# On the calculation of roots of unity in a number field

Pascal Molin

*IMJ*
*Université Paris 7*
*75013 Paris*

**Abstract**

We review some algorithms for the calculation of roots of unity in a number field, and provide evidence that hard cases exist for each of them. We suggest a hybrid approach with garanteed polynomial complexity which proves to be efficient in practice.

*Key words:* roots of unity, Kannan's algorithm, LLL algorithm, polynomial factorization, linear programming, effective Čebotarev's theorem.

## 1. Introduction

Let $\mathbb{K}$ be a number field. The computation of its torsion units $\mu(\mathbb{K})$ is a basic task in algorithmic number theory, necessary in particular for the computation of the class group. The problem is not considered to be hard, and Cohen (1993) recommends to use a lattice enumeration technique due to Kannan. This has become a standard for computer algebra systems.

This enumeration algorithm is efficient for most cases, however its estimated complexity is exponential. In the context of extensive computations linked to class group heuristics, many examples of moderate size have been found recently for which the automatic computation of torsion units bottlenecked the whole process, if not definitely stopping it.

In addition, the computational context has evolved during the last 20 years, and great improvements have been made in the directions of short vectors enumeration (Hanrot and Stehlé, 2007), as well as polynomial factorization over number fields (Belabas, 2004).

⋆ This research was carried out during my Ph.D. thesis at university Bordeaux 1.
*Email address:* pascal.molin@math.univ-paris-diderot.fr (Pascal Molin).
*URL:* http://www.math.jussieu.fr/~molinp (Pascal Molin).

This paper reconsiders several strategies for the computation of roots of unity: we first recall Kannan's small vectors point of vue; then we separate the two problems of computing the order $m = \#\mu(\mathbb{K})$, for which we propose heuristics, and the actual algebraic computation of a primitive unit $\zeta_m \in \mathcal{O}_\mathbb{K}$, for which we give two algorithms: an optimization of Belabas's polynomial factorization algorithm to the cyclotomic setting, and a LLL approach obtained via the complex embeddings.

We exhibit or construct critical examples for each technique. Along the way we present a linear programming approach to build number fields with prescribed ramification.

A hybrid approach having polynomial complexity is proposed. It has been successfully implemented as default algorithm in the `PARI/gp` software (function `nfrootsof1`).

**Notations**

For the following:

- $\mathbb{K}$ is a number field of degree $n$, $\mathcal{O}_\mathbb{K}$ its ring of integers and $\mathrm{disc}(\mathbb{K})$ its discriminant. The algebraic norm of an element $x \in \mathbb{K}$ is denoted $\mathrm{Norm}(x)$.
- For $m \geqslant 2$, $\mu_m$ is the set of $m$-th roots of unity. A $m$-th primitive root is denoted $\zeta_m$. We write $\mu(\mathbb{K})$ for the roots of unity present in $\mathbb{K}$.
- $p$ is a prime number, $\mathfrak{p}$ a prime integral ideal dividing it in $\mathcal{O}_\mathbb{K}$. Let $\mathbb{k}(\mathfrak{p})$ be its residual field and $\mathrm{Frob}_\mathfrak{p}$ the Frobenius automorphism induced in $\mathbb{K}$, if the extension is Galois.
- for $\sigma$ an embedding $\mathbb{K} \hookrightarrow \mathbb{C}$, we denote by $x^\sigma$ its action on $x$.

## 2. Torsion units as short vectors: Kannan's algorithm

$\mathbb{K}$ being a separable extension, it has $n = [\mathbb{K} : \mathbb{Q}]$ complex embeddings

$$\sigma : \mathbb{K} \hookrightarrow \mathbb{C}.$$

This makes it possible to define a product

$$\langle x, y \rangle = \sum_\sigma \overline{x^\sigma} y^\sigma, x, y \in \mathbb{K} \tag{1}$$

endowing $\mathbb{K} \otimes \mathbb{R}$ with a Euclidean norm

$$\|x\|_\mathbb{C} = \sqrt{\sum_\sigma |x^\sigma|^2}. \tag{2}$$

This norm is related to the usual algebraic norm $\mathrm{Norm}(x) = \prod_\sigma x^\sigma$ by the arithmetic-geometric means inequality

$$\|x\|_\mathbb{C}^2 \geqslant n \left|\mathrm{Norm}(x)\right|^{\frac{2}{n}}. \tag{3}$$

This allows to characterize the roots of unity in $\mathbb{K}$ as the shortest non-zero vectors of the lattice $\mathcal{O}_\mathbb{K}$. More precisely, we have (Cohen, 1993):

**Proposition 1** (Kronecker)**.** *For all $x \in \mathcal{O}_\mathbb{K} \setminus \{0\}$, one has $\|x\|_\mathbb{C}^2 \geqslant [\mathbb{K} : \mathbb{Q}]$, with equality if and only if $x$ is a root of unity.*

Thus the computation of roots of unity in $\mathbb{K}$ amounts to enumerating vectors in the ellipsoid $\|x\|_\mathbb{C}^2 \leqslant n$.

Contrary to other approaches, one advantage of this technique is that it combines the problem of computing the order $m = \#\mu(\mathbb{K})$, and that of finding an actual primitive root $\zeta_m \in \mathcal{O}_{\mathbb{K}}$.

Two closely related algorithms perform this task: the first is due to Fincke and Pohst (1985), the other to Kannan (1985). These are deterministic algorithms which rely on an initial reduction of the lattice and a exhaustive enumeration of its short vectors. The binary complexity of this task is in any case exponential, respectively $2^{O(n^2)}$ and $O(n^{\frac{n}{2}})$ binary operations (Hanrot and Stehlé, 2007).

### *2.1. Results*

Despite its huge theoretic complexity, this exhaustive search performs well in practice in the following settings: low dimension (say $n \leqslant 50$); when there are no non-trivial roots of unity; or when $\mathbb{K}$ is cyclotomic.

However, one can easily construct number fields for which the enumeration step is time consuming. In particular, random composita of fields of small degree provide many hard cases.

As an example, the polynomial

$$\begin{aligned} P =& x^{66} - x^{65} + x^{64} - x^{62} + 2x^{61} - 2x^{60} + x^{59} + x^{58} - 3x^{57} + 4x^{56} - 3x^{55} \\ &+4x^{53} - 7x^{52} + 7x^{51} - 3x^{50} - 4x^{49} + 11x^{48} - 14x^{47} + 10x^{46} + x^{45} - 15x^{44} \\ &-20x^{43} + 21x^{42} - 36x^{41} + 16x^{40} + 5x^{39} - 41x^{38} + 57x^{37} - 52x^{36} + 11x^{35} \\ &+46x^{34} - 98x^{33} + 109x^{32} - 63x^{31} - 35x^{30} + 144x^{29} - 207x^{28} + 172x^{27} \\ &-28x^{26} - 179x^{25} + 351x^{24} - 379x^{23} + 200x^{22} + 151x^{21} + 114x^{20} + 86x^{19} \\ &+65x^{18} + 49x^{17} + 37x^{16} + 28x^{15} + 21x^{14} + 16x^{13} + 12x^{12} + 9x^{11} + 7x^{10} \\ &+5x^9 + 4x^8 + 3x^7 + 2x^6 + 2x^5 + x^4 + x^3 + x^2 + 1 \end{aligned} \tag{4}$$

defines a field containing the forty-sixth roots of unity. The search for roots of unity using Fincke-Pohst algorithm (with the `PARI/gp` implementation) has been interrupted after four weeks on a dedicated machine.

## 3. Find the order

Computing the order $m = \#\mu(\mathbb{K})$, or at least finding a close upper bound is much simpler than computing a generator $\zeta_m$. This is also a prerequisite for the algorithms we will present next.

First of all, if there exist one real embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{R}$, then $\mu(\mathbb{K}) = \mu(\mathbb{R}) = \{\pm 1\}$. In particular this is the case for all fields of odd degree $n$.

### *3.1. Ramification of primes*

Greater restrictions can be obtained by the ramification of primes induced by the inclusion $\mathbb{Q}(\zeta_m) \subset \mathbb{K}$.

**Proposition 2.** *Let $p$ be a prime. If $\mu_{p^k} \subset \mathbb{K}$, one has*
- $(p-1) \mid n$ *and* $k \leqslant 1 + v_p(n)$*;*
- $k \leqslant \lfloor \frac{v_p(\mathrm{disc}(\mathbb{K}))}{n} + \frac{1}{p-1} \rfloor$.

*where $n = [\mathbb{K} : \mathbb{Q}]$ and $v_p$ denotes the p-adic valuation.*

**Proof.** The first point derives from the multiplicativity of degrees

$$[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = (p-1)p^{k-1} \mid n = [\mathbb{K} : \mathbb{Q}].$$

The second is obtained from the discriminants relation: if $K \subset \mathbb{K}$ then $\mathrm{disc}(K)^{[\mathbb{K}:K]} \mid \mathrm{disc}(\mathbb{K})$.

The cyclotomic field $\mathbb{Q}(\zeta_{p^k})$ having degree $(p-1)p^{k-1}$ and discriminant (Lang, 1964)

$$\mathrm{disc}(\mathbb{Q}(\zeta_{p^k})) = \pm p^{p^{k-1}(pk-k-1)},$$

the second inequality follows. □

### *3.2. Decomposition of primes*

The local global principle works for roots of unity.

**Proposition 3.** *The following statements are equivalent:*

*(i)* $\mu_m \subset \mathbb{K}$*;*

*(ii)* $\mu_m \subset \mathbb{K}_{\mathfrak{p}}$ *for each prime ideal* $\mathfrak{p}$*;*

*(iii) for every prime p not dividing* $m \times \mathrm{disc}\mathbb{K}$ *and all prime ideals* $\mathfrak{p}$ *dividing p,* $\mathrm{Norm}(\mathfrak{p}) \equiv 1 \bmod m$*.*

**Proof.** We consider the Galois extension $\mathbb{K}(\zeta_m)/\mathbb{K}$. Let us suppose that for each non ramified prime $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ one has $\mathrm{Norm}(\mathfrak{p}) \equiv 1 \bmod m$, then the action of $\mathrm{Frob}_{\mathfrak{p}}$ on $\zeta_m$ is given by $\zeta_m \mapsto \zeta_m^{\mathrm{Norm}(\mathfrak{p})} = \zeta_m$, so that this Frobenius acts as identity. Čebotarev's density theorem concludes that the Galois group contains only the trivial class of conjugacy, which means that the extension has degree 1. □

**Remark 4.** Čebotarev's theorem allows to replace *every prime p* by *almost all primes*, that is *a set of primes of density 1.*

This proposition makes it possible to guess the number of roots of unity in $\mathbb{K}$ with the following procedure: "compute the gcd of a number of values $\mathrm{Norm}(\mathfrak{p}) - 1$ until it stabilizes".

Computationaly speaking, this is easy to implement, and one does not even need to compute $\mathcal{O}_{\mathbb{K}}$ nor perform any arithmetic in $\mathbb{K}$. If $p$ is unramified in $\mathbb{K} = \mathbb{Q}[x]/R(x)$, write

$$R(x) = \prod_{i=1}^{r} R_i(x) \bmod p \tag{5}$$

the factorization of $R(x)$ in $\mathbb{F}_p$, which corresponds to the prime ideal decomposition

$$p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{r} \mathfrak{p}_i \tag{6}$$

with $f_i = \deg(R_i)$ the inertia degree of the prime ideal $\mathfrak{p}_i$. Then the gcd of $\mathrm{Norm}(\mathfrak{p}_i) - 1$ is simply $p^f - 1$ where $f = \gcd\{f_i\}$.

Combining this idea with proposition 2, we obtain the following algorithm, in which the parameter $N$ will be discussed later.

**Input**: $\mathbb{K}$ a number field, $N$ integer
**Output**: a multiple $m$ of the number of roots of unity in $\mathbb{K}$;
Set $m = 0$ and $p = 2$;
**repeat**
1 | set $p$ next unramified prime;
| compute the decomposition of $p$ in $\mathcal{O}_{\mathbb{K}}$;
| compute the gcd $f$ of the inertia degrees;
| set $m = \gcd(m, p^f - 1)$;
**until** *$m$ stable since the last $N$ loops*;
**for each** *divisor $p_i^{k_i}$ of $m$* **do**
| **if** $p_i - 1 \nmid [\mathbb{K} : \mathbb{Q}]$ **then**
| | $k_i = 0$
| **else**
| | $k_i = \min(k_i, 1 + v_{p_i}([\mathbb{K} : \mathbb{Q}])$;
| | $k_i = \min(k_i, \lfloor \frac{v_{p_i}(\mathrm{disc}(\mathbb{K}))}{[\mathbb{K}:\mathbb{Q}]} + \frac{1}{p_i - 1} \rfloor)$;
| **end**
**done**
**return** *the product of $p_i^{k_i}$*

**Algorithm 1:** Heuristic on the number of roots

This heuristic is quite precise in practice: the output number is in any case a multiple of the number of roots of unity in $\mathbb{K}$, and in most cases it matches the true value.

However, one can build "bad" number fields $\mathbb{K}$, which means that any sensible implementation of Algorithm 1 (i.e. any reasonable value of $N$) will output a strict multiple of $m$.

As an example, the number field

$$\mathbb{K} = \mathbb{Q}(\sqrt{-51}, \sqrt{-230}, \sqrt{263}, \sqrt{307}) \tag{7}$$

has degree $n = 8$, and no real embedding. Running Algorithm 1,

- the ramification criterion gives $\mu(\mathbb{K}) \subset \mu_{24}$;
- the decomposition criterion of primes $(p)$ gives $\mu(\mathbb{K}) \subset \mu_{24}$ for $p \leqslant 317$, then $\mu(\mathbb{K}) \subset \mu_4$ for all primes $p \leqslant 2999$.

However, these conclusions are still inaccurate. In fact, $\mathbb{K}$ contains only the trivial roots $\mu_2$.

### *3.3. Randomized version*

The example above seems to show that Algorithm 1 is ineffective. In fact, algorithm 1 can be made rigorous for explicit values of the parameter $N$. However such values must be large, this will be discussed in the next section.

On the other hand, it is quite easy to randomize the algorithm so that it outputs the correct value $m$ with probability

$$P(m = \#\mu(\mathbb{K})) > 1 - 2^{-N}. \tag{8}$$

One needs to replace the line 1 *"set $p$ next unramified prime"* by *"set $p \not\equiv 1 \bmod m$ a random unramified prime"*.

In fact, if $d = [\mathbb{K}(\zeta_m) : \mathbb{K}]$, only a density $\frac{1}{d}$ of unramified primes satisfy $\mathrm{Norm}(\mathfrak{p}) = 1 \bmod m$, hence the result.

*3.4. Effective Čebotarev's theorems*

In order to make proposition 3 effective, we introduce two quantities:

- the upper bound for $m$ computed by considering all primes up to $x$

$$m_{\mathbb{K}}(x) = \gcd\left\{\mathrm{Norm}(\mathfrak{p}) - 1, \mathfrak{p} \mid p\mathcal{O}_{\mathbb{K}}, p \leqslant x \text{ unramified }\right\}. \tag{9}$$

- the number of primes one needs to consider to get the correct value $m = \#\mu(\mathbb{K}) = \lim_{x\to\infty} m_{\mathbb{K}}(x)$

$$S(\mathbb{K}) = \inf\left\{x \geqslant 2, m_{\mathbb{K}}(x) = m \text{ where } \mu(\mathbb{K}) = \mu_m\right\}. \tag{10}$$

Algorithm 1 can be made rigorous if one is able to bound $S(\mathbb{K})$. This question is solved with effective versions of Čebotarev's density theorems.

Under the generalized Riemann's hypothesis (GRH), Lagarias and Odlyzko (1977, cor1.2) give the following statement, (where the constant is due to Serre (1981)):

**Theorem 5.** *Let $\mathbb{L}/\mathbb{K}$ be a Galois extension, and assume that the Dedekind zeta function of $\mathbb{L}$ does not have any zero of real part greater that $\frac{1}{2}$. Then for every conjugacy class $C$ of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, there exists an unramified prime $\mathfrak{p}$ of $\mathbb{K}$ with $\mathrm{Frob}_{\mathfrak{p}} \in C$ and*

$$\mathrm{Norm}(\mathfrak{p}) \leqslant c(\log \mathrm{disc}(\mathbb{L}))^2$$

*where $c$ is an absolute constant, which one can take equal to 70.*

One applies this theorem to any non trivial class of automorphisms of $\mathbb{K}(\mu_m)/\mathbb{K}$, which gives

**Proposition 6.** *Under GRH, if $\mu_m \notin \mathbb{K}$ then $m \nmid m_{\mathbb{K}}(x)$ for*

$$x = 70\big(\log \mathrm{disc}(\mathbb{K}(\mu_m))\big)^2.$$

On the other hand, one can use the bounds of (Serre, 1981, prop.4') to give a criterion which does not depend on $\mathrm{disc}(\mathbb{K}(\mu_m))$:

**Proposition 7.** *Under GRH, for all $p, k$ such that $\mu_{p^k} \notin \mathbb{K}$, then $p^k \nmid m_{\mathbb{K}}(x)$ for*

$$x \geqslant 70\varphi(p^k)^2\left[\log \mathrm{disc}(\mathbb{K}) + n\log(p\varphi(p^k))\right]^2$$

*where $n = [\mathbb{K} : \mathbb{Q}]$.*

**Corollary 8.** *Under GRH, and with the notation of proposition 7, Algorithm 1 outputs the correct value $m = \#\mu(\mathbb{K})$ for the choice of parameter*

$$N = 70\big(n^2\mathrm{disc}(\mathbb{K}) + 2n^3\log(n)\big)^2. \tag{11}$$

**Proof.** Let $p^k$ be an integer such that $\mu_{p^k} \subset \mathbb{K}$. From the ramification criterion, we know that $\phi(p^k) \mid n$, in particular $\phi(p^k) \leqslant n$. The corresponding primes are then filtered by the decomposition criterion under the bound of proposition 7. □

| $\{D_i\}$ | $S(\mathbb{K})$ | $S(\mathbb{K})/\Delta_6^2$ | $S(\mathbb{K})/\Delta_6$ |
|---|---|---|---|
| {-1} | 5 | 0.33 | 1.29 |
| {-7} | 11 | 0.44 | 2.20 |
| {-23} | 23 | 0.42 | 3.12 |
| {-177} | 59 | 0.29 | 4.15 |
| {-2033} | 101 | 0.28 | 5.29 |
| {-172417} | 149 | 0.19 | 5.32 |
| {-58, 73} | 227 | 0.14 | 5.67 |
| {-311, 58} | 317 | 0.15 | 6.91 |
| {-1167, 389} | 389 | 0.14 | 7.31 |
| {-467, 1401} | 467 | 0.16 | 8.54 |
| {-1671, 557} | 557 | 0.18 | 9.93 |
| {-1707, 569} | 569 | 0.18 | 10.12 |
| {-2, -7, -1} | 113 | 0.06 | 2.55 |
| {-19, 5, 2} | 191 | 0.07 | 3.53 |
| {-47, -2, -7} | 347 | 0.08 | 5.41 |
| {-7, 5, 41} | 359 | 0.10 | 6.06 |
| {-87, -10, 19} | 653 | 0.06 | 6.47 |
| {-86, 17, 105} | 977 | 0.08 | 9.07 |

**Table 1.** $S(\mathbb{K})$ for quadratic fields, comparison with $\Delta_6 = \log \mathrm{disc}\mathbb{K}(\zeta_6)$

This bound is by far too big to be used in practice: on the example (4), Proposition 7 states we need to check all primes less than $p = 12159134333$ to prove (under GRH) that $\mu(\mathbb{K}) = \mu_{46}$. In practice, $S(\mathbb{K}) = 5$ already proves $m \mid 46$, and the next step is to find $\zeta_{46}$.

In the next section, we investigate the sharpness of this bound on $S(\mathbb{K})$.

*3.4.1. Finding bad examples*

We are looking for large values of $S(\mathbb{K})$: our strategy is to choose a value $m > 2$, and find numerically fields $\mathbb{K}$ such that $m \mid m_{\mathbb{K}}(x)$ for large values of $x$, but $\mu_m \not\subset \mathbb{K}$.

As a first example, we consider quadratic fields $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ for $m = 4$ or $m = 6$ (*i.e.* $\varphi(m) = 2$).

**$m = 4$:** We want $\mathrm{Norm}(\mathfrak{p}) \equiv 1 \bmod 4$, which means that primes congruent to $3 \bmod 4$ are inert, that is $\left(\frac{D}{p}\right) = -1$.

**$m = 6$:** This time, we demand that $\mathrm{Norm}(\mathfrak{p}) \equiv 1 \bmod 3$, so that the primes $p \equiv 2 \bmod 3$ (except 2) should be inert ($\left(\frac{D}{p}\right) = -1$).

With a compositum of two fields $K = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, we can also mimic the eighth roots of unity when all primes congruent to $3, 5, 7 \bmod 8$ have a non trivial inertia in at least one quadratic subfield.

As an example $\mathbb{K} = \mathbb{Q}(\sqrt{7}, \sqrt{-723})$, for which $S(\mathbb{K}) = 131$. The heuristic detects wrongly $\mu_{24}$ (or $\mu_{12}$ with the ramification criterion).

Focusing on 8-th roots, one obtains for example $\mathbb{K} = \mathbb{Q}(\sqrt{11}, \sqrt{-23})$ which passes all tests up to $S(\mathbb{K}) = 127$.

Another nice example is $\mathbb{K} = \mathbb{Q}(\sqrt{-7}, \sqrt{5}, \sqrt{41})$, which seems to contain $\mu_{24}$ until $S(\mathbb{K}) = 359$.

Table 1 shows a list of fields $\mathbb{K} = \mathbb{Q}(\sqrt{D}_1, \dots)$ such that $\mu(\mathbb{K}) = \mu_2$ but (at least) $3 \mid m_{\mathbb{K}}(x)$ for $x < S(\mathbb{K})$.

In particular, we tried to obtain good lower bounds of the $c$ constant appearing in theorem 5, that is of the ratio $S(\mathbb{K})/\Delta_m^2$, where $\Delta_m = \log \mathrm{disc}\mathbb{K}(\zeta_m)$.

The values obtained are small compared to the proven value 70, and they are decreasing when we aim at larger $S(\mathbb{K})$.

On the other hand, it is asked in Serre (1981) if the exponent 2 in proposition 5 can be replaced by $1 + \varepsilon$. In this context, the last column of table 1 shows increasing values of $S(\mathbb{K})/\delta_m$.

*3.4.2. Generalization with linear programming*

Larger values of $S(\mathbb{K})$ can be reached with the same idea of composing small fields, in order to distribute inertia degrees among them.

Linear programming can be used to find good combinations with a degree as small as possible. Let $\mathbb{K} = \mathbb{K}_1 \dots \mathbb{K}_n$ be the compositum of the $\mathbb{K}_j = \mathbb{Q}[X]/(Q_j)$.

As before, one demands that for each prime $p$ up to a certain fixed bound, the inertia degree $f_{\mathfrak{p}/p}$ of $\mathfrak{p} \mid p\mathcal{O}_{\mathbb{K}}$ is a multiple of the order of $p$ in $(\mathbb{Z}/m\mathbb{Z})^*$.

Let us write

$$(\mathbb{Z}/m\mathbb{Z})^\times = \prod_q \prod_i \mathbb{Z}/q^{e_{q,i}}\mathbb{Z},$$

the $p$-primary decomposition of $(\mathbb{Z}/m\mathbb{Z})^\times$ and

$$o(p) = \prod_q q^{\alpha_{p,q}}$$

the decomposition into prime factors of the order of $p$ modulo $m$.

Then define the coefficients

$$\delta(\mathbb{K}_j, p, q^\alpha) = \begin{cases} 1 \text{ if } \forall \mathfrak{p} \mid p\mathcal{O}_{\mathbb{K}_j}, \mathrm{Norm}(\mathfrak{p}) \equiv 1 \bmod [q^\alpha] \\ 0 \text{ otherwise.} \end{cases}$$

The fact that $m \mid m_{\mathbb{K}}(x)$ is then coded by the following linear program, where the columns are indexed by a family of polynomials $Q_j$, and the lines describe the inertia degree with respect to every prime $p$ less than $x$:

$$\forall p \leqslant x,\ \forall q \mid o(p),\ \sum_j x_j \delta(\mathbb{K}_j, p, q^{\alpha_{p,q}}) \geqslant 1 \tag{12}$$

We add the following objective function:

$$\text{Minimize } \sum_j x_j \deg(Q_j) - \mathrm{disc}(Q_j)^{-1}$$

| $m$ | $\deg(\mathbb{K})$ | $\Delta_m = \log \operatorname{disc}(\mathbb{K}(\mu_m))$ | $S(\mathbb{K})$ | $S(\mathbb{K})/\Delta_m^2$ | $S(\mathbb{K})/\Delta_m$ |
|---|---|---|---|---|---|
| 6 | 8 | 29.1 | 131 | 1.55e-1 | 4.50 |
| 6 | 8 | 29.9 | 149 | 1.67e-1 | 4.98 |
| 4 | 16 | 137.3 | 991 | 5.26e-2 | 7.21 |
| 4 | 32 | 249.4 | 2003 | 3.22e-2 | 8.03 |
| 4 | 32 | 364.0 | 2999 | 2.26e-2 | 8.24 |
| 6 | 32 | 344.0 | 2999 | 2.53e-2 | 8.72 |
| 6 | 32 | 397.1 | 3089 | 1.96e-2 | 7.78 |
| 12 | 64 | 1354.2 | 8009 | 4.37e-3 | 5.91 |

**Table 2.** Fields found with linear programming (using GLPK [2] library)

in order to minimize the degree of the compositum $\mathbb{K}$, and to a minor extent its discriminant.

As is, this program would output the $m$-th cyclotomic extension as a compositum of some of its subfields. Thus we add some low inertia constraints on a prime $p > p_n$ to avoid this situation.

Running this integer linear program [1] , even without reaching the true optimum, yields extensions with interesting extremal ramification properties in the context of the effective Čebotarev theorem.

The table 2 shows some of the constructions obtained this way. The remarks made about table 1 are still valid here, in particular one can increase the ratio $S(\mathbb{K})/\Delta_m$. The method described here could help further investigations on this topic.

## 4. Roots via Hensel lifting

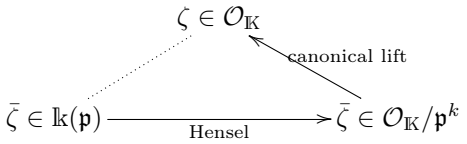
This section is an restriction to the roots of unity setting of the general algorithm of polynomial factorisation in number fields, for which we refer to (Belabas, 2004).

### *4.1. Principle*

Once a multiple $m$ of the order of $\mu(\mathbb{K})$ is known, the true order can be found by factoring the cyclotomic polynomial $\Phi_m$ over $\mathbb{K}$. The modular algorithm of Belabas consists in the following steps:

(1) compute a local root $\overline{\zeta}$ modulo a prime ideal $\mathfrak{p}$;
(2) lift $\overline{\zeta}$ modulo $\mathfrak{p}^k$ with Hensel's lemma;
(3) take a representative $\zeta \in \mathcal{O}_{\mathbb{K}}$ as soon as the fundamental domain of the lattice $\mathfrak{p}^k$ is sufficiently large so that it contains the ellipsoid $\|x\|_{\mathbb{C}}^2 \leqslant n$, hence $\mu(\mathbb{K})$.

[1] available at `http://www.math.jussieu.fr/~molinp`.
[2] Gnu Linear Programming Kit, see references.




The first two steps are straightforward. As for the third, one must make sure that the lift will be a root of unity, if it exists. If such a lift does not exists, it then proves that the heuristic on $m$ has to be refined and we proceed with its divisors.

In the next paragraphs, we give some details for each step of Algorithm 2.

**Input**: $\mathbb{K}$ a number field with a basis of $\mathcal{O}_{\mathbb{K}}$, a multiple $m$ of the order of $\mu_{\mathbb{K}}$
**Output**: the expression of a primitive root in $\mu_{\mathbb{K}}$
**begin**
  choose a prime ideal $\mathfrak{p}$;
  evaluate the lift exponent $k$;
  **repeat for** $k$ increasing
    compute $\mathfrak{p}^k$ and determine a LLL-reduced basis;
    compute the maximal radius in its fundamental domain $D$;
  **until** $B(n) \subset D$;
  **for each** $q = p^l$ *dividing* $m$ **do**
    compute $\overline{\zeta_q} \in \mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ a primitive $q$-th root of unity;
    lift it modulo $\mathfrak{p}^k$ by Hensel;
    **repeat** for $l$ decreasing
      take central lift $\zeta_q \in \mathcal{O}_{\mathbb{K}}$;
    **until** $\zeta_q \in B(n)$, otherwise set $\overline{\zeta_q} \leftarrow \overline{\zeta_q^p}$;
  **done**
  **return** *product of* $\zeta_q$
**end**

**Algorithm 2:** Modular calculation of roots of unity

*4.1.1. Choice of* $\mathfrak{p}$ *and computation in* $\Bbbk(\mathfrak{p})$

In theory, every non ramified prime allows to perform the following steps. In practice, one must balance two aspects: a large value of $p$ or a greater inertia degree result in a lattice $\mathfrak{p}$ of larger volume, thus reducing the exponent $k$. The drawback is however the cost of calculations in $\Bbbk(\mathfrak{p})$.

In practice, it is interesting to choose a small prime of big inertia degree.

We then use the standard Cantor-Zassenhaus algorithm to find a root of the cyclotomic polynomial $\Phi_q$ in the finite field $\Bbbk(\mathfrak{p}) = \mathbb{F}_p[X]/\overline{P}$.

If there is no root, $m$ was overestimated and we proceed to the next value of $q$; otherwise we obtaind one $\bar{\zeta}$.

A prime ideal $\mathfrak{p}$ is represented by two generators $\mathfrak{p} = \langle p, \beta \rangle$, its powers are given by

$$\mathfrak{p}^k = \langle p^k, \beta^k \rangle$$

before one applies LLL to obtain a nicer fundamental domain.

*4.1.2. Lifting in $\mathcal{O}_{\mathbb{K}}$*

The lattice $\mathfrak{p}^k \subset \mathcal{O}_{\mathbb{K}}$ is represented with a $\mathbb{Z}$-basis $(v_1, \dots v_n)$, and the canonical lift $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}^k \to \mathcal{O}_{\mathbb{K}}$ is the lift belonging to the centered fundamental domain

$$D = \left\{ \sum x_i v_i, x_i \in ]-\tfrac{1}{2}; \tfrac{1}{2}] \right\}.$$

We use the geometric setting of section 2, in particular the Euclidean space inherited from the complex embeddings. For $r \geqslant 0$, we introduce the ball

$$B(r) = \left\{ x \in \mathcal{O}_{\mathbb{K}}, \|x\|_{\mathbb{C}}^2 \leqslant r \right\}. \tag{13}$$

We note

$$G = \left( \langle v_i, v_j \rangle \right) \tag{14}$$

the Gram matrix of $(v_1, \dots v_n)$, so that $\langle x, y \rangle =^t xGy$ for $x = \sum_i x_i v_i$ and $y = \sum_i y_i v_i \in \mathfrak{p}^k$.

Proposition 1 asserts that $\mu(\mathbb{K}) \subset B(n)$, so that one can make sure that the lift $\overline{\zeta} \in \mathcal{O}_{\mathbb{K}}/\mathfrak{p}^k \to \zeta \in D$ will give a root of unity if $B(n) \subset D$. The following criterion answers this question.

**Lemma 9.**

$$B(r) \subset D \Leftrightarrow r \leqslant R_{max} = \frac{1}{2 \max_j \sqrt{(G^{-1})_{j,j}}}. \tag{15}$$

*where $(G^{-1})_{j,j}$ denote the diagonal terms of the inverse matrix $G^{-1}$.*

**Proof.** This radius is the shortest distance of the centre of $D$ to its facets. These distances are given by

$$d(\sum \frac{v_i}{2}, H_j) = \frac{1}{2} d(v_j, H_j)$$

where $H_j = \mathrm{Vect}(v_1, \dots \check{v}_j, \dots v_n)$ is the hyperplane spanned by the $v_i$ for $i \neq j$.

Let us write $\tilde{v}_j$ the vector orthogonal to $H_j$ defined by

$$\forall i, \langle \tilde{v}_j, v_i \rangle = \delta_{i,j},$$

so that $\tilde{v}_j$ is precisely the $j$-th column of $G^{-1}$.

We then obtain $d(v_j, H_j) = \frac{|\langle \tilde{v}_j, v_j \rangle|}{\|\tilde{v}_j\|_{\mathbb{C}}}$, hence $d(v_j, H_j) = \left\| (G^{-1})_j \right\|_{\mathbb{C}}^{-1}$.

It remains to compute the norm

$$\left\| (G^{-1})_j \right\|_{\mathbb{C}}^2 =^t (G^{-1})_j G (G^{-1})_j = (G^{-1})_{j,j},$$

which concludes the proof. □

For calculations, it is preferable to express $\tilde{v_i}$ on the orthonormal basis $(v_j^*)$, that is to replace the Gram matrix $G$ by the Gram-Schmidt orthogonalization matrix

$$K = \left( \langle v_i^*, v_j \rangle \right)_{i,j}.$$

The inversion step is simpler since this matrix is triangular. The computations have to be adapted only when taking the norm, where the orthogonality gives

$$\left\| K_j^{-1} \right\|_{\mathbb{C}}^2 = \sum_i \frac{K_{i,j}^2}{\|v_i^*\|_{\mathbb{C}}^2}.$$

As a consequence we have the alternative expression

$$R_{\max} = \frac{1}{2} \min_j \sqrt{\sum_i \frac{K_{i,j}^2}{\|v_i^*\|_{\mathbb{C}}^2}}^{-1} . \tag{16}$$

*4.1.3. Estimates for the exponent k*

The radius (16) will be bigger if the basis $(v_1, \dots v_n)$ is almost orthogonal and made of short vectors. This explains why we first take $(v_1, \dots v_n)$ to be LLL-reduced.

This LLL-reduction of $\mathfrak{p}^k$ is the most time-consuming part of the algorithm, since the matrix has dimension $n$ and entries of size $p^k$, using the best $\tilde{L}^1$ algorithm of Novocin et al. (2011), the complexity $O_\varepsilon(n^{5+\varepsilon} k \log p + n^{3.5+\varepsilon} (k \log p)^{1+\varepsilon})$ can be quasi-linear in terms of $k$.

If one adopts a LLL-reduction with a quality factor $\gamma$, a study of the formula (16) gives the following upper bound for $k$ (Belabas, 2004)

$$R_{\max} \geqslant \frac{\|v_1\|_{\mathbb{C}}}{2\big(\frac{3\sqrt{\gamma}}{2}\big)^{n-1}}.$$

Moreover, the norm of $v_1 \in \mathfrak{p}^k$ is a multiple of $\mathrm{Norm}(\mathfrak{p})^k$ and the arithmetic-geometric means inequality (3) gives

$$\|v_1\|_{\mathbb{C}} \geqslant n \mathrm{Norm}(\mathfrak{p})^{\frac{2k}{n}}.$$

Thus we have the following upper bound:

$$k \leqslant \frac{n \log(2n^{\frac{3}{2}} \big(\frac{3\sqrt{\gamma}}{2}\big)^{n-1})}{2f \log(p)} = O\big(\frac{n^2}{f \log(p)}\big). \tag{17}$$

All in all, using latest LLL algorithms, Algorithm **??** has polynomial running time $O_\varepsilon(n^{7+\varepsilon})$.

## 5. Integral linear system

Assume we know that $\mu(\mathbb{K}) = \mu_m$. A primitive root $\zeta_m \in \mathcal{O}_{\mathbb{K}}$ is obtained as a solution of the integer linear system

$$\sum_{i=1}^{n} \alpha_i \omega_i^\sigma = e^{\frac{2i\pi}{m}}, \, (a_i) \in \mathbb{Z}^n, \tag{18}$$

where $\mathcal{O}_{\mathbb{K}} = \bigoplus \mathbb{Z}\omega_i$ and $\sigma : \mathbb{K} \to \mathbb{C}$ is a fixed embedding.

This system has complex coefficients and is hard to solve. However there is a standard way to find integral relations with small coefficients between complex numbers, based on the LLL algorithm.

We consider the lattice $\Lambda = \mathbb{Z}^{n+1} A$, where $A$ is the $(n+1) \times (n+2)$ matrix

$$A = \begin{bmatrix} 1 & \cdots & 0 & \lfloor M\mathrm{Re}(\omega_1^\sigma) \rfloor & \lfloor M\mathrm{Im}(\omega_1^\sigma) \rfloor \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & \lfloor M\mathrm{Re}(\omega_n^\sigma) \rfloor & \lfloor M\mathrm{Im}(\omega_n^\sigma) \rfloor \\ 0 & \cdots & 0 & \lfloor M\mathrm{Re}(e^{\frac{2i\pi}{m}} \rfloor) & \lfloor M\mathrm{Im}(e^{\frac{2i\pi}{m}} \rfloor) \end{bmatrix} \tag{19}$$

and depends on a big constant $M$ chosen on purpose, so that the shortest non-zero vector of the lattice

$$Z = (\alpha_1, \dots \alpha_n, k)A$$

corresponds to an equality

$$\sum_{i=1}^{n} \alpha_i \omega_i^\sigma = k e^{\frac{2i\pi}{m}}, k = \pm 1,$$

and has its two last components almost equal to zero, while other vectors should be of norm in the greater range given by $M$.

Rigorously setting up this knapsack strategy demands two estimates: an upper bound for the expected vector norm, and a lower bound for other unwanted vectors. We give such bounds in the proposition 14 below.

Then, the properties of LLL-reduced basis (proposition 15) allow to choose the constant $M$ to select exactly the desired of unity:

**Theorem 10.** *For the explicit values $C_{\mathcal{O}}$ and $C_\sigma$ defined in equations* (24) *and* (25) *below, if one choses*

$$M > 2^{n(n+1)+1/2} C_\sigma (\sqrt{n+2}(nC_{\mathcal{O}} + 1))^n. \tag{20}$$

*then the first vector $Z_1$ of a LLL reduced basis of $\Lambda$ satisfies:*

- *either its $n$ first components give the expression of a $m$-th primitive root of unity $\zeta_m$;*
- *or $\mathcal{O}$ does not contain the group of $m$-th roots of unity.*

We prove this theorem in the following paragraphs.

In practice, the size of $M$ would lead to huge computations. However we can decide to run the LLL reduction with a much smaller value $M$, and test whether the first vector $Z_1$ corresponds to a root of unity or not, in which case one has to switch to a more rigorous approach to refine the result.

**Input**: a number field $\mathbb{K}$ with a basis of $\mathcal{O}_{\mathbb{K}}$ and the order $m$ of $\mu_m$
**Output**: an expression of a $m$-th primitive root $\zeta$ or failure
**begin**
  choose $M$ to be, say, the $n$-th root of (20);
  build the matrix $A$ of (19);
  perform its LLL reduction;
  compute the vector $x \in \mathcal{O}_{\mathbb{K}}$ defined by its first components;
  **if** *$x$ is of order $m$* **then**
    **return** $(m, x)$;
  **else**
    **return** *failure*;
  **end**
**end**

**Algorithm 3:** Linear dependency

### *5.1. Norm inequalities*

Every vector $Z$ of $\Lambda$ is the data of an algebraic integer $x$ given by its coordinates on the basis of $\mathcal{O}$, and the decimal approximation of a complex number $Mz$ formed of the two last components.

More precisely, to any couple $(x,k) \in \mathcal{O}_{\mathbb{K}} \times \mathbb{Z}$, with $x = \sum \alpha_i \omega_i$, we define

- the vector $X = (\alpha_1, \dots \alpha_n, k) \in \mathbb{Z}^{n+1}$;
- its image $Z = (\alpha_1, \dots \alpha_n, a, b) \in \Lambda$;
- the complex $z = \sum \alpha_i \omega_i^\sigma + k e^{2i\pi/m} \in \mathbb{C}$.

Each space above is endowed with its Euclidean norm $\|\cdot\|_2$, for which we have

$$\|Z\|_2^2 = \sum \alpha_i^2 + a^2 + b^2 = \|x\|_2 + a^2 + b^2. \tag{21}$$

We also consider the 1-norm $\|x\|_1 = \sum |\alpha_i|$.

**Lemma 11.** *With the notations above, we have*

$$\|X\|_2^2 + \left(M|z| - \sqrt{2}\|X\|_1\right)^2 \leqslant \|Z\|_2^2 \leqslant \|X\|_2^2 + \left(M|z| + \sqrt{2}\|X\|_1\right)^2.$$

**Proof.** In fact, the definition of integer part implies

$$M\mathrm{Re}(z) - \sum |\alpha_i| \leqslant a \leqslant M\mathrm{Re}(z) + \sum |\alpha_i|$$

and the same inequality on imaginary parts, so that when taking the square

$$\begin{aligned} a^2 + b^2 &\geqslant M^2|z|^2 - 2M\|X\|_1 (|\mathrm{Re}(z)| + |\mathrm{Im}(z)|) + 2\|X\|_1^2 \\ &\geqslant \left(M|z| - \sqrt{2}\|X\|_1\right)^2. \end{aligned}$$

□

The conversion from and to the norm $\|\cdot\|_{\mathbb{C}}$ introduced in section 2 is straightforward: introducing the matrix of conjugates

$$V = (\omega_j^\sigma)_{\sigma:\mathbb{K}\hookrightarrow\mathbb{C}, 1\leqslant j\leqslant n} \tag{22}$$

we have

$$\|x\|_{\mathbb{C}} = \|Vx\|_2. \tag{23}$$

We define the constants

$$C_{\mathcal{O}} = \left\|V^{-1}\right\|_2 \tag{24}$$

and

$$C_\sigma = \prod_{\tau\neq\sigma} \max(1, \|V_\tau\|_2) \tag{25}$$

where $\tau$ runs over the complex embeddings, and $V_\tau$ is the line $(\omega_1^\tau, \dots \omega_n^\tau)$ of $V$.

From proposition 1 we deduce

**Lemma 12.** *For all $\zeta \in \mu(\mathbb{K})$,*

$$\|\zeta\|_2^2 \leqslant nC_{\mathcal{O}}. \tag{26}$$

On the other hand, we have the lower bound

**Lemma 13.** *Suppose $\zeta_m \in \mathcal{O}$, then keeping current notations, if $z \neq 0$ we have*

$$|z| \geqslant \frac{1}{C_\sigma \|X\|_1^{n-1}}. \tag{27}$$

**Proof.** Since we supposed $\zeta_m \in \mathcal{O}$, there exist some $y = x + k\zeta_m \in \mathcal{O}_{\mathbb{K}}$, with $x = \sum \alpha_i \omega_i$ such that $z = y^\sigma$. For each embedding $\tau : \mathbb{K} \hookrightarrow \mathbb{C}$ we have

$$|y^\tau| \leqslant |x^\tau| + \left| k e^{2i\pi k/m} \right| \leqslant \|V_\tau\|_2 \, \|(\alpha_1, \dots \alpha_n)\|_2 + |k| \leqslant \max(\|V_\tau\|_2, 1) \, \|X\|_1$$

and since $y \in \mathcal{O}_{\mathbb{K}}$, we obtain the result from (25) and $1 \leqslant |\mathrm{Norm}(y)| = |y^\sigma| \prod_{\tau \neq \sigma} |y^\tau|$. □

From these inequalities we deduce

**Proposition 14.** *Suppose $\mu_m \subset \mathcal{O}$, and set $\zeta_m = \sum \alpha_i \omega_i$ the root of unity whose image by $\sigma$ is $e^{\frac{2i\pi}{m}}$. Then*

- *the vector $Z \in \Lambda$ obtained as image of the vector $X$ of components $(\alpha_1, \dots \alpha_n, -1)$ satisfies*
$$\|Z\|_2^2 \leqslant 2nC_{\mathcal{O}} + 2; \tag{28}$$
- *for all vector $Z$ in $\Lambda$ whose associated complex number $z$ is non zero, we have*
$$\|Z\|_2 \geqslant \frac{1}{\sqrt{n+1}} \left( \frac{M}{\sqrt{2} C_\sigma} \right)^{\frac{1}{n}}. \tag{29}$$

**Proof.** The vector $Z$ corresponds to the complex $z = 0$, so lemma 11 implies $\|Z\|_2^2 \leqslant \|X\|_2^2 + \|X\|_1^2 = \|\zeta\|_2^2 + \|\zeta\|_1 + 2$. With the trivial upper bound $\|\zeta\|_1 \leqslant \|\zeta\|_2^2$, the lemma 12 proves the assertion.

The second part is deduced from the other inequality in lemma 11 combined with the lower bound of lemma 13: let $U = \|X\|_1 \geqslant 1$, $|z|$ is a solution of the system

$$\begin{cases} \sqrt{n+2} \, \|Z\|_2 \geqslant U + \left| M \, |z| - \sqrt{2} U \right| \\ |z| \geqslant \frac{1}{C_\sigma U^{n-1}}. \end{cases}$$

If $M \, |z| \leqslant \sqrt{2} U$, then

$$U \geqslant \left( \frac{M}{\sqrt{2} C_\sigma} \right)^{\frac{1}{n}} = U_M \tag{30}$$

so that

$$\sqrt{n+2} \, \|Z\|_2 \geqslant U_M.$$

On the other hand, if $M \, |z| \geqslant \sqrt{2} U$, then

$$\sqrt{n+2} \, \|Z\|_2 \geqslant \frac{M}{C_\sigma U^{n-1}} - (\sqrt{2} - 1) U$$

with a right-hand member which is decreasing in $U$, hence always greater than its value for $U_M$, which is $U_M$. Thus, if $|z| \neq 0$ we obtain the inequality (29). □

We finish the proof of theorem 10. The theory of LLL reduction gives a quality bound on the short vector output:

**Proposition 15.** *Let $\Lambda$ be a lattice of dimension $n$, and $Z_1$ the first vector of a LLL reduced basis. Then for all non-zero vector $Z$ of $\Lambda$ we have*

$$\|Z_1\|_2 \leqslant 2^n \, \|Z\|_2 .$$

**Proof.** See (von zur Gathen and Gerhard, 2003). Note that the lattice here has dimension $n+1$. □

To make sure that, under the hypotheses of proposition 14, the short vector output by the LLL reduction is $\zeta_m$, we only need to make the inequality

$$\frac{1}{\sqrt{n+1}}\left(\frac{M}{\sqrt{2}C_\sigma}\right)^{\frac{1}{n}} \leqslant 2^n(2nC_{\mathcal{O}}+2)$$

impossible. Therefore we set

$$M > 2^{n(n+1)+1/2}C_\sigma(\sqrt{n+2}(nC_{\mathcal{O}}+1))^n,$$

which concludes the proof of theorem 10.

## 6. Suggested Algorithm

Collecting the results of the previous sections, we suggest the following steps, each one making the algorithm stop if it manages to give a definitive answer.

**Input**: a number field $\mathbb{K}$ with a basis of $\mathcal{O}_{\mathbb{K}}$
**Output**: the order of $\mu(\mathbb{K})$ and the expression of a primitive root $\zeta$
**begin**
  guess $m = \#\mu_{\mathbb{K}}$ with heuristic algorithm 1;
  **if** $m = 2$ **then**
    **return** $(m = 2, \zeta = -1)$;
  **else**
    try algorithm 3;
    **if** *we obtain* $\zeta$ *of order* $m$ **then**
      **return** $(m, \zeta)$;
    **else**
      run the modular algorithm 2;
      **return** *its result* $(m', \zeta)$;
    **end**
  **end**
**end**

**Algorithm 4:** Complete strategy

## 7. Timings

The table 3 below gives the results obtained by the different algorithms studied on a panel of polynomials. The factorisation algorithm means algorithm 2 run after heuristic 1; and lindep refers to algorithm 3, also after the guess of heuristic 1. A star ($\star$) indicates that the test had to be interrupted after long calculations.

These results illustrate the strength of the factorisation algorithm: it always give the result in a reasonable time, even in the case we fooled the heuristic step with fields built on purpose (last lines), compelling it to factor more polynomials. The hybrid approach we suggest amounts to taking the lindep column, and eventually add the factorisation column when there is a failure. It manages to solve quickly all simple cases for which Kannan's algorithm performs well, and remains polynomial in hard cases.

| degree | roots $m$ | factorisation | Kannan | lindep |
|---|---|---|---|---|
| *small fields* | | | | |
| 12 | 36 | 20.0ms | 0.0ms | 20.0ms |
| 32 | 96 | 310.0ms | 30.0ms | 440.0ms |
| *large cyclotomics* | | | | |
| 96 | 194 | 2mn | 690.0ms | 5.2s |
| 180 | 362 | 1.6h | 5.4s | 17.4s |
| *compositum of small fields* | | | | |
| 54 | 18 | 7.7s | $\star > 3$ days | 2.3s |
| 66 | 46 | 17.4s | $\star > 4$ weeks | 1.1s |
| 72 | 24 | 15.3s | 5h27 | *fail* |
| *fields constructed with linear programming* | | | | |
| 24 | 72 | 0.2s | 0.1s | 0.2s |
| 48 | 24 | 11s | 0.2s | 1.7s |
| 54 | 6 | 12s | 0.2s | 2.1s |
| 64 | 4 | 18.6s | 0.4s | 3.3s |
| 64 | 6 | 36.4s | 0.4s | 3.7s |

**Table 3.** comparison of all approaches


## Acknowledgements

The author would like to thank Karim Belabas who has suggested this work, and Régis de la Bretèche for pointing an error in a previous version.


## References


Belabas, K., 2004. A relative van Hoeij algorithm over number fields. J. Symbolic Comput. 37 (5), 641–668.

Cohen, H., 1993. A course in computational algebraic number theory. Vol. 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin.

Fincke, U., Pohst, M., 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math. Comp. 44 (170), 463–471.

Hanrot, G., Stehlé, D., 2007. Improved analysis of Kannan's shortest lattice vector algorithm (extended abstract). In: Advances in cryptology—CRYPTO 2007. Vol. 4622 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 170–186.

Kannan, R., 1985. Lattices, basis reduction and the shortest vector problem. In: Theory of algorithms (Pécs, 1984). Vol. 44 of Colloq. Math. Soc. János Bolyai. North-Holland, Amsterdam, pp. 283–311.

Lagarias, J. C., Odlyzko, A. M., 1977. Effective versions of the Chebotarev density theorem. In: Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975). Academic Press, London, pp. 409–464.

Lang, S., 1964. Algebraic numbers. Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London.

Novocin, A., Stehlé, D., Villard, G., 2011. An LLL-reduction algorithm with quasi-linear time complexity. In: Proceedings of the 43rd annual ACM symposium on Theory of computing. ACM New York, NY, USA, San Jose, United States, pp. 403–412.

Serre, J.-P., 1981. Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. (54), 323–401.

von zur Gathen, J., Gerhard, J., 2003. Modern computer algebra, 2nd Edition. Cambridge University Press, Cambridge.