A rigorous time bound for factoring integers

Lenstra, H.W.; Pomerance, C.

JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 5, Number 3, July 1992

A RIGOROUS TIME BOUND FOR FACTORING INTEGERS

H. W. LENSTRA, JR. AND CARL POMERANCE

1. Introduction

For real numbers x, a and b with $x > e$, we write

$$L_x[a, b] = \exp\left(b(\log x)^a(\log\log x)^{1-a}\right).$$

The main result of the present paper is as follows.

Theorem. *There exists a probabilistic algorithm that factors any given positive integer n completely into prime factors, and that takes expected time at most $L_n[\frac{1}{2}, 1 + o(1)]$ for $n \to \infty$.*

For a discussion of the notions "probabilistic algorithm" and "expected time" we refer to §12. The proof of the theorem is given in §10.

There are many factoring algorithms that are conjectured to have expected running time at most $L_n[\frac{1}{2}, 1 + o(1)]$, including the quite practical quadratic sieve and elliptic curve methods. However, for none of these methods has this conjecture been proved, and for one of them it must be withdrawn, as we shall see below.

The best prior results on rigorously analyzed probabilistic factoring algorithms were a time bound of $L_n[\frac{1}{2}, \sqrt{2} + o(1)]$ obtained by Pomerance [28] and a time bound of $L_n[\frac{1}{2}, \sqrt{4/3} + o(1)]$ by Vallée [33]. These algorithms are refinements of the *random squares method* of Dixon [10].

The algorithm on which the proof of our theorem is based is rather less elementary, and depends on the use of class groups of binary quadratic forms. More precisely, let Δ be a negative integer with $\Delta \equiv 0$ or $1 \bmod 4$, and denote by C_Δ the set of $\mathrm{SL}_2\mathbf{Z}$-equivalence classes of positive definite, primitive, binary quadratic forms of discriminant Δ, where $\mathrm{SL}_2\mathbf{Z}$ denotes the group of 2×2-matrices of determinant 1 with coefficients in the ring $\mathbf{Z}$ of rational integers. Gaussian composition makes C_Δ into a finite abelian group; we shall call its elements simply "forms." In §2 we recall the main properties of C_Δ. In particular, we shall see that there is an explicit correspondence between elements of order dividing 2 in C_Δ, the so-called *ambiguous forms*, and factorizations of $|\Delta|$ into two coprime factors. There are several factoring algorithms that exploit this correspondence. Thus to factor an odd number n that is not a

Received by the editors March 6, 1991.

1991 *Mathematics Subject Classification*. Primary 11Y05, 11R44, 11N25.

Key words and phrases. Factorization algorithm, class groups, binary quadratic forms, smooth numbers.

prime power, one could choose a negative number Δ with $\Delta \equiv 0$ or $1 \bmod 4$ that is a multiple of n, and then somehow find elements of order 2 in C_Δ.

One such algorithm, the *class group relations method*, is due to Seysen [32]. Under the assumption of the generalized Riemann hypothesis (GRH) for L-functions of abelian characters of imaginary quadratic fields, Seysen showed that his method runs in expected time at most $L_n[\frac{1}{2}, \sqrt{5/4} + o(1)]$. A. K. Lenstra [20] improved one of the ingredients of Seysen's algorithm, obtaining the bound $L_n[\frac{1}{2}, 1 + o(1)]$ for the expected running time, but still under the assumption of the GRH.

In the present paper we remove the GRH assumption from the analysis of the Seysen-Lenstra class group relations algorithm. This enables us to prove the theorem.

It may very well be that some variant of the class group relations algorithm has practical value. However, any choices and recommendations we make in this paper are inspired only by the desire to give a valid and efficient proof of our theorem, and not by any practical considerations.

Another algorithm that exploits the connection between ambiguous forms and factorizations of $|\Delta|$ is the *random class groups method* proposed by Schnorr and Lenstra [29]. This algorithm sometimes goes under the name "SPAR," after Shanks, Pollard, Atkin and Rickert. This was the first factoring algorithm of which the expected running time was conjectured to be $L_n[\frac{1}{2}, 1 + o(1)]$, and it is now also the first algorithm for which that conjecture must be withdrawn. Namely, we shall show in the present paper that there is a fairly dense sequence of positive integers n for which the assumption underlying the conjectural running time analysis is incorrect. There is no reason to think that the random class groups method can factor those numbers in time $L_n[\frac{1}{2}, 1 + o(1)]$.

With our theorem, we hoped to bridge the gap between rigorously analyzed factoring algorithms and heuristically analyzed factoring algorithms. Our victory has turned out to be an empty one, however, since in 1989 factoring broke through the $L_n[\frac{1}{2}, 1]$ barrier in a rather dramatic fashion. The number field sieve (see [23; 4]) is conjectured to run in time at most $L_n[\frac{1}{3}, c + o(1)]$, where the current best value for c, due to Coppersmith [6], is $((92+26\sqrt{13})/27)^{1/3} \doteq 1.90188$. This method is practical for numbers of a special form, and may in fact prove to be practical for all numbers.

We now provide a brief description of the tools that we use for avoiding the GRH assumption. The main idea is the use of a multiplier d; that is, instead of working with a single discriminant $\Delta = -n$ or $\Delta = -3n$, whichever is $1 \bmod 4$, we work with the four discriminants $\Delta = -dn$, where d ranges over the set $\{3, 4, 7, 8\}$ if $n \equiv 1 \bmod 4$ and over the set $\{1, 5, 8, 12\}$ if $n \equiv 3 \bmod 4$; for our purposes, any set of four positive integers d for which $-dn \equiv 0$ or $1 \bmod 4$ will do, provided that the product of no two of them is a square and that d is bounded independently of n.

To see how this helps us, let us consider at which points the GRH enters into the proofs in [32] and [20]. It turns out that the GRH is used twice. First, it is needed to guarantee the existence of sufficiently many *smooth forms* in C_Δ. For the definition of smooth forms we refer to (2.9); roughly speaking, they are defined in terms of *smooth numbers*, that is, numbers built up from small prime factors. Proving that there are sufficiently many smooth forms comes down to proving that there are sufficiently many smooth numbers that are built up from prime numbers p for which the Kronecker symbol $(\frac{\Delta}{p})$ equals 1. It is to guarantee the existence of sufficiently many such primes that the GRH is used. We show that for our purposes it suffices that each of two key intervals contains enough such primes p. It is not difficult to see that each of these intervals contains, for all but at most one of the four multipliers d, enough primes p with $(\frac{-dn}{p}) = 1$; but the possible exception d depends on the interval. Sacrificing at most two values of d, we conclude that at least two multipliers d are left for which there do exist enough smooth forms in C_{-dn}.

The second use of the generalized Riemann hypothesis in [32; 20] is that it makes it possible to construct a small set of generators of C_Δ, namely the set of *prime forms* f_p (see (2.7)) for all prime numbers $p \le c_0(\log|\Delta|)^2$ with $(\frac{\Delta}{p}) = 1$; here c_0 is some absolute positive constant. In our algorithm we obtain generators in a different way, namely by choosing $(\log|\Delta|)^{O(1)}$ random prime forms f_p for prime numbers p with $(\frac{\Delta}{p}) = 1$ that range up to the much larger bound $\exp(c_4(\log|\Delta|)^2)$; here c_4 is another absolute positive constant. To prove that this works, it would suffice to show (a) that there are sufficiently many such p, and (b) that the corresponding prime forms f_p are approximately uniformly distributed over C_Δ, so that choosing sufficiently many of them at random, one is very likely to obtain a set of generators for C_Δ. Both (a) and (b) are valid if GRH is true.

Actually, we can neither show (a) nor (b). For (a), we get around this by again sacrificing one of our four multipliers, so that at least one is left. Once (a) is valid, the only obstruction towards a proof of (b) is the possible existence of exceptional zeros of certain Dirichlet L-functions. Since these *cannot* be avoided by the use of a multiplier, it is fortunate that exceptional zeros actually help us: their presence makes it *more* likely that the randomly chosen prime forms generate C_Δ than if (b) were true (see the proof of Theorem 4.1).

Our ideas for removing the GRH assumption do not appear likely to work in the context of [13], where a probabilistic algorithm is given to compute the invariants of the group C_Δ. This algorithm, which is also based on Seysen's class group relations method, is proved to run in expected time $L_{|\Delta|}[\frac{1}{2}, \sqrt{2} + o(1)]$ for $\Delta \to -\infty$ on assumption of GRH. If one tries using a multiplier d, say, to avoid the need for the GRH, then the group C_Δ is changed to the group $C_{d\Delta}$. If d is not a square, then but for the parts annihilated by 2, these groups need bear little resemblance.

The structure of this paper is as follows. In §2 we recall the basic results on class groups that we need. In §3 we prove an estimate of certain character sums for Dirichlet characters of algebraic number fields, with an explicit dependence on possible exceptional zeros of the corresponding L-functions. This result is not new, but it does not appear explicitly in the literature in the form we wish to use, so we give a new proof here. Section 4 is devoted to an algorithm for finding generators of the class group C_Δ. The analysis of this algorithm depends on the result of §3. In particular we show that the algorithm is very likely to find a set of generators of C_Δ provided that a certain interval contains enough primes p with $(\frac{\Delta}{p}) = 1$. In §5 we show how a set of generators can be used to draw random elements from C_Δ, with an approximately uniform distribution. Section 6 contains a result about the distribution of smooth numbers with restricted prime factors. In §7 we discuss the method by which we recognize smooth numbers, which is the elliptic curve factoring method [24]. Unfortunately we are not able to prove that the elliptic curve method can recognize *all* smooth numbers efficiently. For this reason we introduce the notion of a *recognizable* smooth number. A result from [28] shows that not only do recognizable smooth numbers have a good probability of being recognized as smooth by the elliptic curve method, but a fair fraction of smooth numbers are recognizable. The corresponding notion of recognizable smooth forms is studied in §8. In particular, we shall see that there are sufficiently many recognizable smooth forms provided that each of two particular intervals contains enough primes p with $(\frac{\Delta}{p}) = 1$. In this section we also present a supplement to [20], as communicated to us by the author of [20]. In §9 we prove by an elementary argument that the conditions on which §§4 and 8 depend can be achieved by means of a multiplier. In §10 we formulate the basic factoring algorithm, and we show how it leads to a proof of our main result. The reader who just wants to see the algorithm, and is not interested in the proof, can turn directly to §10 after §2 and a glance at Algorithms 4.4 and 7.2.

In §11 we exhibit a serious flaw in the heuristic analysis of the random class groups method, as announced above. Finally, in §12 we indicate, by lack of a suitable reference, what we mean by a probabilistic algorithm and its expected running time. Logically, this section precedes all others, and we assume familiarity with its contents throughout the paper.

All algorithms in this paper are probabilistic, and their running time is measured in bit operations.

Except for §11, when we write "constant" in this paper, we mean an effectively computable, absolute, positive constant, even when this is not explicitly mentioned. The same applies to all constants that are implicit in the O-symbol.

In several algorithms in this paper we need to round real numbers t to integers. For example, in Step 3 of Algorithm 7.2 the number $t = \exp((\log y)^{6/7})$ is rounded down to an integer. We do not mean by this to round it to its integer part $[t]$, since for all we know that might be very hard to compute, namely if t lies very close to an integer. It will be sufficient to round it to an integer m with $0 \le t - m < 2$. It is left to the reader to show that, in all cases when this is done, such an integer m can be efficiently calculated (cf. [3]). A similar convention applies to rounding up.

2. Class groups

In this section we review a few basic facts about class groups of positive definite quadratic forms. For more theoretical and algorithmic information the reader may consult [2; 7; 9; 15; 25; 30].

Let Δ be a negative integer with $\Delta \equiv 0$ or $1 \bmod 4$. Such an integer will be called a *negative discriminant*. A *positive definite primitive binary quadratic* *form* of discriminant Δ is a polynomial $aX^2+bXY+cY^2 \in \mathbf{Z}[X, Y]$ for which

$$(2.1) \qquad \gcd(a, b, c) = 1, \qquad b^2 - 4ac = \Delta, \qquad a > 0.$$

The group $\mathrm{SL}_2\mathbf{Z}$ acts in a natural way on the set of such forms, and each orbit contains exactly one form that satisfies

$$(2.2) \qquad 0 \le b \le a \le c \quad \text{or} \quad 0 < -b < a < c.$$

A form satisfying (2.2) is called *reduced.* There is a *reduction algorithm* that, given any form $aX^2 + bXY + cY^2$ as in (2.1), finds the unique reduced form in the same $\mathrm{SL}_2\mathbf{Z}$-orbit in time $O((\log(|b| + 1) + (\log|\Delta|)^2)\log(a + 1))$.

We denote by C_Δ the set of $\mathrm{SL}_2\mathbf{Z}$-orbits of forms. For algorithmic purposes, we identify C_Δ with the set of triples of integers (a, b, c) satisfying (2.1) and (2.2). The elements of C_Δ will simply be called *forms.*

Each form (a, b, c) satisfies $|b| \le a \le \sqrt{|\Delta|/3}$, and since c is determined by a, b and Δ it follows that C_Δ is finite. Its cardinality is called the *class number* belonging to Δ.

To obtain an explicit upper bound for the class number, note that for each value of a the number of integers b with $-a < b \le a$ and $b \equiv \Delta \bmod 2$ equals a. Therefore

$$(2.3) \qquad \#C_\Delta \le \sum_{a=1}^{[\sqrt{|\Delta|/3}]} a \le \tfrac{1}{6}(|\Delta| + \sqrt{3|\Delta|}) \le \tfrac{1}{3}|\Delta|.$$

Observing that a is a divisor of $b^2 + |\Delta|$ and using an upper bound for the divisor function one can prove that $\#C_\Delta \le |\Delta|^{1/2+o(1)}$ for $\Delta \to -\infty$. By using a more complicated argument involving the average order of a function similar to the divisor function, one can prove that $\#C_\Delta = O(|\Delta|^{1/2}\log|\Delta|)$. In (2.13) we give an explicit upper bound for $\#C_\Delta$ of this nature, derived by other means. Siegel's theorem, which states that $\#C_\Delta = |\Delta|^{1/2+o(1)}$ for $\Delta \to -\infty$, will not be needed in this paper; the lower bound in Siegel's theorem is not effective.

Gaussian composition makes C_Δ into an abelian group, which is called the *class group* corresponding to Δ. The neutral element of C_Δ will be denoted by 1_Δ; it is the unique form $(a, b, c) \in C_\Delta$ with $a = 1$. There is an algorithm that performs the group operation—which will be written as multiplication—in C_Δ in time $O((\log|\Delta|)^3)$. The inverse of (a, b, c) is $(a, -b, c)$ if the latter is reduced, and (a, b, c) otherwise.

(2.4) *Ambiguous forms.* An ambiguous form is an element $f \in C_\Delta$ of order dividing 2. The ambiguous forms form a subgroup of C_Δ, which is denoted by $C_{\Delta,2}$. A form (a, b, c) is ambiguous if and only if it is equal to its own inverse, which by the above is equivalent to

$$b = 0 \quad \text{or} \quad b = a \quad \text{or} \quad a = c.$$

In these three cases we see from (2.1) that

$$\Delta = -4a \cdot c \quad \text{or} \quad a \cdot (a - 4c) \quad \text{or} \quad (b - 2a) \cdot (b + 2a),$$

respectively, where the gcd of the two factors on the right divides 4. Hence, removing factors 2 and passing to absolute values, we see that each element of $C_{\Delta,2}$ gives rise to a coprime factorization of the largest odd divisor of Δ. Let $\mathscr{F}$ be the set of these factorizations; so an element of $\mathscr{F}$ is an unordered pair d_0, d_1 of odd coprime positive integers with $-2^k \cdot d_0 \cdot d_1 = \Delta$ for some $k \in \mathbf{Z}_{\geq 0}$.

Theorem 2.5. *Let t be the number of distinct prime factors of Δ. The order of $C_{\Delta,2}$ is equal to 2^t if $\Delta \equiv 0 \bmod 32$, to 2^{t-2} if $\Delta \equiv 4 \bmod 16$, and to 2^{t-1} in all remaining cases. Further, the map $C_{\Delta,2} \to \mathscr{F}$ defined above is surjective, and the number of elements of $C_{\Delta,2}$ mapping to any given element of $\mathscr{F}$ is equal to 1 if Δ is odd or $\Delta \equiv 4 \bmod 16$, to 4 if $\Delta \equiv 0 \bmod 32$, and to 2 in all remaining cases.*

Proof. This is a classical result, which is proved by a straightforward computation. See [7, Proposition 3.11] and the references given there.

Remark. It can be shown that the map $C_{\Delta,2} \to \mathscr{F}$ is a group homomorphism if one makes $\mathscr{F}$ into a group by letting the product of the factorizations $d_0 \cdot d_1$ and $e_0 \cdot e_1$ be the factorization $(\operatorname{lcm}(d_0, e_0)/\gcd(d_0, e_0)) \cdot (\operatorname{lcm}(d_0, e_1)/\gcd(d_0, e_1))$.

(2.6) *The Kronecker symbol.* For any integer d that is 0 or 1 mod 4 and any positive integer a, the Kronecker symbol $(\frac{d}{a})$ is defined as follows. First let p be prime. If p divides d then $(\frac{d}{p}) = 0$. If p does not divide d, then $(\frac{d}{p})$ is 1 if d is a square modulo $4p$ and -1 otherwise. Finally, the definition is extended to nonprime numbers by the rule $(\frac{d}{ab}) = (\frac{d}{a})(\frac{d}{b})$. Note that the Kronecker symbol is equal to the Jacobi symbol when both are defined.

(2.7) *Prime forms.* We write

$$\mathscr{P}_\Delta = \{p : p \text{ is prime}, (\tfrac{\Delta}{p}) = 1\}.$$

If p is even, then $p \in \mathscr{P}_\Delta$ if and only if $p = 2$ and $\Delta \equiv 1 \bmod 8$, by (2.6). If p is odd, then $p \in \mathscr{P}_\Delta$ if and only if $\Delta^{(p-1)/2} \equiv 1 \bmod p$ and p passes a primality test, for example the Jacobi sum test [1; 26]. It follows that a positive integer p can be tested for membership in $\mathscr{P}_\Delta$ in time $O((\log|\Delta|)\log p) + (\log p)^{O(\log\log\log p)}$ (for $p > e^e$).

Let $p \in \mathscr{P}_\Delta$. We claim that there is a unique integer $b = b_p$ for which $0 < b < p$ and $b^2 \equiv \Delta \bmod 4p$. For $p = 2$ this is obvious. For $p > 2$, it follows from $(\frac{\Delta}{p}) = 1$ that there are exactly two integers b for which $0 < b < p$ and $b^2 \equiv \Delta \bmod p$, and that they add up to p; the one that has the same parity as Δ is b_p.

Let $p \in \mathscr{P}_\Delta$ and b_p be as just defined. Then $pX^2 + b_pXY + ((b_p^2 - \Delta)/(4p))Y^2$ is a positive definite primitive binary quadratic form of discriminant Δ. We denote its $\mathrm{SL}_2\mathbf{Z}$-orbit by f_p, which is an element of C_Δ. We call f_p the *prime form* corresponding to p.

Given $p \in \mathscr{P}_\Delta$, the prime form f_p can be computed by means of a probabilistic algorithm that runs in expected time $O((\log \max\{p, |\Delta|\})^3)$; namely, one first calculates b_p using a probabilistic algorithm for factoring $X^2 - (\Delta \bmod p)$ over $\mathbf{Z}/p\mathbf{Z}$ (see [19]), and next one applies the reduction algorithm mentioned above to $(p, b_p, (b_p^2 - \Delta)/(4p))$.

(2.8) *Factoring forms into prime forms.* Let $(a, b, c) \in C_\Delta$ be such that $\gcd(a, \Delta) = 1$. From $b^2 \equiv \Delta \bmod 4a$ it follows that each prime divisor p of a belongs to $\mathscr{P}_\Delta$. Moreover, if $t(p)$ denotes the number of factors p in a, then we have

$$(a, b, c) = \prod_{p|a} f_p^{e(p)t(p)},$$

where $e(p) \in \{1, -1\}$ is such that $b \equiv e(p)b_p \bmod 2p$. Note that from $a \leq \sqrt{|\Delta|/3}$ it follows that the number of primes p appearing in the product is less than $\log|\Delta|$.

(2.9) *Smooth forms.* Let y be a real number. A positive integer a is called *y-smooth* if a does not have any prime factors exceeding y. An element $(a, b, c) \in C_\Delta$ is called *y-smooth* if a is y-smooth and $\gcd(a, \Delta) = 1$. The following result will be used to estimate the number of smooth forms.

Lemma 2.10. *Let a be an integer with $1 \leq a \leq \frac{1}{2}\sqrt{|\Delta|}$ all of whose prime factors belong to $\mathscr{P}_\Delta$. Then there exist $b, c \in \mathbf{Z}$ such that $(a, b, c) \in C_\Delta$.*

Proof. Since all prime factors of a belong to $\mathscr{P}_\Delta$, there exists $b \in \mathbf{Z}$ with $b^2 \equiv \Delta \bmod 4a$; note that $\gcd(a, b) = 1$ for any such b. Adding multiples of $2a$ to b we can achieve that $-a < b \leq a$. The integer $c = (b^2 - \Delta)/(4a)$ satisfies $4ac = b^2 + |\Delta| \geq |\Delta| \geq 4a^2$, and equality is possible only if $b = 0$. It follows that (2.1) and (2.2) hold, so $(a, b, c) \in C_\Delta$. This proves Lemma 2.10.

(2.11) *Class number formula.* Let the character $\chi: \mathbf{Z}_{>0} \to \{-1, 0, 1\}$ be defined by $\chi(a) = \left(\frac{\Delta}{a}\right)$ (see (2.6)). For a complex number s with $\operatorname{Re} s > 0$ we put

$$L(s, \chi) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^s},$$

which for $\operatorname{Re} s > 1$ equals $\prod_p (1 - \chi(p)p^{-s})^{-1}$, where p runs through the prime numbers. Then we have

$$\#C_\Delta = \frac{w\sqrt{|\Delta|}}{2\pi} \cdot L(1, \chi), \tag{2.12}$$

where $w = 6$ for $\Delta = -3$, $w = 4$ for $\Delta = -4$, and $w = 2$ for $\Delta < -4$. It was proved by Schur [31] that

$$L(1, \chi) < \tfrac{1}{2}\log|\Delta| + \log\log|\Delta| + 1.$$

From this it follows that

$$\#C_\Delta < \sqrt{|\Delta|} \cdot \log|\Delta|. \tag{2.13}$$

3. A CHARACTER SUM ESTIMATE

In this section we prove a character sum estimate for Dirichlet characters of algebraic number fields. This estimate is essentially known (see [17] and the references cited there), but we have not been able to find a statement in the literature that gives an explicit and effective dependence on all parameters involved. Since that is what we need, we present a proof in this section.

By $\mathbf{C}$ we denote the field of complex numbers, and by $\mathbf{C}^*$ its multiplicative group. For background on algebraic number theory we refer to [18]

Let K be an algebraic number field, i.e., a field extension of finite degree of the field $\mathbf{Q}$ of rational numbers We write $\mathscr{O}$ for the ring of integers of K and $\mathscr{I}$ for the group of fractional ideals of $\mathscr{O}$. By a *cycle* $\mathfrak{m}$ of K we mean a formal product $\prod \mathfrak{p}^{m(\mathfrak{p})}$ extending over all primes $\mathfrak{p}$ of K, where the $m(\mathfrak{p})$ are nonnegative integers that are almost all 0, with $m(\mathfrak{p}) = 0$ for complex $\mathfrak{p}$ and $m(\mathfrak{p}) \leq 1$ for real $\mathfrak{p}$. If $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ is a cycle, then $\mathscr{I}(\mathfrak{m})$ denotes the subgroup of $\mathscr{I}$ generated by the finite primes $\mathfrak{p}$ for which $m(\mathfrak{p}) = 0$, and $P_{\mathfrak{m}} \subset \mathscr{I}(\mathfrak{m})$ is the subgroup generated by the nonzero ideals of the form $\mathscr{O}\alpha$, where $\alpha \in \mathscr{O}$ is such that $\alpha \equiv 1 \bmod \mathfrak{p}^{m(\mathfrak{p})}$ for each finite prime $\mathfrak{p}$, and $\alpha > 0$ under each embedding of K in the field of real numbers corresponding to a real prime $\mathfrak{p}$ with $m(\mathfrak{p}) = 1$ The *norm* $\mathfrak{N}(\mathfrak{m})$ of a cycle $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ is defined to be the number $\prod \mathfrak{N}(\mathfrak{p})^{m(\mathfrak{p})}$, where $\mathfrak{p}$ in the latter product ranges only over the finite primes, and $\mathfrak{N}(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$.

By a *Dirichlet character* of K we mean a pair consisting of a cycle $\mathfrak{m}$ of K and a group homomorphism $\chi . \mathscr{I}(\mathfrak{m}) \to \mathbf{C}^*$ such that $P_{\mathfrak{m}}$ is contained in the kernel of χ. We shall, by abuse of language, simply refer to χ as a Dirichlet character, and call $\mathfrak{m}$ the *modulus* of χ. A character is called *principal* if it maps all elements of $\mathscr{I}(\mathfrak{m})$ to 1. We extend any Dirichlet character χ to a map $\mathscr{I} \to \mathbf{C}$, also denoted by χ, by putting $\chi(\mathfrak{a}) = 0$ whenever $\mathfrak{a} \in \mathscr{I}$, $\mathfrak{a} \notin \mathscr{I}(\mathfrak{m})$. The Dirichlet L-series $L(s, \chi)$ of a Dirichlet character χ is defined by

$$L(s, \chi) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s},$$

the sum ranging over the set of nonzero ideals $\mathfrak{a}$ of $\mathscr{O}$, and $\mathfrak{N}(\mathfrak{a})$ denoting the norm of $\mathfrak{a}$. This series is absolutely convergent for all $s \in \mathbf{C}$ with $\operatorname{Re} s > 1$. It can be analytically continued to a meromorphic function on $\mathbf{C}$, it is entire if χ is nonprincipal, and it has a single pole, which is simple, at $s = 1$ if χ is principal.

Let χ and χ' be Dirichlet characters of K with moduli $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ and $\mathfrak{m}' = \prod \mathfrak{p}^{m'(\mathfrak{p})}$, respectively. Then χ is said to be *induced* by χ' if $\mathfrak{m}'$ divides $\mathfrak{m}$—that is, $m'(\mathfrak{p}) \leq m(\mathfrak{p})$ for all $\mathfrak{p}$—and χ is the composition of the inclusion $\mathscr{I}(\mathfrak{m}) \subset \mathscr{I}(\mathfrak{m}')$ and the map $\chi' \cdot \mathscr{I}(\mathfrak{m}') \to \mathbf{C}^*$. A Dirichlet character is called *primitive* if it is not induced by any character different from itself. Each Dirichlet character χ is induced by exactly one primitive character, and the modulus of the latter is called the *conductor* of χ.

By class field theory, the primitive characters of an algebraic number field K can be identified with the one-dimensional continuous characters of the Galois group of the algebraic closure of K over K. The Dirichlet L-series of a primitive character χ coincides with the Artin L-series of χ when viewed as a character of the Galois group. These are the L-series that occur in [17]; so when we make use of [17], as we shall frequently do in this section, we have to restrict to primitive characters. In [16] this restriction is dropped; what is called "Hecke character" and "conductor" in that paper is called "Dirichlet character" and "modulus" here.

For a nonzero ideal $\mathfrak{a}$ of $\mathscr{O}$, we define $\Lambda(\mathfrak{a}) = \log \mathfrak{N}(\mathfrak{p})$ if $\mathfrak{a} = \mathfrak{p}^k$ for some prime ideal $\mathfrak{p}$ and some positive integer k, and $\Lambda(\mathfrak{a}) = 0$ otherwise. The main result of this section is an estimate for the sum

$$\psi(x, \chi) = \sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \chi(\mathfrak{a})\Lambda(\mathfrak{a}),$$

the sum ranging over nonzero ideals $\mathfrak{a}$ of $\mathscr{O}$.

We introduce some additional notation. For an algebraic number field K, we write n_K for the degree of K over $\mathbf{Q}$ and Δ_K for the discriminant of K over $\mathbf{Q}$. When χ is a Dirichlet character of a number field K, with modulus $\mathfrak{m}$, then we write

$$A(\chi) = |\Delta_K| \mathfrak{N}(\mathfrak{m}),$$
$$\mathscr{M}(x, \chi) = \log A(\chi) + n_K \log(x + 2),$$

for any nonnegative real number x.

Theorem 3.1. *There are effectively computable positive constants* c_1 *and* c_2 *such that for all algebraic number fields* K, *all Dirichlet characters* χ *of* K *and all real numbers* $x \geq 2$ *one has*

$$\left| \psi(x, \chi) - \delta(\chi)x + \sum_{\rho \in S(\chi)} \frac{x^\rho}{\rho} \right| \\ \leq c_2 x \mathscr{M}(x, \chi)(\log x) A(\chi)^{1/(2n_K)} \exp\left(- \sqrt{\frac{c_1}{n_K} \log x} \right).$$

Here we write $\delta(\chi) = 1$ *or* 0 *according as* χ *is principal or not, and* $S(\chi)$ *denotes the set of real zeros of* $L(s, \chi)$ *that exceed* $1 - c_1/\mathscr{M}(0, \chi)$

Remark The set $S(\chi)$ in this theorem consists of the "Siegel zeros" of $L(s, \chi)$, and it satisfies $\#S(\chi) \leq 1$ (by Lemma 3.5).

Proof In this proof, we abbreviate $\mathscr{M}(x, \chi)$ to $\mathscr{M}(x)$. We first give the proof with the additional assumption that χ is primitive. This assumption will be removed at the end. Our proof leans heavily on arguments from [17].

Let $x \geq 2$. We begin by approximating $\psi(x, \chi)$ with the negative of the truncated inverse Mellin transform

$$I_\chi(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{L'}{L}(s, \chi)\, ds,$$

where $\sigma_0 = 1 + (\log x)^{-1}$ and $T \geq 2$, and the path of integration is a vertical line segment. We have

$$-\frac{L'}{L}(s, \chi) = \sum_{\mathfrak{a}\neq 0} \frac{\chi(\mathfrak{a})\Lambda(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s},$$

where the sum is over nonzero ideals $\mathfrak{a}$ of $\mathscr{O}$. The convergence is uniform for $\operatorname{Re} s = \sigma_0 > 1$, so

$$I_\chi(x, T) = -\frac{1}{2\pi i}\sum_{\mathfrak{a}\neq 0} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) \int_{\sigma_0 - iT}^{\sigma_0+iT} \frac{1}{s}\frac{x^s}{\mathfrak{N}(\mathfrak{a})^s}\,ds.$$

Applying Lemma 3.1 from [17] to each of the integrals, we find that

$$|I_\chi(x, T) + \psi(x, \chi)| \leq \Big(\sum_{\mathfrak{a},\, \mathfrak{N}(\mathfrak{a})=x} (\tfrac{1}{2} + \sigma_0 T^{-1})\Lambda(\mathfrak{a})\Big) + R_0(x, T),$$

where the error term $R_0(x, T)$ is given by [17, (3.9) (p. 424)]. The sum on the right, which corresponds to a term that is incorrectly given in [17, (3.8)], is easily seen to be $O(n_K \log x)$ for $x \geq 2$, $T \geq 2$ and σ_0 as above. From the estimate [17, (3.17) (p. 428)] for $R_0(x, T)$ we find

$$I_\chi(x, T) + \psi(x, \chi) = O\Big(n_K \log x + \frac{n_K}{T} x(\log x)^2\Big) \tag{3.2}$$

for $x \geq 2$, $T \geq 2$, which is our approximation of $\psi(x, \chi)$ by $-I_\chi(x, T)$.

To estimate $I_\chi(x, T)$ we use the last displayed equation on p. 450 of [17]. Correcting a sign error, we find that

$$\begin{aligned} I_\chi(x, T) + \delta(\chi)x - \sum_{\rho,\, |\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} + \sum_{\rho,\, |\rho|<1/2} \frac{1}{\rho} \\ = O\Big(\mathscr{M}(x) + \frac{\mathscr{M}(T)}{T} x \log x\Big) \end{aligned} \tag{3.3}$$

for $x \geq 2$, $T \geq 2$, if T does not coincide with the absolute value of the imaginary part of any zero of $L(s, \chi)$. The sum over ρ, here and below, extends over the zeros of $L(s, \chi)$ for which $0 < \operatorname{Re}\rho < 1$, with the proper multiplicities. It is for the proof of (3.3), given in [17], that we need χ to be primitive; this assumption is needed for the existence of the functional equation for $L(s, \chi)$.

We now quote two results about the zeros ρ of $L(s, \chi)$.

Lemma 3.4. *There is an effectively computable constant c_3 such that for any Dirichlet character χ of any algebraic number field, and any real number t, the number of zeros ρ of $L(s, \chi)$ with $0 < \operatorname{Re}\rho < 1$, $|t - \operatorname{Im}\rho| \leq 1$, counting multiplicities, is at most $c_3\mathscr{M}(|t|)$.*

Proof. This is Lemma 5.4 of [17] in the case that χ is primitive, which is the only case that we shall need; for the general case, see [16, Lemma 2.1].

Lemma 3.5. *There is an effectively computable positive constant $c_1 < 1/3$ with the following properties. For each algebraic number field K and each Dirichlet character χ of K the Dirichlet L-function $L(s, \chi)$ has at most one zero ρ with*

$$\operatorname{Re}\rho > 1 - \frac{c_1}{\mathscr{M}(0)}, \qquad |\operatorname{Im}\rho| \leq \frac{c_1}{\mathscr{M}(0)}.$$

If this zero exists, then it is real and simple and χ^2 is principal. Every other zero ρ of $L(s, \chi)$ satisfies

$$\operatorname{Re}\rho \leq 1 - \frac{c_1}{\mathscr{M}(|\operatorname{Im}\rho|)}.$$

Proof. This is Lemma 2.3 in [16].

We remark that $0 < c_1 < 1/3$ implies that

$$\frac{c_1}{\mathscr{M}(T)} \leq \frac{c_1}{\mathscr{M}(0)} \leq \frac{c_1}{\log 2} < \frac{1}{2}$$

for every real number $T \geq 0$, a fact that we shall use several times.

Let $T \geq 2$. From Lemma 3.4, we have

$$\sum_{\substack{\rho,\, |\rho| \geq 1/2 \\ |\operatorname{Im}\rho| < T}} \frac{1}{|\rho|} = O(\mathscr{M}(T)\log T).$$

Denote by $\sum'$ a sum over zeros ρ of $L(s, \chi)$ with $0 < \operatorname{Re}\rho < 1$ and $\rho \notin S(\chi)$, where $S(\chi)$ is as in Theorem 3.1. Combining the estimate just proved with the last assertion of Lemma 3.5 we find that

$$\text{(3.6)} \qquad \sum_{\substack{\rho,\, |\rho| \geq 1/2 \\ |\operatorname{Im}\rho| < T}}{}' \frac{x^\rho}{\rho} = O(x^{1-c_1/\mathscr{M}(T)}\mathscr{M}(T)\log T).$$

By Lemma 3.4 there are at most $c_3\mathscr{M}(0)$ zeros ρ of $L(s, \chi)$ with $\operatorname{Re}\rho > 0$ and $|\rho| < \frac{1}{2}$. For each of these zeros we have

$$|x^\rho - 1| = \left|\int_0^\rho x^s(\log x)\, ds\right| < |\rho| x^{1/2}\log x.$$

Hence

$$\sum_{\rho,\, |\rho| < 1/2} \left(\frac{-x^\rho}{\rho} + \frac{1}{\rho}\right) = O(x^{1/2}(\log x)\mathscr{M}(0)) = O(x^{1-c_1/\mathscr{M}(T)}\mathscr{M}(T)).$$

Combining this estimate with (3.6), we obtain

$$-\sum_{\rho,\, |\operatorname{Im}\rho| < T}{}' \frac{x^\rho}{\rho} + \sum_{\rho,\, |\rho| < 1/2} \frac{1}{\rho} = O(x^{1-c_1/\mathscr{M}(T)}\mathscr{M}(T)\log T).$$

Putting this into (3.3) we conclude from (3.2) that if x, T are real numbers with $2 \leq T \leq x$, and T is not the absolute value of the imaginary part of any zero of $L(s, \chi)$, then we have

$$\text{(3.7)} \qquad \psi(x, \chi) - \delta(\chi)x + \sum_{\rho \in S(\chi)} \frac{x^\rho}{\rho} = O(x\mathscr{M}(x)(\log x)(T^{-1} + x^{-c_1/\mathscr{M}(T)})).$$

Since the left side does not depend on T, we can now drop the restriction that T is not the absolute value of the imaginary part of any zero of $L(s, \chi)$.

Let

$$T = A(\chi)^{-1/(2n_K)} \exp\left(\sqrt{\frac{c_1}{n_K}\log x}\right) - 2.$$

If $T < 2$, then we have

$$A(\chi)^{1/(2n_K)} \exp\left(- \sqrt{\frac{c_1}{n_K} \log x} \right) > \frac{1}{4}.$$

In this case the inequality in the theorem holds with a suitable c_2, because $\psi(x, \chi) = O(n_K x)$ for $x \geq 2$. Assume now that $T \geq 2$. From

$$\mathcal{M}(T) = \tfrac{1}{2} \log A(\chi) + \sqrt{c_1 n_K \log x}$$

and an easy calculation one sees that $\mathcal{M}(T) \log(T+2) \leq c_1 \log x$, and therefore

$$T < x^{c_1/\mathcal{M}(T)} < x, \tag{3.8}$$

so that we may use this value of T in (3.7). But (3.8) shows that the right-hand side of (3.7) is $O(2x\mathcal{M}(x)(\log x)/T)$, which implies the theorem, in the case that χ is primitive.

In the general case, let χ' be the primitive character that induces χ, and $\mathfrak{m}'$ the modulus of χ'. Then we have

$$\psi(x, \chi') = \psi(x, \chi) + \sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \chi'(\mathfrak{a})\Lambda(\mathfrak{a}),$$

with $\mathfrak{a}$ ranging only over those ideals of $\mathcal{O}$ that are powers of prime ideals $\mathfrak{p}$ that divide $\mathfrak{m}$ but not $\mathfrak{m}'$. Since each such $\mathfrak{p}$ contributes $[(\log x)/\log \mathfrak{N}(\mathfrak{p})]$ terms to the sum, we find that

$$\psi(x, \chi') - \psi(x, \chi) = O\left(\sum_{\mathfrak{p}} \log x \right) = O((\log \mathfrak{N}(\mathfrak{m}/\mathfrak{m}')) \log x).$$

Now we apply (3.7) for the primitive character χ'. Note that

$$A(\chi')\mathfrak{N}(\mathfrak{m}/\mathfrak{m}') = A(\chi), \qquad \mathcal{M}(x, \chi') + \log \mathfrak{N}(\mathfrak{m}/\mathfrak{m}') = \mathcal{M}(x, \chi),$$
$$\delta(\chi') = \delta(\chi), \qquad S(\chi') \supset S(\chi)$$

(cf. [16, (2.9) (p. 276)]). From Lemma 3.5 we see that

$$\sum_{\rho \in S(\chi'),\, \rho \notin S(\chi)} \frac{x^{\rho}}{\rho} = O(x \cdot x^{-c_1/\mathcal{M}(0\ \chi)}).$$

It follows that (3.7) also holds for χ, for $2 \leq T \leq x$, and we obtain the desired inequality in the same way.

This proves Theorem 3.1.

4. Generators of the class group

Let Δ be a negative discriminant. This section is devoted to an algorithm for finding a set of generators of C_Δ. We prove that it is likely to be successful provided that the set $\mathcal{P}_\Delta$ (see (2.7)) contains enough prime numbers up to a certain bound z (condition (4.3)). We write $\pi(x, \mathcal{P}_\Delta) = \#\{p \in \mathcal{P}_\Delta : p \leq x\}$ for a positive real number x.

Theorem 4.1. *There is an effectively computable positive constant c_4 with the following property. Let Δ be a negative discriminant and z a real number satisfying*

$$z > \exp(c_4(\log|\Delta|)^2), \tag{4.2}$$

$$\pi(z; \mathscr{P}_\Delta) \geq \frac{z}{6\log z}. \tag{4.3}$$

Further let H be a subgroup of C_Δ with $H \neq C_\Delta$. Then we have

$$\#\{p \in \mathscr{P}_\Delta : p \leq z, f_p \notin H\} \geq \frac{z}{20\log z}.$$

Proof. We begin by recalling the connection between C_Δ and the ideal groups of the previous section.

Let K be the field $\mathbf{Q}(\sqrt{\Delta})$ and $\mathscr{O}$ the ring of integers of K. Denote by Δ_K the discriminant of K over $\mathbf{Q}$. It is well known that there is a positive integer f with $\Delta = \Delta_K f^2$; namely, f is the index of $\mathbf{Z}[(\Delta + \sqrt{\Delta})/2]$ in $\mathscr{O}$. Let $\mathfrak{m}$ be the $\mathscr{O}$-ideal $f\mathscr{O}$; replacing $\mathfrak{m}$ by its prime ideal factorization, we shall view $\mathfrak{m}$ as a cycle of K. Let $\mathscr{I}(\mathfrak{m})$, $P_\mathfrak{m}$ be as in §3. There is a surjective group homomorphism $\mathscr{I}(\mathfrak{m}) \to C_\Delta$, the kernel of which is generated by the set of nonzero ideals of the form $\mathscr{O}\alpha$, where $\alpha \in \mathscr{O}$ is such that $\alpha \equiv k \bmod f\mathscr{O}$ for some $k \in \mathbf{Z}$ with $\gcd(k, f) = 1$; see [7, Proposition 7.22]. Note that $P_\mathfrak{m}$ is contained in this kernel. Checking the definition of the map one finds that for each prime number p with $(\frac{\Delta}{p}) = 1$ the two prime ideals of norm p in $\mathscr{I}(\mathfrak{m})$ are sent to the elements $f_p^{\pm 1}$ of C_Δ.

Let H be as in the theorem, and choose a nontrivial group homomorphism $\lambda: C_\Delta \to \mathbf{C}^*$ with $H \subset \ker\lambda$. Denote by χ the composed map $\mathscr{I}(\mathfrak{m}) \to C_\Delta \to \mathbf{C}^*$. By the above, this is a nonprincipal Dirichlet character of K with modulus $\mathfrak{m}$.

Now let z be as in the theorem, with c_4 sufficiently large, as dictated by the proof. We compare two expressions for $\psi(z, \chi)$. The first is found from Theorem 3.1, with $x = z$. We have

$$A(\chi) = |\Delta|, \qquad \mathscr{M}(z, \chi) = \log|\Delta| + 2\log(z+2), \qquad \delta(\chi) = 0,$$

and from $z > \exp(c_4(\log 3)^2)$ it follows that the condition $z \geq 2$ of Theorem 3.1 is satisfied for c_4 sufficiently large. Hence we find

$$\left|\psi(z, \chi) + \sum_{\rho \in S(\chi)} \frac{z^\rho}{\rho}\right|$$
$$\leq c_2 z(\log|\Delta| + 2\log(z+2))(\log z)|\Delta|^{1/4} \exp\left(-\sqrt{\frac{c_1}{2}\log z}\right).$$

Using that $|\Delta| < \exp(\sqrt{(\log z)/c_4})$ one easily sees that the right-hand side is less than $z/100$, for c_4 sufficiently large. Therefore

$$\psi(z, \chi) = s_0 - \sum_{\rho \in S(\chi)} \frac{z^\rho}{\rho}, \quad \text{where } |s_0| < \frac{z}{100}.$$

The second expression for $\psi(z, \chi)$ is obtained from its definition

$$\psi(z, \chi) = \sum_{\mathfrak{N}(\mathfrak{a}) \le z} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = s_1 + s_2 + s_3$$

Here s_1 is the sum over those $\mathfrak{a}$ for which $\mathfrak{N}(\mathfrak{a}) = p^a$ for some prime number $p \le z^{1/2}$ and some integer $a \ge 1$, and s_2, s_3 are the sums over those prime ideals $\mathfrak{a} = \mathfrak{p}$ whose norm is a prime number p satisfying $z^{1/2} < p \le z$ and for which the image of $\mathfrak{p}$ under the map $\mathscr{I}(\mathfrak{m}) \to C_\Delta$ is or is not in H, respectively

For each prime number $p \le z^{1/2}$, the ideals $\mathfrak{a}$ of p-power norm contribute at most $2 \log z$ to s_1, so $|s_1| \le 2z^{1/2} \log z$ Note that for c_4 sufficiently large all primes $\mathfrak{p}$ dividing Δ are subsumed in s_1, as we shall now assume

The norm of each $\mathfrak{a} = \mathfrak{p}$ occurring in s_3 belongs to the set

$$\mathscr{H} = \{p \;\; p \in \mathscr{P}_\Delta,\, z^{1/2} < p \le z,\, f_p \notin H\}$$

Conversely, each $p \in \mathscr{H}$ gives rise to two $\mathfrak{p}$'s in s_3 Therefore $|s_3| \le 2 \cdot \#\mathscr{H}$ $\log z$

By construction, we have $\chi(\mathfrak{p}) = 1$ for each $\mathfrak{a} = \mathfrak{p}$ that appears in s_2, so s_2 is a nonnegative real number Each prime number $p \in \mathscr{P}_\Delta$ with $z^{1/2} < p \le z$, $p \notin \mathscr{H}$, gives rise to two $\mathfrak{p}$'s in s_2 Using (4 3) we thus find

$$s_2 \ge 2\left(\frac{z}{6 \log z} - z^{1/2} - \#\mathscr{H}\right) \log(z^{1/2})$$

The two expressions for $\psi(z, \chi)$ combine to show that

$$s_2 + \sum_{p \in S(\chi)} \frac{z^p}{p} = s_0 - s_1 - s_3$$

Using the inequalities for the s_i, and noticing that the sum over $S(\chi)$ is a nonnegative real number, we find that

$$\left(\frac{z}{6 \log z} - z^{1/2} - \#\mathscr{H}\right) \log z \le \frac{z}{100} + 2z^{1/2} \log z + 2 \cdot \#\mathscr{H} \log z,$$

For c_4 sufficiently large, this implies that $\#\mathscr{H} \ge z/(20 \log z)$ From the definition of $\mathscr{H}$ given above we see that this estimate proves Theorem 4 1

Algorithm 4.4. We describe an algorithm that, given a negative discriminant Δ and a positive integer z, produces a set $\mathscr{G}$ of elements of C_Δ that, under suitable hypotheses, is likely to generate C_Δ (see Theorem 4 5) Initially, $\mathscr{G}$ is empty

Draw a random positive integer p with $p \le z$, from a uniform distribution Test whether p belongs to $\mathscr{P}_\Delta$, as in (2 7) If it does, determine the prime form $f_p \in C_\Delta$ as in (2 7), and add it to the set $\mathscr{G}$

Repeat the above $60(\log|\Delta|) \log z$ times (rounded up to an integer) This completes the description of the algorithm

Remark We will apply this algorithm with $\log z = O((\log|\Delta|)^2)$ (cf (4 2))

Theorem 4.5. *If z satisfies* (4.2), *then the expected running time of Algorithm* 4.4 *is* $(\log z)^{O(\log\log\log z)}$, *and the set $\mathscr{G}$ determined by the algorithm satisfies $\#\mathscr{G} < 2 + 60(\log|\Delta|)\log z$. If in addition* (4.3) *is satisfied, then the set $\mathscr{G}$ determined by the algorithm generates C_Δ with probability at least $\frac{1}{2}$.*

Proof. The running time estimate is straightforward from (2.7), and the upper bound for $\#\mathscr{G}$ is obvious.

To estimate the success probability of the algorithm, let us first consider the variant of the algorithm that does *not* stop after having processed $60(\log|\Delta|)\log z$ values of p. Let, at each stage of that algorithm, H denote the subgroup of C_Δ generated by $\mathscr{G}$; so initially $H = \{1_\Delta\}$. As long as H is different from C_Δ, the next p that is drawn will enlarge H with probability at least $1/(20\log z)$, by Theorem 4.1. Hence the expected number of p's that one needs to draw until H changes is at most $20\log z$. Adding up expectations, one finds that the expected number of p's that one needs to draw until H either becomes equal to C_Δ or has changed k times is at most $20k\log z$, for any nonnegative integer k.

From $\#C_\Delta < |\Delta|$ (see (2.3)) it follows that the longest strictly increasing chain of proper subgroups of C_Δ has length at most $[(\log|\Delta|)/\log 2]$. Thus the expected number of p's that one needs to draw until $H = C_\Delta$ is at most

$$20(\log z)(\log|\Delta|)/\log 2 < 30(\log z)\log|\Delta|.$$

We conclude that drawing twice as many p's—as the actual algorithm does—will guarantee that in the end H equals C_Δ with probability at least $\frac{1}{2}$.

This proves Theorem 4.5.

Remark. One obtains a more efficient algorithm, running in expected time $(\log z)^{O(1)}$, by omitting the Jacobi sum primality test in (2.7), and discarding p if the construction of f_p is unsuccessful within a reasonable amount of time.

Remark. We know of no efficient way to test whether or not the set $\mathscr{G}$ determined by the algorithm actually generates C_Δ. If it does not, then a later algorithm that depends on 4.4 may fail; this provides an indirect test.

Remark. To achieve success probability at least $1 - 2^{-k}$, for a positive integer k, it suffices to investigate k times as many values of p. To prove this, apply Theorem 4.5 to k successive independent runs of the algorithm.

5. Random forms

In the present section we prove that, given a set $\mathscr{G}$ of generators of a class group C_Δ, we can find random elements of C_Δ with an approximately uniform distribution.

Lemma 5.1. *Let m, h, d, b be positive integers with $d \le b$, and $\Lambda \subset \mathbf{Z}^m$ a subgroup of index h with $(d\mathbf{Z})^m \subset \Lambda$. Further let $\mathscr{C} \subset \mathbf{Z}^m$ be a coset of Λ. Then*

$$\#(\{1, 2, \dots, b\}^m \cap \mathscr{C}) = \frac{b^m}{h}\exp\epsilon$$

for some real number ϵ *satisfying*

$$|\epsilon| \le \frac{\min\{h-1, m(d-1)\}}{b-d+1}.$$

Proof. By Lemma (4.1) in [20] and its proof, there are positive integers h_1, $\dots$, h_m dividing d for which $\prod_{i=1}^m h_i = h$ and

$$\prod_{i=1}^m \left(1 - \frac{h_i - 1}{b}\right) \le \frac{h}{b^m} \cdot \#(\{1, 2, \dots, b\}^m \cap \mathscr{C}) \le \prod_{i=1}^m \left(1 + \frac{h_i - 1}{b}\right).$$

Combining this with the inequalities $\log(1+x) \le x$ (for $x \ge 0$) and $|\log(1-x)| = \log(1 + x/(1-x)) \le x/(1-x)$ (for $0 \le x < 1$) we obtain

$$|\epsilon| \le \sum_{i=1}^m \left(\frac{h_i - 1}{b - h_i + 1}\right) \le \frac{1}{b-d+1} \sum_{i=1}^m (h_i - 1),$$

and the lemma follows easily.

Theorem 5.2. *Let* Δ *be a negative discriminant,* $\mathscr{G}$ *a set of generators of* C_Δ, *and* $f \in C_\Delta$. *Then the number of vectors* $r = (r(g))_{g\in\mathscr{G}}$ *in* $\{1, 2, \dots, |\Delta|\}^{\mathscr{G}}$ *satisfying* $\prod_{g\in\mathscr{G}} g^{r(g)} = f$ *equals*

$$\frac{|\Delta|^{\#\mathscr{G}}}{\#C_\Delta} \cdot \exp\epsilon$$

for some real number ϵ *satisfying*

$$|\epsilon| < \frac{\#C_\Delta}{|\Delta| - \#C_\Delta} < 1.$$

Proof. Let L be the kernel of the group homomorphism $\varphi: \mathbf{Z}^{\mathscr{G}} \to C_\Delta$ sending $(r(g))_{g\in\mathscr{G}}$ to $\prod_{g\in\mathscr{G}} g^{r(g)}$. By hypothesis, this map is surjective. The theorem follows from the lemma applied to $m = \#\mathscr{G}$, $h = d = \#C_\Delta$, $b = |\Delta|$, $\Lambda = L$ and $\mathscr{C} = \varphi^{-1}f$; note that $d < \frac{1}{2}b$ by (2.3).

In the following lemma, let Δ and $\mathscr{G}$ be as in Theorem 5.2, and let $L = \ker\varphi$ be as in the proof just given. We remark that there is a group isomorphism

$$((2\mathbf{Z})^{\mathscr{G}} \cap L)/2L \to C_{\Delta,2} \tag{5.3}$$

sending r to $\varphi(\frac{1}{2}r)$; here $C_{\Delta,2}$ is as in (2.4).

Lemma 5.4. *With the above notation, let* $\mathscr{A} \subset \mathbf{Z}^{\mathscr{G}}$ *be a coset of* $2L$ *and* $\mathscr{B} \subset \mathbf{Z}^{\mathscr{G}}$ *the coset of* $(2\mathbf{Z})^{\mathscr{G}} \cap L$ *containing* $\mathscr{A}$. *Then*

$$\frac{\#(\{1, 2, \dots, |\Delta|\}^{\mathscr{G}} \cap \mathscr{A})}{\#(\{1, 2, \dots, |\Delta|\}^{\mathscr{G}} \cap \mathscr{B})} = \frac{1}{\#C_{\Delta,2}} \cdot \exp\epsilon$$

for some real number ϵ *satisfying*

$$|\epsilon| < \frac{4 \cdot \#\mathscr{G} \cdot \#C_\Delta}{|\Delta| - 2\#C_\Delta}.$$

Proof. One proves this by applying Lemma 5.1 twice, once with $\Lambda = 2L$ and once with $\Lambda = (2\mathbf{Z})^{\mathscr{G}} \cap L$, and both times with $b = |\Delta|$ and $d = 2 \cdot \#C_\Delta$; note that $d < b$ by (2.3). By (5.3), the index of $2L$ in $\mathbf{Z}^{\mathscr{G}}$ is $\#C_{\Delta,2}$ times as large as the index of $(2\mathbf{Z})^{\mathscr{G}} \cap L$ in $\mathbf{Z}^{\mathscr{G}}$. This proves Lemma 5.4.

(5.5) *Remark.* We shall apply Lemma 5.4 with $\#\mathscr{G} = O((\log|\Delta|)^3)$ (see Theorem 4.5). From (2.13) we then see that $|\epsilon| \le \log 2$ if $|\Delta|$ is sufficiently large.

6. Smooth numbers with restricted prime factors

For positive real numbers v, x, y, and any set of prime numbers $\mathscr{P}$, we let $\psi(x, y; \mathscr{P})$ denote the number of positive integers $\le x$ all of whose prime factors are at most y and belong to $\mathscr{P}$, and

$$\pi(x; \mathscr{P}) = \#\{p : p \in \mathscr{P},\ p \le x\},$$

$$S(v, y; \mathscr{P}) = \sum_{p \in \mathscr{P},\ v < p \le y} \frac{1}{p}.$$

This section is devoted to the proof of the following theorem.

Theorem 6.1. *There is an effectively computable positive constant c_5 with the following property. Let $\mathscr{P}$ be any set of prime numbers, η a real number with $0 \le \eta \le 1$, and x, y real numbers satisfying*

$$x \ge c_5, \qquad 2 \le y \le \exp\left((\log x)^{1/2}(\log\log x)^\eta\right). \tag{6.2}$$

Let

$$u = \frac{\log x}{\log y}, \qquad v = y^{1-1/\log u}, \qquad w = v^{(\log u)^{-\eta}}. \tag{6.3}$$

Suppose that there are real numbers $\alpha \ge 1$, $\beta \ge 1$ for which

$$S(v, y; \mathscr{P}) \ge \frac{1}{\alpha \log u}, \qquad \pi(w; \mathscr{P}) \ge \frac{w}{\beta \log w}. \tag{6.4}$$

Then we have

$$\psi(x, y; \mathscr{P}) \ge x \cdot \exp\left(-u\left(\log u + 12(\log u)^\eta + \log\log u + 2(\log u)^{\eta-1}\log\beta + \log\alpha\right)\right).$$

Proof. From (6.2) we have $\log u \ge \frac{1}{2}\log\log x - \eta\log\log\log x$. We let c_5 be so large that this implies

$$\log u \ge \tfrac{2}{5}\log\log x \ge 3. \tag{6.5}$$

Let $\mathscr{M}$ denote the set of integers that are the product of $[u]$ not necessarily distinct primes $p \in \mathscr{P}$ with $v < p \le y$. Since $w \le v$, we have

$$\psi(x, y; \mathscr{P}) \ge \sum_{m \in \mathscr{M}} \psi(x/m, w; \mathscr{P}). \tag{6.6}$$

Let $m \in \mathscr{M}$. We estimate $\psi(x/m, w; \mathscr{P})$ from below. From $v^{u-1} < m \le y^u = x$ we have

$$1 \le \frac{x}{m} < \frac{x}{v^{u-1}} = v^{u/((\log u)-1)+1} < v^{2u/\log u}, \tag{6.7}$$

the last inequality being a consequence of (6.5). Let $l(m) = (\log \frac{x}{m})/\log w$. From (6.7) we have

$$0 \le l(m) < 2u(\log u)^{\eta-1}. \tag{6.8}$$

With (6.5) this gives

$$l(m)\log\log(x/m) < 2u(\log u)^{\eta-1}\log\log x \le 5u(\log u)^{\eta}. \tag{6.9}$$

Assume, for the moment, that $l(m) \ge 1$. One obtains a lower bound for $\psi(x/m, w; \mathscr{P})$ by considering all products of $[l(m)]$ not necessarily distinct primes $p \in \mathscr{P}$ with $p \le w$. Since no integer has more than $[l(m)]!$ representations as such a product, we find

$$\begin{aligned}\psi(x/m, w; \mathscr{P}) &\ge \frac{\pi(w; \mathscr{P})^{[l(m)]}}{[l(m)]!}\\ &\ge \pi(w; \mathscr{P})^{l(m)-1} l(m)^{-l(m)}\\ &\ge \frac{1}{w}\left(\frac{w}{\beta l(m)\log w}\right)^{l(m)}\\ &= \frac{x}{mw}\left(\frac{1}{\beta\log(x/m)}\right)^{l(m)}\\ &= \frac{x}{mw}\exp(-l(m)(\log\log(x/m) + \log\beta)),\end{aligned}$$

where in the last inequality we use that $\pi(w; \mathscr{P}) \le w$. Combining this with (6.8) and (6.9) we obtain

$$\psi(x/m, w; \mathscr{P}) > \frac{x}{mw}\exp(-5u(\log u)^{\eta} - 2u(\log u)^{\eta-1}\log\beta), \tag{6.10}$$

which is our lower bound for $\psi(x/m, w; \mathscr{P})$. It is also valid if $l(m) < 1$, since in that case $\psi(x/m, w; \mathscr{P}) \ge 1 > x/(mw)$.

Since no element of $\mathscr{M}$ has more than $[u]!$ representations as a product of $[u]$ primes $p \in \mathscr{P}$, $v < p \le y$, we have

$$\begin{aligned}\sum_{m\in\mathscr{M}} \frac{1}{m} &\ge \frac{1}{[u]!}S(v, y; \mathscr{P})^{[u]} \ge \frac{1}{[u]!}\left(\frac{1}{\alpha\log u}\right)^{[u]}\\ &> \exp(-u(\log u + \log\log u + \log\alpha)).\end{aligned}$$

Using this and (6.10) in (6.6), we have

$$\begin{aligned}\psi(x, y; \mathscr{P}) > \frac{x}{w}\exp(-u(\log u + 5(\log u)^{\eta} + \log\log u\\ + 2(\log u)^{\eta-1}\log\beta + \log\alpha)).\end{aligned} \tag{6.11}$$

It remains to estimate w. From (6.2) and (6.5) we see that

$$\begin{aligned}\log w \le \frac{\log y}{(\log u)^{\eta}} \le (\log x)^{1/2}\left(\frac{\log\log x}{\log u}\right)^{\eta} \le \tfrac{5}{2}(\log x)^{1/2}\\ \le \tfrac{5}{2}u(\log\log x)^{\eta} \le \tfrac{25}{4}u(\log u)^{\eta}.\end{aligned}$$

Putting this into (6.11) we obtain the theorem.

7 The elliptic curve smoothness test

The *elliptic curve method*, as described in [24], is a probabilistic algorithm that, given four integers a, y, w, h exceeding 1, attempts to find a nontrivial divisor of a. The number y may be thought of as an upper bound for the divisor that one is trying to find, h is an upper bound for the number of elliptic curves that one tries, and w is proportional to the time spent on a single elliptic curve. The following theorem summarizes the results that we shall need about the elliptic curve method.

Let $\psi_0(x, w)$ denote the number of w-smooth integers in the interval $(x - \sqrt{x}, x + \sqrt{x})$.

Theorem 7.1. *There is an effectively computable constant c_6 with $0 < c_6 < 1$ such that the following holds Let a, y, w, h be integers exceeding 1 such that a has at least two distinct prime factors, and such that the least prime factor p of a satisfies $3 < p \leq y$ Suppose further that $\psi_0(p, w) \geq 3$ Then the probability that the elliptic curve method, given a, y, w, h, succeeds in finding a nontrivial factor of a, is at least*

$$1 - c_6^{h\psi_0(p, w)/(\sqrt{p}\log y)}.$$

The running time of the method is $O(hw(\log y)(\log a)^2)$

Proof The first assertion is [24, Corollary (2.8)], up to a harmless change in the definition of $\psi_0(p, w)$ For the running time, see [24, (2.9)]. This proves Theorem 7.1.

Theorem 7.1 asserts that the elliptic curve method will probably be effective in splitting a if the least prime factor p of a is such that there are many w-smooth numbers in $(p - \sqrt{p}, p + \sqrt{p})$. Let $\mathscr{S}$ denote the set of primes p for which

$$\psi_0(p, \exp((\log p)^{6/7})) > \sqrt{p} \cdot \exp(-\tfrac{1}{5}(\log p)^{1/7}\log\log p) \geq 3.$$

For a positive real number y, let a *recognizable y-smooth number* be a positive integer all of whose prime factors are at most y and belong to $\mathscr{S}$.

Algorithm 7.2. Given integers a and y, with $a > 0$, $y > 1$, this algorithm attempts to factor a completely into primes. It is designed to be very likely to succeed if a is a recognizable y-smooth number.

Step 1. Remove all factors 2 and 3 from a, and replace a by the quotient. If now $a = 1$, the algorithm terminates at this point

Step 2. Find the largest integer k such that $a = m^k$ for some positive integer m (cf. [22, §2]), and replace a by m.

Step 3. If $a \leq y$, test a for primality using the Jacobi sum test [1]. If a is composite or $a > y$, run the elliptic curve method with parameters a, y, w, h, where w and h are the numbers

$$\exp((\log y)^{6/7}),$$
$$(1 - c_6)^{-1}(\log y)(\log a)\exp(\tfrac{1}{5}(\log y)^{1/7}\log\log y),$$

rounded down to integers, with c_6 as in Theorem 7.1. When a proper splitting of a is achieved, perform Steps 2 and 3 recursively with a replaced by each factor that is discovered. This completes the description of the algorithm.

Theorem 7.3. *If a is a recognizable y-smooth number, then the probability that Algorithm* 7.2 *factors a completely into primes is at least* $1-(\log a)/a$. *Further, the running time of the algorithm is* $O((\log(a+1))^4 \cdot \exp(2(\log y)^{6/7}))$.

Proof. This is a straightforward consequence of Theorem 7.1 and the definition of $\mathcal{S}$. For a fuller discussion of a similar result, see [28], in particular Theorem 2.1 in that paper. This proves Theorem 7.3.

The following result provides an upper bound for the number of primes not in $\mathcal{S}$. Denote by $\mathcal{S}'$ the set of primes that are not in $\mathcal{S}$, and let $\pi(x;\mathcal{S}')$ be the number of primes in $\mathcal{S}'$ up to x, as in §6.

Theorem 7.4. *There is an effectively computable constant c_7 such that for all real numbers $x \geq 2$ we have*

$$\pi(x;\mathcal{S}') \leq c_7 x \cdot \exp\left(-\tfrac{1}{2}(\log x)^{1/6}\right).$$

Proof. This follows from Theorem B$'$ in [28], which in turn relies heavily on the work of Friedlander and Lagarias [12]. The fact that c_7 is effectively computable was not stated in [28; 12], but follows from the proof in [12] and the effective computability of the constants in the Vinogradov-Korobov zero-free region $\sigma > 1 - c(\log|t|)^{-2/3}(\log\log|t|)^{-1/3}$, $|t| \geq t_0$ for the Riemann zeta function $\zeta(\sigma+it)$, see [11, Théorème 11.2 (p. 423)]. This proves Theorem 7.4.

The notation $S(v, y;\mathcal{S}')$ in the following result was introduced in §6.

Corollary 7.5. *For any two real numbers v, y with $2 \leq v < y$ we have*

$$S(v, y;\mathcal{S}') < c_7 \exp\left(-\tfrac{1}{2}(\log v)^{1/6}\right) \cdot \left(1+\log(y/v)\right),$$

with c_7 as in Theorem 7.4.

Proof. Using partial summation and Theorem 7.4 we find

$$\begin{aligned} S(v, y;\mathcal{S}') &= \frac{1}{y}(\pi(y;\mathcal{S}') - \pi(v;\mathcal{S}')) + \int_v^y \frac{1}{t^2}(\pi(t;\mathcal{S}') - \pi(v;\mathcal{S}'))\,dt \\ &< c_7 \exp\left(-\tfrac{1}{2}(\log v)^{1/6}\right) \cdot \left(1 + \int_v^y \frac{1}{t}\,dt\right) \\ &= c_7 \exp\left(-\tfrac{1}{2}(\log v)^{1/6}\right) \cdot \left(1+\log(y/v)\right). \end{aligned}$$

This proves Corollary 7.5.

Remark. It is clear that combining Theorem 6.1 with Theorem 7.4 and Corollary 7.5, one can obtain for certain ranges of x and y the lower bound estimate $\psi(x, y;\mathcal{S}) \geq x \cdot \exp(-(1+o(1))u\log u)$ for $u = (\log x)/\log y \to \infty$, where $\psi(x, y;\mathcal{S})$ is the number of recognizable y-smooth integers up to x. It is known ([5]) that $\psi(x, y) = x \cdot \exp(-(1+o(1))u\log u)$, in these ranges of x and y, where $\psi(x, y)$ is the number of all y-smooth integers up to x. Thus in some sense there are essentially just as many recognizable y-smooth numbers in the ranges we consider as there are y-smooth numbers.

8. Recognizable smooth forms

If Δ is a negative discriminant and y is a positive real number, then by a *recognizable y-smooth form* in C_Δ we mean a form $(a, b, c) \in C_\Delta$ for which a is a recognizable y-smooth number (see §7) with $\gcd(a, \Delta) = 1$.

In this section we prove that if the set $\mathscr{P}_\Delta$ defined in (2.7) has sufficiently many elements in each of two particular intervals (condition (8.2)), then C_Δ has a fair proportion of recognizable y-smooth elements.

The role of the additional parameter d in Theorem 8.1 will become clear in § 9. For the moment, the reader may think of $d = 1$, so that $x = \frac{1}{2}\sqrt{|\Delta|}$. The notation $\pi(x; \mathscr{P})$, $S(v, y; \mathscr{P})$ is from §6.

Theorem 8.1. *There are effectively computable positive constants c_8, c_9 with the following property. Let Δ be a negative discriminant, and let d, x, y be real numbers satisfying*

$$x = \tfrac{1}{2}\sqrt{|\Delta|/d}, \qquad 1 \le d \le 12, \qquad x > c_9,$$
$$\exp(c_8 \log\log x) \le y \le \exp\big((\log x)^{1/2}(\log\log x)^{1/2}\big).$$

Suppose that the numbers

$$u = \frac{\log x}{\log y}, \qquad v = y^{1-1/\log u}, \qquad w = v^{(\log u)^{-1/2}}$$

satisfy

$$S(v, y; \mathscr{P}_\Delta) \ge \frac{1}{6\log u}, \qquad \pi(w; \mathscr{P}_\Delta) \ge \frac{w}{6\log w}. \tag{8.2}$$

Then the number of recognizable y-smooth forms in C_Δ is at least

$$\#C_\Delta \cdot \exp\big(-u(\log u + 13(\log u)^{1/2})\big).$$

Proof. We begin by applying Theorem 6.1, with $\mathscr{P} = \mathscr{P}_\Delta \cap \mathscr{S}$ and $\eta = \frac{1}{2}$. We take $c_9 \ge c_5$, with c_5 as in Theorem 6.1, and we assume that (6.5) holds. The lower bound on y implies that

$$w = \exp\left(\left(1 - \frac{1}{\log u}\right)(\log u)^{-1/2}\log y\right) \ge \exp\left(\tfrac{2}{3}c_8\frac{\log\log x}{(\log u)^{1/2}}\right) \ge \exp(\tfrac{2}{3}c_8).$$

Combining this with Theorem 7.4 we see that

$$\pi(w; \mathscr{S}') \le \frac{w}{42\log w}$$

if c_8 is taken large enough. With (8.2) this gives

$$\pi(w; \mathscr{P}_\Delta \cap \mathscr{S}) \ge \frac{w}{7\log w},$$

which is the second condition of (6.4), with $\beta = 7$.

Next we apply Corollary 7.5. We have

$$\log(y/v) = \frac{\log y}{\log u} > \frac{c_8 \log\log x}{\log\log x} = c_8 ,$$
$$\log v = (1 - \tfrac{1}{\log u})\log y \ge \tfrac{2}{3}\log y ,$$

using (6.5), so from Corollary 7.5 we obtain

$$S(v, y; \mathcal{S}') \le c_7 \exp(-\tfrac{1}{2}(\tfrac{2}{3}\log y)^{1/6}) \cdot (c_8^{-1} + 1) \cdot \frac{\log y}{\log u} \le \frac{1}{42\log u},$$

the last inequality by increasing c_9, if necessary. With (8.2) this yields

$$S(v, y; \mathcal{P}_\Delta \cap \mathcal{S}) \ge \frac{1}{7\log u},$$

which is the first condition of (6.4), with $\alpha = 7$.

Theorem 6.1 now implies that $\psi(x, y; \mathcal{P}_\Delta \cap \mathcal{S})$ is at least

$$x \cdot \exp(-u(\log u + 12(\log u)^{1/2} + \log\log u + 2(\log u)^{-1/2}\log 7 + \log 7))$$
$$\ge x \cdot \exp(-u(\log u + \tfrac{25}{2}(\log u)^{1/2})),$$

where again we may have to increase c_9. From $x \le \frac{1}{2}\sqrt{|\Delta|}$ and Lemma 2.10 it follows that this is also a lower bound for the number of recognizable y-smooth forms in C_Δ. To prove the theorem, it remains to find an upper bound for $\#C_\Delta$. From (2.13) and $|\Delta| \le 48x^2$ we obtain

$$\begin{aligned}\#C_\Delta &< \sqrt{48} \cdot x \cdot \log(48x^2) \\ &= x \cdot \exp(\log\log(48x^2) + \tfrac{1}{2}\log 48) \\ &\le x \cdot \exp\left(\tfrac{1}{2}u(\log u)^{1/2}\right),\end{aligned}$$

by (6.5). This proves Theorem 8.1.

Remark. If the generalized Riemann hypothesis is correct, then (8.2) is satisfied if c_9 is sufficiently large; cf. [32, Theorem 5.3] (in which one should read $\frac{1}{2}\,\mathrm{Li}(x)$ for $\mathrm{Li}(x)$). So in that case there are sufficiently many y-smooth forms in C_Δ. The corresponding point was not satisfactorily dealt with in [20, eq. (2.10)]. To correct this, one can either apply Theorem 8.1, or, as the author of [20] communicated to us, follow the proof of [32, Theorem 5.2] to estimate the number of smooth integers built up from the primes in $\mathcal{P}_\Delta \cap \mathcal{S}$; this requires Theorem 7.4 in addition to [32, Theorem 5.3].

9. The choice of a multiplier

In this section we show that the conditions (4.3) and (8.2) of Theorems 4.1 and 8.1 can be achieved by means of a small multiplier.

Theorem 9.1. *There is an effectively computable positive constant c_{10} with the following property. Let n be an odd integer with $n > 1$, and let u, v, w, y, z be real numbers satisfying*

$$w \ge c_{10}\log n , \qquad z \ge c_{10}\log n ,$$
$$\log\frac{\log y}{\log v} \ge \frac{1}{\log u} > 0 , \qquad \log v \ge c_{10}\log u , \qquad v \ge \log n. \tag{9.2}$$

Further let $\mathscr{D} = \{3, 4, 7, 8\}$ *if* $n \equiv 1 \bmod 4$ *and* $\mathscr{D} = \{1, 5, 8, 12\}$ *if* $n \equiv 3 \bmod 4$. *Then there exists an integer* $d \in \mathscr{D}$ *for which the number* $\Delta = -dn$ *is a negative discriminant satisfying the conditions*

$$\pi(z\,; \mathscr{P}_\Delta) \geq \frac{z}{6\log z}, \tag{9.3}$$

$$\pi(w\,; \mathscr{P}_\Delta) \geq \frac{w}{6\log w}, \tag{9.4}$$

$$S(v\,, y\,; \mathscr{P}_\Delta) \geq \frac{1}{6\log u}. \tag{9.5}$$

Proof. For each $d \in \mathscr{D}$, the number $\Delta = -dn$ is a negative discriminant. It will thus suffice to show that each of the three conditions (9.3), (9.4), (9.5) is violated by at most one $d \in \mathscr{D}$.

Let d_1, $d_2 \in \mathscr{D}$ be two distinct elements of $\mathscr{D}$, put $\Delta_1 = -d_1 n$, $\Delta_2 = -d_2 n$, and $\mathscr{P} = \{p : p \text{ is prime}, \left(\frac{d_1 d_2}{p}\right) = -1\}$. Writing $\mathscr{N}$ for the set of prime divisors of n, we have from the multiplicativity of the Kronecker symbol

$$\mathscr{P} \subset \mathscr{P}_{\Delta_1} \cup \mathscr{P}_{\Delta_2} \cup \mathscr{N}.$$

It follows that for all x we have

$$\pi(x\,; \mathscr{P}_{\Delta_1}) + \pi(x\,; \mathscr{P}_{\Delta_2}) \geq \pi(x\,; \mathscr{P}) - \#\mathscr{N}.$$

We have $\#\mathscr{N} = O((\log n)/\log\log n)$, so for c_{10} sufficiently large we have $\#\mathscr{N} < \frac{1}{12}x/\log x$ whenever $x \geq c_{10}\log n$. Also, because $d_1 d_2$ is not a square, we have $\pi(x\,; \mathscr{P}) \sim \frac{1}{2}x/\log x$ for $x \to \infty$, so $\pi(x\,; \mathscr{P}) \geq \frac{5}{12}x/\log x$ for all x beyond some effectively computable constant; this constant is *absolute* because $\mathscr{D}$ is finite (see [8, Chapter 20]). Hence, increasing c_{10} if necessary, we have

$$\pi(x\,; \mathscr{P}_{\Delta_1}) + \pi(x\,; \mathscr{P}_{\Delta_2}) \geq \frac{x}{3\log x}$$

whenever $x > c_{10}\log n$. Applying this to $x = z$ we conclude that Δ_1 and Δ_2 cannot both violate (9.3), and likewise for (9.4).

For (9.5), we have

$$S(v\,, y\,; \mathscr{P}_{\Delta_1}) + S(v\,, y\,; \mathscr{P}_{\Delta_2}) \geq S(v\,, y\,; \mathscr{P}) - S(v\,, y\,; \mathscr{N}).$$

Since n has at most $(\log n)/\log v$ prime divisors $> v$, we have

$$S(v\,, y\,; \mathscr{N}) < \frac{\log n}{v\log v} \leq \frac{1}{c_{10}\log u}.$$

Further, since $d_1 d_2$ is not a square, we have

$$S(v\,, y\,; \mathscr{P}) = \tfrac{1}{2}\log\log y - \tfrac{1}{2}\log\log v + O(1/\log v),$$

with an effectively computable, absolute O-constant (again, see [8]). It follows that, for c_{10} sufficiently large, we have

$$S(v\,, y\,; \mathscr{P}_{\Delta_1}) + S(v\,, y\,; \mathscr{P}_{\Delta_2}) \geq \frac{1}{2\log u} - \frac{1}{6\log u} = \frac{1}{3\log u},$$

which shows that Δ_1 and Δ_2 cannot both violate (9.5). This concludes the proof of Theorem 9.1.

Remark. We shall apply Theorem 9.1 with u, v, w, y as in Theorem 8.1, with $x = \frac{1}{2}\sqrt{n}$, and z as in (4.2). One verifies in a straightforward manner that these numbers satisfy (9.2) if

$$y \geq \exp(c_{11}(\log\log x)^{3/2})$$

for some absolute constant c_{11}.

10. The factoring algorithm

Algorithm 10.1. Given an odd positive integer n, this algorithm attempts to find a nontrivial factorization of n.

Step 1. *Choose a multiplier.* Let $\mathscr{D} = \{3, 4, 7, 8\}$ if $n \equiv 1 \bmod 4$ and $\mathscr{D} = \{1, 5, 8, 12\}$ if $n \equiv 3 \bmod 4$. Select $d \in \mathscr{D}$ at random, with the uniform distribution. Put $\Delta = -dn$. (Note that Δ is a negative discriminant, in the sense of §2.)

Step 2. *Find a generating set.* Run Algorithm 4.4 on Δ and z, where z is the number $\exp(c_4(\log(12n))^2)$, rounded up to an integer, with c_4 as in Theorem 4.1. This yields a set $\mathscr{G}$ of elements of C_Δ. (Note that $\#\mathscr{G} = O((\log|\Delta|)^3)$.)

Step 3. *Construct the factor base.* Let y be the number $L_x[\frac{1}{2}, \frac{1}{2}\sqrt{2}]$, rounded down to an integer, where $x = \frac{1}{2}\sqrt{n}$. Find the prime numbers $q \leq y$ with $(\frac{\Delta}{q}) = 1$. We write $\mathscr{Q}$ for the set of these q. Construct the prime forms f_q for $q \in \mathscr{Q}$, as in (2.7). (Note that $\#\mathscr{Q} \leq y = L_n[\frac{1}{2}, \frac{1}{2} + o(1)]$ for $n \to \infty$.)

Step 4. *Collect relations.* In this step, one attempts to produce a sequence of $\#\mathscr{G} + \#\mathscr{Q} + 1$ relations between $\mathscr{G}$ and $\{f_q : q \in \mathscr{Q}\}$. Such a relation is, by definition, an element $(r, t) \in \mathbf{Z}^{\mathscr{G}} \times \mathbf{Z}^{\mathscr{Q}}$ satisfying

$$\left(\prod_{g \in \mathscr{G}} g^{r(g)}\right) \cdot \left(\prod_{q \in \mathscr{Q}} f_q^{t(q)}\right) = 1_\Delta, \tag{10.2}$$

where $r = (r(g))_{g \in \mathscr{G}}$, $t = (t(q))_{q \in \mathscr{Q}}$. Initially, the sequence of relations is empty.

Draw a random vector $r = (r(g))_{g \in \mathscr{G}} \in \{1, 2, \ldots, |\Delta|\}^{\mathscr{G}}$, with the uniform distribution. Calculate $\prod_{g \in \mathscr{G}} g^{r(g)}$; let it be (a, b, c). Test whether $\gcd(a, \Delta) = 1$, and if so, attempt to factor a into prime numbers $\leq y$ using Algorithm 7.2. If this attempt is successful, use the method of (2.8) to find a vector $t = (t(q))_{q \in \mathscr{Q}} \in \mathbf{Z}^{\mathscr{Q}}$ such that

$$(a, b, c) = \prod_{q \in \mathscr{Q}} f_q^{-t(q)}.$$

Then $(r, t) \in \mathbf{Z}^{\mathscr{G}} \times \mathbf{Z}^{\mathscr{Q}}$ is clearly a relation between $\mathscr{G}$ and $\{f_q : q \in \mathscr{Q}\}$; it is the next term in the sequence of relations.

Repeat the above until a sequence of $\#\mathscr{G} + \#\mathscr{Q} + 1$ relations has been found, or until at least

$$2(\#\mathscr{G} + \#\mathscr{Q} + 1) \cdot \exp(u(\log u + 13(\log u)^{1/2}) + 2)$$

(rounded up to an integer) vectors r have been drawn and inspected, whatever happens first; here $u = (\log(\frac{1}{2}\sqrt{n}))/\log y$ is as in Theorem 8.1. (Thus at most $L_n[\frac{1}{2}, 1 + o(1)]$ vectors r are processed, for $n \to \infty$.)

If in this way fewer than $\#\mathcal{G}+\#\mathcal{Q}+1$ relations are found, then Algorithm 10.1 terminates unsuccessfully at this point. Suppose now that Step 4 is successful, and denote by (r_i, t_i) the ith relation that is found, for $1 \le i \le \#\mathcal{G} + \#\mathcal{Q} + 1$.

Step 5. *Solve the linear system.* For $1 \le i \le \#\mathcal{G} + \#\mathcal{Q} + 1$, let $v_i \in \mathbf{F}_2^{\mathcal{G}} \times \mathbf{F}_2^{\mathcal{Q}}$ be the vector that one obtains by reducing the coordinates of (r_i, t_i) modulo 2; here we put $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. Use the coordinate recurrence method [34; 21, §2.19] to find a nonempty subset $\mathcal{J} \subset \{1, 2, \dots, \#\mathcal{G} + \#\mathcal{Q} + 1\}$ for which $\sum_{i\in\mathcal{J}} v_i = 0$. (Note that such a $\mathcal{J}$ exists, since $\#\mathcal{G}+\#\mathcal{Q}+1 > \dim_{\mathbf{F}_2}(\mathbf{F}_2^{\mathcal{G}}\times\mathbf{F}_2^{\mathcal{Q}})$.)

Step 6. *Construct an ambiguous form.* Compute the components $s(g)$, $u(q)$ ($g \in \mathcal{G}$, $q \in \mathcal{Q}$) of the vector $\frac{1}{2}\sum_{i\in\mathcal{J}}(r_i, t_i) \in \mathbf{Z}^{\mathcal{G}} \times \mathbf{Z}^{\mathcal{Q}}$. Compute the form

$$f = \Big(\prod_{g\in\mathcal{G}} g^{s(g)}\Big)\cdot\Big(\prod_{q\in\mathcal{Q}} f_q^{u(q)}\Big).$$

This is an ambiguous form. Calculate the corresponding factorization of Δ (see (2.4)) and, by taking a gcd, the resulting factorization of n. This factorization is the output of the algorithm. This completes the description of Algorithm 10.1.

Remark. The fact that, in the last step, $\frac{1}{2}\sum_{i\in\mathcal{J}}(r_i, t_i)$ is an integer vector follows from $\sum_{i\in\mathcal{J}} v_i = 0$. To see that f is ambiguous note that

$$f^2 = \prod_{i\in\mathcal{J}}\Big(\Big(\prod_{g\in\mathcal{G}} g^{r_i(g)}\Big)\cdot\Big(\prod_{q\in\mathcal{Q}} f_q^{t_i(q)}\Big)\Big) = 1_\Delta,$$

by (10.2).

Remark. The factorization of n obtained in Step 6 is a *coprime* factorization of n, see (2.4). It may, however, be the trivial factorization $1 \cdot n$.

Theorem 10.3. *The expected running time of Algorithm* 10.1 *is at most* $L_n[\frac{1}{2}, 1 + o(1)]$ *for* $n \to \infty$. *There is an effectively computable constant* c_{12}, *such that if* n *is an odd number and* $n > c_{12}$, *then the probability that Algorithm* 10.1 *succeeds in finding a nontrivial factorization of* n *is at least* $\frac{1}{32}(1 - 2^{-h+1})$, *where* h *is the number of distinct prime factors of* n; *this is at least* $\frac{1}{64}$ *if* n *is not a power of a prime number.*

Proof. We first estimate the time; $o(1)$ will always be for $n \to \infty$. Steps 1 and 2 take only time $(\log n)^{O(\log\log\log n)}$, by Theorem 4.5, and Step 3 takes expected time at most $y^{1+o(1)} = L_n[\frac{1}{2}, \frac{1}{2} + o(1)]$. Processing a single vector r in Step 4 can be done in expected time $(\log|\Delta|)^{O(1)}\exp(2(\log y)^{6/7})$, by Theorem 7.3. This is absorbed in the upper bound of $L_n[\frac{1}{2}, 1 + o(1)]$ for the number of vectors r to be considered in Step 4. In Step 5, we solve a system of m linear equations in $m + 1$ variables over $\mathbf{F}_2$, where $m \le L_n[\frac{1}{2}, \frac{1}{2} + o(1)]$. From (2.8) it follows that each of the vectors v_i has less than $\#\mathcal{G} + \log|\Delta|$ nonzero coordinates. Therefore the number of nonzero coefficients in the system of linear equations is at most $L_n[\frac{1}{2}, \frac{1}{2}+o(1)]$. Thus from [34] it follows that Step 5 takes expected time at most $L_n[\frac{1}{2}, 1+o(1)]$. Finally, Step 6 takes time at most $L_n[\frac{1}{2}, \frac{1}{2}+o(1)]$. This concludes the running time analysis.

Next we estimate the probability that a nontrivial factorization is obtained. We shall suppose that $n \geq c_{12}$, with c_{12} sufficiently large, as dictated by the proof.

By Theorem 9.1, the discriminant $\Delta = -dn$ constructed in Step 1 satisfies (9.3), (9.4) and (9.5) with probability at least $\frac{1}{4}$; and if this is the case, then by Theorem 4.5 the set $\#\mathscr{G}$ found in Step 2 generates C_Δ with probability at least $\frac{1}{2}$.

Suppose now that Δ satisfies (9.3), (9.4) and (9.5), and that $\mathscr{G}$ generates C_Δ. We first show that the conditional probability that Step 4 of the algorithm is successful is at least $\frac{1}{2}$. First consider the variant of Step 4 that stops only when $\#\mathscr{G}+\#\mathscr{Q}+1$ relations have been found. From Theorem 8.1 and Theorem 5.2 it follows that whenever a vector r is drawn, the form (a, b, c) computed by the algorithm is a recognizable y-smooth form with probability at least

$$\exp\left(-u(\log u + 13(\log u)^{1/2}) - 1\right).$$

If (a, b, c) is a recognizable y-smooth form, then the probability that Algorithm 7.2 factors a into primes $\leq y$ is at least $1-(\log a)/a > \exp(-1)$. It follows that a random r gives a relation with probability at least

$$\exp\left(-u(\log u + 13(\log u)^{1/2}) - 2\right),$$

so that the expected number of vectors r that one needs to draw until one has $\#\mathscr{G}+\#\mathscr{Q}+1$ relations is at most

$$(\#\mathscr{G}+\#\mathscr{Q}+1)\cdot\exp\left(u(\log u + 13(\log u)^{1/2}) + 2\right).$$

Hence if one draws twice as many vectors r, one is successful with probability at least $\frac{1}{2}$. This implies that the actual Step 4 has success probability at least $\frac{1}{2}$, as asserted.

We now restrict attention to those runs of the algorithm for which d assumes a given value satisfying (9.3), (9.4) and (9.5), the set $\mathscr{G}$ is a given set of less than $2+60(\log|\Delta|)\log z$ generators of C_Δ (see Theorem 4.5), and Step 4 is successful. It will suffice to prove that the conditional probability of obtaining a nontrivial factorization of n is at least $\frac{1}{2}(1-2^{-h+1})$. We do this by an argument that is similar to the one presented in [20].

The number n has 2^{h-1} coprime factorizations, and only one of them is trivial. Hence Theorem 2.5 implies that the number of ambiguous forms that yield a nontrivial factorization of n is $(1-2^{-h+1})\cdot\#C_{\Delta,2}$. Thus it suffices to prove that the ambiguous form f constructed in Step 6 is equal to a given ambiguous form with probability at least $\frac{1}{2}\cdot(\#C_{\Delta,2})^{-1}$. Note that f is completely determined by $\mathscr{J}$ and by the r_t, since each t_t is determined by r_t.

Put $\mathscr{I} = \{1, 2, \ldots, \#\mathscr{G}+\#\mathscr{Q}+1\}$, and let $\mathscr{J}$ be any nonempty subset of $\mathscr{I}$. The probability that $\mathscr{J}$ is the subset found by the coordinate recurrence method in Step 5 depends only on the vectors v_t, which in turn depend only on the vectors t_i and the cosets of the vectors r_i modulo $(2\mathbf{Z})^{\mathscr{G}}$. Further, t_i depends only on the coset of r_i modulo the lattice L (defined in §5) of vectors $r \in \mathbf{Z}^{\mathscr{G}}$ with $\prod_{g\in\mathscr{G}} g^{r(g)} = 1_\Delta$. We conclude that the probability of finding a particular $\mathscr{J}$ in Step 5 depends only on the cosets of the vectors r_i modulo $(2\mathbf{Z})^{\mathscr{G}} \cap L$.

Consider a pair consisting of a sequence of vectors $(r_i)_{i\in\mathscr{I}}$ and a nonempty subset $\mathscr{J} \subset \mathscr{I}$, and suppose that this pair can be produced by the algorithm. One such pair is called *equivalent* to another such pair (r_i'), $\mathscr{J}'$ if, first of all, we have $\mathscr{J} = \mathscr{J}'$; and, second, if j denotes the smallest element of $\mathscr{J}$, then $r_i = r_i'$ for all $i \in \mathscr{I}$, $i \neq j$; and, finally, r_j and r_j' lie in the same coset, $\mathscr{B}$ (say), of $\mathbf{Z}^{\mathscr{G}}$ modulo $(2\mathbf{Z})^{\mathscr{G}} \cap L$. It is obvious that this is indeed an equivalence relation, and from what we said in the previous paragraph it follows that any two equivalent pairs have the same probability of being produced by the algorithm. Hence we may now fix $\mathscr{J}$ and the vectors r_i for $i \neq j$, as well as the coset $\mathscr{B}$ of $\mathbf{Z}^{\mathscr{G}}$ modulo $(2\mathbf{Z})^{\mathscr{G}} \cap L$. It is to be proved that the fraction of elements $r_j \in \mathscr{B} \cap \{1, 2, \dots, |\Delta|\}^{\mathscr{G}}$ that give rise to a given ambiguous form is at least $\frac{1}{2} \cdot (\#C_{\Delta,2})^{-1}$.

Note that one of the terms in the sum $\sum_{i\in\mathscr{J}}(r_i, t_i)$ computed in Step 6 is equal to (r_j, t_j). From this it follows that the ambiguous form f is equal to a given ambiguous form if and only if r_j belongs to a certain coset $\mathscr{A}$ modulo $2L$ contained in $\mathscr{B}$. Thus the fraction to be estimated is

$$\frac{\#(\mathscr{A} \cap \{1, 2, \dots, |\Delta|\}^{\mathscr{G}})}{\#(\mathscr{B} \cap \{1, 2, \dots, |\Delta|\}^{\mathscr{G}})}.$$

By Lemma 5.4 this is at least $\frac{1}{2} \cdot (\#C_{\Delta,2})^{-1}$, if c_{12} is sufficiently large (cf. (5.5)), as required.

The last assertion of the theorem is obvious. This concludes the proof of Theorem 10.3.

Remark. It can be shown that the expected running time of Algorithm 10.1 is actually *equal* to $L_n[\frac{1}{2}, 1+o(1)]$, for $n \to \infty$, and that one cannot improve this by choosing the parameter y differently. The storage needed by the algorithm is at most $L_n[\frac{1}{2}, \frac{1}{2}+o(1)]$, for $n \to \infty$. This follows easily from [34].

To obtain an algorithm for the complete prime factorization of positive integers it now suffices to add a few embellishments to Algorithm 10.1. In §7 we saw the elliptic curve method similarly transformed into a smoothness test (Algorithm 7.2).

Algorithm 10.4. This is an algorithm that factors a given positive integer n into prime factors.

Step 1. Remove all factors 2 from n, and replace n by the quotient. Stop if $n = 1$.

Step 2. Find the largest integer k such that $n = m^k$ for some positive integer m, and replace n by m.

Step 3. If $n \le c_{12}$, with c_{12} as in Theorem 10.3, factor n into primes by trial division.

Step 4. If $n > c_{12}$, first test n for primality using the Jacobi sum test [1]. Stop if n is prime. Next suppose that n is composite. Apply Algorithm 10.1 repeatedly, until it finds a nontrivial factorization of n. Apply Steps 2, 3 and 4 recursively to both factors of n that are found. This completes the description of the algorithm.

Theorem 10.5. *Algorithm* 10.4 *completely factors any positive integer* n *into prime factors in expected time at most* $L_n[\frac{1}{2}, 1 + o(1)]$, *for* $n \to \infty$.

Proof. The running time estimate for Steps 1, 2 and 3 is left to the reader. It is easy to see that the total number of divisors of n to which Steps 2, 3 and 4 are applied is at most the number of distinct odd prime factors of n, which is at most $\log n$. In Step 4, the primality test takes time $(\log n)^{O(\log\log\log n)}$ (for $n > e^e$), by [1]. Algorithm 10.1 is applied only to odd integers larger than c_{12} that are not prime powers. For each such number, the expected number of applications of Algorithm 10.1 that is necessary to find a nontrivial factorization is at most 64, by Theorem 10.3. Hence all applications of Algorithm 10.1 together take expected time at most $L_n[\frac{1}{2}, 1 + o(1)]$ for $n \to \infty$. This proves Theorem 10.5.

The theorem stated in the introduction is a direct consequence of Theorem 10.5.

11. The random class groups method

It is the purpose of this section to point out a serious flaw in the heuristic running time analysis of the random class groups method that was proposed in [29]. We refer to [29; 21, §4.A] for a description of this method. For our purposes it suffices to know that, in order to factor n, the random class groups method needs a "small" positive integer d for which $\Delta = -dn$ is a negative discriminant with the property that $\#C_\Delta$ is y-smooth for some "small" value of y. The dominating contribution to the expected running time is then, roughly, the upper bound for d multiplied by y. The heuristic running time analysis assumes that, for fixed n and variable d, the class number $\#C_{-dn}$ is essentially just as likely to be smooth as a random number of the same approximate size. This assumption implies that one can take both d and y to be no larger than $L_n[\frac{1}{2}, \frac{1}{2} + o(1)]$, leading to an upper bound $L_n[\frac{1}{2}, 1 + o(1)]$ for the expected running time of the random class groups algorithm, for $n \to \infty$.

In this section we prove that the assumption just stated is incorrect for a fairly dense sequence of integers n. Theorem 11.1 shows that for many integers n there is not even a *single* multiplier d for which $\#C_{-dn}$ is smooth, for a very wide range of smoothness bounds. For example, if the smoothness bound is taken to be $x^{1/9}$, then the number of such n up to x is at least $cx^{2/3}/\log x$ for some positive constant c; there is no reason to suppose that the random class groups method can find a nontrivial factor of any of those n in time less than $n^{1/9}$.

Theorem 11.1. *There is a positive constant c_{13} with the following property Let $\mathcal{N}(x, y)$ be the set of positive integers $n \leq x$ such that for every negative discriminant $\Delta \equiv 0 \bmod n$, the class number $\#C_\Delta$ has a prime factor exceeding y Then for all x, y with $c_{13} < y \leq x^{1/9}$ we have*

$$\#\mathcal{N}(x, y) \geq \frac{x}{40y^3 \log y}.$$

Remark Due to the use of the Bombieri-Vinogradov theorem in the proof of Lemma 11.3, the constant c_{13} in the theorem is ineffective.

Before we give the proof we treat a few lemmas First we describe the "bad" integers n. Let the greatest prime factor of an integer $m \geq 2$ be denoted by $P(m)$, and put $P(1) = 1$. We write $\mathcal{T}$ for the set of prime numbers p with the property that $\min\{P(p-1), P(p+1)\} > p^{1/3} > 3$.

Lemma 11.2. *Let n be an integer that is divisible by p^2 for some prime number $p \in \mathcal{T}$ with $p \geq y^3$ Further let Δ be a negative discriminant that is divisible by n Then the class number $\#C_\Delta$ has a prime factor exceeding y*

Proof We can write $\Delta = p^2\Delta'$, where Δ' is also a negative discriminant. Dividing the class number formula (2.12) by the same formula for Δ' we find that $\#C_\Delta = \frac{2}{w'}(p - (\frac{\Delta'}{p}))\cdot\#C_{\Delta'}$, where $w' \in \{2, 4, 6\}$. Hence $6\cdot\#C_\Delta$ is divisible by one of the prime numbers $P(p-1)$, p, $P(p+1)$, depending on the value of $(\frac{\Delta'}{p})$. By hypothesis, each of these primes is larger than 3 and exceeds y This implies Lemma 11.2.

In the following lemma, $\mathcal{T}$ is as above and $\pi(x, \mathcal{T})$ is as in §6 The lemma asserts that, asymptotically, at least one third of all primes belong to $\mathcal{T}$.

Lemma 11.3. *We have*

$$\liminf_{x\to\infty} \frac{\pi(x, \mathcal{T})}{x/\log x} \geq \frac{1}{3}$$

Proof It suffices to show that

$$\sum_{p\in\mathcal{T},\, p\leq x} \log p \geq \left(\tfrac{1}{3} + o(1)\right)x, \qquad \text{for } x \to \infty \tag{11.4}$$

This sum is at least

$$\sum_{27<p\leq x} \log p - \sum_{\substack{p\leq x\\ P(p-1)\leq x^{1/3}}} \log p - \sum_{\substack{p\leq x\\ P(p+1)\leq x^{1/3}}} \log p. \tag{11.5}$$

The first sum is $(1 + o(1))x$ for $x \to \infty$, by the prime number theorem. The other two sums in (11.5) can be estimated with one argument Let $a \in \{1, -1\}$. Then

$$\sum_{\substack{p\leq x\\ P(p+a)\leq x^{1/3}}} \log p = \sum_{\substack{p\leq x\\ P(p+a)\leq x^{1/3}}} \log(p + a) + O(\log\log x). \tag{11.6}$$

Now

$$\sum_{\substack{p\le x\\ P(p+a)\le x^{1/3}}} \log(p+a) = \sum_{\substack{p\le x\\ P(p+a)\le x^{1/3}}} \sum_{d\mid p+a} \Lambda(d)$$
$$\le \sum_{d\le x^{1/3}} \Lambda(d)\pi(x;d,-a) + \sum_{\substack{d> x^{1/3}\\ P(d)\le x^{1/3}}} \Lambda(d)\pi(x;d,-a),$$

where Λ is the von Mangoldt function and $\pi(x;d,-a)$ is the number of primes $p\le x$ with $p\equiv -a \bmod d$. Trivially, we have $\pi(x;d,-a)\le \frac{x}{d}+1$, so the second sum is at most

$$\sum_{\substack{x^{1/3}<d\le x+a\\ P(d)\le x^{1/3}}} \Lambda(d)\left(\frac{x}{d}+1\right) = O(x^{5/6}),$$

which we can see by noting that the sum is dominated by those d that are squares of primes. By the Bombieri-Vinogradov theorem (see [8, Chapter 28]), the first sum is

$$(1+o(1))\sum_{d\le x^{1/3}} \Lambda(d)\frac{x}{\varphi(d)\log x} = (\tfrac{1}{3}+o(1))x$$

for $x\to\infty$. Assembling these calculations in (11.6), we have

$$\sum_{\substack{p\le x\\ P(p+a)\le x^{1/3}}} \log p \le (\tfrac{1}{3}+o(1))x,$$

which when put in (11.5) gives (11.4). This proves Lemma 11.3.

Remark. The same proof shows that for each c with $0<c<\frac{1}{2}$ the set of primes p for which $\min\{P(p-1), P(p+1)\}>p^c$ has lower density at least $1-2c$.

We now prove Theorem 11.1. Let x, y be as in the theorem. We write $t=y^3$. By Lemma 11.2, each integer $n\le x$ that is divisible by the square of a prime $p\ge t$, $p\in\mathscr{T}$, belongs to $\mathscr{N}(x,y)$. Therefore

$$\#\mathscr{N}(x,y) \ge \sum_{\substack{p\in\mathscr{T}\\ t\le p\le x^{1/2}}} \left[\frac{x}{p^2}\right] - \sum_{\substack{p,q\in\mathscr{T}\\ p,q\ge t}} \left[\frac{x}{p^2q^2}\right].$$

The second sum is at most

$$x\left(\sum_{p\ge t}\frac{1}{p^2}\right)^2 = O(x/t^2).$$

The first sum is at least

$$\sum_{\substack{p\in\mathscr{T}\\ t\le p\le x^{1/2}}} \frac{x}{p^2} - \pi(x^{1/2}).$$

It remains to note that $\pi(x^{1/2}) = o(x/(t\log t))$ for $x \to \infty$ and that

$$\sum_{\substack{p\in\mathcal{T} \\ t\leq p\leq x^{1/2}}} \frac{1}{p^2} \geq \frac{\pi(6t;\mathcal{T}) - \pi(t;\mathcal{T})}{(6t)^2} \geq \left(\frac{1}{36} + o(1)\right)\frac{1}{t\log t}$$

for $t \to \infty$. This last inequality follows from Lemma 11.3 and an upper bound for $\pi(t;\mathcal{T})$ afforded by the prime number theorem. Thus if c_{13} is taken sufficiently large, we have Theorem 11.1.

Remark. Let n, p, Δ be as in Lemma 11.2. If the number of factors p in Δ is *odd*, then the large prime factor that we show to exist in $\#C_\Delta$ is p itself, hence divides n. We can protect the random class groups method against such large prime divisors by working only with nth powers of elements in C_Δ. If the random class groups method is modified in this way, we should only consider integers n in Lemma 11.2 that have an *even* number of factors p, and restrict to discriminants $\Delta = -dn$ for which the multiplier d is not divisible by p. The arguments in this section then go through with very few changes, and the conclusion is that the modified random class groups method has the same shortcoming as the original method.

12. Probabilistic algorithms

In this section we discuss briefly what we mean by a "probabilistic" algorithm and by the "expected" running time of such an algorithm. Several definitions have been proposed for these notions, and the fact that they are not all mathematically equivalent is not generally appreciated. We have chosen the definitions below because they are natural and convenient to use. See [14] for a further discussion.

By a probabilistic algorithm we mean an algorithm that is allowed to employ a random number generator. Every time the random number generator is called it outputs 0 or 1, each with probability $\frac{1}{2}$. Any collection of calls is supposed to be independent; this also applies to calls that are made in different runs of the algorithm. It will be supposed that a call to the random number generator takes unit time. We are not concerned with the question of how the random number generator is to be implemented, or indeed whether this is possible at all.

It is easy to see that a random number generator can be used to draw, for a given positive integer m, a random number from $\{0, 1, \ldots, m-1\}$ with the uniform distribution, in expected time $O(\log m)$.

The course of a probabilistic algorithm is determined, not only by its input (for example, the number n to be factored, in the case of a factoring algorithm), but also by the random bits that are drawn. This means that, for a given value of the input, the running time of the algorithm may not be constant; instead, it has a *distribution.* The same applies to the *output* of the algorithm; for example, *which* factor of n is found by a factoring algorithm. Also, the correctness of the output of the algorithm may be subject to a distribution, as is the case for certain primality tests.

The "expected running time" of a probabilistic algorithm, for a given value of the input, is defined as the expectation of the running time. Note that we average *only* over the possible outputs of the random number generator, *not* over different values of the input of the algorithm. For example, when we say that a factoring algorithm has expected running time $f(n)$, then this is true for *each* individual value of n, without a single exception.

We mention a few rules that are helpful in computing expected running times. If a probabilistic algorithm consists of performing several other probabilistic algorithms, one after the other, and all with the same input, then its expected running time is simply the sum of the expected running times of the component algorithms. This obvious rule would not have been worth mentioning had its analogue not been incorrect for other definitions that have been proposed. The rule is even valid if one of the algorithms involved can in principle run forever; of course, if the expected running time is finite, this happens with probability zero.

The situation is a little more complicated if the component algorithms do not all have the same input. This occurs, for example, if the output of each algorithm is the input of the next one. In such a case it is often possible to find an upper bound for the input of each algorithm, and hence for its expected running time; the sum of the latter upper bounds is then a valid upper bound for the expected running time of the entire algorithm.

Another convenient rule is the following. Suppose that some of the outputs of a probabilistic algorithm are pronounced "successes" and the others "failures"; for example, finding the factor 1 or n in a factoring algorithm is a failure, or finding a nonsmooth number if it is the purpose of the algorithm to find a smooth one. Let p be the success probability, and suppose that $p > 0$. Then the expected number of times that one has to perform the algorithm until the first success occurs equals p^{-1}, and the expected time that this takes is p^{-1} times the expected running time of the algorithm itself; this is even true if the average running time of a successful run of the algorithm is different from the average running time of an unsuccessful run. If one needs k successes one has to replace p^{-1} by kp^{-1}. In the examples just given one can tell the successes from the failures, but this is not always the case (see Algorithm 4.4). For an algorithm for which we cannot easily recognize when we are successful we have the option of bounding the number of iterations in advance. If this bound is at least $2p^{-1}$, then the probability that at least one iteration of the algorithm is successful is at least $\frac{1}{2}$ (see, for example, the proof of Theorem 4.5).

Acknowledgments

The authors are grateful to the Institute for Advanced Study (Princeton) for hospitality and support while this paper was being written. They are obliged to B. de Smit for pointing out an error in an earlier version of §12. They also gratefully acknowledge help with several of the references from P. van Emde Boas, A. Hildebrand, and P. Stevenhagen. The first author was supported by NSF under Grant No. DMS 90-02939. The second author was supported by NSF under Grant No. DMS 90-02538.

REFERENCES

1. L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206.
2. Z. I. Borevič and I. R. Šafarevič, *Teorija čisel*, Izdat. "Nauka", Moscow, 1964; English transl., *Number theory*, Academic Press, New York, 1966.
3. R. P. Brent, *Fast multiple-precision evaluation of elementary functions*, J. Assoc. Comput. Mach. **23** (1976), 242–251.
4. J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance, *Factoring integers with the number field sieve*, in preparation.
5. E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum,"* J. Number Theory **17** (1983), 1–28.
6. D. Coppersmith, *Modifications to the number field sieve*, IBM Research Report RC 16264 (#72241), Yorktown Heights, 1990.
7. D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.
8. H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York, 1980.
9. P. G. Lejeune Dirichlet and R. Dedekind, *Vorlesungen uber Zahlentheorie*, 4th ed., Vieweg, Braunschweig, 1893, reprint, Chelsea, New York, 1968.
10. J. D. Dixon, *Asymptotically fast factorization of integers*, Math. Comp. **36** (1981), 255–260.
11. W. J. Ellison, *Les nombres premiers*, Hermann, Paris, 1975.
12. J. B. Friedlander and J. C. Lagarias, *On the distribution in short intervals of integers having no large prime factor*, J. Number Theory **25** (1987), 249–273.
13. J. L. Hafner and K. S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), 837–850.
14. D. S. Johnson, *The NP-completeness column: an ongoing guide*, J. Algorithms **5** (1984), 433–447.
15. J. C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. Algorithms **1** (1980), 142–186.
16. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.
17. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, A. Frohlich (ed.), Algebraic Number Fields: *L*-functions and Galois Properties, Academic Press, London, 1977, pp. 409–464.
18. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
19. A. K. Lenstra, *Factorization of polynomials*, in [27], pp. 169–198.
20. ——, *Fast and rigorous factorization under the generalized Riemann hypothesis*, Nederl. Akad. Wetensch. Proc. Ser. A **91** (Indag. Math. **50**) (1988), 443–454.
21. A. K. Lenstra and H. W. Lenstra, Jr., *Algorithms in number theory*, J. van Leeuwen (ed.), Handbook of Theoretical Computer Science, Volume A, Algorithms and Complexity, Elsevier, Amsterdam, 1990, Chapter 12, pp. 673–715.
22. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, *The factorization of the ninth Fermat number*, in preparation.
23. ——, *The number field sieve*, in preparation. Extended abstract: Proc. 22nd Annual ACM Symp. on Theory of Computing (STOC), Baltimore, May 14–16, 1990, pp. 564–572.
24. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.
25. ——, *On the calculation of regulators and class numbers of quadratic fields*, J. Armitage (ed.), Journées Arithmétiques 1980, London Math. Soc. Lecture Note Ser., no. 56, Cambridge University Press, Cambridge, 1982, pp. 123–150.
26. ——, *Primality testing algorithms*, Seminaire Bourbaki **33**, exp. no. 576, Lecture Notes in Math., vol. 901, Springer-Verlag, Heidelberg, 1981, pp. 243–257.

27 H W Lenstra, Jr and R Tijdeman (eds), *Computational methods in number theory*, Mathematical Centre Tracts **154/155**, Mathematisch Centrum, Amsterdam, 1982

28 C Pomerance, *Fast, rigorous factorization and discrete logarithm algorithms*, D S Johnson, T Nishizeki, A Nozaki, H S Wilf (eds), Discrete Algorithms and Complexity, Academic Press, Orlando, 1987, pp 119–143

29 C P Schnorr and H W Lenstra, Jr , *A Monte Carlo factoring algorithm with linear storage*, Math Comp **43** (1984), 289–311

30 R J Schoof, *Quadratic fields and factorization*, in [27], pp 235–286

31 I Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G Polya Uber die Verteilung der quadratischen Reste und Nichtreste*, Nachr Kon Ges Wiss Gottingen, Math - phys Kl (1918), 30–36, Gesammelte Abhandlungen, vol II, Springer, Berlin, 1973, pp 239–245

32 M Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Math Comp **48** (1987), 757–780

33 B Vallee, *Generation of elements with small modular squares and provably fast integer factoring algorithms*, Math Comp **56** (1991), 823–849

34 D Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans Inform Theory **32** (1986), 54–62

ABSTRACT In this paper a probabilistic algorithm is exhibited that factors any positive integer n into prime factors in expected time at most $L_n[\frac{1}{2}, 1+o(1)]$ for $n \to \infty$, where $L_x[a, b] = \exp(b(\log x)^a(\log\log x)^{1-a})$ Many practical factoring algorithms, including the quadratic sieve and the elliptic curve method, are conjectured to have an expected running time that satisfies the same bound, but this is the first algorithm for which the bound can be rigorously proved Nevertheless, this does not close the gap between rigorously established time bounds and merely conjectural ones for factoring algorithms This is due to the advent of a new factoring algorithm, the number field sieve, which is conjectured to factor any positive integer n in time $L_n[\frac{1}{3}, O(1)]$

The algorithm analyzed in this paper is a variant of the class group relations method, which makes use of class groups of binary quadratic forms of negative discriminant This algorithm was first suggested by Seysen, and later improved by A K Lenstra, who showed that the algorithm runs in expected time at most $L_n[\frac{1}{2}, 1+o(1)]$ if one assumes the generalized Riemann hypothesis The main device for removing the use of the generalized Riemann hypothesis from the proof is the use of multipliers In addition a character sum estimate for algebraic number fields is used, with an explicit dependence on possible exceptional zeros of the corresponding L-functions

Another factoring algorithm using class groups that has been proposed is the random class groups method It is shown that there is a fairly large set of numbers that this algorithm cannot be expected to factor as efficiently as had previously been thought

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720
E mail address hwl@math berkeley edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602
E mail address carl@ada math uga edu