MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 178
APRIL 1987, PAGES 757–780

A Probabilistic Factorization Algorithm with Quadratic Forms of Negative Discriminant

By Martin Seysen

Abstract. We propose a probabilistic algorithm for factorization of an integer N with run time $(\exp\sqrt{\log N \log\log N})^{\sqrt{5/4}+o(1)}$. Asymptotically, our algorithm will be as fast as the well-known factorization algorithm of Morrison and Brillhart. The latter algorithm will fail in several cases and heuristic assumptions are needed for its run time analysis. Our new algorithm will be analyzed under the assumption of the Extended Riemann Hypothesis and it will be of Las Vegas type. On input N, the new algorithm will factor N with probability $\geq \frac{1}{2}$. In case of prime N the algorithm will prove the primality of N with probability $\geq \frac{1}{2}$.

Introduction. Until the last decade, the centuries-old problem of factoring integers was mainly a problem for specialists. Worldwide interest in factoring integers increased dramatically in 1978, when Rivest, Shamir, and Adleman [32] published their public key cryptosystem, whose security relies on the fact that some large integers are hard to factor.

Gauss [9] already discovered a close connection between the factorization of a natural number N and the theory of quadratic forms of discriminant $-4N$. Now, quadratic forms are one of the most important tools for factoring integers. Examples for efficient factorization algorithms are (among others) the algorithms of Morrison and Brillhart [26] and Lenstra and Schnorr [22]. The former works with the continued fraction expansion of $\sqrt{N}$ (which is closely related to the theory of quadratic forms of discriminant $4N$, see [20]) while the latter works with quadratic forms of discriminant $-4N$. At present, the most efficient factorization algorithm is the quadratic sieve algorithm, see [29], which can also be expressed in terms of quadratic forms. For an overview of modern factorization algorithms we refer to the papers of Guy [10], Monier [25], and Pomerance [29].

A deeper understanding of the theory of quadratic forms is of great importance for the analysis of modern factorization algorithms. In this paper we shall only deal with the theory of quadratic forms of negative discriminant, which is considerably more simple than the theory of forms of positive discriminants. Using this theory, we obtain a probabilistic factorization algorithm with run time $(\exp\sqrt{\log N \log\log N})^{\sqrt{5/4}}$ (in this paper we denote by $\log X$ the natural logarithm of X). We have $\sqrt{5/4} \sim 1.118$.

Received May 17, 1985; revised June 12, 1986.
1980 *Mathematics Subject Classification.* Primary 10A30, 68C25.

0025-5718/87 $1.00 + $.25 per page

Pomerance [29] obtains the same run time for a variant of the factorization algorithm of Morrison and Brillhart. While Pomerance uses heuristic assumptions for his proofs, our probabilistic algorithm will be analyzed solely under the assumption of the Extended Riemann Hypothesis (ERH). Our new algorithm will be of Las Vegas type: On input N, it will give the complete factorization of N with probability $\geqslant \frac{1}{2}$. In case of prime N it will prove the primality of N (provided that ERH is true). Note that all previously known factorization algorithms of comparable run time never yield a proof of primality.

We need the Extended Riemann Hypothesis to get an effective version of the Chebotarev density theorem, see [14], [15] for details. There are also unconditional effective versions of the Chebotarev density theorem, see [14], [15], but they are not sufficiently sharp for our purposes.

At present, the asymptotically fastest probabilistic factorization algorithm is the algorithm of Dixon [8]. A variant of that algorithm has run time $(\exp \sqrt{\log N \cdot \log\log N})^{\sqrt{5/2}+o(1)}$. (We have $\sqrt{5/2} \sim 1.581$.)

Our new algorithm is not designed for implementation; its purpose is to give a deeper understanding of the run time behavior of the algorithms similar to the Morrison-Brillhart algorithm.

I am greatly indebted to Professor Dr. C. P. Schnorr for valuable hints and critical discussions of the subject.

1. The Idea Behind the New Factorization Algorithm. Gauss [9] introduced a binary operation "composition" on the set QF_Δ of binary integral quadratic forms of discriminant Δ. This composition gives the set C_Δ of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of QF_Δ the structure of a finite Abelian group called the class group. The cardinality h_Δ of this group is called the class number. In case $\Delta < 0$ we can effectively determine a representative of each class in C_Δ. This allows us to do computations in the class group. Furthermore, Gauss [9] established a correspondence between the ambiguous classes (i.e., classes which are square roots of the unit class) and the disjoint factorizations of the discriminant.

Shanks [38] developed methods for computing the class group and used ambiguous forms for factoring the discriminant. Under the assumption of the ERH these ideas yield a factorization algorithm with run time $O(N^{1/5})$, cf. Schoof [36].

In the sequel, let

$$L(x) := \exp\sqrt{\log x \cdot \log\log x} \tag{1.1}$$

for all $x \in \mathbf{R}$, $x > e$. Schnorr [34] introduced a probabilistic factorization algorithm using the class group C_Δ, $\Delta = -N$ (or $\Delta = -3N$). In order to compute C_Δ, he introduced a system of prime classes $I_{p_1,\Delta}, \ldots, I_{p_n,\Delta} \in C_\Delta$ (with $n = L(N)^{1/\sqrt{3}+o(1)}$) generating the class group. He used a probabilistic algorithm to obtain relations between these generators and he constructed ambiguous forms by combining these relations. He proved an upper bound of $L(N)^{\sqrt{3}+o(1)}$ for the run time of his algorithm, using heuristic assumptions. By the methods of Pomerance [29] this upper bound can be improved to $L(N)^{\sqrt{5/4}+o(1)}$.

Under the assumption of the ERH, Schoof [36] proved that the first $O(\log^2|\Delta|)$ prime classes $I_{p_i,\Delta}$ will already generate the whole class group C_Δ.

In order to compute C_Δ, we construct a generating system $(I_{p_1,\Delta}, \ldots, I_{p_n,\Delta})$ of C_Δ with $n = O(\max[\log^2|\Delta|,\ L(|\Delta|)^{1/\sqrt{8}}])$. Based on the ideas of Schnorr [34], we will

construct n linearly independent relations between these generators of C_Δ by means of a probabilistic algorithm. Then C_Δ is a homomorphic image of the free Abelian group generated by the n prime forms $I_{p_j,\Delta}$, $j = 1, \ldots, n$. In the sequel, the latter group will be identified with the additive group of the lattice $\mathbf{Z}^n$. Then the kernel of the above homomorphism is a sublattice Γ of $\mathbf{Z}^n$. Obviously, the index of Γ in $\mathbf{Z}^n$ is the class number h_Δ. Consider the lattice Λ generated by the vectors of $\mathbf{Z}^n$ corresponding to the n linearly independent relations computed above. Λ is a sublattice of Γ with finite index in Γ. Hence the index H of Λ in $\mathbf{Z}^n$ is a multiple of the class number h_Δ. The index H is the determinant of the coefficients of the n relations in C_Δ.

Once a multiple H of the class number is found, we can easily obtain a generating system of the 2-Sylow group $S_{2,\Delta}$ of the class group simply by raising each generator of C_Δ to the $\overline{H}$th power, where $\overline{H}$ is the odd part of H. Using the methods of Lenstra and Schnorr [22], we will obtain the complete factorization of Δ from any generating system of $S_{2,\Delta}$.

In order to analyze the algorithm, which generates relations in the class group, we need some elementary lattice theory and some information about the distribution of prime forms, which at present is only available under the assumption of the ERH. Altogether, we obtain a probabilistic factorization algorithm with run time $L(N)^{\sqrt{2}+o(1)}$. Using some more sophisticated techniques, as discussed in Sections 7 and 8, we can improve the run time to $L(N)^{\sqrt{5/4}+o(1)}$.

2. Quadratic Forms with Negative Discriminant. Let N be an odd natural number. We want to find the complete factorization of N. Without loss of generality, we assume $N = -1 \bmod 4$. (Otherwise, we factor $3N$ instead of N.) Let QF_{-N} be the set of positive binary integer primitive quadratic forms $aX^2 + bXY + cY^2$, $a, b, c \in \mathbf{Z}$, $\gcd(a, b, c) = 1$, $a > 0$, with discriminant $-N = b^2 - 4ac$. [Notation (a, b, c) or (a, b), $c = (b^2 + N)/(4a)$.] Note that QF_{-N} is nonempty if and only if $-N = 0$ or $1 \bmod 4$.

In this paper we only deal with negative discriminants. For the more complicated theory of quadratic forms with positive discriminant we refer to [2] and [21].

Two forms (a, b, c) and (a', b', c') are called equivalent if and only if there is a 2×2-matrix $A \in \mathrm{SL}_2(\mathbf{Z})$ with determinant 1 such that

$$\begin{pmatrix} b'/2 & c' \\ a' & b'/2 \end{pmatrix} = A^T \begin{pmatrix} b/2 & c \\ a & b/2 \end{pmatrix} A.$$

For $f \in QF_{-N}$ let $[f]$ be its $\mathrm{SL}_2(\mathbf{Z})$-equivalence class and let C_{-N} be the set of equivalence classes in QF_{-N}. C_{-N} is a finite Abelian group with respect to an operation called "composition" defined as follows (see [21]):

$$\begin{aligned} &[(a_1, b_1, c_1)] \cdot [(a_2, b_2, c_2)] = [(a_3, b_3, c_3)] \quad \text{with} \\ &a_3 = a_1 a_2 / d^2; \quad b_3 = b_2 + 2\frac{a_2}{d} R; \quad c_3 = \frac{b_3^2 + N}{4a_3} \quad \text{with } d, R \text{ such that:} \\ &d = \gcd\left(a_1, a_2, \frac{b_1 + b_2}{2}\right) = \lambda a_2 + \mu a_1 + \nu \frac{b_1 + b_2}{2}; \qquad \lambda, \mu, \nu \in \mathbf{Z}; \\ &R = \lambda \frac{b_1 - b_2}{2} - \nu c_2. \end{aligned} \tag{2.1}$$

The group C_{-N} is called the *class group*, its cardinality h_{-N} is called the *class number* of the discriminant $-N$. The class number can be bounded by the following old theorem of Schur [37] (see also [21]).

THEOREM 2.2. *For any discriminant $-N$ with $N > 4$ one has*

$$h_{-N} < \frac{\sqrt{N}}{\pi} \cdot \left(\frac{\log N}{2} + \log\log N + 1 \right) < \frac{1}{2} \cdot \sqrt{N} \cdot \log N.$$

A form (a, b, c) is called reduced if

$$|b| \leqslant a \leqslant c \quad \text{and} \quad (b \geqslant 0 \text{ or } |b| < a < c).$$

Gauss [9] already proved

THEOREM 2.3. *Each class $[f]$ in C_{-N} contains exactly one reduced form.*

In the sequel we identify C_{-N} with the set of reduced forms in QF_{-N}. The following algorithm gives the reduced form in the class of (a, b, c) in at most $O(\max\{1, \log a/N\})$ steps (see [13] or [35]):

While (a, b, c) is not reduced *do*
begin choose $\lambda \in \mathbf{Z}$ such that $-a \leqslant b + 2\lambda a < a$;
$(a, b, c) := (c + \lambda b + \lambda^2 a, -b - 2\lambda a, a)$
end.

The composition formula (2.1), Theorem 2.3 and the above reduction algorithm yield an effective composition algorithm for reduced forms.

A reduced form $f \in QF_{-N}$ is called *ambiguous* if $[f]^2 = 1_{C_{-N}}$.

THEOREM 2.4. *For each negative discriminant $-N$ with $-N \equiv 1 \bmod 4$ there is a bijective correspondence between the set of ambiguous forms in QF_{-N} and the set $\{(p, q) \in \mathbf{Z}^2 : n = p \cdot q, \gcd(p, q) = 1, p < q\}$ of factorizations of N into two coprime factors.*

For a proof of Theorem 2.4 see [9] or [24]. For a complete enumeration of ambiguous forms of negative discriminant see [22]. The correspondence in Theorem 2.4 can be pictured as follows:

$$N = p \cdot q \sim \left(p, p, \frac{p+q}{4} \right) \qquad \text{if } 3p \leqslant q,$$

$$N = p \cdot q \sim \left(\frac{p+q}{4}, \frac{p-q}{4}, \frac{p+q}{4} \right) \qquad \text{if } p < q < 3p.$$

Thus the construction of all ambiguous forms of discriminant $-N$ gives us the complete factorization of N. Note that the number of ambiguous forms may be quite large when N has many different very small prime factors. On the other hand, the very small prime factors of N can easily be found by trial division. For simplicity, we make the following assumptions.

Throughout the paper we let

$$L = L(N) = \exp\left(\sqrt{\log N \cdot \log\log N}\right),$$

and we assume that N has no factors less than L (apart from possibly one single factor 3). Then the reader will easily verify that there are at most $L^{o(1)}$ ambiguous forms in QF_{-N}.

Remark. In the sequel we shall use several procedures that help us to construct ambiguous forms. They will have run time $L^{c+o(1)}$, which is not polynomial in the binary length of N if c is any positive real number. Since we shall not bother about the $o(1)$-part in our run time analysis, we may use any reasonable machine model. For example, we may count the number of bit-operations on a Turing machine or we may count the number of arithmetic operations of numbers of size $O(N)$.

3. Outline of the New Factorization Algorithm. For any discriminant Δ and prime p let $(\frac{\Delta}{p})$ be the Kronecker symbol (see [16]),

$$\left(\frac{\Delta}{p}\right) := \begin{cases} 1 & \text{if } \Delta \text{ is a quadratic residue mod } 4p \text{ and } \gcd(\Delta, p) = 1, \\ 0 & \text{if } \gcd(\Delta, p) \neq 1, \\ -1 & \text{otherwise.} \end{cases}$$

Let N be fixed as in Section 2. For any prime p with $(\frac{-N}{p}) = 1$ let the *prime form* I_p be defined by $I_p := [(p, b_p)]$, where $b_p := \min\{b \in \mathbf{N}: b^2 = -N \bmod 4p\}$.

The following theorem is a simple consequence of the composition formula (2.1) and the definition of the Kronecker symbol (compare [34, fact 8 and Lemma 4]).

THEOREM 3.1. *Let $(a, b) \in QF_{-N}$ and let $a = \prod_{i=1}^{n} p_i^{e_i}$, $e_i \in \mathbf{N}$, p_i prime, be the prime factorization of a. Then*

(1) $(\frac{-N}{p_i}) = 1$, $b = \pm b_{p_i} \bmod 2p_i$ *for all* p_i, $i = 1, \ldots, n$ (*with* b_{p_i} *as above*);

(2) $[(a, b)] = \prod_{i=1}^{n} (I_{p_i})^{\pm e_i}$, *where the plus sign in the exponent* e_i *holds if and only if* $b = b_{p_i} \bmod 2p_i$.

Every form $(a, b) \in QF_{-N}$ with $\gcd(a, N) = 1$ can easily be factored into prime forms by Theorem 3.1, provided that the prime factorization of a is known.

Let the *prime form base* P_l, $l \in \mathbf{N}$, be defined as follows:

$$P_l := \left\{ I_p \in C_{-N}: p \text{ prime}, p \leqslant l, \left(\frac{-N}{p}\right) = 1 \right\}. \tag{3.2}$$

If we assume the Extended Riemann Hypothesis (ERH) to be valid, the following theorem gives us a finite generating system of C_{-N}.

THEOREM 3.3 (ERH). *There is an absolute, effectively computable constant c_1 such that $P_{c_1 \cdot \log^2 N}$ generates C_{-N}.*

Proof. See Schoof [36, Corollary 6.3].

Remark. Using the results of [27], one can show that Theorem 3.3 holds for $c_1 = 280$. Using the results of [1], c_1 can be improved to 2.

We choose a fixed prime form base P_l generating C_{-N}. Let n be the cardinality of P_l and let $p_1, \ldots, p_n$ be the primes $\leqslant l$ with $(-N/p) = 1$ in natural order.

Remark concerning the size of the prime form base. For factoring N we shall use a prime form base P_l with $l = L(N)^z$, where z is a fixed positive number. z will be optimized subject to certain conditions. Since $L(N)$ grows faster than any polynomial of $\log N$, the prime form base P_l generates the whole class group for sufficiently large N by Theorem 3.3. Hence, for asymptotic considerations we may always assume that P_l generates C_{-N}.

Let $\varphi: \mathbf{Z}^n \to C_{-N}$ be the homomorphism defined by

$$\varphi(x_1, \ldots, x_n) = \prod_{j=1}^{n} (I_{p_j})^{x_j}; \qquad (x_1, \ldots, x_n) \in \mathbf{Z}^n.$$

φ is surjective since P_l generates C_{-N}. An additive subgroup of $\mathbf{Z}^n$ will be called a lattice (in $\mathbf{Z}^n$). For example, $\ker\varphi$ is a lattice.

For any integer $k \times n$ matrix $A = (a_{ij})$, let $\Lambda(A)$ be the lattice generated by the row vectors of A:

$$\Lambda(A) := \mathfrak{a}_1\mathbf{Z} + \cdots + \mathfrak{a}_m\mathbf{Z} \quad \text{with } \mathfrak{a}_i = (a_{i1}, \ldots, a_{in});\ i = 1, \ldots, k.$$

A matrix A with $\Lambda(A) \subset \ker\varphi$ will be called a *form matrix*. Any form matrix (a_{ij}) satisfies

$$\prod_{j=1}^{n} \left(I_{P_j}\right)^{a_{ij}} = 1_{C_{-N}}; \qquad i = 1, \ldots, m.$$

The determinant of any form matrix A is a multiple of the class number h_{-N}, since C_{-N} is a factor group of $\mathbf{Z}^n/\Lambda(A)$.

In Section 4 we will prove under the assumption of the Extended Riemann Hypothesis:

THEOREM 3.4 (ERH). *There is a probabilistic algorithm with run time $L^{\sqrt{2}+o(1)}$ which on input N computes a nonsingular form matrix A for the prime form base P_l, $l = L^{1/\sqrt{8}}$, with probability $> \frac{1}{2}$. A has coefficients of size $O(N)$.*

Let A be a matrix as in Theorem 3.4. Using Hadamard's inequality (see [12]), we can easily obtain an upper bound of $\exp[O(n \cdot \log N)]$ for the determinant $\det A$. (Here $n = \#P_l = o(L^{1/\sqrt{8}})$.) Thus $\log\det A$ can be bounded by $L^{1/\sqrt{8}+o(1)}$.

We compute $\det A$ modulo $L^{1/\sqrt{8}+o(1)}$ different primes q_i of size $O(N)$. Using Gaussian elimination, this costs $L^{3\cdot 1/\sqrt{8}+o(1)}$ steps for each prime, i.e., $L^{\sqrt{2}+o(1)}$ steps in total. By combining these results with the Chinese remainder theorem, we easily obtain the exact value of $\det A$ in time less than $L^{\sqrt{2}+o(1)}$. This proves

THEOREM 3.5 (ERH). *There is a probabilistic algorithm with run time $L^{\sqrt{2}+o(1)}$ which computes a multiple H of the class number h_{-N} with $\log H = L^{1/\sqrt{8}+o(1)}$.*

Let $\overline{H}$ be the odd part of H. By raising each generator of the class group to its $\overline{H}$th power, we obtain a generating system of the 2-Sylow group $S_{2,-N}$ of C_{-N}. The 2-Sylow group of C_{-N} is defined by

$$S_{2,-N} = \left\{ f \in C_{-N} \mid \exists\, u \in \mathbf{N}\colon f^{2^u} = 1_{C_{-N}} \right\}.$$

The cost for computing a generating system of $S_{2,-N}$ is $L^{1/\sqrt{8}+o(1)}$. (Note that Theorem 3.3 gives us a generating system of C_{-N} of size $L^{o(1)}$.) Next we prove

THEOREM 3.6. *Given any generating system of $S_{2,-N}$ of cardinality r, we can compute all ambiguous forms in time $r \cdot L^{o(1)}$ (provided that N has at most one factor less than L).*

Proof. The assumptions of Theorem 3.6 imply that there are at most $L^{o(1)}$ ambiguous forms in C_{-N} (compare Section 2). Let $f_1, \ldots, f_r \in S_{2,-N} \setminus 1_{C_{-N}}$ be a generating system of the 2-Sylow group $S_{2,-N}$. From $f_1, \ldots, f_r$ we compute all

ambiguous forms of C_{-N} by the following algorithm:

ALGORITHM 3.7 (H. W. Lenstra, Jr., see [21])

1. *input* $f_1, \ldots, f_r$; $i := 1$; $\lambda := 0$
2. $\bar{f} := f_i$
3. compute $\bar{f}, \bar{f}^2, \ldots, \bar{f}^{2^{\log N}}$ and let $m := \min\{u \in \mathbf{N}: \bar{f}^{2^u} = 1_{C_{-N}}\}$; $g := \bar{f}^{2^{m-1}}$
4. *if* there exists $\alpha_1, \ldots, \alpha_\lambda \in \{0, 1\}$ with $g = \prod_{j=1}^{\lambda} g_j^{\alpha_j}$
   then compute the set J with $g = \prod_{j \in J} g_j$ and *goto* 5
   else $\lambda := \lambda + 1$; $\bar{f}_\lambda := \bar{f}$; $g_\lambda := g$; $m_\lambda := m$; *goto* 7.
5. *if* there exists a $j \in J$ with $m_j < m$ *then* choose a $k \in J$ with minimal m_k; exchange $\bar{f}$ with $\bar{f}_k$, g with g_k, m with m_k.
6. [now we have $g = \bar{f}_i^{2^{m-1}} = \prod_{j \in J} \bar{f}^{2^{m_j - 1}}$; and $m \leqslant m_j$ for all $j \in J$].
   $\bar{f} := \bar{f} \cdot \prod_{j \in J} \bar{f}^{2^{m_j - m}}$; *if* $\bar{f} \neq 1$ *then goto* 3 *else goto* 7.
   [the new m to be computed in step 3 will be smaller than the present m since $\bar{f}^{2^m} = 1$ holds for the new $\bar{f}$].
7. *if* $i = n$ *then output* all ambiguous forms generated by $g_1, \ldots, g_\lambda$ and *stop*
   else put $i := i + 1$ and *goto* 2.

Whenever the algorithm has run through step 4, the group generated by $\bar{f}_1, \ldots, \bar{f}_r$ is the direct product of the r different cyclic groups generated by $\bar{f}_i$, $i = 1, \ldots, r$, and, furthermore, the following properties hold:

$$2^{m_j} = \operatorname{ord}(\bar{f}_j); \quad \bar{f}_j^{2^{m_j - 1}} = g_j; \qquad j = 1, \ldots, n$$

(here $\operatorname{ord}(f)$ is the order of the class f in the class group C_{-N}).

When the algorithm has run k times through the main loop from step 2 to step 7, then all forms generated by $f_1, \ldots, f_k$ are contained in the group generated by $\bar{f}_1, \ldots, \bar{f}_\lambda$. Hence the algorithm outputs all ambiguous forms of C_{-N} when the input is a generating system of $S_{2,-N}$. This proves the correctness of Algorithm 3.7.

For the run time analysis of Algorithm 3.7 we remark that the main loop (from step 2 to step 7) is performed r times and the inner loop (from step 3 to step 7) is performed at most $O(\log h_{-N})$ times. The most expensive step is step 4. The run time of step 4 can be bounded by $L^{o(1)}$ since there are at most $L^{o(1)}$ ambiguous forms. Hence the algorithm has run time $r \cdot L^{o(1)}$.

This finishes the proof of Theorem 3.6. □

Theorem 3.5, the above discussion, and Theorem 3.6 yield a probabilistic algorithm which computes all ambiguous forms in the class group C_{-N}. Using the connection between ambiguous forms and factorization (see Theorem 2.4) we obtain

THEOREM 3.8 (ERH). *There is a probabilistic algorithm with run time* $L(N)^{\sqrt{2}+o(1)}$ *which computes the complete factorization of* N *with probability* $> \frac{1}{2}$.

Remark. All factorization algorithms considered in this paper are probabilistic. Apart from the number N to be factored, they take some input from a random source. By repeating the same algorithm (with different input from the random source) the probability of failure decreases exponentially with the number of repetitions. In our theorems we will always state the total amount of run time needed to factor N with probability at least $\frac{1}{2}$.

4. Generation of a Nonsingular Form Matrix. The purpose of this section is to prove Theorem 3.4. Let z be a fixed positive real number. In order to factor N we choose a prime form base P_l with $l = L(N)^z$. We want to compute a nonsingular form matrix for the prime form base P_l. A sufficient condition for a matrix (a_{ij}) to be nonsingular is that (a_{ij}) is strictly diagonally dominant, i.e., $|a_{ii}| > \sum_{j \neq i} |a_{ij}|$ for all i, see [41]. We prove

THEOREM 4.1. *There is a probabilistic algorithm with run time $L^{z+o(1)}$ which on input N, i computes the ith row vector of a strictly diagonally dominant form matrix with probability $> L^{-1/4z+o(1)}$. The coefficients of this row vector are of size $O(N)$.*

Proof of Theorem 3.4. By iterating the algorithm in Theorem 4.1 $L^{1/(4z)+o(1)} \cdot \log(l^z)$ times, we obtain an algorithm which succeeds with probability $> 1 - L^{-z}$. Altogether, we have to generate n, $n < L^z$, row vectors of the matrix. This gives us an algorithm for generating a form matrix with run time $L^{2z+1/(4z)+o(1)}$. Choosing $z = 1/\sqrt{8}$ yields Theorem 3.4. □

Proof of Theorem 4.1. Consider the prime form base P_l, $l = L(N)^z$. Let $n = n(N)$ be the cardinality of P_l, let $I_{p_1}, \ldots, I_{p_n}$ be the prime forms in natural order, and let r be the integral part of $\sqrt{N} + 1$.

On input N, i, the following probabilistic algorithm computes the ith row of a strictly diagonally dominant form matrix of the prime form base P_l.

ALGORITHM 4.2.

1. choose $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ with $0 \leqslant \alpha_1, \ldots, \alpha_n < r \cdot l$ at random and independently with respect to equidistribution
2. compute the reduced form $(a, b) \in (I_{p_j})^{2n \cdot r \cdot l} \cdot \prod_{j=1}^{n} (I_{p_j})^{\alpha_j}$
3. *if* there is a factorization $a = \prod_{j=1}^{n} p_j^{\beta_j}$, *then goto* 4 *else* fail and *stop*. (Here we factor a by trial division.)
4. compute $\gamma_j = \pm\beta_j$ such that $(a, b) \in \prod_{j=1}^{n} (I_{p_j})^{\gamma_j}$ according to Theorem 3.1. For $j = 1, \ldots, n$ let $a_{ij} = \alpha_j - \gamma_j + \delta_{ij} \cdot 2n \cdot r \cdot l$ (with $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$).
5. *output* $a_{i1}, \ldots, a_{in}$ and *stop*

Obviously, the run time of Algorithm 4.2 is bounded by $L^{z+o(1)}$, and in case of success (i.e., if the algorithm terminates in step 5) it computes coefficients $a_{i1}, \ldots, a_{in}$ of size $O(N)$ satisfying $\prod_{j=1}^{n} (I_{p_j})^{a_{ij}} = 1_{C_{-N}}$. (Note that $(I_{p_i})^{2n \cdot r \cdot l} \cdot \prod_{j=1}^{n} (I_{p_j})^{\alpha_j} = \prod_{j=1}^{n} (I_{p_j})^{\gamma_j}$ and $a_{ij} = \alpha_j - \gamma_j + \delta_{ij} \cdot 2n \cdot r \cdot l$ by construction.) Furthermore, $|a_{ii}| > \sum_{j \neq i} |a_{ij}|$ is satisfied.

Hence $(a_{i1}, \ldots, a_{in})$ is the ith row vector of a strictly diagonally dominant form matrix. It remains to compute the probability of success of Algorithm 4.2. For this, we have to prove two propositions.

PROPOSITION 4.3. *Let (a, b) be the form computed in step* 2 *of Algorithm* 4.2. *For any class $f \in C_{-N}$ the probability that (a, b) lies in f is at least $(1 - o(1))/h_{-N}$, where $o(1)$ is a function depending only on N with $o(1) \to 0$ for $N \to \infty$.*

Proposition 4.3 says that all classes in step 2 occur with approximately equal probability. In Section 5 we prove

PROPOSITION 4.4 (ERH). *The number of reduced forms* $(a, b) \in C_{-N}$ *such that* a *factors completely over the primes* $p_1, \ldots, p_n$ *of the prime form base* P_l, $l = L^z$, *is at least* $h_{-N} \cdot L^{-1/(4z)+o(1)}$.

Propositions 4.3 and 4.4 immediately imply that Algorithm 4.2 succeeds with probability at least $L^{-1/(4z)+o(1)}$, since Algorithm 4.2 succeeds whenever the a computed in step 2 completely factors over the primes $p_1, \ldots, p_n$. This finishes the proof of Theorem 4.1. □

Proof of Proposition 4.3. Let $\alpha_1, \ldots, \alpha_n$ be chosen at random as in step 1 and let (a, b) be the form computed in step 2. For any class $f \in C_{-N}$ let w_f be the probability that $\prod_{j=1}^{n} (I_{p_i})^{\alpha_i} = f$. Then the probability that (a, b) lies in f equals $w_{f \cdot (I_{p_i})^{2n \cdot r \cdot l}}$ for any $f \in C_{-N}$. Hence it suffices to show $w_f > (1 - o(1))/h_{-N}$ for all $f \in C_{-N}$. Let f be an arbitrary class in C_{-N}.

The numbers $(\alpha_1, \ldots, \alpha_n)$ chosen in step 1 will be considered as a vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}^n$. Let $W(m) \subset \mathbf{Z}^n$ be the cube defined by $W(m) = \{(\alpha_1, \ldots, \alpha_n)\colon 0 \leqslant \alpha_j < m,\ j = 1, \ldots, n\}$. Let φ be the homomorphism defined in Section 3,

$$\varphi(\alpha_1, \ldots, \alpha_n) = \prod_{j=1}^{n} \left(I_{p_j}\right)^{\alpha_j}.$$

Then w_f can be expressed as follows:

$$w_f = \frac{\#\{\alpha \in W(r \cdot l)\colon \varphi(\alpha) = f\}}{\#W(r \cdot l)},$$

since $\alpha_1, \ldots, \alpha_n$ were chosen independently and equidistributed in the interval $[0, \ldots, r \cdot l)$. Let x be any element of $\mathbf{Z}^n$ with $\varphi(x) = f$. Then we have

$$w_f = \frac{\#[W(r \cdot l) \cap (x + \ker \varphi)]}{\#W(r \cdot l)}.$$

Now we need a lemma to finish our proof.

LEMMA 4.5. *Let* $\Lambda \subset \mathbf{Z}^n$ *be a lattice with* $\#(\mathbf{Z}^n/\Lambda) = h$. *Then for any* $x \in \mathbf{Z}^n$,

$$\frac{\#[W(m) \cap (x + \Lambda)]}{\#W(m)} \geqslant \frac{1}{h} \cdot \left(1 - \frac{h - 1}{m}\right).$$

Proof of Lemma 4.5. We use induction on the dimension n of the lattice. The lemma is clearly true for $n = 1$. Now let us assume that the lemma holds for dimension n. Then we show that it also holds for dimension $n + 1$. We cut the $(n + 1)$-dimensional cube $W(m)$ into m different n-dimensional slices $W_0, \ldots, W_{m-1}$ with $W_i = \{(x_1, \ldots, x_{n+1}) \in W(m)\colon x_{n+1} = i\}$, each slice being an n-dimensional cube containing m^n integer points. Let Q_i be the set of cosets in $\mathbf{Z}^{n+1}/\Lambda$ which have a representative in the hyperplane generated by the n-dimensional cube W_i. Since $\mathbf{Z}^{n+1}/\Lambda$ is a group, all Q_i have equal cardinality h', and we have $Q_i = Q_j$ if and only if $i = j \bmod h''$ [with $h' \cdot h'' = h = \#(\mathbf{Z}^{n+1}/\Lambda)$]. For any $x \in \mathbf{Z}^{n+1}$, the set $(x + \Lambda) \cap Q_i$ is nonempty for a suitable i. Hence there are at least $(m - (h'' - 1))/h''$ different n-dimensional cubes W_i, $0 \leqslant i < m$, containing at least one point of $x + \Lambda$. Using our induction hypothesis on the lattice Q_0 in $\mathbf{Z}^n$, we

can easily show that each of these W_i contains at least $m^n/h' \cdot (1 - (h' - 1)/m)$ points of $x + \Lambda$. Hence,

$$\#[W(m) \cap (x + \Lambda)] \geqslant \left(\frac{m - (h'' - 1)}{h''}\right) \cdot \frac{m^n}{h'} \cdot \left(1 - \frac{h' - 1}{m}\right)$$

$$= \frac{m^{n+1}}{h' \cdot h''} \cdot \left(1 - \frac{h'' - 1}{m}\right) \cdot \left(1 - \frac{h' - 1}{m}\right) \geqslant \frac{m^{n+1}}{h} \cdot \left(1 - \frac{h - 1}{m}\right).$$

This proves the lemma for dimension $n + 1$. □

Applying our lemma to the lattice $\ker \varphi$ we obtain

$$w_f = \frac{\#\{\alpha \in W(r \cdot l) : \varphi(\alpha) = f\}}{\#W(r \cdot l)} \geqslant \frac{1}{h_{-N}} \cdot \left(1 - \frac{h_{-N} - 1}{r \cdot l}\right)$$

$$= \frac{1}{h_{-N}} \cdot [1 - o(1)],$$

since $h_{-N} = O(\sqrt{N}) \cdot \log N$ (by Theorem 2.2), $r \cdot l > \sqrt{N} \cdot l$, and $\log N = o(l)$. This finishes the proof of Proposition 4.3. □

5. The Number of Reduced Forms with Leading Coefficient Free of Prime Factors $> y$. The purpose of this section is to prove Proposition 4.4. For this, we need a lower bound for the number of reduced forms with leading coefficient free of prime factors $> y$. At present, satisfactory lower bounds for the number of reduced forms are only available under the assumption of the Extended Riemann Hypothesis which we assume to be true throughout this section.

For any fixed negative discriminant $-N$, $N > 0$, we denote by $F_{-N}(x, y)$ the set of reduced forms $(a, b) \in QF_{-N}$ with $a \leqslant x$ such that for any prime p dividing a the properties $\left(\frac{-N}{p}\right) = 1$ and $p \leqslant y$ hold. For counting the set $F_{-N}(x, y)$ we introduce the function

$$\psi_{-N}(x, y) := \#\left\{a \leqslant x : \text{any prime } p \text{ dividing } a \text{ satisfies } p \leqslant y \text{ and } \left(\tfrac{-N}{p}\right) = 1\right\}.$$

LEMMA 5.1. *For any $x \leqslant \sqrt{N}/2$ we have $\#F_{-N}(x, y) \geqslant \psi_{-N}(x, y)$.*

Proof. Any natural number a counted by $\psi_{-N}(x, y)$ splits into prime factors p with $\left(\frac{-N}{p}\right) = 1$ and $p \leqslant y$. Hence for any such a there is a form $(a, b, c) \in QF_{-N}$ (which may be obtained by multiplying prime forms according to Theorem 3.1). Using a suitable $\mathrm{SL}_2(\mathbf{Z})$-transformation $(a, b) \to (a, b + 2\lambda a)$, $\lambda \in \mathbf{Z}$, we may ensure that $-a < b \leqslant a$ holds. Then we have

$$c = \frac{b^2 + N}{4a} \geqslant \frac{N}{4 \cdot \sqrt{N}/2} \geqslant \sqrt{N}/2 \geqslant a,$$

i.e., (a, b, c) is reduced. Thus we have constructed an injective mapping from the set counted by $\psi_{-N}(x, y)$ into the set $F_{-N}(x, y)$. □

We now show the following lower bound for $\psi_{-N}(x, y)$.

THEOREM 5.2 (ERH). *For any $\varepsilon > 0$ there is a $c(\varepsilon)$ such that for any x, y, N with $x > 10$ and*

$$\max\left\{(\log x)^{1+\varepsilon}, (\log N)^{2+\varepsilon}\right\} \leqslant y \leqslant \exp\left[(\log x)^{1-\varepsilon}\right]$$

the following property holds:

$$\psi_{-N}(x, y) \geqslant x \cdot \exp[-u \cdot (\log u + \log\log u + c(\varepsilon))], \qquad u = \frac{\log x}{\log y}.$$

Proof of Proposition 4.4. We have to show for any fixed real z with $0 < z \leqslant 1$ that

$$\#F_{-N}(\infty, L^z) \geqslant h_{-N} \cdot L^{-1/(4z)+o(1)},$$

where $L = \exp(\sqrt{\log N \cdot \log\log N})$. From Theorem 2.2 and Lemma 5.1 we obtain

$$\frac{\#F_{-N}(\infty, L^z)}{h_{-N}} \geqslant \frac{\psi_{-N}(\sqrt{N}/2, L^z)}{\sqrt{N} \cdot \log N}.$$

A simple computation using Theorem 5.2 yields

$$\psi_{-N}(\sqrt{N}/2, L^z) \geqslant \sqrt{N} \cdot L^{-1/(4z)+o(1)}$$

for sufficiently large N. This proves

$$\#F_{-N}(\infty, L^z) \geqslant h_{-N} \cdot L^{-1/(4z)+o(1)}. \quad \square$$

It remains to prove Theorem 5.2. Canfield, Erdös, and Pomerance [4] and Pomerance [29] have shown lower bounds for the number-theoretic function $\psi(x, y)$ defined by

$$\psi(x, y) := \#\{a \leqslant x: \text{any prime } p \text{ dividing } a \text{ satisfies } p \leqslant y\}.$$

To prove Theorem 5.2, we proceed exactly as in [29]. In order to show a lower bound for $\psi(x, y)$, a good estimation for the prime number counting function $\pi(x)$ is needed. For our purposes we need a good estimation for the following modified prime number counting function:

$$\pi_{-N}(x) := \#\{\text{prime numbers } p \leqslant x \text{ with } (-N/p) = 1\}.$$

At present, a sufficiently sharp estimation for $\pi_{-N}(x)$ is only available under the assumption of the Extended Riemann Hypothesis:

THEOREM 5.3 (ERH). *We have*

$$|\pi_{-N}(x) - \mathrm{Li}(x)| = O(\sqrt{x} \cdot \log(Nx)).$$

Here, $\mathrm{Li}(x) = \int_2^x dx/\log x$ *is the logarithmic integral.*

Sketch of the Proof. For the proof of Theorem 5.3 we use an effective version of the Chebotarev density theorem shown by Lagarias and Odlyzko [15]. First, we briefly state some facts from algebraic number theory. For details we refer to [2], [17].

Let $\mathbf{Q}$ be the field of rational numbers, and let E be an algebraic extension of $\mathbf{Q}$ with degree n and Abelian Galois Group $\mathrm{Gal}(E/\mathbf{Q})$. Let M be the maximal order of E and let d be the discriminant of E. Let $\mathfrak{P}$ be the set of prime ideals in M. For any rational prime p let $(p) = p \cdot M$ be the principal ideal of p in M. Then (p) has a unique decomposition,

$$(p) = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}, \qquad \mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathfrak{P}.$$

The prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are called the prime ideals above p, and the rational prime p is called unramified in E if all exponents in the above decomposition equal 1.

For any prime p unramified in E there is a unique automorphism $(p, E/\mathbf{Q}) \in \mathrm{Gal}(E/\mathbf{Q})$, called the *Frobenius automorphism* of the prime p, which induces the automorphism $x \to x^p$, $x \in M/\mathfrak{p}_\nu$, on the field $M/\mathfrak{p}_\nu$ for any prime ideal $\mathfrak{p}_\nu$ lying above p. For any $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$ let $\pi_\sigma(x)$ be the number of rational primes $p \leqslant x$ unramified in E which satisfy $(p, E/\mathbf{Q}) = \sigma$. Under the assumption of the Extended Riemann Hypothesis the following proposition holds.

PROPOSITION 5.3 (ERH). *We have*

$$\left|\pi_\sigma(x) - \frac{\mathrm{Li}(x)}{\#\mathrm{Gal}(E/\mathbf{Q})}\right| \leqslant \frac{\sqrt{x}\cdot(2\cdot\log|d| + n\cdot\log x)}{\#\mathrm{Gal}(E/\mathbf{Q})}.$$

For a proof of Proposition 5.3 we refer to [15] or [27]. We apply Proposition 5.3 to the field $\mathbf{Q}(\sqrt{-N})$. Let us first assume that N is squarefree. Then $\mathrm{Gal}(\mathbf{Q}(\sqrt{-N})/\mathbf{Q})$ is isomorphic to $\{\pm 1\}$ (where 1 corresponds to the identity and -1 corresponds to the automorphism induced by $\sqrt{-N} \to -\sqrt{-N}$ of $\mathbf{Q}(\sqrt{-N})$). The Frobenius automorphism is given by

$$\left(p, \mathbf{Q}(\sqrt{-N})/\mathbf{Q}\right) = \left(\tfrac{-N}{p}\right).$$

(The primes ramified in $\mathbf{Q}(\sqrt{-N})$ are exactly the primes with $(\frac{-N}{p}) = 0$.) Thus Proposition 5.3 implies that

$$\left|\pi_{-N}(x) - \tfrac{1}{2}\cdot\mathrm{Li}(x)\right| = O\left(\sqrt{x}\cdot\log(Nx)\right).$$

This proves Theorem 5.3 for squarefree N. For nonsquarefree N (with $N = N'\cdot f^2$, N' squarefree) it suffices to remark that $|\pi_{-N}(x) - \pi_{-N'}(x)| = O(\log f)$, since any prime p with $(\frac{-N}{p}) \neq (\frac{-N'}{p})$ necessarily divides f. □

Now we are going to show Theorem 5.2. Let P be the set of prime numbers with $(\frac{-N}{p}) = 1$. We put

$$w_1 := y^{1-2/(3\log u)}, \qquad w_2 := y^{1-1/(3\log u)} \tag{5.4}$$

with $u = \log x/\log y$ as in Theorem 5.2. Let $[u]$ be the integral part of u and let M be the set of all positive integers which are products of exactly $[u]$ primes $p_1, \ldots, p_{[u]} \in P$ satisfying $w_1 < p_\nu \leqslant w_2$, $\nu = 1, \ldots, [u]$. Then

$$\psi_{-N}(x, y) \geqslant \sum_{m\in M} \psi_{-N}(x/m, w_1), \tag{5.5}$$

since every natural number a counted by $\psi_{-N}(x/m, w_1)$ is free of prime factors $> w_1$ and all prime factors of m, $m \in M$, lie in the interval $(w_1, w_2]$, $w_2 < y$. For all $m \in M$ we have

$$w_1^{u-1} < m \leqslant w_2^u. \tag{5.6}$$

The properties $y \leqslant \exp((\log x)^{1-\varepsilon})$ and $u = \log x/\log y$ imply $u \geqslant (\log x)^\varepsilon$. Hence, for sufficiently large x,

$$\begin{aligned} x^{1/\log u} &> x^{1/u}\cdot x^{2/(3\log u)} > y\cdot y^{2(u-1)/(3\log u)} \\ &= x\cdot y^{-(u-1)}\cdot y^{2(u-1)/(3\log u)} = x/w_1^{u-1} \geqslant x/m \\ &\geqslant x/w_2^u = x/x^{1-1/(3\log u)} = x^{1/(3\log u)} \end{aligned} \tag{5.7}$$

by (5.4) and (5.6). Now we put $u(m) := 1 + [(\log(x/m))/(\log w_1)]$. By definition of w_1 and $u(m)$, and by (5.7), we obtain

$$\begin{aligned} &1 + \frac{\log x}{\log u}\cdot\frac{1}{\log y\cdot(1 - 2/(3\log u))} \\ &\geqslant u(m) \geqslant \frac{\log x}{3\log u}\cdot\frac{1}{\log y\cdot(1 - 2/(3\log u))}. \end{aligned}$$

Now, using $u = \log x/\log y$, we obtain

$$\frac{u}{\log u}\cdot\left(1 + O\left(\frac{1}{\log u}\right)\right) \geqslant u(m) \geqslant \frac{u}{3\log u}. \tag{5.8}$$

We now put $w(m) := (x/m)^{1/u(m)}$. Then,

$$
\begin{aligned}
w_1 &= (x/m)^{(\log w_1)/\log(x/m)} \\
&\geqslant (x/m)^{1/u(m)} && [\text{def. of } u(m)] \\
&= w(m) && [\text{def. of } w(m)] \\
&\geqslant (x/m)^{1/(1+\log(x/m)/\log w_1)} && [\text{def. of } u(m)] \\
&= \exp\left(\frac{\log(x/m)\cdot\log w_1}{\log(x/m)+\log w_1}\right) \\
&= w_1^{1/(1+(\log w_1)/\log(x/m))} \\
&\geqslant w_1^{1-(\log w_1)/\log(x/m)} \\
&\geqslant w_1^{1-(\log y)/\log(x/m)} && [\text{since } w_1 < y] \\
&= w_1^{1-(\log x)/(u\cdot\log(x/m))} && [\text{def. of } u] \\
&\geqslant w_1^{1-(\log x)/(u\cdot\log x/(3\log u))} && [\text{by (5.7)}] \\
&= w_1^{1-3\cdot(\log u)/u}.
\end{aligned} \tag{5.9}
$$

The product of $u(m)$ different primes less than $w(m)$ does not exceed the value $w(m)^{u(m)} = x/m$. Hence (5.9) implies

$$
\psi_{-N}(x/m, w_1) \geqslant \binom{\pi_{-N}(w(m))}{u(m)} \geqslant \left(\frac{\pi_{-N}(w(m))}{u(m)}\right)^{u(m)}. \tag{5.10}
$$

From $w(m) \geqslant w_1^{1-(3\log u)/u} \geqslant y^{1-2/(3\log u)-(3\log u)/u}$ and $y \geqslant (\log N)^{2+\varepsilon}$ we obtain $w(m) \geqslant (\log N)^{2+\varepsilon/2}$ for sufficiently large x and y. With this information, a straightforward computation using our "prime number theorem" (5.3) yields

$$
\pi_{-N}(w(m)) \geqslant \frac{w(m)}{4\log w(m)}
$$

for sufficiently large x and y. Applying this fact to (5.10), we obtain

$$
\begin{aligned}
\psi_{-N}(x/m, w_1) &\geqslant \left(\frac{(w(m))}{4\cdot u(m)\cdot\log w(m)}\right)^{u(m)} \\
&= \frac{x}{m}\cdot\exp(-u(m)\cdot(\log u(m) + \log\log w(m) + \log 4)) \\
&\qquad [\text{since } w(m)^{u(m)} = x/m] \\
&\geqslant \frac{x}{m}\cdot\exp(-u(m)\cdot(\log u(m) + \log\log y + \log 4)) \\
&\qquad [\text{since } w(m) < w_1 < y] \\
&= \frac{x}{m}\cdot\exp(-u(m)\cdot(\log u - \log\log u + \log\log y + O(1))) \\
&\qquad [\text{by (5.8)}].
\end{aligned} \tag{5.11}
$$

From $y \leqslant \exp((\log x)^{1-\varepsilon})$ and $y = x^{1/u}$ we obtain

$$
\log\log y \leqslant (1-\varepsilon)\cdot\log\log(y^u) = (1-\varepsilon)\cdot(\log u + \log\log y)
$$

and hence

$$
\varepsilon\cdot\log\log y \leqslant (1-\varepsilon)\cdot\log u \leqslant \log u. \tag{5.12}
$$

By (5.11) and (5.12) there is a real constant $c'(\varepsilon)$ such that

$$\begin{aligned}\psi_{-N}(x/m, w_1) &\geqslant \frac{x}{m} \cdot \exp\left(\frac{c'(\varepsilon)}{2} \cdot u(m) \cdot \log u\right) \\ &\geqslant \frac{x}{m} \cdot \exp(-c'(\varepsilon) \cdot u) \qquad \text{[by (5.8)]}\end{aligned} \tag{5.13}$$

for sufficiently large x. Inequalities (5.5) and (5.13) imply

$$\psi_{-N}(x, y) \geqslant x \cdot \exp(-c'(\varepsilon) \cdot u) \cdot \sum_{m \in M} m^{-1}. \tag{5.14}$$

To finish the proof of Theorem 5.2, we have to estimate the sum $\Sigma_{m \in M} m^{-1}$. By definition of M we have

$$\sum_{m \in M} m^{-1} \geqslant \left(\sum_{p \in P, w_1 < p \leqslant w_2} p^{-1}\right)^{[u]} / [u]!. \tag{5.15}$$

Using standard partial summation arguments from number theory (see, e.g., [11]), we can easily prove the following corollary of our "prime number theorem" 5.3:

COROLLARY 5.16 (ERH). *For any $\varepsilon > 0$ there is an $\varepsilon' > 0$ such that*

$$\sum_{p \in P, w_1 < p \leqslant w_2} p^{-1} \geqslant \frac{1}{2}(\log\log w_2 - \log\log w_1) - O\left(w_1^{-\varepsilon'}\right)$$

for any w_1, w_2 with $(\log N)^{2+\varepsilon/2} \leqslant w_1 \leqslant w_2$.

Inequality (5.15) and Corollary 5.16 imply

$$\begin{aligned}\sum_{m \in M} m^{-1} &\geqslant \left(\frac{1}{2}\log\log w_2 - \frac{1}{2}\log\log w_1 - O\left(w_1^{-\varepsilon'}\right)\right)^{[u]} / [u]! \\ &\geqslant \left(\frac{1}{2}\log\left[\frac{1 - 1/(3\log u)}{1 - 2/(3\log u)}\right] - O\left(y^{-\varepsilon'/2}\right)\right)^{[u]} / [u]! \qquad \text{[by 5.4]} \\ &\geqslant \left(\frac{1}{8\log u} - O(u^{-\varepsilon'/2})\right)^{[u]} / [u]! \qquad \text{[since } u < \log x < y\text{]} \\ &\geqslant \left(\frac{1}{9\log u}\right)^{[u]} / [u]! \qquad \text{[for sufficiently large } x\text{]}.\end{aligned} \tag{5.17}$$

Using Stirling's formula $\log(n!) = n \cdot \log n - O(n)$, we finally obtain

$$\sum_{m \in M} m^{-1} \geqslant \exp(-u \cdot (\log u + \log\log u + O(1))) \tag{5.18}$$

for sufficiently large x. Inequalities (5.14) and (5.18) imply Theorem 5.2. □

6. Refinements of the New Factorization Algorithm. Our new factorization algorithm consists of two parts. First we have to generate a form matrix A by Algorithm 4.2. Next we have to evaluate the form matrix A. This means we have to compute a generating system of the 2-Sylow group of the class group from A which gives us the complete factorization of N.

The run time of the new factorization algorithm depends on the size L^z of the prime form base. If we choose z too small, only few of the forms (a, b) computed by Algorithm 4.2 can be factored over the chosen prime form base. If we choose z too

large, the factorization of the leading coefficient a will consume too much time. A third problem arises when we choose z too large: The evaluation of the form matrix will consume too much time. To speed up our factorization algorithm, we have to look at both generation and evaluation of a form matrix.

1. *Fast Generation of a Form Matrix.* First we can speed up Algorithm 4.2. The critical part of Algorithm 4.2 is step 3 where the leading coefficient a of a reduced form must be factored. This step has run time L^z when executed once. Note that the reduced form to be factored over the prime form base P_l is (almost) equidistributed in the class group C_{-N}.

In order to speed up our factorization algorithm, we need a fast method to factor the leading coefficient of a reduced form over a given base of prime forms. This means that we look for a fast method to find the small factors of a natural number. Pollard [28] and Strassen [40] introduced a fast method based on the fast Fourier transform for finding small factors of a number a. Using the Pollard-Strassen method, we can find all prime factors $p < L^z$ of a natural number $a < \sqrt{N}$ in time $L^{z/2+o(1)}$, see Schnorr [34].

There is still another way for speeding up the generation of a form matrix, called the early abort strategy, see [29]. For the overwhelming majority of the a generated by Algorithm 4.2 the full allotment of time ($L^{z/2}$ for the Pollard-Strassen method) is spent just for finding that a cannot be factored over the chosen prime form base. A natural idea that many have had is to abort working with a special form (a, b) if at some prechosen point the coefficient a does not look likely to be composed solely of primes below L^z, and to generate another form (a,b) instead. We shall make this idea more precise in Section 7. In the analysis of the early abort strategy, which is a bit difficult, we follow Pomerance [29]. In Section 7 we prove the following result:

THEOREM 6.1 (ERH). *There is an algorithm with average run time $T = L^{o(1)}$ which factors a fraction of at least $w = L^{-z/4-1/(4z)+o(1)}$ of the reduced forms of the class group C_{-N} over a given prime form base P_{L^z}, $0 < z \leqslant 1$.* (It is assumed that the input form is equidistributed in the class group.)

2. *Fast Evaluation of a Form Matrix.* In Section 3 we saw that the determinant of a nonsingular form matrix is a multiple of the class number and that a multiple of the class number immediately gives us a generating system of the 2-Sylow group of the class group and hence the complete factorization of the discriminant N. Computing the determinant of an $n \times n$-matrix, $n \leqslant L^z$, can be done via Gaussian elimination in $L^{3z+o(1)}$ arithmetic operations. Unfortunately, the coefficients of the matrix may grow dramatically, and we saw in Section 3 that this costs another factor L^z if modular arithmetic is used.

Fast matrix multiplication techniques introduced by Strassen [39] and others can be used to advantage for speeding up the computation of the determinant of a matrix. The present state of the art is represented by the algorithm of Coppersmith and Winograd [6], which allows us to perform multiplication, inversion and computing the determinant of an $n \times n$-matrix in $O(n^{2.495548})$ arithmetic operations. Using this fast algorithm, we can evaluate a form matrix in time $L^{(3.495548)z+o(1)}$.

There is a new method that solves sparse linear equations $Ax = b$ in a finite field in time $H(A) \cdot n \cdot (\log n)^{O(1)}$, see [43]. Here $H(A)$ denotes the number of nonzero entries of the sparse $n \times n$-matrix A. This method can be used to find nontrivial

linear dependences modulo 2 in a form matrix. Having found such a linear dependence $u \in \{0,1\}^n$, $A \cdot u^T = 0 \bmod 2 \cdot \mathbf{Z}^n$, we can compute the ambiguous form $\varphi(A \cdot u^T/2)$ which corresponds to a nontrivial factorization of N with a reasonable chance. (Here, φ: $\mathbf{Z}^n \to C_{-N}$ is the homomorphism defined in Section 3.) In Section 8 we prove

THEOREM 6.2. *Suppose there are functions* $c = c(N)$, $l = l(N)$, $T = T(N)$, $w = w(n)$, $c(n) \leqslant l(n) \leqslant N^{1/4}$ *with the following properties*:

6.2.1. *The prime forms* $I_{p_j} \in C_{-N}$, $p_j \leqslant c$ *generate the subgroup of the ambiguous forms of the class group* C_{-N}.

6.2.2. *There is an algorithm with average run time* T *which factors a fraction of at least* w *of the reduced forms of* C_{-N} *over the prime form base* P_l *of* C_{-N} *into at most* $(\log N)^{O(1)}$ *prime form factors.*

Then there is a probabilistic algorithm with run time $c \cdot (T \cdot w^{-1} \cdot l + l^2) \cdot \log(N)^{O(1)}$ *which factors a composite number* N *with probability* $\geqslant 1/2$.

Remark. With some additional effort, the algorithm in Theorem 6.2 can be modified in such a way that it yields a proof of primality for prime numbers N.

Conclusion. From Theorems 6.1 and 6.2 (with $c = 2 \cdot (\log n)^2$, $w = L^{-1/(4z)-z/4+o(1)}$, $T = L^{o(1)}$, $l = L^z$) we obtain a factorization algorithm with run time $L^{\max\{2z,5z/4+1/(4z)\}+o(1)}$. The optimal choice for z is $1/\sqrt{5}$. This gives us the following

MAIN THEOREM (ERH). *There is a probabilistic factorization algorithm which yields the complete factorization of a natural number* N *in time* $L^{\sqrt{5/4}+o(1)}$ *with probability* $\geqslant 1/2$ (*where* $L = \exp\sqrt{\log N \log\log N}$).

Using the Pollard-Strassen method, the early abort strategy and a fast elimination method, Pomerance [29] obtains the same run time exponent for the factorization algorithm of Morrison and Brillhart. Instead of the Extended Riemann Hypothesis he uses other heuristic assumptions.

Open Problems. 1. There is a new factorization algorithm due to Lenstra [23] which uses elliptic curves. This new algorithm is very efficient in finding the small prime factors of a natural number. If may turn out that this factorization algorithm can be used to improve Theorem 6.1. Using elliptic curve methods to factor the leading coefficient of a reduced form, we may possibly obtain a factorization algorithm with run time $L^{1+o(1)}$.

2. In Algorithm 4.2, which is used for generating a form matrix, we try to factor the leading coefficient a of the *reduced* form $f = (a, b, c)$ in a certain class $[f]$ of the class group C_{-N}. It would be sufficient to factor the leading coefficient a' of *any* form (a', b', c') in the same class $[f]$. It is easy to see that an integer a' is the leading coefficient of any form (a', b', c') in the class $[f]$ if and only if a' is *represented* by the form f, i.e., there are integers x and y with

$$a' = f(x, y) = ax^2 + bxy + cy^2.$$

$f(x, y)$ is a quadratic polynomial in x and y. When we restrict the domain R of this polynomial in a suitable way, we can find the small factors of all values $f(x, y)$, $(x, y) \in R$, by sieve methods. The elaboration of this idea yields a factorization algorithm which is very similar to the quadratic sieve algorithm introduced in [29]. For analyzing this modified algorithm we need an assumption of the following type:

Assumption 6.4. The forms $(a, b) \in QF_{-N}$ with a free of prime factors $> L^z$, $a \leqslant x$ (where x is in the range $\sqrt{N} \cdots L \cdot \sqrt{N}$) are approximately equidistributed over all classes of the class group.

It is not known whether a suitable precise version of Assumption 6.4 can be shown under the assumption of the Extended Riemann Hypothesis. If this were the case, we could also analyze our modified algorithm and possibly obtain a run time of $L^{1+o(1)}$.

7. Analysis of the Early Abort Strategy. The purpose of this section is to show Theorem 6.1. In order to factor the leading coefficient a of a reduced form we use the following procedure instead of trial division.

Let $k \in \mathbf{N}$ and let $c_1, \ldots, c_k$, $\vartheta_1, \ldots, \vartheta_k$ be fixed positive real numbers with $c_1 + \cdots + c_k < 1$ and $0 < \vartheta_1 < \cdots < \vartheta_k < 1$. For any natural number a let $a[t]$ be the part of a that consists entirely of prime factors $> t$. Let $(a, b) \in C_{-N}$ be a reduced form selected at random with respect to equidistribution in the class group C_{-N}.

$$
\begin{aligned}
&(a,b) \text{ is aborted in stage } 0 && \text{if } \gcd(a,N) > 1,\\
&(a,b) \text{ is aborted in stage } i,\ i = 1,\ldots,k && \text{if } a[L^{\vartheta_i \cdot z}] > \sqrt{N^{1-c_1-\cdots-c_i}},\\
&(a,b) \text{ is aborted in stage } k+1 && \text{if } a[L^z] > 1.
\end{aligned} \tag{7.1}
$$

If (a, b) is not aborted, it will completely factor over the prime form base P_{L^z}. Otherwise, our attempt to factor the reduced form (a, b) fails. This modified procedure will be called the early abort method with k early aborts and parameters $c_1, \ldots, c_k$, $\vartheta_1, \ldots, \vartheta_k$. Let M_i, $i = 1, \ldots, k+1$, be the set of reduced forms of QF_{-N} with the property that a is not aborted at stage $0, 1, \ldots, i$. Then the success rate w of the early abort method (with k early aborts and parameters $c_1, \ldots, c_k$, $\vartheta_1, \ldots, \vartheta_k$) is given by

$$w = \#M_{k+1}/h_{-N}. \tag{7.2}$$

Its average run time T is given by

$$T = \sum_{i=1}^{k+1} L^{\vartheta_j \cdot z + o(1)} \cdot \#M_{i-1}/h_{-n}, \tag{7.3}$$

where we have put $M_0 := h_{-N}$ and $\vartheta_{k+1} := 1$. Using the Pollard-Strassen method for finding small factors, the run time can be improved to

$$T = \sum_{i=1}^{k+1} L^{\vartheta_j \cdot z/2 + o(1)} \cdot \#M_{i-1}/h_{-N}. \tag{7.4}$$

Our goal is to minimize the product $T \cdot w^{-1}$. For this, we have to evaluate M_i, $i = 1, \ldots, k+1$. The result, which we will prove at the end of this section, is

PROPOSITION 7.6 (ERH). *We have*

$$
\begin{aligned}
\#M_i &\leqslant \sqrt{N} \cdot L^{-c_1/(4\vartheta_1 \cdot z) - \cdots - c_i/(4\vartheta_i \cdot z) + o(1)}, \qquad i = 1, \ldots, k,\\
\#M_{k+1} &\geqslant \sqrt{N} \cdot L^{-c_1/(4\vartheta_1 \cdot z) - \cdots - c_k/(4\vartheta_k \cdot z) - (1-c_1-\cdots-c_k)/(4z) + o(1)},\\
\#M_0 = h_{-N} &\leqslant \sqrt{N} \cdot L^{o(1)} \quad (\textit{by Theorem } 2.2).
\end{aligned}
$$

Remark. It can be shown that the bounds in Proposition 7.6 are sharp, see [29].

Now, from (7.2), (7.4), and Proposition 7.6 we obtain

$$
\begin{aligned}
&T \cdot w^{-1} \leqslant L^{\max\{f_1,\dots,f_{k+1}\}+o(1)} \quad \text{with} \\
&\qquad f_i = \vartheta_i \cdot z/2 + c_i/(4\vartheta_i \cdot z) + \cdots + c_k/(4\vartheta_k \cdot z) \\
&\qquad\qquad + (1 - c_1 - \cdots - c_k)/(4z), \qquad i = 1,\dots,k, \\
&\qquad f_{k+1} = z/2 + (1 - c_1 - \cdots - c_k)/(4z).
\end{aligned} \tag{7.7}
$$

The optimal choice for the c_i, ϑ_i, $i = 1,\dots,k$, is

$$
c_i = \frac{2i \cdot z^2}{(k+1)^2}, \qquad \vartheta_i = \frac{i}{k+1};
$$

compare [29]. Using these optimal values we obtain from (7.7)

$$
\begin{aligned}
&T \cdot w^{-1} \leqslant L^{z/4+z/(4k+4)+1/4z+o(1)}, \qquad T \leqslant L^{z/(2k+2)+o(1)}, \\
&\qquad w^{-1} \leqslant L^{z/4+1/4z-z/(4k+4)+o(1)}.
\end{aligned} \tag{7.8}
$$

By letting k slowly grow towards infinity we finally obtain

$$
T \cdot w^{-1} \leqslant L^{z/4+1/(4z)+o(1)}, \quad T = L^{o(1)}, \quad w^{-1} \leqslant L^{z/4+1/(4z)+o(1)}. \tag{7.9}
$$

This proves Theorem 6.1.

We still have to prove Proposition 7.6. For this, we need some additional information about the number of reduced forms which split over certain sets of prime forms. Let $F_{-N}(x, y, z)$ be the set of all reduced forms $(a, b) \in QF_{-N}$ with $a \leqslant x$, $\gcd(a, N) = 1$, such that any prime p dividing a satisfies $z < p \leqslant y$. Note that the set $F_{-N}(x, y)$ defined in Section 5 equals $F_{-N}(x, y, 1)$. Then we need

THEOREM 7.10 (ERH). *Let α, β, ε be fixed nonnegative numbers with $0 \leqslant \beta < \alpha \leqslant 1$ and $\varepsilon > 0$. Then for any c with $\varepsilon < c \leqslant 1$ we have*

$$
F_{-N}(\sqrt{N^c}, L^\alpha, L^\beta) = \sqrt{N^c} \cdot L^{-c/(4\alpha)+o(1)}, \tag{7.10.1}
$$

$$
F_{-N}(\sqrt{N^c}, \sqrt{N^c}, L^\beta) = \sqrt{N^c} \cdot L^{o(1)}. \tag{7.10.2}
$$

Here, $o(1)$ is a function depending only on N with $o(1) \to 0$ for $N \to \infty$.

Sketch of the Proof. We first show the lower bounds in (7.10.1) and (7.10.2). For this, we define

$$
\begin{aligned}
&\psi_{-N}(x, y, z) \\
&\qquad := \#\left\{a \leqslant x\text{: any prime } p \text{ dividing } a \text{ satisfies } z < p \leqslant y \text{ and } \left(\tfrac{-N}{p}\right) = 1\right\}.
\end{aligned}
$$

Then for any $x \leqslant \sqrt{N}/2$ there follows $F_{-N}(x, y, z) \geqslant \psi_{-N}(x, y, z)$, compare Lemma 5.1. With the method discussed in Section 5 we can prove the following analog of Theorem 5.2 (compare [29, Theorem 2.2]):

PROPOSITION 7.11 (ERH). *For any $\varepsilon > 0$ there is a $c(\varepsilon)$ such that for any x, y, z, N with $x > 10$ and*

$$
\max\left\{(\log x)^{1+\varepsilon}, (\log N)^{2+\varepsilon}\right\} \leqslant y \leqslant \exp\left[(\log x)^{1-\varepsilon}\right], \qquad z < y^{1-1/\log u},
$$

the following property holds:

$$
\psi_{-N}(x, y, z) \geqslant x \cdot \exp[-u \cdot (\log u + \log\log u + c(\varepsilon))],
$$

where $u = \log x/\log y$.

This yields the lower bound in (7.10.1). The lower bound in (7.10.2) follows from $\psi_{-N}(x, x, z) \geqslant \pi_{-N}(x) - \pi_{-N}(z)$ and our "prime number theorem" 5.3. Now we show the upper bounds in (7.10.1) and (7.10.2). Here we use a method due to Rankin [31] and de Bruijn [3]. Let

$P_{y,-N}$ be the set of primes $p \leqslant y$ with $\left(\frac{-N}{p}\right) = 1$,

$N_{y,-N}$ be the set of natural numbers a such that all factors p of a satisfy $p \in P_{y,-N}$,

$f(a)$ be the number of *different* prime factors of a.

Theorem 3.1 implies that for any a with $\gcd(a, N) = 1$ there are at most $2^{f(a)}$ different reduced forms with leading coefficient a. Hence, for any $\eta > 0$,

$$
\begin{aligned}
F_{-N}(x, y, z) &\leqslant \sum_{a \in N_{y,-N};\ a \leqslant x} 2^{f(a)} \leqslant \sum_{a \in N_{y,-N};\ a \leqslant x} 2^{f(a)} \cdot (x/a)^{\eta} \\
&\leqslant x^{\eta} \cdot \sum_{a \in N_{y,-N}} 2^{f(a)} \cdot a^{-\eta} = x^{\eta} \cdot \prod_{p \in P_{y,-N}} \left(1 + 2 \cdot \sum_{\nu=1}^{\infty} p^{-\nu\eta}\right) \\
&\leqslant x^{\eta} \cdot \prod_{p \in P_{y,-N}} (1 - p^{-\eta})^{-2} \leqslant x^{\eta} \cdot \prod_{p \leqslant y,\ p \text{ prime}} (1 - p^{-\eta})^{-2} \qquad (7.12) \\
&= x^{\eta} \cdot \exp\left(-2 \cdot \sum_{p \leqslant y} \log(1 - p^{-\eta})\right) \\
&= x^{\eta} \cdot \exp\left(2 \cdot \sum_{p \leqslant y} p^{-\eta} + O\left(\sum_{p \leqslant y} p^{-2\eta}\right)\right).
\end{aligned}
$$

For further estimation of (7.12) we use the following fact:

$$
\sum_{p \leqslant y} p^{-\eta} = \begin{cases} O\left(\dfrac{y^{1-\eta}}{(1-\eta) \cdot \log y} + |\log(1-\eta)|\right) & \text{if } 0 < \eta < 1, \\ \log\log y + O(1) & \text{if } \eta = 1, \\ O\left((\eta - 1)^{-1}\right) & \text{if } \eta > 1, \end{cases} \qquad (7.13)
$$

which can be proved with standard methods of number theory, see [11], [30]. We will get the upper bound in (7.10.1) with $\eta = 1 - (\log u + \log\log u)/\log y$, where $u = \log x/\log y$ and x, y are the first two arguments of the function F_{-N} in (7.10.1). The upper bound in (7.10.2) is obtained with $\eta = 1$. The details of this computation, which are a bit tedious, are left to the reader.

This finishes the proof of Theorem 7.10. □

Remark. Note that the Extended Riemann Hypothesis is only needed for the proof of the lower bounds in Theorem 7.10.

Proof of Proposition 7.6. We show the proposition for the case $k = 1$, and we write c, ϑ for c_1, ϑ_1. We leave the case $k > 1$ to the reader. So let us assume $k = 1$.

First we prove the lower bound for $\#M_2$. By definition of M_2 we have

$$
\#M_2 \geqslant \#F_{-N}(\sqrt{N^c}, L^{\vartheta \cdot z}, 1) \cdot \#F_{-N}\left(\frac{\sqrt{N^{1-c}}}{2}, L^{z}, L^{\vartheta \cdot z}\right),
$$

since the product of two reduced forms (a, b) and (a', b') with $a \cdot a' \leqslant \sqrt{N}/2$ is reduced. Now a simple application of Theorem 7.10 yields the desired lower bound for M_2.

Now we prove the upper bound for M_1 in Proposition 7.6. By definition of M_1 we have

$$\#M_1 = \sum_{(a,b)\in Q} \sum_{(a',b')\in Q'} 1, \tag{7.14}$$

where $Q = F_{-N}(\sqrt{N^{1-c}}, \sqrt{N^{1-c}}, L^{\vartheta\cdot z})$ and $Q' = Q'(a) = F_{-N}(\sqrt{N}/a, L^{\vartheta\cdot z}, 1)$. (Note that any reduced form $(a,b) \in QF_{-N}$ satisfies $a < \sqrt{N}$.) (7.14) implies $a < \sqrt{N^{1-c}}$, i.e., $\sqrt{N}/a > \sqrt{N^c}$. Hence by Theorem 7.10 we obtain

$$\sum_{(a',b')\in Q'} 1 = \#F_{-N}\left(\frac{\sqrt{N}}{a}, L^{\vartheta\cdot z}, 1\right) \leqslant \frac{\sqrt{N}}{a} \cdot L^{-c/(4\vartheta\cdot z)}.$$

With this, and (7.14), we obtain

$$\#M_1 \leqslant \sqrt{N} \cdot L^{-c/(4\vartheta\cdot z)} \cdot \sum_{(a,b)\in Q} a^{-1}. \tag{7.15}$$

Now, using Theorem 7.10, part (7.10.2), it is easy to show that $\sum_{(a,b)\in Q} a^{-1} = L^{o(1)}$ by standard partial summation arguments (see, e.g., [30]). This yields the desired upper bound for M_1. □

8. Fast Evaluation of a Form Matrix. The purpose of this section is to prove Theorem 6.2. Let N, l, c, w, T be as in Theorem 6.2. We assume that N is composite. Then h_{-N} is even. Let $n = \#\{I_{p_j}: p_j \leqslant l\}$, $m = \#\{I_{p_j}: p_j \leqslant c\}$. Let φ: $\mathbf{Z}^n \to C_{-N}$ be the mapping defined in Section 3 and let $\Gamma = \ker\varphi$. For any integer $k \times n$-matrix $A = (a_{ij})$ let $\Lambda(A)$ be the lattice generated by the row vectors of A,

$$\Lambda(A) := \mathfrak{a}_1\mathbf{Z} + \cdots + \mathfrak{a}_k\mathbf{Z} \quad \text{with } \mathfrak{a}_i = (a_{i1}, \ldots, a_{in}), \qquad i = 1, \ldots, k,$$

as in Section 3. A form matrix is a matrix A with $\Lambda(A) \subset \ker\varphi$. We denote the group of ambiguous forms in C_{-N} by B. Then $B = \varphi(\Gamma/2 \cap \mathbf{Z}^n)$. We generate a form matrix $A = (a_{ij})$, $i, j = 1, \ldots, n$, as follows:

ALGORITHM 8.1.

1. put $i = 1$
2. choose $\alpha_{i1}, \ldots, \alpha_{im} \in \mathbf{Z}$ with $0 \leqslant \alpha_{i1}, \ldots, \alpha_{im} < N$ at random and independently with respect to equidistribution
3. compute the reduced form $f_i \in \prod_{j=1}^{m}(I_{p_j})^{\alpha_{ij}}$
4. try to find a factorization $(\beta_{i1}, \ldots, \beta_{in})$ with $f_i = \prod_{j=1}^{n}(I_{p_j})^{\beta_{ij}}$ using the algorithm described in (6.2.2). If f_i is successfully factored, goto step 5, else goto step 2
5. output the ith row vector $a_i = (a_{i1}, \ldots, a_{in})$ with $a_{ij} = \alpha_{ij} - \beta_{ij}$ for $j = 1, \ldots, n$ and $\alpha_{ij} = 0$ for $j > m$
6. put $i = i + 1$. If $i \leqslant n$ goto step 2, else stop.

The following lemma states that the form f_i computed in step 3 of the algorithm is approximately equidistributed in the class group.

LEMMA 8.2. *Let f be any reduced form in C_{-N}. Then the form f_i computed in step* 3 *of Algorithm* 8.1 *satisfies $f_i = f$ with probability $h_{-N}^{-1} \cdot (1 + o(1))$.*

Proof. With $h_{-N} \leqslant N^{1/2+o(1)}$ (see Theorem 2.2) and $0 \leqslant \alpha_{ij} < N$ the lemma follows immediately from Lemma 4.5. (Note that $I_{p_1}, \ldots, I_{p_m}$ generate C_{-N}). □

By Assumption 6.2.2 and Lemma 8.2 the average number of iterations of steps 2, 3, 4 of Algorithm 8.1 which are performed to compute the n row vectors of the form matrix A is $n \cdot w^{-1} \leqslant l \cdot w^{-1}$. The average run time for a single iteration of steps 2, 3, 4 can be bounded by $c \cdot T \cdot (\log N)^{O(1)}$. This leads to the following fact.

LEMMA 8.3. *Algorithm* 8.1 *computes a form matrix in time* $c \cdot l \cdot T \cdot w^{-1} \cdot (\log N)^{O(1)}$ *with probability* $\geqslant \frac{1}{2}$.

Let $H(A)$ be the number of nonzero entries of the matrix A. By construction of A we have

$$H(A) \leqslant \left(c + (\log N)^{O(1)}\right) \cdot n. \tag{8.4}$$

This means that A is sparse. By combining the row vectors of A we can find a nonzero vector $v \in \Gamma \cap 2 \cdot \mathbf{Z}^n$. Then the form $g = \varphi(v/2)$ is ambiguous and we have a reasonable chance that g leads to a nontrivial factorization of N. At the end of this section we will prove

PROPOSITION 8.5. *Let* B' *be a fixed proper subgroup of the group* B *of ambiguous forms of* C_{-N}. *Then the form matrix* A *computed by Algorithm* 8.1 *satisfies*

$$\varphi\left[\Lambda(A)/2 \cap \mathbf{Z}^n\right] \cap \left(B \setminus B'\right) \neq \varnothing$$

with probability $\geqslant \frac{1}{2} - o(1)$.

For composite N we let B' be the group of ambiguous forms which lead to a trivial factorization of N. Then Proposition 8.5 states that with probability $\geqslant \frac{1}{2} - o(1)$ there is a linear dependence (modulo 2) $u = (u_1, \ldots, u_n) \in \{0,1\}^n$ with $A \cdot u^T = 0 \pmod{2 \cdot \mathbf{Z}^n}$ among the row vectors of the matrix A with the property that the ambiguous form $\varphi(A \cdot u^T/2)$ leads to a nontrivial factorization of N. This means that at least half of the linear dependencies u of A (modulo 2) lead to a nontrivial ambiguous form $\varphi(A \cdot u^T/2) \in B \setminus B'$. Note that the linear dependencies u of A (modulo 2) which lead to a trivial ambiguous form $\varphi(A \cdot u^T/2) \in B'$ form a proper subgroup of the additive group of all linear dependencies of A (modulo 2). Thus we obtain

PROPOSITION 8.6. *Let* A *be a random form matrix computed by Algorithm* 8.1 *and let* u *be a linear dependence (modulo* 2*) among the row vectors of* A *selected at random with respect to equidistribution. Then for composite* N *the ambiguous form* $\varphi(A \cdot u^T/2)$ *leads to a nontrivial factorization of* N *with probability at least* $\frac{1}{4} - o(1)$.

So what we need is a fast method to find a linear dependence modulo 2 among the row vectors of a sparse matrix. Note that this process is similar to the elimination part in the factorization algorithms of Morrison and Brillhart and Dixon and the quadratic sieve algorithm of Pomerance, see [29] for details.

There is a new method to solve sparse linear equations in a finite field, see Wiedemann [43]. This method can also be used to find linear dependencies among the row vectors of a sparse matrix. In [43] the following theorem is shown.

THEOREM 8.7. *Let* A *be an* $n \times n$*-matrix over a finite field* K. *Then there is a probabilistic algorithm with run time* $n \cdot H(A) \cdot \log(n \cdot \#K)^{O(1)}$ *which computes a uniform distributed random solution* $u \in K^n$ *to the equation* $A \cdot u^T = 0$.

From Lemma 8.3, (8.4), Proposition 8.6, Theorem 8.7 and $n < 1$ we obtain

PROPOSITION 8.8. *There is a probabilistic algorithm which factors a composite number N in time*

$$(l^2 + l \cdot T \cdot w^{-1}) \cdot c \cdot (\log N)^{O(1)}$$

with probability at least $\frac{1}{4} - o(1)$.

Theorem 6.2 is an immediate consequence of Proposition 8.8. It remains to prove Proposition 8.5.

Proof of Proposition 8.5. We are going to show that $\varphi[\Lambda(A)/2 \cap \mathbf{Z}^n] \subset B'$ is true with probability at most $\frac{1}{2} + o(1)$. Let $A = (a_{ij})$; $a_i = \alpha_i - \beta_i$, $a_i = (a_{i1}, \ldots, a_{in})$, $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{in})$, $\beta_i = (\beta_{i1}, \ldots, \beta_{in})$ be as in Algorithm 8.1. Let N_0 be the greatest multiple of $2h_{-N}$ which is less than or equal to N. Let $W \subset \mathbf{Z}^n$ be the set $\{(x_1, \ldots, x_m, 0, \ldots, 0) \in \mathbf{Z}^n : 0 \leqslant x_j < N_0,\ j = 1, \ldots, m\}$. To simplify our proof, we assume

$$\alpha_i \in W, \qquad i = 1, \ldots, n. \tag{8.5.1}$$

Assumption (8.5.1) is true with probability $> 1 - 2 \cdot c \cdot l \cdot h_{-N} \cdot N^{-1} = 1 - o(1)$. It suffices to show that under Assumption (8.5.1) the property $\varphi[\Lambda(A)/2 \cap \mathbf{Z}^n] \subset B'$ is true with probability at most $\frac{1}{2}$. Let $X \subset \mathbf{Z}^n$ be the set of all possible vectors $(\beta_{i1}, \ldots, \beta_{in})$ computed by Algorithm 8.1. Then we may consider the values α_{ij}, β_{ij} computed by Algorithm 8.1 as a random variable in $W^n \times X^n$ in a natural way. For $x \in W^n \times X^n$ let $p(x)$ be the probability that Algorithm 8.1 computes x. Let $Q \subset W^n \times X^n$ be the set of all random matrices $((\alpha_{ij}), (\beta_{ij}))$ such that $\varphi(\Lambda[(\alpha_{ij}) - (\beta_{ij})]/2 \cap \mathbf{Z}^n) \subset B'$. Then our goal is to show $p(Q) \leqslant \frac{1}{2}$. For this purpose, we construct a bijection ξ from $W^n \times X^n$ onto $W^n \times X^n$ with the following properties:

$$p(x) = p(\xi(x)) \quad \text{for any } x \in W^n \times X^n, \tag{8.5.2}$$

$$x \in Q \quad \text{implies} \quad \xi(x) \notin Q \text{ for any } x \in W^n \times X^n. \tag{8.5.3}$$

Such a bijection ξ exists only if $p(Q) \leqslant \frac{1}{2}$. It remains to construct ξ.

Construction of ξ. Let f be any ambiguous form with $f \in B \setminus B'$. Since B is generated by the I_{p_j} with $j \leqslant m$, there is a vector $v = (v_1, \ldots, v_m, 0, \ldots, 0) \in \mathbf{Z}^n$ with $\varphi(v) = f$. We have $2v \in \ker\varphi$ since f is ambiguous. For any vector $u = (u_1, \ldots, u_n) \in \mathbf{Z}^n$ let $u \bmod N_0$ be the vector $(u_1', \ldots, u_n') \in \mathbf{Z}^n$ with $u_j' = u_j \bmod N_0$, $0 \leqslant u_j' < N_0$ for $j = 1, \ldots, n$. Note that $u' = u \bmod N_0$ implies $u' = u \bmod 2 \cdot \ker\varphi$.

For any $n \times n$-matrix U with integer coefficients and even determinant let $\nu(U)$ be the smallest index i such that there exists a linear combination

$$u_i = \sum_{j=1}^{i-1} \lambda_j \cdot u_j \bmod 2 \cdot \mathbf{Z}^n, \qquad \lambda_j \in \{0, 1\},\ j = 1, \ldots, i-1.$$

(Here $u_1, \ldots, u_n$ denote the row vectors of U.) If $\det U$ is odd, we define $\nu(U) = 0$. Now we define the bijection ξ: $W^n \times X^n \to W^n \times X^n$ as follows:

$$\xi(U, V) = (U', V), \qquad U, U' \in W^n,\ V \in X^n$$

with $u_i' = (u_i + 2 \cdot v) \bmod N_0$ for $i = \nu(U - V)$ and $u_i' = u_i$ for $i \neq \nu(U - V)$.

(Here $u_1', \dots, u_n'$ denote the row vectors of the matrix $U' \in W^n$.) ξ is a bijection on $W^n \times X^n$ since $\nu(U - V) = \nu(U' - V)$ by definition of ν and U'.

Since $u_i' = u_i \bmod \ker \varphi$ for all i we have $\varphi(u) = \varphi(u')$, and since the distribution of the ith row vector of V (under the assumption that U has a fixed value) is completely determined by $\varphi(u_i')$, we have $p(U', V) = p(U, V)$. This proves (8.5.2).

Next we show (8.5.3). Let $A = U - V$, $\nu = \nu(A)$. By definition of $\nu(A)$ there is a column vector $t = (t_1, \dots, t_n)^T$ with $t_\nu = 1$, $1 \leqslant \nu \leqslant n$, such that

$$A \cdot t = 0 \bmod 2 \cdot \mathbf{Z}^n.$$

(Note that $\det A$ is a multiple of h_{-N} and hence even, if N is composite.) Then $\varphi(A \cdot t/2)$ is well defined and we have $\varphi(A \cdot t/2) \in B$, since $\Lambda(A) \subset \ker \varphi$. We may assume $\varphi(A \cdot t/2) \in B'$. (Otherwise, we have $\varphi([\Lambda(A)/2] \cap \mathbf{Z}^n) \not\subset B'$ and hence $(U, V) \notin Q$, so that there is nothing to show.)

Let $A' = U' - V$. Since $t_\nu = 1$ and A differs from A' only in the νth row, we have

$$\varphi(A' \cdot t/2) = \varphi(A \cdot t/2) + \varphi\left[\left(u_\nu' - u_\nu\right)/2\right].$$

By definition of u_ν' we have $u_\nu' - u_\nu = 2v \bmod 2 \cdot \ker \varphi$ and hence

$$\varphi(A' \cdot t/2) = \varphi(A \cdot t/2) + \varphi(v) \in B' + f.$$

Since $f \notin B'$, this implies $\varphi(A' \cdot t/2) \notin B'$ and hence $(U', V) = \xi(U, V) \notin Q$.

Siemens A. G.
Funk- und Radarsysteme
Landshuter Strasse 26
D-8044 Unterschleissheim
Postfach 1661
West Germany

1. E. BACH, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, Cambridge, Mass., 1985.

2. Z. I. BOREVIČ & I. R. ŠAFAREVIČ, *Teorija Čisel*, Izdat. "Nauka", Moscow, 1964; English transl., Academic Press, New York and London, 1966.

3. N. G. DE BRUIJN, "On the number of positive integers $\leqslant x$ free of prime factors $> y$. II," *Nederl. Akad. Wetensch. Proc. Ser. A*, v. 69, 1966, pp. 239–247.

4. E. R. CANFIELD, P. ERDŐS & C. POMERANCE, "On a problem of Oppenheimer concerning "factorisatio numerorum"," *J. Number Theory*, v. 17, 1983, pp. 1–28.

5. J. W. S. CASSELS, *Rational Quadratic Forms*, Academic Press, London and New York, 1978.

6. D. COPPERSMITH & S. WINOGRAD, "On the asymptotic complexity of matrix multiplication," *SIAM J. Comput.*, v. 11, 1982, pp. 472–492.

7. L. E. DICKSON, *History of the Theory of Numbers*, Vol. 1, Carnegie Institution, Washington, D. C., 1919.

8. J. D. DIXON, "Asymptotically fast factorization of integers," *Math. Comp.*, v. 36, 1981, pp. 255–260.

9. C. F. GAUSS, *Disquisitiones Arithmeticae*, Leipzig, 1801.

10. R. K. GUY, "How to factor a number," *Proc. Fifth Manitoba Conf. Numer. Math.*, Utilitas, Winnipeg, 1975, pp. 49–89.

11. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.

12. D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

13. J. C. LAGARIAS, "Worst case complexity bounds for algorithms in the theory of integral quadratic forms," *J. Algorithms*, v. 1, 1980, pp. 142–186.

14. J. C. LAGARIAS, H. L. MONTGOMERY & A. M. ODLYZKO, "A bound for the last prime ideal in the Chebotarev density theorem," *Invent. Math.*, v. 54, 1975, pp. 137–144.

15. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem," in *Algebraic Number Fields, L-Functions and Galois Properties* (A. Fröhlich, ed.), Academic Press, London and New York, 1977, pp. 409–464.

16. E. LANDAU, *Vorlesungen über Zahlentheorie, Band* 1: *Elementare und additive Zahlentheorie*, Hirzel, Leipzig, 1927; reprinted, Chelsea, New York, 1982.

17. S. LANG, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1968.

18. A. M. LEGENDRE, *Théorie des Nombres*, Paris, 1798, pp. 313–320.

19. D. H. LEHMER & R. E. POWERS, "On factoring large numbers," *Bull. Amer. Math. Soc.*, v. 37, 1931, pp. 770–776.

20. P. G. L. DIRICHLET & R. DEDEKIND, *On Factoring Large Numbers*, Braunschweig, 1893; reprinted, New York, 1968.

21. H. W. LENSTRA, JR., "On the calculation of regulators and class numbers of quadratic fields," *Journées Arithmétiques* 1980 (J. V. Armitage, ed.), Cambridge Univ. Press, New York, 1982, pp. 123–150.

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

23. H. W. LENSTRA, JR., *Factoring Integers with Elliptic Curves*, preprint, Amsterdam, 1986.

24. G. B. MATHEWS, *Theory of Numbers*, reprinted, Chelsea, New York, 1982.

25. L. MONIER, *Algorithmes de Factorisation d'Entiers*, Thèse d'Informatique, Université Paris Sud, 1980.

26. M. A. MORRISON & J. BRILLHART, "A method of factorization and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 331–334.

27. J. OESTERLE, "Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisé," in *Astérisque* 61 (1979), *Journées Arithmétiques de Luminy*, Soc. Math. de France, 1979, pp. 165–167.

28. J. M. POLLARD, "Theorems on factorisation and primality testing," *Proc. Cambridge Philos. Soc.*, v. 76, 1974, pp. 521–528.

29. C. POMERANCE, "Analysis and comparison of some integer factoring algorithms," *Computational Methods in Number Theory* (R. Tijdeman & H. Lenstra, eds.), Mathematisch Centrum, Amsterdam, Tract 154, 1982, pp. 89–139.

30. K. PRACHAR, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

31. R. A. RANKIN, "The difference between two consecutive prime numbers," *J. London Math. Soc.*, v. 13, 1938, pp. 242–297.

→ R. L. RIVEST, A. SHAMIR & L. ADLEMAN, "A method for obtaining digital signatures and public key cryptosystems," *Comm. ACM*, v. 21, 1978, pp. 120–126.

33. J. SATTLER & C. P. SCHNORR, "Ein Effizienzvergleich der Faktorisierungsverfahren von Morrison-Brillhart und Schroeppel," *Computing*, v. 30, 1983, pp. 91–110.

34. C. P. SCHNORR, "Refined analysis and improvements on some factoring algorithms," *J. Algorithms*, v. 2, 1982, pp. 101–127.

35. C. P. SCHNORR & M. SEYSEN, *An Improved Composition Algorithm*, preprint, Universität Frankfurt, 1984.

36. R. J. SCHOOF, "Quadratic fields and factorisation," *Computational Methods in Number Theory* (R. Tijdeman & H. Lenstra, eds.), Mathematisch Centrum, Amsterdam, Tract 154, 1982, pp. 235–286.

37. I. SCHUR, "Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste," *Nachr. Kön. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, 1918, pp. 30–36. In: *Gesammelte Abhandlungen*, Bd. II, Springer, Berlin, 1973, pp. 239–245.

38. D. 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.

39. V. STRASSEN, "Gaussian elimination is not optimal," *Numer. Math.*, v. 13, 1969, pp. 354–356.

40. V. STRASSEN, "Einige Resultate über Berechnungskomplexität," *Jber. Deutsch. Math.-Verein.*, v. 78, 1976, pp. 1–8.

41. R. S. VARGA, *Matrix Iterative Analysis*, Prentice-Hall, Englewood Cliffs, N. J., 1962.

42. B. L. VAN DER WAERDEN, *Algebra*, Zweiter Teil, Fünfte Auflage, Springer-Verlag, Berlin, 1967.

43. D. WIEDEMANN, "Solving sparse linear equations over finite fields," *IEEE Trans. Inform. Theory*, v. 32, 1986, pp. 54–62.