MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 619–632

Some Computational Results on a Problem Concerning Powerful Numbers

By A. J. Stephens and H. C. Williams*

Abstract. Let D be a positive square-free integer and let $X+Y\sqrt{D}$ be the fundamental unit in the order with $\mathbf{Z}$-basis $\{1,\sqrt{D}\}$. An algorithm, which is of time complexity $O(D^{1/4+\varepsilon})$ for any positive ε, is developed for determining whether or not $D \mid Y$. Results are presented for a computer run of this algorithm on all $D < 10^8$. The conjecture of Ankeny, Artin and Chowla is verified for all primes $\equiv 1 \pmod 4$ less than 10^9.

1. Introduction. An integer N is said to be powerful if for any prime p such that $p \mid N$ we must have $p^2 \mid N$. In [4] Erdős conjectured that there do not exist three consecutive powerful numbers, and Granville [5] has shown that if this is true, then there exists an infinitude of primes p such that $p^2 \nmid 2^{p-1}-1$. Mollin and Walsh [7] have pointed out that if there exist three consecutive powerful numbers, then there must exist some square-free $D \equiv 7 \pmod 8$ with $X+Y\sqrt{D}$ being the fundamental unit of $\mathcal{Q}(\sqrt{D})$ such that for some odd k, X_k is an even powerful number and $Y_k \equiv 0 \pmod D$ is an odd integer, where $X_k+Y_k\sqrt{D} = (X+\sqrt{D}Y)^k$.

If, for a given value of D, we have $D \nmid Y$, then it is a relatively easy matter to show that the least possible value for k such that X_k is powerful and $D \mid Y_k$ must be very large (see [7] for an example with $D = 7$). Thus, for this and other reasons, Mollin and Walsh asked the second author whether it was possible to find those values of D such that $D \mid Y$. In general, however, this seems to be a very difficult problem. Indeed, Ankeny, Artin and Chowla [1] conjectured several years ago that if $(x+y\sqrt{p})/2$ is the fundamental unit of $\mathcal{Q}(\sqrt{p})$ when p is a prime and $p \equiv 1 \pmod 4$, then $p \nmid y$. Later, Mordell [8] conjectured that if $X+Y\sqrt{p}$ is the fundamental unit of $\mathcal{Q}(\sqrt{p})$ when $p \equiv -1 \pmod 4$ and p is a prime, then $p \nmid Y$. Neither of these conjectures has been proved, but the Ankeny, Artin, Chowla (AAC) conjecture has been verified, most recently, by Soleng [13] for all $p \leq 100028009$ and Mordell's conjecture has been verified for all $p < 7679299$ by Beach, Williams and Zarnke [2].

Because of the difficulty of this problem, we decided to investigate it numerically. In this paper we discuss how we found all the square-free values of D $< 10^8$ for which $D \mid Y$. We also verified the AAC conjecture for all $p < 10^9$. We describe two algorithms for conducting these numerical investigations. The first of these (the Small Step Algorithm) is basically the algorithm that has been used for previous work. We develop some general results concerning symmetric continued fractions

Received March 9, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R11, 11R27, 11Y16, 11Y40, 11Y65.

*Research supported by NSERC of Canada Grant #A7649.

in order to give a slightly more compact form of this procedure than has been used in the past. We then make use of the class group infrastructure ideas of Shanks [12] as developed and modified by Lenstra [6], Schoof [10], and Williams and Wunderlich [15] in order to derive a second algorithm (the Large Step Algorithm). The complexity of the first algorithm is $O(D^{1/2+\varepsilon})$ for all $\varepsilon > 0$; but the complexity of the second is $O(D^{1/4+\varepsilon})$. We then describe the results of implementing and running both of these algorithms on an AMDAHL 5850 computer.

2. Continued Fractions and Ideals. All previous search methods for testing the AAC conjecture have made use of the properties of continued fractions. As the methods that we will employ here also involve continued fractions, we will first provide a brief review of some relevant results. Several of these can be found in standard reference works like Perron [9] or Chrystal [3], and others can be found in [15].

We first assume that $\phi = (P + \sqrt{D})/Q$, where D is a nonsquare positive integer and P, Q are integers such that $Q \mid D - P^2$. The continued fraction expansion of $\phi_0 = \phi$ which we write as

$$\phi_0 = \langle q_0, q_1, q_2, \ldots, q_{n-1}, \phi_n \rangle$$

can be obtained by using** $q_0 = [\phi_0]$ and the recursive formulas

$$\begin{aligned} \phi_{i+1} &= 1/(\phi_i - q_i) > 1, \\ q_{i+1} &= [\phi_{i+1}], \end{aligned} \qquad (i = 0, 1, 2, \ldots).$$

Under the aforementioned conditions, it is well known that

$$\phi_n = (P_n + \sqrt{D})/Q_n,$$

where we can find P_n and Q_n by using $P_0 = P$, $Q_0 = Q$ and

$$P_{i+1} = q_i Q_i - P_i, \tag{2.1}$$

$$Q_{i+1} Q_i = D - P_{i+1}^2, \qquad (i = 0, 1, 2, \ldots), \tag{2.2}$$

$$q_{i+1} = [(P_{i+1} + d + \sigma_{i+1})/Q_{i+1}], \tag{2.3}$$

where $d = [\sqrt{D}]$ and

$$\sigma_{i+1} = \begin{cases} 0, & Q_{i+1} > 0, \\ 1, & Q_{i+1} < 0. \end{cases}$$

A somewhat more efficient method of determining these numbers has been given by Tenner (see [15]).

If we define $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$ and

$$A_{i+1} = q_{i+1} A_i + A_{i-1}, \tag{2.4}$$

$$B_{i+1} = q_{i+1} B_i + B_{i-1}, \qquad (i = -1, 0, 1, 2, \ldots), \tag{2.5}$$

$$\theta_{i+1} = (-1)^i (A_{i-1} - \phi B_{i-1}), \tag{2.6}$$

then

$$\theta_{i+1} = (-1)^i (G_{i-1} - \sqrt{D} B_{i-1})/Q_0 \qquad (i \geq -1), \tag{2.7}$$

where

$$G_{i-1} = Q_0 A_{i-1} - P_0 B_{i-1} \qquad (i \geq -1). \tag{2.8}$$

**We use $[\alpha]$ to denote that integer such that $\alpha - 1 < [\alpha] \leq \alpha$.

In [14] it is pointed out that***

$$\theta_{i+1}\bar{\theta}_{i+1} = (G_{i-1}^2 - DB_{i-1}^2)/Q_0^2 = (-1)^i Q_i/Q_0, \tag{2.9}$$

$$\theta_{i+1}^{-1} = \prod_{j=1}^{i} \phi_i, \tag{2.10}$$

and

$$G_{i-1} = P_i B_{i-1} + Q_i B_{i-2}, \tag{2.11}$$

$$DB_{i-1} = P_i G_{i-1} + Q_i G_{i-2}. \tag{2.12}$$

Let $\alpha, \beta \in \mathcal{Q}(\sqrt{D_0})$ and denote by $[\alpha, \beta]$ the set $\{u\alpha + v\beta \mid u, v \in \mathbf{Z}\}$. Let $\omega_0 = (r - 1 + \sqrt{D_0})/r$, where D_0 (> 0) is square-free, $r = 1$ when $D_0 \equiv 2, 3 \pmod 4$ and $r = 2$ when $D_0 \equiv 1 \pmod 4$. Any order $\mathcal{O}$ of $\mathcal{Q}(\sqrt{D_0})$ must have $\mathbf{Z}$-basis $\{1, n\omega_0\}$, where $n \in \mathbf{Z}$. We can denote such an order by $[1, n\omega_0]$. Now $\mathcal{O}_1$ is the maximal order of $\mathcal{Q}(\sqrt{D_0})$ and if ε_0 $(0 < \varepsilon_0 < 1)$ is the fundamental unit of $\mathcal{Q}(\sqrt{D_0})$ and η $(0 < \eta < 1)$ is the fundamental unit of the order $\mathcal{O}_r = [1, \sqrt{D_0}]$, then either $\eta = \varepsilon_0$ or $\eta = \varepsilon_0^3$. Thus, if $\varepsilon_0 = (x + y\sqrt{D_0})/r$ and $\eta = x + \sqrt{D_0}Y$ $(x, y, X, Y \in \mathbf{Z})$, we see that if $D_0 \mid y$, then $D_0 \mid Y$ and if $D_0 \mid Y$, then $D_0 \mid 3y$. It follows that if $3 \nmid D_0$, any algorithm that determines whether or not $D_0 \mid Y$ can be used to determine whether or not $D_0 \mid y$.

Let $\mathcal{O} = \mathcal{O}_n$ be any order in $\mathcal{Q}(\sqrt{D})$ and let $\mathfrak{a}$ be any primitive, integral ideal of $\mathcal{O}$. As mentioned in [15], we can write $\mathfrak{a}$ in the form $[Q/\sigma, (P + \sqrt{D})/\sigma]$, where $\sigma = r/g$, $D = (n/g)^2 D_0$, $g = \gcd(r, n)$. Here we have $\sigma Q \mid D - P^2$, and if we develop the continued fraction expansion of $\phi = (P + \sqrt{D})/Q$, we find that each of the primitive ideals

$$a_{i+1} = [Q_i/\sigma,\ (P_i + \sqrt{D})/\sigma] \qquad (i = 0, 1, 2, \dots)$$

is equivalent to $\mathfrak{a} = \mathfrak{a}_1$. Also, we have

$$(Q_0\theta_m)\mathfrak{a}_m = (Q_{m-1})\mathfrak{a}_1, \tag{2.13}$$

where by (α) we denote the principal ideal with generator α.

If by $L(\mathfrak{a})$ we denote the least positive integer of the ideal $\mathfrak{a}$, then $L(\mathfrak{a}) = |Q|/\sigma$. Also, if $\mathfrak{a}$ is a primitive ideal and $\mathfrak{a}$ does not contain any nonzero α such that both

$$|\alpha| < L(\mathfrak{a}), \qquad |\bar{\alpha}| < L(\mathfrak{a})$$

hold, then we say that $\mathfrak{a}$ is a *reduced* ideal. If $\mathfrak{a}_1 = \mathfrak{a}$ is a reduced ideal and if $\mathfrak{b}$ is a reduced ideal equivalent to $\mathfrak{a}$, then $b = \mathfrak{a}_k$ for some k. Also, if $\mathfrak{a}_1$ is a reduced ideal, then by results given in [15], we have $|Q_0| < 2\sqrt{D}$ and $-1 < \bar{\phi}_k < 0$ $(k \geq 1)$; hence,

$$0 < P_i < \sqrt{D}, \qquad 0 < Q_i < 2\sqrt{D} \quad (i \geq 1). \tag{2.14}$$

As there are only a finite number of distinct pairs (P_i, Q_i) satisfying (2.14) we must get $\phi_m = \phi_{m+p}$ for some $p > 0$, $m \geq 0$. By (2.2) we must have $Q_{m-1} = Q_{m-1+p}$

***We use $\bar{\alpha}$ to denote the conjugate of $\alpha \in \mathcal{Q}(\sqrt{D})$.

and by Lemma 6.1 of [15] and (2.1) we get $P_{m-1} = P_{m+p-1}$ $(m \geq 2)$. Thus, we have $P_1 = P_{p+1}$, $Q_1 = Q_{p+1}$ and

$$Q_0 = Q_p, \qquad P_0 \equiv P_p \pmod{Q_0}. \tag{2.15}$$

Let p be the least positive integer for which (2.15) holds. If η $(0 < \eta < 1)$ is the fundamental unit of $\mathcal{O}$, by Theorem 4.5 of [15] we must have $\eta = \theta_k$ for some $k \geq 1$. Since, in this case, $\mathfrak{a}_k = \mathfrak{a}_1$, we get $k = p + 1$ and by (2.5),

$$\eta = \theta_{p+1} = (-1)^p(A_{p-1} - \theta B_{p-1}). \tag{2.16}$$

If $\mathfrak{a} = [Q/\sigma,\ (P + \sqrt{D})/\sigma]$, define $\bar{\mathfrak{a}}$ to be $[Q/\sigma,\ (P - \sqrt{D})/\sigma]$. If $\mathfrak{a} = \bar{\mathfrak{a}}$, we say that $\mathfrak{a}$ is an *ambiguous* ideal. We can now give a result which is well known in the case $\mathfrak{a} = [1, \sqrt{D}]$.

THEOREM 2.1. *If $\mathfrak{a} = [Q_0/\sigma,\ (P_0 + \sqrt{D})/\sigma]$ $(Q_0 > 0)$ is a reduced, ambiguous ideal, then in the continued fraction expansion of $\phi_0 = (P_0 + \sqrt{D})/Q_0$, we have*

$$Q_{p-i} = Q_i, \tag{2.17}$$

$$P_{p-i} = P_{i+1} \qquad (0 \leq i \leq p), \tag{2.18}$$

where p is the least positive integer for which (2.15) *holds.*

Proof. Since $\bar{\mathfrak{a}}_1 = \mathfrak{a}_1$ $(= \mathfrak{a})$ and $\mathfrak{a}_1 = \mathfrak{a}_{p+1}$, we get $\mathfrak{a}_1 = \bar{\mathfrak{a}}_{p+1}$. Thus, $Q_p = Q_0$ and $P_0 \equiv -P_p \pmod{Q_0}$. Since $-1 < \bar{\phi}_1 < 0$ ($\mathfrak{a}_1$ is reduced), we get

$$P_p = [(d + P_0)/Q_0]Q_p - P_p = q_0Q_0 - P_0 = P_1$$

by Lemma 6.2 of [14]. Thus, (2.17) and (2.18) hold for $i = 0$. On using (2.2), the result of Lemma 6.1 of [15] and (2.1), it is a simple matter to verify by induction on i that (2.17) and (2.18) hold for $0 \leq i \leq p$. □

COROLLARY 2.1.1. *Under the conditions of the theorem we have $\mathfrak{a}_{i+1} = \bar{\mathfrak{a}}_{p+1-i}$. If $p = 2r$, then $\mathfrak{a}_{r+1} = \bar{\mathfrak{a}}_{r+1}$; if $p = 2s + 1$, then $\mathfrak{a}_{s+1} = \bar{\mathfrak{a}}_{s+2}$.* □

Let $\mathfrak{a}$ be a primitive ideal of $\mathcal{O} = \mathcal{O}_n$, then it is a simple matter to show that

$$\mathfrak{a}\bar{\mathfrak{a}} = (L(\mathfrak{a})) \tag{2.19}$$

when $\gcd(L(\mathfrak{a}), n) = 1$. We also point out that if $\mathfrak{a} = \mathfrak{a}_1$ is a reduced ideal of $\mathcal{O}$, then

$$\bar{\theta}_{k+1} = (1/\bar{\phi}_k)\bar{\theta}_k \quad \text{and} \quad 1/|\bar{\phi}_k| > 1$$

$(-1 < \bar{\phi}_k < 0)$ for $k \geq 1$. Hence,

$$|\bar{\theta}_{k+1}| > |\bar{\theta}_k| \qquad (k \geq 1). \tag{2.20}$$

If $\mathfrak{a}_1$ is a reduced, ambiguous ideal of $\mathcal{O}_n$ such that $\gcd(L(\mathfrak{a}_1), n) = 1$, then we can find B_{p-1} in (2.16) by only going up to about $p/2$ terms in the continued fraction expansion of ϕ. We show how this can be done in

THEOREM 2.2. *Let $\mathfrak{a} = [Q/\sigma,\ (D + \sqrt{D})/\sigma]$ be a reduced, ambiguous ideal in $\mathcal{O} = \mathcal{O}_n$ such that $\gcd(Q/\sigma, n) = 1$. If r is the least positive integer such that $P_r = P_{r+1}$ in the continued fraction expansion of $\phi = (P + \sqrt{D})/Q$, then $p = 2r$*

and $B_{p-1} = B_{r-1}(B_r + B_{r-2})$; *if* s *is the least positive integer such that* $Q_s = Q_{s+1}$, *then* $p = 2s + 1$ *and* $B_{p-1} = B_s^2 + B_{s-1}^2$.

Proof. By Corollary 2.1.1 we know that there must exist a value for r or a value for s. Suppose $P_r = P_{r+1}$. In this case we get

$$\begin{aligned}\mathfrak{a}_{r+1} &= [Q_r/\sigma,\ (P_r + \sqrt{D})/\sigma] = [Q_r/\sigma,\ (P_{r+1} + \sqrt{D})/\sigma] \\ &= [Q_r/\sigma,\ (-P_r + \sqrt{D})/\sigma] = \bar{\mathfrak{a}}_{r+1};\end{aligned}$$

also, by (2.13) we get

$$(L(\mathfrak{a}_1)\bar{\theta}_{r+1})\bar{\mathfrak{a}}_{r+1} = (L(\mathfrak{a}_{r+1}))\bar{\mathfrak{a}}_1 = (L(\mathfrak{a}_{r+1}))\mathfrak{a}_1 = (L(\mathfrak{a}_1)\theta_{r+1})\mathfrak{a}_{r+1}.$$

Hence, by (2.19) we see that $\varepsilon = \theta_{r+1}/|\bar{\theta}_{r+1}|$ is a unit of $\mathcal{O}$. Since $r \leq p/2 < p$, we have $\eta = \theta_{p+1} < \theta_{r+1} < 1$ and

$$\eta = 1/|\bar{\theta}_{p+1}| < 1/|\bar{\theta}_{r+1}| < 1$$

by (2.20). Since ε must be an integral power of η, we must have $\varepsilon = \eta$. On using (2.7), (2.9), and (2.16), we get

$$(-1)^p B_{p-1} = (2B_{r-1}G_{r-1})/Q_r.$$

By (2.14) and (2.11) we know that $G_{r-1} > 0$; hence, p is even and

$$Q_r B_{p-1} = 2B_{r-1}(P_r B_{r-1} + Q_r B_{r-2}).$$

Since $P_{r+1} = P_r$, we have $2P_r = q_r Q_r$ by (2.1); hence, by (2.5) we get

$$B_{p-1} = B_{r-1}(B_r + B_{r-2}).$$

Also, since B_k is a strictly increasing function of k for $k \geq 1$ and $B_k \geq 0$ $(k \geq -2)$, we must have $r = p/2$ by Corollary 2.1.1.

Suppose next that $Q_s = Q_{s+1}$. In this case we have $P_{s+1} \equiv -P_s \pmod{Q_s}$ and

$$\mathfrak{a}_{s+1} = [Q_s/\sigma,\ (P_s + \sqrt{D})/\sigma] = [Q_{s+1}/\sigma,\ (-P_{s+1} + \sqrt{D})/\sigma] = \bar{\mathfrak{a}}_{s+2}.$$

By using the same reasoning as above, we get $\eta = \theta_{s+1}/|\bar{\theta}_{s+2}|$. It follows that

$$(-1)^{p+1} Q_{s+1} B_{p-1} = B_{s-1}G_s + B_s G_{s-1};$$

hence, p is odd and

$$Q_{s+1}B_{p-1} = q_s Q_s B_s B_{s-1} + Q_{s+1}B_{s-1}^2 + Q_s B_s B_{s-2}$$

by (2.11) and (2.1). Since $Q_s = Q_{s+1}$, we have

$$B_{p-1} = B_s^2 + B_{s-1}^2$$

by (2.5). Also, we must have $p = 2s + 1$. □

We can use Theorem 2.2 to develop the Small Step Algorithm for determining whether or not $D \mid Y$. We assume here that $D = D_0$ is square-free and $\mathfrak{a}_1 = \mathcal{O}_1$.

THE SMALL STEP ALGORITHM (SSA)

(1) Put $P_0 = 0$, $Q_0 = 1$ when $D \equiv 2, 3 \pmod 4$ or $P_0 = 1$, $Q_0 = 2$ when $D \equiv 1 \pmod 4$.

(2) Compute the continued fraction expansion of $(P_0 + \sqrt{D})/Q_0$ by evaluating

$$P_i, Q_i, B_{i-1} \pmod D \qquad (i = 1, 2, 3, \ldots)$$

until we find the least r or s such that

$$P_r = P_{r+1}$$

or

$$Q_s = Q_{s+1}.$$

(3) If $P_r = P_{r+1}$, then $D \mid Y$ if and only if $D \mid B_{r-1}(B_r + B_{r-2})$. If $Q_s = Q_{s+1}$, then $D \mid Y$ if and only if $D \mid B_s^2 + B_{s-1}^2$.

As mentioned above, simple variants of this algorithm have been used to obtain the known numerical results on the AAC conjecture. As D increases, however, this algorithm tends to slow down. Since we know that $p = O(D^{1/2+\varepsilon})$ for any $\varepsilon > 0$ (see, for example, Williams [14]), we see that this algorithm is of complexity $O(D^{1/2+\varepsilon})$. In the following sections we will develop an algorithm, called the Large Step Algorithm, which will solve this problem in time complexity $O(D^{1/4+\varepsilon})$.

In order to do this, we will need to know how to find a reduced ideal which is equivalent to a given primitive ideal $\mathfrak{a}$. We point out here that by results in [15] we know that if $\mathfrak{a}_1 = \mathfrak{a} = [Q_0/\sigma,\ (P_0 + \sqrt{D})/\sigma]$ and $\phi_0 = (P_0 + \sqrt{D})/Q_0$, then the continued fraction expansion of ϕ must yield some Q_m such that $0 < Q_m \leq d$. When this occurs, we know that $\mathfrak{a}_{m+1}$ is a reduced ideal equivalent to $\mathfrak{a}_1$. Further, the value of m is $O(\log |Q_0|)$.

3. A Regulator Algorithm and Further Results. In order to develop our next algorithm we must first mention that if $\mathfrak{a} = [Q/\sigma,\ (P + \sqrt{D})/\sigma]$, $\mathfrak{b} = [Q'/\sigma,\ (P' + \sqrt{D})/\sigma]$ are both primitive ideals of an order $\mathcal{O}$, then we can find the primitive ideal $\mathfrak{c} = [Q''/\sigma,\ (P'' + \sqrt{D})/\sigma]$ and an integer U such that

$$\mathfrak{a}\mathfrak{b} = (U)\mathfrak{c}$$

by using the formulas below. These formulas are essentially those of Shanks [11] and can be easily derived by using the method discussed in [6] or [10].

We put $G = \gcd(Q/\sigma, Q'/\sigma)$ and solve

$$(Q/\sigma)x_1 \equiv G \pmod{Q'/\sigma}$$

for $x_1 \pmod{Q'/\sigma}$. Put

$$U = \gcd(G, (P + P')/\sigma) = \gcd(Q/\sigma, Q'/\sigma,\ (P + P')/\sigma) \tag{3.1}$$

and solve

$$x_2(P + P')/\sigma + Gy_2 = U$$

for x_2, y_2. Then

$$Q'' = QQ'/(\sigma U^2), \tag{3.2}$$

$$P'' \equiv P + XQ/(\sigma U) \pmod{Q''}, \tag{3.3}$$

where

$$X \equiv y_2 x_1 (P' - P) + x_2(D - P^2)/Q \pmod{Q'/U}.$$

Note that when, as frequently occurs, $U = G$, we can put $x_2 = 0$, $y_2 = 1$.

If we denote the pair (P, Q) $(Q > 0)$ by $\mathcal{A}$ and the pair (P', Q') $(Q' > 0)$ by $\mathcal{B}$, we use $\mathcal{A} \circ \mathcal{B}$ to denote the pair (P'', Q'') given by the formulas (3.2) and (3.3).

Also, since the ideal $\mathfrak{a}$ which corresponds to $\mathcal{A}$ is the same as that corresponding to $\mathcal{B}$ when and only when $Q = Q'$ and $P \equiv P' \pmod{Q}$, we will define equality of $\mathcal{A}$ and $\mathcal{B}$ by these conditions.

Let $\mathfrak{a} = \mathfrak{a}_1$ be any reduced ideal in $\mathcal{O}$ and let $\mathfrak{b}$ be any reduced ideal which is equivalent to $\mathfrak{a}$. By our remarks at the end of Section 2 we know that $\mathfrak{b} = \mathfrak{a}_m$ for some $m \leq p$. Define $\delta(\mathfrak{a}_m, \mathfrak{a}_1) = \log|\bar{\theta}_m|$. Notice that, by (2.20), $\delta(\mathfrak{a}_m, \mathfrak{a}_1)$ is a strictly increasing function of m. Also,

$$\delta(\mathfrak{a}_{p+1}, \mathfrak{a}_1) = \log|\bar{\theta}_{p+1}| = -\log\eta.$$

Thus we can always assume that

$$0 < \delta(\mathfrak{b}, \mathfrak{a}) < R,$$

where $R = -\log\eta$ is the regulator of $\mathcal{O}$.

Now let $\mathfrak{b}_1$ and $\mathfrak{a}_1$ be ideals of $\mathcal{O}$ and assume that $\mathfrak{b}_1 = [Q_0'/\sigma,\ (P_0' + \sqrt{D})/\sigma]$ $(Q_0' > 0)$ is a reduced ideal and $\mathfrak{a}_1 = (1)$. If

$$(U)\mathfrak{c} = \mathfrak{a}_s\mathfrak{b}_t,$$

where $\mathfrak{c}_1 = \mathfrak{c}$ is a primitive ideal of $\mathcal{O}$ and $\mathfrak{c}_{m+1} \sim \mathfrak{c}_1 \sim \mathfrak{b}_1$ is found by using the continued fraction method of reduction described at the end of Section 2, then by Theorem 5.2 of [15], we have $\mathfrak{c}_{m+1} = \mathfrak{b}_k$ for some $k \geq 1$ and

$$\theta_k' = (\theta_s\theta_t'\theta_{m+1}'')/U,$$

where $(L(\mathfrak{b}_1)\theta_t')\mathfrak{b}_t = (L(\mathfrak{b}_t))\mathfrak{b}_1$, $(\theta_s)\mathfrak{a}_s = (L(\mathfrak{a}_s))$, $(L(\mathfrak{c}_1)\theta_m'')\mathfrak{c}_m = (L(\mathfrak{c}_m))\mathfrak{c}_1$. It follows that if we put $\delta_i' = \delta(\mathfrak{b}_i, \mathfrak{b}_1)$, $\delta_j = \delta(\mathfrak{a}_j, \mathfrak{a}_1)$, then

$$\delta_k' = \delta_s + \delta_t' + \lambda, \tag{3.4}$$

where $\lambda = \log(|\bar{\theta}_{m+1}''|/U)$. By Theorem 4.3 of [15] we have

$$(\theta_{m+1}'')^{-1} < 2Q_0''/\theta_m'';$$

hence, by (2.9) we get $|\bar{\theta}_{m+1}''| < 2$. Also, since $0 < \theta_{m+1}'' < 1$, we have

$$|\theta_{m+1}''| > Q_m''/Q_0'' \geq 1/Q_0'';$$

thus,

$$\lambda > -\log(Q_0''U) \geq -\log(Q_{s-1}Q_{t-1}') > -\log 4D$$

by (2.14). We have shown, then, that in (3.4) we have

$$-\log 4D < \lambda < \log 2. \tag{3.5}$$

We will also require the following simple lemma.

LEMMA 3.1. *If $\mathfrak{a}_1$ is a reduced ideal of $\mathcal{O}$ and*

$$\delta(\mathfrak{a}_k, \mathfrak{a}_1) < \delta(\mathfrak{a}_s, \mathfrak{a}_1) + \log 2,$$

then $\mathfrak{a}_k = \mathfrak{a}_i$ for some i such that $1 \leq i \leq s+1$.

Proof. Let $\psi_i = 1/\phi_i$. Now $\psi_{i+1} = 1/\psi_i - [\phi_i]$; hence, $\bar{\psi}_i\bar{\psi}_{i+1} = 1 - \bar{\psi}_i[\phi_i]$. Since $-1 < \bar{\phi}_i < 0$ and $\phi_i > 1$, we have

$$|\bar{\psi}_i\bar{\psi}_{i+1}| \geq 1 + |\bar{\psi}_i| > 2 \qquad (i \geq 1). \tag{3.6}$$

Now

$$\delta(\mathfrak{a}_{s+2}, \mathfrak{a}_1) = \log|\bar{\theta}_{s+2}| = \delta(\mathfrak{a}_s, \mathfrak{a}_1) + \log|\bar{\psi}_i\bar{\psi}_{s+1}|;$$

thus, since $\delta(\mathfrak{a}_{s+2}, \mathfrak{a}_1) > \delta(\mathfrak{a}_s, \mathfrak{a}_1) + \log 2$ and δ is an increasing function of s, the lemma follows. □

We are now able to present an algorithm which can be used to compute the regulator R of $\mathcal{O}$ in $O(D^{1/4+\varepsilon})$ $(\varepsilon > 0)$ elementary operations. We let $\mathfrak{a}_1 = (1)$, $\delta_i = \delta(\mathfrak{a}_{i-1}, \mathfrak{a}_1)$, $\mathcal{A}_i = (P_i, Q_i)$, and put $L = [cD^{1/4}]$ where $L \in \mathbf{Z}$ and c is some constant. We usually use $c \geq 2$.

ALGORITHM TO COMPUTE R.

(1) Using the continued fraction algorithm, compute and store $\mathcal{A}_i$, δ_i for $i = 0, 1, 2, \ldots, s+1$, where $s = L+1$. If any $Q_i = Q_0$ with $0 < i \leq s+1$, then $R = \delta_i$ and we can exit from the algorithm.

(2) Put $\mathcal{B}_1 = \mathcal{A}_s$, $\delta_1^* = \delta_s$, $j = 1$.

(3) Compute U and (P'', Q'') from $\mathcal{C} = (P'', Q'') = \mathcal{A}_s \circ \mathcal{B}_j$. By expanding the continued fraction of $(P'' + \sqrt{D})/Q''$, find the least nonnegative m such that $0 < Q_m \leq d$ and put

$$\lambda_j = \log(|\theta''_{m+1}|/U), \qquad \delta^*_{j+1} = \delta^*_j + \delta_s + \lambda_j. \tag{3.7}$$

(4) If $\mathcal{C} = \mathcal{A}_i$ for some i such that $0 \leq i \leq s+1$, then

$$R = \delta^*_{j+1} - \delta_i,$$

and we can exit from the algorithm; otherwise, we replace j by $j+1$, $\mathcal{B}_j$ by $\mathcal{C}$, and go to (3).

Proof of the Regulator Algorithm. From (3.6) and (2.10) we see that $|\bar{\theta}_k| > 2^{[(k-1)/2]}$; hence,

$$\delta_k > (k/2 - 2)\log 2$$

and

$$\delta_s > (s/2 - 2)\log 2 > (cL/2 - 2)\log 2 > \log 4D \tag{3.8}$$

when D is sufficiently large. (Certainly, this is so if $c \geq 2$ and $D > 10^6$.) Since by (3.5) we have $\lambda_j > -\log 4D$ in (3.7), we must have

$$\delta^*_{j+1} > \delta^*_j.$$

Further, if we do not exit the algorithm at Step (1), then $R > \delta_s = \delta_1^*$; thus, there must be some integer t such that

$$\delta_t^* < R \leq \delta^*_{t+1}. \tag{3.9}$$

From (3.7) we get

$$\delta^*_{k+1} = \delta_1^* + k\delta_s + \sum_{i=1}^{k} \lambda_i > \delta_1^* + k\delta_s - k\log 4D.$$

Now if

$$k > (R - \delta_1^*)/(\delta_s - \log 4D),$$

then, since $\delta_s - \log 4D > (D^{1/4} - 2)\log 2 - \log 4D$ by (3.8) and selection of L, we see that

$$k = O(R/D^{1/4}) = O(D^{1/4+\varepsilon})$$

and $\delta^*_{k+1} > R$. Thus, $t = O(D^{1/4+\varepsilon})$.

Let $(P'', Q'') = \mathcal{A}_s \circ \mathcal{B}_t$ and let $\mathfrak{c}_{m+1} = [Q''_m/\sigma, (P'' + \sqrt{D})/\sigma]$. Since $\mathfrak{c}_{m+1}$ is reduced and $\mathfrak{c}_{m+1} \sim \mathfrak{a}_1$, we must have $\mathfrak{c}_{m+1} = \mathfrak{a}_{j-1}$ for some $1 \le j \le p+1$. Now since (3.9) holds, we must have

$$\delta(\mathfrak{a}_{j-1}, \mathfrak{a}_1) = \delta^*_{t+1} - R = \delta^*_t - R + \delta_s + \lambda_t < \delta_s + \log 2$$

by (3.5). It follows from Lemma 3.1 that $(P''_m, Q''_m) = \mathcal{A}_i$ for some $0 \le i \le s+1$. Since $R = \delta^*_{t+1} - \delta(\mathfrak{a}_{i-1}, \mathfrak{a}_1)$, we get $R = \delta^*_{t+1} - \delta_i$. □

Notice that we have shown that the algorithm is correct and that it will execute in $LD^\varepsilon + tD^\varepsilon = O(D^{1/4+\varepsilon})$ elementary operations when we assume that the $\mathcal{A}_i$'s in step (1) have been sorted.

We will now modify this algorithm in order to make it useful in determining whether or not $D \mid Y$. In the case of $\mathcal{O} = \mathcal{O}_r$ and $\mathfrak{a}_1 = \mathcal{O}$, we have $Q_0 = 1$ and $Y = B_{p-1}$ in the continued fraction expansion of $\sqrt{D}$, where we assume $D = D_0$ is square-free. We note here that $D \mid B_{p-1}$ if and only if $D \mid MB_{p-1}$ for M any integer such that $\gcd(M, D) = 1$. In our algorithm we will compute $MB_{p-1} \pmod D$ for some unknown M such that $\gcd(M, D) = 1$.

If $\mathfrak{a} = [Q, P + \sqrt{D}]$, $\mathfrak{b} = [Q', P' + \sqrt{D}]$ are ideals of $\mathcal{O}$ and $V = \gcd(Q, D)$, $V' = \gcd(Q', D)$, then V, V' are both square-free and since $Q \mid D - P^2$, $Q' \mid D - P'^2$, we have $V \mid P$, $V' \mid P'$. Put $W = \gcd(V, V')$. Since V, V', W are each square-free, we have $\gcd(V/W, W) = \gcd(V'/W, W) = \gcd(V'/W, V/W) = 1$; hence,

$$VV' \mid DW. \tag{3.10}$$

Since $W \mid Q$, $W \mid Q'$ and $W \mid P + P'$, we have $W \mid U$, where U is given by (3.1). If $U = WW^*$, then $\gcd(W^*, D) = 1$. Since $W^* \mid Q$ and $V \mid Q$, we know that $T = QQ'/(VV'W^*)$ is an integer. Since D is square-free, we have $\gcd(Q/V, D) = \gcd(Q'/V, D) = 1$; thus, $\gcd(T, D) = 1$. It follows that if Q'' is given by (3.2), we have

$$UQ'' = T(VV'/W), \tag{3.11}$$

where $\gcd(T, D) = 1$. Also, since $W^*Q'' = T(V/W)(V'/W)$, we have

$$VV' \mid W^2Q''. \tag{3.12}$$

As before, we will let $\mathfrak{a}_1 = (1)$ and put

$$(U)\mathfrak{c} = \mathfrak{a}_{s+1}\mathfrak{a}_{t+1},$$

where $\mathfrak{c}$ is a primitive ideal. Let $\mathfrak{c}_{m+1}$ $(\sim \mathfrak{c}_1)$ be the reduced ideal found by using the continued fraction reduction method. Then $\mathfrak{c}_{m+1} = \mathfrak{a}_{k+1}$ for some $k \ge 0$ and

$$\theta_{k+1} = (\theta_{s+1}\theta_{t+1}\theta''_{m+1})/U. \tag{3.13}$$

If we define $V_i = \gcd(Q_i, D)$, then we have $V_i \mid P_i$ and $V_i \mid A_{i-1}$ by (2.11). Set

$S_{i-1} = A_{i-1}/V_i$. We conclude this section with

THEOREM 3.1. *If* (3.13) *holds, then for some* $\tau = \pm 1$, *we have*

$$\tau T_k S_{k-1} \equiv L_1 H + L_2 K, \qquad \tau T_k B_{k-1} \equiv L_3 H + L_4 K \pmod{D},$$

where $\gcd(T_k, D) = 1$,

$$H \equiv W S_{s-1} S_{t-1} + (D/(W Z_s Z_t)) B_{s-1} B_{t-1},$$
$$K \equiv Z_s S_{s-1} B_{t-1} + Z_t S_{t-1} B_{s-1} \pmod{D},$$

and $W = \gcd(V_s, V_t)$, $Z_s = V_s/W$, $Z_t = V_t/W$, $Q_k = Q''_m$, $G''_{m-1} = P''_m B''_{m-1} + Q''_m B''_{m-2}$, $L_1 = G''_{m-1}/V_k$, $L_2 \equiv D B''_{m-1}/(Z_s Z_t V_k) \pmod{D}$, $L_3 = B''_{m-1}$, $L_4 = G''_{m-1}/(Z_s Z_t)$, $T_k = UWQ''_0/(V_s V_t)$.

Proof. By our previous remarks and (3.11), we see that $\gcd(T_k, D) = 1$. We next point out that from (2.6) we get

$$(-1)^{s+k} \theta_{s+1} \theta_{t+1} = H_1 (V_t V_s)/W - W K_1 \sqrt{D},$$

where $H_1 \equiv H$, $K_1 \equiv K \pmod{D}$; hence,

$$\begin{aligned} UQ''(-1)^j (A_{k-1} - \sqrt{D} B_{k-1}) = {} & G''_{m-1} H_1 (V_t V_s)/W + DW K_1 B'_{m-1} \\ & - \sqrt{D}(W K_1 G''_{m-1} + B''_{m-1} H_1 (V_t V_s)/W), \end{aligned} \tag{3.14}$$

where $j = s + t + m + k$. Now $Z_s Z_t \mid Q''_0$, and since $\mathfrak{c}$ is an ideal of $\mathcal{O}$, we have $Z_s Z_t \mid D - P''^2_0$; thus, $Z_s Z_t \mid P''_0$, and by (2.8) we deduce that $Z_s Z_t \mid G''_{i-1}$ $(i \geq 0)$. It follows immediately that L_4 is an integer. Also, since $V_k = \gcd(Q_k, D)$ and $Q_k \mid D - P''^2_m$, we have $V_k \mid P''_m$ and $V_k \mid G''_{m-1}$ by (2.11). Now $B''_{-1} = 0$ and from (2.12)

$$D B''_{m-1} = P''_m G''_{m-1} + Q''_m G''_{m-2};$$

hence, since $Z_s Z_t \mid G''_{m-1}$, $Z_s Z_t \mid G''_{m-2}$ $(m \geq 1)$, we get $Z_s Z_t V_k \mid D B''_{m-1}$. Thus, L_i $(i = 1, 2, 3, 4)$ are all integers and by (3.11) so is $D/(W Z_s Z_t)$. □

4. The Large Step Algorithm. We are now able to present our second algorithm for determining whether or not $D \mid Y$.

THE LARGE STEP ALGORITHM (LSA)

(1) Let L be defined as above. In the continued fraction expansion of $\sqrt{D}$, compute and store $\mathcal{A}_i = (P_i, Q_i)$ and $B_{i-1} \pmod{D}$ for $i = 1, 2, 3, \ldots, s+1$, where $L+1 \leq s \leq L+2$ and $Q_s < \sqrt{D}$. (If $Q_i > \sqrt{D}$, then $Q_{i+1} < \sqrt{D}$ by (2.14) and (2.2)). If any $Q_i = 1$ $(1 \leq i \leq s+1)$, put $Y' \equiv B_{i-1} \pmod{D}$ and go to (5).

(2) Put $V = \gcd(Q_s, D)$, $V' = V$, $P' = P$, $Q' = Q_s$, $E = E' \equiv (P/V) B_{s-1} + (Q/V) B_{s-2} \pmod{D}$, $F = F' \equiv B_{s-1} \pmod{D}$.

(3) Let $(P''_0, Q''_0) = \mathcal{A}_s \circ (P', Q')$. In the continued fraction expansion of $(P''_0 + \sqrt{D})/Q''_0$, compute (P''_i, Q''_i) and $B''_{i-1} \pmod{D}$ until the least nonnegative m is found such that $0 < Q''_m \leq d$. Put $Q' = Q''_m$, $G''_{m-1} = P''_m B''_{m-1} + Q''_m B''_{m-2}$, $P' \equiv P_m \pmod{Q'}$ $(0 < P' < Q')$, $W = \gcd(V, V')$,

$V'' = \gcd(Q', D)$, $Z = V/W$, $Z' = V'/W$, $L_1 = G''_{m-1}/V''$, $L_2 \equiv DB''_{m-1}/(ZZ'V'')$ (mod D), $L_3 = B''_{m-1}$, $L_4 = G''_{m-1}/(ZZ')$. Compute

$$H \equiv WEE' + (D/(WZZ'))FF',$$
$$K \equiv ZEF' + Z'E'F,$$
$$E' \equiv L_1H + L_2K,$$
$$F' \equiv L_3H + L_4K \pmod{D}.$$

(4) If $(P', Q') = \mathcal{A}_i$ for some i such that $0 \le i \le s+1$, put

$$S \equiv (P_i/V'')B_{i-1} + (Q_i/V'')B_{i-2},$$
$$Y' \equiv B_{i-1}E' - F'S \pmod{D};$$

otherwise, put $V' = V''$ and go to (3).

(5) $D \mid Y$ if and only if $D \mid Y'$.

Proof of the Large Step Algorithm. Since $Q_p = 1$, it is clear that the algorithm is correct when $p \le s+1$. We will suppose, therefore, that $p > s+1$. By (2.11) we have $E = A_{s-1}/V_s$, where $V_s = \gcd(Q_s, D)$. Thus, by Theorem 3.1 we see that at any stage of the execution of the algorithm the ideal $[Q', P' + \sqrt{D}] = \mathfrak{a}_{k+1}$ for some $k \ge 0$ and $S_{k-1} \equiv ME'$, $B_{k-1} \equiv MF'$ (mod D), where M is some (undetermined by the algorithm) integer such that $\gcd(M, D) = 1$. By the reasoning in the proof of the Regulator Algorithm, we must eventually have some $(P', Q') = \mathcal{A}_i$ where i is some integer such that $0 \le i \le s+1$. When this occurs, we have

$$\eta = \theta_{i+1}/\theta_{k+1},$$

where $\mathfrak{a}_{k+1} = [Q', P' + \sqrt{D}]$; hence, by (2.6),

$$(-1)^{p+i}Q_iB_{p-1} = B_{i-1}A_{k-1} - B_{k-1}A_{i-1}.$$

Now $S \equiv S_{i-1} \equiv (P_i/V_i)B_{i-1} + (Q_i/V_i)B_{i-2}$ (mod D), $\gcd(Q_k/V_k, D) = 1$, $Q_k = Q_i$, and $V_k = V_i$; hence,

$$(-1)^{p+i}(Q_k/V_k)Y \equiv B_{i-1}ME' - SF'M \equiv MY' \pmod{D}.$$

Thus, $Y' \equiv MY$ (mod D), where $\gcd(M, D) = 1$. □

Notice that by the reasoning used in the proof of the Regulator Algorithm, this algorithm too will execute in $O(D^{1/4+\varepsilon})$ elementary operations when we sort the $\mathcal{A}_i$'s in step (1) and do a binary search each time we wish to execute the search in step (4). In practice, however, it is faster to conduct this search by using hashing techniques. In our implementation we hashed on the last byte of each Q_i in $\mathcal{A}_i$.

Because B''_{i-1}, Q''_i, P''_i $(i \le m)$ and G''_{m-1} must be computed explicitly (not just modulo D) for this algorithm, it is important for implementation purposes to know just how large these numbers can get. We answer these questions in the following two theorems.

THEOREM 4.1. *Let* $\mathfrak{a} = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$ *with* $0 \le P_0 < Q_0$ *and let* m *be the least nonnegative integer such that* $0 < Q_m \le d$ *in the continued fraction expansion of* $(P_0 + \sqrt{D})/Q_0$. *We must have* $|Q_k| \le Q_0$ $(0 \le k \le m)$.

Proof. Certainly, if $m = 0$, we get our result. Thus, we may assume that $m > 0$.

Suppose $k = 1$, then $\theta_2 = 1/\phi_1 < 1$ and $\bar{\theta}_2 = (-\sqrt{D} - P_1)/Q_0$. Since $Q_0 > \sqrt{D}$ $(m > 0)$, we see that $0 \leq q_0 = [(P_0 + \sqrt{D})/Q_0] < 2$. If $q_0 = 0$, then $P_1 = -P_0$, $Q_1 = (D - P_0^2)/Q_0$; when $P_0 < \sqrt{D}$, then $0 < Q_1 < \sqrt{D} < Q_0$. If $q_0 = 0$ and $P_0 > \sqrt{D}$, then $|Q_1| = (P_0^2 - D)/Q_0 < P_0^2/Q_0 < Q_0$. If $q_0 = 1$, then $(P_0 + \sqrt{D})/Q_0 > 1$, $0 < Q_0 - P_0 < \sqrt{D}$, and $P_1 = Q_0 - P_0$. Hence, $0 < Q_1 = (D - P_1^2)/Q_0 < \sqrt{D} < Q_0$.

Thus the result holds when $k = 1$; it also holds for $k = m$. We may now assume that $1 < k < m$. By Theorem 2.4 of [15] we have $\bar{\phi}_k > 0$ and by Theorem 2.5 of [15] we get

$$B_{k-2}\theta_{k+1}^{-1} < Q_0/|Q_k|.$$

Since $\theta_{k+1} < 1$, $B_{k-2} \geq 1$, we have $Q_0/|Q_k| > 1$. □

COROLLARY 4.1.1. *Under the conditions of the theorem we have* $|P_k| < \sqrt{D} + Q_0$ $(0 \leq k \leq m)$.

Proof. Since $q_{k-1} = [(P_{k-1} + \sqrt{D})/Q_{k-1}]$, we have from (2.1)

$$P_k = D - \varepsilon Q_{k-1},$$

where $0 < \varepsilon < 1$. Since $0 < P_0 < Q_0$ and $|Q_{k-1}| < Q_0$, we have our result. □

THEOREM 4.2. *Under the conditions of Theorem* 4.1 *we have* $|G_{m-1}| < Q_0$, $B_{m-1} < Q_0/\sqrt{D}$.

Proof. If $m = 0$, then $G_{m-1} = Q_0$, $B_{m-1} = 0$; if $m = 1$, then $G_{m-1} = Q_0 q_0 - P_0 = P_1$, $B_{m-1} = B_0 = 1$. Since, as shown in the previous theorem, we have $P_1 = -P_0$ or $P_1 = Q_0 - P_0$, we see that the theorem holds for $m = 0, 1$. If $m = 2$ and $q_0 = 1$, then $Q_0 - P_0 < \sqrt{D}$ and $0 < P_1 < \sqrt{D}$; hence, $0 < Q_1 < (D - P_1^2)/Q_0 < \sqrt{D}$, which contradicts the definition of m. Thus, if $m = 2$, we have $q_0 = 0$, $P_1 = -P_0$, $Q_1 = (D - P_0^2)/Q_0$, $G_{m-1} = Q_0 - q_1 P_0$, $B_{m-1} = q_1 = [Q_0/(\sqrt{D} + P_0)] < Q_0/\sqrt{D}$. It follows that $G_{m-1} = Q_0\sqrt{D}/(P_0 + \sqrt{D}) + \varepsilon P_0$ $(0 < \varepsilon < 1)$; hence, $0 < G_{m-1} < Q_0$.

Suppose $m \geq 3$ and $\bar{\phi}_m > 0$. We get

$$0 < \bar{\theta}_{m+1} < 1/B_{m-2} \leq 1$$

from Theorem 2.5 of [15]. Since

$$2(-1)^m G_{m-1} = (\theta_{m+1} + \bar{\theta}_{m+1})Q_0$$

and

$$2(-1)^m \sqrt{D} B_{m-1} = (\bar{\theta}_{m+1} - \theta_{m+1})Q_0,$$

we have $|G_{m-1}| < Q_0$, $B_{m-1} < Q_0/\sqrt{D}$. If $m \geq 3$ and $\bar{\phi}_m < 0$, we have

$$0 < \bar{\theta}_m < 1/B_{m-3} \leq 1.$$

Putting $\psi_m = (\sqrt{D} - P_m)/Q_{m-1} = 1/\phi_m < 1$, we note that

$$\bar{\psi}_m = (-\sqrt{D} - P_m)/Q_{m-1}.$$

Since $\bar{\phi}_m < 0$, we have $|P_m| < \sqrt{D}$ and $Q_{m-1} > 0$; thus, $-\bar{\psi}_m < 2$, and we have $2(-1)^m G_{m-1}/Q_0 = \theta_m \psi_m + \bar{\theta}_m \bar{\psi}_m > -2$. Also, $2(-1)^m G_{m-1}/Q_0 < 1$. Further, since $\theta_{m+1} \leq \psi_m$ and $-\theta_{m+1} = -\bar{\psi}_m \bar{\theta}_m < -\psi_m$, we get

$$2\sqrt{D} B_{m-1} < Q_0(\psi_m - \bar{\psi}_m) = 2Q_0\sqrt{D}/Q_{m-1} < 2Q_0. \quad \square$$

Both the SSA and a version of the LSA were written in IBM/370 assembly language and run on an AMDAHL 5850 computer. The SSA program was run up to 10^7 only and succeeded in finding 8 values of D such that $D \mid Y$. These are: $46 = 2 \cdot 23$, $430 = 2 \cdot 5 \cdot 43$, $1817 = 23 \cdot 79$, $58254 = 2 \cdot 3 \cdot 7 \cdot 19 \cdot 73$, $209991 = 3 \cdot 69997$, $1752299 = 41 \cdot 79 \cdot 541$, $3124318 = 2 \cdot 1562159$, $4099215 = 3 \cdot 5 \cdot 273281$. The total amount of machine time consumed by this run was 2.25 hours. Tests with the LSA revealed that our version of it became faster than the SSA at values of D somewhat in excess of 2×10^6. Experiments in finding a good value for c for the numbers in the range that we considered resulted in our using $c = 2.5$.

The LSA program was run on all values of D from 10^6 to 10^8. The three D values given above in the range between 10^6 and 10^7 were found, but no further values of D were discovered. This run took about 40 hours of CPU time. Because of the interest in the AAC conjecture, we ran our LSA program on all primes ($\equiv 1 \pmod 4$) in the range 10^8 to 10^9. When D is a prime we always have $V_i = \gcd(Q_i, D) = 1$ and this allows for considerable simplification of step (3) of the LSA. This run required 31 additional CPU hours and found no prime which did not satisfy the conjecture. Notice that since the word size for the AMDAHL 5850 is 32 bits and all of the D values which we considered were less than 10^9 and $Q_0'' < \sqrt{D} \cdot \sqrt{D} = D$, we were able to use single-precision arithmetic throughout most of the algorithm.

Since none of the D values given above is a prime, we have, incidentally, verified Mordell's conjecture for all primes $< 10^8$. Finally, we remark that Mollin has proved that for each of the values of $D \equiv 7 \pmod 8$ in the list above, i.e., 209991 and 4099215, the corresponding X value is not powerful.

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

→ N. C. ANKENY, E. ARTIN & S. CHOWLA, "The class number of real quadratic number fields," *Ann. of Math.*, v. 56, 1952, pp. 479–493.

2. B. D. BEACH, H. C. WILLIAMS & C. R. ZARNKE, *Some Computer Results on Units in Quadratic and Cubic Fields*, Proc. 25th Summer Meeting Canad. Math. Congr., Lakehead Univ., 1971, pp. 609–648.

3. G. CHRYSTAL, *Textbook of Algebra*, part 2, 2nd ed., Dover reprint, New York, 1969, pp. 423–490.

4. P. ERDŐS, "Consecutive numbers," *Eureka* 38, 1975/76, pp. 3–8.

5. A. GRANVILLE, "Powerful numbers and Fermat's Last Theorem," *C. R. Math. Rep. Acad. Sci. Canada*, v. 8, 1986, pp. 215–218.

6. H. W. LENSTRA, JR., *On the Calculation of Regulators and Class Numbers of Quadratic Fields*, London Math. Soc. Lecture Note Series, vol. 56, 1982, pp. 123–150.

7. R. A. MOLLIN & P. G. WALSH, "A note on powerful numbers, quadratic fields, and the Pellian," *C. R. Math. Rep. Acad. Sci. Canada*, v. 8, 1986, pp. 109–111.

8. L. J. MORDELL, "On a Pellian equation conjecture," *Acta Arith.*, v. 6, 1960, pp. 137–144.

9. OSKAR PERRON, *Die Lehre von den Kettenbrüchen*, 2nd ed., Chelsea, New York, 1950.

10. R. J. SCHOOF, "Quadratic fields and factorization," *Computational Methods in Number Theory* (H. W. Lenstra, Jr. and R. Tijdemann, eds.), Math. Centrum Tracts, Number 155, Part II, Amsterdam, 1983, pp. 235–286.

11. D. SHANKS, *Class Number, A Theory of Factorization and Genera*, Proc. Sympos. Pure Math., vol. 20 (1969 Institute on Number Theory), Amer. Math. Soc., Providence, R. I., 1971, pp. 415–440.

12. D. SHANKS, *The Infrastructure of a Real Quadratic Field and Its Applications*, Proc. 1972 Number Theory Conference, Boulder, 1972, pp. 217–224.

13. R. SOLENG, "A computer investigation of units in quadratic number fields," unpublished manuscript.

14. H. C. WILLIAMS, "A numerical investigation into the length of the period of the continued fraction expansion of $\sqrt{D}$," *Math. Comp.*, v. 34, 1981, pp. 593–601.

15. H. C. WILLIAMS & M. C. WUNDERLICH, "On the parallel generation of the residues for the continued fraction factoring algorithm," *Math. Comp.*, v. 48, 1987, pp. 405–423.