MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 405–423

On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm

By H. C. Williams* and M. C. Wunderlich

Dedicated to Daniel Shanks on the occasion of his 70th birthday

Abstract. In order to implement the continued fraction algorithm on a highly parallel computer, like the Massively Parallel Processor, it is necessary to be able to compute certain numbers which occur at widely-spaced intervals within the continued fraction expansion of $\sqrt{N}$, where N is the number to be factored. In this paper several properties of the continued fraction expansion of a quadratic irrational are developed. These results are then applied to the development of a very simple algorithm for finding the widely-spaced numbers referred to above.

1. Introduction. The continued fraction algorithm (CFRAC) [8], [11] is a general factoring method which has received a great deal of attention in recent years. If we denote by N the integer which we wish to factor, the CFRAC algorithm is one of a class of factoring techniques which determine integers X and Y such that

$$X^2 \equiv Y^2 \pmod{N}.$$

If $1 < \gcd(X - Y, N) < N$, then we have a factor of N; if not, then we must generate another (X, Y) pair and try again.

One way to calculate a pair (X, Y) is to first generate sequences $\{Z(i)\}$ and $\{Q(i)\}$ such that

$$Z(i)^2 \equiv Q(i) \pmod{N}.$$

If we can find a set $\mathcal{Q} = \{Q(i_1), Q(i_2), Q(i_3), \ldots, Q(i_t)\}$ such that

$$\prod_{j=1}^{t} Q(i_j) = Y^2, \tag{1.1}$$

where Y is an integer, then we have

$$X^2 \equiv Y^2 \pmod{N},$$

where

$$X \equiv \prod_{j=1}^{t} Z(i_j) \pmod{N}.$$

Received March 18, 1986.
1980 *Mathematics Subject Classification.* Primary 12A25, 10A32, 10A25.
* Research supported by NSERC of Canada Grant A7649 and the I. W. Killam Programme.

Leaving aside for the moment the problem of producing the sequences $\{Z(i)\}$ and $\{Q(i)\}$, we are left with the problem of determining a set $\mathscr{Q}$. To do this, we can first establish a *factor base* $\mathscr{P} = \{p_0, p_1, p_2, \ldots, p_k\}$, where $p_0 = -1$ and p_i $(i = 1, 2, 3, \ldots, k)$ are distinct primes. We then trial divide the Q's by the elements of $\mathscr{P}$ and consider only those which completely factor over $\mathscr{P}$; that is, those $Q(i)$'s such that

$$Q(i) = \prod_{j=0}^{k} p_j^{\alpha_{ij}}.$$

We associate with such a $Q(i)$ a binary vector $e_i = (a_{i0}, a_{i1}, \ldots, a_{ik})$, where $a_{ij} \equiv \alpha_{ij} \pmod 2$. Clearly, we can use as a set $\mathscr{Q}$ a set of $Q(i)$'s which corresponds to a set of linearly dependent (over GF(2)) e_i vectors. Both the continued fraction algorithm and the quadratic sieve (QS) [10], [3] are examples of this type of factoring method. They differ only in how the residues are computed and how they are factored.

In the case of CFRAC we make use of some properties of the continued fraction expansion of quadratic irrationals $\phi = (P + \sqrt{D})/Q$, where $P, Q, D \in \mathscr{Z}$ (the rational integers) and D is positive and not a perfect square. If we put** $\phi_0 = \phi$, $q_i = [\phi_i]$, $\phi_{i+1} = 1/(\phi_i - q_i)$, $i = 0, 1, 2, 3, \ldots, m$, we get

$$\begin{aligned}\phi &= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots\, q_m + \cfrac{1}{\phi_{m+1}}}}} \\ &= \langle q_0, q_1, \ldots, q_m, \phi_{m+1} \rangle.\end{aligned}$$

If we let $C_m = \langle q_0, q_1, q_2, \ldots, q_m \rangle$, then it is well known that $C_m = A_m/B_m$, where we compute A_m and B_m by the recurrence formulas

$$(1.2) \quad A_{r+1} = q_{r+1}A_r + A_{r-1}, \qquad B_{r+1} = q_{r+1}B_r + B_{r-1} \qquad (r = -1, 0, 1, 2, \ldots),$$

together with the boundary conditions $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$.

In the case of $P = 0$, $Q = 1$, we know that $\phi_r = (P_r + \sqrt{D})/Q_r$ $(P_r, Q_r \in \mathscr{Z})$,

$$(1.3) \qquad 0 < Q_r < 2\sqrt{D},$$

and

$$(1.4) \qquad A_{r-1}^2 - DB_{r-1}^2 = (-1)^r Q_r.$$

If we put $D = N$, we see by (1.4) that

$$A_{r-1}^2 \equiv (-1)^r Q_r \pmod N,$$

and (1.3) suggests that the quadratic residues $(-1)^r Q_r$ might be small enough to be factored over a small prime base. Thus we can put

$$Z(r) = A_{r-1}, \qquad Q(r) = (-1)^r Q_r.$$

** We use the symbol $[x]$ to denote that integer such that $x - 1 < [x] \leqslant x$.

The second author has been attempting an implementation of the continued fraction algorithm on the Massively Parallel Processor (MPP) built by Goodyear Aerospace at Goddard Space Flight Center. This computer consists of 16,384 processors in which arithmetic operations can be performed simultaneously on different data. Since the operation of attempting to factor the quadratic residues consumes most of the computer time in this algorithm, an obvious way to exploit the parallel architecture of the MPP is to perform the trial divisions in parallel. A batch of 16,384 different quadratic residues can be computed and they can be factored simultaneously by dividing by successive primes in the prime base. This procedure succeeds in dramatically reducing the computer time necessary to factor the Q's but we still have the problem of generating the Q's and their corresponding squares A^2. It was originally believed that the host computer to the MPP, a VAX 11-780, could serially compute the $((-1)^k Q_k, A_{k-1})$ pairs rapidly enough for the MPP to factor them in parallel; however, recent timings indicate that the host computer would not adequately keep up with the MPP for values of N much in excess of 60 decimal digits. Daniel Shanks has suggested that by extending the ideas described in [13], it should be possible to develop a procedure for generating the successive values of Q and A themselves in parallel, thereby removing the need for a fast serial host computer in implementing a parallel version of CFRAC. In this paper we explain how this can be done.

2. Some Results Concerning Continued Fractions. In order to solve the main problem of this paper, we shall require a number of results concerning the continued fraction expansion of an expression of the form $(P + \sqrt{D})/Q$, where $P, Q, D \in \mathscr{Z}$ and D (> 0) is not a perfect square. Most of these results are well known and are presented here for the convenience of the reader. For a more detailed discussion of this material the reader is referred to Perron [9] or Chrystal [1].

We assume with no loss of generality that $Q \mid D - P^2$ (if not, simply replace Q by $Q|Q|$, P by $|Q|P$ and D by Q^2D). If we put $d = [\sqrt{D}]$, $P_0 = P$, $Q_0 = Q$, $q_0 = [\phi_0]$, $\phi = \phi_0 = (P_0 + \sqrt{D})/Q_0$, then $\phi_m = (P_m + \sqrt{D})/Q_m$, where P_m and Q_m may be computed by using the formulas

$$\begin{aligned} P_{k+1} &= q_k Q_k - P_k, \\ Q_{k+1} &= \left(D - P_{k+1}^2\right)/Q_k, \qquad k = 0, 1, 2, 3, \ldots. \\ q_{k+1} &= \left[(P_{k+1} + d)/Q_{k+1}\right], \end{aligned} \tag{2.1}$$

If we put $Q_{-1} = (D - P_0^2)/Q_0$, $R_0 = P_0 + d - q_0 Q_0$, it is a simple matter to show that we can generate $\{Q_{n+1}, Q_n, P_{n+1}, q_{n+1}, R_{n+1}, A_{n+1} \pmod D, A_n \pmod D\}$ from $\{Q_n, Q_{n-1}, P_n, q_n, R_n, A_n \pmod D, A_{n-1} \pmod D\}$ by using Tenner's algorithm [4, p. 372]. We will call this algorithm

ALGORITHM 1. (*Single-Step Algorithm*)

$$\begin{aligned} P_{n+1} &= d - R_n, \\ Q_{n+1} &= Q_{n-1} - q_n(P_{n+1} - P_n), \\ q_{n+1} &= [(P_{n+1} + d)/Q_{n+1}], \\ R_{n+1} &= P_{n+1} + d - q_{n+1}Q_{n+1} \\ &= \text{remainder on dividing } P_{n+1} + d \text{ by } Q_{n+1}, \\ A_{n+1} &\equiv q_{n+1}A_n + A_{n-1} \pmod D. \end{aligned}$$

We exemplify this procedure for $D = 103$, $P = 0$, $Q = 1$ in Table 1 below.

TABLE 1

j	P_j	Q_j	q_j	R_j	A_j
−2	—	—	—	—	0
−1	—	103	—	0	1
0	0	1	10	2	10
1	10	3	6	2	61
2	8	13	1	5	71
3	5	6	2	3	100
4	7	9	1	8	68
5	2	11	1	1	65
6	9	2	9	1	35
7	9	11	1	8	100
8	2	9	1	3	32
9	7	6	2	5	61
10	5	13	1	2	93
11	8	3	6	0	1
12	10	1	20	0	10
13	10	3	6	2	61

Now since $\phi_{m+1} = 1/(\phi_m - [\phi_m])$, we have $\phi_n > 1$ for $n \geqslant 1$. Thus, we see that $q_n \geqslant 1$ for $n \geqslant 1$, and from (1.2), $B_n \geqslant F_{n+1}$ $(n \geqslant 0)$. Here F_k is the kth Fibonacci number ($F_0 = 0$, $F_1 = 1$). Since

$$F_{k+2} \geqslant \tau^k \qquad (\tau = (1 + \sqrt{5})/2),$$

we have

$$B_k \geqslant \tau^{k-1}. \tag{2.2}$$

We also note that

$$A_n B_{n-1} - B_n A_{n-1} = (-1)^{n-1} \qquad (n = -1, 0, 1, 2, \ldots). \tag{2.3}$$

Now

$$\phi = \phi_0 = \frac{\phi_m A_{m-1} + A_{m-2}}{\phi_m B_{m-1} + B_{m-2}}; \tag{2.4}$$

hence,

$$\phi_m = \frac{A_{m-2} - \phi B_{m-2}}{\phi B_{m-1} - A_{m-1}}. \tag{2.5}$$

Replacing m by $m + 1$, putting $\phi_0 = (P_0 + \sqrt{D})/Q_0$, $\phi_{m+1} = (P_{m+1} + \sqrt{D})/Q_{m+1}$ in (2.5), and equating rational and irrational parts, we get

$$G_m = P_{m+1} B_m + Q_{m+1} B_{m-1}, \qquad D B_m = P_{m+1} G_m + Q_{m+1} G_{m-1}, \tag{2.6}$$

where $G_m = Q_0 A_m - P_0 B_m$.

Put $\psi_m = (\sqrt{D} - P_m)/Q_{m-1} = 1/\phi_m$. We have $0 < \psi_m < 1$. Define

$$\theta_1 = 1, \qquad \theta_k = \prod_{i=1}^{k-1} \psi_i \qquad (k > 1). \tag{2.7}$$

Let $Q(\sqrt{D})$ denote the quadratic field formed by adjoining $\sqrt{D}$ to the rationals Q. Let $\bar{\alpha}$ denote the conjugate of $\alpha \in Q(\sqrt{D})$ and $N(\alpha) = \alpha\bar{\alpha}$. We now give a generalization of (1.4) in

THEOREM 2.1. *For θ_k defined as above, we have*

$$N(\theta_k) = (-1)^{k-1} Q_{k-1}/Q_0 \tag{2.8}$$

and

$$\theta_k = (-1)^{k-1}(A_{k-2} - \phi B_{k-2}). \tag{2.9}$$

Proof. (2.8) follows easily from (2.7) and (2.1); (2.9) can be easily deduced by using induction on k and (2.5). □

In much of what follows we shall be concerned with the problem of when $\bar{\phi}_m < 0$. We first give

THEOREM 2.2. *For $m \geqslant 1$, we have $\bar{\phi}_m < 0$ if and only if $P_m < \sqrt{D}$ and $Q_m > 0$.*

Proof. Clearly, $\bar{\phi}_m = (P_m - \sqrt{D})/Q_m < 0$ when $P_m < \sqrt{D}$ and $Q_m > 0$. If $\bar{\phi}_m < 0$, then since $\phi_m > 1$, we have $2\sqrt{D}/Q_m = \phi_m - \bar{\phi}_m > 0$. Hence $Q_m > 0$ and $P_m < \sqrt{D}$. □

Note also that since $\phi_m > 1$, we have $P_m > Q_m - \sqrt{D} > -\sqrt{D}$; thus, if $\bar{\phi}_m < 0$, then $|P_m| < \sqrt{D}$ and $Q_m < P_m + \sqrt{D} < 2\sqrt{D}$. Note further that if $\bar{\phi}_m < 0$, then $\bar{\phi}_{m+1} = 1/(\bar{\phi}_m - [\phi_m]) < 0$.

The question of whether $\bar{\phi}_m$ is ever negative is answered in

THEOREM 2.3. *If $|\phi_0 - \bar{\phi}_0| > 1/B_{m-1}B_{m-2}$ $(m \geqslant 2)$, then $\bar{\phi}_m < 0$.*

Proof. From (2.5) and (2.3) we get

$$\bar{\phi}_m = \left(-B_{m-2} + (-1)^m \rho_m B_{m-1}\right)/B_{m-1} \tag{2.10}$$

where $\rho_m = A_{m-1}/B_{m-1} - \bar{\phi}_0$. If we put $\varepsilon = |A_{m-1}/B_{m-1} - \phi_0|$, then it is well known that $A_{m-1}/B_{m-1} - \phi_0 = (-1)^m\varepsilon$ and $\varepsilon < 1/B_m B_{m-1}$; also,

$$(-1)^m \rho_m = (-1)^m\left(A_{m-1}/B_{m-1} - \phi_0 + \phi_0 - \bar{\phi}_0\right) = (-1)^m\left(\phi_0 - \bar{\phi}_0\right) + \varepsilon.$$

Now if $(-1)^m\rho_m < 0$, then $\bar{\phi}_m < 0$. Suppose $(-1)^m\rho_m > 0$. If $(-1)^m(\phi_0 - \bar{\phi}_0) < 0$, then

$$(-1)^m \rho_m < -1/B_{m-1}B_{m-2} + 1/B_{m-1}B_m < 0,$$

a contradiction. If $(-1)^m(\phi_0 - \bar{\phi}_0) > 0$, then $(-1)^m(\phi_0 - \bar{\phi}_0) > 1/B_{m-1}B_{m-2}$ and $(-1)^m\rho_m > 1/B_{m-1}B_{m-2}$. It follows from (2.10) that $\bar{\phi}_m < 0$. □

COROLLARY 2.3.1. *If $B_{m-2}^2 > |Q_0/2\sqrt{D}|$ $(m \geqslant 2)$, then $\bar{\phi}_m < 0$.*

Proof. We have $|\phi_0 - \bar{\phi}_0| = 2\sqrt{D}/|Q_0| > B_{m-2}^{-2} > 1/B_{m-2}B_{m-1}$. □

COROLLARY 2.3.2. *If $m > \max[1, 3 + \log(|Q_0|/2\sqrt{D})/(2\log\tau)]$, then $\bar{\phi}_m < 0$.*

Proof. If $m > 3 + \log(|Q_0|/2\sqrt{D})/(2\log\tau)$, then $\tau^{2(m-3)} > |Q_0|/2\sqrt{D}$ and by (2.2) we have $B_{m-2}^2 > |Q_0|/2\sqrt{D}$ and $m \geqslant 2$. □

Hence, we see that for some m $(\geqslant 0)$ we must eventually have $\bar{\phi}_m < 0$. By Theorem 2.2 we have $Q_m > 0$ and $|P_m| < \sqrt{D}$. If $Q_m > \sqrt{D}$, then $0 < Q_{m-1} = (D - P_m^2)/Q_m < \sqrt{D}$. In fact, we have

THEOREM 2.4. *Let t be the least integer $(\geqslant 0)$ such that $\bar{\phi}_t < 0$. If s is the least integer $(\geqslant 0)$ such that $0 < Q_s < \sqrt{D}$, then $t = s$ or $t = s + 1$, unless $(t, s) = (0, 1)$.*

Proof. If $t \geqslant 1$, then $0 < Q_t < \sqrt{D}$ or $0 < Q_{t-1} < \sqrt{D}$; hence, $s \leqslant t$. If $t = 0$, then $\bar{\phi}_1 < 0$ and $s = 0$ or 1. Now

$$q_s = \left(P_s + \sqrt{D}\right)/Q_s - \varepsilon \quad (0 < \varepsilon < 1) \quad \text{and} \quad 2\sqrt{D}/Q_s > 2 > 1 + \varepsilon;$$

hence, $q_s Q_s > P_s - \sqrt{D} + Q_s$. It follows that $P_{s+1} > -\sqrt{D} + Q_s$ and $-\bar{\psi}_{s+1} = -1/\bar{\phi}_{s+1} > 1$; thus, $\bar{\phi}_{s+1} < 0$ and $t \leqslant s + 1$. Thus, if $(t, s) \neq (0, 1)$, we have $t = s$ or $t = s + 1$. □

We close this section with

THEOREM 2.5. *If* $m \geqslant 3$, $\bar{\phi}_{m-1} > 0$, *then* $0 < \theta_m^{-1} < |Q_0/Q_{m-1}B_{m-3}|$.

Proof. If ρ_m is defined as in the proof of Theorem 2.3, we see by (2.9) that $\bar{\theta}_m = (-1)^{m-1}B_{m-2}\rho_{m-1}$. If $\bar{\phi}_{m-1} > 0$, then by (2.10) we have

$$-B_{m-3} + 1/\bar{\theta}_m > 0.$$

It follows that $0 < \bar{\theta}_m < 1/B_{m-3}$. By (2.8) we have $\theta_m\bar{\theta}_m = (-1)^{m-1}Q_{m-1}/Q_0$. By (2.7) we know that $\theta_m > 0$, and since $\theta_m^{-1} = |\theta_m^{-1}| = |Q_0/Q_{m-1}|\bar{\theta}_m$, the result follows. □

3. The Ideals in $\mathcal{O}_n$. Let D_0 be a square-free positive integer and put

$$r = \begin{cases} 1 & \text{when } D_0 \equiv 2 \text{ or } 3 \pmod 4, \\ 2 & \text{when } D_0 \equiv 1 \pmod 4. \end{cases}$$

Define $\omega_0 = (r - 1 + \sqrt{D_0})/r$, $\Delta_0 = (\omega_0 - \bar{\omega}_0)^2 = 4D_0/r^2$, $\omega = n\omega_0 + h$, where $n, h \in \mathcal{Z}$. Let $[\alpha, \beta]$ denote the module $\{xa + y\beta \mid xy \in \mathcal{Z}\}$ and note that $[\alpha, \beta] = [\gamma, \delta]$ if and only if

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = X\begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

where $X \in \mathrm{GL}_2(\mathcal{Z})$, the group of all 2×2 matrices with entries from $\mathcal{Z}$ and determinant ± 1.

Put $\mathcal{O}_n = [1, n\omega_0] = [1, \omega]$, $\Delta = (\omega - \bar{\omega})^2 = n^2\Delta_0$. For $g = \gcd(r, n)$, $\sigma = r/g$, put $D = (n/g)^2D_0$; then $\Delta = 4D/\sigma^2$. Of course, $\mathcal{O}_n$ is an integral domain and $\mathcal{O}_n \subseteq \mathcal{O}_1$, the set of all algebraic integers of $Q(\sqrt{D_0})$.

Now $\mathfrak{a}$ is an ideal in $\mathcal{O}_n$ if $\mathfrak{a} \subseteq \mathcal{O}_n$ and $\mathfrak{a}$ possesses the following properties:

(i) if $\alpha, \beta \in \mathfrak{a}$, then $\alpha + \beta \in \mathfrak{a}$,

(ii) if $\alpha \in \mathfrak{a}$ and $\eta \in \mathcal{O}_n$, then $\alpha\eta \in \mathfrak{a}$.

In this section we shall summarize several properties of the ideals in $\mathcal{O}_n$. Most of these can be found in any standard text, for example Cohn [2]. Those that are not explicitly in [2] can be easily demonstrated. Another useful source for some of this material is Ince [5].

THEOREM 3.1. *If* $\mathfrak{a}$ *is an ideal in* $\mathcal{O}_n$ *and* $\mathfrak{a} \not\subseteq \mathcal{Z}$, *then* $\mathfrak{a} = [a, b + c\omega]$, *where* $a, b, c \in \mathcal{Z}$, $a > 0$, $b > 0$, $c \mid b$ *and* $c \mid a$. □

COROLLARY 3.1.1. *For a given* $\mathfrak{a}$ *in* $\mathcal{O}_n$, *the integers a and c are unique. Indeed, a is the least positive rational integer in* $\mathfrak{a}$. □

We will denote the least positive rational integer of $\mathfrak{a}$ by $L(\mathfrak{a})$ and we will denote the value of $cL(\mathfrak{a})$ by $N(\mathfrak{a})$.

THEOREM 3.2. *Let* $\mathfrak{a} = [a, b + c\omega]$. $\mathfrak{a}$ *is an ideal in* $\mathcal{O}_n$ *if and only if* $c \mid a$, $c \mid b$. *and* $ac \mid N(b + c\omega)$. □

Definition. If $\mathfrak{a} = [a, b + \omega]$ and $a \mid N(b + \omega)$, we say that $\mathfrak{a}$ is a *primitive* ideal of $\mathcal{O}_n$. Note that if $\mathfrak{a}$ is primitive, then $N(\mathfrak{a}) = L(\mathfrak{a})$. If we denote by $(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m)$ the set

$$\mathfrak{a} = \left\{ \sum_{i=1}^{m} \eta_i \alpha_i \mid \eta_i \in \mathcal{O}_n,\ i = 1, 2, 3, \ldots, m \right\},$$

then clearly $\mathfrak{a}$ is an ideal in $\mathcal{O}_n$; indeed, we say that $\mathfrak{a}$ is the ideal *generated* by $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ and call $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ the *generators* of $\mathfrak{a}$. If $\mathfrak{a}$ $(= (\alpha))$ has a single generator, we say that $\mathfrak{a}$ is a *principal* ideal of $\mathcal{O}_n$. It is an easy matter to show that $(\alpha_1, \alpha_2) = [\alpha_1, \alpha_2]$; thus, any ideal of $\mathcal{O}_n$ need have at most two generators.

Definition. If $\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m)$, $\mathfrak{b} = (\beta_1, \beta_2, \beta_3, \ldots, \beta_k)$ are ideals of $\mathcal{O}_n$, we define the product ideal $\mathfrak{a}\mathfrak{b}$ to be that ideal generated by the mk generators $\alpha_i \beta_j$ $(i = 1, 2, 3, \ldots, m;\ j = 1, 2, 3, \ldots, k)$.

THEOREM 3.3. *Let $\alpha \in \mathcal{O}_n$ and let $\mathfrak{a}$ be any ideal in $\mathcal{O}_n$. If $\mathfrak{b} = (\alpha)\mathfrak{a}$, we have $N(\mathfrak{b}) = |N(\alpha)| N(\mathfrak{a})$.*

COROLLARY 3.3.1. *If $\mathfrak{a} = (\alpha)$, then $N(\mathfrak{a}) = |N(\alpha)|$.* □

If $\mathfrak{a} = [\alpha, \beta]$ is an ideal of $\mathcal{O}_n$ we call $\{\alpha, \beta\}$ an *integral basis* of $\mathfrak{a}$. We partially address the problem of finding an integral basis of the product of two ideals in

THEOREM 3.4. *If $\mathfrak{a}_1 = [a_1, b_1 + \omega]$ and $\mathfrak{a}_2 = [a_2, b_2 + \omega]$ are primitive ideals of $\mathcal{O}_n$ and $\gcd(a_1, a_2) = 1$, then $\mathfrak{a}_3 = \mathfrak{a}_1 \mathfrak{a}_2 = [a_3, b_3 + \omega]$, where $a_3 = a_1 a_2$ and*

$$b_3 \equiv \begin{cases} b_1 \pmod{a_1}, \\ b_2 \pmod{a_2}. \end{cases}$$ □

We can, of course, obtain a more general result than Theorem 3.4 (see, for example, Lenstra [6] or Schoof [12]), but this particular result will be adequate for the purposes of this paper.

The concept of a reduced ideal and the properties of such ideals will be very important in subsequent work. We first give the following

Definition. We say that $\mathfrak{a} = [L(\mathfrak{a}), \beta]$ is a *reduced* ideal in $\mathcal{O}_n$ if $\mathfrak{a}$ is primitive and there does not exist any nonzero $\alpha \in \mathfrak{a}$ such that both $|\alpha| < L(\mathfrak{a})$ and $|\bar{\alpha}| < L(\mathfrak{a})$ hold.

THEOREM 3.5. *$\mathfrak{a}$ is a reduced ideal in $\mathcal{O}_n$ if and only if there exists some $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, $\beta > L(\mathfrak{a})$, and $-L(\mathfrak{a}) < \bar{\beta} < 0$.*

Proof. Suppose $\mathfrak{a}$ is a reduced ideal in $\mathcal{O}_n$ and $\mathfrak{a} = [L(\mathfrak{a}), \gamma]$, where $\gamma = b + \omega$ $(b \in \mathscr{Z})$. There certainly exists an infinitude of pairs $(x, y) \in \mathscr{Z}^2$ such that

$$|xa + y\bar{\gamma}| < a,$$

where $a = L(\mathfrak{a})$. (For example, $x = [-y\bar{\gamma}/a]$, $y = 1, 2, 3, \ldots$.) Let (t, s) be one such pair and put $\upsilon = ta + s\gamma$; let β be that element of $\mathfrak{a}$ such that $|\bar{\beta}| < a$, $\beta > 0$ and β is least. Since there can only be a finite number of elements $\alpha \in \mathfrak{a}$ such that $|\alpha| < |\upsilon|$ and $|\bar{\alpha}| < a$, we see that β is well defined. Since $|\bar{\beta}| < a$ and $\mathfrak{a}$ is a reduced ideal of $\mathcal{O}_n$, we must have $\beta > a$. Now $0 < \beta - a < \beta$; hence, by selection of β we have

$$|\bar{\beta} - a| > |\bar{\beta}|.$$

It follows that $\bar{\beta}$ and a have different signs and $\bar{\beta} < 0$.

Let $\beta = pa + q\gamma$, where $p, q \in \mathscr{Z}$. If $|q| > 1$, let $p \equiv s \pmod{|q|}$, where $|s| \leqslant |q|/2$. Then $(\beta - sa)/q = \gamma + xa \in \mathfrak{a}$ $(x \in \mathscr{Z})$. If we let $\mu = |(\beta - sa)/q| \in \mathfrak{a}$, we have

$$|\bar{\mu}| = |(\bar{\beta} - sa)/q| \leqslant |\bar{\beta}/q| + |sa/q| < a/2 + a/2 = a.$$

Also, $\mu > 0$ and

$$\mu \leqslant |\beta/q| + |sa/q| \leqslant \beta/2 + a/2 < \beta.$$

But such a $\mu \in \mathfrak{a}$ is impossible by the selection of β; hence, $|q| \leqslant 1$. Since $q \neq 0$, we have $q = \pm 1$ and $\mathfrak{a} = [L(\mathfrak{a}), \beta]$.

Next, suppose $\mathfrak{a} = [a, \beta]$, where $a = L(\mathfrak{a})$, $\beta > a$, $-a < \bar{\beta} < 0$. If $\mathfrak{a}$ is not a reduced ideal of $\mathcal{O}_n$ there must exist $\rho \in \mathfrak{a}$ such that $\rho \neq 0$, $|\rho| < a$, and $|\bar{\rho}| < a$. Also, $\rho = xa + y\beta$ $(x, y \in \mathscr{Z})$. Now since $|xa + y\beta| < a$ and $|xa + y\bar{\beta}| < a$, we see that if $x = 0$, then $y = 0$; and, if $y = 0$, then $x = 0$; thus, $xy \neq 0$. If $xy > 0$, the first inequality cannot hold; if $xy < 0$, the second inequality cannot hold. It follows that $\mathfrak{a}$ must be a reduced ideal in $\mathcal{O}_n$. □

COROLLARY 3.5.1. *If $\mathfrak{a}$ is a reduced ideal in $\mathcal{O}_n$, then $L(\mathfrak{a}) < \sqrt{\Delta}$.*

Proof. By the theorem, $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, where $\beta > L(\mathfrak{a})$ and $-L(\mathfrak{a}) < \bar{\beta} < 0$. Thus, $L(\mathfrak{a}) < \beta - \bar{\beta} = \omega - \bar{\omega} = \sqrt{\Delta}$. □

We have a simple sufficient condition for an ideal in $\mathcal{O}_n$ to be reduced in

THEOREM 3.6. *If $\mathfrak{a}$ is a primitive ideal in $\mathcal{O}_n$ and $L(\mathfrak{a}) < \sqrt{\Delta}/2$, then $\mathfrak{a}$ is a reduced ideal in $\mathcal{O}_n$.*

Proof. Let $\mathfrak{a} = [L(\mathfrak{a}), \gamma]$, where $\gamma = b + \omega$ $(b \in \mathscr{Z})$. Put $\beta = \gamma + [-\bar{\gamma}/L(\mathfrak{a})]L(\mathfrak{a})$. Then $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, where $-L(\mathfrak{a}) < \bar{\beta} < 0$. Since $\beta - \bar{\beta} = \omega - \bar{\omega}$ and $\bar{\beta} > -L(\mathfrak{a})$, we get $\beta > \omega - \bar{\omega} - L(\mathfrak{a})$. Also, $\omega - \bar{\omega} = \sqrt{\Delta} > 2L(\mathfrak{a})$; thus, $\beta > L(\mathfrak{a})$ and our result follows immediately from Theorem 3.5. □

If $\mathfrak{a}$ is any reduced ideal in $\mathcal{O}_n$, then $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$ and we may certainly assume that $0 < b < L(\mathfrak{a})$. Since $L(\mathfrak{a}) < \sqrt{\Delta}$, we see that there can only be a finite number of reduced ideals in $\mathcal{O}_n$.

We say, as usual, that two ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_n$ are *equivalent* (written $\mathfrak{a} \sim \mathfrak{b}$) if there exist nonzero $\alpha, \beta \in \mathcal{O}_n$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. Now if α $(\neq 0) \in \mathcal{O}_n$ and $(\alpha)\mathfrak{a} = (\alpha)\mathfrak{b}$, then $(\alpha\bar{\alpha})\mathfrak{a} = (\alpha\bar{\alpha})\mathfrak{b}$ and $(a)\mathfrak{a} = (a)\mathfrak{b}$, where $a = \alpha\bar{\alpha} \in \mathscr{Z}$. Thus, $\mathfrak{a} = \mathfrak{b}$.

LEMMA 3.1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent ideals of $\mathcal{O}_n$, there exists some $\gamma \in \mathfrak{a}$ such that*

$$(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a} \tag{3.1}$$

and $0 < \gamma < L(\mathfrak{a})$.

Proof. Since $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, where α, β $(\neq 0) \in \mathcal{O}_n$, then $|\beta|L(\mathfrak{b}) = |\alpha|\lambda$ for some $\lambda \in \mathfrak{a}$. Let η (> 0) be any unit of $\mathcal{O}_n$. There must exist some power η^k of η such that $\eta^k\lambda < L(\mathfrak{a})$. Put $\gamma = \eta^k\lambda$. If we put $\mathfrak{c} = (\gamma)\mathfrak{b} = (\lambda)\mathfrak{b}$, then $(L(\mathfrak{b})\beta)\mathfrak{b} = (\alpha)\mathfrak{c}$ and $(L(\mathfrak{b})\alpha)\mathfrak{a} = (\alpha)\mathfrak{c}$; hence, $\mathfrak{c} = (L(\mathfrak{b}))\mathfrak{a}$ and $(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$. □

We also point out that if $\mathfrak{a}, \mathfrak{b} \neq (0)$ are ideals in $\mathcal{O}_n$ and $\alpha \in \mathcal{O}_n$, $s \in \mathscr{Z}$, $\alpha, s \neq 0$, and

$$(\alpha)\mathfrak{b} = (sL(\mathfrak{b}))\mathfrak{a},$$

then there exists $\gamma \in \mathfrak{a}$ such that $sL(\mathfrak{b})\gamma = L(\mathfrak{b})\alpha$; hence, $\gamma = \alpha/s \in \mathfrak{a}$.

4. Ideals and Continued Fractions. In this section we will draw together the results of the last two sections in order to show the connection between the ideals in $\mathcal{O}_n$ and the continued fraction expansion of $\phi = (P + \sqrt{D})/Q$. We first suppose that $[a, b + \omega]$ is any primitive ideal in $\mathcal{O}_n$. If we put $\phi = (b + \omega)/a$, we see that $\phi = (P + \sqrt{D})/Q$, where

$$P = (rb + n(r - 1) + hr)/g \in \mathscr{Z}, \qquad Q = ar/g \in \mathscr{Z}, \tag{4.1}$$

and r, n, g, h are defined at the beginning of Section 3. Since $a \mid N(b + \omega)$, it is a simple matter to deduce that $\sigma Q \mid P^2 - D$; hence, $Q \mid P^2 - D$. We also have $P \equiv -n/g \pmod{\sigma}$, $\sigma \mid 2$, and $\gcd(n/g, \sigma) = 1$; thus, $P \equiv 1 \pmod{\sigma}$. We now see that

$$\mathfrak{a} = \left[Q/\sigma, (P + \sqrt{D})/\sigma\right].$$

If we have $Q, P \in \mathscr{Z}$ such that $\sigma \mid Q$, $P \equiv 1 \pmod{\sigma}$ and $\sigma Q \mid D - P^2$, then

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

must be an ideal in $\mathcal{O}_n$. For, if we put

$$a = |Q|/\sigma, \qquad b = (P - 1)/\sigma - n - h + (n + g)/r \in \mathscr{Z},$$

we have $\mathfrak{a} = [a, b + \omega]$ and $a \mid N(b + \omega)$.

In the following theorem we see that if we are given a primitive ideal $\mathfrak{a}_1$ in $\mathcal{O}_n$, the continued fraction algorithm can be used to find a sequence of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ such that $\mathfrak{a}_k \sim \mathfrak{a}_1$ $(k = 1, 2, 3, \ldots)$.

THEOREM 4.1. *Let* $\mathfrak{a}_1 = \mathfrak{a} = [a, b + \omega]$ $(a, b \in \mathscr{Z})$ *and define* $P_0 = P$, $Q_0 = Q$, $\phi_0 = (P_0 + \sqrt{D})/Q_0$, *where* P, Q *are given by* (4.1). *If*

$$\mathfrak{a}_m = \left[Q_{m-1}/\sigma, \left(P_{m-1} + \sqrt{D}\right)/\sigma\right],$$

where $\phi_{m-1} = (P_{m-1} + \sqrt{D})/Q_{m-1}$ *is found by expanding* ϕ_0 *into a continued fraction by using* (2.1), *then* $\mathfrak{a}_m$ *is an ideal in* $\mathcal{O}_n$ *and*

$$(Q_0\theta_m)\mathfrak{a}_m = (Q_{m-1})\mathfrak{a}, \tag{4.2}$$

where θ_m *is defined by* (2.7).

Proof. Certainly $\mathfrak{a}_1$ is an ideal in $\mathcal{O}_n$, $\sigma \mid Q_0$, $P_0 \equiv 1 \pmod{\sigma}$, and $\sigma Q_0 \mid D - P_0^2$. Suppose $\mathfrak{a}_k$ is an ideal in $\mathcal{O}_n$; we have $\sigma \mid Q_{k-1}$, $P_{k-1} \equiv 1 \pmod{\sigma}$, and $\sigma Q_{k-1} \mid D - P_{k-1}^2$. Since $P_k = q_{k-1}Q_{k-1} - P_{k-1}$, we see that $P_k \equiv 1 \pmod{\sigma}$. Further,

$$Q_k = \left(D - P_k^2\right)/Q_{k-1} = \left(D - P_{k-1}^2\right)/Q_{k-1} - q_{k-1}^2 Q_{k-1} + 2q_{k-1}P_{k-1};$$

thus, since $\sigma \mid (D - P_{k-1}^2)/Q_{k-1}$, $\sigma \mid Q_{k-1}$, and $\sigma \mid 2$, we have $\sigma \mid Q_k$. Also, $\sigma Q \mid D - P_k^2$. Hence, $\mathfrak{a}_{k+1}$ is an ideal in $\mathcal{O}_n$. It follows by induction that $\mathfrak{a}_m$ is an ideal in $\mathcal{O}_n$.

Now by (2.9) we have

$$\begin{pmatrix} \theta_m \\ \theta_{m+1} \end{pmatrix} = X \begin{pmatrix} 1 \\ \phi \end{pmatrix},$$

where

$$X = (-1)\begin{pmatrix} -A_{m-2} & B_{m-2} \\ A_{m-1} & -B_{m-1} \end{pmatrix}$$

and $|X| = \pm 1$ by (2.3). Thus,

$$(\theta_m)[1, \psi_m] = [\theta_m, \theta_{m+1}] = [1, \phi]$$

and

$$(Q_0\theta_m)\mathfrak{a}_m = (Q_{m-1})\mathfrak{a}_1. \quad \square$$

Note that we can write (4.2) as

$$(L(\mathfrak{a}_1)\theta_m)\mathfrak{a}_m = (L(\mathfrak{a}_m))\mathfrak{a}_1. \tag{4.3}$$

We will now describe conditions which are sufficient for $\mathfrak{a}_m$ to be a reduced ideal in $\mathcal{O}_n$.

THEOREM 4.2. *If* $\bar{\phi}_m < 0$, *then* $\mathfrak{a}_{m+1}$ *is a reduced ideal in* $\mathcal{O}_n$.

Proof. Put $\gamma = |P_m + \sqrt{D}|/\sigma$. Since $\phi_m > 1$, we have $\gamma > |Q_m/\sigma| = L(\mathfrak{a}_{m+1})$. Also, $N(\gamma) = \phi_m\bar{\phi}_m L(\mathfrak{a}_{m+1})^2 < 0$; hence, $\bar{\gamma} < 0$. Put

$$\beta = \left[-\bar{\gamma}/L(\mathfrak{a}_{m+1})\right] L(\mathfrak{a}_{m+1}) + \gamma.$$

We have

$$\mathfrak{a}_{m+1} = \left[L(\mathfrak{a}_{m+1}), \gamma\right] = \left[L(\mathfrak{a}_{m+1}), \beta\right]$$

and $\beta > L(\mathfrak{a}_{m+1}), -L(\mathfrak{a}_{m+1}) < \bar{\beta} < 0$. It follows by Theorem 3.5 that $\mathfrak{a}_{m+1}$ is a reduced ideal of $\mathcal{O}_n$. □

COROLLARY 4.2.1. *If* $\mathfrak{a} = \mathfrak{a}_1 = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$ *is any primitive ideal in* $\mathcal{O}_n$, *then* $\mathfrak{a}_m$ *is a reduced ideal in* $\mathcal{O}_n$ *when*

$$m > \max\left(2, 4 + \log\left(|Q_0|/2\sqrt{D}\right)/(2\log\tau)\right).$$

Proof. Follows easily from the theorem and Corollary 2.3.2. □

THEOREM 4.3. *If, by developing* $\phi_0 = (P_0 + \sqrt{D})/Q_0$ *into a continued fraction, we find the least* m ($\geqslant 1$) *such that* $0 < Q_{m-1} < \sqrt{D}$, *then* $\mathfrak{a}_m$ *is a reduced ideal in* $\mathcal{O}_n$ *and*

$$\theta_m^{-1} < 2Q_0/Q_{m-1}.$$

Proof. Since $L(\mathfrak{a}_m) = Q_{m-1}/\sigma < \sqrt{D}/\sigma = \sqrt{\Delta}/2$, we see by Theorem 3.6 that $\mathfrak{a}_m$ is a reduced ideal in $\mathcal{O}_n$. If $m = 1$, then $\theta_m = 1 < 2Q_0/Q_0$. If $m = 2$, then since $Q_0 > 0$, we must have $Q_0 > \sqrt{D}$. Also, $\theta_m^{-1} = \phi_1 = (P_1 + \sqrt{D})/Q_1$. Since $D - P_1^2 = Q_0Q_1 > 0$, we have $\theta_m^{-1} < 2\sqrt{D}/Q_1 < 2Q_0/Q_{m-1}$. Suppose $m \geqslant 3$.

Let k be the least integer ($\geqslant 0$) such that $\bar{\phi}_k < 0$. If $k = 2$, then from the proof of Theorem 2.5, we get $Q_1 < 0$. Since $|P_2| < \sqrt{D}$, $Q_2 > 0$ by Theorem 2.2, and $Q_2Q_1 = D - P_2^2$, this is impossible; hence $k \neq 2$. By Theorem 2.4 we have $k = m$ or $k = m - 1$. If $k = m \geqslant 3$, then $\bar{\phi}_{m-1} > 0$ and

$$\theta_m^{-1} < Q_0/Q_{m-1}B_{m-3} \leqslant Q_0/Q_{m-1}$$

by Theorem 2.5. If $k = m - 1 \geqslant 3$, then $\bar{\phi}_{m-2} > 0$. Also, we must have $Q_{m-1} > 0$, $|P_{m-1}| < \sqrt{D}$; thus, we find that $Q_{m-2} = (D - P_{m-1}^2)/Q_{m-1} > 0$ and, as a consequence of the definition of Q_{m-1}, we get $Q_{m-2} > \sqrt{D}$. By Theorem 2.5 we have

$$\theta_{m-1}^{-1} < Q_0/Q_{m-2}B_{m-4};$$

hence

$$\theta_m^{-1} = \theta_{m-1}^{-1}\phi_{m-1} < (Q_0/Q_{m-2}B_{m-4})\left(2\sqrt{D}/Q_{m-1}\right) < 2Q_0/Q_{m-1}. \quad \square$$

Thus, the continued fraction expansion algorithm applied to any primitive ideal $\mathfrak{a} = \mathfrak{a}_1$ in $\mathcal{O}_n$ will ultimately yield an ideal $\mathfrak{a}_m$ equivalent to $\mathfrak{a}_1$ such that $\mathfrak{a}_m$ is a reduced ideal in $\mathcal{O}_n$. We now show that if the continued fraction algorithm is applied to any reduced ideal $\mathfrak{a}$ in $\mathcal{O}_n$, it will produce *all* of the reduced ideals in $\mathcal{O}_n$ which are equivalent to $\mathfrak{a}$.

THEOREM 4.4. *If* $\mathfrak{a} = \mathfrak{a}_1$ *is a reduced ideal in* $\mathcal{O}_n$, *then* $-1 < \bar{\phi}_1 < 0$.

Proof. Since $\mathfrak{a}_1$ is a reduced ideal in $\mathcal{O}_n$ and $L(\mathfrak{a}_1) = Q_0/\sigma$, we have $Q_0/\sigma < \sqrt{\Delta} = 2\sqrt{D}/\sigma$ by Corollary 3.5.1. Also, $\gamma = L(\mathfrak{a}_1)\psi_1 = (P_0 + \sqrt{D})/\sigma - q_0 Q_0/\sigma$; hence, $\gamma \in \mathfrak{a}_1$. Since $\gamma = Q_0/\sigma\phi_1$ and $\phi_1 > 1$, we have $0 < \gamma < Q_0/\sigma$ and $|\bar{\gamma}| > Q_0/\sigma$ ($\mathfrak{a}_1$ is a reduced ideal in $\mathcal{O}_n$); thus, $0 < \sqrt{D} - P_1 < 2\sqrt{D}$ and $P_1 + \sqrt{D} > 0$. Since $\bar{\psi}_1 = (-P_1 - \sqrt{D})/Q_0$ and $\bar{\phi}_1 = 1/\bar{\psi}_1$, we get our result. □

COROLLARY 4.4.1. *If* $\mathfrak{a}_1$ *is a reduced ideal in* $\mathcal{O}_n$, *then so is* $\mathfrak{a}_m$ *for any* $m \geqslant 1$.

Proof. Follows easily from Theorem 4.2 and the fact that if $-1 < \bar{\phi}_1 < 0$, then $-1 < \bar{\phi}_m < 0$ for any $m \geqslant 1$. □

THEOREM 4.5. *If* $\mathfrak{a} = \mathfrak{a}_1$ *and* $\mathfrak{b}$ *are two reduced, equivalent ideals in* $\mathcal{O}_n$ *and* $\gamma \in \mathfrak{a}$ *such that*

$$(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$$

with $0 < \gamma < L(\mathfrak{a})$, *then there must exist some* $m \geqslant 1$ *such that* $\mathfrak{b} = \mathfrak{a}_m$ *and* $\theta_m = \gamma/L(\mathfrak{a})$.

Proof. By Lemma 3.1, we certainly know that such a $\gamma \in \mathfrak{a}$ exists. We also know (Theorem 4.1) that

$$\mathfrak{a}_1 = [Q_0\theta_{k-1}/\sigma, Q_0\theta_k/\sigma]$$

for any $k \geqslant 1$. Since $\mathfrak{a}_1$ is a reduced ideal of $\mathcal{O}_n$, we have $\bar{\phi}_i < 0$ for any $i \geqslant 1$ by the previous theorem; hence, $\bar{\theta}_{k-1}$ and $\bar{\theta}_k$ have different signs. Since $\gamma < L(\mathfrak{a})$ and the θ_k's decrease as k increases, we must have either

$$\theta_m = \gamma/L(\mathfrak{a}), \quad \text{or} \quad \theta_{m+1} < \gamma/L(\mathfrak{a}) < \theta_m$$

for some m, or $\gamma/L(\mathfrak{a}) < \theta_i$ for all θ_i. Since

$$|\theta_m/B_{m-2}| = |A_{m-2}/B_{m-2} - \phi| < 1/B_{m-1}B_{m-2},$$

we see that $0 < \theta_m < 1/B_{m-1}$; hence, by (2.2) we cannot have the latter case. Suppose

$$\theta_{m+1} < \gamma/L(\mathfrak{a}) < \theta_m$$

for some m. Since $\gamma \in \mathfrak{a}$, we have $\gamma/L(\mathfrak{a}) = x\theta_m + y\theta_{m+1}$ for some $x, y \in \mathscr{Z}$. Since $\gamma > \theta_{m+1}L(\mathfrak{a})$, we must also have $|\bar{\gamma}| < |\bar{\theta}_{m+1}|L(\mathfrak{a})$. For, if $|\bar{\gamma}| > |\bar{\theta}_{m+1}|L(\mathfrak{a})$, and $\lambda = L(\mathfrak{a})\theta_{m+1}$, then $\lambda \in \mathfrak{a}$ and $L(\mathfrak{b})\lambda = \gamma\rho$ for some $\rho \in \mathfrak{b}$ ($\rho \neq 0$). Further,

$$|\rho| = L(\mathfrak{b})|\lambda/\gamma| < L(\mathfrak{b}) \quad \text{and} \quad |\bar{\rho}| = L(\mathfrak{b})|\bar{\lambda}/\bar{\gamma}| < L(\mathfrak{b}).$$

Since this contradicts the fact that $\mathfrak{b}$ is reduced, we can only have $|\bar{\gamma}| < |\bar{\theta}_{m+1}|L(\mathfrak{a})$. It follows that

$$|x\theta_m + y\theta_{m+1}| < \theta_m \quad \text{and} \quad |x\bar{\theta}_m + y\bar{\theta}_{m+1}| < |\bar{\theta}_{m+1}|.$$

Since $\bar{\theta}_m$ and $\bar{\theta}_{m+1}$ have different signs, both of these inequalities cannot hold; hence, we must have $\gamma = \theta_m L(\mathfrak{a})$ for some $m \geqslant 1$. Since $(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$ and $(L(\mathfrak{a})\theta_m)\mathfrak{a}_m = (L(\mathfrak{a}_m))\mathfrak{a}$ by (4.3), we get $|N(\gamma)|N(\mathfrak{b}) = L(\mathfrak{b})^2 N(\mathfrak{a})$ and $L(\mathfrak{a})^2|N(\theta_m)|N(\mathfrak{a}_m) = L(\mathfrak{a}_m)^2 N(\mathfrak{a})$. Since $N(\gamma) = N(\theta_m)L(\mathfrak{a})^2$, $N(\mathfrak{b}) = L(\mathfrak{b})$ and $N(\mathfrak{a}) = L(\mathfrak{a})$, we have $L(\mathfrak{b}) = L(\mathfrak{a}_m)$. Since $(\gamma)\mathfrak{b} = (L(\mathfrak{a}_m))\mathfrak{a} = (L(\mathfrak{a})\theta_m)\mathfrak{a}_m = (\gamma)\mathfrak{a}_m$, we have $\mathfrak{b} = \mathfrak{a}_m$. □

Thus, we have shown that if $\mathfrak{a}_1$ is any primitive ideal in $\mathcal{O}_n$ to which the continued fraction expansion of a corresponding ϕ_0 is applied, we must ultimately produce a reduced ideal $\mathfrak{a}_m$ ($\sim \mathfrak{a}_1$), and once this has occurred, the subsequent

ideals determined will be all of those which are reduced ideals in $\mathcal{O}_n$ and equivalent to $\mathfrak{a}_1$. As there are only a finite number of such ideals, this continued fraction expansion must (as is well known) become periodic. Incidentally, we have also shown that the preperiod of the continued fraction expansion of any quadratic irrational of the form ϕ above corresponds to the process of finding a reduced ideal equivalent to an ideal in some $\mathcal{O}_n$. By Corollary 4.2.1, we can even bound the length of this preperiodic part of the continued fraction expansion of ϕ.

5. Distance Between Ideals. Let $\mathfrak{a}_1 = \mathfrak{a}$ and $\mathfrak{b}$ be any two reduced and equivalent ideals in $\mathcal{O}_n$. By Theorem 4.5 we know that $\mathfrak{b} = \mathfrak{a}_m$ for some $m \geqslant 1$, and by (4.3),

$$(L(\mathfrak{a}_1)\theta_m)\mathfrak{a}_m = (L(\mathfrak{a}_m))\mathfrak{a}_1.$$

We will define the distance, $d(\mathfrak{a}, \mathfrak{b})$, from $\mathfrak{a}$ to $\mathfrak{b}$ to be $-\log\theta_m$. We note here that $d(\mathfrak{a}_m, \mathfrak{a}_1) > d(\mathfrak{a}_{m-1}, \mathfrak{a}_1) \geqslant 0$ and $d(\mathfrak{a}_m, \mathfrak{a}_1) = 0$ if and only if $m = 1$. The notion of distance was first discussed by Shanks [13] and later refined by Lenstra [6] and Schoof [12]. We are essentially using Shanks' definition of distance here. Notice that distance is only defined between ideals of $\mathcal{O}_n$ that are equivalent and reduced.

A connection between $d(\mathfrak{a}_m, \mathfrak{a}_1)$ and m is furnished in the following result of Lévy [7].

THEOREM 5.1 (LÉVY). *Let*

$$\phi = [q_0, q_1, q_2, \ldots, q_{k-1}, \phi_k].$$

For almost all irrationals ϕ we have

$$\lim_{k\to\infty} \sqrt[k]{\phi_1\phi_2\phi_3\cdots\phi_k} = e^{\lambda},$$

where $\lambda = \pi^2/(12\log 2) \approx 1.1866$. □

Since

$$\theta_m = \prod_{t=1}^{m-1} \psi_t \quad \text{and} \quad \theta_m^{-1} = \prod_{t=1}^{m-1} \phi_t,$$

we expect that $d(\mathfrak{a}_m, \mathfrak{a}_1) = -\log\theta_m \approx (m-1)\lambda$.

Let $\mathfrak{a}_1$ $(= (1))$, $\mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_k, \ldots$ be the sequence of reduced principal ideals in $\mathcal{O}_n$ and suppose that $\mathfrak{b}$ is any reduced ideal in $\mathcal{O}_n$. Let $(u)\mathfrak{c} = \mathfrak{a}_s\mathfrak{b}_t$, where $u \in \mathcal{Z}$ and $\mathfrak{c}$ is a primitive ideal in $\mathcal{O}_n$. Let $\mathfrak{c}_m$ be a reduced ideal equivalent to $\mathfrak{c} = \mathfrak{c}_1$, which we find by using the continued fraction algorithm on $\mathfrak{c}_1$, with m defined as in Theorem 4.3. Since

$$\mathfrak{c}_m \sim \mathfrak{c}_1 \sim \mathfrak{a}_s\mathfrak{b}_t \sim \mathfrak{b}_t \sim \mathfrak{b}_1 \quad (\mathfrak{a}_s \text{ is principal}),$$

and $\mathfrak{c}_m$ is reduced, we must have $\mathfrak{c}_m = \mathfrak{b}_k$ for some $k \geqslant 1$. We can now prove

THEOREM 5.2. *If*

$$d_t' = d(\mathfrak{b}_t, \mathfrak{b}_1), \qquad d_k' = d(\mathfrak{b}_k, \mathfrak{b}_1),$$

and $d_s = d(\mathfrak{a}_s, \mathfrak{a}_1)$, *then*

$$d_k' = d_t' + d_s + \delta,$$

where $0 < \delta < \log 8D$.

Proof. Let $(\theta_s)\mathfrak{a}_s = (L(\mathfrak{a}_s))$ $(L(\mathfrak{a}_1) = 1,\ \mathfrak{a}_1 = (1))$, $(L(\mathfrak{b}_1)\theta_t')\mathfrak{b}_t = (L(\mathfrak{b}_t))\mathfrak{b}_1$, $(L(\mathfrak{c}_1)\theta_m'')\mathfrak{c}_m = (L(\mathfrak{c}_m))\mathfrak{c}_1$. Since $(u)\mathfrak{c}_1 = \mathfrak{a}_s\mathfrak{b}_t$, we get $L(\mathfrak{b}_t)L(\mathfrak{a}_s) = u^2L(\mathfrak{c}_1)$ by Theorem 3.3. Also,

$$\left(uL(\mathfrak{b}_1)\theta_s\theta_t'\right)\mathfrak{c}_1 = \left(L(\mathfrak{a}_s)L(\mathfrak{b}_t)\right)\mathfrak{b}_1;$$

hence,

$$\left(L(\mathfrak{c}_m)L(\mathfrak{c}_1)\theta_s\theta_t'\right)\mathfrak{c}_1 = \left(uL(\mathfrak{c}_1)L(\mathfrak{c}_m)\right)\mathfrak{b}_1$$

and

$$\left(L(\mathfrak{b}_1)\theta_s\theta_t'\theta_m''/u\right)\mathfrak{c}_m = \left(L(\mathfrak{c}_m)\right)\mathfrak{b}_1.$$

Now $u \geqslant 1$ and $0 < \theta_s, \theta_t', \theta_m'' < 1$; hence,

$$0 < \gamma = L(\mathfrak{b}_1)\theta_s\theta_t'\theta_m''/u < L(\mathfrak{b}_1) \quad \text{and} \quad \gamma \in \mathfrak{b}_1.$$

By Theorem 4.5 we must have $\gamma/L(\mathfrak{b}_1) = \theta_k'$. It follows that

$$d_k' = d_s + d_t' + \delta,$$

where $\delta = \log(u/\theta_m'')$. By Theorem 4.3 we have

$$\left(\theta_m''\right)^{-1} < 2Q_0''/Q_{m-1}'' \leqslant 2Q_0''/\sigma,$$

where $L(\mathfrak{c}_1) = Q_0''/\sigma$ and $Q_{s-1}Q_{t-1}'/\sigma^2 = u^2L(\mathfrak{c}_1)$. Since $\mathfrak{a}_s$ and $\mathfrak{b}_t$ are reduced ideals in $\mathcal{O}_n$, we must have $L(\mathfrak{a}_s)$, $L(\mathfrak{b}_t) < \sqrt{\Delta}$ by Corollary 3.5.1; hence, Q_{s-1}, $Q_{t-1}' < 2\sqrt{D}$ and $\delta < \log 8D$. Also, since $\theta_m'' < 1$, we have $u(\theta_m'')^{-1} > u \geqslant 1$ and $\delta > 0$. □

Thus, if s and t are large, the value of δ would be small compared to λx and λt. It follows that we would expect to have

$$k \approx t + s$$

by Lévy's law.

We will also require

THEOREM 5.3. *If* $\mathfrak{c}_m$, $\mathfrak{b}_k$, θ_k, θ_s, θ_t', θ_m'', u, *have the meanings assigned to them in Theorem* 5.2, *then* $\mathfrak{b}_{k+1} = \mathfrak{c}_{m+1}$ *and* $\theta_{k+1}' = \theta_s\theta_t'\theta_{m+1}''/u$.

Proof. Since $\mathfrak{c}_m = \mathfrak{b}_k$, we get

$$\left[Q_{m-1}''/\sigma, \left(P_{m-1}'' + \sqrt{D}\right)/\sigma\right] = \left[Q_{k-1}'/\sigma, \left(P_{k-1}' + \sqrt{D}\right)/\sigma\right];$$

consequently,

$$Q_{m-1}'' = Q_{k-1}' \quad \text{and} \quad P_{m-1}'' \equiv P_{k-1}' \left(\operatorname{mod} Q_{m-1}''\right).$$

Thus,

$$\phi_{m-1}'' = \left(P_{m-1}'' + \sqrt{D}\right)/Q_{m-1}'' = j + \left(P_{k-1}' + \sqrt{D}\right)/Q_{k-1}' = j + \phi_{k-1}',$$

where $j \in \mathscr{Z}$, and $\phi_m'' = \dot{\phi}_k'$. It follows that $\mathfrak{c}_{m+1} = \mathfrak{b}_{k+1}$.

Now $\theta_{k+1}' = \psi_k'\theta_k' = \theta_k'/\phi_k' = \theta_k'/\phi_m''$; hence,

$$\theta_{k+1}' = \theta_s\theta_t'\theta_m''/\phi_m''u = \theta_s\theta_t'\theta_{m+1}''/u. \quad \square$$

6. The Algorithm. In order to describe our algorithm for the parallel generation of $((-1)^kQ_k, A_{k-1})$ pairs, we make use of certain sets $\mathscr{S}_k$. If N is the number which we wish to factor by using CFRAC, we may assume that $N = ef^2$, where e is square-free and $e > 1$. We put $D_0 = e$; $n = rf$, $g = r$, $\sigma = 1$, $D = N$, $h = -f(r-1)$. and we get $\omega = \sqrt{D}$ and $\mathcal{O}_n = [1, \sqrt{D}]$. If $\mathfrak{a}_1 = (1)$, then $P_0 = 0$ and $Q_0 = 1$. We use the same notation as in Section 3.

We require two lemmas.

LEMMA 6.1. *If, in the continued fraction expansion of* $\phi_0 = \phi$, *we have* $-1 < \bar{\phi}_1 < 0$, *then*

$$q_k = \left[(P_{k+1} + d)/Q_k\right]$$

for all $k \geqslant 1$.

Proof. Since $-1 < \bar{\phi}_1 < 0$, we have $-1 < \bar{\phi}_k < 0$ for all $k \geqslant 1$. Also, $\phi_{k+1} = 1/(\phi_k - q_k)$; hence,

$$0 < \left(-1/\bar{\phi}_{k+1}\right) - q_k < 1.$$

It follows that

$$q_k = \left[-1/\bar{\phi}_{k+1}\right] = \left[-\bar{\psi}_{k+1}\right] = \left[(P_{k+1} + d)/Q_k\right]. \quad \square$$

LEMMA 6.2. *If* $-1 < \bar{\phi}_1 < 0$ *and* $T_k \equiv P_k \pmod{Q_k}$, *then*

$$P_{k+1} = qQ_k - T_k, \qquad q_k = q + \left[(d - T_k)/Q_k\right],$$

where $q = [(T_k + d)/Q_k]$.

Proof. Let $T_k = P_k + mQ_k$. We have $q = [(P_k + d)/Q_k] + m = q_k + m$ and

$$qQ_k - T_k = (q_k + m)Q_k - P_k - mQ_k = q_kQ_k - P_k = P_{k+1}.$$

By Lemma 6.1, we also have

$$q_k = \left[(P_{k+1} + d)/Q_k\right] = q + \left[(d - T_k)/Q_k\right]. \quad \square$$

Thus, if we are given values for Q_k, T_k, $A_k \pmod D$, $A_{k-1} \pmod D$, where $T_k \equiv P_k \pmod{Q_k}$, we can compute P_{k+1}, q_k by using Lemma 6.2. By using the formulas in Section 2, we can also determine $P_k = q_kQ_k - P_{k+1}$, $Q_{k+1} = (D - P_{k+1}^2)/Q_k$, $Q_{k-1} = (D - P_k^2)/Q_k$, $-A_{k-2} \equiv q_kA_{k-1} - A_k \pmod D$. Let s_k, t_k be integers such that $s_k^2 = t_k^2 = 1$ and define the quadruples

$$\mathcal{U}_k = \left((-1)^{k+1}Q_{k+1},\ P_{k+1},\ s_kA_k \pmod D,\ s_kA_{k-1} \pmod D\right),$$

$$\mathcal{V}_k = \left((-1)^{k-1}Q_{k-1},\ P_k,\ -t_kA_{k-2} \pmod D,\ t_kA_{k-1} \pmod D\right).$$

Suppose $\mathcal{X} = (X, Y, Z, W)$ is either $\mathcal{U}_k$ or $\mathcal{V}_k$. We now describe

ALGORITHM 2. (*Forward or Backward Single-Step Algorithm*) Compute $q = [(Y + d)/|X|]$ and put

$$Y' = q|X| - Y, \qquad X' = (Y'^2 - D)/X,$$

$$Z' = qZ + W, \qquad W' = Z,$$

$$\mathcal{X}' = (X', Y', Z', W').$$

This algorithm is very useful because of

THEOREM 6.1. *Suppose that in the continued fraction expansion of* $\phi_0 = \phi$ *we have* $-1 < \bar{\phi}_1 < 0$. *If* $\mathcal{X} = \mathcal{U}_k$, *then* $\mathcal{X}' = \mathcal{U}_{k+1}$ *with* $s_{k+1} = s_k$; *if* $\mathcal{X} = \mathcal{V}_k$, *then* $\mathcal{X}' = \mathcal{V}_{k-1}$ *with* $t_{k-1} = -t_k$.

Proof. By the results given in Section 2, the theorem follows easily when $\mathcal{X} = \mathcal{U}_k$. If $\mathcal{X} = \mathcal{V}_k$, then $q = [(P_k + d)/Q_{k-1}] = q_{k-1}$ by Lemma 6.1. Hence

$$Y' = q_{k-1}Q_{k-1} - P_k = P_{k-1},$$

$$X' = (-1)^{k-1}\left(P_{k-1}^2 - D\right)/Q_{k-1} = (-1)^{k-2}Q_{k-2},$$

$$Z' = -q_{k-1}t_kA_{k-2} + t_kA_{k-1} = -t_k(q_{k-1}A_{k-2} - A_{k-1}) \equiv -t_k(-A_{k-3}) \pmod D,$$

$$W' \equiv -t_kA_{k-2} \pmod D.$$

If we put $t_{k-1} = -t_k$, we have the theorem when $\mathcal{X} = \mathcal{V}_k$. $\square$

Hence, we see that, depending upon whether we start with a quadruple of the form $\mathscr{U}_k$ or $\mathscr{V}_k$, we can go forward or backward in the continued fraction expansion of ϕ by repeated application of Algorithm 2.

We define

$$\mathscr{S}_k = \big((-1)^k Q_k,\ T_k,\ \varepsilon A_k \pmod D,\ \varepsilon A_{k-1} \pmod D\big),$$

where $T_k \equiv P_k \pmod{Q_k}$ and $\varepsilon^2 = 1$. By using the formulas above we can determine $\mathscr{U}_k$ and $\mathscr{V}_k$. If we can generate 8192 = 16384/2 different widely-spaced $\mathscr{U}_n$ and $\mathscr{V}_n$ quadruples and place each in one of the 16384 processors; by using Algorithm 2 we can then generate quadruples $\mathscr{U}_{n+1}$, $\mathscr{V}_{n-1}$, $\mathscr{U}_{n+2}$, $\mathscr{V}_{n-2}$, etc., and from these extract pairs $((-1)^k Q_k,\ uA_{k-1} \pmod D)$, where

$$u^2 A_{k-1}^2 \equiv A_{k-1}^2 \equiv (-1)^k Q_k \pmod D.$$

To ensure that we do not get duplication of the pairs $((-1)^k Q_k,\ uA_{k-1} \pmod D)$ in the various processors, we must compute initial quadruples $\mathscr{S}_{h_1}, \mathscr{S}_{h_2}, \ldots, \mathscr{S}_{h_{8192}}$ such that

$$h_1 \geqslant x/16384 \quad \text{and} \quad h_{i+1} - h_i > 2x/16384,$$

where x is the number of quadratic residues of the type $(-1)^i Q_i$ needed to factor N.

The problem of generating the $\mathscr{S}_{h_i}$'s is easily solved by making use of the Large-Step Algorithm, which we will now develop. Given $\mathscr{S}_i$ and $\mathscr{S}_j$, this algorithm will rapidly find $\mathscr{S}_k$ where $k \approx i + j$. Notice also that any $\mathscr{S}_t$ can be reached in $O(\log_2 t)$ operations by a combination of large-step and single-step iterations.

By Theorem 3.4, if $\gcd(L(\mathfrak{a}_{i+1}), L(\mathfrak{a}_{j+1})) = 1$ and $\mathfrak{c} = \mathfrak{a}_{i+1}\mathfrak{a}_{j+1}$, then

$$\mathfrak{c} = \big[Q', P' + \sqrt{D}\big]$$

where

$$Q' = Q_i Q_j \quad \text{and} \quad P' \equiv \begin{cases} P_i \pmod{Q_i}, \\ P_j \pmod{Q_j}, \end{cases}$$

$0 < P' < Q'$. Put $M \equiv (Q')^{-1} \pmod D$. (We assume here, as is most likely, that $\gcd(Q', D) = 1$.)

We now expand $\phi' = (P' + \sqrt{D})/Q'$ into a continued fraction until we find the least m such that $0 < Q'_m < \sqrt{D}$. Since $[Q'_m, P'_m + \sqrt{D}] = \mathfrak{c}'_{m+1} \sim \mathfrak{a}_{i+1}\mathfrak{a}_{j+1} \sim \mathfrak{a}_1$ is reduced, we must have $\mathfrak{c}'_{m+1} = \mathfrak{a}_{k+1} = [Q_k, P_k + \sqrt{D}]$; hence, $Q_k = Q'_m$, $P_k \equiv P'_m \pmod{Q_k}$.

Now

$$\theta_{k+1} = \theta_{i+1}\theta_{j+1}\theta'_{m+1} \tag{6.1}$$

and

$$\theta_{k+2} = \theta_{i+1}\theta_{j+1}\theta'_{m+2} \tag{6.2}$$

by Theorems 5.2 and 5.3. Further, by Theorem 2.1 and the definition of G_m in Section 2, we have

$$\theta_{i+1} = (-1)^i\big(A_{i-1} - \sqrt{D}\,B_{i-1}\big), \qquad \theta_{j+1} = (-1)^j\big(A_{j-1} - \sqrt{D}\,B_{j-1}\big),$$

$$\theta'_{m+1} = (-1)^m\big(G'_{m-1} - \sqrt{D}\,B'_{m-1}\big)/Q', \qquad \theta'_{m+2} = (-1)^{m+1}\big(G'_m - \sqrt{D}\,B'_m\big)/Q',$$

$$\theta_{k+1} = (-1)^k\big(A_{k-1} - \sqrt{D}\,B_{k-1}\big).$$

Thus, from (6.1) and (6.2) we derive

$$A_{k-1} \equiv (-1)^{k+\iota+\jmath+m} M A_{\iota-1} A_{\jmath-1} G'_{m-1},$$
$$A_k \equiv (-1)^{k+\iota+\jmath+m} M A_{\iota-1} A_{\jmath-1} G'_m \pmod{D},$$

where

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

By Theorem 2.4 we must have $\bar{\phi}_{m-1} > 0$ $(m > 1)$, and by Theorem 2.3 and Corollary 2.3.1 we see that

$$B'_{m-3} < \sqrt{Q'/\sqrt{D}} < 2\sqrt[4]{D} \qquad (m \geqslant 3)$$

and

$$B'_{m-2} < Q'/2\sqrt{D}\, B_{m-3} < 2\sqrt{D} \qquad (m \geqslant 2);$$

thus, the B''s up to B'_{m-2} do not get large and therefore need not be reduced modulo D as they are calculated.

We now give our Large-Step Algorithm (LS) for going directly to $\mathscr{S}_k$, where $k \approx i + j$, given $\mathscr{S}_i$ and $\mathscr{S}_j$. We denote this by $\mathscr{S}_k = \mathrm{LS}(\mathscr{S}_i, \mathscr{S}_j)$.

ALGORITHM 3. *Large-Step Algorithm* (*LS*). We first assume that for our given $\mathscr{S}_i$ and $\mathscr{S}_j$ we have $\gcd(Q_i, Q_j) = 1$. If $\gcd(Q_i, Q_j) \neq 1$, we would compute $\mathscr{S}_{j+1}$ by Algorithm 1 and try again. If, as in our case, the same $\mathscr{S}_i$ $(i \approx 2x/16384)$ is to be used several times, it is best to find i initially such that Q_i does not have small prime factors. In practice, of course, this happens relatively frequently; otherwise, the CFRAC algorithm would execute much more rapidly than it does.

1. Compute $Q'_0 = Q_i Q_j$ and M such that

$$M Q'_0 \equiv 1 \pmod{D}.$$

Solve the linear Diophantine equation

$$XQ_i - YQ_j = P_j - P_i$$

and put $P'_0 \equiv P_i + XQ_i \pmod{Q'_0}$, where $0 < P'_0 < Q'_0$.

2. By using Algorithm 1 with A'_{-2}, A'_{-1} initialized to 1, 0, respectively (this will actually compute the B_h's for $h = 0, 1, 2, 3, \ldots$), develop the continued fraction expansion of $\phi'_0 = (P'_0 + \sqrt{D})/Q'_0$ until an m is determined such that

$$0 < Q'_m \leqslant d.$$

3. Put $Q_k = Q'_m$, $T_k = P'_m$,

$$F_{k-1} \equiv M A_{\iota-1} A_{\jmath-1} \left(P'_m A'_{m-1} + Q'_m A'_{m-2}\right) \pmod{D},$$
$$F_k \equiv M A_{\iota-1} A_{\jmath-1} \left(P'_{m+1} A'_m + Q'_{m+1} A'_{m-1}\right) \pmod{D}.$$

If $F_{k-1}^2 \equiv Q_k \pmod{D}$, put $(-1)^k = 1$; otherwise, put $(-1)^k = -1$. Put $\mathscr{S}_k = ((-1)^k Q_k, T_k, F_k, F_{k-1})$.

Examples. We give an example of the Large-Step Algorithm with $D = 103$. Of course, no one would consider using this procedure to factor the prime number 103, but we will discuss the simple continued fraction expansion of $\sqrt{103}$ as an illustrative example. By referring to Table 1, we see that $\mathscr{S}_2 = \{13, 8, 71, 61\}$, $\mathscr{S}_3 = \{6, 5, 100, 71\}$.

We will apply the LS algorithm to $\mathscr{S}_2$ and $\mathscr{S}_3$ so that at the beginning of Step 1, $i = 2$ and $j = 3$.

Step 1. $Q'_0 = 78$,
$P'_0 = 47$,
$M = (Q'_0)^{-1} \pmod{D} = 70$.

Step 2. The reduction in Step 2 requires four iterations of the simple continued fraction process before Q satisfies the required relationship. These are given in Table 2 below.

TABLE 2

i	P'_i	Q'_i	q'_i	R'_i	A'_i
−2	—	—	—	—	1
−1	—	−27	—	—	0
0	47	78	0	57	1
1	−47	−27	1	−10	1
2	20	11	2	8	3
3	2	9	1	3	4
4	7	6			

Step 3. We have $m = 3$, $Q_k = 9$, $T_k = 2$,

$$P'_m A'_{m-1} + Q'_m A'_{m-2} = 2 \cdot 3 + 9 \cdot 1 = 15,$$

$$P'_{m+1} A'_m + Q'_{m+1} A'_{m-1} = 7 \cdot 4 + 6 \cdot 3 = 46,$$

$F_{k-1} = 100$, $F_k = 32$, $(-1)^k = 1$. Notice that we cannot evaluate k by using the LS Algorithm. However, if we compare our results with those in Table 1, we see that $k = 8$.

7. Some Remarks Concerning Implementation of the LS Algorithm. The LS Algorithm was implemented in extended precision using the Hanson package from Sandia Corporation. When it was executed on the VAX 11-780, which serves as the host to the MPP, it ran very slowly. To prepare the data required for a 60-digit N, nearly 2.5 hours of VAX time would be needed. This is excessive, since we estimate that only 20 minutes of MPP time would be needed to factor N. Better results were obtained by running the data preparation segment on a CDC 7600 where .52 hours were required for a 60-digit N. Much, if not most, of this time is due to the lack of assembly-coded routines in the Hanson Package. Had an assembler language program been used on the CDC, we estimate that less than 10 minutes would be needed to produce the required data. Another way to correct this mismatch would be to perform the entire LS operation on the MPP in parallel on 16384 items at once. We will explain in the remaining portion of this paper how this could be performed on a slightly expanded version of an MPP and give a speculative estimate of its running time.

The algorithm below assumes that if different quadruples $\mathscr{S}$ of the simple continued fraction expansion are stored in each of the 16834 processors and a "constant" quadruple $\mathscr{S}_\nu$ of the sequence is stored in the MPP as a scalar, then the LS Algorithm can be used to multiply the scalar term with each of the $\mathscr{S}$ quadruples in the processors simultaneously producing translated $\mathscr{S}$ quadruples in each processor. This operation would be difficult to do in the present MPP configuration because of the small amount of storage in each processor. However, with a larger version of an MPP it would be relatively easy to implement. Furthermore, we assume that if $M = \{b_0, b_1, b_2, \ldots, b_{16383}\}$ is a sequence of mask bits, one for each processor, the parallel multiplication described above can be performed under the mask M. This means that the multiplication operation takes place only in those processors having the corresponding mask bit $b_i = 1$.

ALGORITHM 4. Generate 16,384 widely-spaced $\mathscr{S}$ quadruples in parallel.

Step 1. *Preprocessing.* Use the Single-Step and Large-Step Algorithm together to generate $\mathscr{S}_\nu$, where ν is sufficiently large that the number of (Q, A) pairs needed does not exceed 16384ν. Place a copy of $\mathscr{S}_\nu$ in each processor. Also, let $M_0, M_1, \ldots, M_{13}$ be 14 masks defined as follows: Let I be the sequence of integers $\{0, 1, 2, \ldots, 16383\}$. Let M_0 be the sequence of least significant bits of I, M_1 the sequence of second least significant bits of I, and so on, until we define M_{13} as the sequence of most significant bits of I. Thus, we have

$$M_0 = \{0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,\ldots\},$$
$$M_1 = \{0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,\ldots\},$$
$$M_2 = \{0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,\ldots\},$$
$$M_3 = \{0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,\ldots\},$$

and eventually M_{13} consists of a string of 8,192 zeros followed by 8,192 ones.

Step 2. Set $i \leftarrow 0$ and repeat Step 3 fourteen times.

Step 3. Replace $\mathscr{S}_\nu$ by $\mathrm{LS}(\mathscr{S}_\nu, \mathscr{S}_\nu)$. Under the mask M_i, apply the LS Algorithm on $\mathscr{S}_\nu$ and the $\mathscr{S}$ in each processor and then set $i \leftarrow i + 1$.

Proof of Algorithm. Let $\mathscr{T}_1 = \mathscr{S}_\nu$ and $\mathscr{T}_j = \mathrm{LS}(\mathscr{T}_{j-1}, \mathscr{T}_1)$. It follows by induction on i that after Step 3 has been executed i times, the MPP will contain 2^{14-i} collections of the 2^i data items $\mathscr{T}_1, \mathscr{T}_2, \mathscr{T}_3, \ldots, \mathscr{T}_{2^i}$. □

Running Time Estimate. A careful cycle count of Algorithm 2, which generates the next term of a continued fraction expansion on the MPP, comes to .016 seconds per iteration for a 70-digit number. This includes all I/O times required for swapping back and forth between the auxiliary staging memory and the main memory. By Corollary 4.2.1, we see that no more than about 75 iterations of the continued fraction process would be needed to perform the reduction step (Step (2)) of the LS Algorithm when N is a sixty-digit number. In fact, the average number of these iterations seems empirically to be about 30. We can assume that the array time for a reduction iteration will take about as much time as an ordinary continued fraction iteration since, although the values of P and Q are large, the values of A are

correspondingly small. Assuming that 40 steps will be the maximum required for the longest example in a set of 16,384, and further assuming that reduction consumes one-half the total time for the LS Algorithm to execute (this is very conservative—it probably consumes as much as .9), we arrive at the following running time analysis.

Running time for executing the LS Algorithm 14 times equals

$$40 \times 0.16 \times 2 \times 14 = 17.9 \text{ seconds.}$$

Thus, after using the LS Algorithm about twenty times to obtain $\mathscr{S}_v$ such that v is in the neighborhood of 10^6 (a few seconds on the CDC 7600), an additional 20 seconds on the MPP would produce 16,384 distinct paris (Q, A) which are spaced about 1,000,000 units apart. This represents a considerable improvement over the times required on the CDC 7600.

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

Department of Mathematics
Northern Illinois University
DeKalb, Illinois 60115

1. G. CHRYSTAL, *Textbook of Algebra*, Part 2, 2nd ed. reprinted, Dover, New York, 1969, pp. 423–490.

2. H. COHN, *A Second Course in Number Theory*, Wiley, New York, 1962.

3. J. A. DAVIS & D. B. HOLDRIDGE, "Factorization using the quadratic sieve algorithm," *Advances in Cryptology*, Proceedings of Crypto 83, Plenum Press, New York, 1984, pp. 103–113.

4. L. E. DICKSON, *History of the Theory of Numbers*, Vol. II, reprinted, Chelsea, New York, 1952.

5. E. L. INCE, "Cycles of reduced ideals in quadratic fields," *Mathematical Tables*, Vol. IV, British Association for the Advancement of Science, London, 1934.

6. H. W. LENSTRA, JR., "On the calculation of regulators and class number of quadratic fields," *London Math. Soc. Lecture Note Ser.*, v. 56, 1982, pp. 123–150.

7. PAUL LÉVY, "Sur le développement en fraction continue d'un nombre choisi au hasard," *Compositio Math.*, v. 3, 1936, pp. 286–303.

8. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–205.

9. OSKAR PERRON, *Die Lehre von den Kettenbrüchen*, Bd. I, 3rd ed., B. G. Teubner, Stuttgart, 1954.

10. C. POMERANCE, "Analysis and comparison of some integer factoring algorithms," *Computational Methods in Number Theory* (H. W. Lenstra, Jr. and R. Tijdeman, eds.), Math. Centrum Tracts, Number 154, Part I, Amsterdam, 1983, pp. 89–139.

11. C. POMERANCE & S. S. WAGSTAFF, JR., *Implementation of the Continued Fraction Integer Factoring Algorithm*, Proc. 12th Winnipeg Conf. on Numerical Methods of Computing, *Congress. Numer.*, v. 37, 1983, pp. 99–118.

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

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