MATHEMATICS OF COMPUTATION
Volume 70, Number 235, Pages 1311–1328
S 0025-5718(00)01234-5
Article electronically published on March 15, 2000

COMPUTER VERIFICATION OF THE ANKENY–ARTIN–CHOWLA CONJECTURE FOR ALL PRIMES LESS THAN 100 000 000 000

A. J. VAN DER POORTEN, H. J. J. TE RIELE, AND H. C. WILLIAMS

ABSTRACT. Let p be a prime congruent to 1 modulo 4, and let t, u be rational integers such that $(t + u\sqrt{p})/2$ is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$. The Ankeny-Artin-Chowla conjecture (AAC conjecture) asserts that p will not divide u. This is equivalent to the assertion that p will not divide $B_{(p-1)/2}$, where B_n denotes the nth Bernoulli number. Although first published in 1952, this conjecture still remains unproved today. Indeed, it appears to be most difficult to prove. Even testing the conjecture can be quite challenging because of the size of the numbers t, u; for example, when $p = 40\,094\,470\,441$, then both t and u exceed $10^{330\,000}$. In 1988 the AAC conjecture was verified by computer for all $p < 10^9$. In this paper we describe a new technique for testing the AAC conjecture and we provide some results of a computer run of the method for all primes p up to 10^{11}.

1. INTRODUCTION

Let p denote a prime such that $p \equiv 1 \pmod 4$ and let $\varepsilon = (t + u\sqrt{p})/2$ (> 1) be the fundamental unit in the real quadratic number field $\mathbb{Q}(\sqrt{p})$. In 1952 Ankeny, Artin and Chowla [2] asked whether $p \nmid u$ always and noted that $p \nmid u$ for $p < 2000$ $(p \equiv 5 \pmod 8)$. This question was written in the form of a conjecture by Mordell [15], and has since become known as the Ankeny-Artin-Chowla conjecture (AAC conjecture). The conjecture is equivalent to stating that $p \nmid u$ if t, u are the least positive integers such that

$$t^2 - pu^2 = \pm 4.$$

It arose ultimately from expressions which were derived in [2] for the value of hu/t modulo p, where h is the class number of $\mathbb{Q}(\sqrt{p})$. One of these results is

$$hu/t \equiv B_{(p-1)/2} \pmod p, \tag{1.1}$$

where B_n here denotes the nth Bernoulli number. Mordell [15] noted that this was proved only for $p \equiv 5 \pmod 8$ in [2]; it was later established for all $p \equiv 1 \pmod 4$ by Ankeny and Chowla [4]. However, this result had been proved earlier (1948) by Kiselev [12]. Ankeny and Chowla [3] also noted that $h < p$; hence, $p | u$ if and only if $p | B_{(p-1)/2}$, a fact also noted earlier by Kiselev [12] and Carlitz [7].

Received by the editor March 22, 1999 and, in revised form, July 6, 1999.
2000 *Mathematics Subject Classification.* Primary 11A55, 11J70, 11Y40, 11Y65, 11R11.
Key words and phrases. Periodic continued fraction, function field.
The first author was supported in part by a grant from the Australian Research Council.
The research of the third author was supported by NSERC Canada grant #A7649.

TABLE 1.1. Verification of AACC for all $p < L$.

L	Investigator(s)	Date	Machine
2 000	Ankeny, Artin, Chowla $p \equiv 5 \pmod 8$ only [2]	1952	—
100 000	Goldberg [16]	1954	SEAC
6 270 714	Beach, Williams, Zarnke [6]	1971	IBM 360-65
100 028 010	Soleng [20]	1986	Cyber 171
1 000 000 000	Stephens, Williams [21]	1988	Amdahl 5850

Ankeny, Artin and Chowla [1] also announced that

$$2hu/t \equiv (A+B)/p, \tag{1.2}$$

where

$$A = \prod_{0<r<p} r, \qquad B = \prod_{0<n<p} n,$$

and $\left(\frac{r}{p}\right) = 1$, $\left(\frac{n}{p}\right) = -1$. This was proved later by Carlitz [7]. Unfortunately, there does not seem to be any fast method of verifying the AAC conjecture for a given p by making use of either (1.1) or (1.2). The work of Fillebrown [9] suggests that computing Bernoulli numbers is very expensive, and there is no method known currently for computing $A+B \pmod{p^2}$. Indeed, $AB = (p-1)!$ and it has only recently been possible to compute the values of the Wilson quotients $w_p = \big((p-1)!+1\big)/p$ up to 5×10^8 (see Crandall, Dilcher and Pomerance [8]). In fact, in all previous attempts to verify the AAC conjecture for all primes $< L$, the value of u was computed modulo p. We summarize this work in Table 1.1.

Ankeny, Artin and Chowla did not provide any algebraic justification that would suggest a negative response to their question. Perhaps the conjecture is true because of considerations that seem far from our understanding; however, one might ask whether the data so far collected really should be persuasive in making one believe in this conjecture. It is certainly a most tempting conjecture to test, particularly if one subscribes to the familiar "log log argument". This reasoning is based on the seemingly reasonable assumptions that the probability that $p|u$ is $1/p$ and that trials for different p values are independent events. It then follows that we might expect that the number of exceptions to the conjecture in the interval $[x, y]$ is given by

$$\sum_{\substack{x \le p \le y \\ p \equiv 1 \pmod 4}} \frac{1}{p} \approx \tfrac{1}{2} \log\big(\log y / \log x\big) = N(x, y).$$

For $x = 5, y = 10^9$, we get $N(x, y) = 1.28$ and for $x = 5, y = 10^{11}$, we get only a small increase in $N(x, y)$ to 1.37. Thus, even if the AAC conjecture is false, one is not entirely surprised that there are no counterexamples up to 10^9. This also makes the AAC conjecture a most tempting conjecture to test, since it seems that there might be an exception to it within a range that modern computers would have the capability to search.

The purpose of this paper is to present a new algorithm for verifying the AAC conjecture for a given prime p. We will also describe the implementation and

running of this algorithm on two fast computers. Our computer runs allowed us to verify the AAC conjecture for all primes between 10^9 and 10^{11}; hence, we now know that the conjecture holds for all $p < 10^{11}$.

The strategy employed in devising our algorithm is based on the following simple observation. If

$$\varepsilon^k = (X + Y\sqrt{p})/2 = (X_k + Y_k\sqrt{p})/2 \qquad (X_1 = t, Y_1 = u)$$

and $p \nmid k$, then $p|u$ if and only if $p|Y$. This is very easy to see on expanding the kth power of $(t + u\sqrt{p})/2$ by the binomial theorem and noting that

$$2^{k-1}Y \equiv kt^{k-1}u \pmod{p}.$$

We estimate a value of $\log_2 \varepsilon^k$ for some k such that $p \nmid k$ and use the infrastructure ideas of Shanks [18] to determine a value of $\eta \in \mathbb{Z}$ such that $p|Y$ if and only if $p|\eta$. To determine this estimate we make use of the analytic class number formula

$$2hR = \sqrt{p}\, L(1, \chi_p), \tag{1.3}$$

where R $(= \log \varepsilon)$ is the regulator of $\mathbb{K} = \mathbb{Q}(\sqrt{p})$ and $L(1, \chi_p)$ is the Dirichlet L-function for $\mathbb{K}$ evaluated at $s = 1$. We also note that $h < \sqrt{p}$ (see, for example, Slavutskii [19]).

Thus, our intention, then, is to compute quickly an estimate E for $\log_2 \varepsilon^k$ and use this to determine whether or not p divides Y, as above. The value of ε^k for any k could, of course, be determined from the continued fraction expansion of $\left(1 + \sqrt{p}\right)/2$. However, *a priori*, one would have to compute so many terms of the continued fraction that the running time would be prohibitive. Instead, with knowledge of E, we can use Shanks' "infrastructure" to greatly accelerate our search through the continued fraction to determine an accurate value of $\log_2 \varepsilon^k$. Since we need only determine Y mod p, we don't need to compute the integers X and Y, which will usually be unmanageably enormous. Thus, we determine a number η mod p, such that p divides Y if and only if p divides η. Given an accurate value of $\log_2 \varepsilon^k$, we can compute η via the infrastructure of the principal ideal class of $\mathbb{Q}\left(\sqrt{p}\right)$. Thus, our overall algorithm is made up of three components.

1. Find an estimate E of hR_2, where $R_2 = \log_2 \varepsilon$, by estimating $L(1, \chi_p)$ and using (1.3).
2. Use E to determine an integral multiple kR_2 of R_2 and check that $kR_2 < 8p$. This value of k will likely be h, but whether it is or not, our estimate is probably sufficiently good that k is not very different from h $(< \sqrt{p})$. Thus, it is most likely that $p \nmid k$. Since $R_2 = \log_2 \varepsilon \geq \log_2\left(\sqrt{p-4} + \sqrt{p}\right) > 8$ for the values of p in our search range, our check that $kR_2 < 8p$ ensures that $p \nmid k$.
3. Compute $\eta = \eta(kR)$ and verify that $\eta \neq 0$.

2. Estimation of hR_2

It is well known that we can write $L(1, \chi_p)$ in its Euler product form as

$$L(1, \chi_p) = \prod_q \left(1 - \chi_p(q)/q\right)^{-1},$$

where the product is taken over all the primes q and the character $\chi_p(q)$ is the same as the Kronecker symbol (p/q). Bach [5] has developed a technique for estimating

$\log L(1, \chi_p)$ which has been found to be very effective in practice (see §2 of Jacobson, Lukes and Williams [11]). For some suitable T, we compute

$$C(T) = \sum_{i=0}^{T-1} (T+i) \log(T+i)$$

and

$$a_j = (T+j)\log(T+j)/C(T) \qquad (j = 0, 1, 2, \ldots, T-1).$$

By Theorem 9.2 of [5], we have (under the Extended Riemann Hypothesis for $L(s, \chi_p)$)

$$\left| \log L(1, \chi_p) - \sum_{i=0}^{T-1} a_i \log B(T+i) \right| < A(T, p),$$

where

$$\begin{aligned} B(x) &= \prod_{q<x} (1 - \chi_p(q)/q)^{-1}, \\ A(T,p) &= \frac{A \log p + B}{\sqrt{T} \log T}, \end{aligned}$$

and A, B here are constants which are explicitly given in Table 3 of [5]. The important item to note here is that $A(T,p)$ will be quite small for even modest values of T because $\log p$ will not be large compared to $\sqrt{T}$.

Let

$$S(T,p) = \sum_{i=0}^{T-1} a_i \log B(T+i).$$

As pointed out in [11], we can write this as

$$S(T,p) = \sum_{q<2T-1} w(q) \log\left[q/(q-(p/q))\right],$$

where

$$w(q) = \begin{cases} 1, & \text{when} \quad q < T, \\ \sum_{j=q-T+1}^{T-1} a_j, & \text{when} \quad T \le q < 2T-1. \end{cases}$$

Since we will need to evaluate $S(T,p)$ for many values of p, it is convenient to precompute and store in a large table the quadratic residues and nonresidues of p together with the values of $w(q)\ \log[q/(q+1)]$, and $w(q)\ \log[q/(q-1)]$, for all the primes $q < 2T-1$. It is then a simple matter to compute $S(T,p)$ by doing only table look-ups and additions. Our estimate E for hR_2 is then computed as

$$E = \frac{\sqrt{p}}{\log 4} \exp(S(T,p)).$$

It should be emphasized here that this method for finding E usually provides a much better result than what Bach's estimate for the error suggests. Also, although on average the error decreases with increasing T, in many cases the error for small T (say $T = 100$) is comparable to the error for larger T (say $T = 5000$). We illustrate these remarks in Table 2.1.

TABLE 2.1. Some experiments with Bach's method to estimate hR_2.

	T	E	E/R_2
$p = 9\,999\,999\,241$	100	374 191.1	0.9914
$R_2 = 377\,424.5$	200	377 174.2	0.9993
	500	382 290.3	1.0129
	1 000	377 796.8	1.0010
	2 000	375 368.2	0.9946
	5 000	377 872.1	1.0012
$p = 9\,999\,999\,253$	100	152 887.6	3.0043
$R_2 = 50\,890.1$	200	155 708.1	3.0597
	500	154 600.0	3.0379
	1 000	154 297.7	3.0320
	2 000	153 518.1	3.0167
	5 000	152 657.5	2.9997
$p = 9\,999\,994\,117$	100	268 436.8	26.8469
$R_2 = 9\,998.8$	200	268 043.1	26.8075
	500	271 177.0	27.1210
	1 000	271 498.3	27.1531
	2 000	271 266.8	27.1299
	5 000	270 060.7	27.0093

We next need to know how to use E to find kR_2. For this we will require some results concerning continued fractions and their relationship to the ideals in the ring $\mathcal{O}_{\mathbb{K}}$ of algebraic integers in $\mathbb{K} = \mathbb{Q}(\sqrt{p})$.

3. CONTINUED FRACTIONS AND IDEALS

In this section we will briefly review some well-known results concerning the ideals of $\mathcal{O}_{\mathbb{K}}$ and continued fractions. For proofs of these results we refer the reader to Stephens and Williams [21], Mollin [14] or Williams and Wunderlich [22].

By $\langle a_0, a_1, a_2, \ldots, a_n, \ldots \rangle$ we denote the simple continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \quad a_n + \cfrac{1}{\ddots}}}}$$

The *partial quotients* $a_i \geq 1$ $(i \geq 0)$ and the *convergents* $C_n = \langle a_0, a_1, a_2, \ldots, a_n \rangle$ are given by $C_n = A_n/B_n$, where $A_{-2} = 0, B_{-2} = 1$, $A_{-1} = 1$, $B_{-1} = 0$ and

$$A_{i+1} = a_{i+1}A_i + A_{i-1},$$
$$B_{i+1} = a_{i+1}B_i + B_{i-1} \qquad (i = -1, 0, 1, \ldots).$$

Note that $B_0 = 1, B_1 = a_1$ and $B_i \geq 1$ for $i \geq 0$. Also

$$A_nB_{n-1} - B_nA_{n-1} = (-1)^{n+1}. \tag{3.1}$$

Let $P, Q, D \in \mathbb{Z}$ such that $D > 0$, $\sqrt{D} \notin \mathbb{Q}$ and $Q \mid D - P^2$. The continued fraction of $\phi = \phi_0 = (P + \sqrt{D})/Q$ is given by

$$\phi = \langle a_0, a_1, a_2, \ldots, a_{n-1}, \phi_n \rangle.$$

The partial quotients are determined by making use of the formulas

$$\begin{aligned} P_{i+1} &= a_i Q_i - P_i, \\ Q_{i+1} &= (D - P_{i+1}^2)/Q_i = Q_{i-1} - a_i (P_{i+1} - P_i), \\ a_{i+1} &= \lfloor (P_{i+1} + d)/Q_{i+1} \rfloor = \lfloor (P_{i+1} + \sqrt{D})/Q_{i+1} \rfloor, \end{aligned}$$

where $d = \lfloor \sqrt{D} \rfloor, P_0 = P, Q_0 = Q, a_0 = \lfloor \phi_0 \rfloor$. Also,

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

Note that

$$\phi_{i+1} = \frac{1}{\phi_i - a_i}; \tag{3.2}$$

hence, $\phi_i > 1$ when $i > 0$. At some point in the computation of the continued fraction of ϕ, we must find some ϕ_k such that[1] $\overline{\phi}_k < 0$; furthermore, this value of k will be $O(\log |Q|/\sqrt{D})$.

If we put $\theta_1 = 1$ and define

$$\theta_k^{-1} = \prod_{i=1}^{k-1} \phi_i \qquad (k > 1),$$

then

$$\theta_i = (-1)^{i-1} (A_{i-2} - \phi B_{i-2}) \tag{3.3}$$

and

$$\theta_i \overline{\theta}_i = (-1)^{i-1} Q_{i-1}/Q_0. \tag{3.4}$$

We also put $\Psi_1 = 1$ and define

$$\Psi_k = \prod_{i=1}^{k-1} \psi_i \qquad (k > 1),$$

where

$$\psi_i = |(\overline{\phi}_i)^{-1}| = \left| (P_i + \sqrt{D})/Q_{i-1} \right|; \tag{3.5}$$

hence,

$$\Psi_i = |\overline{\theta}_i| = |A_{i-2} - \overline{\phi} B_{i-2}|. \tag{3.6}$$

Since

$$\phi = \frac{\phi_{i-1} A_{i-2} + A_{i-3}}{\phi_{i-1} B_{i-2} + B_{i-3}} \qquad (i \geq 1),$$

we get

$$A_{i-2} - \overline{\phi} B_{i-2} = \frac{A_{i-2} B_{i-3} - A_{i-3} B_{i-2}}{\overline{\phi}_{i-1} B_{i-2} + B_{i-3}};$$

thus, by (3.1) and (3.4) we get

$$\Psi_i = 1/|\overline{\phi}_{i-1} B_{i-2} + B_{i-3}|. \tag{3.7}$$

[1]Here, as is customary, we use $\overline{\alpha}$ to denote the conjugate of α in $\mathbb{K}$.

Let $[\alpha, \beta]$ denote the module $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$. If D is squarefree and if we put $\omega = (1+\sqrt{D})/2$ when $D \equiv 1 \pmod 4$ or $\omega = \sqrt{D}$ otherwise, then the maximal order $\mathcal{O}_{\mathbb{K}}$ (ring of algebraic integers of $\mathbb{K}$) is given by $\mathcal{O}_{\mathbb{K}} = [1, \omega]$. Any ideal of $\mathcal{O}_{\mathbb{K}}$ can be written as $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, where $L(\mathfrak{a})$ is the least positive rational integer in $\mathfrak{a}$, $\beta = b + c\omega$ $(b, c \in \mathbb{Z})$, and $c \big| b$, $c \big| L(\mathfrak{a})$, $L(\mathfrak{a}) \big| \beta\overline{\beta}$. If $c = 1$, we say that $\mathfrak{a}$ is *primitive*. A primitive ideal is said to be *reduced* if $L(\mathfrak{a})$ is a minimum in $\mathfrak{a}$; that is, there does not exist any nonzero $\alpha \in \mathfrak{a}$ such that $|\alpha| < L(\mathfrak{a})$ and $|\overline{\alpha}| < L(\mathfrak{a})$.

Theorem 3.1. *An ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{K}}$ is reduced if and only if there exists some $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, where $\beta > L(\mathfrak{a})$ and $-L(\mathfrak{a}) < \overline{\beta} < 0$.*

If $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, we define $\overline{\mathfrak{a}}$ to be the ideal $[L(\mathfrak{a}), \overline{\beta}]$.

Theorem 3.2. *If $\mathfrak{a}$ is a reduced ideal of $\mathcal{O}_{\mathbb{K}}$, then so is $\overline{\mathfrak{a}}$.*

Proof. Let $\mathfrak{a} = [L(\mathfrak{a}), \beta]$. If $\overline{\mathfrak{a}}$ is not reduced, there must exist some $\alpha \in \overline{\mathfrak{a}}$ such that $|\alpha| < L(\mathfrak{a})$ and $|\overline{\alpha}| < L(\mathfrak{a})$. But since $\overline{\alpha} \in \mathfrak{a}$ and $\mathfrak{a}$ is reduced, this is impossible. □

By our previous observations it is easy to see that any primitive ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{K}}$ can be put in the form $[Q/r, (P + \sqrt{D})/r]$ where $Q, P \in \mathbb{Z}$, $r = 2$ if $D \equiv 1 \pmod 4$ or $r = 1$ otherwise. Furthermore, $Q \big| D - P^2$. Hence we can expand $(P + \sqrt{D})/Q$ into a continued fraction and produce a sequence of ideals

$$\mathfrak{a}_1 (= \mathfrak{a}), \mathfrak{a}_2, \mathfrak{a}_3, \dots, \tag{3.8}$$

where

$$\mathfrak{a}_i = [Q_{i-1}/r, (P_{i-1} + \sqrt{D})/r].$$

All of these ideals lie in the same equivalence class. Indeed,

$$(Q_0\theta_i)\mathfrak{a}_i = (Q_{i-1})\mathfrak{a}_1.$$

Thus, by (3.6) and (3.4) we get

$$(Q_0)\mathfrak{a}_i = (Q_0\Psi_i)\mathfrak{a}_1. \tag{3.9}$$

We are now able to mention some useful theorems.

Theorem 3.3. *If $\mathfrak{a}_k$ is reduced, then $L(\mathfrak{a}_k) < 2\sqrt{D}/r$.*

Theorem 3.4. *If $L(\mathfrak{a}_k) < \sqrt{D}/r$, then $\mathfrak{a}_k$ is reduced.*

Theorem 3.5. *If $\overline{\phi}_k < 0$, then $\mathfrak{a}_{k+1}$ is reduced.*

If we begin the sequence (3.8) with an ideal $\mathfrak{a}$, such as $\mathcal{O}_{\mathbb{K}}$ itself, which is already reduced, then the sequence is completely periodic and is made up exclusively of the reduced ideals that are equivalent to $\mathfrak{a}$. If, moreover, l is the least positive integer such that $\mathfrak{a}_1 = \mathfrak{a}_{l+1}$, then it is readily shown that for any positive integer k

$$\epsilon^k = \Psi_{lk+1}.$$

Furthermore, when $\mathfrak{a} = \overline{\mathfrak{a}}$ ($\mathfrak{a}$ is an *ambiguous* ideal), there is a symmetry property, namely $\overline{\mathfrak{a}}_{l-i+1} = \mathfrak{a}_{i+1}$, by which we are able to compute ϵ by looking only halfway through the cycle $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_l$.

Theorem 3.6. *If $\mathfrak{a}_1 = \mathfrak{a}$ is reduced and ambiguous, there must exist a least positive integer s such that either $P_s = P_{s+1}$ or $Q_s = Q_{s+1}$. If $P_s = P_{s+1}$, then $l = 2s$ and*

$$\epsilon = \Psi_{s+1}/|\overline{\Psi}_{s+1}| = Q_0\Psi_{s+1}^2/Q_s.$$

If $Q_s = Q_{s+1}$, *then* $l = 2s + 1$,

$$\epsilon = \Psi_{s+2}/|\overline{\Psi}_{s+1}| = Q_0\Psi_{s+1}\Psi_{s+2}/Q_s, \tag{3.10}$$

and

$$R_2 = \log_2 \epsilon = \log_2(Q_0\psi_{s+1}/Q_s) + 2\sum_{i=1}^{s} \log_2 \psi_i. \tag{3.11}$$

4. Some results concerning ideals and continued fractions

In order to develop our algorithms, we will need some further results concerning ideals and continued fractions. We first require a simple lemma.

Lemma 4.1. *If* $k > 1$ *and* $\overline{\phi}_k < 0$, *then* $0 < Q_k < 2\sqrt{D}$, $|P_k| < \sqrt{D}$ *and* $Q_{k-1} > 0$. *If* $-1 < \overline{\phi}_k < 0$, *then* $P_k > 0$.

Proof. Since $\phi_k > 1$, we have $\phi_k - \overline{\phi}_k = 2\sqrt{D}/Q_k > 1$; hence, $0 < Q_k < 2\sqrt{D}$. Since $P_k + \sqrt{D} > Q_k > 0$ and $P_k - \sqrt{D} < 0$, we must also have $|P_k| < \sqrt{D}$. Since $Q_kQ_{k-1} = D - P_k^2$, we get $Q_{k-1} > 0$. Finally, since $2P_k/Q_k = \phi_k + \overline{\phi}_k$, we see that $P_k > 0$ when $\overline{\phi}_k > -1$. □

Our next result and its converse provide us with a simple criterion for determining when $\mathfrak{a}_k$ is reduced.

Theorem 4.2. *If* $k \geq 1$, $Q_{k-1} > 0$ *and* $\mathfrak{a}_k$ *is reduced, then* $-1 < \overline{\phi}_k < 0$ *and* $\psi_k > 1$.

Proof. We know that $L(\mathfrak{a}_k) = Q_{k-1}/r$ and, by Theorem 3.3, that $L(\mathfrak{a}_k) < 2\sqrt{D}/r$ when $\mathfrak{a}_k$ is reduced. Hence, $0 < Q_{k-1} < 2\sqrt{D}$. Put

$$\gamma = L(\mathfrak{a}_k)\phi_k^{-1} = (\sqrt{D} - P_k)/r = (-a_{k-1}Q_{k-1} + P_{k-1} + \sqrt{D})/r \in \mathfrak{a}_k\,.$$

Since $\phi_k > 1$, we get $0 < \gamma < L(\mathfrak{a}_k)$ which means that $0 < \sqrt{D} - P_k < Q_{k-1} < 2\sqrt{D}$; consequently, $P_k + \sqrt{D} > 0$ and $Q_k > 0$. Since $\mathfrak{a}_k$ is reduced, we must have $|\overline{\gamma}| > L(\mathfrak{a}_k)$. It follows that $|\overline{\phi}_k| < 1$. Also, since $D - P_k^2 = Q_kQ_{k-1} > 0$, we have $|P_k| < \sqrt{D}$ and $\overline{\phi}_k < 0$. □

Theorem 4.3. *If* $-1 < \phi_k < 0$ $(k \geq 1)$, *then* $Q_{k-1} > 0$ *and* $\mathfrak{a}_k$ *is reduced.*

Proof. By (3.2) we have

$$\overline{\phi}_k = \frac{1}{\overline{\phi}_{k-1} - a_{k-1}};$$

hence, we must have $\overline{\phi}_{k-1} - a_{k-1} < -1$. Thus

$$a_{k-1} - \overline{\phi}_{k-1} = a_{k-1} + (\sqrt{D} - P_{k-1})/Q_{k-1} > 1.$$

Now $Q_{k-1} > 0$ by Lemma 4.1 and $\overline{\mathfrak{a}}_k = [Q_{k-1}/r, (P_{k-1} - \sqrt{D})/r] = [L(\mathfrak{a}_k), \beta]$, where $L(\mathfrak{a}_k) = Q_{k-1}/r$ and $\beta = a_{k-1}Q_{k-1}/r + (\sqrt{D} - P_{k-1})/r > L(\mathfrak{a}_k)$. Note further that

$$\overline{\beta} = a_{k-1}Q_{k-1}/r - (\sqrt{D} + P_{k-1})/r \quad \text{and} \quad a_{k-1} = \lfloor (P_{k-1} + \sqrt{D})/Q_{k-1} \rfloor;$$

hence, $-L(\mathfrak{a}_k) < \overline{\beta} < 0$. By Theorem 3.2 we know that $\overline{\mathfrak{a}}_k$ is reduced, and by Theorem 3.1 we know that $\mathfrak{a}_k$ is reduced. □

We next suppose that

$$\mathfrak{a} = [Q/r, (P + \sqrt{D})/r],$$

where $Q > 0$ and $0 < P < Q$. Notice that any ideal of $\mathcal{O}_{\mathbb{K}}$ must have such a representation.

Theorem 4.4. *If k (> 0) is the least integer such that $\overline{\phi}_k < 0$, then $\Psi_i \leq 1$ for $1 \leq i \leq k$.*

Proof. The theorem is certainly true if $i = 1$. If $k \geq i = 2$, then $\Psi_i = \psi_1 = |P_1 + \sqrt{D}|/Q_0$. Since $\overline{\phi}_1 > 0$, we cannot have $\mathfrak{a}_1$ reduced by Theorem 4.2; hence, by Theorem 3.4 we must have $Q_0 > \sqrt{D}$, and therefore $0 \leq a_0 \leq 1$. If $a_0 > 0$, then $P_1 = -P_0$ and $\psi_1 = |-P_0 + \sqrt{D}|/Q_0$. In this case $0 < \sqrt{D}/Q_0 < 1$ and $-1 < -P_0/Q_0 < 0$; hence, $\psi_1 < 1$. If $a_0 = 1$, then $P_1 = Q_0 - P_0$ and $P_1 + \sqrt{D} = Q_0 - P_0 + \sqrt{D} > 0$. If $P_0 > \sqrt{D}$, then $0 < (P_1 + \sqrt{D})/Q_0 < 1$; if $P_0 < \sqrt{D}$, then $\overline{\phi}_0 < 0$, which by Theorem 3.5 means that $\mathfrak{a}_1$ must be reduced, a contradiction. If $k \geq i \geq 3$, then we have $\overline{\phi}_{i-1} > 0$, $B_{i-2} > 1$, $B_{i-3} \geq 1$; hence, by (3.7) we get $\Psi_i < 1$. □

Corollary 4.5. *If, in the sequence of ideals* (3.8), *$\mathfrak{a}_i$ is not reduced, then $\Psi_i \leq 1$.*

Proof. Since $\mathfrak{a}_i$ is not reduced, we must have $\overline{\phi}_{i-1} > 0$ by Theorem 3.5. Thus, $k > i - 1$ or $i \leq k$. □

Corollary 4.6. *If, in the sequence* (3.8), *$\mathfrak{a}_i$ is the first reduced ideal, then $\Psi_i \leq 1$.*

Proof. Since $\mathfrak{a}_i$ is reduced, we must have $i \leq k + 1$ by Theorem 3.5. If $i \leq k$, the result follows from the theorem. Suppose $i = k + 1$. If $\overline{\phi}_k < -1$, then $|\psi_k| < 1$ and $\Psi_i = |\psi_k|\Psi_k < 1$; if $-1 < \overline{\phi}_k < 0$, then $\mathfrak{a}_k$ is a reduced ideal by Theorem 4.3, contradicting the definition of $\mathfrak{a}_i$. □

In developing the algorithms that follow, it is essential to be able to perform baby-steps (the process of moving through the sequence (3.8) one step at a time) and giant-steps (the process of moving through the sequence (3.8) by taking several baby-steps at once). In what follows we will describe a simple procedure for taking baby-steps, and in the next section we will show how to take giant steps. We will assume that $\mathfrak{a}_1$ is reduced.

We define $\zeta_j = \zeta(\mathfrak{a}_j)$ and $\rho_j = \rho(\mathfrak{a}_j)$ by

$$2^{\zeta_j - 1} < \Psi_j < 2^{\zeta_j}, \quad \rho_j = 2^{\zeta_j}/\Psi_j.$$

We now have the following baby-step algorithm.

Algorithm 4.7. Given $\mathfrak{a}_j$, ζ_j, ρ_j; compute $\mathfrak{a}_{j+1}$, ζ_{j+1}, ρ_{j+1}.

1. $\mathfrak{a}_{j+1} = [Q_j/r, (P_j + \sqrt{D})/r]$, $\chi_j = (\sqrt{D} - P_j)/Q_j$.
2. Put $\rho \leftarrow \rho_j \chi_j$, $\zeta \leftarrow \zeta_j$.
3. **while** $\rho < 1$
   $\rho \leftarrow 2\rho$
   $\zeta \leftarrow \zeta + 1$
   end while
4. $\rho_{j+1} \leftarrow \rho$, $\zeta_{j+1} \leftarrow \zeta$.

Note that the process of determining Q_j, P_j $(\mathfrak{a}_{j+1})$ from Q_{j-1}, P_{j-1} $(\mathfrak{a}_j)$ is given in §3.

Proof (of correctness of Algorithm 4.7). We have $\rho = 2^k \rho_j \chi_j$ and $\zeta = \zeta_j + k$ for some $k \geq 0$.

If $k = 0$, then $\rho_j \chi_j \geq 1$. Note that $\chi_j = \psi_j^{-1}$; hence, we get $2^{\zeta_j}/\Psi_{j+1} \geq 1$. Since all of the ideals in (3.8) are reduced, we must have $-1 < \overline{\phi}_k < 0$, $\psi_j > 1$ and $0 < \chi_j < 1$. It follows that $\Psi_{j+1} > \Psi_j > 2^{\zeta_j - 1}$ and $2^{\zeta_j - 1} < \Psi_{j+1} \leq 2^{\zeta_j}$; therefore, $\zeta_{j+1} = \zeta_j$ and $\rho_{j+1} = \rho_j \chi_j$.

If $k > 0$, then

$$2^{\zeta_j + k}/\Psi_{j+1} \geq 1 \quad \text{and} \quad 2^{\zeta_j + k - 1}/\Psi_{j+1} < 1.$$

Thus, $\zeta_{j+1} = \zeta_j + k = \zeta$, $\rho_{j+1} = 2^k \rho_j \chi_j = \rho$. □

In order to take giant-steps, it will be useful to have the following definition.

Definition 4.8. Let $\mathfrak{a}$ be any reduced ideal and let x (≥ 0) be a real number. We define $\mathfrak{a}(x)$ to be that reduced ideal in the sequence (3.8) such that $\Psi_j \leq 2^x$ and $\Psi_{j+1} > 2^x$. We also define $\rho(x) = 2^x/\Psi_j$.

Note that $1 \leq \rho(x) < \psi_j < 2\sqrt{D}/r$, and

$$1 \leq L(\mathfrak{a}(x))\rho(x) < (P_j + \sqrt{D})/r < 2\sqrt{D}/r\,,$$

by Lemma 4.1 and (3.5).

We conclude this section with a minor technical lemma.

Lemma 4.9. *If* $\mathfrak{a}_1 = \mathcal{O}_{\mathbb{K}} = [1, \omega]$, *then* $\psi_1 > 2$ *when* $D > 9$.

Proof. By (3.5), $\psi_1 = (P_1 + \sqrt{D})/Q_0 = a_0 + (\sqrt{D} - P_0)/Q_0$ and $a_0 = \lfloor \omega \rfloor$, $P_0 = r - 1$, $Q_0 = r$. It follows that $\psi_1 \geq \lfloor (\sqrt{D} + 1)/2 \rfloor + (\sqrt{D} - 1)/2 > 2$ when $D > 9$. □

Corollary 4.10. *If* $D > 9$, $\mathfrak{a}_1 = \mathcal{O}_{\mathbb{K}}$ *and* $0 \leq y \leq 1$, *then* $\mathfrak{a}(y) = \mathfrak{a}_1$.

Proof. In this case, $\Psi_2 = \psi_1 > 2$; hence $\Psi_2 > 2^y$ and $\mathfrak{a}(y) = \mathfrak{a}_1$. □

5. The infrastructure and some algorithms

Let $\mathfrak{b}_1 = \mathcal{O}_{\mathbb{K}} = [1, \omega]$ and consider the sequence of ideals $\mathfrak{b}_i$, $i = 1, 2, 3, \ldots$, generated by the associated continued fraction algorithm. By (3.9) we can write these ideals as $\mathfrak{b}_i = (\Psi_i')$, where the Ψ_i' values are strictly increasing with increasing i. We define the *distance* δ_i from $\mathfrak{b}_1$ to $\mathfrak{b}_i$ by $\delta_i = \log_2 \Psi_i'$. Now consider the product $\mathfrak{b}_i \mathfrak{b}_j$ of two ideals in the sequence. Both $\mathfrak{b}_i$ and $\mathfrak{b}_j$ are reduced, but $\mathfrak{b}_i \mathfrak{b}_j$ need not be. We can write $\mathfrak{b}_i \mathfrak{b}_j = (u)\mathfrak{a}_1$, where $\mathfrak{a}_1$ is primitive and $u \in \mathbb{Z}$ but $\mathfrak{a}_1$ may need to be reduced by applying the continued fraction algorithm to it until we find a reduced ideal $\mathfrak{a}_k = (\Psi_k)\mathfrak{a}_1 = (\Psi_k \Psi_i' \Psi_j'/u)$. Since $\mathfrak{b}_1$ is principal, we know that $\mathfrak{b}_i, \mathfrak{b}_j$ are principal and that therefore $\mathfrak{b}_i \mathfrak{b}_j$ is principal. Thus $\mathfrak{a}_k$ is a reduced principal ideal, which means that $\mathfrak{a}_k = \mathfrak{b}_m$ for some m. Furthermore,

$$\delta_m = \log_2(\Psi_k \Psi_i' \Psi_j'/u) = \delta_i + \delta_j + \delta,$$

where $\delta = \log_2(\Psi_k/u)$. It can be shown that $\delta = O(\log D)$ and is, as a consequence, not very large; thus we expect that

$$\delta_m \approx \delta_i + \delta_j.$$

From this we see that the reduced ideals in the principal class are organized by the continued fraction algorithm into a very specific order. This organization was called the "infrastructure" of the class by Shanks, the discoverer of this phenomenon.

Thus, we can find a reduced principal ideal of distance x from $\mathfrak{b}_1 = [1, \omega]$ by performing about x/δ_s multiply-reduction steps, using an ideal $\mathfrak{b}_s$ as a multiplier, instead of the roughly $x/1.186569$ (Lévy's law, see [14, pp. 243–244]) baby-steps that would likely be required. This is the process of taking giant-steps (of size δ_s). We will now show how this idea can be used in the development of some algorithms.

Algorithm 5.1. Given $\mathfrak{b}(x)$, $\mathfrak{b}(y)$, $\rho(x)$, $\rho(y)$; compute $\mathfrak{b}(x+y)$, $\rho(x+y)$.

1. Compute $(u)\mathfrak{a}_1 = \mathfrak{b}(x)\mathfrak{b}(y)$ (say by using the technique described in §3 of [21]). Put $\rho_1 = u\rho(x)\rho(y)$.
2. $\mathfrak{a}_1 := [Q_0/r, (P_0 + \sqrt{D})/2]$, $a_0 = \lfloor (P_0 + d)/Q_0 \rfloor$, $i \leftarrow 1$.
3. **while** $\rho_i \geq 1$
   $P_i = a_{i-1}Q_{i-1} - P_{i-1}$
   $Q_i = (D - P_i^2)/Q_{i-1}$
   $a_i = \lfloor (P_i + d)/Q_i \rfloor$
   $\rho_{i+1} = \rho_i |(\sqrt{D} - P_i)/Q_i|$
   $i \leftarrow i + 1$
   end while
4. $\mathfrak{b}(x+y) = \mathfrak{a}_{i-1} = [Q_{i-2}/r, (P_{i-2} + \sqrt{D})/r]$, $\rho(x+y) = \rho_{i-1}$.

Proof (of correctness of Algorithm 5.1). We have $\mathfrak{b}_s = \mathfrak{b}(x)$, $\mathfrak{b}_t = \mathfrak{b}(y)$ for some s, t, and $\rho_i = \rho_1/\Psi_i$. Put $j = i - 1$ for the value of i produced after the execution of step 3. We must have $\rho_{j+1} < 1$ and $\mathfrak{a}_j = (\Psi_j \Psi_s' \Psi_t'/u)$. Let k be the least positive integer such that $\mathfrak{a}_k$ is reduced.

Case 1. $(j < k)$. Here $j + 1 \leq k$ and $\mathfrak{a}_j$ is not reduced; hence, by Corollary 4.5 we have $\Psi_j \leq 1$. If $\mathfrak{a}_{j+1}$ is reduced, then $j + 1 = k$ and $\Psi_{j+1} \leq 1$ by Corollary 4.6. If $\mathfrak{a}_{j+1}$ is not reduced, then we also have $\Psi_{j+1} \leq 1$. Thus, $\Psi_j \leq \rho_1$ and $\Psi_{j+1} \leq \rho_1$, a contradiction.

Case 2. $(j \geq k)$. In this case $\mathfrak{a}_j$ is reduced and $\mathfrak{a}_j = \mathfrak{b}_m$, where $\Psi_m' = \Psi_j \Psi_s' \Psi_t'/u$ and $\Psi_{m+1}' = \Psi_{j+1} \Psi_s' \Psi_t'/u$. It follows that

$$\Psi_m' \leq 2^{x+y}, \quad \Psi_{m+1}' > 2^{x+y};$$

hence $\mathfrak{a}_j = \mathfrak{b}_m = \mathfrak{b}(x+y)$. Also, $\rho(x+y) = 2^{x+y}/\Psi_m' = \rho_1/\Psi_j = \rho_j$. □

Algorithm 5.2. $(D > 9)$ Given some real $x \geq 1$, compute $\mathfrak{b}(x)$, $\rho(x)$.

1. Put $j = \lceil \log_2 x \rceil$, $y = x/2^j$.
2. Put $\mathfrak{b}(y) = \mathfrak{b}_1$, $\rho(y) = 2^y$.
3. **for m = 1 to j**
   $\mathfrak{b}(y) \leftarrow \mathfrak{b}(2y)$
   $\rho(y) \leftarrow \rho(2y)$
   $y \leftarrow 2y$
   end for
4. $\mathfrak{b}(x) \leftarrow \mathfrak{b}(y)$, $\rho(x) \leftarrow \rho(y)$.

Proof (of correctness of Algorithm 5.2). Since $0 < y \leq 1$, we know by Corollary 4.10 that $\mathfrak{b}(y) = \mathfrak{b}_1$. Let $v = x/2^j$. Since $x = 2^j v$, we see that in step 4 we have $\mathfrak{b}(y) = \mathfrak{b}(2^j v) = \mathfrak{b}(x)$, $\rho(y) = \rho(2^j v) = \rho(x)$. □

We will now show how to incorporate Algorithms 4.7, 5.1, and 5.2 into an algorithm which determines an integral multiple of R_2. We first need the following definition.

Definition 5.3. If $\mathfrak{a}_1$ is any principal ideal of $\mathcal{O}_{\mathbb{K}}$ and $(Q_0)\mathfrak{a}_i = (Q_0\Psi_i)\mathfrak{a}_1$ as in (3.9), we define $\delta(\mathfrak{a}_i, \mathfrak{a}_1) = \log_2 \Psi_i$. If $\mathfrak{a}_1 = \mathcal{O}_{\mathbb{K}}$, we write $\delta(\mathfrak{a}_i)$ for $\delta(\mathfrak{a}_i, \mathfrak{a}_1)$.

Note that $\delta(\mathfrak{b}(x)) = x - \log_2 \rho(x)$. Also, it is easy to see that $\overline{\mathfrak{b}}_j \mathfrak{b}_j = (L(\mathfrak{b}_j))$; hence,

$$\overline{\Psi}_j \Psi_j = L(\mathfrak{b}_j)\theta,$$

where θ is some positive unit of $\mathbb{K}$. It follows that

$$\delta(\overline{\mathfrak{b}}_j) = -\delta(\mathfrak{b}_j) + tR_2 + \log_2 L(\mathfrak{b}_j), \tag{5.1}$$

where $t \in \mathbb{Z}$. If, for reals a, b, c with $c \neq 0$, we say that $a \equiv b \pmod{c}$ whenever $(a-b)/c \in \mathbb{Z}$, we can write (5.1) as

$$\delta(\overline{\mathfrak{b}}_j) \equiv -\delta(\mathfrak{b}_j) + \log_2 L(\mathfrak{b}_j) \pmod{R_2}. \tag{5.2}$$

Furthermore, since $\delta(\mathfrak{b}_i)$ is a strictly increasing function of i, we observe that if $\delta(\mathfrak{b}_k) \equiv \delta(\mathfrak{b}_j) + u \pmod{R_2}$ $(k \geq j)$ and $0 \leq u \leq \delta(\mathfrak{b}_t, \mathfrak{b}_j)$, then $\mathfrak{b}_k \in \{\mathfrak{b}_j, \mathfrak{b}_{j+1}, \ldots, \mathfrak{b}_t\}$.

Now let θ be any positive unit of $\mathbb{K}$ such that

$$|\log_2 \theta - E| < K.$$

Then $\log_2 \theta = E - V$ with $|V| < K$ and

$$E \equiv V \pmod{R_2}.$$

We are now able to present our algorithm for determining an integral multiple of R_2.

Algorithm 5.4. Find an integral multiple of R_2 from an estimate E.

1. Select (by trial) some parameter c with $c > B = \lceil \log_2(2\sqrt{D}/r) \rceil$.
2. Compute $\mathfrak{a}_1 = \mathfrak{b}(E)$ and $\rho(E)$ (Algorithm 5.2). Compute the set of ideals $S = \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_t\}$ together with their associated ρ and ζ values (Algorithm 4.7) until $\zeta_i > c + B$.
3. Compute the ideals $\mathfrak{b}(c), \mathfrak{b}(2c), \ldots$ and associated $\rho(c), \rho(2c), \ldots$ (Algorithms 4.7 and 5.1) until either $\mathfrak{b}(ic) \in S$ or $\overline{\mathfrak{b}}(ic) \in S$.
   (a) If $\mathfrak{b}(ic) \in S$, then
   $$kR = E - ic + \zeta_j + \log_2 \left(\rho(ic)/\rho_j \rho(E)\right),$$
   when $\mathfrak{b}(ic) = \mathfrak{a}_j$.
   (b) If $\overline{\mathfrak{b}}(ic) \in S$, then
   $$kR = E + ic + \zeta_j - \log_2 \left(L(\mathfrak{b}(ic))\rho(ic)\rho_j \rho(E)\right),$$
   when $\overline{\mathfrak{b}}(ic) = \mathfrak{a}_j$.

Proof (of correctness of Algorithm 5.4). Put $m = \lfloor K/c \rfloor + 2$.

Case 1. $(V - \log_2 \rho(E) + B > 0)$. In this case we put $i = \lceil (V - \log_2 \rho(E) + B)/c \rceil$. Then

$$V - \log_2 \rho(E) + B = ic - f \ (0 \leq f < c)$$

and

$$ic = V - \log_2 \rho(E) + B + f < V + B + c < K + 2c.$$

It follows that $i \leq m$. Now

$$\begin{aligned}\delta(\mathfrak{b}(ic)) - \delta(\mathfrak{a}_1) &= ic - \log_2 \rho(ic) - E + \log_2 \rho(E) \\ &\equiv ic - \log_2 \rho(ic) - V + \log_2 \rho(E) \\ &= f + B - \log_2 \rho(ic) \pmod{R_2}.\end{aligned}$$

Since $\log_2 \rho(ic) < B$, we have $f + B - \log_2 \rho(ic) > 0$ and $f + B - \log_2 \rho(ic) < c + B$. Thus, we must have $\mathfrak{b}(ic) \in S$. If $\mathfrak{b}(ic) = a_j$, then

$$\delta(\mathfrak{b}(ic)) \equiv \delta(\mathfrak{a}_1, \mathfrak{a}_j) + \delta(\mathfrak{b}(E)) \pmod{R_2}.$$

From this we get

$$ic - \log_2 \rho(ic) \equiv E - \log_2(\rho(E)) + \zeta_j - \log_2 \rho_j \pmod{R_2}.$$

Case 2. $(V - \log_2 \rho(E) + B \leq 0)$. If we put $i = \lfloor |V - \log_2 \rho(E)|/c \rfloor$, then

$$-V + \log_2 \rho(E) = ic + f \qquad (0 \leq f < c),$$

and since $ic + f < K + B$, we see that $i \leq m - 1$. Furthermore, by (5.2)

$$\begin{aligned}\delta(\overline{\mathfrak{b}}(ic)) - \delta(\mathfrak{a}_1) &\equiv -ic + \log_2(L(\mathfrak{b}(ic))\rho(ic)) - E + \log_2 \rho(E) \\ &\equiv f + \log_2(L(\mathfrak{b}(ic))\rho(ic)) \pmod{R_2}.\end{aligned}$$

Since $0 < f + \log_2(L(\mathfrak{b}(ic))\rho(ic)) < c + B$, we must have $\overline{\mathfrak{b}}(ic) \in S$. If $\mathfrak{a}_j = \overline{\mathfrak{b}}(ic)$, then by (5.2)

$$\delta(\mathfrak{a}_1, \mathfrak{a}_j) + \delta(\mathfrak{b}(E)) \equiv -\delta(\mathfrak{b}(ic)) + \log_2(L(\mathfrak{b}(ic))) \pmod{R_2}.$$

Thus, $kR_2 = E + ic + \zeta_j - \log_2 (L(\mathfrak{b}(ic))\rho(ic)\rho_j\rho(E))$. □

6. The algorithm for determining η

There remains the problem of determining whether or not $p \mid Y$. Let $\mathfrak{b}(x) = \mathfrak{b}_j = (\Psi_j')$, where

$$\Psi_j' = (W_j + Z_j\sqrt{D})/2$$

and $W_j, Z_j \in \mathbb{Z}$. If $(W_j, D) = 1$, we define a pair $(\xi(x), \eta(x))$ by:

1. $\xi(x)$, $\eta(x) \in \mathbb{Z}$;
2. $0 \leq \xi(x)$, $\eta(x) < D$;
3. $\xi(x)$, $\eta(x)$ not both zero;
4. $Z_j\xi(x) \equiv W_j\eta(x) \pmod{D}$.

Note that any particular pair $(\xi(x), \eta(x))$ for a given Ψ_j' is not unique. For if (ξ, η) is any pair satisfying properties 1–4 above, then so does (ξ_1, η_1), where $\xi_1 \equiv a\xi, \eta_1 \equiv a\eta \pmod{D}$ and $(a, D) = 1$. Also, if D is a prime p (> 4), then $(D, W_j) = (p, W_j) = 1$. For if $p \mid W_j$, we must have $p \mid Q_{j-1}'$ by (3.6) and (3.4), which, since $0 < Q_{j-1}' < 2\sqrt{p}$ (Lemma 4.1), is impossible for $p > 4$. Finally, if D is a prime p, then $p \mid Z_1$ if and only if $\eta(x) = 0$. For if $\eta(x) = 0$, then $p \mid Z_1\xi(x)$. Since $p \nmid \xi(x)$ by property 3, we must have $p \mid Z_1$. On the other hand, if $p \mid Z_1$, then $p \mid W_j\eta(x)$ and we have already seen that $p \nmid W_j$.

For $\mathfrak{b}(x)$ above, we have $\mathfrak{b}(2x) = \Psi_m'$, where

$$\Psi_m' = \Psi_i(\Psi_j')^2/u$$

and $\mathfrak{a}_i = (\Psi_i)$ is reduced. Now by (3.6) we have $\Psi_i = (G + \sqrt{D}B)/Q_0$, where

$$G = G_{i-2} = Q_0 A_{i-2} - P_0 B_{i-2} = P_{i-1} B_{i-2} + Q_{i-1} B_{i-3}$$

(by (2.11) of [22]). Hence, we get

$$4Q_0 \Psi_m' \equiv GW_j^2 + (2GW_j Z_j + BZ_j^2)\sqrt{D} \pmod{D}.$$

Putting $\xi \equiv \xi(x)G \pmod{D}$, $\eta \equiv 2\eta(x)G + \xi(x)B \pmod{D}$ we see that

$$GW_j^2 \eta - (2GW_j Z_j + BZ_j^2)\xi \equiv 2G^2 W_j(\eta(x)W_j - \xi(x)Z_j) \equiv 0 \pmod{D}.$$

Since $Q_0 = (Q_{j-1}')^2/(ru)$, we see that $(Q_0, D) = 1$ when $D = p$. Also, if $D = p$ and $\xi \equiv \eta \equiv 0 \pmod{p}$, then $p \mid \xi(x)G$. If $p \mid G$, then $p \mid Q_{i-1}Q_0$ by (3.6) and (3.4). Since $p \nmid Q_0$, we must have $p \mid Q_{i-1}$. But since $\mathfrak{a}_i$ is reduced, we must have $0 < Q_{i-1} < 2\sqrt{p}$ which means that $p \nmid G$. If $p \mid \xi(x)$, then $p \mid \eta$ implies that $p \mid \eta(x)$, which contradicts property 3. From these observations, we see that we may put

$$\xi(2x) \equiv \xi(x)G \pmod{p},$$
$$\eta(2x) \equiv 2\eta(x)G + B\xi(x) \pmod{p},$$

when $D = p$.

Algorithm 6.1. Given $D = p > 9$ and $x = kR_2$, compute $\mathfrak{b}(x)$, $\xi(x)$, $\eta(x)$.

1. Put $j = \lceil \log_2 x \rceil, y = x/2^j$ $(0 \le y < 1)$.
2. Put $\mathfrak{b}(y) = \mathfrak{b}_1$, $\rho(y) = 2^y$, $\xi(y) = 1$, $\eta(y) = 0$.
3. **for** $m = 1$ **to** j
   - Compute $(u)\mathfrak{a}_1 = \mathfrak{b}^2(y)$, $\rho_1 = u\rho(y)^2$.
   - Put $\mathfrak{a}_1 = [Q_0/r, (P_0 + \sqrt{p})/r], B_{-1} = 0, B_{-2} = 1, i = 1$,
   - $a_0 = \lfloor (P_0 + \sqrt{p})/Q_0 \rfloor$.
   - **while** $\rho_i \ge 1$
     - $P_i = a_{i-1}Q_{i-1} - P_{i-1}, Q_i = (p - P_i^2)/Q_{i-1}$
     - $a_i = \lfloor (P_i + \sqrt{p})/Q_i \rfloor$
     - $B_{i-1} = a_{i-1}B_{i-2} + B_{i-3}$
     - $\rho_{i+1} = \rho_i |(\sqrt{p} - P_i)/Q_i|$
     - $i \leftarrow i + 1$
   - **end while**
   - $\mathfrak{b}(2y) = \mathfrak{a}_{i-1}$
   - $\rho(2y) = \rho_{i-1}$
   - $G \equiv P_{i-2}B_{i-3} + Q_{i-2}B_{i-4} \pmod{p}$
   - $\xi(2y) \equiv \xi(y)G \pmod{p}$
   - $\eta(2y) \equiv 2\eta(y)G + B_{i-3}\xi(y) \pmod{p}$
   - $y \leftarrow 2y$

   end for
4. $\mathfrak{b}(x) \leftarrow \mathfrak{b}(y), \xi(x) \leftarrow \xi(y), \eta(x) \leftarrow \eta(y)$

Note that if $x = kR_2$ where $k \in \mathbb{Z}^{>0}$, then $\mathfrak{b}(x) = \mathcal{O}_{\mathbb{K}}$ and $L(\mathfrak{b}(x)) = 1$.

7. Implementation and computational results

The complete algorithm for testing the AAC conjecture was implemented in Fortran 77 and tested and run on an SGI O_2 workstation and on one processor of an SGI Origin 2000 computer system at CWI in Amsterdam. Both of these machines support 64-bit arithmetic, which is particularly helpful in the third step

of the overall algorithm (Algorithm 6.1). The program executes about four times more quickly on the Origin 2000 than it does on the O_2.

A basic step in the computations is the continued fraction evaluation,

$$\begin{aligned} P_{i+1} &= a_i Q_i - P_i, \\ Q_{i+1} &= (p - P_{i+1}^2)/Q_i, \\ a_{i+1} &= \lfloor (P_i + \sqrt{p})/Q_i \rfloor, \end{aligned}$$

where it is known that $Q_i \big| (p - P_{i+1}^2)$. Special precautions were taken to guarantee the correctness of this routine, taking into consideration that p can be as large as 10^{11}, and using the relation $Q_{i+1} = Q_{i-1} - a_i(P_{i+1} - P_i)$. Furthermore, we made use of a computing trick of Head [10] to deal with integers that become as large as $p^2 \approx 10^{22}$ $(> 2^{64})$. This was very useful in the third phase of the procedure.

In view of the result of Lenstra [13], that computation of R can be done in about $p^{1/5}$ elementary operations, we put $c = p^{1/5}$ in Algorithm 5.4. Since baby-steps are much cheaper to compute than giant-steps, it was important to do some experimentation to find the best value for t in the set S of Algorithm 5.4. To this end, we introduced a parameter f and computed S until $\zeta_i > fp^{1/5}$. Since $p^{1/5} > 0.5 \log_2 p$ for $p > 10^9$, we have $\zeta_i > c + B$ when $f \geq 2$. Usually we used $f = 3$, but as p became larger, we occasionally used $f = 10$ and $f = 20$. We also experimented with the value for T. We found that for values of p up to about 6×10^{10}, a value of $T = 2000$ worked reasonably well, but beyond that point we used $T = 5000$. Thus our T, f pairs were usually $(2000, 3)$ or $(5000, 3)$, but when we failed to find a value for kR_2 for a modest value of i such that $\overline{\mathfrak{b}}(ic)$ or $\mathfrak{b}(ic) \in S$, we used a different parameter set. We usually bounded i in our program by 60. When this failed to produce a value for kR_2, we tried $T = 1000$, $f = 10$, i-bound $= 200$ or $T = 2000$, $f = 20$, i-bound $= 500$.

Of course, in running such a complex algorithm, it is essential to perform some checks to ensure that the program is performing properly. We have already mentioned the simple check that our value for kR_2 be less than $8p$, but we also always checked that $\mathfrak{b}(kR_2) = \mathfrak{b}_1 = [1, \omega]$ whenever we ran Algorithm 6.1. This was a very useful confirmation that our value for kR_2 is correct. It was also a very cheap check.

We less frequently carried out a more expensive check. From the continued fraction expansion of $(1 + \sqrt{p})/2$, we computed t, u modulo p and the value of R_2 by using (3.10) and (3.11). (When $D = p \equiv 1 \pmod 4$, we must always find some s such that $Q_s = Q_{s+1}$. See, for example, Perron [17, pp. 106–108]. The actual values of t and u can become enormous; for example, if $p = 40\,094\,470\,441$, then both t and u exceed $10^{330\,000}$.) We next divided this value of R_2 into our computed value of kR_2 to check that this is very close to an integer k. We then computed X_k and Y_k modulo p by putting $X_0 = 2$, $Y_0 = 0$, $X_1 \equiv t, Y_1 \equiv u \pmod p$ and using

$$\begin{aligned} X_{n+1} &= X_1 X_n + X_{n-1} \pmod p, \\ X_{n+1} &= X_1 Y_n + Y_{n-1} \pmod p. \end{aligned}$$

We checked that the computed values for $\xi(kR_2)$ and $\eta(kR_2)$ satisfied

$$\xi(kR_2) Y_k \equiv \eta(kR_2) X_k \pmod p.$$

As this check is very costly, we carried it out only for a small subset of the values p on which we ran our main program. This check was carried out successfully for every 100 000-th prime for which we verified the AAC conjecture.

In all our runs, we did not find a single counterexample of the conjecture; thus, we have confirmed the truth of the AAC conjecture for all primes between 10^9 and 10^{11}. Computing times on the O_2 and Origin 2000 were about 250 and 700 CPU hours, respectively. We used the O_2 to search the range 10^9–9×10^9 and the Origin to search the range 9×10^9–10^{11}.

8. A DETAILED EXAMPLE

We will now illustrate how our algorithm works by using a nontrivial numerical example with $p = 97\,843\,343\,893$. We put $T = 1000$ and obtain $S(T,p) = 1.475146$, $E = 986\,410.691$. We next put $c = p^{1/5} = 157.7997$, $f = 10$, and i-bound $= 200$. We find

$$\mathfrak{a}_1 = \mathfrak{b}(E) = [Q_0/2, (P_0 + \sqrt{p})/2]$$

with

$$P_0 = 295\,721, \quad Q_0 = 46\,766, \quad \rho(E) = 11.23627.$$

Furthermore, we compute $\mathfrak{a}_i$ for $i = 2, 3, \ldots, 941$ (ζ_{941} is the first $\zeta_i > fc = 1\,577.9973$):

i	P_{i-1}	Q_{i-1}	ζ_i	ρ_i
2	312 237	7 514	4	1.19714
3	311 425	114 162	11	1.84453
...				
926	312 243	13 426	1 551	1.35561
...				
939	81 187	23,294	1 576	1.30055
940	152 107	320 226	1 577	1.30525
941	168 119	217 282	1 578	1.73824

Next, we find $\mathfrak{b}(c) = [92\,354/2, (286\,825 + \sqrt{p})/2]$ and compute at most 199 more ideals $\mathfrak{b}(2c), \mathfrak{b}(3c), \ldots, \mathfrak{b}(200c)$ until $\mathfrak{b}(ic)$ or $\overline{\mathfrak{b}}(ic)$ is one of the previously determined $\mathfrak{a}_i$. We find

i	P'_{i-1}	Q'_{i-1}	$\rho(ic)$
1	286 825	92 354	2.24634
2	282 267	97 594	4.45638
...			
12	305 353	13 426	32.65983

and $\overline{\mathfrak{b}}(12c) = \mathfrak{a}_{926}$. That is $Q_{i-1} = Q'_{j-1}$ and $P_{i-1} \equiv -P'_{j-1} \pmod{Q_{i-1}}$ ($i = 926, j = 12$). We find, then, that

$$kR_2 = E + ic + \zeta_j - \log_2 (L(\mathfrak{b}(ic))\rho(ic)\rho_j\rho(E)) = 989\,833.617.$$

Next, we compute $\mathfrak{b}(kR_2)$, starting with $\mathfrak{b}(y) = \mathfrak{b}_1$, where $y = kR_2/2^{20} = 0.9439789$ and computing $\mathfrak{b}(2y), \mathfrak{b}(4y), \ldots, \mathfrak{b}(2^{20}y)$. We find that $\mathfrak{b}(kR_2) = [1, (312\,799 + \sqrt{p})/2] = [1, \omega]$. Together with computing $\mathfrak{b}(2^i y)$ we also compute $\xi(2^i y)$ and $\eta(2^i y)$, finding

$$\xi(kR_2) \equiv 73\,973\,607\,135 \pmod{p},$$
$$\eta(kR_2) \equiv 6\,870\,136\,643 \pmod{p}.$$

Since $\eta(kR_2) \not\equiv 0 \pmod{p}$, we have confirmed the AAC conjecture for $p = 97\,843\,343\,893$.

To run our expensive check we compute the continued fraction expansion of $\omega = (1 + \sqrt{p})/2$ until two consecutive Q values are equal. We find that $Q_s = Q_{s+1}$ for $s = 96\,929$. We also find $R_2 = 329\,944.539$, and on dividing this into kR_2 obtain $k = 3.00000\,0000$. Furthermore, we get $t \equiv 84\,779\,576\,991$, $u \equiv 38\,999\,918\,048 \pmod{p}$. We then compute $X_3 \equiv 13\,063\,766\,902 \pmod{p}$, $Y_3 \equiv 78\,686\,933\,642 \pmod{p}$, and finally verify that

$$\xi(kR_2)Y_3 \equiv \eta(kR_2)X_3 \pmod{p}.$$

References

[1] N. C. Ankeny, E. Artin and S. Chowla, The class number of real quadratic fields, *Proc. Nat. Acad. Sci. USA* **37** (1951), 524–525. MR **13:**212c

[2] N. C. Ankeny, E. Artin and S. Chowla, The class number of real quadratic fields, *Annals of Math.* **56** (1952), 479–493. MR **14:**251h

[3] N. C. Ankeny and S. Chowla, A note on the class number of real quadratic fields, *Acta Arith.* **6** (1960), 145–147. MR **22:**6780

[4] N. C. Ankeny and S. Chowla, A further note on the class number of real quadratic fields, *Acta Arith.* **7** (1962), 271–272. MR **25:**1147

[5] E. Bach, Improved approximations for Euler products, *Number Theory, CMS Conference Proceedings*, Vol. 15, AMS, 1995, 13–28. MR **96i:**11124

[6] B. D. Beach, H. C. Williams and C. R. Zarnke, Some computer results on units in quadratic and cubic fields, *Proc. 25th Summer Meeting Can. Math. Congress*, Lakehead University, 1971, 609–648. MR **49:**2656

[7] L. Carlitz, Note on the class number of real quadratic fields, *Proc. Amer. Math. Soc.* **4** (1953), 535–537. MR **15:**104g

[8] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449. MR **97c:**11004

[9] S. Fillebrown, Faster computation of Bernoulli numbers, *J. of Algorithms* 13(1992), 431–445.

[10] A. K. Head, Multiplication modulo n, *BIT* **20** (1980), 115–116. MR **94d:**68044

[11] M. J. Jacobson, R.F. Lukes and H.C. Williams, An investigation of the bounds for the regulator of quadratic fields, *Experimental Math.* **4** (1995), 211–225. MR **81g:**68001

[12] A. A. Kiselev, An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers, *Doklady Akad. Nauk SSSR (N.S.)* **61** (1948), 777–779. (Russian) MR **10:**236h

[13] H. W. Lenstra, Jr., On the calculation of regulators and class numbers of quadratic fields, *London Math. Soc. Lecture Note Series* **56** (1982), 123–150. MR **86g:**11080

[14] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996. MR **97e:**11135

[15] L. J. Mordell, On a Pellian equation conjecture, *Acta Arith.* **6** (1960), 137–144. MR **22:**9470

[16] L. J. Mordell, On a Pellian equation conjecture (II), *J. London Math. Soc.* **36** (1961), 282–288. MR **23:**A3707

[17] O. Perron, *Die Lehre von den Kettenbrüchen*, 2nd ed., Chelsea, New York, 1950. MR **12:**254b

[18] D. Shanks, The infrastructure of real quadratic number fields and its applications, *Proc. 1972 Number Theory Conf.*, Boulder Colorado, 1973, 217–224. MR **52:**10672

[19] I. S. Slavutskii, Upper bounds and numerical calculation of the number of ideal classes of real quadratic fields, *Amer. Math. Soc. Transl.* (2) **82** (1969), 67–71.

[20] R. Soleng, *A computer investigation of units in quadratic number fields*, Unpublished ms., 1986.
[21] A. J. Stephens and H. C. Williams, Some computational results on a problem concerning powerful numbers, *Math. Comp.* **50** (1988), 619–632. MR **89d:**11091
[22] H. C. Williams and M. C. Wunderlich, On the parallel generation of the residues for the continued fraction algorithm, *Math. Comp.* **48** (1987), 405–423. MR **88i:**11099

Centre for Number Theory Research, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: alf@math.mq.edu.au

CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
E-mail address: Herman.te.Riele@cwi.nl

Dept. of Computer Science, University of Manitoba, Winnipeg, Manitoba Canada R3T 2N2
E-mail address: williams@cs.umanitoba.ca