THE NUMBER FIELD SIEVE

Peter Stevenhagen

Abstract. We describe the main ideas underlying the factorization of integers using the number field sieve.

1. Introduction

The number field sieve is a factoring algorithm that tries to factor a 'hard' composite number by exploiting factorizations of smooth numbers in a well-chosen algebraic number field. It is similar in nature to the quadratic sieve algorithm, but the underlying number theory is less elementary, and the actual implementation involves a fair amount of optimization of the various parameters.

The key idea of the algorithm, the use of smooth numbers in number rings different from $\mathbf{Z}$, was proposed in 1988 by Pollard. Many people have contributed theoretical and practical improvements since then. An excellent reference for many of the details left out in this paper is [4]. It contains a complete bibliography of the early years of the number field sieve, as well as original contributions by most of the main developers of the algorithm.

Among the successes of the algorithm are the 1999 factorization of the 512-bit RSA challenge number

$$\text{RSA-155} = p_{78} \cdot q_{78}$$

into a product of two primes of 78 decimal digits each, and the factorization in 2000 of the 233-digit Cunningham number

$$2^{773} + 1 = 3 \cdot 533371 \cdot p_{55} \cdot p_{71} \cdot p_{102}$$

into a product of 3, 533371 and three primes of 55, 71, and 102 digits, respectively. Unlike RSA-155, the second number has a 'special form' that can be exploited by the number field sieve. No other algorithm is currently capable of factoring integers of this size.

For the quadratic sieve algorithm and the elliptic curve method, the conjectural asymptotic expected running time for factoring a large number n is

$$\exp(\sqrt{\log n \log\log n}),$$

Typeset by $\mathcal{AMS}$-TEX
version October 7, 2004

which is on a loglog-scale 'half way' between exponential and polynomial. The number field sieve conjecturally improves this bound to

$$\exp(c(\log n)^{1/3}(\log\log n)^{2/3}), \tag{1.1}$$

where the constant $c = (64/9)^{1/3} \approx 1.93$ can be lowered to $(32/9)^{1/3} \approx 1.53$ if we are dealing with numbers n of the 'special form' explained in section 3.

2. Factoring by congruent squares

The number field sieve is one of the algorithms that tries to factor n by producing *congruent squares* modulo n, as explained in [8]. For this we will assume from now on that n is odd, composite and not a power of a prime number. Note that each of these conditions can easily be checked for large n. One tries to find integers x and y satisfying $x \not\equiv \pm y \bmod n$ and

$$x^2 \equiv y^2 \bmod n. \tag{2.1}$$

In this case, $\gcd(x - y, n)$ is a non-trivial factor of n. As at least half of all pairs (x, y) of invertible residue classes modulo n satisfying (2.1) satisfy $x \not\equiv \pm y \bmod n$, we may expect to find a non-trivial factor of n within a few tries if we can produce solutions (x, y) to (2.1) in a pseudo-random way.

An old factoring algorithm based on this idea is the *continued fraction method*. It uses the convergents $x_i/y_i \in \mathbf{Q}$ $(i = 1, 2, \dots)$ occurring in the continued fraction expansion of $\sqrt{n}$ as defined in [1]. These fractions, which can be computed from simple two-term recursive relations for the integers x_i and y_i, provide rational approximations to the real number $\sqrt{n}$. The associated integers

$$Q_i = x_i^2 - ny_i^2$$

are of absolute value at most $2\sqrt{n}$, and we may hope to be able to find a fair number of these Q_i which are *smooth*. As we saw in [8], it is a matter of linear algebra over the field of two elements to construct a square from a sufficiently large set of integers that factor over a given factor base. From every *square* $y^2 = \prod_{i \in I} Q_i$, we find a solution

$$(\prod_{i \in I} x_i)^2 \equiv y^2 \bmod n$$

to the congruence (2.1).

The *quadratic sieve* replaces the integers Q_i in the continued fraction algorithm by the values of the polynomial

$$Q(X) = X^2 - n.$$

For integers x satisfying $|x - \sqrt{n}| < M$ for some small bound M, the absolute value of $Q(x)$ is not much larger than $2M\sqrt{n}$. As M has to be large enough to allow for a reasonable supply of x-values, the numbers $Q(x)$ we encounter here are somewhat larger than the Q_i above. However, the advantage of using values of the polynomial Q is that the values of x for which $Q(x)$ is smooth may be detected by *sieving*.

From the smooth values of Q, we construct a *square* $y^2 = \prod_{x\in S} Q(x)$ and a solution

$$(\prod_{x\in S} x)^2 \equiv y^2 \bmod n,$$

to the basic congruence (2.1) exactly as for the continued fraction algorithm.

The algebraic description one may give of both methods is as follows. We have constructed squares $(x^2, y^2) \in \mathbf{Z} \times \mathbf{Z}$ whose images under the reduction map

$$\begin{array}{rcl} \mathbf{Z} \times \mathbf{Z} & \xrightarrow{\phi} & \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ (x_i^2, x_i^2 - ny_i^2) & \longmapsto & (x_i^2, x_i^2) \\ (x^2, x^2 - n) & \longmapsto & (x^2, x^2) \end{array}$$

lie in the 'diagonal'. If we are lucky, $\phi(x, y)$ does *not* land in

$$D = \{(x, \pm x) : x \in \mathbf{Z}/n\mathbf{Z}\}$$

and we find a non-trivial factor of n. As (x^2, y^2) is constructed in such a way that $\phi(x, y)$ has no obvious reason to always end up in D, we expect to be lucky in at least half of all cases.

The construction of squares in the continued fraction and quadratic sieve methods requires many auxiliary numbers Q_i or $Q(x)$ of size $O(\sqrt{n})$ to be smooth. The superior performance of the number field sieve stems from the fact that it is a sieving method that requires substantially smaller auxiliary numbers to be smooth: they are of size

$$\exp(c'(\log n)^{2/3}(\log\log n)^{1/3})$$

with $c' = (64/3)^{1/3} \approx 2.77$. Informally phrased, the 'length' of these numbers is not *half* of the length of n, but only the $2/3$-*rd power* of the length of n. This improvement is obtained by replacing $\mathbf{Z} \times \mathbf{Z}$ by $\mathbf{Z} \times \mathbf{Z}[\alpha]$ for a suitable *number ring* $\mathbf{Z}[\alpha]$ and producing squares (x^2, γ^2) with diagonal image under the reduction map

$$\mathbf{Z} \times \mathbf{Z}[\alpha] \xrightarrow{\phi} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

Exactly as before, this yields a solution

$$x^2 \equiv \phi(\gamma)^2 \bmod n \tag{2.2}$$

to our basic congruence (2.1).

3. Number rings

A number field is a finite field extension of the field $\mathbf{Q}$ of rational numbers, and a *number ring* [10] is by definition a subring of a number field. The basic type of number ring used in the number field sieve is the ring

$$\mathbf{Z}[\alpha] = \mathbf{Z}[X]/f\mathbf{Z}[X]$$

generated by a 'formal zero' $\alpha = (X \bmod f\mathbf{Z}[X])$ of some *irreducible* polynomial $f \in \mathbf{Z}[X]$ of degree $d \geq 1$. The elements of this ring are finite expressions $\sum_{i\geq 0} a_i\alpha^i$ with $a_i \in \mathbf{Z}$. One may obtain an embedding $\mathbf{Z}[\alpha] \subset \mathbf{C}$ by taking α to be a *complex* zero of f. Note that even though the field of fractions of a number ring is always of the form $\mathbf{Q}(\alpha)$ for some root α of an irreducible polynomial in $\mathbf{Z}[X]$, there are many number rings that are of finite rank over $\mathbf{Z}$ but not of the form $\mathbf{Z}[\alpha]$.

We will take f to be a *monic* irreducible polynomial in $\mathbf{Z}[X]$, such that

$$\mathbf{Z}[\alpha] = \mathbf{Z}\cdot 1 \oplus \mathbf{Z}\cdot\alpha \oplus \mathbf{Z}\cdot\alpha^2 \oplus \ldots \oplus \mathbf{Z}\cdot\alpha^{d-1}$$

is *integral* over $\mathbf{Z}$. It is an *order* in the field of fractions $\mathbf{Q}(\alpha)$ of $\mathbf{Z}[\alpha]$.

The *norm*

$$N : \mathbf{Q}(\alpha) \to \mathbf{Q}$$

takes $x \in \mathbf{Q}(\alpha)$ to the determinant of the multiplication-by-x map on the $\mathbf{Q}$-vector space $\mathbf{Q}(\alpha)$. It is multiplicative, and for non-zero $x \in \mathbf{Z}[\alpha]$, the absolute value

$$|N(x)| = \#(\mathbf{Z}[\alpha]/x\mathbf{Z}[\alpha]) \in \mathbf{Z}$$

of the norm of x measures the 'size' of x.

Example 3.1. The best known example of a number ring with $d = \deg(f) > 1$ is probably the ring $\mathbf{Z}[i]$ of *Gaussian integers* obtained by putting $f = X^2 + 1$ and $\alpha = i = \sqrt{-1}$. For this ring, the norm function is given by the simple formula

$$N(a + bi) = a^2 + b^2. \qquad //$$

More generally, one can find the norm of an element $x = a - b\alpha \in \mathbf{Q}(\alpha)$ from the irreducible polynomial $f = \sum_{i=0}^{d} c_iX^i$ of α as

$$N(a - b\alpha) = b^d f(a/b) = \textstyle\sum_{i=0}^{d} c_ia^ib^{d-i}. \tag{3.2}$$

For polynomial expressions $g(\alpha)$ in α of higher degree the norm can efficiently be computed from the resultant of f and g, but we won't need this.

For a number ring $\mathbf{Z}[\alpha]$ to be useful in factoring n, it needs to come with a reduction homomorphism

$$\phi : \mathbf{Z}[\alpha] \to \mathbf{Z}/n\mathbf{Z}.$$

Giving such a homomorphism amounts to giving a zero $m = \phi(\alpha)$ of f modulo n. In order to have a 'small' number ring $\mathbf{Z}[\alpha]$, one tries to choose a polynomial f of moderate degree—in practice d is usually between 3 and 10, although its optimal value does slowly tend to infinity with n—and having small coefficients. This is not an easy problem, but for certain *special* n one can find very small f.

Example 3.3. For the Fermat number

$$n = F_9 = 2^{2^9} + 1 = 2^{512} + 1$$

the polynomial $f = X^5 + 8$ is irreducible in $\mathbf{Z}[X]$ and satisfies

$$f(2^{103}) = 2^{515} + 8 = 8n \equiv 0 \bmod n.$$

Similarly, for the record factorization of the Cunningham number $n = 2^{773} + 1$ mentioned in the introduction, the polynomial $f = X^6 + 2$ is irreducible in $\mathbf{Z}[X]$ and satisfies

$$f(2^{129}) = 2^{774} + 2 = 2n \equiv 0 \bmod n. \qquad //$$

For numbers n of the special form $n = r^e - s$, with r, s and e 'small', one can find a small polynomial f as in the example. For *general* n we cannot hope to be so lucky in finding f, and one has to deal with 'large' number rings. The *special* and the *general* number field sieve stand for the versions of the algorithm corresponding to these two cases. As is to be expected, the special number field sieve has a somewhat better conjectural running time, and this is reflected by the size of the record factorizations for each of these versions.

We will mainly be concerned with the case of general integers n to be factored. For such n, the 'base m' method yields a polynomial f of any desired degree $d > 1$ such that $m = m(d)$ is a zero of f modulo n. One simply puts

$$m = \Big(\text{integer part of } n^{1/d}\Big)$$

and writes n in base m as

$$n = \textstyle\sum_{i=0}^{d} c_i m^i.$$

Then $f = \sum_{i=0}^{d} c_i X^i$ is a polynomial in $\mathbf{Z}[X]$ satisfying $f(m) = n$. In realistic situations n is much larger than d, which ensures that f will be *monic*; one may further assume that f is *irreducible*, as non-trivial factors of f yield non-trivial factors of n.

From $|c_i| < m < n^{1/d}$ we deduce that the discriminant $\Delta(f)$ of f satisfies

$$|\Delta(f)| < d^{2d} n^{2-3/d}. \tag{3.4}$$

As $|\Delta(f)|$ often exceeds n, we cannot hope to be able to factor $\Delta(f)$.

4. Sieving for smooth elements

Having chosen d, f and m as above, we can combine the ordinary reduction map on $\mathbf{Z}$ with our reduction map on $\mathbf{Z}[\alpha]$ to obtain a ring homomorphism

$$\begin{array}{ccc} \mathbf{Z}\times\mathbf{Z}[\alpha] & \xrightarrow{\phi} & \mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/n\mathbf{Z} \\ (x, \sum_{i=0}^{d-1} a_i\alpha^i) & \longmapsto & (x \bmod n, \sum_{i=0}^{d-1} a_i m^i \bmod n). \end{array}$$

By construction, the elements $(a-bm, a-b\alpha)$ have ϕ-image in the 'diagonal'. In order to combine them into squares, we need to find sets S of coprime integer pairs (a,b) for which we have

$$\prod_{(a,b)\in S}(a-bm) \quad \text{is a square in } \mathbf{Z}; \tag{4.1}$$

$$\prod_{(a,b)\in S}(a-b\alpha) \quad \text{is a square in } \mathbf{Z}[\alpha]. \tag{4.2}$$

As in the case of the quadratic sieve, this is in principle done by sieving for *smooth* elements $(a-bm, a-b\alpha)$ and combining them into a square via linear algebra methods over $\mathbf{F}_2$. The details are however more involved.

Let us define an element $(a-bm, a-b\alpha)\in\mathbf{Z}\times\mathbf{Z}[\alpha]$ to be *y-smooth* if $a-bm$ is a y-smooth rational integer and $a-b\alpha$ is a y-smooth algebraic integer in $\mathbf{Z}[\alpha]$. The latter condition simply means that the norm $N(a-b\alpha)\in\mathbf{Z}$ is a y-smooth integer. On the rational side, the procedure to find a set S for which (4.1) holds is more or less standard. We pick a 'universe'

$$U = \{(a,b) : |a|\le u, \quad 0<b\le u \quad \text{and} \quad \gcd(a,b)=1\}$$

of coprime integer pairs (a,b) depending on a parameter u.

Using the factor base B_1 consisting of primes $p\le y$ and a sign-bit, we can determine the subset of pairs $(a,b)\in U$ for which $a-bm$ is y-smooth by sieving. here we have a 2-dimensional array of pairs (a,b) over which the sieving with the primes in B_1 needs to be done. One may simply choose to sieve over a for each value of b, but there exist other methods than this straightforward 'line-by-line' sieving. Recent record factorizations have used a combination of different sieving methods.

On the algebraic side, the pairs $(a,b)\in U$ for which $N(a-b\alpha)$ is y-smooth can also be found by sieving with the primes in B_1, since we see from (3.2) that the norms

$$N(a-b\alpha) = b^d f(a/b) = \sum_{i=0}^{d} c_i a^i b^{d-i} \tag{4.3}$$

are the (a,b)-values of the homogeneous polynomial $f(X,Y)$. It is however *not* sufficient to find elements $a-b\alpha$ whose norm factors over our factor base B_1. This information will only enable us to construct a product $\prod_{(a,b)\in S}(a-b\alpha)$ with square norm, which is far too weak to imply (4.2). A square in $\mathbf{Z}[\alpha]$ certainly has square norm, but the converse only holds in the trivial case $\mathbf{Z}[\alpha]=\mathbf{Z}$, where the norm of an element is the element itself.

Example 4.4. In the ring of Gaussian integers $\mathbf{Z}[i]$ we have

$$N(3+4i)=3^2+4^2=5^2=N(5).$$

Now $3+4i=(2+i)^2$ is indeed a square, but $5=(2+i)(2-i)$ is not. //

The problem we encounter is that *different* prime divisors of an element $x\in\mathbf{Z}[\alpha]$ can give rise to the *same* prime factor p in its norm $N(x)$. This forces us to keep track of 'prime factors' of x *in the ring* $\mathbf{Z}[\alpha]$.

5. Primes dividing $a-b\alpha$

The theory of prime divisors in number rings lies at the very heart of algebraic number theory, and understanding the workings of the number field sieve is not possible without entering this area. Rather than assuming the more extensive exposition on the arithmetic of number rings in [10], we use the concrete example of our number ring $\mathbf{Z}[\alpha]$ to illustrate and motivate the more general statements of algebraic number theory in that paper.

Let R be any number ring. A *prime* in R is a non-zero prime ideal $\mathfrak{p}\subset R$. The residue class ring $F=R/\mathfrak{p}$ of a prime is a finite field. We say that $\mathfrak{p}$ *divides* an element $x\in R$ if x is contained in $\mathfrak{p}$. For the number ring $\mathbf{Z}$ the primes $p\mathbf{Z}$ correspond to the prime numbers $p\in\mathbf{Z}$. A prime $\mathfrak{p}\subset R$ *lies over* a unique prime $p\mathbf{Z}=\mathfrak{p}\cap\mathbf{Z}$ of $\mathbf{Z}$. The corresponding prime number p is the characteristic of the field F. It is the unique prime number contained in $\mathfrak{p}$. The *degree* of $\mathfrak{p}$ is the degree of F over its prime field $\mathbf{F}_p$.

A *prime of degree* 1 in $\mathbf{Z}[\alpha]$ is nothing but the kernel $\mathfrak{p}$ of a ring homomorphism

$$\pi:\mathbf{Z}[\alpha]\longrightarrow\mathbf{F}_p$$

for some prime number p. As π may be specified by giving the rational prime p together with the zero $r_p=\pi(\alpha)\in\mathbf{F}_p$ of $(f \bmod p)$ to which α is mapped, we use the ad hoc notation $\mathfrak{p}\sim(p,r_p)$ to denote $\mathfrak{p}=\ker\pi$.

Primes of degree 1 are the only primes we need for the number field sieve. Indeed, suppose that we have $(a,b)\in U$ as in the previous section, and that $\mathfrak{p}$ is a prime over p dividing $a-b\alpha$. Then we have $p\nmid b$, since $p|b$ would imply $a\in\mathfrak{p}\cap\mathbf{Z}=p\mathbf{Z}$, contradicting the coprimality of a and b. From $\overline{a}=\overline{b}\overline{\alpha}\in F=\mathbf{Z}[\alpha]/\mathfrak{p}$ we find that $r_p=\overline{\alpha}=ab^{-1} \bmod p$ is a zero of $(f \bmod p)$, and that

$$\mathfrak{p}=p\mathbf{Z}[\alpha]+(a-b\alpha)\mathbf{Z}[\alpha]$$

is the kernel of the map

$$\begin{aligned}\mathbf{Z}[\alpha]&\xrightarrow{\pi}\mathbf{F}_p\\ \alpha&\longmapsto(ab^{-1} \bmod p).\end{aligned}$$

Thus $\mathfrak{p} \sim (p, r_p)$ is of degree 1, with $r_p = ab^{-1} \bmod p$ a zero of $f \bmod p$. Conversely, a prime (p, r_p) of degree 1 divides $a - b\alpha$ if we have $r_p = ab^{-1} \bmod p$.

From our norm formula (3.2), we see that $ab^{-1} \bmod p$ is a zero of $(f \bmod p)$ if and only if $N(a - b\alpha)$ is divisible by p. We conclude that for a rational prime number p, there is a prime divisor $\mathfrak{p}$ of $a - b\alpha$ in $\mathbf{Z}[\alpha]$ that lies over p if and only if p divides the norm $N(a - b\alpha)$. If p divides $N(a - b\alpha)$, the prime $\mathfrak{p} \sim (p, r_p)$ with $r_p = (ab^{-1} \bmod p)$ is the unique such prime, and we call

$$e_{\mathfrak{p}}(a - b\alpha) = \mathrm{ord}_p(N(a - b\alpha))$$

the *exponent* to which $\mathfrak{p}$ occurs in $a - b\alpha$. For the primes $\mathfrak{p}$ of $\mathbf{Z}[\alpha]$ that do not divide $a - b\alpha$, we put $e_{\mathfrak{p}}(a - b\alpha) = 0$. We then have the following fundamental fact.

5.1. Lemma. *For each prime $\mathfrak{p}$ of degree 1, the exponent $e_{\mathfrak{p}}$ extends to a homomorphism*

$$e_{\mathfrak{p}} : \mathbf{Q}(\alpha)^* \to \mathbf{Z}.$$

This Lemma is slightly less innocent than it may appear at first sight, and we will define $e_{\mathfrak{p}}(x)$ for arbitrary $x \in \mathbf{Q}(\alpha)^*$ in (7.4). There is actually no need to restrict to primes of degree 1, but we do so as we have not defined the exponent at other primes. For our purposes, it suffices to know that we have $e_{\mathfrak{p}}(x) = 0$ whenever x is a product of elements $a - b\alpha$ with $(a, b) \in U$ and $\mathfrak{p}$ is a prime of degree at least 2.

6. Sieving and linear algebra

On the rational side, we already chose a factor base B_1 consisting of the primes $p \leq y$ and a sign bit. For the factorization of our numbers $a - b\alpha$ in $\mathbf{Z}[\alpha]$, we choose a factor base B_2 consisting of all primes $\mathfrak{p} \sim (p, r_p)$ with $p \leq y$ prime and $r_p \in \mathbf{F}_p$ a root of $(f \bmod p)$. There may be several primes in B_2 lying over a given rational prime p, and the notation (p, r_p) enables us to distinguish between such primes, and to identify the prime that accounts for the p-contribution (if any) to $N(a - b\alpha)$.

For each rational p, there are at most $d = \deg(f)$ values r_p. On average, there is 1 root of $(f \bmod p)$ in $\mathbf{F}_p$ if we let y tend to infinity. This elegant result of Kronecker, which was generalized by Frobenius, is now often proved as a corollary of the Chebotarev density theorem [9]. We deduce that both B_1 and B_2 are of size $y^{1+o(1)}$.

The combination of rational and algebraic sieving yields a subset $U' \subset U$ of pairs $(a, b) \in U$ that give rise to a y-smooth factorization of $a - bm$ in $\mathbf{Z}$ and a y-smooth factorization of $a - b\alpha$ in $\mathbf{Z}[\alpha]$. Such a pair $(a, b) \in U'$, together with the exponents of the rational primes $p \in B_1$ in $a - bm$ and the exponents of the algebraic primes $\mathfrak{p}$ in $a - b\alpha$, is usually referred to as a *relation*. All exponents are taken modulo 2, so they can be stored in a single bit.

In order to obtain dependencies between the exponent vectors of elements in U', the number $\#U'$ of relations should exceed $\#B_1 + \#B_2$. For large factorizations, collecting sufficiently many relations may take several years of computer time. As different computers can independently test elements $(a, b) \in U$ for smoothness, distribution of the computation over a large number of computers is usually necessary to perform this step of the algorithm in practice.

The set U', which may consist of millions of relations, is often so large that the linear algebra step over $\mathbf{F}_2$ needs to be performed on a computer that is equipped to handle huge amounts of data. It is important that the matrix of exponents is a very *sparse* matrix, which can be transformed into a much smaller 'dense' matrix before it is given to the reduction algorithm that yields the desired dependencies. A practical reduction algorithm, such as the so-called block Lanczos method, may run for several days on a single large computer. In this case, distribution of the problem over more computers is not an easy matter.

Every dependency in the matrix of exponent vectors coming from the pairs $(a, b) \in U'$ corresponds to a subset $S \subset U'$ such that the following two conditions are satisfied:

$$(6.1) \qquad \prod_{(a,b)\in S} (a - bm) \quad \text{is positive with even exponents at all primes } p \in \mathbf{Z};$$

$$(6.2) \qquad \prod_{(a,b)\in S} (a - b\alpha) \quad \text{has even exponents at all primes } \mathfrak{p} \subset \mathbf{Z}[\alpha].$$

What we need is the validity of (4.1) and (4.2) in order to obtain the required square in $\mathbf{Z} \times \mathbf{Z}[\alpha]$. It is a simple and well known fact that (6.1) implies (4.1): requiring positivity is enough to produce true squares from integers having even exponents at all prime numbers. The situation is not so simple in $\mathbf{Z}[\alpha]$: several obstructions may prevent the validity of the implication (6.2) $\Rightarrow$ (4.2). Writing $\beta = \prod_{(a,b)\in S}(a - b\alpha)$ for the element in (6.2), they are the following.

6.3. The ring $\mathbf{Z}[\alpha]$ is possibly not the *ring of integers* $\mathcal{O}$ of $\mathbf{Q}(\alpha)$. The ring of integers, which is the *maximal* order in $\mathbf{Q}(\alpha)$, is the 'text book ring' for which the theorem of unique prime ideal factorization holds. If we have $\mathbf{Z}[\alpha] \neq \mathcal{O}$, then (6.2) need not imply that $\beta\mathcal{O}$ is the square of an ideal.

6.4. If $\beta\mathcal{O}$ is the square of some *ideal* $\mathfrak{c}$, then $\mathfrak{c}$ does not have to be a *principal* $\mathcal{O}$-ideal. This is exactly the reason why unique prime element factorization has to be replaced by unique prime ideal factorization in general number fields.

6.5. If $\beta\mathcal{O}$ is the square of some principal ideal $\gamma\mathcal{O}$, we only have $\beta = \gamma^2$ up to multiplication by *units* in $\mathcal{O}$. This obstruction already occurs in the case for $\mathcal{O} = \mathbf{Z}$. Unlike $\mathbf{Z}$, the ring $\mathcal{O}$ usually has infinitely many units.

6.6. If we do obtain an equality $\beta = \gamma^2$ in $\mathcal{O}$, we may have $\gamma \notin \mathbf{Z}[\alpha]$. If this happens, the reduction map ϕ is not defined on γ and we do not obtain our final congruence (2.2).

Algebraic number theory provides the tools for dealing with all of these obstructions. In the next section, we will deal with the obstructions 6.3 and 6.6, which arise from the fact that $\mathbf{Z}[\alpha]$ may be strictly smaller than $\mathcal{O}$. Section 8 is devoted to the obstructions 6.4 and 6.5, which are classical and lie at the roots of algebraic number theory. It will be our aim to bound the index $[V : (V \cap \mathbf{Q}(\alpha)^{*2})]$ of the subgroup of true squares inside the group $V \subset \mathbf{Q}(\alpha)^*$ generated by the elements that meet condition (6.2).

7. Non-maximality of $\mathbf{Z}[\alpha]$

The ring of integers $\mathcal{O} \subset \mathbf{Q}(\alpha)$, which consists by definition of all elements of $\mathbf{Q}(\alpha)$ that occur as the zero of some monic polynomial in $\mathbf{Z}[X]$, is the maximal order contained in $\mathbf{Q}(\alpha)$. It is free of rank $d = \deg(f)$ over $\mathbf{Z}$, and contains $\mathbf{Z}[\alpha]$ as a subring of *finite* index. There is the classical identity

$$\Delta(f) = [\mathcal{O} : \mathbf{Z}[\alpha]]^2 \cdot \Delta \tag{7.1}$$

relating the index $[\mathcal{O} : \mathbf{Z}[\alpha]]$ to the discriminant $\Delta(f)$ of the polynomial f from (3.4) and the discriminant Δ of the number field $\mathbf{Q}(\alpha)$. As Δ is known to be a non-zero integer, we find that $[\mathcal{O} : \mathbf{Z}[\alpha]]$ is bounded by $|\Delta(f)|^{1/2}$. As we do not want to factor the possibly huge number $\Delta(f)$, we may not be able to determine $[\mathcal{O} : \mathbf{Z}[\alpha]]$ or $\mathcal{O}$. However, it is a standard fact that for any $x \in \mathcal{O}$, we have

$$f'(\alpha) \cdot x \in \mathbf{Z}[\alpha].$$

This is enough to deal with obstruction 6.6: we simply multiply our purported square in $\mathbf{Z} \times \mathbf{Z}[\alpha]$ by

$$(f'(m)^2, f'(\alpha)^2).$$

Then its square root gets multiplied by $(f'(m), f'(\alpha))$, so it will lie in $\mathbf{Z} \times \mathbf{Z}[\alpha]$. In order to keep an element that is invertible modulo n, we need to assume that $f'(m)$ is coprime to n. This is not a serious restriction as this condition is always satisfied in practice; if it isn't, we have found a factor of n without applying the number field sieve!

Example 7.2. Let us take $f = X^2 + 16$. Then the order $\mathbf{Z}[\alpha] = \mathbf{Z}[4i]$ has index 4 in the maximal order $\mathcal{O} = \mathbf{Z}[i]$ in $\mathbf{Q}(i)$. Example 4.4 shows that $3 + \alpha = 3 + 4i$ is a square in $\mathcal{O}$, but its square root $\gamma = 2 + \frac{1}{4}\alpha$ is not in $\mathbf{Z}[\alpha]$. However, the element $f'(\alpha) \cdot \gamma = 2\alpha \cdot \gamma = 4\alpha - 8$ does lie in $\mathbf{Z}[\alpha]$. //

In order for an ideal $\mathfrak{c} \subset \mathcal{O}$ to be a square of some other ideal, it is necessary and sufficient that the exponents $\mathrm{ord}_{\mathfrak{q}}(\mathfrak{b})$ are even at all primes $\mathfrak{q}$ of $\mathcal{O}$. This is an immediate corollary of the classical theorem of unique prime ideal factorization in $\mathcal{O}$. Now the primes $\mathfrak{q}$ of $\mathcal{O}$ coprime to the index $[\mathcal{O} : \mathbf{Z}[\alpha]]$ are 'the same' as the ideals $\mathfrak{p}$ of $\mathbf{Z}[\alpha]$ coprime to the index. By this we mean that there is a natural bijection between the sets of such primes given by $\mathfrak{q} \mapsto \mathfrak{p} = \mathfrak{q} \cap \mathbf{Z}[\alpha]$. Moreover, if $\mathfrak{p}$ and $\mathfrak{q}$ are corresponding prime ideals, the inclusion map $\mathbf{Z}[\alpha] \subset \mathcal{O}$ induces an isomorphism of the local rings

$$\mathbf{Z}[\alpha]_{\mathfrak{p}} \xrightarrow{\sim} \mathcal{O}_{\mathfrak{q}}. \tag{7.3}$$

Both rings are discrete valuation rings, and the exponent $e_{\mathfrak{p}} : \mathbf{Q}(\alpha)^* \to \mathbf{Z}$ is in this case equal to the familiar prime ideal exponent $e_{\mathfrak{q}}$ for the ring of integers $\mathcal{O}$, which is multiplicative on the set of *all* non-zero $\mathcal{O}$-ideals, not just the principal ones.

For primes $\mathfrak{q}$ of $\mathcal{O}$ dividing the index $[\mathcal{O} : \mathbf{Z}[\alpha]]$, the situation is more complicated. There may be more primes $\mathfrak{q}$ lying above the same prime $\mathfrak{p} = \mathfrak{q} \cap \mathbf{Z}[\alpha]$, and even if $\mathfrak{p}$ has a single extension $\mathfrak{q}$ in $\mathcal{O}$, the natural map (7.3) need not be an isomorphism. If either of these happens, $\mathfrak{p}$ is said to be a *singular* prime of $\mathbf{Z}[\alpha]$. The other primes are the *regular* primes of $\mathbf{Z}[\alpha]$.

For a prime $\mathfrak{p}$ of $\mathbf{Z}[\alpha]$, we define the *exponent* at $\mathfrak{p}$ as the homomorphism $e_{\mathfrak{p}} : \mathbf{Q}(\alpha)^* \to \mathbf{Z}$ by

$$e_{\mathfrak{p}}(x) = \sum_{\mathfrak{q} \supset \mathfrak{p}} f(\mathfrak{q}/\mathfrak{p})\, e_{\mathfrak{q}}(x), \tag{7.4}$$

where the sum ranges over the primes $\mathfrak{q} \subset \mathcal{O}$ lying over $\mathfrak{p}$, and $f(\mathfrak{q}/\mathfrak{p})$ is the degree of the residue field extension $\mathbf{Z}[\alpha]/\mathfrak{p} \subset \mathcal{O}/\mathfrak{q}$. This definition provides the extension of the homomorphism $e_{\mathfrak{p}}$ occurring in Lemma 5.1. For regular primes $\mathfrak{p}$, formula (7.4) reduces to $e_{\mathfrak{p}} = e_{\mathfrak{q}}$.

We now consider, inside the subgroup of $\mathbf{Q}(\alpha)^*$ that is generated by the elements $a - b\alpha \in \mathbf{Z}[\alpha]$ having $\gcd(a, b) = 1$, the group V of those elements that have even exponents at the primes $\mathfrak{p}$ of $\mathbf{Z}[\alpha]$. We let $V_1 \subset V$ be the subgroup of elements $x \in V$ that have even exponents at all primes $\mathfrak{q}$ of $\mathcal{O}$, i.e., the elements $x \in V$ for which $x\mathcal{O}$ is the square of a $\mathcal{O}$-ideal. We have an injective homomorphism

$$\begin{aligned} V/V_1 &\longrightarrow \bigoplus_{\mathfrak{q} | [\mathcal{O}:\mathbf{Z}[\alpha]]} \mathbf{Z}/2\mathbf{Z} \\ x &\longmapsto (e_{\mathfrak{q}}(x) \bmod 2)_{\mathfrak{q}}, \end{aligned}$$

so V/V_1 is an $\mathbf{F}_2$-vector space of dimension bounded by the number of primes $\mathfrak{q}$ of $\mathcal{O}$ dividing the index $[\mathcal{O} : \mathbf{Z}[\alpha]]$. In view of (7.1), the number of rational primes dividing the index is no more than $\frac{1}{2} \log |\Delta(f)|$. For each of these primes there are at most $d = \deg(f)$ primes $\mathfrak{q}$ in $\mathcal{O}$ that divide it, so we find

$$\dim_{\mathbf{F}_2}(V/V_1) \leq \tfrac{1}{2} d \cdot \log(\Delta(f)). \tag{7.5}$$

This is a quantitative version of obstruction 6.3. Note that we have completely disregarded the fact that the elements of V have even exponents at the singular primes of $\mathbf{Z}[\alpha]$. It is possible to obtain a slightly better upper bound for the index $[V : (V \cap \mathbf{Q}(\alpha)^{*2})]$ than that in 8.4 by taking this into account.

8. Finiteness results from algebraic number theory

Inequality (7.5) is the first step in bounding the successive $\mathbf{F}_2$-dimensions of the quotient spaces in the filtration

$$V \supset V_1 \supset V_2 \supset V_3 = V \cap \mathbf{Q}(\alpha)^{*2}.$$

Here V_1 is the subgroup from the previous section consisting of those $x \in V$ for which $x\mathcal{O}$ is an ideal square, and V_2 is the subgroup of those $x \in V$ for which $x\mathcal{O}$ is the square of a *principal* $\mathcal{O}$-ideal. Thus, the $\mathbf{F}_2$-spaces V_1/V_2 and V_2/V_3 measure the obstructions 6.4 and 6.5, respectively. We can bound their dimensions using two fundamental finiteness results from algebraic number theory.

The first result says that the class group of $\mathbf{Q}(\alpha)$, which is the group of all fractional $\mathcal{O}$-ideals modulo the subgroup of principal $\mathcal{O}$-ideals, is a finite abelian group. One can derive from [5, Theorem 6.5] that its order h can be bounded in terms of the degree d and the discriminant $\Delta(f)$ of f by

$$h < |\Delta(f)|^{1/2} \cdot \frac{d - 1 + \log|\Delta(f)|^{d-1}}{(d-1)!}. \tag{8.1}$$

We can map V_1 to the class group by sending $x \in V_1$ to the ideal class of the ideal $\mathfrak{a}$ satisfying $\mathfrak{a}^2 = x\mathcal{O}$. This map has kernel V_2, so we find the dimension of the $\mathbf{F}_2$-vector space V_1/V_2 to be bounded by $\log(h)$, yielding

$$\dim_{\mathbf{F}_2}(V_1/V_2) \leq \log(h)/\log(2). \tag{8.2}$$

As the elements in V_2 are squares in $\mathbf{Q}(\alpha)^*$ up to multiplication by elements of the unit group $\mathcal{O}^*$, the order of V_2/V_3 does not exceed the order of $\mathcal{O}^*/\mathcal{O}^{*2}$. By the Dirichlet unit theorem [10], the group $\mathcal{O}^*$ is the product of a finite cyclic group of roots of unity in $\mathbf{Q}(\alpha)$ with a free abelian group of rank at most $d-1$. It follows that $\mathcal{O}^*/\mathcal{O}^{*2}$ is finite of order at most 2^d, and we find

$$\dim_{\mathbf{F}_2}(V_2/V_3) \leq d. \tag{8.3}$$

Putting the estimates (3.4), (7.5), (8.1), (8.2) and (8.3) together, we arrive after a short computation at the following theorem for the values of n and d that we need.

8.4 Theorem. *Let V be as above, and suppose we have $n > d^{2d^2} > 1$. Then the subgroup $V_3 = V \cap \mathbf{Q}(\alpha)^{*2}$ of squares in V satisfies*

$$\dim_{\mathbf{F}_2}(V/V_3) \leq (\log n)^{3/2}.$$

A more careful analysis using the information at the singular primes of $\mathbf{Z}[\alpha]$ shows [4, Theorem 6.7, p. 61] that the exponent $3/2$ can be replaced by 1.

9. Quadratic character columns

The algorithm described so far is only able to produce elements in $\mathbf{Z}\times\mathbf{Z}[\alpha]$ for which the second component is in V, but not necessarily in the subgroup $V_3 = V \cap \mathbf{Q}(\alpha)^{*2}$ of squares. In order for an element $x \in V$ to be V_3, it is necessary and sufficient that all characters $\chi : V/V_3 \to \mathbf{F}_2$ vanish on x. At most $k = \dim(V/V_3)$ characters are needed to span the dual space $W = \mathrm{Hom}(V/V_3, \mathbf{F}_2)$, and an element $x \in V$ is a square if and only if all these spanning characters assume the value 1 on x. As there is no easy way to produce a spanning set of characters, we will use *random* quadratic characters instead. An elementary calculation shows that if W is any k-dimensional $\mathbf{F}_2$-vector space, a randomly chosen set of $k+e$ elements has probability at least $1-2^{-e}$ of generating W. As this probability converges exponentially to 1 in the number e of 'extra' random elements, we can be 'morally sure' to generate W for moderate values of e.

We are now faced with the problem of exhibiting suffciently many 'quadratic characters' on $\mathbf{Z}[\alpha]$. On $\mathbf{Z}$, quadratic characters can be obtained from Legendre symbols $x \mapsto \left(\frac{x}{p}\right)$, which are easily evaluated. If $x \in \mathbf{Z}$ is *not* a square, we have, in a sense that is easily made precise,

$$\left(\tfrac{x}{p}\right) = -1$$

for 'half' of the primes p. More precisely, they are the odd primes p that remain prime in the number ring $\mathbf{Z}[\sqrt{x}]$.

Example 9.1. We have $\left(\frac{-16}{p}\right) = -1$ for all primes $p \equiv 3 \bmod 4$. //

Loosely speaking, we can say that an integer $x \neq 0$ that satisfies $\left(\frac{x}{p}\right) = 1$ for t randomly chosen primes p is a square with 'probability' $1-2^{-t}$. We can use an analogue of this idea over $\mathbf{Z}[\alpha]$.

Every prime $\mathfrak{q} = \ker \pi \sim (q, r_q)$ of degree 1 of $\mathbf{Z}[\alpha]$ gives rise to a Legendre symbol

$$\left(\tfrac{\cdot}{\mathfrak{q}}\right) : \mathbf{Z}[\alpha] \xrightarrow{\pi} \mathbf{F}_q \xrightarrow{\left(\frac{\cdot}{q}\right)} \{\pm 1\} \cup \{0\}$$

such that for non-square $x \in \mathbf{Z}[\alpha]$, we have $\left(\frac{x}{\mathfrak{q}}\right) = -1$ 'half of the time'. For y-smooth elements $x \in \mathbf{Z}[\alpha]$, we can avoid the character value 0 by restricting to Legendre symbols coming from primes $\mathfrak{q} \sim (q, r_q)$ of degree 1 with $q > y$. It is a consequence of the Chebotarev density theorem that the Legendre symbols coming from such $\mathfrak{q}$ are equidistributed over $\mathrm{Hom}(V/V_3, \{\pm 1\})$.

In the rational factor base B_1 consisting of primes $p \leq y$, we incorporated a 'sign bit' to ensure that the integers with even prime exponents at all primes p are actually squares. This 'sign bit' for $\mathbf{Z}$ is nothing but the non-trivial chracter on the 1-dimensional $\mathbf{F}_2$-vector space that becomes V/V_3 if we replace $\mathbf{Z}$ by $\mathbf{Z}[\alpha]$.

In a similar way, we incorporate in our algebraic factor base B_2, which so far consisted of the primes (p, r_p) with $p \leq y$, a sufficiently large number of $\mathbf{F}_2$-valued characters $\chi_{\mathfrak{q}} : V \to \mathbf{F}_2$ coming from the Legendre symbols of primes $\mathfrak{q} \sim (q, r_q)$ of degree 1 with $q > y$. The character $\chi_{\mathfrak{q}}$ is simply the Legendre symbol in additive notation, and the values $\chi_{\mathfrak{q}}(a - b\alpha)$ for $(a, b) \in U$ are treated exactly like the exponent values $e_{\mathfrak{p}}(a - b\alpha)$. In this way, we obtain a probabilistic algorithm for producing y-smooth elements $x \in V$ that do not only satisfy (6.2) but that are true squares. In this set-up the outcome of the linear algebra step, which reduces a matrix of approximate size $y \times y$, consists of subsets $S \subset U$ such that not only we have (6.1) and (6.2), but in addition

$$(f'(m)^2 \prod_{(a,b)\in S}(a-bm),\quad f'(\alpha)^2 \prod_{(a,b)\in S}(a-b\alpha))$$

is with very high probability a square $(x^2, \gamma^2) \in \mathbf{Z} \times \mathbf{Z}[\alpha]$.

10. Square root extraction

The element (x^2, γ^2) just found yields a solution to our basic congruence (2.1). In order to obtain a factorization of n, we now need the values $(x \bmod n)$ and $\phi(\gamma)$ in $\mathbf{Z}/n\mathbf{Z}$. The gcd of n with their difference is hopefully a non-trivial factor of n. Thus, we need to compute a square root (x, γ) of our square $(x^2, \gamma^2) \in \mathbf{Z}\times\mathbf{Z}[\alpha]$. On the rational side, this is immediate since we know how to extract squares in $\mathbf{Z}$. It is even possible to avoid computing the large number $x^2 = f'(m)^2 \prod_{(a,b)\in S}(a-bm)$ as we have a complete prime factorization of each of the elements $a-bm$ occurring in the product, and therefore a prime factorization of the product itself.

On the number field side, the situation is more complicated. The prime ideal factorization of $\prod_{(a,b)\in S}(a-b\alpha)$ is easily determined, but this is not immediately useful as prime ideals may not have generators at all and, moreover, we most likely will be unable to compute generators for the unit group $\mathcal{O}^*$ in the large number field $\mathbf{Q}(\alpha)$. Only for the special number field sieve [4, p. 21ff], which often yields rings of integers $\mathcal{O}$ with small units and trivial class group, one may be able to compute a square root of the element $\gamma^2 \in \mathbf{Z}[\alpha]$ using explicit generators of the primes in $\mathbf{Z}[\alpha]$.

For the general number field sieve, one can compute a root of the polynomial $X^2 - \gamma^2$ in $\mathbf{Q}(\alpha)$ by standard methods, such as successive approximation using Hensel's lemma [1] at an appropriate prime. Theoretically, this can be done without affecting the expected asymptotic running time of the algorithm. In practice, it is feasible as well but rather cumbersome because of the size of the number γ^2, which necessitates the handling of very large numbers in the final iterations. Montgomery's method [6, 7], which uses complex approximations, has a better practical performance but has not yet been carefully analyzed.

11. Running time

From the analysis given in [8], it follows that the conjectural asymptotic expected running time the quadratic sieve takes to factor n is

$$\exp((1+o(1))\sqrt{\log n \log\log n})$$

for n tending to infinity. The elliptic curve method has the same running time, which is 'half way' between exponential and polynomial.

For the number field sieve, we can do better if we carefully choose d and f, and optimize the smoothness bound y and the parameter u for the size of the universe U

of pairs (a, b) accordingly. We briefly sketch how to find heuristically the asymptotic optimal values, disregarding all lower order terms that occur along the way.

The basic cost of the algorithm, which is computed as in [8], is $u^{2+o(1)} + y^{2+o(1)}$ as n tends to infinity. The first term represents the sieving part of the algorithm, and equals the length of the sieve times a lower order factor. The second term is the matrix reduction part, which assumes that fast asymptotic methods are applied to a matrix of size at most $y \times y$. In order to balance these contributions, we will take $\log(u) \approx \log(y)$.

The numbers $a - b\alpha$ we consider are y-smooth if the integer $(a - bm) \cdot N(a - b\alpha)$ is, and using (4.3) and the size $n^{1/d}$ of m and of the coefficients of f, we may bound this integer by

$$un^{1/d} \cdot (d+1)u^d n^{1/d} \approx n^{2/d} u^{d+1}, \tag{11.1}$$

Here we already take into account that d will be chosen in (11.3) to be of much smaller order than the other factors. The 'u^u-philosophy' in [8] shows that a number $x \approx n^{2/d} u^{d+1}$ is y-smooth with 'probability' r^{-r}, where $r = \log x / \log y$. In order to maximize this probability, we minimize the quantity

$$r = \frac{\log x}{\log y} \approx \frac{\log x}{\log u} \approx \left(\frac{2 \log n}{\log u}\right) \frac{1}{d} + d + 1 \tag{11.2}$$

by taking the degree of f to be $d = (\frac{2 \log n}{\log u})^{1/2}$.

In order to obtain sufficiently many relations from our pairs $(a, b) \in U$ to create a dependent matrix, we need $u^2 \cdot r^{-r} \approx y$. Taking logarithms and replacing $\log y$ by $\log u$, we find $\log u \approx r \log r$ or, equivalently, $r \approx \log u / \log \log u$. Comparison with (11.2) for d as above now leads to

$$\left(\frac{2 \log n}{\log u}\right)^{1/2} \approx \frac{\log u}{\log \log u},$$

and we take 2/3-rd powers to obtain $\log u (\log \log u)^{-2/3} \approx 2(\log n)^{1/3}$. In order to rewrite this, we observe that if we have real quantities s, t satisfying $s = t(\log t)^a$ for some $a \in \mathbf{R}$, then, as t tends to infinity, we have $t = (1 + o(1))s(\log s)^{-a}$. Applying this for $t = \log u$ and $s = 2(\log n)^{1/3}$ with $a = -2/3$ we arrive at

$$\log y \approx \log u \approx 2(\log n)^{1/3} (\tfrac{1}{3} \log \log n)^{2/3} = (8/9)^{1/3} (\log n)^{1/3} (\log \log n)^{2/3}.$$

With this choice of the basic parameters u and y, the asymptotic running time $u^{2+o(1)} + y^{2+o(1)}$ becomes

$$\exp\left(\left((64/9)^{1/3} + o(1)\right) \left(\log n\right)^{1/3} \left(\log \log n\right)^{2/3}\right),$$

as claimed in (1.1). The optimal asymptotic value of the degree d of f comes out as

$$d \approx \left(\frac{2\log n}{\log u}\right)^{1/2} \approx \left(\frac{3\log n}{\log\log n}\right)^{1/3}, \tag{11.3}$$

and we find that the size in (11.1) of the integers we require to be smooth is

$$\exp\Big(\big((64/3)^{1/3}+o(1)\big)\big(\log n\big)^{2/3}\big(\log\log n\big)^{1/3}\Big).$$

This bound, which we mentioned already in section 2, makes the number field sieve the fastest general purpose factoring algorithm that is currently known.

As with the quadratic sieve, there are various practical improvements to the basic number field sieve as we have described it here. The most important "bells and whistles" are mentioned in [3, Section 6.2.7]. Although they do not significantly change the asymptotic running time of the algorithm, they greatly enhance its practical performance, and they are instrumental in completing the record factorizations that mark the borderlines of what is currently feasible in factoring.

References

1. J. P. Buhler, S. Wagon, *Basic algorithms in number theory*, this volume.
3. R. E. Crandall, C. Pomerance, *Prime numbers – a computational perspective*, Springer Verlag, 2001.
4. A. K. Lenstra, H. W. Lenstra, Jr. (Eds.), *The development of the number field sieve*, vol. 1554, Springer Lecture Notes in Mathematics, 1993.
5. H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), no. 2, 211–244.
6. P. Montgomery, *Square roots of products of algebraic numbers*, Mathematics of Computation 1943–1993 (W. Gautschi, ed.), Proc. Sympos. Appl. Math., vol. 48, 1994, pp. 567–571.
7. P. Nguyen, *A Montgomery-like square root for the number field sieve*, Algorithmic Number Theory (J. P. Buhler, ed.), proceedings of ANTS-III, vol. 1423, Springer Lecture Notes in Computer Science, 1998, pp. 151–168.
8. C. Pomerance, *Smooth numbers and the quadratic sieve*, this volume.
9. P. Stevenhagen, H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
10. P. Stevenhagen, *The arithmetic of number rings*, this volume.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

E-mail address: psh@math.leidenuniv.nl