MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 95-101

Computing in the Jacobian of a Hyperelliptic Curve

By David G. Cantor*

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

Abstract. In this paper we present algorithms, suitable for computer use, for computation in the Jacobian of a hyperelliptic curve. We present a reduction algorithm which is asymptotically faster than that of Gauss when the genus g is very large.

1. Introduction. In [9], Shanks introduced the use of the class group of a quadratic number field as a tool in computational number theory and provided an efficient algorithm for multiplying (composing) ideal classes. A number of improvements have since occurred, and new algorithms using the class group have appeared. See, for example, Schnorr and Lenstra [7]. More recently, Lenstra [4] has shown how to use the group of points on an elliptic curve, defined over a finite field, in a factorization algorithm. Elliptic curves are the "genus 1" case of the Jacobian groups of hyperelliptic curves. The latter are the analogues of the class groups of quadratic number fields (henceforth we shall say simply "*class group*").

While many explicit formulas for addition on an elliptic curve have appeared (for practical examples, see Chudnovsky and Chudnovsky [2], and Montgomery [5]), and numerous algorithms for computing in the class group of a quadratic number field and number fields of higher degree have appeared (see, for example, Lenstra [4], Shanks [9], and Williams, Dueck, and Schmid [10]), explicit formulas for addition in the Jacobian group of a hyperelliptic curve (henceforth we shall simply say *Jacobian*), which are suitable for computation, do not appear to have been published. The purpose of this paper is to present such algorithms. While computation in the Jacobian is entirely analogous to computation in the class group and consists of "composition" followed by "reduction", we shall present formulas which are (asymptotically) more efficient than those used for the class group. In particular, our reduction procedure will use the Euclidean algorithm and be faster (when the genus is large) than the classical reduction procedure due to Gauss. A modification of it can be used for computation in the class group of an algebraic number field.

By a *hyperelliptic* curve we shall mean, as usual, a curve $\mathbf{C}$ (with a model) of the form $v^2 = f(u)$, where $f(u)$ is a polynomial of degree $2g + 1$, with all roots distinct, and with coefficients in a field K of characteristic $\neq 2$; here g is a positive integer (the *genus* of the the curve $\mathbf{C}$).

Received May 16, 1986; revised July 3, 1986.

1980 *Mathematics Subject Classification*. Primary 10A30, 68C20.

*This research was supported in part by the National Security Agency.

2. Preliminaries. We summarize here the facts about the Jacobian of **C** that we shall use; see, for example, Mumford [6] for more details. Note that Mumford works over the field of complex numbers; however, the results that we use, and their proofs, are valid over any algebraically closed field of characteristic $\neq 2$ (indeed, they are true in fields of characteristic 2, also, if appropriate modifications of the statements are made). By a point P on **C** we mean a pair (x, y) of elements of A (the algebraic closure of K) satisfying $y = f(x)$ or one other element, conventionally denoted ∞. If σ is an automorphism of A, P^σ denotes (x^σ, y^σ) (with ∞^σ defined to be ∞). A *divisor* D of **C** is a finite formal sum of the form $D = \sum_i m_i P_i$, where the m_i are integers and the P_i are points of **C**; the *degree* of D is $\sum_i m_i$. We define $D^\sigma = \sum_i m_i P_i^\sigma$ and say that D is $\geqslant 0$ if all of the m_i are $\geqslant 0$.

Since $v^2 = f(u)$ on the curve **C**, any polynomial $p = p(u, v)$, when considered as a function on **C**, can be written in the form $p = a + bv$, where $a = a(u)$ and $b = b(u)$ are polynomials in u. If p vanishes at the point (x, y) (so that $y^2 = f(x)$), then the *order* of the zero (x, y) of p is the exponent of the highest power of $(u - x)$ which divides $a^2 - b^2 f$.

By a *function* on **C** we shall mean a rational function of the form $h = h(u, v) = p/q$, where $p = p(u, v)$ and $q = q(u, v)$ are polynomials in $K[u, v]$ such that $q(u, v)$ is not divisible by $v^2 - f(u)$. The function h has a finite number of zeros and poles on **C**, and we associate with h its divisor $(h) = \sum_i m_i P_i$, where the P_i are the zeros and poles of h (on **C**) with multiplicities m_i (positive if P_i is a zero of h and negative if it is a pole); a divisor of a nonzero function, such as (h), is called *principal*; a principal divisor has degree 0. The divisors form an additive group $\mathbf{D}$ (under formal addition: $\sum_i m_i P_i + \sum_i n_i P_i = \sum_i (m_i + n_i) P_i$) and the divisors of degree 0 form a subgroup $\mathbf{D}_0$. We define $\gcd(\sum_i m_i P_i, \sum_i n_i P_i)$ to be $\sum_i \min(m_i, n_i) P_i$. The principal divisors form a subgroup $\mathbf{P}$ of $\mathbf{D}_0$, and the Jacobian $\mathbf{J}$ of **C** is defined to be the quotient group $\mathbf{J} = \mathbf{D}_0/\mathbf{P}$. This is analogous to the definition of the class group of an algebraic number field as the quotient of the group of ideals modulo group of principal ideals. If D_1 and D_2 are principal divisors, we shall write $D_1 \equiv D_2 \pmod{\mathbf{P}}$ if D_1 is equivalent to D_2 in the Jacobian (i.e., $D_1 - D_2 \in \mathbf{P}$).

If $P = (x, y)$ is a point on the curve, then so is $P' = (x, -y)$. The points P and P' are the zeros of the function $(u - x)$, which has a double pole at ∞. Thus the divisor $P + P' - 2 \cdot \infty \equiv 0 \pmod{\mathbf{P}}$ or $-P' \equiv P - 2 \cdot \infty \pmod{\mathbf{P}}$. It follows that each element of $\mathbf{J}$ can be represented in the form

$$D = \sum_{i=1}^{r} P_i - r \cdot \infty$$

with the following condition satisfied: If the point $P_i = (x_i, y_i)$ appears in D, then the point $P_i' = (x_i, -y_i)$ does not appear as one of the P_j $(j \neq i)$. This implies, in particular, that points of the form $(x, 0)$ appear at most once in D. We shall call such a divisor *semireduced*. It follows from the Riemann-Roch Theorem [3] that each element of $\mathbf{J}$ can be represented uniquely by such a divisor, subject to the additional restriction that $r \leqslant g$. Such divisors will be called *reduced*. Any semireduced divisor D can be represented uniquely by a pair of polynomials $(a(u), b(u))$ satisfying $D = \gcd((a), (b - v))$, where $a = a(u) = \prod(u - x_i)$ and $b = b(u)$ is the unique polynomial of degree $< \deg(a)$, satisfying $b(x_i) = y_i$ $(1 \leqslant i \leqslant r)$, with appropriate multiplicity when the point P_i appears more than once in D. Explicitly, if P_i appears k times in D, then $b - y_i$ must be divisible by $(u - x_i)^k$. This is equivalent to requiring that $b^2 - f$ be divisible by a. We shall denote this divisor D by $\operatorname{div}(a, b)$. Note that D is reduced if and only if $\deg(a)$ is $\leqslant g$. If we define $c = (b^2 - f)/a$, then the representation (a, b, c) of D is analogous to the similar representation of the quadratic form $aX^2 + 2 \cdot bXY + cY^2$ with discriminant f. If a and b have coefficients in K, we shall call the divisor D *rational* over K. If K is perfect, then D will be rational over K if and only if $D = D^\sigma$ for all automorphisms σ of A over K. The set of principal divisors which are rational over K forms a subgroup of the group of principal divisors; its image $\mathbf{J}_K$ in $\mathbf{J}$ is a subgroup of $\mathbf{J}$, and it is $\mathbf{J}_K$ which is useful in computational number theory. If the genus $g = 1$, then a is a linear polynomial $u - x$ and b is a constant y; in this case, $\mathbf{J}$ is isomorphic to $\mathbf{C}$, and the reduced divisor (a, b), considered as an element of $\mathbf{J}$, corresponds to the point (x, y) on $\mathbf{C}$ (which is an elliptic curve); the elements of $\mathbf{J}_K$ correspond to those points of $\mathbf{C}$ with coordinates in K. Henceforth, we shall not distinguish between an element of $\mathbf{J}$ and its reduced representative $\operatorname{div}(a, b)$.

To add two elements $D_1 = \operatorname{div}(a_1, b_1)$ and $D_2 = \operatorname{div}(a_2, b_2)$ of $\mathbf{J}$, we proceed as in the classical composition of quadratic forms. We shall obtain a (semireduced) representative for the sum of the two divisors and then reduce it.

3. Composition. We will describe the algorithm and then verify its correctness.

Use the Euclidean algorithm twice, first to compute $d_0 = \gcd(a_1, a_2)$ and then $d = \gcd(d_0, b_1 + b_2) = \gcd(a_1, a_2, b_1 + b_2)$ and polynomials h_1, h_2, h_3 satisfying

$$(\mathrm{C}_1) \qquad d = h_1a_1 + h_2a_2 + h_3(b_1 + b_2).$$

(Note that "$\gcd(a_1, a_2)$" is used here to denote the ordinary greatest common divisor of the two polynomials $a_1 = a_1(u)$ and $a_2 = a_2(u)$, as polynomials in u; earlier, the term "gcd" was used to denote the greatest common divisor of two divisors on $\mathbf{C}$. The meaning will be clear from the context.) Then compute

$$(\mathrm{C}_2) \qquad a = a_1a_2/d^2$$

and

$$(\mathrm{C}_3) \quad b \equiv \left(h_1a_1b_2 + h_2a_2b_1 + h_3 \cdot (b_1b_2 + f)\right)/d \pmod{a}, \deg(b) < \deg(a).$$

Then $\operatorname{div}(a, b)$ is semireduced and represents the divisor sum (in the Jacobian); cf. Schnorr and Lenstra [7], and Shanks [9]. We shall indicate some simplifications shortly.

We first verify correctness. As usual, if $c = c(u)$ is a polynomial in one variable u, then $\operatorname{ord}_x(c)$ denotes the largest integer r for which $(u - x)^r$ divides c.

Using (C_1), we can rewrite (C_3) as

$$(\mathrm{C}_{3\mathrm{a}}) \quad \begin{aligned} b &\equiv \left(b_2(d - h_2a_2 - h_3(b_1 + b_2)) + h_2a_2b_1 + h_3(b_1b_2 + f)\right)/d \\ &\equiv b_2 + h_2a_2(b_1 - b_2)/d + h_3\left(f - b_2^2\right)/d. \end{aligned}$$

Since $f - b_2^2 \equiv 0 \pmod{a_2}$, the division in formula (C_3) is exact, so that b is a polynomial. We can multiply $(\mathrm{C}_{3\mathrm{a}})$ by $(b_1 + b_2)$ and simplify to obtain

$$(b_1 + b_2)b = b_1b_2 + f + \left(h_1a_1\left(b_2^2 - f\right) + h_2a_2\left(b_1^2 - f\right)\right)/d$$

or, since $v^2 = f$,

$$\begin{aligned}(b_1 + b_2)(b - v) = {} & (b_1 - v)(b_2 - v) \\ & + \big(h_1 a_1\big(b_2^2 - f\big) + h_2 a_2\big(b_1^2 - f\big)\big)/d.\end{aligned} \tag{C$_{3\text{b}}$}$$

Case A. Suppose that the point $P = (x, y)$ has multiplicity $r_h \geqslant 0$ in D_h, $h = 1$, 2, and if $y \neq 0$, then $-P = (x, -y)$ does not occur in either. We will show that

(i) $\operatorname{ord}_x(a) = r$, where $r = r_1 + r_2$ if $y \neq 0$; while r is 0 or 1 and $\equiv r_1 + r_2 \pmod 2$ if $y = 0$, and

(ii) $\operatorname{ord}_x(b - y)$ is $\geqslant r$.

There are several subcases:

1. The multiplicities $r_1 = r_2 = 0$. In this case it follows from Eq. (C$_2$) that $\operatorname{ord}_x(a) = 0$.

2. At least one of r_1, r_2 is positive and $y \neq 0$. In this case $\operatorname{ord}_x(d_0) = 0$ and hence, by (C$_2$), $\operatorname{ord}_x(a) = r$, verifying (i). Each term on the right of (C$_{3\text{b}}$) has order $\geqslant r$ and since $b_1(x) + b_2(x) = 2 \cdot y \neq 0$, we obtain $\operatorname{ord}_x(b - v)$ is $\geqslant r$.

3. Both r_1, r_2 are positive and $y = 0$. In this case $r_1 = r_2 = 1$; $\operatorname{ord}_x(a_1) = \operatorname{ord}_x(a_2) = \operatorname{ord}_x(d) = 1$. By (C$_3$), $a(x) \neq 0$, verifying (i) and (ii) with $r = 0$.

4. Exactly one of r_1, r_2 is positive and $y = 0$. In this case $d(x) \neq 0$. Hence $\operatorname{ord}_x(a) = 1$ and, as in subcase 2, each term on the right of (C$_{3\text{b}}$) has order $\geqslant 1$ and since $b_1(x) + b_2(x) = 2 \cdot y \neq 0$, we find that $\operatorname{ord}_x(b - v)$ is $\geqslant 1$, verifying (i) and (ii) with $r = 1$.

Case B. Now suppose that $P = (x, y)$ has multiplicity $r_1 > 0$ in D_1 and $-P = (x, -y)$ has multiplicity $r_2 > 0$ in D_2. Put $r = |r_1 - r_2|$. We will show that

(i) $\operatorname{ord}_x(a) = r$, and

(ii) if $r_1 \geqslant r_2$, then $\operatorname{ord}_x(b - y)$ is $\geqslant r$ while if $r_1 \leqslant r_2$, then $\operatorname{ord}_x(b + y)$ is $\geqslant r$.

For $\operatorname{ord}_x(b_1 + b_2) \geqslant \min(r_1, r_2)$ and $\operatorname{ord}_x(d) = \min(r_1, r_2)$; hence $\operatorname{ord}_x(a) = r_1 + r_2 - 2 \cdot \min(r_1, r_2) = r$, verifying (i). Assume, without loss of generality, that $r_2 \geqslant r_1$. Now $\operatorname{ord}_x(b_2 - y) \geqslant r_2$, $\operatorname{ord}_x(h_2 a_2(b_1 - b_2)) = r_2$, and $\operatorname{ord}_x(h_3(f - b_2^2)/d) \geqslant r_2 - r_1$. Hence using (C$_{3\text{a}}$), $\operatorname{ord}_x(b - y)$ is $\geqslant r$, verifying (ii).

If classical algorithms are used, then the computation of the product of two polynomials of degree m and the computation of their gcd each take $O(m^2)$ field operations, while if modern "fast" algorithms are used, then the computation of their product takes $O(m \log m)$ operations and the computation of their gcd takes $O(m(\log m)^2)$ operations [1]. It follows that the composition algorithm takes $O(g(\log g)^2)$ operations.

For computational purposes, in the important special case when $\gcd(a_1, a_2) = 1$ (which is extremely likely if the ground field K is large and a_1 and a_2 are the coordinates of two randomly chosen elements of the Jacobian), we find that $d = 1$ and (C$_3$) may be replaced by the simpler

$$b \equiv h_1 a_1 b_2 + h_2 a_2 b_1 \pmod a, \ \deg(b) < \deg(a), \tag{C$_4$}$$

or equivalently,

$$b \equiv b_2 + h_2 a_2 (b_1 - b_2) \pmod a, \ \deg(b) < \deg(a). \tag{C$_{4\text{a}}$}$$

In the special case when $\operatorname{div}(a_1, b_1) = \operatorname{div}(a_2, b_2)$ ("doubling" an element of **J**), we may choose $h_2 = 0$ and then (C$_3$) simplifies to

$$b \equiv h_1 a_1 b_1 + h_3\big(b_1^2 + f\big)/d \pmod a, \ \deg(b) < \deg(a), \tag{C$_5$}$$

or equivalently,

$$(\mathrm{C}_{5\mathrm{a}}) \qquad b \equiv b_1 + h_3(f - b_1^2)/d.$$

4. Reduction. We describe algorithms for reducing the semireduced divisor D represented by $\operatorname{div}(a, b)$ to the reduced form described above, in which $\deg(a)$ is $\leqslant g$. The classical Gauss algorithm for reducing quadratic forms may be applied here. We may replace $D = \operatorname{div}(a, b)$ by the equivalent divisor $E = -((b - v) - D) = \operatorname{div}(a', b')$, where $a' = (f - b^2)/a$, $b' \equiv -b \pmod{a'}$, and $\deg(b') < \deg(a)$.

If $\deg(a) = m$, $\deg(b) = n$, with $m > n$, then $\deg(a') = \max(2g + 1, 2) - m$. If $m > g + 1$, then $\deg(a') \leqslant 2(m - 1) - m = m - 2$ and if $m = g + 1$, then $\deg(a') \leqslant g$.

We may apply this reduction method repeatedly until $\deg(a') \leqslant g$. In the worst case (which, both in probability and in common calculation, is the most common case) where all inequalities are, in fact, equalities, and $\deg(a)$ is initially $2 \cdot g$, this method of reduction requires g long divisions (to compute the polynomials a' and b'). Explicitly, the computation of a' requires division of a polynomial of degree $2 \cdot m - 2$ by a polynomial of degree m and the computation of b' requires division of a polynomial of degree m by a polynomial of degree $m - 2$. Here m is initially $2 \cdot g$ and decreases by 2 until it is $\leqslant g$. If classical algorithms are used, then this reduction requires (asymptotically) $O(g^3)$ field operations, while if modern "fast" algorithms are used, then it requires $O(g^2 \cdot \log g)$ field operations.

We now describe a new reduction algorithm which is (asymptotically) faster by a factor of g. We shall do this by finding a function of the form $c - dv$, where c and d are nonzero polynomials, such that the divisor $E = -((c - dv) - D)$ is reduced. We must choose c and d so that E is $\geqslant 0$. This will be true if a divides $(c^2 - d^2 f)$. Since a divides $(b^2 - f)$, it will divide $(c^2 - d^2 f)$ if $c \equiv db \pmod{a}$. We will choose c and d so that $\deg(c) \leqslant (m + g)/2$ and $\deg(d) \leqslant (m - g - 1)/2$; then E will have degree $\leqslant g$.

If $\deg(b) \leqslant (m - g - 1)/2$, then we may put $c = b$ and $d = 1$. Otherwise, we shall obtain them by means of the Euclidean algorithm. To this purpose, define sequences of polynomials $a_{-2}, a_{-1}, a_0, \ldots$ and $q_0, q_1, q_2, \ldots$, by setting

$$a_{-2} = a, \qquad a_1 = b,$$

and successively for $i = 0, 1, 2, \ldots$, setting

$$a_{i-2} = -q_i a_{i-1} + a_i,$$

where q_i is a polynomial of degree $(\deg(a_{i-2}) - \deg(a_{i-1}))$, and $\deg(a_i) < \deg(a_{i-1})$. (Use of the minus sign in the above formula defining q_i will simplify subsequent formulas.) Now define

$$r_{-2} = 1, \quad r_{-1} = 0, \quad s_{-2} = 0, \quad s_{-1} = 1,$$

and inductively for $i = 0, 1, 2, \ldots$, define

$$r_i = q_i r_{i-1} + r_{i-2}, \qquad s_i = q_i s_{i-1} + s_{i-2}.$$

Then

$$a_{-2} = r_{-2}a + s_{-2}b, \qquad a_{-1} = r_{-1}a + s_{-1}b,$$

and, inductively for $i = 0, 1, 2, \ldots$,

$$\begin{aligned} a_i = q_i a_{i-1} + a_{i-2} &= q_i(r_{i-1}a + s_{i-1}b) + (r_{i-2}a + s_{i-2}b) \\ &= (q_i r_{i-1} + r_{i-2})a + (q_i s_{i-1} + s_{i-2})b = r_i a + s_i b. \end{aligned}$$

One can then verify the following formulas for $i = 0, 1, 2, \ldots,$

$$\deg(r_i) = \sum_{h=1}^{i} \deg(q_h), \qquad \deg(s_i) = \sum_{h=0}^{i} \deg(q_h) = \deg(a) - \deg(a_{i-1}),$$

and $r_{i-2}s_{i-1} - r_{i-1}s_{i-2} = (-1)^i$. Now let i be the least integer $\geqslant 0$ such that $\deg(a_i) \leqslant (m + g)/2$. Then $\deg(s_j) = m - \deg(a_{i-1}) < m - (m + g)/2$; hence $\deg(s_j) \leqslant (m - g - 1)/2$. Put $c = a_i$, $d = s_i$, and $\lambda = r_i$. With these choices $c = \lambda a + db$, where the degrees of c and d are as specified above.

We now describe the reduction algorithm. Suppose $D = \operatorname{div}(a, b)$ is a divisor of (arbitrary) degree m. The following algorithm will reduce D in one step.

(R_1) Use the Euclidean algorithm, as above, to obtain c and d.

(R_2) Put $a_2 = \gcd(c, d)$ $(= \gcd(a, d))$ and define $a_1 = a/a_2$, $c_1 = c/a_2$, and $d_1 = d/a_2$.

(R_3) Put $a_3 = (c_1^2 - d_1^2 f)/a_1$ and compute d' so that $dd' \equiv 1 \pmod{a_3}$.

(R_4) Let E be the divisor which is the sum of $E_1 = \operatorname{div}(a_3, -d'c_1)$ and $E_2 = \operatorname{div}(a_2, b)$ (computed using the composition algorithm).

Then E is reduced and equivalent to D.

We now prove correctness. First $c_1 = \lambda a_1 + bd_1$. Then $D = D_1 + E_2$, where $D_1 = \operatorname{div}(a_1, b) = \gcd((a_1), (b - v))$ and $E_2 = \operatorname{div}(a_2, b) = \gcd((a_2), (b - v))$. Since $\gcd(a_1, d_1) = 1$, we have $D_1 = \gcd((a_1), (d_1 b - d_1 v)) = \gcd((a_1), (c_1 - d_1 v))$. Thus $D_1 \equiv -D_3 \pmod{\mathbf{P}}$, where $D_3 = (c_1^2 - d_1^2 f) - D_1 = -\gcd((a_3), (c_1 - d_1 v))$. Since $\gcd(c_1, d_1) = 1$ and $\gcd(a_3, d_1) = 1$, there exists a polynomial d' such that $d'd_1 \equiv 1 \pmod{a_3}$ and $D_3 = -\gcd((a_3), (d'c_1 + v)) = E_1$. Thus $E \equiv D \pmod{\mathbf{P}}$. Put $n = \deg(a_2)$. Then

$$\begin{aligned}\deg(a_3) &= \max(2 \cdot \deg(c_1), 2 \cdot \deg(d_1) + \deg(f)) - \deg(a_1)\\ &\leqslant \max(m + g - 2 \cdot n, m + g - 2 \cdot n) - (m - n) = g - n.\end{aligned}$$

Thus $\deg(E_1) \leqslant g - n$ and $\deg(E_2) = n$. Hence $\deg(E) \leqslant g$ and E is reduced.

The number of steps required by this algorithm is determined by the number of steps required to compute the gcd of two polynomials of degree m. Hence, if classical algorithms are used, then this reduction takes $O(m^2)$ steps, while if modern "fast" algorithms are used, then it takes $O(m(\log m)^2)$ steps, i.e., asymptotically the same number of steps as is taken by the composition algorithm when applied to two divisors of degree m.

In [8] Seysen describes a simplification of the classical reduction algorithm. The number of steps it requires is of the same order of magnitude as the classical reduction algorithm. However, as is often the case for algorithms which are asymptotically faster, in "small" cases (i.e., when the genus is small) his algorithm will be preferable to the asymptotically faster algorithm described here.

Department of Mathematics
University of California
Los Angeles, California 90024

1. ALFRED V. AHO, JOHN E. HOPCROFT & JEFFREY D. ULLMAN, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Mass., 1974.

2. D. V. CHUDNOVSKY & G. V. CHUDNOVSKY, *Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests*, Research report RC 11262 (#50739), IBM Thomas J. Watson Research Center, Yorktown Heights, N. Y., 1985.

3. SERGE LANG, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.

4. H. W. LENSTRA, JR., "Factorization using elliptic curves." (To be published.)

5. PETER MONTGOMERY, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp.*, v. 48, 1977, pp. 243–264.

6. DAVID MUMFORD, *Tata Lectures on Theta II*, Birkhäuser, Boston, 1984, ISBN 0-8176-3110-0.

7. C. P. SCHNORR & H. W. LENSTRA, JR., "A Monte Carlo factoring algorithm with linear storage," *Math. Comp.*, v. 43, 1984, pp. 289–311.

8. MARTIN SEYSEN, "A probabilistic factorization algorithm with quadratic forms of negative discriminant," *Math. Comp.* (To appear.)

9. DANIEL SHANKS, *Class Number, A Theory of Factorization, and Genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 415–440.

10. H. C. WILLIAMS, G. W. DUECK & B. K. SCHMID, "A rapid method of evaluating the regulator and class number of a pure cubic field," *Math. Comp.*, v. 41, 1983, pp. 235–286.