2.25 h	50	1.92 h	1.72 h
331	60	1.04 d	7.84 h	60	1.97 d	4.85 h

number and regulator of $\mathcal{O}_\Delta$, and by t_{ver} the CPU time required for the ERH verification.

6. LARGER $C(\Delta)$ VALUES WITH FEWER SIEVE MODULI

All the examples given above were generated by sieving with odd primes $q \leq 229$. However, the more moduli used, the harder it is to find solutions. For example, in order to generate the 40 solutions X for $A_{331}^+ + B_{331}X$ it took almost a week of sieve time. Hence, we also ran two sieve jobs using primes $q \leq 199$ in an effort to find $C(\Delta) > 5.49456617$, the largest value found using the methods in the previous section. The first of these was designed to generate 70-digit negative discriminants. We used the MSSU to search for values of X such that $\left(\frac{-(C_{337}^- + D_{337}X)}{q_i}\right) = -1$ for odd primes $3 \leq q_i \leq 199$ and $-(C_{337}^- + D_{337}X) \equiv 5 \pmod 8$. We used

$$C_{337}^- = 1613265, \quad \text{and} \quad D_{337} = \prod_{\substack{q \geq 211 \\ q \text{ prime}}}^{337} q,$$

where C_{337}^- is the smallest integer such that $\left(\frac{-C_{337}^-}{q}\right) = -1$ for all primes q $(211 \leq q \leq 337)$. Thus, every solution X is such that $\left(\frac{-(C_{337}^- + D_{337}X)}{q}\right) = -1$ for all odd primes $3 \leq q \leq 337$, and we only need to sieve with primes less than 200.

The second sieve job was designed to generate positive discriminants of about 70 decimal digits. We searched for solutions X such that $\left(\frac{C_{337}^+ + D_{337}X}{q_i}\right) = -1$ for all odd primes $3 \leq q_i \leq 199$ and $C_{337}^+ + D_{337}X) \equiv 5 \pmod 8$. $C_{337}^+ = 14130195$ is the smallest integer such that $\left(\frac{C_{337}^+}{q}\right) = -1$ for all primes q $(211 \leq q \leq 337)$. In this case, every solution X is such that $\left(\frac{C_{337}^+ + D_{337}X}{q}\right) = -1$ for all odd primes $3 \leq q \leq 337$, and as above we only need to sieve with primes less than 200.

In both cases we generated 500 solutions to the sieve problem, and ordered the solutions according to $C(\Delta)$ estimates computed from (1.1) using only the odd primes less than 300000. We were able to find these solutions much faster than in the previous problems using sieve moduli up to 229. For the negative discriminants, it took just over 4 days to find the 500 solutions, compared to over a week for only 40 solutions when sieving with $q \leq 229$. The composite and prime solutions with the largest $C(\Delta)$ estimates for each pair (C_{337}^-, D_{337}) and (C_{337}^+, D_{337}) were selected, and their corresponding $C(\Delta)$ values were approximated to 8 significant digits using (2.9). The values of X yielding these best composite and prime values of Δ are listed in Table 6.1.

TABLE 6.1. X values yielding Δ with large $C(\Delta)$.

	Composite Δ		Prime Δ	
Δ	X	n_p	X	n_p
$-(C_{337}^{-} + D_{337}X)$	25455834532981358	70	313761223204200542	71
$C_{337}^{+} + D_{337}X$	480364831229973862	72	344681809987259902	71

TABLE 6.2. $C(\Delta)$ values for $\Delta = -(C_{337}^{-} + D_{337}X)$.

	h_Δ	$r(\Delta)$	$C(\Delta)$
D	3970294065612579776224498944560096	0.61158214	5.53388912
p	14171128122001880660726087303711577	0.59973638	5.44325560

TABLE 6.3. $C(\Delta)$ values for $\Delta = C_{337}^{+} + D_{337}X$.

	h_Δ	R_Δ	$r(\Delta)$	$C(\Delta)$
D	4	6625291330661652053429358727545606.5573	0.62299738	5.65726388
p	3	7748091868989848744375988664484659.1689	0.60191933	5.46368497

TABLE 6.4. Run times for $\Delta = -(C_{337}^{-} + D_{337}X)$ and $\Delta = C_{337}^{+} + D_{337}X$.

	Composite Δ			Prime Δ		
p	n_p	t_h	t_{ver}	n_p	t_h	t_{ver}
337^{-}	70	5.84 d	3.57 s	71	5.81 d	2.99 s
337^{+}	72	10.68 d	7.83 d	71	7.55 d	7.30 d

In Table 6.2 and 6.3 we present the class numbers, regulators, $r(\Delta)$ values, and $C(\Delta)$ approximations for composite and prime $\Delta = -(C_{337}^{-} + D_{337}X)$ and $\Delta = C_{337}^{+} + D_{337}X$, respectively. In both tables, the entry D denotes the composite discriminant and p indicates the prime discriminant. The CPU time needed on a 296 MHz SUN UltraSPARC-II processor to compute the class numbers and verify them under the ERH are given in Table 6.4.

Although we have been able to find significantly larger $C(\Delta)$ values than those in [11], the fact that the $r(\Delta)$ values corresponding to these Δ are somewhat small suggests that larger $C(\Delta)$ values should be obtainable for other Δ of the same size. However, as of yet we know of no way to use the MSSU to find Δ such that $\left(\frac{\Delta}{q}\right) = -1$ for primes $q \le p$ and $p > 229$ without resorting to Lehmer's idea, which unfortunately causes the sizes of Δ under consideration to increase rapidly. The Δ presented in [11] are minimal in the sense that they are taken from the set of the smallest integers in absolute value for which $\left(\frac{\Delta}{q}\right) = -1$ for primes $q \le 199$, and hence the $r(\Delta)$ values are larger than ours, as expected.

The largest value of $C(\Delta)$ we found is

$$C(\Delta) = 5.65726388$$

for the 72-digit $\Delta = C_{337}^{+} + D_{337}\,480364831229973862$. Thus, according to Conjecture F and under the assumption of the ERH, we expect the polynomial $x^2 + x - A$ for A given by

$$33251810980696878103150085257129508857312847751498190349983874538507313$$

to have the largest asymptotic density of prime values for any polynomial of this type currently known.

Acknowledgments

The authors wish to thank an anonymous referee for several helpful suggestions for improving the paper, as well as the Centre for Applied Cryptographic Research at the University of Waterloo for their support and for the use of their computing facilities.

References

1. C.S. Abel, *Ein Algorithmus zur Berechnung der Klassenzahl und des Regulators reellquadratischer Ordnungen*, Ph.D. thesis, Universität des Saarlandes, Saarbrücken, Germany, 1994.
2. E. Bach, *Improved approximations for Euler products*, Number Theory: CMS Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 13–28. MR **96i:**11124
3. N.G.W.H. Beeger, *Report on some calculations of prime numbers*, Nieuw Archief voor Wiskunde (2) **20** (1939), 48–50. MR **1:**65g
4. J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres (Paris), 1988-89, Birkhäuser, Boston, 1990, pp. 27–41. MR **92g:**11125
5. H. Cohen, F. Diaz y Diaz, and M. Olivier, *Calculs de nombres de classes et de régulateurs de corps quadratiques en temps sous-exponentiel*, Séminaire de Théorie des Nombres (Paris), 1990–91, Birkhäser, Boston, 1993, pp. 35–46. MR **94m:**11151
6. S. Düllmann, *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter binärer quadratischer Formen*, Ph.D. thesis, Universität des Saarlandes, Saarbrücken, Germany, 1991.
7. G.W. Fung and H.C. Williams, *Quadratic polynomials which have a high density of prime values*, Math. Comp. **55** (1990), 345–353. MR **90j:**11090
8. The LiDIA Group, *LiDIA: a* `c++` *library for computational number theory*, Software, Technische Universität Darmstadt, Germany, 1997, See http://www.informatik.tu-darmstadt.de/TI/LiDIA.
9. J.L. Hafner and K.S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), 837–850. MR **91f:**11090
10. G.H. Hardy and J.E. Littlewood, *Partitio numerorum III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.
11. M.J. Jacobson, Jr., *Computational techniques in quadratic fields*, Master's thesis, University of Manitoba, Winnipeg, Manitoba, 1995.
12. ———, *Subexponential class group computation in quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, Darmstadt, Germany, 1999.
13. P.T. Joshi, *The size of $L(1,\chi)$ for real nonprincipal residue characters χ with prime modulus*, J. Number Theory **2** (1970), 58–73. MR **40:**4215
14. D.H. Lehmer, *On the function $x^2 + x + A$*, Sphinx **6** (1937), 212–214, 1936 and 7:40.
15. D.H. Lehmer, E. Lehmer, and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. **24** (1970), no. 110, 433–451. MR **42:**5889
16. J.E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$*, Proc. London Math. Soc. **27** (1928), 358–372.
17. R.F. Lukes, *A very fast electronic number sieve*, Ph.D. thesis, University of Manitoba, Winnipeg, Manitoba, 1995.

18. R.F. Lukes, C.D. Patterson, and H.C. Williams, *Numerical sieving devices: Their history and some applications*, Nieuw Archief voor Wiskunde (4) **13** (1995), 113–139. MR **96m:**11082
19. R.A. Mollin and H.C. Williams, *Computation of the class number of a real quadratic field*, Utilitas Mathematica **41** (1992), 259–308. MR **93d:**11134
20. S. Paulus, *An algorithm of subexponential type computing the class group of quadratic orders over principal ideal domains*, Algorithmic Number Theory - ANTS-II (Université Bordeaux I, Talence, France), Lecture Notes in Computer Science, vol. 1122, Springer-Verlag, Berlin, 1996, pp. 243–257. MR **98c:**11143
21. L. Poletti, *Il contributo italiano alla tavola dei numeri primi*, Rivista di Matematica della Università di Parma **2** (1951), 417–434. MR **14:**121d
22. M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Math. Comp. **48** (1987), 757–780. MR **88d:**11129
23. D. Shanks, *On the conjecture of Hardy and Littlewood concerning the number of primes of the form* $n^2 + a$, Math. Comp. **14** (1960), 320–332. MR **22:**10960
24. R.D. Silverman, *The multiple polynomial quadratic sieve*, Math. Comp. **48** (1987), 329–339. MR **88c:**11079

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

E-mail address: `jacobs@cs.umanitoba.ca`

Department of Mathematics and Statistics, MS 360, 2500 University Drive N.W., University of Calgary, Calgary, Alberta, Canada T2N 1N4

E-mail address: `williams@math.ucalgary.ca`