Archiv der Mathematik

Exceptional units and Euclidean number fields

Julien Houriet

Abstract. By a result of H.W. Lenstra, one can prove that a number field is Euclidean with the aid of exceptional units. We describe two methods computing exceptional sequences, i.e., sets of units such that the difference of any two of them is still a unit. The second method is based on a graph theory algorithm for the maximum clique problem. This yielded 42 new Euclidean number fields in degrees 8, 9, 10, 11 and 12.

Introduction. Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers and $\mathcal{O}_K^*$ be its group of units. An element $u \in \mathcal{O}_K^*$ is said to be an *exceptional unit* if $1 - u \in \mathcal{O}_K^*$. Besides their intrinsic interest, exceptional units have also been studied because they can be used to show that certain algebraic number fields are Euclidean. Indeed, Lenstra has shown that if there exist sufficiently many exceptional units with the property that all of their differences are also units, then the number field is Euclidean with respect to the norm [7]. This method has been used by H.W. Lenstra himself, and by A. Leutbecher, J. Martinet and G. Niklasch ([8], [9], [10], [11]) to obtain many examples of Euclidean number fields of degree at most 10.

The aim of the present paper is to study families of exceptional units in some number fields, of degrees up to 12, and give new examples of Euclidean number fields with Lenstra's method. Some basic tools for this are N. Elkies' new bounds for sphere packings, D. Simon's table of polynomials for number fields of small discriminant and algorithms from graph theory.

1. Exceptional sequences. Let K be a number field with ring of integers $\mathcal{O}_K$ and group of units $\mathcal{O}_K^*$. Let E_K be the set of exceptional units of K, i.e.

$$E_K = \{\omega \in \mathcal{O}_K^* | 1 - \omega \in \mathcal{O}_K^*\}$$

A sequence $\omega_1, \omega_2, \ldots, \omega_m$ of elements in $\mathcal{O}_K$ such that for every $1 \le i < j \le m$, we have $\omega_i - \omega_j \in \mathcal{O}_K^*$ is called an *exceptional sequence in K*. *Lenstra's constant*, denoted by $\Lambda(K)$, is the maximal length of an exceptional sequence in K. We notice that, if $\omega_1, \omega_2, \ldots, \omega_m \in \mathcal{O}_K$ is an exceptional sequence, then the sequence $\left(\omega_i' = \frac{\omega_i - \omega_1}{\omega_2 - \omega_1}\right)_{i=1}^m$ is exceptional as well. So, it is sufficient to consider sequences with $\omega_1 = 0$ and $\omega_2 = 1$. In this case, ω_j is contained in E_K for every $j \ge 3$.

One can also define Lenstra's constants of higher order as follows. For a positive integer k, denote $\Lambda_k(K)$ the maximal length of sequences of algebraic integers of K (not necessarily distinct) such that among any $k+1$ elements of the sequence, there are at least two whose difference is a unit. In particular, we have $\Lambda_1(K) = \Lambda(K)$.

There are upper bounds on the constants $\Lambda_k(K)$. The first one, $\Lambda(K)$, is bounded from above by the smallest norm of a proper ideal of $\mathcal{O}_K$, denoted here by $L(K)$, and, more generally, we have $\Lambda_k(K) \le k \cdot L(K)$, proving finiteness of $\Lambda_k(K)$, for every k. The value of $L(K)$ is easily computable for any number field K.

The set E_K is known to be finite as well ([2] or [12]). There are algorithms to compute it (for example [16], [17]). However the number of exceptional units in the number fields studied in this paper is very large, and, as we only need a sufficiently large lower bound of $\Lambda(K)$, it is enough to get a subset of E_K and then look for large exceptional sequences in it. Our aim in the sequel is to describe a method for computing exceptional sequences in number fields, without entirely computing the set E_K.

2. Euclidean number fields. For a number field K we denote n its degree over $\mathbb{Q}$, $[r_1, r_2]$ its signature, $d(K)$ its discriminant over $\mathbb{Q}$ and $N_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$ the usual number field norm. The field K is embedded in $K \otimes_\mathbb{Q} \mathbb{R}$ which is isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. For an element $\alpha = (\alpha_j)_{j=1}^{r_1+r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ we define $N(\alpha) = \prod_{j=1}^{r_1} |\alpha_j| \prod_{j=r_1+1}^{r_1+r_2} |\alpha_j|^2 \in \mathbb{R}$.

The number field K is said to be *norm-Euclidean* or, for short, *Euclidean*, if its ring of integers is *Euclidean with respect to the absolute value of the norm*, i.e. for every $\alpha, \beta \in \mathcal{O}_K$, $\beta \ne 0$, there exists $\gamma \in \mathcal{O}_K$ such that $\left|N_{K/\mathbb{Q}}(\alpha - \beta\gamma)\right| < \left|N_{K/\mathbb{Q}}(\beta)\right|$.

H.W. Lenstra showed the following theorem giving a condition for a number field to be Euclidean relying on exceptional sequences [7].

Theorem 2.1. *Let K be a number field of degree n and discriminant $d(K)$. Let $U \subset \mathbb{R}^n$ be a bounded Lebesgue measurable set with $\mu(U) > 0$ and such that $N(u - v) < 1$ for all $u, v \in U$. Let $\delta(U)$ be the packing center density of the set U, that is $\delta(U) = \frac{\Delta(U)}{\mu(U)}$, where $\Delta(U)$ is the packing density of U. Then K is norm-Euclidean if the following inequality is satisfied:*

$$\Lambda(K) > \delta(U)\sqrt{|d(K)|}$$

Since it is difficult to compute the packing density of sets, there are few practical choices for the set U. In fact, there are only two "good" sets known. The first is the largest set satisfying the condition of the theorem. This set leads to center densities similar to "Minkowski bounds" $(\delta(U) = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2})$. The second "good" set is a sphere since the topic of packings of spheres is widely studied. The best known upper bounds on sphere packings are provided by H. Cohn and N. Elkies in [3].

Using densities of these two sets and, in (i), the generalization of theorem 2.1 (theorem (1.17) in [7]), we have :

Corollary 2.2. *A number field K is norm-Euclidean if it satisfies one of the following inequalities :*

(i) $\Lambda_k(K) > k \cdot \alpha(n, r_2) \cdot \sqrt{|d(K)|}$ *with* $\alpha(n, r_2) = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2}$, *for some k.*

(ii) $\Lambda(K) > \alpha(n) \cdot \sqrt{|d(K)|}$ *with* $\left(\frac{n}{4}\right)^{\frac{n}{2}} \cdot \alpha(n)$ *the upper bounds on sphere packings given in [3].*

A. Leutbecher and J. Martinet [9] suggest that number fields having small discriminants should have a rather large Lenstra's constant. Therefore, and as a consequence of the formula given in the theorem 2.1 itself, it is natural to apply the algorithm to a list of number fields with small discriminants. In degree larger than 8, there does not exist any systematic list of number fields, but D. Simon has computed a list of irreducible polynomials having small discriminants ([14], [15]), from which one can define number fields with small discriminants.

3. Computations. Two methods were used to construct exceptional sequences. Both were implemented using computer algebra system *PARI/GP* [1].

3.1. First approach. The first method is simple and, consequently, fast. First we compute a system of fundamental units $\{u_1, u_2, \dots, u_m, u_t\}$, with $m = r_1 + r_2 - 1$ and u_t a torsion unit. Then, choosing bounds $a_{\min}$ and $a_{\max}$, we consider every unit of the form $u = u_1^{a_1} \cdot u_2^{a_2} \cdots u_m^{a_m} \cdot u_t^{a_t}$, with $a_{\min} \le a_i \le a_{\max}$ for all $i = 1, 2, \dots, m$ and a_t varying between 0 and the order of u_t. Among these, we keep those for which $1 - u$ is a unit as well, getting a subset F of E_K. To get an exceptional sequence, we then repeat the following steps until F is empty : choose a unit $v \in F$, put in F' the units $u \in F$ satisfying $v - u \in \mathcal{O}_K^*$, replace F by F'.

The crucial point is clearly the way of choosing the unit $v \in F$, so that we get a sequence as long as possible. The first idea is to make this choice randomly.

Sufficiently repeated, this provides exceptional sequences which are long enough to prove that some number fields are Euclidean.

Remark 3.1. The method described above may also be used to compute a lower bound on $\Lambda_2(K)$. We try to compute a lower bound on $\Lambda_2(K)$ when $2m + 1 > 2 \cdot \alpha(n, r_2) \cdot \sqrt{|d(K)|}$, where m is the length of the longest sequence that we found. If this is verified, we try to find an exceptional sequence $\{0, 1, \omega_3, \dots, \omega_{m-1}\}$ and two units u_1 and u_2 such that $\omega_i - u_j \in \mathcal{O}_K^*$ for all i and j. Then, take an exceptional units v satisfying, say, $u_1 - v \in \mathcal{O}_K^*$ and search for another exceptional sequence of length $m - 1$ among the exceptional units w satisfying $u_1 - v \in \mathcal{O}_K^*$. This gives a set of $2m + 1$ units such that among any three of them there are at least two whose difference is a unit. This proves that the number field K is Euclidean. This method may be generalized for higher order Lenstra's constants.

Remark 3.2. A problem appearing with the first approach is that it provides sequences which look very complicated, and, in particular, useless in the point of view of the previous articles on this subject. Indeed, as written by Leutbecher and Martinet, a search for fields with long exceptional sequence often reveals fields with small discriminants. So, if we could identify some new sequences, it should be possible to construct new number fields having small discriminant, and maybe not appearing in D. Simon's lists. From this point of view, instead of computing an arbitrary system of fundamental units, we tried to construct a system of units which are written as simple as possible on the integral basis of the number field. Then we tried to find exceptional sequences among units being products of not too many fundamental units. Unfortunately, even using the method described in the sequel, we were not able to identify new exceptional sequences and find some number fields not appearing in D. Simon's table.

3.2. Approach by the theory of graphs. The second method is based on algorithms from graph theory searching the maximum clique in a given graph and on the principle given by H. W. Lenstra in [7], that, if we have some exceptional units, then we may compute more by some simple rules.

One can associate a graph with a set of exceptional units as in [8], that is vertices of the graph are exceptional units and two vertices u and v are connected if $u - v \in \mathcal{O}_K^*$. In this way, an exceptional sequence is exactly a clique in this graph, that is a subgraph in which any two vertices are connected. Finding the maximum clique is known to be a NP-hard optimization problem. Among all the algorithms written on this problem, two were used in our work, a branch-and-bound method [4] and a variable neighborhood search [5].

On another side, the following proposition ([7] et [9]) may be used in order to construct subsets of E_K.

Proposition 3.3. *Let K be a number field and E_K the set of exceptional units. We have:*

(i) *Let G be the group generated by $x \mapsto 1 - x$ and $x \mapsto x^{-1}$, which is isomorphic to the symmetric group S_3. The action of G on E_K is faithful unless $\sqrt{-3} \in K$. So, if $u \in E_K$ then the six (resp. two) elements su, for $s \in G$, belong to E_K if $\sqrt{-3} \notin K$ (resp. $\sqrt{-3} \in K$).*

(ii) *Let $(u, v) \in E_K$ satisfying $u - v \in \mathcal{O}_K^*$, then the three following units uv^{-1}, $(1 - u)(1 - v)^{-1}$ and $(1 - u^{-1})(1 - v^{-1})^{-1}$ belong to E_K as well.*

3.2.1. Description of the method. The method is the following. First we construct a small subset F of E_K containing products of only some fundamental units and their orbit under the action of G, and compute the associated graph. Then we apply the branch-and-bound algorithm [4] which is an improved exhaustive search. The result is the maximal exceptional sequence in F. The algorithm ends here if a stopping condition is satisfied, and else the variable neighborhood search [5] is applied.

This algorithm consists in computing another subset of E_K, constructed around the maximal previously found clique, denoted by C. This means that we compute exceptional units from the previously found exceptional units using the above proposition. Initializing d at $\#C - 1$, we keep only the ones which are "connected" with at least d units of C. Then we compute the maximal clique in this new subset of E_K. This clique may be C itself. Then, until a stopping condition is met, decrease the value of d and repeat these operations.

The main stopping conditions is the size of C. That is achievement either of the theoretical bound given by the smallest ideal norm or of the bound allowing proof that the number field is Euclidean. Other stopping conditions used here are elapsed time and size of the graphs to be taken in account.

4. Results. Tables 1 to 6 contain the number fields K for which we could find an exceptional sequence long enough to prove that K is Euclidean.

TABLE 1. Euclidean number fields of degree 8 and signature [4,2]

$d(K)$	$a_0, a_1, \dots, a_8$									α	$\Lambda \geq$	L
15297613	−1,	−2,	1,	5,	2,	−6,	−3,	2,	1	15.23	17	25
15908237	−1,	−1,	3,	1,	−9,	4,	6,	−5,	1	15.53	16	23
16324589	−1,	4,	4,	−11,	−6,	11,	1,	−4,	1	15.74	16	23
16374773	−1,	−2,	0,	7,	4,	−5,	−4,	1,	1	15.76	16	17
16526789	−1,	0,	3,	0,	0,	−1,	−3,	0,	1	15.83	16	19
16623109	1,	−8,	4,	14,	−17,	−1,	11,	−6,	1	15.88	17	23
16643125	1,	1,	0,	−1,	0,	2,	−2,	−1,	1	15.89	16	19
16706269	−1,	−6,	−6,	13,	11,	−9,	−6,	2,	1	15.92	16	19

We found exactly the same number fields using the two methods. The columns respectively give, the discriminant of the number field, the coefficients of the polynomial $P(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n$ defining the number field, the bound α

Table 2. Euclidean number fields of degree 8 and signature [4,2], with Λ_2

$d(K)$	$a_0, a_1, \ldots, a_8$									2α	$\Lambda_2 \geq$	$2L$
16877741	1,	−2,	−3,	5,	7,	−4,	−5,	1,	1	32.00	33	46
16981229	1,	−2,	1,	15,	3,	−14,	−6,	2,	1	32.10	33	46
17025973	−1,	−5,	−9,	−9,	−7,	−2,	1,	2,	1	32.14	33	46
17318125	−1,	−5,	4,	13,	−5,	−11,	1,	4,	1	32.42	33	38

Table 3. Euclidean number fields of degree 9 and signature [3,3]

$d(K)$	$a_0, a_1, \ldots, a_9$										α	$\Lambda \geq$	L
−109880167	−1,	−2,	0,	3,	1,	−3,	1,	1,	−2,	1	16.08	17	29
−110852311	1,	3,	−2,	−8,	−1,	8,	2,	−4,	−1,	1	16.15	18	27
−111543479	1,	0,	1,	2,	1,	−2,	−3,	−1,	1,	1	16.20	18	23
−112700719	−1,	0,	4,	−12,	5,	22,	−37,	25,	−8,	1	16.29	17	23
−112978759	1,	−1,	−3,	3,	1,	−5,	3,	2,	−3,	1	16.31	17	23
−112992391	−1,	2,	−4,	2,	3,	−6,	3,	1,	−2,	1	16.31	17	27
−113501567	−1,	0,	4,	1,	−3,	0,	1,	−1,	−1,	1	16.35	17	25
−113511599	−1,	−1,	9,	0,	−18,	2,	13,	−3,	−3,	1	16.35	17	23
−113931487	1,	1,	2,	0,	−1,	−1,	−2,	0,	0,	1	16.38	17	25
−114479303	−1,	9,	−27,	18,	27,	−23,	−16,	7,	6,	1	16.42	18	23
−114807607	−1,	0,	−4,	2,	12,	−1,	−11,	−2,	3,	1	16.44	17	23
−115041127	1,	4,	0,	−7,	5,	−5,	0,	7,	−5,	1	16.46	17	27
−115270559	1,	1,	−1,	−9,	2,	14,	−1,	−7,	0,	1	16.47	17	19
−115691111	−1,	−1,	−2,	−1,	1,	5,	2,	−4,	−1,	1	16.50	17	25
−116188367	1,	0,	−1,	1,	3,	1,	−3,	−2,	0,	1	16.54	17	23
−118246927	1,	−3,	1,	6,	−7,	−6,	8,	2,	−4,	1	16.68	17	23
−121510799	−1,	0,	2,	3,	−1,	−5,	−4,	1,	3,	1	16.91	17	19

Table 4. Euclidean number fields of degree 10 and signature [2,4]

$d(K)$	$a_0, a_1, \ldots, a_{10}$											α	$\Lambda \geq$	L
799905449	−1,	−1,	0,	1,	−1,	−1,	1,	1,	0,	−1,	1	16.80	17	25
801214577	1,	−1,	−1,	4,	−3,	1,	0,	−1,	3,	−3,	1	16.82	18	29
801589013	−1,	3,	−2,	2,	0,	−9,	0,	2,	2,	3,	1	16.82	17	25
802448461	−1,	−3,	0,	5,	1,	−4,	1,	2,	−2,	−1,	1	16.83	17	25
803282693	−1,	4,	−6,	4,	2,	−8,	12,	−11,	7,	−3,	1	16.84	18	29
809040437	1,	0,	−1,	−1,	3,	0,	−4,	4,	0,	−2,	1	16.90	17	29
814270253	1,	1,	−3,	1,	5,	−5,	−1,	4,	−2,	−1,	1	16.95	17	23
817298432	−1,	0,	−1,	2,	1,	0,	0,	−2,	1,	0,	1	16.99	17	23
838803593	−1,	1,	2,	−1,	−1,	−1,	1,	3,	−2,	−1,	1	17.21	18	29

TABLE 5. Euclidean number fields of degree 11 and signature [1,5]

$d(K)$	$a_0, a_1, \ldots, a_{11}$											α	$\Lambda \geq$	L
–5781612911	–1,	3,	–6,	7,	–7,	7,	–8,	6,	–3,	2,	–2,	1	17.29	18	29
–5807103943	–1,	1,	0,	–3,	2,	2,	–4,	0,	3,	–1,	–1,	1	17.33	18	29
–5901091967	1,	–3,	3,	2,	–6,	4,	2,	–5,	3,	1,	–2,	1	17.47	18	29
–5939843699	–1,	0,	1,	1,	3,	0,	–1,	–2,	–2,	1,	0,	1	17.52	18	29
–5999947987	1,	–2,	2,	1,	–5,	5,	1,	–5,	3,	1,	–2,	1	17.61	18	29
–6046447999	–1,	2,	–4,	4,	–6,	5,	–5,	4,	–2,	3,	0,	1	17.68	18	19

TABLE 6. Euclidean number fields of degree 12 and signature [0,6]

$d(K)$	$a_0, a_1, \ldots, a_{12}$												α	$\Lambda \geq$	L
41223887921	1,	–3,	4,	–3,	4,	–7,	8,	–5,	2,	–1,	2,	–2,	1	17.48	19	37
42058512657	1,	5,	13,	25,	39,	52,	59,	57,	47,	30,	15,	5,	1	17.66	18	31
42194001221	1,	–4,	10,	–17,	22,	–24,	24,	–21,	17,	–12,	7,	–3,	1	17.69	18	31
42925852301	1,	–1,	–2,	2,	3,	–2,	–1,	–1,	1,	3,	–2,	–1,	1	17.84	18	29

given by theorem 2.1, the length of the longest found exceptional sequence and the smallest norm of a proper ideal of $\mathcal{O}_K$. The value of α is given by Minkowski's bound, denoted by $\alpha(n, r_2)$ in section 2, in degree 8 and by the center density of spheres for degree 9 to 12. In degree 8, when the computed exceptional sequences failed to achieve the required bound but was close enough (see remark 3.1), we computed lower bounds for the second Lenstra's constant. This was successful for the four number fields of table 2.

In degree 8 and 9, some of these number fields were already proven to be Euclidean. This is the case for four of the number fields of degree 8 and for two of degree 9. So these tables give 42 new Euclidean number fields, and, in particular, give the first examples of Euclidean number fields of degree 10 and signature [2,4], and of degree 11 and signature [1,5].

Remark 4.1. Number fields appearing in tables 1 to 6 have unit rank $r_1 + r_2 = 6$. We computed exceptional sequences in some number fields with small discriminant and $r_1 + r_2 > 6$ as well. We could observe that, for a given degree, maximal length of an exceptional sequence grows with unit rank. However the increase appeared to be of at most one or two units as the required bounds are multiplied by a factor between 1.5 and 2, when increasing unit rank by one (except for totally real number fields, bounds given in [13] being smaller). So it seems hopeless to show that some number fields with $r_1 + r_2 > 6$ are Euclidean with this method. Nevertheless it is interesting to note that we can find longer exceptional sequences considering number fields with greater unit rank. As an example, table 7 gives lower bounds on Lenstra's constants for number fields of smallest discriminant in degree 9.

TABLE 7. Bounds on Lenstra's constant in degree 9

$[r_1, r_2]$	$d(K)$	α	$\Lambda \geq$	L
[1,4]	29510281	8.49	**16**	23
[3,3]	–109880167	16.38	**18**	29
[5,2]	453771377	32.35	**19**	25
[7,1]	–1904081383	52.04	**21**	37
[9,0]	9685993193	39.07	**22**	27

References

[1] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN AND M. OLIVIER, PARI/GP, online available at: http://pari.math.u-bordeaux.fr/.

[2] S. CHOWLA, Proof of a conjecture of Julia Robinson. Norske Vid. Selsk. Forh. (Trondheim) **34**, 100–101 (1961).

[3] H. COHN AND N. ELKIES, New upper bounds on sphere packings I. Ann. of Math. (2) **157**(2), 689–714 (2003).

[4] T. FAHLE, Simple and fast: improving a branch-and-bound algorithm for maximum clique. Algorithms—ESA 2002, 485–498, Lecture Notes in Computer Science, 2461, Springer-Verlag, Berlin, 2002.

[5] P. HANSEN, N. MLADENOVIĆ AND D. UROŠEVIĆ, Variable neighborhood search for the maximum clique. Discrete Appl. Math. **145**(1), 117–125 (2004).

[6] F. LEMMERMEYER, The Euclidean algorithm in algebraic number fields. Expo. Math. **13**, 385–416 (1995).

[7] H. W. LENSTRA, Euclidean number fields of large degree. Invent. Math. **38**, 237–254 (1977).

[8] A. LEUTBECHER, Euclidean fields having a large Lenstra constant. Ann. Inst. Fourier (Grenoble) **35**, 83–106 (1985).

[9] A. LEUTBECHER AND J. MARTINET, Lenstra's constant and Euclidean number fields. Journées arithmétiques Metz, Astérisque, **94**, 87–131 (1982).

[10] A. LEUTBECHER AND G. NIKLASCH, On cliques of exceptional units and Lenstra's construction of Euclidean fields. Number Theory Ulm 1987, Lecture Notes Math. **1380**, 150–178 (1989).

[11] J. MARTINET, Sur la constante de Lenstra des corps de nombres, Sém. de théorie des nombres de Bordeaux, 1979–1980, exp. 17, Univ. Bordeaux I, Talence, 1980.

[12] T. NAGELL, Sur une propriété des unités d'un corps algébrique. Ark. Mat. **5**, 343–356 (1964).

[13] G. Niklasch and R. Quême, An improvement of Lenstra's criterion for Euclidean number fields: The totally real case, Acta Arith. **58**, 443–446 (1991).

[14] D. Simon, Table de petits Discriminants de Polynômes Irréductibles. http://www.math.unicaen.fr/simon/maths/TableSmallDisc.html.

[15] D. Simon, Équations dans les corps de nombres et discriminants minimaux. Thèse, Univ. Bordeaux I, 1998.

[16] N. P. Smart, The solution of triangularly connected decomposable form equations. Math. Comp. **64**, 819–840 (1995).

[17] K. Wildanger, Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. J. Number Theory **82**(2), 188–224 (2000).

Julien Houriet, Ecole Polytechnique Fédérale de Lausanne, Chaire de structures algébriques et géométriques, CH-1015 Lausanne, Switzerland
e-mail: `julien.houriet@epfl.ch`