SQUARE ROOTS OF PRODUCTS OF ALGEBRAIC NUMBERS

PETER L. MONTGOMERY

ABSTRACT. Let α be an algebraic number. Let $\gamma(\alpha) = \prod_i g_i(\alpha)$ be a product which we suspect is a nonzero square in $\mathbb{Q}(\alpha)$. We assume that the prime ideal factorization of each $(g_i(\alpha))$ (and hence of $(\gamma(\alpha)))$ is known; in particular, each prime ideal should have even exponent in $(\gamma(\alpha))$. Using this ideal factorization, we construct a square root of $\gamma(\alpha)$, if it exists. The algorithm uses lattice basis reduction to estimate a square root, successively replacing the problem by a simpler one until the problem can be done directly. Like the original $\gamma(\alpha)$, its constructed square root will have a product form. The algorithm generalizes to k–th roots for arbitrary $k > 0$.

CONTENTS

Date: Draft of May 16, 1997 — little different from May, 1995 version. Comments welcome.
WARNING — Not proofread very carefully.

1991 *Mathematics Subject Classification.* 11Y40; Secondary 11Y05.

Key words and phrases. Lattice basis reduction, number field sieve, fractional ideal, factorization.

Work supported in part by NSF grant DMS–9012989 while the author was at Oregon State University, by Centrum voor Mathematica en Informatica in Amsterdam, and by Stieltjes Institute for Mathematics, Leiden, The Netherlands.

List of Tables

1. Preliminaries

Let $f(X) = \sum_{j=0}^{d} c_j X^j \in \mathbb{Z}[X]$ be an irreducible polynomial of degree d, where $\gcd(c_0, c_1, \cdots, c_d) = 1$. Let α be a root of f. Denote the conjugates of α by α_j for $1 \le j \le d$. Given $\beta = \beta(\alpha) \in \mathbb{Q}(\alpha)$, define its *norm*

$$N(\beta) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta) = \prod_{j=1}^{d} \beta(\alpha_j)$$

to be the product of all algebraic conjugates of β. This norm is a rational number. We let $\hat{f}(X) = c_d^{d-1} f(X/c_d)$ denote the monic polynomial with root $\hat{\alpha} = c_d\alpha$ and conjugates $\hat{\alpha}_j = c_d\alpha_j$ for $1 \le j \le d$.

Let n be a composite integer which is not a prime power. Let $\mathbb{Q}_n$ denote the ring of rational numbers with denominator coprime to n and let $\mathbb{Q}_n^*$ denote the elements of $\mathbb{Q}_n$ whose numerator is also coprime to n. The simplest form of the number field sieve (NFS) [2] attempts to factor n by working in some $\mathbb{Q}(\alpha)$ where $\gcd(c_d, n) = 1$; The NFS also requires an $m \in \mathbb{Q}_n$ such that $f(m) \equiv 0 \pmod{n}$ and $f'(m) \in \mathbb{Q}_n^*$. The NFS finds several integer pairs $\{(a_i, b_i)\}$ and a finite nonempty set S such that

$$\prod_{i \in S}(a_i - b_i\alpha) \qquad \text{and} \qquad \prod_{i \in S}(a_i - b_i m) \tag{1.1}$$

are squares (or believed to be squares) in $\mathbb{Q}(\alpha)$ and in $\mathbb{Q}$ respectively, and where $a_i - b_i m \in \mathbb{Q}_n^*$ for all i. Let $\phi : \mathbb{Q}_n[\alpha] \to \mathbb{Z}/n\mathbb{Z}$ denote the natural ring homomorphism induced by $\phi(\alpha) \equiv m \pmod{n}$. Then

$$\phi\left(\prod_{i \in S}(a_i - b_i\alpha)\right) = \prod_{i \in S}\phi(a_i - b_i\alpha) \equiv \prod_{i \in S}(a_i - b_i m) \pmod{n}.$$

We can rewrite this as

$$\left[\phi\left(\sqrt{\prod_{i \in S}(a_i - b_i\alpha)}\right)\right]^2 \equiv \left[\sqrt{\prod_{i \in S}(a_i - b_i m)}\right]^2 \pmod{n} \tag{1.2}$$

after extracting the square roots in (1.1). Equation (1.2) has the form $x^2 \equiv y^2 \pmod{n}$ where $x, y \in \mathbb{Q}_n$; if we are lucky, then the numerator of $\gcd(x - y, n)$ will be a nontrivial factor of n.

The NFS does not specify how to evaluate the square roots in (1.2) (or these square roots modulo n). The square root of the rational number $\prod_{i\in S}(a_i - b_i m)$ can be found quickly using the known prime factorizations of $a_i - b_i m$. Extracting a square root of $\prod_{i\in S}(a_i - b_i\alpha)$ without explicitly evaluating the product (but using the factorizations of the $N(a_i - b_i\alpha)$) is the subject of this paper.

2. Existing methods

If α is an algebraic integer and the ring $\mathbb{Z}[\alpha]$ is a unique factorization domain with known units, then each $a_i - b_i\alpha$ can be factored completely into primes and units, after which the problem is straightforward. Early implementations [7] of the NFS made these assumptions, but modern implementations require algorithms which work in arbitrary number fields.

Buhler et al [2, §9] work with the monic polynomial $\hat{f}$. If

$$\gamma(\alpha) = \prod_{i\in S}(a_i - b_i\alpha) = \frac{\prod_{i\in S}(c_d a_i - b_i\hat{\alpha})}{c_d^{|S|}} \tag{2.1}$$

is a square in $\mathbb{Q}(\alpha) = \mathbb{Q}(\hat{\alpha})$ and if all a_i, $b_i \in \mathbb{Z}$, then $c_d^{2\lceil |S|/2\rceil}\hat{f}'(\hat{\alpha})^2\gamma(\alpha)$ is a square in $\mathbb{Z}[\hat{\alpha}]$, where $\hat{f}'$ denotes the formal derivative of $\hat{f}$. Expand the polynomial $\hat{f}'(\hat{\alpha})^2\gamma(\alpha)$ in terms of $\hat{\alpha}$ and reduce it modulo $\hat{f}$ until the result has degree at most $d-1$ in $\hat{\alpha}$. Then use existing methods (q–adic or other) to factor $X^2 - c_d^{2\lceil |S|/2\rceil}\hat{f}'(\hat{\alpha})^2\gamma(\alpha)$ over $\mathbb{Q}(\hat{\alpha})$. If the latter polynomial is irreducible, then $\gamma(\hat{\alpha})$ is not a square.

This works well when the cardinality $|S|$ is small. But when applied to the NFS, the number of terms $|S|$ often exceeds 10^5, and the coefficients of $\gamma(\alpha)$ may have over 10^6 decimal digits even if f is monic. Computing these gigantic coefficients explicitly can dominate the cost of the NFS.

If f has odd degree d, Couveignes [3] observes that the square root of $\hat{f}'(\hat{\alpha})^2\gamma(\alpha)$ is uniquely determined by specifying its norm. Since the prime factorization of $N(\gamma(\alpha))$ is known, the integer

$$N\left(c_d^{\lceil |S|/2\rceil}\sqrt{\hat{f}'(\hat{\alpha})^2\gamma(\alpha)}\right) = |c_d|^{d\lceil |S|/2\rceil}\, N(\hat{f}'(\hat{\alpha}))\,\sqrt{N(\gamma(\alpha))}$$

can be efficiently computed modulo any prime q. If we further require that q be inert (i.e., that $f(X)$ be irreducible modulo q), then $c_d^{\lceil |S|/2\rceil}\hat{f}'(\hat{\alpha})\sqrt{\gamma(\alpha)}$ mod q can be computed after expanding $\gamma(\alpha)$ mod q. When this is done for enough q, the Chinese Remainder Theorem uniquely determines the coefficients of $c_d^{\lceil |S|/2\rceil}\hat{f}'(\hat{\alpha})\sqrt{\gamma(\alpha)} \in \mathbb{Z}[\hat{\alpha}]$.

Then these coefficients can be reduced modulo n. Bernstein and Lenstra [1] used this while factoring the 145-digit number $(2^{488}+1)/257$.

If all q are single precision, then the number of different q used by Couveignes's algorithm grows linearly with the size of the coefficients of $\sqrt{\gamma}$, and the work to get each $\sqrt{\gamma} \bmod q$ grows linearly with the number $|S|$ of terms in (2.1). So the time for the algorithm grows at least quadratically with the size $|S|$. This can be improved to $\mathbb{O}(M(|S|) \log |S|)$, where $M(|S|)$ is the time required to multiply two $|S|$–bit integers, by using a single $|S|$–bit modulus and fast multiplication algorithms. Couveignes's algorithm fails when the degree d is even. The algorithm also fails if no inert prime exists (a rare problem which occurs only for certain Galois groups). We present an algorithm whose time is linear in $|S|$ (ignoring the implicit growth of a_i and b_i as $|S| \to \infty$) and which works for all values of d.

3. Generators for ideals

We review some material about fractional ideals in number fields. For background and justifications see standard texts, such as [4, pp. 16ff], [5, pp. 18ff], [8, pp. 264ff].

Denote the set of algebraic integers in $\mathbb{Q}(\alpha) = \mathbb{Q}(\hat{\alpha})$ by $\mathbb{O}_\alpha = \mathbb{O}_{\hat{\alpha}}$. In particular, $\hat{\alpha} \in \mathbb{O}_\alpha$.

A *fractional ideal* of $\mathbb{O}_\alpha$ is a subset $I \subseteq \mathbb{Q}(\alpha)$ such that

(1) There exists $r \in \mathbb{Q}(\alpha)$ such that $I \subseteq r\mathbb{O}_\alpha$;
(2) $I \neq \emptyset$ and $I \neq \{0\}$;
(3) I is closed under addition;
(4) I is closed under multiplication by elements of $\mathbb{O}_\alpha$.

If equality holds in (1), then I is said to be a *principal ideal* with generator r; this ideal is sometimes written (r). More generally, if $r_1, r_2, \cdots, r_k \in \mathbb{Q}(\alpha)$, where not all r_i are zero, then $(r_1, r_2, \cdots, r_k)$ denotes the smallest subset of $\mathbb{Q}(\alpha)$ containing all r_i and satisfying (3) and (4).

If I_1 and I_2 are fractional ideals, then their product $I_1 I_2$ is the smallest subset of $\mathbb{Q}(\alpha)$ which is closed under addition and which contains all products $i_1 i_2$ where $i_1 \in I_1$ and $i_2 \in I_2$.

A fractional ideal I of $\mathbb{O}_\alpha$ is said to be an *integral ideal* if $I \subseteq \mathbb{O}_\alpha$ (i.e., if $r = 1$ works in (1)).

A *prime ideal* is an integral ideal I such that if I_1 and I_2 are integral ideals with $I_1 I_2 \subseteq I$, then $I_1 \subseteq I$ or $I_2 \subseteq I$.

Theorem 3.1. *The fractional ideals of $\mathbb{O}_\alpha$ form an abelian group under multiplication, with identity $(1) = \mathbb{O}_\alpha$. Any fractional ideal I can* *be uniquely expressed as a product*

$$I = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdot \cdots \cdot \mathfrak{P}_k^{e_k}, \tag{3.2}$$

where the $\mathfrak{P}_i$*'s are distinct prime ideals and* $e_i \in \mathbb{Z}$.

Definition 3.3. *If* I *is a fractional ideal of* $\mathbb{O}_\alpha$*, then its* norm $N(I)$ *is the largest positive rational* q *such that* $N(r)/q \in \mathbb{Z}$ *for all* $r \in I$.

Definition 3.4. *Let* I *be a fractional ideal of* $\mathbb{O}_\alpha$*, with factorization* (3.2). *Define the* numerator *and* denominator *of* I *to be* $\operatorname{numer}(I)$ *and* $\operatorname{denom}(I)$ *respectively where*

$$\begin{aligned} \operatorname{numer}(I) &= \mathfrak{P}_1^{\max(e_1,0)} \cdot \mathfrak{P}_2^{\max(e_2,0)} \cdot \cdots \cdot \mathfrak{P}_k^{\max(e_k,0)}, \\ \operatorname{denom}(I) &= \mathfrak{P}_1^{\max(-e_1,0)} \cdot \mathfrak{P}_2^{\max(-e_2,0)} \cdot \cdots \cdot \mathfrak{P}_k^{\max(-e_k,0)}. \end{aligned}$$

Equivalently, $\operatorname{numer}(I) = I \cap \mathbb{O}_\alpha$ and $\operatorname{denom}(I) = I^{-1} \cap \mathbb{O}_\alpha$.

Theorem 3.5. *If* I *is a fractional ideal of* $\mathbb{O}_\alpha$*, then* $\operatorname{numer}(I)$ *and* $\operatorname{denom}(I)$ *are integral ideals. Also* $I = \operatorname{numer}(I)/\operatorname{denom}(I)$ *and* $N(I) = N(\operatorname{numer}(I))/N(\operatorname{denom}(I))$.

Lemma 3.6. *Let* $f(X) = \sum_{j=0}^{d} c_j X^j$ *be a polynomial with integer coefficients and root* α*. If* $0 \le k \le d$ *and* $\beta = \sum_{j=0}^{k} c_{d-k+j}\alpha^j$*, then* β *is an algebraic integer.*

Proof (by Joe Buhler). An element β of a number field K is an algebraic integer if there is a free module M of dimension $[K : \mathbb{Q}]$ such that $\beta M \subseteq M$. It is readily checked that $M = \langle 1, \alpha, \cdots, \alpha^{d-1}\rangle$ satisfies this condition, since

$$\begin{aligned} \alpha^\ell \beta &= \sum_{j=0}^{k} c_{d-k+j}\alpha^{\ell+j} && (0 \le \ell < d-k), \\ \alpha^{d-k+\ell}\beta &= \sum_{j=0}^{k} c_{d-k+j}\alpha^{d-k+\ell+j} = \sum_{j=d-k}^{d} c_j \alpha^{\ell+j} \\ &= -\sum_{j=0}^{d-k-1} c_j \alpha^{\ell+j} && (0 \le \ell < k). \quad \blacksquare \end{aligned}$$

Corollary 3.7. *Under the conditions of Lemma 3.6, if*

$$J = (c_d,\ c_d\alpha + c_{d-1},\ c_d\alpha^2 + c_{d-1}\alpha + c_{d-2},\ \cdots,\ c_d\alpha^{d-1} + c_{d-1}\alpha^{d-2} + \cdots + c_1), \tag{3.8}$$

and $\gcd(c_0, c_1, \cdots, c_d) = 1$*, then* $(1, \alpha)J = (1)$.

Proof.

$$\alpha J = (c_d\alpha,\ c_d\alpha^2 + c_{d-1}\alpha,\ c_d\alpha^2 + c_{d-1}\alpha + c_{d_2},\ \cdots,\ c_d\alpha^d + c_{d-1}\alpha^{d-1} + \cdots + c_1\alpha).$$

By Lemma 3.6, J and αJ contain only algebraic integers, so $(1,\ \alpha)J \subseteq (1)$. On the other hand

$$\begin{aligned} c_j &= \left(c_d\alpha^{d-j} + c_{d-1}\alpha^{d-j-1} + \cdots + c_j\right) \\ &\quad - \left(c_d\alpha^{d-j-1} + c_{d-1}\alpha^{d-j-2} + \cdots + c_{j+1}\right)\alpha \\ &\in J - \alpha J \subseteq (1,\ \alpha)J \end{aligned}$$

for all j. Since the c_j are assumed to be relatively prime, $1 \in (1,\ \alpha)J$. ∎

Corollary 3.9. *If J is defined by* (3.8)*, then* (i) $\operatorname{numer}((\alpha)) = \alpha J$*,* (ii) $\operatorname{denom}((\alpha)) = J$*, and* (iii) $N(J) = |c_d|$*.*

Proof. As in the last proof, both J and αJ are integral ideals. That proof showed that these are relatively prime. This proves (i) and (ii).

For (iii), HELP! Certainly $N(1) = 1$ and $N(\alpha) = (-1)^d c_0/c_d$, so $N((1,\ \alpha))$ divides $\gcd(c_0,\ c_d)/c_d$, implying $c_d/\gcd(c_0,\ c_d)$ divides $N(J)$. ∎

4. Lattice basis reduction

Lovász et al [6, Section 1] give a polynomial-time algorithm for constructing a basis of short vectors from an arbitrary basis. Specifically, given a basis $\{\mathbf{b}_j\}_{j=1}^d$ of a lattice, define its Gram-Schmidt orthogonalization $\{\mathbf{b}_j^*\}_{j=1}^d$ by

$$\mathbf{b}_j^* = \mathbf{b}_j - \sum_{i=1}^{j-1} \frac{\mathbf{b}_j \cdot \mathbf{b}_i^*}{\|\mathbf{b}_i^*\|^2}\mathbf{b}_i^*$$

for $1 \le j \le d$, where $|\cdot|$ denotes the Euclidean dot product. The $\mathbf{b}_j^*$ have rational rather than integer coefficients. The given basis is said to be *LLL–reduced* if

$$|\mathbf{b}_j \cdot \mathbf{b}_i^*| \le \|\mathbf{b}_i^*\|^2/2 \qquad (1 \le i < j \le d) \tag{4.1}$$

and

$$\left\|\mathbf{b}_j^* + \frac{\mathbf{b}_j \cdot \mathbf{b}_{j-1}^*}{\|\mathbf{b}_{j-1}^*\|^2}\mathbf{b}_{j-1}^*\right\|^2 \ge \frac{3}{4}\|\mathbf{b}_{j-1}^*\|^2 \qquad (1 < j \le d).$$

The authors show, in (1.7) to (1.9) of [6],

$$\|\mathbf{b}_j\|^2 \le 2^{i-1}\|\mathbf{b}_i^*\|^2 \qquad (1 \le j \le i \le d), \tag{4.2}$$

$$\prod_{j=1}^{d} \|\mathbf{b}_j\| \le 2^{d(d-1)/4}\det(L), \tag{4.3}$$

$$\|\mathbf{b}_1\| \le 2^{(d-1)/4}\det(L)^{1/d}, \tag{4.4}$$

in any LLL–reduced basis. Here $\det(L)$ denotes the determinant of the sublattice. The article gives a polynomial-time algorithm to obtain an LLL–reduced basis from a given basis; we term that process *LLL reduction*.

The next lemma will be used in the proof of Proposition 5.15.

Lemma 4.5. *Let $\{\mathbf{b}_j\}_{j=1}^d$ be an LLL–reduced basis for a lattice L. Suppose $\mathbf{u} = \sum_{j=1}^d a_j\mathbf{b}_j$ where $a_j \in \mathbb{R}$. Then, for $1 \le j \le d$,*

$$|a_j|^2\,\|\mathbf{b}_j\|^2 \le 2^{j-1}\|\mathbf{u}\|^2\frac{(9/2)^{d-j}+6}{7}.$$

Proof. Let $\{\mathbf{b}_j^*\}_{j=1}^d$ be the corresponding orthogonal basis. Write

$$\mathbf{u} = \sum_{j=1}^{d} a_j\mathbf{b}_j = \sum_{j=1}^{d} a_j^*\mathbf{b}_j^*, \tag{4.6}$$

where $a_j^* \in \mathbb{R}$. Since $\{\mathbf{b}_j^*\}$ is orthogonal, $\|\mathbf{u}\|^2 = \sum_{j=1}^d |a_j^*|^2\|\mathbf{b}_j^*\|^2$.

Take the dot product of (4.6) with $\mathbf{b}_j^*$. Use orthogonality and (4.1) to derive

$$a_j^*\,\|\mathbf{b}_j^*\|^2 = \sum_{i=1}^{d}(a_i\mathbf{b}_i\cdot\mathbf{b}_j^*) = \sum_{i=j}^{d} a_i(\mathbf{b}_i\cdot\mathbf{b}_j^*) = a_j\|\mathbf{b}_j^*\|^2 + \sum_{i=j+1}^{d} a_i(\mathbf{b}_i\cdot\mathbf{b}_j^*),$$

$$a_j = a_j^* - \sum_{i=j+1}^{d} a_i\frac{\mathbf{b}_i\cdot\mathbf{b}_j^*}{\|\mathbf{b}_j^*\|^2},$$

$$|a_j| \le |a_j^*| + \frac{1}{2}\sum_{i=j+1}^{d}|a_i|.$$

By induction on $d-j$,

$$\sum_{i=j}^{d}|a_i| \le \sum_{i=j}^{d}(3/2)^{i-j}|a_i^*| \qquad (1 \le j \le d),$$

$$|a_j| \le |a_j^*| + \frac{1}{3}\sum_{i=j+1}^{d}(3/2)^{i-j}|a_i^*| \qquad (1 \le j \le d).$$

Property (4.2) says $\|\mathbf{b}_j\| \le 2^{(i-1)/2}\|\mathbf{b}_i^*\|$ for $j \le i \le d$. Therefore

$$\begin{aligned}|a_j|\,\|\mathbf{b}_j\| &\le 2^{(j-1)/2}|a_j^*|\,\|\mathbf{b}_j^*\| + \frac{1}{3}\sum_{i=j+1}^{d} 2^{(i-1)/2}(3/2)^{i-j}|a_i^*|\,\|\mathbf{b}_j^*\| \\ &= 2^{(j-1)/2}\left(|a_j^*|\,\|\mathbf{b}_j^*\| + \frac{1}{3}\sum_{i=j+1}^{d}(9/2)^{(i-j)/2}|a_i^*|\,\|\mathbf{b}_j^*\|\right).\end{aligned}$$

By Cauchy-Schwarz,

$$\begin{aligned}|a_j|^2\,\|\mathbf{b}_j\|^2 &\le 2^{j-1}\left(\sum_{i=j}^{d}|a_i^*|^2\|\mathbf{b}_i^*\|^2\right)\left(1+\frac{1}{3^2}\left((9/2)+\cdots+(9/2)^{d-j}\right)\right) \\ &\le 2^{j-1}\|\mathbf{u}\|^2\left(1+\frac{1}{9}\,\frac{9}{2}\,\frac{(9/2)^{d-j}-1}{9/2-1}\right) \\ &= 2^{j-1}\|\mathbf{u}\|^2\frac{(9/2)^{d-j}+6}{7}. \quad \blacksquare\end{aligned}$$

5. Square roots via successive approximations

We generalize (2.1) to allow

$$\gamma = \gamma(\alpha) = \prod_{i\in S} g_i(\alpha), \tag{5.1}$$

where $g_i \in \mathbb{Q}(\alpha)^*$. In the present application $g_i(\alpha) = a_i - b_i\alpha$. We assume that the prime factorization of each $N(g_i(\alpha))$ is known.

Let α have r real conjugates and $2s$ complex conjugates, where $d = r + 2s$. Number them so that $\alpha_j \in \mathbb{R}$ for $1 \le j \le r$ and $\alpha_{j+s} = \overline{\alpha_j}$ for $r < j \le r+s$. Choose an integral basis

$$O = \{o_1, o_2, \cdots, o_d\} \tag{5.2}$$

for $\mathbb{O}_\alpha$. Also select a set of primes Q, which will be used for Chinese remaindering. The primes in Q should not divide any of the norms $N(g_i(\alpha))$. We will say more about O and Q in TBD.

Define $\gamma_1 = \gamma$. Initialize $\ell = 1$. If $\ell \ge 1$, then step ℓ constructs $\delta_\ell = \delta_\ell(\alpha)$ from γ_ℓ such that $\gamma_{\ell+1}$ is in some sense "smaller" than γ_ℓ, where

$$\gamma_{\ell+1} = \gamma_\ell\delta_\ell^{-2s_\ell}, \qquad s_\ell \in \{\pm 1\}.$$

The identity

$$\gamma(\alpha) = \gamma_\ell(\alpha)\left[\prod_{k=1}^{\ell-1}\delta_k(\alpha)^{s_k}\right]^2. \tag{5.3}$$

will hold for $\ell \geq 1$. Eventually some γ_ℓ will be sufficiently small that its coefficients can be determined explicitly (using the Chinese Remainder Theorem) and a square root constructed using another method.

At the start of step ℓ, we will know the following about $\gamma_\ell = \gamma_\ell(\alpha)$:

- Approximations to the embeddings $|\gamma_\ell(\alpha_j)|$ for $1 \leq j \leq d$.
- The coefficients of $\gamma_\ell(\alpha)$ (as a polynomial of degree at most $d-1$ in α) modulo each $q \in Q$.
- The prime ideal factorization of the remaining fractional ideal $(\gamma_\ell(\alpha))\left(H_\ell^-/H_\ell^+\right)^2$. Here H_ℓ^+ and H_ℓ^- are known integral ideals of small norm. All exponents will be even.

For $\ell = 1$, these approximations are found using the defining equation (5.1) for $\gamma_1 = \gamma$. We set $H_1^+ = H_1^- = (1)$ (unit ideal).

Remark 5.4. *Use logarithms, to prevent floating point exponent overflow. Although crude estimates of $|\gamma_\ell(\alpha_j)|$ (say within 1%) will suffice, double precision arithmetic is suggested, to reduce round-off accumulation in the product* (5.1).

Remark 5.5. *If J is defined by* (3.8)*, then $(a - b\alpha)J$ is an integral ideal whenever a and b are integers, since J and αJ are integral ideals. For the present problem* (2.1)*, one can accumulate the exponents of J and of the prime ideals dividing $(a-b\alpha)J$ (i.e., can treat J as an extra prime ideal). By Corollary 3.7, the latter ideal has norm*

$$N(J)N(a - b\alpha) = \left|\sum_{j=0}^{d} c_j a^{d-j} b^j\right|.$$

Remark 5.6. *This initialization (i.e., approximating γ_1) takes about half of the running time when $|S|$ is large, if most prime ideals have small exponents in $\gamma(\alpha)$ as suggested in §8. There are many opportunities for parallelism while expanding* (5.1).

At the start of step ℓ where $\ell \geq 1$, we will have a product formula for $\gamma_\ell(\alpha)$. obtained from (5.3). Choose $s_\ell = +1$ to try to simplify the numerator of γ_ℓ, or $s^\ell = -1$ to try to simplify the denominator of γ_ℓ.

Assuming $s_\ell = +1$, the algorithm selects an ideal I_ℓ divisible by H_ℓ^+ and by several of the prime ideals known to divide the numerator of $(\sqrt{\gamma_\ell})/H_\ell^+$. Then it selects $\delta_\ell \in I_\ell$ such that $N(\delta_\ell)$ is small but nonzero. This δ_ℓ is an approximation to $\sqrt{\gamma_\ell}$. Although (δ_ℓ) may be divisible by other prime ideals as well, we can bound the norm of these additional ideals in terms of the coefficients of f (see Theorem **??**). If we make $N(I_\ell)$ sufficiently large, then the product of norms of the numerator and denominator of $(\gamma_\ell/\delta_\ell^2)$ will be smaller than the corresponding product for γ_ℓ. Once this product becomes sufficiently small, subsequent γ_ℓ

will be algebraic integers (i.e., denominator norm 1). The algorithm also attempts to reduce the unit contribution, by choosing δ_ℓ so as to minimize the absolute values $\delta_\ell(\alpha_j)/|\gamma_\ell(\alpha_j)|^{1/2}$ of the embeddings, for $1 \le j \le d$. When these are also small, the coefficients of $\gamma(\alpha)$ can be computed from their values modulo the primes in Q.

More precisely, select a bound $L_{\max}$ (probably independent of ℓ) representing the largest determinant which the LLL–reduction algorithm can accept and still perform well. Assuming $s_\ell = +1$, choose an ideal I_ℓ divisible by H_ℓ^+ and dividing numer$(\sqrt{\gamma_\ell})$, with $N(I_\ell) < L_{\max}$ (but as large as convenient subject to this bound).

Construct a basis for I_ℓ. Apply LLL reduction to find $\mathbf{v} \in I_\ell$ with small but nonzero Euclidean norm relative to the integral basis O in (5.2) for $\mathbb{O}_\alpha$. The lattice for I_ℓ has determinant $N(I_\ell)$. Equation (4.4) gives

$$\|\mathbf{v}\| \le 2^{(d-1)/4} N(I_\ell)^{1/d}.$$

The power basis $\{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{d-1}\}$ has determinant at least $|c_d|^{1-d}$ relative to O, by Lemma 3.6. By the determinantal formula for the resultant, if $\mathbf{v} = \sum_{i=0}^{d-1} v_i\alpha^i$, then

$$c_d^{d-1} N(\mathbf{v}) = \pm \begin{vmatrix} v_{d-1} & v_{d-2} & v_{d-3} & \dots & v_0 & 0 & \dots & 0 \\ 0 & v_{d-1} & v_{d-2} & \dots & v_1 & v_0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \dots & 0 \\ 0 & 0 & 0 & 0 & v_{d-1} & v_{d-2} & \dots & v_0 \\ c_d & c_{d-1} & c_{d-2} & \dots & c_1 & c_0 & & 0 \\ 0 & c_d & c_{d-1} & \dots & c_2 & c_1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \dots & 0 \\ 0 & 0 & \dots & c_d & c_{d-1} & c_{d-2} & \dots & c_0 \end{vmatrix},$$

where the matrix is $(2d-1) \times (2d-1)$. Hadamard's inequality gives TBD I had a comment "WRONG" here – what did I mean?

$$\begin{aligned} \left| c_d^{d-1} N(\mathbf{v}) \right| &\le \left[\sum_{i=0}^{d-1} v_i^2 \right]^{d/2} \left[\sum_{j=0}^{d} c_j^2 \right]^{(d-1)/2} \\ &= \|\mathbf{v}\|^d \, \|f\|^{d-1} \le 2^{d(d-1)/4} |c_d|^{d-1} N(I_\ell) \, \|f\|^{d-1}, \end{aligned}$$

where $\|f\| = \left(\sum_{j=0}^{d} c_j^2\right)^{1/2}$. Hence

$$\left| \frac{N(\mathbf{v})}{N(I_\ell)} \right| \le 2^{d(d-1)/4} \, \|f\|^{d-1}. \tag{5.7}$$

The left side of (5.7) is an integer since $\mathbf{v} \in I_\ell$ by construction. More importantly, the right side of (5.7) (call it C) is independent of $N(I)$.

If we define

$$\gamma_{\ell+1} = \gamma_\ell/\mathbf{v}^2, \qquad H_{\ell+1}^{+} = (1), \qquad H_{\ell+1}^{-} = \frac{(\mathbf{v})}{I_\ell} H_\ell^{-}, \tag{5.8}$$

then

$$(\sqrt{\gamma_{\ell+1}}) = \frac{(\sqrt{\gamma_\ell})}{(\mathbf{v})} = \frac{(\sqrt{\gamma_\ell})/I_\ell}{H_{\ell+1}^{-}/H_\ell^{-}}.$$

The numerator norm of $(\sqrt{\gamma_{\ell+1}})$ has been reduced by a factor of $N(I_\ell) \approx L_{\max}$, while its denominator has increased by at most a factor of $N(H_{\ell+1}^{-}/H_\ell^{-}) \leq C$. If $L_{\max} \gg C$, then repeated application of this construction will reduce the product of the numerator and denominator norms of $\sqrt{\gamma}$ until both are below C. One additional pair of iterations (in which I is the entire remaining numerator or entire remaining denominator) will replace γ by an algebraic integer of norm at most C^2; its square root can be completed by other means.

The alert reader may sense a problem. If the coefficients of γ_ℓ are small, then we can bound $N(\gamma_\ell)$, but the converse is false (e.g., γ_ℓ might be a power of a unit, with norm 1 and huge coefficients).

One way to bound the coefficients of γ_ℓ is to bound the embeddings $|\gamma_\ell(\alpha_j)|$ for $1 \leq j \leq d$. By Lagrange's interpolation formula, if h is a polynomial of degree at most $d-1$, then

$$h(X) = \sum_{j=1}^{d} h(\alpha_j) \frac{\prod_{k\neq j}(X-\alpha_k)}{\prod_{k\neq j}(\alpha_j-\alpha_k)} = \sum_{j=1}^{d} h(\alpha_j) \frac{f(X)}{(X-\alpha_j)\, f'(\alpha_j)}. \tag{5.9}$$

Write

$$\frac{f(X)}{(X-\alpha_j)\, f'(\alpha_j)} = \sum_{i=0}^{d-1} c_{ij} X^i.$$

Then

$$h(X) = \sum_{j=1}^{d} h(\alpha_j) \sum_{i=0}^{d-1} c_{ij} X^i = \sum_{i=0}^{d-1} X^i \sum_{j=1}^{d} h(\alpha_j) c_{ij}.$$

The c_{ij} can be estimated in terms of the roots of f. Then the triangle inequality bounds the coefficients of h in terms of the $|h(\alpha_j)|$.

One way to bound the embeddings when all α_j are real is to find a nonzero

$$\mathbf{v} = \mathbf{v}(\alpha) = \sum_{i=0}^{d-1} v_i \alpha^i \in I_\ell$$

such that $T\mathbf{v}$ is small, where T is the linear transformation such that

$$T\mathbf{v} = \left[v_0,\ v_1,\ \cdots,\ v_{d-1},\ c\frac{\mathbf{v}(\alpha_1)}{|\gamma_\ell(\alpha_1)|^{1/2}},\ \cdots,\ c\frac{\mathbf{v}(\alpha_d)}{|\gamma_\ell(\alpha_d)|^{1/2}} \right]^{\mathrm{T}}. \tag{5.10}$$

The constant $c > 0$ remains to be specified. Given an LLL–reduced basis $\{\mathbf{v}^{(j)}\}_{j=1}^{d}$ for I_ℓ, form a $2d \times d$ matrix with the corresponding $\{T\mathbf{v}^{(j)}\}_{j=1}^{d}$. If $\mathbf{v}^{(j)} = \sum_{i=0}^{d-1} v_i^{(j)} \alpha^j$, then the absolute value of the determinant of the image of the last d coordinates of $\{T\mathbf{v}^{(j)}\}_{j=1}^{d}$ is

$$\begin{aligned}
&\pm \left(\prod_{j=1}^{d} \frac{c}{|\gamma_\ell(\alpha_j)|^{1/2}} \right) \begin{vmatrix} \mathbf{v}^{(1)}(\alpha_1) & \mathbf{v}^{(1)}(\alpha_2) & \dots & \mathbf{v}^{(1)}(\alpha_d) \\ \mathbf{v}^{(2)}(\alpha_1) & \mathbf{v}^{(2)}(\alpha_2) & \dots & \mathbf{v}^{(2)}(\alpha_d) \\ \vdots & \vdots & & \vdots \\ \mathbf{v}^{(d)}(\alpha_1) & \mathbf{v}^{(d)}(\alpha_2) & \dots & \mathbf{v}^{(d)}(\alpha_d) \end{vmatrix} \\
&= pm \frac{c^d}{|N(\gamma_\ell)|^{1/2}} \begin{vmatrix} v_0^{(1)} & v_1^{(1)} & \dots & v_{d-1}^{(1)} \\ v_0^{(2)} & v_1^{(2)} & \dots & v_{d-1}^{(2)} \\ \vdots & \vdots & & \vdots \\ v_0^{(d)} & v_1^{(d)} & \dots & v_{d-1}^{(d)} \end{vmatrix} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_d \\ \vdots & \vdots & & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \dots & \alpha_d^{d-1} \end{vmatrix} \\
&= \pm \frac{c^d}{|N(\gamma_\ell)|^{1/2}} \det\left(\{\mathbf{v}^{(j)}\}_{j=1}^{d}\right) \prod_{1 \le i < j \le d} (\alpha_j - \alpha_i) \\
&\le \frac{c^d}{|N(\gamma_\ell)|^{1/2}} |c_d|^{d-1} N(I_\ell)\, |\mathrm{Disc}(f/c_d)|^{1/2}.
\end{aligned}$$

If we choose c so that

$$c^d = \frac{L_{\max}}{N(I_\ell)} \frac{|N(\gamma_\ell)|^{1/2}}{|c_d|^{d-1}|\mathrm{Disc}(f/c_d)|^{1/2}}, \tag{5.11}$$

then the determinant of the last d coordinates is at most $\pm L_{\max}$, which is where the LLL–reduction algorithm supposedly performs best.

TBD — Give numerical result about how close to 1.0 the new $|\gamma_{\ell+1}(\alpha_j)|$ are.

Remark 5.12. *Theoretically one could use a single LLL reduction rather than two reductions, since T is linear. But the last d coordinates of $T\mathbf{v}$ are real rather than integer, and one prefers integer arithmetic whenever possible. It will probably suffice to begin with an LLL–reduced basis for the $\{\mathbf{v}^{(j)}\}$, and construct the corresponding $\{T\mathbf{v}^{(j)}\}$ while rounding all coordinates to integers. I anticipate that the optimal $T\mathbf{v}$ will usually be a linear combination of the $\{T\mathbf{v}^{(j)}\}$ with small coefficients, so there will be little additional round-off accumulation during the second LLL reduction. But this awaits being tested in practice. If* *one is in doubt, he may reapply T to the first coordinates of the new basis, to check the last coordinates thereof.*

Remark 5.13. *If f has complex roots, replace any complex conjugate pairs z and $\overline{z}$ of coordinates in the definition of T by the corresponding real and imaginary parts of $\sqrt{2}z$. This leaves the absolute value of the determinant unchanged, but makes all entries real. Since*

$$|z|^2 + |\overline{z}|^2 = 2|z|^2 = \left|\sqrt{2}\Re(z)\right|^2 + \left|\sqrt{2}\Im(z)\right|^2$$

for all complex z, Proposition 5.15 (below) remains valid.

Remark 5.14. *If $s_\ell = -1$, then use γ_ℓ^{-1} rather than γ_ℓ in the definitions of T and c.*

Proposition 5.15. *There exists a computable constant $C = C(f)$ such that the second LLL reduction outputs a vector $\mathbf{u}$ with $N(\mathbf{u}) \leq CN(I_\ell)$, where C is independent of $N(I_\ell)$ and c.*

Proof (long). Define

$$\mu_j = \frac{cd \max(|\alpha_j|,\, 1)^{d-1}|c_d|^{1-1/d}}{|\gamma_\ell(\alpha_j)|^{1/2}} \tag{5.16}$$

for $1 \leq j \leq d$.

For $1 \leq i \leq d$, suppose m_i is an integer satisfying

$$|m_i| < \frac{MN(I_\ell)^{1/d}|c_d|^{1-1/d}}{\|\mathbf{v}^{(i)}\|}, \tag{5.17}$$

where M remains unspecified. The number of possible selections of $\{m_i\}_{i=1}^d$ in which all $m_i \geq 0$ is

$$\begin{aligned}\prod_{i=1}^{d}\left\lceil \frac{MN(I_\ell)^{1/d}|c_d|^{1-1/d}}{\|\mathbf{v}^{(i)}\|}\right\rceil &\geq \prod_{i=1}^{d}\frac{MN(I_\ell)^{1/d}|c_d|^{1-1/d}}{\|\mathbf{v}^{(i)}\|}\\ &= \frac{M^dN(I_\ell)|c_d|^{d-1}}{\prod_{i=1}^d\|\mathbf{v}^{(i)}\|} \geq \frac{M^d}{2^{d(d-1)/4}},\end{aligned}$$

where the last inequality comes from (4.3).

Define $\mathbf{w} = \sum_{i=1}^d m_i\mathbf{v}^{(i)}$. Write $\mathbf{w} = \sum_{i=0}^{d-1} w_i\alpha^i$. Then, by (5.17),

$$\left(\sum_{i=0}^{d-1} w_i^2\right)^{1/2} = \|\mathbf{w}\| \leq \sum_{i=1}^{d}|m_i|\,\|\mathbf{v}^{(i)}\| \leq dMN(I_\ell)^{1/d}|c_d|^{1-1/d}. \tag{5.18}$$

Consider $T\mathbf{w}$. Its first d coordinates are those of $\mathbf{w}$. If $1 \le j \le d$, then, by the Cauchy–Schwarz inequality and (5.18) and (5.16),

(5.19)
$$
\begin{aligned}
|(T\mathbf{w})_{d+j}| &= \frac{c}{|\gamma_\ell(\alpha_j)|^{1/2}} |\mathbf{w}(\alpha_j)| = \frac{c}{|\gamma_\ell(\alpha_j)|^{1/2}} \left| \sum_{i=0}^{d-1} w_i \alpha_j^i \right| \\
&\le \frac{c}{|\gamma_\ell(\alpha_j)|^{1/2}} \left(\sum_{i=0}^{d-1} w_i^2 \right)^{1/2} \left(\sum_{i=0}^{d-1} |\alpha_j|^{2i} \right)^{1/2} \\
&\le \frac{c}{|\gamma_\ell(\alpha_j)|^{1/2}} \left(dMN(I_\ell)^{1/d} |c_d|^{1-1/d} \right) \left(d \max(|\alpha_j|,\, 1)^{2d-2} \right)^{1/2} \\
&= \mu_j d^{1/2} MN(I_\ell)^{1/d}.
\end{aligned}
$$

Let $S = \{j : \mu_j > 1\}$. The set S does not depend on M. Given $\epsilon > 0$, choose M such that

$$(1+\epsilon) 2^{d(d-1)/4} \prod_{j \in S} 3\mu_j \ge M^d > 2^{d(d-1)/4} \prod_{j \in S} \lceil 2\mu_j \rceil .$$

By the pigeon-hole principle, there exist two distinct sequences $\{m_i'\}_{i=1}^d$ and $\{m_i''\}_{i=1}^d$ of nonnegative integers each satisfying (5.17) and where all corresponding

$$\left\lfloor \frac{|(T\mathbf{w})_{d+j}|}{d^{1/2} MN(I_\ell)^{1/d}} + \mu_j \right\rfloor$$

are identical in pairs, for $1 \le j \le d$. The differences $m_i = m_i' - m_i''$ satisfy (5.17), and the corresponding $\mathbf{w}$ satisfies

$$
\begin{aligned}
&|(T\mathbf{w})_{d+j}| \le d^{1/2} MN(I_\ell)^{1/d} && (j \in S) && \text{(by construction and linearity of } T\text{)}, \\
&|(T\mathbf{w})_{d+j}| \le \mu_j d^{1/2} MN(I_\ell)^{1/d} && (j \notin S) && \text{(by (5.19))}.
\end{aligned}
$$

This $\mathbf{w}$ therefore satisfies

(5.20)
$$\|T\mathbf{w}\|^2 \le \|\mathbf{w}\|^2 + dM^2 N(I_\ell)^{2/d} \bigl(|S| + \sum_{j \notin S} \mu_j^2\bigr) \le (d^2 + d^2) M^2 N(I_\ell)^{2/d}.$$

Suppose the second LLL reduction outputs a basis with shortest vector $T\mathbf{u}$ where $\mathbf{u} = \sum_{i=1}^d n_i \mathbf{v}^{(i)}$. By Lemma 4.5,

$$|n_i|^2 \|\mathbf{v}^{(i)}\|^2 \le 2^{i-1} \|\mathbf{u}\|^2 \frac{(9/2)^{d-i} + 6}{7}$$

for $1 \le i \le d$. By (1.11) in [6] and (5.20),

$$\|\mathbf{u}\|^2 \le \|T\mathbf{u}\|^2 \le 2^{d-1} \|T\mathbf{w}\|^2 \le 2^{d-1} (2d^2) M^2 N(I_\ell)^{2/d}. \tag{5.21}$$

Combining these, we find there exists $C_1 > 0$ dependent only on d such that

$$|n_i|\,\|\mathbf{v}^{(i)}\| < C_1 M N(I_\ell)^{1/d}$$

for all i.

By (5.19), with M replaced by $C_1 M$,

$$|(T\mathbf{u})_{d+j}| \le \mu_j d^{1/2} C_1 M N(I_\ell)^{1/d}.$$

If $S \neq \emptyset$, then, by the arithmetic-geometric mean inequality and (5.21),

$$\begin{aligned}\prod_{j\in S} |(T\mathbf{u})_{d+j}|^2 &\le \left(\frac{1}{|S|}\sum_{j\in S}|(T\mathbf{u})_{d+j}|^2\right)^{|S|}\\ &\le \frac{(\|T\mathbf{u}\|^2)^{|S|}}{|S|^{|S|}} \le \frac{\left(2^d d^2 M^2 N(I_\ell)^{2/d}\right)^{|S|}}{|S|^{|S|}}.\end{aligned}$$

This is also valid when $S = \emptyset$ if 0^0 is interpreted as 1. Therefore

$$\begin{aligned}&|N(\mathbf{u}(\alpha))|\\ &= \prod_{j=1}^{d} |\mathbf{u}(\alpha_j)| = \prod_{j=1}^{d} \frac{|\gamma_\ell(\alpha_j)|^{1/2}}{c}|(T\mathbf{u})_{d+j}|\\ &= M^d N(I_\ell)|c_d|^{d-1}\prod_{j=1}^{d} d\max(|\alpha_j|,\,1)^{d-1}\frac{|(T\mathbf{u})_{d+j}|}{\mu_j M N(I_\ell)^{1/d}} \qquad \text{(by (5.16))}\\ &= d^d N(I_\ell)|c_d|^{d-1}\frac{M^d}{\prod_{j\in S}\mu_j}\left(\prod_{j=1}^{d}\max(|\alpha_j|,\,1)\right)^{d-1}\\ &\qquad \left(\prod_{j\notin S}\frac{|(T\mathbf{u})_{d+j}|}{\mu_j M N(I_\ell)^{1/d}}\right)\frac{\prod_{j\in S}|(T\mathbf{u})_{d+j}|}{M^{|S|}N(I_\ell)^{|S|/d}}\\ &\le d^d N(I_\ell)|c_d|^{d-1}\left((1+\epsilon)2^{d(d-1)/4}\cdot 3^{|S|}\right)\\ &\qquad \left(\prod_{j=1}^{d}\max(|\alpha_j|,\,1)\right)^{d-1}\left(d^{1/2}C_1\right)^{d-|S|}\ \frac{(2^{d/2}d)^{|S|}}{|S|^{|S|/2}}\\ &\le C_2 N(I_\ell),\end{aligned}$$

where C_2 depends only on f (and d), since there are only finitely many choices for $|S|$. ■

6. Implementation remarks

Our present implementation uses version 1.39 of the PARI library [?] developed by Henri Cohen et al. Some PARI library functions used are:

- Compute polynomial roots $\hat{\alpha}_j$ to high precision;
- Computation of an integral basis;
- Construction of basis for selected ideal I_ℓ;
- LLL reductions;
- Computation of leftover ideals $H^+_{\ell+1}$ and $H^-_{\ell+1}$ in (5.8);
- Chinese remaindering;
- Factoring the final $X^2 - \gamma(\alpha)$ over $\mathbb{Q}(\hat{\alpha})$.

The integral basis computation uses the factorization of the discriminant of the polynomial. We factor the discriminant in another job, and notify PARI about any large primes dividing either the discriminant or c_d. This is done using **addprimestotable**, which was introduced in PARI 1.39 especially for this application.

Another new PARI 1.39 routine is **idealdivexact**. If I and I' are nonzero ideals, then PARI 1.38 routine **idealdiv** computes the quotient $I'' = I'/I$ as $I^{-1} * I'$. This computation was very slow when applied to the quotient $(\mathbf{v})/I_\ell$ in (5.8). Suppose I'' is known to be integral. Then we can compute $N(I'')$ as $N(I')/N(I)$. Let k be an integer dividing $\gcd(N(I'), N(I))$ but not $N(I'')$. Then $I' \cap (k) = I \cap (k)$ and

$$\frac{I' + (k)}{I + (k)} = \frac{I' \cdot (k)/(I' \cap (k))}{I \cdot (k)/(I \cap (k))} = \frac{I'}{I}. \tag{6.1}$$

All entries of the HNFs for $I' + (k)$ and $I + (k)$ will be divisible by k. They can be cancelled before calling **idealdiv** to divide $I' + (k)$ by $I + (k)$. TBD – Define HNF. When we do not know beforehand that I'' is integral, we can compute I'' as $\frac{I'/(I'+I)}{I/(I'+I)}$ if $N(I' + I)$ is large compared to $N(I)$.

Remark 6.2. *In practice $\gamma_\ell(\alpha) \equiv 1$ occurs frequently in practice, but this might not occur if $\mathbb{O}_\alpha$ has other small squares, such as if $\sqrt{2} \in \mathbb{Q}(\alpha)$, or if $\mathbb{Q}(\alpha)$ has complex roots of unity.*

Remark 6.3. *When evaluating a g_i (or δ_ℓ) at an α_j, direct application of Horner's rule for polynomial evaluation may cause excessive cancellation, if α_j is close to a root of $g_i(X)$. In this case $g_i(\alpha)$ should be rewritten in an algebraically equivalent form which is more amenable to accurate evaluation at $\alpha = \alpha_j$. As a check, after approximating one g_i at all roots α_j, verify that $\prod_j g_i(\alpha_j) = N(g_i(\alpha))$, where the right side* *is computed using exact arithmetic (there is little additional cost, since the factorization of the right side is used elsewhere in the algorithm).*

7. Example

Warning. The algorithm was revised after this section was written. The computations herein do not reflect those revisions.

While attempting to factor $n = 6913$ with $d = 3$, the NFS might select $m = 10$ and $f(X) = 7X^3 - X^2 + X + 3$. Then $f(m) = n$. Subsequently (i.e., after completing the sieving and linear algebra phases) one may suspect that both $\gamma(m)$ and $\gamma(\alpha)$ are perfect squares, where

$$\gamma(X) = (X-6)(X+1)(3X-2)(3X+2)(7X-15)(7X+2)(13X-5)(23X+15)(32X-5) \tag{7.1}$$

and α is a root of f. Indeed they are, because

$$\begin{aligned}\gamma(\alpha) &= \frac{-24129268236\alpha^2 + 77411935842\alpha + 60562982034}{7^4} \\ &= \left(\frac{20239\alpha^2 - 28982\alpha - 27537}{7}\right)^2, \\ \gamma(m) &= 2^{12} \cdot 3^4 \cdot 5^6 \cdot 7^4 \cdot 11^2 = 38808000^2.\end{aligned} \tag{7.2}$$

The congruence $3812^2 \equiv 5331^2$ factors n.

The real root of f is $\alpha_1 \approx -0.650$; the complex roots are $\alpha_2 \approx 0.397 + 0.708i$ and $\alpha_3 = \overline{\alpha_2}$.

The discriminant of f is $\operatorname{Disc}(f) = -2^2 \cdot 3 \cdot 5^2 \cdot 41 = -12300$, whereas $\operatorname{Disc}(f/c_d) = -12300/2401$.

If p is prime and $p \neq 7$ (so $p \nmid c_d$) and $f(q) \equiv 0 \pmod{p}$, denote $I_{p,q} = (p,\ 7\alpha - 7q)$. Also denote $J = (7,\ 7\alpha - 1,\ 7\alpha^2 - \alpha + 1)$. The ideal factorizations of the terms in $(\gamma(\alpha))$ are listed in Table 7.1.

Term	Norm	Ideal factorization
$\alpha - 6$	$-3^3 \cdot 5 \cdot 11/7$	$I_{3,0}^3\, I_{5,1}\, I_{11,6}/J$
$\alpha + 1$	$2 \cdot 3/7$	$I_{2,1}\, I_{3,2}/J$
$3\alpha - 2$	$-11 \cdot 13/7$	$I_{11,8}\, I_{13,5}/J$
$3\alpha + 2$	$5/7$	$I_{5,1}/J$
$7\alpha - 15$	$-2 \cdot 3^5 \cdot 7$	$I_{2,1}\, I_{3,0}^5\, J$
$7\alpha + 2$	-11^2	$I_{11,6}^2$
$13\alpha - 5$	$-2 \cdot 3 \cdot 11^3/7$	$I_{2,1}\, I_{3,2}\, I_{11,8}^3/J$
$23\alpha + 15$	$2 \cdot 3^2 \cdot 13/7$	$I_{2,1}\, I_{3,0}^2\, I_{13,5}/J$
$32\alpha - 5$	$-11 \cdot 97^2/7$	$I_{11,6}\, I_{97,82}^2/J$

Table 7.1. Example ideal factorizations

Use the product representation (7.1) of $\gamma_1(\alpha) = \gamma(\alpha)$ to derive

$$
\begin{aligned}
N(\gamma_1(\alpha)) &= \frac{2^4 \cdot 3^{12} \cdot 5^2 \cdot 11^8 \cdot 13^2 \cdot 97^2}{7^6}, \\
(\gamma_1(\alpha)) &= \frac{I_{2,1}^4\, I_{3,0}^{10}\, I_{3,2}^2\, I_{5,1}^2\, I_{11,6}^4\, I_{11,8}^4\, I_{13,5}^2\, I_{97,82}^2}{J^6}, \\
|\gamma_1(\alpha_1)| &\approx 306, \\
|\gamma_1(\alpha_2)| &= |\gamma_1(\alpha_3)| \approx 4.49 \cdot 10^7.
\end{aligned}
\tag{7.3}
$$

Suppose $L_{\max} = 10^5$. Observing $97 \cdot 13 \cdot 11 \cdot 5 = 69355 < L_{\max}$, we might choose $s_\ell = +1$, searching for δ_1 such that

$$
\begin{aligned}
\delta_1 J^2 &\subseteq I_{97,82}\, I_{13,5}\, I_{11,8}\, I_{5,1} = I_{97,82} \cap I_{13,5} \cap I_{11,8} \cap I_{5,1}, \\
\delta_1 &\in \frac{I_{97,82}}{J^2} \cap \frac{I_{13,5}}{J^2} \cap \frac{I_{11,8}}{J^2} \cap \frac{I_{5,1}}{J^2}.
\end{aligned}
$$

The four sublattices have triangular bases

$$
\begin{aligned}
\{97,\ \alpha - 82,\ \alpha^2 - 82^2\} &\quad \text{for} \quad I_{97,82}/J^2, \\
\{13,\ \alpha - 5,\ \alpha^2 - 5^2\} &\quad \text{for} \quad I_{13,5}/J^2, \\
\{11,\ \alpha - 8,\ \alpha^2 - 8^2\} &\quad \text{for} \quad I_{11,8}/J^2, \\
\{5,\ \alpha - 1,\ \alpha^2 - 1^2\} &\quad \text{for} \quad I_{5,1}/J^2.
\end{aligned}
$$

A triangular basis for the intersection is

$$\{69355,\ \alpha - 3671,\ \alpha^2 - 21371\}.$$

An LLL–reduced (but non-triangular) basis for the intersection is $\{\mathbf{v}_1,\ \mathbf{v}_2,\ \mathbf{v}_3\}$, where

$$\mathbf{v}_1 = 13\alpha^2 - 19\alpha - 9, \qquad \mathbf{v}_2 = 21\alpha^2 + 10\alpha - 16, \qquad \mathbf{v}_3 = -62\alpha^2 + 2\alpha - 85.$$

Use this to construct the matrix

$$
\begin{pmatrix}
-9 & -16 & -85 \\
-19 & 10 & 2 \\
13 & 21 & -62 \\
c\dfrac{\mathbf{v}_1(\alpha_1)}{|\gamma_1(\alpha_1)|^{1/2}} & c\dfrac{\mathbf{v}_2(\alpha_1)}{|\gamma_1(\alpha_1)|^{1/2}} & c\dfrac{\mathbf{v}_3(\alpha_1)}{|\gamma_1(\alpha_1)|^{1/2}} \\
c\sqrt{2}\dfrac{\Re(\mathbf{v}_1(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}} & c\sqrt{2}\dfrac{\Re(\mathbf{v}_2(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}} & c\sqrt{2}\dfrac{\Re(\mathbf{v}_3(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}} \\
c\sqrt{2}\dfrac{\Im(\mathbf{v}_1(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}} & c\sqrt{2}\dfrac{\Im(\mathbf{v}_2(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}} & c\sqrt{2}\dfrac{\Im(\mathbf{v}_3(\alpha_2))}{|\gamma_1(\alpha_2)|^{1/2}}
\end{pmatrix}
\approx
\begin{pmatrix}
-9 & -16 & -85 \\
-19 & 10 & 2 \\
13 & 21 & -62 \\
402 & -618 & -5109 \\
-4 & -3 & -11 \\
-1 & 3 & -6
\end{pmatrix},
\tag{7.4}
$$

where

$$c = \left(\frac{L_{\max}}{97 \cdot 13 \cdot 11 \cdot 5} \frac{|N(\gamma_1)|^{1/2}}{|\mathrm{Disc}(f/c_d)|^{1/2}} \right)^{1/3} \approx 794,$$

as in (5.11). The determinant of the bottom three rows of (7.4) is 105171, close to $L_{\max}$ (but inexact due to rounding while converting floating to integer).

Applying LLL reduction to the columns of (7.4) yields

(7.5)

$$\begin{pmatrix} 59 & -50 & -34 \\ 37 & -143 & -28 \\ -81 & -102 & 47 \\ 30 & -9 & 186 \\ 18 & -16 & -11 \\ -3 & -26 & 1 \end{pmatrix} = \begin{pmatrix} -9 & -16 & -85 \\ -19 & 10 & 2 \\ 13 & 21 & -62 \\ 402 & -618 & -5109 \\ -4 & -3 & -11 \\ -1 & 3 & -6 \end{pmatrix} \begin{pmatrix} -3 & 5 & 2 \\ -2 & -5 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

From the first column of (7.5), we select $\delta_1 = -81\alpha^2 + 37\alpha + 59$. Define $\gamma_2 = \gamma_1/\delta_1^2$. Use these definitions and (7.3) to compute

(7.6)

$$\begin{aligned} N(\delta_1) &= \frac{5^2 \cdot 11 \cdot 13 \cdot 97}{7^2}, & (\delta_1) &= \frac{I_{5,1}^2\, I_{11,8}\, I_{13,5}\, I_{97,82}}{J^2}, \\ N(\gamma_2) &= \frac{N(\gamma_1)}{N(\delta_1)^2} = \frac{2^4 \cdot 3^{12} \cdot 11^6}{5^2 \cdot 7^2}, & (\gamma_2) &= \frac{I_{2,1}^4\, I_{3,0}^{10} I_{3,2}^2\, I_{11,6}^4\, I_{11,8}^2}{I_{5,1}^2\, J^2}, \\ |\gamma_2(\alpha_1)| &\approx 697, & |\gamma_2(\alpha_2)| &= |\gamma_2(\alpha_3)| \approx 4200. \end{aligned}$$

We eliminated some ideals of combined norm 69355 in the numerator of $\sqrt{\gamma_1}$ in exchange for a new ideal of norm 5 in the denominator of $\sqrt{\gamma_2}$ (we also transferred a $J^2 = J^{d-1}$, but such will be transferred back if we ever have $s_\ell = -1$). We also brought $|\gamma(\alpha_1)|$, $|\gamma(\alpha_2)|$, and $|\gamma(\alpha_3)|$ closer numerically, thereby removing some of the unit contribution. In actuality

$$\gamma_2 = \frac{6240\alpha^2 + 15666\alpha + 11034}{5} = \left(\frac{7\alpha^2 + 166\alpha + 237}{5} \right)^2.$$

The coefficients of the numerator of γ_2 are 5 digits, down from 11 in (7.2).

The denominator of $J^2(\sqrt{\gamma_2})$ is smaller than that of $J^2/(\sqrt{\gamma_2})$, so we elect to focus on the numerator of γ_2 rather than its denominator, choosing $s_2 = +1$. Observing that $11^3 \cdot 3^3 \cdot 2 = 71874 < L_{\max}$, we might decide to search for δ_2 such that

$$\delta_2 J^2 \subseteq I_{11,8}\, I_{11,6}^2\, I_{3,2}\, I_{3,0}^2\, I_{2,1}$$

Unlike when $\ell = 1$, the exponents on two of these ideals exceed 1, requiring us to factor $f(X)$ modulo the prime powers 3^2 and 11^2. The prime 11 does not divide $\mathrm{Disc}(f)$, so the linear factors of $f(X) \pmod{11}$ remain linear when factoring $f(X)$ modulo powers of 11. The prime 3 *does* divide $\mathrm{Disc}(f)$; the repeated factor $(X+1)^2 \pmod 3$ becomes a quadratic factor during Hensel lifting:

$$\begin{aligned}
f(X) &\equiv 7(X-5)(X-6)(X-8) \pmod{11},\\
f(X) &\equiv 7(X-16)(X-17)(X-19) \pmod{11^2},\\
f(X) &\equiv X(X+1)^2 \pmod{3},\\
f(X) &\equiv 7(X+3)(X^2+2X-2) \pmod{3^2}.
\end{aligned}$$

The five sublattices have triangular bases

$$\begin{aligned}
\{11,\ \alpha-8,\ \alpha^2-8^2\} &\quad \text{for} \quad I_{11,8}/J^2,\\
\{11^2,\ \alpha-17,\ \alpha^2-17^2\} &\quad \text{for} \quad I_{11,6}^2/J^2,\\
\{3,\ \alpha-2,\ \alpha^2-4\} &\quad \text{for} \quad I_{3,2}/J^2,\\
\{3^2,\ \alpha+3,\ \alpha^2-9\} &\quad \text{for} \quad I_{3,0}^2/J^2,\\
\{2,\ \alpha-1,\ \alpha^2-1\} &\quad \text{for} \quad I_{2,1}/J^2.
\end{aligned}$$

A triangular basis for the intersection is

$$\{2178,\ 33\alpha+891,\ \alpha^2+19\alpha+840\}.$$

An LLL–reduced basis for the intersection is $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, where

$$\mathbf{v}_1 = 31\alpha^2+28\alpha+3, \quad \mathbf{v}_2 = -41\alpha^2+13\alpha+12, \quad \mathbf{v}_3 = 9\alpha^2-27\alpha+36.$$

After weighing these vectors at $\{\alpha_j\}_{j=1}^3$, we choose $\delta_2 = \mathbf{v}_1 = 31\alpha^2 + 28\alpha + 3$ and define $\gamma_3 = \gamma_2/\delta_2^2$. Use these definitions and (7.6) to compute

$$\begin{aligned}
N(\delta_2) &= -\frac{2^2\cdot 3^3\cdot 11^3}{7^2}, & (\delta_2) &= \frac{I_{2,1}^2\, I_{3,0}^2 I_{3,2}^2 I_{11,6}^2\, I_{11,8}}{J^2},\\
N(\gamma_3) &= \frac{N(\gamma_2)}{N(\delta_2)^2} = \frac{3^6\cdot 7^2}{5^2}, & (\gamma_3) &= \frac{I_{3,0}^6 J^2}{I_{5,1}^2},\\
|\gamma_3(\alpha_1)| &\approx 158, & |\gamma_3(\alpha_2)| &= |\gamma_3(\alpha_3)| \approx 3.00.
\end{aligned}$$

By chance, we removed an extra $I_{2,1}^2$ from the numerator of (γ_2) while constructing γ_3. The new γ_3 turns out to be

$$\gamma_3 = \frac{490\alpha^2 - 406\alpha + 321}{5} = \left(\frac{49\alpha^2 - 28\alpha + 24}{5}\right)^2.$$

The numerator and denominator of $\sqrt{\gamma_3}$ have norms 189 and 5 respectively, both much smaller than $L_{\max}$. We may elect to switch to q–adic methods now, after using Lagrange's formula (5.9) to bound the coefficients of the algebraic integer

$$5^2 f'(\alpha)^2\gamma_3 = 323400\alpha^2 - 242550\alpha + 201150 = (385\alpha^2 - 440\alpha + 255)^2$$

or

$$189^2 f'(\alpha)^2/\gamma_3 = -713600\alpha^2 + 1185050\alpha + 1100950 = (595\alpha^2 - 700\alpha - 875)^2.$$

If instead we decide to iterate further, then we should plan on (at least) two more iterations, first using $s_3 = +1$ to reduce the numerator while possibly transferring an ideal to the denominator and then using $s_4 = -1$ to reduce the updated denominator. Each iteration will introduce an ideal J^{d-1}, but these will cancel each other.

Start by removing $I_{3,0}^3\, J$ from the numerator of $\sqrt{\gamma_3}$. This has norm $3^3 \cdot 7 = 189 < L_{\max}$. Triangular bases are

$$\{3^3,\ \alpha - 6,\ \alpha^2 - 6^2\} \quad \text{for} \quad I_{3,0}^3/J^2,$$
$$\{1,\ \alpha,\ 7\alpha^2\} \quad \text{for} \quad J/J^2.$$

The intersection has triangular basis

$$\{27,\ \alpha - 6,\ 7\alpha^2 - 9\}.$$

An LLL–reduced basis is

$$\{4\alpha + 3,\ 5\alpha - 3,\ 7\alpha^2 + 3\alpha\}.$$

After weighing these vectors at the α_j (with larger weights than previously since $189 \ll L_{\max}$), we choose $\delta_3 = 7\alpha^2 - 7\alpha + 6$ and define $\gamma_4 = \gamma_3/\delta_3^2$. Then

$$N(\delta_3) = \frac{2\cdot 3^4}{7}, \qquad (\delta_3) = \frac{I_{2,1}\, I_{3,0}^4}{J},$$
$$N(\gamma_4) = \frac{N(\gamma_3)}{N(\delta_3)^2} = \frac{7^4}{2^2\cdot 3^2\cdot 5^2}, \qquad (\gamma_4) = \frac{J^4}{I_{2,1}^2\, I_{3,0}^2\, I_{5,1}^2},$$
$$|\gamma_4(\alpha_1)| \approx 0.868, \qquad |\gamma_4(\alpha_2)| = |\gamma_4(\alpha_3)| \approx 1.75.$$

Next we search for δ_4 such that

$$\delta_4 J^2 \subseteq I_{2,1}\, I_{3,0}\, I_{5,1}.$$

A triangular basis for the intersection is

$$\{30,\ \alpha+9,\ \alpha^2-9^2\}.$$

After LLL reduction and weighing, we select $\delta_4 = \alpha^2 - \alpha$. The new $\gamma_5 = \gamma_4\delta_4^2$ has norm 1 and has absolute value 1.00 when evaluated at each α_j. We therefore suspect γ_5 to be a root of unity, and it turns out to be $+1$. Therefore

$$\sqrt{\gamma(\alpha)} = \pm\frac{(-81\alpha^2+37\alpha+59)(31\alpha^2+28\alpha+3)(7\alpha^2-7\alpha+6)}{\alpha^2-\alpha}.$$

8. Adjustments for number field sieve

If one wants $\sqrt{\gamma(\alpha)} \bmod n$, then the coefficients of each $\delta_\ell(\alpha)$ can be computed modulo n. For the NFS (see §1), it suffices to compute each $\phi(\delta_\ell(\alpha)) \bmod n$. There is a tiny chance that some intermediate denominator will share a factor with n. If that factor is not n itself, then a factor of n has been found. If the factor is n, then the power of n can be remembered and removed later, using n–adic arithmetic.

The final homomorphism (1.2) can be computed iteratively, rather than postponed until the end of the square root. Applying ϕ to (5.3) gives

$$\phi\left(\sqrt{\gamma(\alpha)}\right) = \phi\left(\sqrt{\gamma_\ell(\alpha)}\right)\prod_{k=1}^{\ell-1}\phi(\delta_k(\alpha))^{s_k}.$$

If all e_i are odd integers, then (1.2) generalizes to

(8.1)
$$\left[\phi\left(\sqrt{\prod_{i\in S}(a_i-b_i\alpha)^{e_i}}\right)\right]^2 \equiv \left[\sqrt{\prod_{i\in S}(a_i-b_im)^{e_i}}\right]^2 \pmod{n}.$$

The square root algorithm permits negative exponents in γ. Heuristicly, it should need fewer iterations when $|N(\text{numer}(\gamma))\,N(\text{denom}(\gamma))|$ is small. This suggests that it may run faster when the exponents of most prime ideals in γ have small absolute values.

If one randomly selects $e_i = \pm 1$ in (8.1), and lets $g_i(\alpha) = (a_i - b_i\alpha)^{e_i}$ in (5.1), then statistical arguments predict considerable cancellation. For example, a prime ideal dividing $2t$ of the $(a_i - b_i\alpha)^{e_i}$ terms each with exponent ± 1 will typically have exponent $\mathbb{O}(t^{1/2})$ in the product. Choosing approximately equal numbers of terms in the numerator and in the denominator makes it likely that all embeddings $\log|\gamma(\alpha_j)|$ will have comparable magnitudes (to within $O\left(|S|^{1/2}\right)$). A clever implementation might choose the e_i so as to cause much more cancellation than statistically expected.

9. Experimental results

All timings in this section are for one processor on a MIPS R4400 (SGI Challenge) running in 32–bit mode.

In November, 1994, I helped Arjen Lenstra and Bruce Dodson complete the factorization of a 119–digit cofactor of the partition number $p(13171)$ using the polynomial

$$\begin{aligned} f(X) = 229712700994770930X^5 &- 75244909504476954X^4 \\ &- 349192234242831010X^3 + 213343035765348142X^2 \\ &- 133732623127145009X - 83887843530130136 \end{aligned}$$

with root 144999999598687668083. The factor bases (including large primes) went to 2^{31}. Each dependency had about 2 million relations. It took the square root code about 25 hours per dependency to do both square roots. The algebraic side took 43000 iterations with $L_{\max} = 10^{200}$ to reduce a γ_1 whose numerator and denominator norms had about 4.1 million decimal digits each.

For special number field sieve, where the polynomial $f(X)$ typically has small coefficients, the square root usually completes in an hour. For example, when factoring a 112–digit cofactor of $10^{192}+1$ in May, 1995, using $f(X) = X^4 - X^2 + 1$ with root $m = 10^{32}$, it took 54 minutes to process a dependency with 506472 pairs (a_1, b_i).

References

[1] Daniel J. Bernstein and A.K. Lenstra, *A general number field sieve implementation*, The Development of the Number Field Sieve (A.K. Lenstra and H.W. Lenstra, Jr., eds.), Lecture Notes in Mathematics, vol. 1554, Springer–Verlag, Berlin, 1993, pp. 103–126.

[2] J.P. Buhler, H.W. Lenstra, Jr., and Carl Pomerance, *Factoring integers with the number field sieve*, The Development of the Number Field Sieve (A.K. Lenstra and H.W. Lenstra, Jr., eds.), Lecture Notes in Mathematics, vol. 1554, Springer–Verlag, Berlin, 1993, pp. 50–94.

[3] Jean-Marc Couveignes, *Computing a square root for the number field sieve*, The Development of the Number Field Sieve (A.K. Lenstra and H.W. Lenstra, Jr., eds.), Lecture Notes in Mathematics, vol. 1554, Springer–Verlag, Berlin, 1993, pp. 95–102.

[4] Gerald J. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.

[5] Serge Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, Springer–Verlag, New York, 1986.

[6] A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
[7] A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard, *The number field sieve*, Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing, Baltimore, May 14–16, 1990 (New York), ACM, 1990, pp. 564–572.
[8] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, England, 1989.

780 Las Colindas Road, San Rafael, CA 94903–2346 USA
E-mail address: `pmontgom@@cwi.nl` or `pmontgom@@math.orst.edu`