Family Portraits of Exceptional Units

Gerhard Niklasch

Mathematisches Institut / SCM
Technische Universität München
80290 München
GERMANY

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI 95-117

Family Portraits of Exceptional Units

Gerhard Niklasch

Mathemat. Institut / SCM, Technische Universität München,
D–80290 München, Germany

Oct.–Dec. 1995: Max-Planck-Institut für Mathematik,
Gottfried-Claren-Str. 26, D–53225 Bonn, Germany

E-mail: <nikl@mathematik.tu-muenchen.de>

Abstract

The number of solutions of the "unit equation" $x+y=1$ in units of (the ring of integers of) an algebraic number field of degree n and unit rank r is known to be bounded above by an exponential function of n or r, but the best known lower bounds yield merely some fields with at least a constant times r^3 solutions, or infinitely many fields of each degree with at least a constant times n solutions.

We will present some data about solution numbers in various individual fields of low degree, and then outline a programme for obtaining more general results. This involves the study of parametric families of polynomials defining fields in which the unit equation has certain forced solutions, and applying Baker's method and diophantine approximation techniques to show that for almost all parameter values, these fields contain no other solutions than the forced ones.

1. Introduction

In spite of a 66-year history of research — the unit equation $x+y=1$, to be solved in invertible algebraic integers, first appears in C. L. SIEGEL 1929 [33] — not very much is known in general about how many solutions $x, 1-x$ it can have in any given algebraic number field. (Such x are called *exceptional units*, a term introduced by T. NAGELL in 1969 [25].) Siegel already knew that their number in any given field is finite, an easy consequence of Satz 7, Zusatz 1 of his dissertation [32], and it follows from A. BAKER's theory of linear forms in logarithms that the solutions are effectively computable, which was first made explicit by K. GYŐRY in the 1970s [13]. J. H. EVERTSE proved in 1983 [6,7] that the number of solutions is at most $3 \cdot 7^{n+2r+2}$, where $n = [K : \mathbf{Q}]$ is the degree and r the rank of the group of units of the field K. (By DIRICHLET's theorem, $r = r_1 + r_2 - 1$ if the field has r_1 real and r_2 pairs of complex embeddings; since $r_1 + 2r_2 = n$, we have $n/2 \le r+1 \le n$.) Although the numbers 3 and 7 can be reduced somewhat, EVERTSE's bound has not yet been improved in substance; all known upper bounds are of this form — exponential in n or in r or in some combination of n and r.

EVERTSE's method, which does not produce effective bounds for the solutions themselves, applies to a wider class of equations. In particular, his bound remains valid for the

S-unit equation $x + y = 1$ where now x and y range over the subgroup of elements of $K^\times$ which are integral with integral inverse at all places except those in the finite set S. The rank of this group is $r + s$ where s is the number of finite places in S, and the exponent $n+2r+2$ in the bound has to be replaced accordingly by $n+2(r+s+1)$. In this situation, one has at least a subexponential lower bound as far as the dependence on s is concerned, i.e., when we keep the field K fixed and let S grow by inserting suitable primes. Clearly it suffices to consider $K = \mathbf{Q}$ here. This bound is due to P. ERDŐS, C. L. STEWART and R. TIJDEMAN 1988 [5]. It says that by choosing S carefully, one can produce at least a constant times $\exp\bigl((4 + o(1))(s/\log s)^{1/2}\bigr)$ solutions.

Unfortunately, it is very much harder to exhibit large numbers of solutions when we restrict ourselves to ordinary units and let K vary among the fields of a given degree n and unit rank r. A lower bound which is valid for infinitely many fields of any given degree n, but which is merely linear in n, is straightforward to establish (see section 2 below); moreover, the maximal real subfields of cyclotomic fields of prime level possess at least a constant times n^3 exceptional units [28], but this applies to at most one field up to isomorphism of given degree.

To the extent that numbers of exceptional units (e.u.s) in individual fields are known — a survey is presented in section 3 — they seem to suggest that the true rate of growth of the largest number of solutions for a given signature (n, r) is somewhat faster than polynomial, and that the maximum should be attained by one or more fields near the smallest absolute field discriminant in that signature. We can also ask for a sharp upper bound on the number of e.u.s valid for all but finitely many fields of a given signature. Experimental data suggest that this latter bound tends to be rather smaller than the former. It is in order to study this kind of bound that we will consider parametric families of number fields containing e.u.s of a prescribed form in section 4. In the final section, we indicate some possible further developments, point out some stumbling blocks, and provide a few links to related topics.

Much work remains to be done here, and this article offers more conjectures and heuristics than definite results. We hope to be able to present some theorems in the not too distant future.

Acknowledgements. The question, "How many exceptional units... ?", was first posed to the author by K. GYŐRY in 1989, and since then repeatedly by several others, in conversation and in correspondence.

Some of the computational results of this paper were obtained with the aid of Maple V.3 running on a Sun SPARCstation ELC; a few last-minute checks involved Maple and PARI/GP on a Sun SPARCclassic.

I would like to thank the organisers of the 19$^{\text{èmes}}$ *Journées Arithmétiques* for all their efforts which have succeeded in providing a very enjoyable and fertile atmosphere during the conference. The `telnet` terminals they kindly made available to the participants were instrumental in carrying out, between lectures, some of the computations on which section 3 is based. This article was written while the author was a guest at the Max-Planck-Institut für Mathematik in Bonn whose support in terms of desk space, computer

facilities, finance, and creative atmosphere throughout the day, seven days a week, it is my great pleasure to acknowledge.

2. Basic facts

First we recall some well-known simple properties of exceptional units. (See [19] and the references cited there for more details.) Let R be a commutative ring with an identity element 1 for multiplication; write $R^\times$ for its group of units and

$$E(R) = R^\times \cap (1 - R^\times)$$

for the set of exceptional units of R. Homomorphisms of such rings are understood to preserve identity elements.

2.1 Lemma. a) *If $x \in E(R)$ is an exceptional unit, then so are*

$$x^i := 1/x\,, \quad x^j := 1 - x\,, \quad x^k := x/(x-1)\,, \quad x^{ij} = 1 - 1/x\,, \quad x^{ji} = 1/(1-x)\,.$$

These are distinct unless either $x^2 - x + 1 = 0$, in which case we have $x = x^{ij} = x^{ji}$ and $x^i = x^j = x^k$, or $1{+}1 \in R^\times$ and $x \in \{-1, 1{+}1, (1{+}1)^{-1}\}$, when $x = x^i$ or x^k or x^j, respectively. We write

$$\mathcal{H} = \langle i, j, k\,;\ i^2 = j^2 = k^2 = (ij)^3 = ijik = \mathrm{id}\rangle$$

for this nonabelian group of order 6 of homographic transformations.

b) *Ring homomorphisms map units to units and exceptional units to exceptional units.* ∎

In general, a surjective ring homomorphism need not induce a surjective morphism between the groups of units, and b) can then be replaced with a stronger statement. This will not be needed here. Note that b) applies in particular to automorphisms of R.— It will always be clear from the context whether i, j, k are used to denote the involutions in $\mathcal{H}$ or carry some other meaning.

Clearly b) will prevent R from possessing any exceptional units at all if there exist an epimorphic image ring of R without exceptional units, e.g., if R has an ideal of index 2. Since many algebraic number fields have ideals (of their maximal orders) of norm 2, there is no hope of a nontrivial lower bound for the number of exceptional units in *all* fields of a given degree and unit rank. The best we can hope for are lower bounds which apply to infinitely many nonisomorphic fields of the same signature.

Now let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial, x a root of f (in some fixed algebraic closure of $\mathbf{Q}$) and $\mathbf{Z}[x]$ the subring of the ring of integers of the number field $K = \mathbf{Q}(x)$ generated by x. The intersection of $\mathbf{Z}[x]$ with the group of units of K is a subgroup of finite index and hence of full rank. In particular, whenever an element of $\mathbf{Z}[x]$ is invertible in the full ring of integers of K, then it is already a unit of $\mathbf{Z}[x]$.

2.2 Lemma. a) *If $g \in \mathbf{Z}[X]$ is such that $g(x) \in \mathbf{Z}[x]^\times$, then the canonical homomorphism from $\mathbf{Z}[X]$ onto $\mathbf{Z}[x]$ which takes X to x extends to a unique homomorphism of the ring* *of Laurent polynomials* $\mathbf{Z}[X][g^{-1}]$ *onto* $\mathbf{Z}[x]$. *The same is true, mutatis mutandis, when the single polynomial* g *is replaced with a subset of nonconstant elements of* $\mathbf{Z}[X]$.

b) [19] *The exceptional units* $x \in E(R)$ *are in one-to-one correspondence with the homomorphisms from the ring* $\mathbf{Z}[X][X^{-1}, (1-X)^{-1}]$ *into* R.

c) [16, Lemma (2.5)] *If* $g \in \mathbf{Z}[X]$ *is also monic and irreducible, and if* y *denotes a root of* g, *then* $g(x)$ *is a unit in* $\mathbf{Z}[x]$ *if and only if* $f(y)$ *is a unit in* $\mathbf{Z}[y]$.

PROOF of c): $g(x) \in \mathbf{Z}[x]^\times$ if and only if the norm $N_{K|\mathbf{Q}}(g(x))$ is ± 1, if and only if the resultant of f and g is ± 1, and this last condition is symmetric in f and g when both are monic. (By analogy with function fields [35, Ex. 2.11], this might be called "Weil reciprocity".) ∎

Combining a) and c), we see that the monic irreducible polynomial $f \in \mathbf{Z}[X]$ is the minimal polynomial of an exceptional unit if and only if $f(0), f(1) \in \{\pm 1\}$. The following proposition is an immediate consequence.

2.3 Proposition. *The only exceptional units in (the rings of integers of) quadratic number fields are the roots of the four polynomials*

$$X^2 - X + 1\,,\quad X^2 - X - 1\,,\quad X^2 + X - 1\,,\quad X^2 - 3X + 1\,;$$

i.e., the sixth roots of unity $\zeta_6^{\pm 1}$ *and the* $\mathcal{H}$*-orbit of the golden ratio* $\vartheta = \frac{1}{2}(1+\sqrt{5})$. ∎

In [19] it is shown how one can compute the exceptional units (e.u.s from now on) of rings of Laurent polynomials (finitely generated quotient rings of $\mathbf{Z}[X]$). Here are a few such rings which we will use below. In each case the claim that the elements listed are indeed e.u.s is trivial, and the claim that there are no others can be verified by a tedious but straightforward computation.

2.4 Proposition. a) *The ring* $\mathbf{Z}[X][X^{-1}, (X-1)^{-1}]$ *from* 2.2 b) *contains only the six built-in e.u.s.*

b) *The ring*

$$\mathbf{Z}[X]\big[X^{-1},\,(X-1)^{-1},\,(X+1)^{-1}\big]$$

contains 18 *e.u.s, whose orbits under the action of* $\mathcal{H}$ *are represented by* X, $-X$ *and* X^2. (Thus homomorphisms out of this ring classify what J.-D. THÉROND has called *unités vraiment exceptionnelles* [39].)

c) *The ring*

$$\mathbf{Z}[X]\big[X^{-1},\,(X-1)^{-1},\,(X^2-X+1)^{-1}\big]$$

contains 24 *e.u.s, represented by* X *and the results of substituting* X^i, X^j *and* X^k *for* X *into* $X^2 - X + 1$. *On this ring,* $\mathcal{H}$ *acts as a group of automorphisms from the left, with* $i \in \mathcal{H}$ *corresponding to the substitution* $X \mapsto X^i$, *etc.* (In fact, it gives the whole automorphism group of the ring, but we will not need this.)

d) *The ring*

$$\mathbf{Z}[X]\big[X^{-1},\,(X-1)^{-1},\,(X+1)^{-1},\,(X^2-X-1)^{-1}\big]$$

contains 48 *e.u.s, those from* b) *and the* $\mathcal{H}$*-orbits of* $X(X-1)$, $(X-1)^2(X+1)$, $(X^2-1)/X$, $(X+1)/X^2$, *and* $(X+1)^2(X-1)/X^3$. ∎

By generalizing the progression from a) to b), we obtain the following weak lower bound for the number of e.u.s in infinitely many fields of any prescribed degree $n > 2$.

2.5 Proposition. *For each* $n \geq 3$, *infinitely many number fields of degree* n *contain at least* $12n - 30$ *e.u.s.*

PROOF: Fix n and consider the set of monic polynomials $f \in \mathbf{Z}[X]$ of degree n which satisfy $f(0) = \ldots = f(n-2) = 1$. It is easy to see that there is one such polynomial for each integer value prescribed for the coefficient of X^{n-1} in f. At most finitely many of them can be reducible, because any nontrivial factor g of such an f would have to take values ± 1 at each of $0, \ldots, n-2$ and thus would have to come from among a finite set of candidates. Also, any field generated by a root of an irreducible f can contain roots of only finitely many others, since otherwise it would contain infinitely many e.u.s. It follows that infinitely many nonisomorphic fields of degree n possess a subring $\mathbf{Z}[x]$ of algebraic integers which receives an epimorphism from the ring

$$R = \mathbf{Z}[X][X^{-1}, (X-1)^{-1}, \ldots, (X-n+2)^{-1}].$$

Without looking too hard, we can see at least $2n - 5$ $\mathcal{H}$-orbits of e.u.s in R, represented by X, $X-1$, ... , $X-n+3$ and by $(X-1)^2$, ... , $(X-n+3)^2$. It remains to show that these will sufficiently often map to distinct elements of $\mathbf{Z}[x]$ under the substitution $X \mapsto x$. But if, picking one example at random, it should happen that $x/(x-1) = (x-3)^2$, then

$$(X-3)^2(X-1) - X = X^3 - 7X^2 + 14X - 9$$

is in the kernel of that substitution, and x lives in the cubic number field of discriminant -31 (which shows that this particular coincidence could not have happened at all — the elements we had used exist only for $n \geq 6$). In the same way one shows that every identification of two e.u.s of R under $X \mapsto x$ forces x to be a root of a particular polynomial, and even determines the field $\mathbf{Q}(x)$ up to isomorphism when this polynomial is irreducible. Thus we lose only finitely many of the remaining examples.— At least for $3 \leq n \leq 5$, the Laurent ring used here has exactly $12n - 30$ e.u.s. ∎

2.6 Remark. J. H. SILVERMAN [36] has recently obtained an upper bound for the number of e.u.s which can be powers of a fixed algebraic unit, and more generally for the number of exponents $m > 0$ such that $x^m - 1 \in \mathbf{Z}[x]^\times$ for a fixed algebraic integer x, which depends on x only via the degree $n = [\mathbf{Q}(x) : \mathbf{Q}]$ and which is of the form $c \cdot n^{1+o(1)}$ with an effectively computable absolute constant c. But, as he points out himself, his approach does not seem to generalize to our situation.

3. Numbers of exceptional units in fields of small rank

We have already seen that among the fields of unit rank $r = 0$, only $\mathbf{Q}(\zeta_6)$ contains any exceptional units at all, that one real quadratic field ($r = 1$) contains 6 e.u.s, and that all other fields of degree $n = 2$ and rank 1 contain none. The cubic fields with exceptional units are given by four families of monic irreducible cubic polynomials, one family for each choice of signs in the conditions $f(0) \in \{\pm 1\}$, $f(1) \in \{\pm 1\}$, with each family depending on a single integer parameter. The action of $\mathcal{H}$ permutes three of the families and fixes the fourth, and this latter produces only cyclic (hence real, hence rank two) cubic fields, whereas the former are responsible for 12, 6 and 18 e.u.s in the rank-one cubic fields of discriminants -23, -31 and in the cyclic cubic field of discriminant $+7^2$, respectively, and define real non-cyclic cubic fields for all other parameter values. These families have been the subject of numerous studies, e.g., in roughly chronological order, by NAGELL [24,25], SHANKS [31], M.-N. GRAS [10,11], ENNOLA [4], E. THOMAS [40], MIGNOTTE [21] and the present author [27]. The main result of [27] is that cyclic cubic fields contain at most 6 e.u.s — as was known already to NAGELL, infinitely many cyclic cubic fields *do* contain at least 6 e.u.s — except for the four such fields of smallest discriminants 7^2, 9^2, 13^2, 19^2, which contain 42, 18, 12 and 12 e.u.s, respectively. NAGELL conjectured that non-cyclic real cubic fields contain either 6 e.u.s or none (and, equivalently, that for the three non-cyclic families of polynomials, distinct parameter values — apart from the action of $\mathcal{H}$ — always lead to nonisomorphic fields). Again, it is clear from the families of polynomials that infinitely many such fields do contain at least 6 e.u.s. The conjecture is still open despite a lot of work [4]. The methods of [27] ought to show that it holds at least up to finitely many exceptions, but treating the potentially exceptional cases may involve a very large computational effort. We will briefly return to this issue in section 5.

In [22] and [23], NAGELL proceeded to determine all e.u.s in the third type of fields of unit rank one, *viz.* totally complex quartic fields. Here one encounters a new phenomenon. Indeed, in contrast to real quadratic and complex cubic fields, infinitely many totally complex quartic fields contain e.u.s. But this is due to the fact that each of the quadratic fields $\mathbf{Q}(\theta)$ and $\mathbf{Q}(\zeta_6)$ possesses infinitely many distinct quadratic extensions which are totally complex. If one counts only those e.u.s which generate quartic fields over $\mathbf{Q}$, the result is the same as for the other rank-one fields: There are only finitely many complex quartic fields with exceptional units *not contained in proper subfields.*

A pattern is beginning to emerge. What we should expect to find in any given signature is: several fields with small absolute discriminants which contain many e.u.s, infinitely many which contain rather smaller numbers of them, and infinitely many fields which contain none at all, where we are careful to count only e.u.s which generate the fields under consideration for the latter two types of fields. We will see in a moment how this pattern continues into ranks $2 \ldots 3$ and degrees $4 \ldots 5$.

3.1 Remark. In [24], NAGELL wrote: *"Il est intéressant d'observer que les valeurs maximales* [du nombre d'unités exceptionnelles dans un corps] *sont obtenues pour les corps biquadratiques du premier rang qui possèdent les discriminants les plus petits."* This observation extends far beyond the cases known to NAGELL. A. LEUTBECHER and J. MARTINET [18,17] have noted that it can be turned around to discover number fields with small absolute discriminants in degrees up to 11, and recently A. ZIEGLER, a diploma student of LEUTBECHER, has reached degree 15 [26]. It is still not well understood why this kind of heuristics is so successful; it will become obvious in a moment why fields with very many e.u.s should be expected to have small discriminants, but it is far from clear what causes these fields to exist at all. ∎

Let us summarise the above in the first half of a little table. We list fields by increasing absolute discriminant within each signature, and indicate the total numbers of e.u.s as well as the numbers of e.u.s not contained in proper subfields (for complex quartic fields, in square brackets). The discriminants are the signed, slanted figures, the numbers of e.u.s are unsigned and upright, and are highlighted by boldface type to indicate the largest number attained within the signature and the largest number attained infinitely often.— Within the range of the table, there is only one field (up to isomorphism) of given signature and discriminant.

3.2 Table, part I.

Rank $r = 0$, degree $n = 2$:
-3: **2** | $-4, \ldots$: **0**
Rank $r = 1$, degree $n = 2$:
$+5$: **6** | $+8, \ldots$: **0**
Rank $r = 1$, degree $n = 3$:
-23: **12** | -31: 6 | $-44, \ldots$: **0**
Rank $r = 1$, degree $n = 4$:
$+117$: **20** [18] | $+125$: 18 [12] | $+144$: 14 [2] | $+189$: 8 [6] | $+225$: 8 [0] | $+229$: 6 | $+256$: 0 [0] | $+257$: 0 | $+272$: 6 [0] | $+320, \ldots$: 0, 2 or 6 [**0**]
Rank $r = 2$, degree $n = 3$:
$+7^2$: **42** | $+9^2$: 18 | $+148$: 0 | $+13^2$: 12 | $+229$, $+257$, $+316$, $+321$: 0 | $+19^2$: 12 | $+404, \ldots$: 0 or **6**, conjecturally; $+31^2, \ldots$: 0 or **6**

Until quite recently, there were hardly any data about numbers of e.u.s in fields of larger degree. Quartic fields of mixed signature with a real quadratic subfield are the subject of a study which the author has been pursuing since 1991; a detailed report will be submitted in due course. Just before and during the Journées Arithmétiques at Barcelona, the author made an effort to determine at least the "small" e.u.s in several quintic fields of rank 2. Thus we can now extend the table, albeit somewhat tentatively.

Only for five of the fields listed below is the number of e.u.s known exactly. The field $\mathbf{Q}(\sqrt{\vartheta})$ of discriminant -400 is very unusual in that it has e.u.s of degree 4, is not a cyclotomic field, and can nevertheless be handled entirely by elementary arguments. The extension of $\mathbf{Q}(\vartheta)$ of discriminant -275 was treated in the author's doctoral dissertation. Both fall of course within the scope of the aforementioned study. For $\mathbf{Q}(\zeta_7)$ and $\mathbf{Q}(\zeta_9)$, see GYŐRY 1971 [12, Lemme 12], together with the known numbers of e.u.s in their real cubic subfields from [25]. The real subfield of the eleventh cyclotomic field is included here courtesy of B. M. M. DE WEGER [pers. comm.]; there are another 90 non-real e.u.s in $\mathbf{Q}(\zeta_{11})$.

Thanks to recent advances in transcendence theory and diophantine approximation, the routine determination of all exceptional units in a few dozen fields is now rather less of a computational chore than it used to be, and we hope soon to be able to eliminate the "$\geq$" signs. (Since "large" solutions tend to be extremely rare, I do not actually expect any of the numbers to increase, and have used boldface as before for the largest numbers seen.)

3.3 Table, part II.

Rank $r = 2$, degree $n = 4$:

−275: **54** [48] | *−283*: $\geq$**54** | *−331*: $\geq$42 | *−400*: 30 [24] | *−448*: $\geq$18 [$\geq$18] |
−475: $\geq$30 [$\geq$24] | *−491*: $\geq$18 | *−507*: $\geq$24 [$\geq$24] | *−563*: $\geq$18 | *−643*: $\geq$18 | ...
infinitely often: [$\geq$**6**]

Rank $r = 2$, degree $n = 5$:

+1609: $\geq$**78** | *+1649*: $\geq$**78** | *+1777*: $\geq$72 | $+2209 = 47^2$: $\geq$54 | *+2297*: $\geq$48 |
+2617: $\geq$42 | *+2665*: $\geq$42 | *+2869*: $\geq$36 | *+3017*: $\geq$36 | *+3089*: $\geq$24 | ...
infinitely often: $\geq$**6**

Rank $r = 2$, degree $n = 6$:

$-9747 = -3^3 19^2$: ? [?] | $-10051 = -19{\cdot}23^2$: $\geq$102 [90] | ... |
$-16807 = -7^5$: 72 [30] | ... | $-19683 = 3^9$: 38 [18] | ...

Rank $r = 3$, degree $n = 4$:

+725: $\geq$**162** [**156**] | *+1125*: $\geq$90 [84] | ...
infinitely often: $\geq$**18** [$\geq$**18**]

Rank $r = 3$, degree $n = 5$:

−4511: $\geq$**228** | ...
infinitely often: $\geq$**24**

Rank $r = 3$, degree $n = 6, 7, 8$:

no data available yet

Rank $r = 4$, degree $n = 5$:

$+14641 = 11^4$: **570** | *+24217*: ? | *+36497*: $\geq$138 | ...
infinitely often: $\geq$**48**

Apart from the growth of the first boldface numbers in each row — naïve interpolation suggests a faster rate of growth than a cubic polynomial in n or r, but well below exponential growth — the most striking observation to be made here is the surprisingly smooth decrease of the numbers of e.u.s as we move away from the minimal absolute discriminant in the signatures $(n, r) = (4, 2)$ and $(5, 2)$. Neither the varying presence or absence of ideals of small norm, nor the different isomorphism types of the Galois groups of the normal closures (symmetric or dihedral) seem to affect this significantly. One is tempted to speculate that some (number-geometric?) mechanism is at work behind the scenes.

What might be expected to play a rôle in the signature $(6, 3)$ is the possible presence of roots of unity of order 4 or 6 in quadratic subfields, since these enlarge the supply of units into which the unit groups of Laurent rings can be mapped. There are hardly any data available for this signature, but we will see later that a far-reaching effect is unlikely.

We have reached the heart of this paper:

3.4 Challenge: a) *To determine, for as many signatures (n, r) as possible, the nonnegative integer $C_1(n, r)$ such that there exist number fields of this signature containing this many exceptional units and none containing more than this number, and to determine all fields of this signature which attain the bound.*

b) *To find for given signatures upper and lower bounds which are as sharp as possible for the nonnegative integer $C_2 = C_2(n, r)$ defined as follows: Infinitely many nonisomorphic fields of this signature possess C_2 e.u.s which do not lie in proper subfields, and only finitely many, up to isomorphism, contain more than C_2 e.u.s of full degree n. Besides the dependence on n and r, C_2 might be considered separately for each type of Galois group acting on the normal closures, and for each possible number of roots of unity contained in a proper subfield.* ∎

The existence of $C_1(n, r)$ follows of course from EVERTSE's bound, and implies that of $C_2(n, r)$. Implicit in this Challenge is the hope that they are effectively computable, along with the witness fields for C_1 or, more ambitiously, along with all fields which exceed the C_2 bound (but see subsection 5.5 at the end of this paper).

From the first part of the table, we read off $C_1(2, 0) = 2$, $C_1(2, 1) = 6$, $C_1(3, 1) = 12$, $C_1(4, 1) = 20$, and (almost certainly) $C_1(3, 2) = 42$; furthermore, $C_2(n, 0) = C_2(n, 1) = 0$ and conjecturally $C_2(3, 2) = 6$. The second part contains hints concerning $C_2(4, 2)$, $C_2(5, 2)$, $C_2(4, 3)$, $C_2(5, 3)$ and $C_2(5, 4)$. We will investigate these more closely in the following section and establish that they are bounded below by 6, 6, 18, 24 and 48, respectively, and it will be explained why the author believes that these are already the true values.

4. Families of fields with exceptional units

To set the scene, we will briefly look at the cyclic cubic family mentioned at the start of the last section. In the usual parametrisation it arises from integral monic cubic polynomials f satisfying $f(0) = f(-1) = -1$. The conditions immediately ensure irreducibility of all such f mod 2. There is an $\mathcal{H}$-orbit of e.u.s represented by $-x$, and the two nontrivial field automorphisms send $-x$ to $(-x)^{ij}$ and to $(-x)^{ji}$. Explicitly, these polynomials take the form

$$f_a(X) = X^3 - aX^2 - (a+3)X - 1$$

with $a \in \mathbf{Z}$, and since the involutions of $\mathcal{H}$ exchange f_a and f_{-a-3}, one can restrict attention to $a \geq -1$. The discriminant of f_a is $(a^2 + 3\,a + 9)^2$, and it is easy to compute the field discriminant from it [10, Prop. 2].

The underlying universal ring, as in the constructions of Prop. 2.4, is obviously $\mathbf{Z}[X][X^{-1},\ (X{+}1)^{-1}]$, the same as in Prop. 2.4 a) except for a change of variable. But the homomorphisms from this ring to the individual $\mathbf{Z}[x] \cong \mathbf{Z}[X]/(f_a)$ factor through a common intermediate ring, universal for the conditions $f(0) = f(-1) = -1$ and "f monic of degree 3". This ring can be constructed by treating the coefficients of f as indeterminates; it is

$$\mathbf{Z}[X, A_2, A_1, A_0]/(A_0{+}1,\ 1{+}A_2{+}A_1{+}A_0{+}1,\ X^3 + A_2X^2 + A_1X + A_0) \qquad (4.1)$$

or, using the conditions to eliminate A_1 and A_0 and writing A for A_2,

$$\mathbf{Z}[X, A]/(X^3 - A\,X^2 - (A{+}3)\,X - 1)\,.$$

It turns out that this last ring is still isomorphic to $\mathbf{Z}[Y][Y^{-1},\ (Y{-}1)^{-1}]$ via the substitution $X \mapsto -Y$, $A \mapsto -Y - Y^{ij} - Y^{ji}$. In other words, the $\mathbf{Z}[x]$ have one *generic* $\mathcal{H}$-orbit of e.u.s, and their unit groups $\mathbf{Z}[x]^\times$ are generically generated by -1, x and $x{+}1$, and any further e.u.s which they or their integral closures in the quotient fields $\mathbf{Q}(x)$ might contain arise only after specializing A to $a \in \mathbf{Z}$.— Notice that in the intermediate ring we had to fix one choice of signs for our conditions, whereas the Laurent ring encompasses all sign combinations.

A family of exceptional units can thus be considered as a ring of the shape (4.1) together with its parameter specializations. Unfortunately, as soon as polynomials g_i of degree 2 or more are made invertible in the Laurent ring, the intermediate ring becomes a rather more complicated object. The ideal by which we have to divide will then contain expressions built from resultants, of the form $\mathrm{Res}(f, g_i) \mp 1$, among its generators, and we are headed for the deep waters of arithmetic geometry. On the other hand, we can still bypass the intermediate ring and work with Lemma 2.2 c) instead, which is what we will do now. We go straight to $(n, r) = (5, 3)$, which offers a rich picture while postponing problems with possible subfields.

4.1 Quintic fields with three real places. Our first task is to choose a Laurent ring. If we pick the generator polynomials g_i of its unit group in such a way that they are monic and irreducible and that the sum of their degrees is 4, and use Lemma 2.2 c) to translate the invertibility of the g_i into prescribed values of f at certain algebraic integers, each choice of algebraic units as values leads to a linear system of 4 equations for the 5 unknown coefficients of f. Since this is an interpolation problem with distinct support points, the four equations are independent, and we have a one-dimensional space of rational solutions. With a little care we can ensure an infinity of integral solutions. E.g., we might have chosen the g_i as in Prop. 2.5 as X, $X-1$, $X-2$, $X-3$, and accordingly prescribed each of $f(0)$, $f(1)$, $f(2)$ and $f(3)$ to take a value chosen from $\{\pm 1\}$, but if we choose $f(0) = \pm 1 = -f(3)$, congruences mod 3 will prevent integral solutions. In fact, this choice of conditions is not a good one for the signature we have in mind:

4.1.1 Heuristics. *A Laurent ring with unit group generated by* -1 *and by* k *multiplicatively independent polynomials* g_i *will admit infinitely many embeddings* $X \mapsto x$ *into the rings of integers of number fields* $\mathbf{Q}(x)$ *of signature* (n, r) only *if* $k \leq r$, *and then the images of the* g_i *in the number rings will usually be multiplicatively independent.*

Rationale: Assume that the images $g_i(x)$ of the g_i in one $\mathbf{Z}[x]$ satisfy a multiplicative relation, as they must when $k > r$. (Roots of unity in the field $\mathbf{Q}(x)$ do not help much; if some product of powers of the $g_i(x)$ is a root of unity of order ℓ, then the ℓ-th power of that product equals 1, so we always get a relation of the form $\prod g_i(x)^{e_i} = 1$.) This relation implies that x is a root of a particular polynomial with integer coefficients. Although the exponents e_i can be chosen in infinitely many ways, we cannot expect more than a finite number of the polynomial relations thus obtained to be compatible with x having a minimal polynomial of given degree n. (In applications, a different line of reasoning is used, *cf.* below.) ∎

We will therefore use three g_i, two linear ones and one which is quadratic. The combination X, $X-1$, X^2-X-1 would work, but guarantees only 12 e.u.s, whereas X, $X-1$, X^2-X+1 guarantees 24 of them by Prop. 2.4 c) — unless some of them should be mapped to the same algebraic number, which can happen only finitely often (as in the proof of Prop. 2.5). These translate into the conditions $f(0) \in \{\pm 1\}$, $f(1) \in \{\pm 1\}$, $f(\zeta_6) \in \{\pm 1, \zeta_6^{\pm 1}, \zeta_6^{\pm 2}\}$. Hence there are 24 such families, but the action of $\mathcal{H}$ on the Laurent ring permutes them in four orbits of six each. We choose representatives as follows:

4.1.2 Proposition. *Each field of degree* 5 *receiving a homomorphism from the ring specified in Prop.* 2.4 c) *taking* X *to an algebraic integer* x *can be defined by one of the following polynomials, with suitable* $a \in \mathbf{Z}$:

$$f_a(X) = X^5 + aX^4 - (2a+2)X^3 + (2a+3)X^2 - (a+2)X + 1 \qquad (4.2.i)$$

with values $+1$, $+1$, $+1$ *for* $f(0)$, $f(1)$, $f(\zeta_6)$;

$$f_a(X) = X^5 + aX^4 - (2a+3)X^3 + (2a+5)X^2 - (a+3)X + 1 \qquad (4.2.ii)$$

with values $+1$, $+1$, ζ_6;

$$f_a(X) = X^5 + aX^4 - (2a+2)X^3 + (2a+5)X^2 - (a+4)X + 1 \qquad (4.2.iii)$$

with values $+1$, $+1$, -1; *or*

$$f_a(X) = X^5 + aX^4 - (2a+4)X^3 + (2a+5)X^2 - (a+4)X + 1 \qquad (4.2.iv)$$

with values $+1$, -1 (forcing at least three real roots), and $+1$.

PROOF: Straightforward linear algebra. We leave it to the reader, as well as working out the other 20 polynomials arising from the action of $\mathcal{H}$. ∎

Next, we must verify that we have succeeded infinitely often in avoiding the totally real quintic fields. Indeed, we will see that we have succeeded in avoiding them entirely. (This is no accident; it has actually been built in on purpose by the choice of $g_3 = X^2 - X + 1$. We leave it as an exercise to show that no totally real algebraic integer x other than 0 or 1 will make $g_3(x)$ an algebraic unit. The theory behind this will be explained in [29].)

Since the discriminant of a quintic field is negative if and only if the field has three real places, one way of showing that we are seeing infinitely many such fields is simply to examine the signs of the polynomial discriminants. One can also compute Sturm chains. Using a slightly modified subresultant algorithm (a combination of algorithms 3.3.7 and 4.1.11 from [3]), one can in fact compute both at the same time, since the Sturm chain properties are unaffected by the positive factors introduced and removed during the pseudodivisions, and one can do this without specifying a particular value for a. E.g., starting from P_0 the polynomial from (4.2.i) and P_1 its derivative with respect to X, one gets

$$\begin{aligned}
P_2 &= -5^2 P_0 + (5X + a)\, P_1 \\
&= (4a^2{+}20a{+}20)\, X^3 \;-\; (6a^2{+}36a{+}45)\, X^2 \;+\; (4a^2{+}26a{+}40)\, X \;-\; (a^2{+}2a{+}25)\,, \\
P_3 &= 5^{-2}\big(-(4a^2{+}20a{+}20)^2 P_1 + (5\,(4a^2{+}20a{+}20)\, X + (16a^3{+}110a^2{+}260a{+}225))\, P_2\big) \\
&= -(4a^4{+}40a^3{+}148a^2{+}240a{+}149)\, X^2 \;+\; (4a^4{+}48a^3{+}188a^2{+}286a{+}164)\, X \\
&\quad -\; (-2a^4{+}63a^2{+}198a{+}193)\,,
\end{aligned}$$

and so forth. The leading coefficients of P_0, P_1 and P_2 are positive for all a; that of P_3 is $-4\,(a^2{+}5a{+}6)^2 - 5$, hence always negative; that of P_4 turns out to be positive precisely for $-3 \le a \le 1$; and the discriminant P_5 is positive precisely for $-4 \le a \le 2$. Thus we have one sign change at $+\infty$ and four at $-\infty$, and therefore 3 real places, for almost every a. In the range $-4 \le a \le 2$ where the discriminant is positive, there exists only one real root, as claimed above. Submitting the other three polynomials to similar treatment gives the following results. (The action of $\mathcal{H}$ does not affect the discriminant since the images of x always generate the same ring, so it is enough to look at one representative from each orbit.)

4.1.3 Proposition. *The polynomials from the previous proposition have, respectively, the following discriminants:*

$$\begin{aligned}
&-3a^8 - 20a^7 - 4a^6 + 230a^5 + 382a^4 - 716a^3 - 1363a^2 + 486a + 2617\,, \\
&-3a^8 - 28a^7 - 96a^6 - 58a^5 + 494a^4 + 1032a^3 - 7a^2 - 1206a + 1649\,, \\
&-3a^8 - 52a^7 - 412a^6 - 1962a^5 - 6046a^4 - 12108a^3 - 14611a^2 - 8006a + 1609\,, \\
&-3a^8 - 44a^7 - 360a^6 - 1890a^5 - 7094a^4 - 18824a^3 - 35759a^2 - 44842a - 33503\,.
\end{aligned}$$

For no value of a does a totally real quintic field arise. The first family gives quintic fields of rank 2 for $-4 \le a \le 2$, the second for $-3 \le a \le 2$, the third for $-4 \le a \le 0$, the fourth never. The rank 2 fields involved are those of discriminants $+1609$ which appears three times, $+1649$ (thrice), $+1777$ (twice), $+2209$ (twice), $+2297$ (twice), $+2617$ (once), $+2665$ (once), $+3017$ (twice), $+3889$ (once) and $+4417$ (once). ∎

We are seeing here one of the mechanisms which contribute to many fields of small absolute discriminants having large numbers of e.u.s: Homomorphisms from Laurent rings with a unit rank defect. The values of the four discriminant expressions are bounded above, so only fields of small positive discriminants can appear here, and those which do appear do so with generators of their maximal orders. The fields of discriminants +2869 and +3089 are missed by these families. They have ideals of norms 4 and 3, respectively, but the Laurent ring has sets of five elements whose pairwise differences are units, and therefore does not accommodate a composite homomorphism into a ring with $0 \neq 1$ and fewer than 5 elements.

Although it is not strictly relevant to our main topic, it may be interesting to note, firstly, that the discriminants are of lower degree in a than might have been expected by looking at the coefficients of the defining polynomials — some cancellation has been going on — and secondly, that it is straightforward to compute the minimal polynomials of the other generic e.u.s. They have coefficients which are at worst quadratic in a, e.g. for the family (4.2.i), x^2-x+1 is a root of

$$X^5 - (a^2+5a+9)X^4 + (2a^2+10a+15)X^3 - (a^2+7a+12)X^2 + (2a+5)X - 1. \quad (4.3)$$

This in itself is not exciting, were it not for the fact that this polynomial has the same discriminant as the corresponding f_a itself, which shows that in this family, the ring $\mathbf{Z}[x]$ can always be generated by single elements which are not of the form $\pm x + k$ with $k \in \mathbf{Z}$. The whole story is: x^2-x+1 generates the full ring $\mathbf{Z}[x]$ for every a in the first three families, and a subring of index $|6a+13|$ in the fourth; $(x^i)^2-x^i+1$ generates subrings of index $|2a-1|$, $|2a+3|$, 1, and $|2a^2+4a+1|$; and $(x^k)^2-x^k+1$ generates subrings of index $|2a^2+4a+1|$, $|2a-1|$, $2a^2+10a+13$, and $|2a^2+10a+11|$ in the first, second, third and fourth family's $\mathbf{Z}[x]$, respectively.

Another amusing observation is that some of these latter polynomials reappear elsewhere in our four defining families. For $a = -2$, the polynomial (4.3) is the image under $j \in \mathcal{H}$ of the member f_{-2} of family (4.2.ii); for $a = -1$, it is the j-image of the f_0 from (4.2.ii). There are a few more coincidences of this type. Clearly they also contribute to the large numbers of e.u.s in the fields involved.

A third contribution to large numbers of e.u.s in the fields belonging to small absolute values of the family parameter comes from additional units of the form $g(x)$ with "simple" polynomials $g \in \mathbf{Z}[X]$. E.g., $g = X+1$ gives a unit in the (4.2.i) family if $a = -1$; and $g = X^2 - X - 1$ gives a unit for $a = -4$ and $a = -2$. For $a = -4$, another unit is $x - 2$, and moreover, $X - 2$, $X^2 - X - 1$ and $X^3 - X - 1$ all yield units under $X \mapsto x^2 - x + 1$ in this case (their resultants with (4.3) become ± 1).

It is clear at this point that $C_2(5,3) \geq 24$. We shall now take a few more steps towards an upper bound. Our ultimate goals are the following, although time and space do not allow us to attain them in these pages.

4.1.4 Heuristics. *Consider a one-parameter family of polynomials coming from a single Laurent ring, as above.*

a) *Write G for the subgroup of $\mathbf{Z}[x]^\times$ generated by -1 together with the $g_i(x)$ — the image of the units of the Laurent ring under $X \mapsto x$. Then when $|a|$ is large enough, every* *exceptional unit* $\xi \in G \cap (1 - \mathbf{Z}[x]^\times)$ *is generic, i.e., it is the image of an exceptional unit of the Laurent ring.*

b) *Write* $\overline{G}$ *for the subgroup of the units of the ring of integers of* $K = \mathbf{Q}(x)$ *which are multiplicatively dependent on* G. *(This is the whole unit group when* G *contains a system of* r *independent units.) Then when* $|a|$ *is large enough, every exceptional unit* $\xi \in \overline{G} \cap (1 - \mathbf{Z}[x]^\times)$ *is generic.* ∎

We will sketch for one half of one of our four families how an assertion like a) can be proved; the discussion of b) will be postponed to section 5.

Furthermore, there remains the task of justifying the choice of Laurent ring. One would like to know that our families constitute essentially the only way of squeezing 24 e.u.s into each of infinitely many number rings of this signature. This is another point to which we will return in section 5.

The next task is now to bracket the real roots. For each of our four families, there is one root close to $b = -a - 2$, in addition to roots which are close to 0 and close to 1, provided that $|a|$ is large enough to give three real roots. One feasible approach here is to apply one or two symbolic Newton iterations starting from each of the three initial approximations we have just indicated. Then one expands the resulting expressions into series in b^{-1}, cutting off after the b^{-1} or b^{-2} term, and evaluates f_a at that point and on either side of it. (A computer algebra package is very helpful here.) The values there will have uniform sign, depending on the sign of a but not on its size, as soon as $|a|$ is large enough. One obtains:

4.1.5 Proposition. *For* $|a| \geq 7$, *the real roots* x_v *of the polynomials* (4.2.x) *are enclosed, one each, in the following intervals* (4.4.x), *where* $b = -a - 2$:

$$\left.\begin{array}{ll}
a < 0\,,\ b > 0: & \left\{\begin{array}{r} -b^{-1} + b^{-2} < x_0 < -b^{-1} + 2\,b^{-2} < 0\,, \\ 1 < 1 + b^{-1} - b^{-2} < x_1 < 1 + b^{-1}\,, \\ b - 2\,b^{-4} < x_b < b - b^{-4} < b\,, \end{array}\right. \\
a > 0\,,\ b < 0: & \left\{\begin{array}{r} b - b^{-4} < x_b < b\,, \\ 0 < -b^{-1} + 2\,b^{-2} < x_0 < -b^{-1} + 3\,b^{-2}\,, \\ 1 + b^{-1} - 2\,b^{-2} < x_1 < 1 + b^{-1} - b^{-2} < 1\,; \end{array}\right.
\end{array}\right\} \qquad (4.4.i)$$

$$\left.\begin{array}{ll}
a < 0\,,\ b > 0: & \left\{\begin{array}{r} -b^{-1} < x_0 < -b^{-1} + b^{-2} < 0\,, \\ 1 < 1 + b^{-1} - b^{-2} < x_1 < 1 + b^{-1}\,, \\ b < x_b < b + b^{-1}\,, \end{array}\right. \\
a > 0\,,\ b < 0: & \left\{\begin{array}{r} b + b^{-1} < x_b < b\,, \\ 0 < -b^{-1} + b^{-2} < x_0 < -b^{-1} + 2\,b^{-2}\,, \\ 1 + b^{-1} - 2\,b^{-2} < x_1 < 1 + b^{-1} - b^{-2} < 1\,; \end{array}\right.
\end{array}\right\} \qquad (4.4.ii)$$

$$\left.\begin{array}{ll}
a<0\,,\ b>0\colon & \left\{\begin{array}{c} -b^{-1} < x_0 < -b^{-1} + b^{-2} < 0\,, \\ 1 < 1 + b^{-1} + b^{-2} < x_1 < 1 + b^{-1} + 2\,b^{-2}\,, \\ b - 3\,b^{-2} < x_b < b - 2\,b^{-2} < b\,, \end{array}\right. \\
a>0\,,\ b<0\colon & \left\{\begin{array}{c} b - 2\,b^{-2} < x_b < b - b^{-2} < b\,, \\ 0 < -b^{-1} + b^{-3} < x_0 < -b^{-1}\,, \\ 1 + b^{-1} < x_1 < 1 + b^{-1} + b^{-2} < 1\,; \end{array}\right.
\end{array}\right\} \qquad (4.4.iii)$$

$$\left.\begin{array}{ll}
a<0\,,\ b>0\colon & \left\{\begin{array}{c} -b^{-1} + b^{-3} < x_0 < -b^{-1} < 0\,, \\ 1 - b^{-1} + b^{-2} < x_1 < 1 - b^{-1} + 2\,b^{-2} < 1\,, \\ b < b + 2\,b^{-1} < x_b < b + 3\,b^{-1}\,, \end{array}\right. \\
a>0\,,\ b<0\colon & \left\{\begin{array}{c} b + 2\,b^{-1} < x_b < b + b^{-1} < b\,, \\ 0 < -b^{-1} - b^{-2} < x_0 < -b^{-1}\,, \\ 1 < 1 - b^{-1} < x_1 < 1 - b^{-1} + b^{-2} < 1\,. \end{array}\right.
\end{array}\right\} \qquad (4.4.iv)$$

Some of these inequalities hold already for smaller $|a|$. ∎

The most useful consequence of these estimates is that one can now compute intervals containing the logarithms of the absolute values of the $g_i(x_v)$ for each of the three condition polynomials and each of the three real embeddings, and justify our Heuristics 4.1.1 by showing that the determinant of these logarithms, when they are arranged as a matrix in the obvious way, does not vanish. One can also stick on a fourth column which is minus the sum of the first three and thus contains the logarithms of the squared absolute values of the complex embeddings of our $g_i(x)$. Let us do this just for the first of the eight subcases of Prop. 4.1.5. Put $\delta_v = 1$ when v labels a real place, $\delta_v = 2$ for complex places, and abbreviate $\lambda = \ln b$. Using the fundamental estimate $y > 0 \Rightarrow \ln(1+y) < y$ several times, together with inequalities of the form $(1 - 2/b)^{-1} < 1 + 3/b$ and some simpler variants all of which are valid for $b \geq 6$, we find that the matrix

$$\left(\delta_v \ln |g_i(x_v)|\right)_{i,v} \tag{4.5}$$

has entries in the following intervals:

$$\begin{pmatrix}
-\lambda - \frac{3}{b} < \bullet < -\lambda & 0 < \bullet < \frac{1}{b} & \lambda - \frac{1}{b} < \bullet < \lambda & -\frac{1}{b} < \bullet < \frac{4}{b} \\
0 < \bullet < \frac{1}{b} & -\lambda - \frac{2}{b} < \bullet < -\lambda & \lambda - \frac{2}{b} < \bullet < \lambda & \frac{1}{b} < \bullet < \frac{4}{b} \\
0 < \bullet < \frac{1}{b} & 0 < \bullet < \frac{2}{b} & 2\lambda - \frac{2}{b} < \bullet < 2\lambda & -2\lambda - \frac{3}{b} < \bullet < -2\lambda + \frac{2}{b}
\end{pmatrix}$$

(the last column here was indeed obtained from the first three; a direct estimate for the complex roots might have yielded somewhat narrower bounds), and the determinant of the first three columns, using SARRUS' rule, is at least

$$2\lambda^3\left(1 - \frac{1}{b\lambda} - \frac{1}{(b\lambda)^2}\right) \;>\; 0\,.$$

Thus we have at our disposal a conveniently parametrised family of three independent units. It was E. THOMAS [40] who first pointed out that in such a situation one can apply BAKER's method simultaneously to all members of the family with large enough parameter. The essence of the method is to combine three kinds of inequalities. Let

$$y = \pm \prod_{i=1}^{3} g_i(x)^{e_i}$$

be a putative exceptional unit in the group G. Its four-component logarithmic embedding $(\delta_v \ln |y_v|)_v$ is obtained by multiplying the three-component row vector of integer exponents (e_1, e_2, e_3) from the right with the matrix (4.5). These vectors are nonzero, and by inspection, at least one coordinate of the result is quite large — a nonzero integer multiple of λ plus something small. (Actually, a rather detailed analysis is required at this point.) Thus at least one embedding y_v is comparable in size to a power of b. If y is to be exceptional, there must be at least one other embedding for which y_v is extremely close to 1. Then, for this v,

$$\Lambda_v = \ln |y_v| = \sum_{i=1}^{3} e_i \ln |g_i(x_v)|$$

is extremely close to zero (but not equal to zero) when v denotes a real place. If it is the complex place where the close approximation is happening, one can fix the three complex logarithms $\ell_{i,v} = \log g_i(x_v)$ arbitrarily among their possible values, and then there must be some integer e_0 such that

$$\Lambda_v = \sum_{i=1}^{3} e_i \ell_{i,v} + e_0 \cdot 2\pi i$$

is extremely close (but not equal) to zero. When "extremely close" is made explicit, it takes the form

$$|\Lambda_v| \ < \ \exp(-c_1 \lambda E)$$

with some positive constant c_1, where $E = \max\{|e_i|\}$. This is the first inequality. The second will be a BAKER-vintage lower bound of the form

$$|\Lambda_v| > \exp\bigl(-c_2(\lambda)(\ln E)^\kappa\bigr) .$$

Here, c_2 is essentially a polynomial in λ (it also depends on the degree, which remains fixed in our application, and on the number of logarithms which actually occur, i.e., for which e_i is nonzero), and $\kappa \in \{1, 2\}$ depending on the type of theorem employed (those from the SCHNEIDER–MIGNOTTE&WALDSCHMIDT line of which the sharpest is [15], for forms in which only two logarithms appear, have $\kappa = 2$ with a very small c_2; the best published result for three or more logarithms is [1], but work in progress by P. VOUTIER is expected to yield further significant improvements). Comparing these two estimates for $|\Lambda_v|$, one obtains an explicit upper bound for E which is still polynomial in λ.

In order to see how the third inequality arises, we must look again at the bounds for the entries of the matrix (4.5). Since we are merely trying to illustrate the method, let us assume that we are not in a special case, i.e., that none of the components of (e_1, e_2, e_3) is zero and that this vector is not a multiple of one which belongs to a generic solution. (The generic solutions, by the way, have exponent vectors $(1,0,0)$, $(0,1,0)$, $(1,-1,0)$; $(0,0,1)$, $(1,1,0)$, $(1,1,-1)$; $(1,0,-1)$, $(1,-2,0)$, $(0,-2,1)$; $(2,0,-1)$, $(2,-1,0)$, $(0,-1,1)$ and their negatives.) Then we find that the only way in which one of the first three columns can become small (the fourth requires special considerations, although the result remains the same) is that one e_i, the one which is multiplied with λ or 2λ, is rather small, and one or both of the others are larger in absolute value by a factor proportional to $b\lambda$. This is an example of what is known in diophantine approximation as a *gap principle*. The generic solutions together with b are responsible for the very disparate sizes of the entries of (4.5), and these in turn force any non-generic solutions to have a very large E, indeed exponentially large when written in terms of λ.

But above we had already obtained an upper bound on E which was only polynomial in λ. Once all the intermediate steps have been filled in, this will give us an upper bound on λ and thus on b beyond which no non-generic e.u.s can exist, as claimed by Heuristics 4.1.4 a). Moreover, we will have done much of the work required to determine any non-generic e.u.s in the small family members. Thanks to the gap principle, these are strongly restricted as soon as b is at all large, and very large numbers of fields can be handled with a moderate computational effort. (See [21] for an example of such a computation in a similar situation.) — We will end our portrait sketch of this family here; a full treatment will have to wait for another occasion. In the remainder of this section we will look very briefly at a few other field signatures.

4.2 Quintic fields with one real place. There are several options for finding families of e.u.s meeting this signature infinitely often, but none of them is entirely satisfactory, and one may have to consider infinitely many distinct families before the whole picture becomes clear. One idea is to enforce polynomials with a Galois group strictly smaller than the symmetric group — dihedral of order 10, affine of order 20, or alternating; none of these being compatible with three real places — and to use condition polynomials g_i which prevent totally real fields. Obviously, we then miss all the fields with normal closures having the full symmetric group as their Galois group. Another idea is to go for sheer quantity and employ combinations of several condition polynomials chosen with a view to obstruct real places, e.g. to use a Laurent ring of the form

$$\mathbf{Z}[X]\left[(X^2+k)^{-1},\ (X^2+k+1)^{-1}\right] \tag{4.6}$$

with a fixed integer $k > 0$, or even

$$\mathbf{Z}[X]\left[X^{-1},\ (X^2+1)^{-1}\right],$$

which leaves two coefficients of our quintic polynomials undetermined (and is therefore more difficult to handle). The ring (4.6) with $k = 1$ suffices to show that infinitely many distinct fields of this signature possess at least 6 e.u.s. Using Lemma 2.2 c) and observing that exchanging X and $-X$ does not alter anything, we may as well fix $f(\sqrt{-2}) = +1$, leaving the four possibilities $+1$, -1, $+\zeta_4$, $-\zeta_4$ for $f(\zeta_4)$ which give, respectively, the polynomials

$$X^5 + aX^4 + 3X^3 + 3aX^2 + 2X + (2a+1),$$
$$X^5 + aX^4 + 3X^3 + (3a-2)X^2 + 2X + (2a-3),$$
$$X^5 + aX^4 + 4X^3 + (3a-1)X^2 + 4X + (2a-1),$$
$$X^5 + aX^4 + 2X^3 + (3a-1)X^2 + (2a-1).$$

Their discriminants

$$32a^8 - 240a^7 + 576a^6 - 800a^5 + 2132a^4 + 224a^3 - 248a^2 + 6596a + 4897,$$
$$32a^8 - 48a^7 + 448a^6 - 1248a^5 + 2164a^4 - 7192a^3 + 10584a^2 - 6484a + 4409,$$
$$32a^8 - 144a^7 + 152a^6 + 68a^5 + 1248a^4 - 2752a^3 - 1284a^2 - 984a + 9137,$$
$$(2a-1)\cdot(16a^7 - 64a^6 + 460a^5 - 520a^4 + 3844a^3 - 1820a^2 + 5250a - 2617)$$

remain positive for all $a \in \mathbf{Z}$, and only fields with one real place are produced. The exceptional unit $-(x^2+1)$ generates the full ring $\mathbf{Z}[x]$ in the first three families, and a subring of index $|2a-1|$ in the fourth. Some coincidences are obvious from the constant coefficients: Whenever these are ± 1, we get at least another two $\mathcal{H}$-orbits of e.u.s since we then get a homomorphism $X \mapsto x^2+1$ from the ring from Prop. 2.4 b), and this happens twice in each of the four families. The corresponding fields have discriminants $+1609$, $+1649$, $+2617$, $+2665$, $+4549$, $+4897$, $+5653$ and $+9137$.

By our heuristics, homomorphisms from the universal ring of Lemma 2.2 b) should generically map X and $X-1$ to multiplicatively independent units of $\mathbf{Z}[x]$, and should therefore obstruct further e.u.s if the unit rank of the field is 2. The large numbers of e.u.s listed in the table for quintic rank 2 fields must then all be due to coincidences.

4.3 Totally real quintic fields. While Prop. 2.5 guarantees 30 e.u.s infinitely often, there is a family which guarantees 48, but the parameter dependence is of a kind we have not seen before. We use the ring from Prop. 2.4 d). Since the sum of the degrees of the g_i is 5, the coefficients of f will be completely determined once we have fixed the values $f(0)$, $f(\pm 1)$ and $f(\vartheta)$. Now $\mathbf{Q}(\vartheta)$ has unit rank one, so there is an infinity of unit values $\{\pm\vartheta^k\,;\ k \in \mathbf{Z}\}$ to choose from for $f(\vartheta)$. If F_k denotes the k-th Fibonacci number, with subscripts arranged to make $F_0 = 0$, these units are $\pm(F_{k-1} + F_k\vartheta)$. There are sixteen ways of choosing the signs of the values. In each case one obtains integer-valued expressions for the coefficients of f which are simple Z-linear combinations of F_{k-1}, F_k and constant summands. As predicted by Heuristics 4.1.1, the families produce totally real fields most of the time, but some others do appear — among others, we see again the discriminants $+1609$, $+1649$, $+1777$, $+2209$, $+2297$, $+2617$, $+2665$ of rank 2 fields, and -4511, -4903, -5519, -5783, -7031, -7367, -7463 and several more of rank 3 fields, many of them more than once. The totally real fields with small discriminants $+11^4$, $+24217$, $+38569$

also appear repeatedly, whereas +36497 is missed (it has an ideal of norm 3, but the Laurent ring again has systems of five elements whose pairwise differences are units).

4.4 Totally real quartic fields. Here, Prop. 2.5 — i.e., prescribing $f(0), f(1), f(2) \in \{\pm 1\}$ — gives a better result (18 generic e.u.s) than using, by analogy with the preceding section, X and $X-1$ and X^2-X-1 as the g_i, which only yields twelve. There is some redundancy due to the actions of $X \mapsto 2-X$ and of $(X-1) \mapsto (X-1)^{-1}$ on the Laurent ring. One can show that each of the possible sign combinations leads to a one-parameter family containing only finitely many non-totally real quartic fields from among the following: the totally complex fields of discriminants +117 and +144, and the fields of mixed signature with discriminants −275, −283 (several times), −331 (twice), −400, −448 and −643. This is a simple exercise, and was carried out already in the course of the proof of Theorem 5.1.1 of [18]. It follows that $C_2(4,3) \geq 18$. Some of the families yield only fields in which $(x-1) \mapsto -(x-1)^{-1}$ is an automorphism, so we do get infinitely many polynomials whose Galois group is not alternating or symmetric. Other families contain polynomials with the full symmetric group as Galois group, and then contain infinitely many of them, e.g. $X^4+(a-4)X^3+(-3a+5)X^2+(2a-2)X-1$ with discriminant $4a^6-47a^4+112a^2-400$. Setting $a=1$ gives a polynomial belonging to the primitive field of discriminant −283. It is irreducible mod 2, and will be so whenever a is odd, ensuring that there are 4-cycles in the Galois group of the polynomial. There are factors of degree 1 and of degree 3 mod 5, hence, whenever $\pm a \equiv 1 \pmod 5$, we also have 3-cycles. (Note that $a \mapsto -a$ has the same effect on the polynomials of this family as $X \mapsto 2-X$.) Thus at least every value $a \equiv \pm 1 \pmod{10}$ yields a polynomial with full symmetric Galois group. Working with other primes, one easily shows that the same is true, e.g., for $a \equiv \pm 3 \pmod{14}$. The value $a=0$, however, produces a dihedral Galois group acting on (the normal closure of) $\mathbf{Q}(\sqrt{\vartheta})$.

4.5 Quartic fields with two real places. We have now established all the lower C_2 bounds claimed in our table above save one, *viz.* that $C_2(4,2) \geq 6$. There are two families of self-reciprocal polynomials with $f(0)=1$ and $f(1)=\pm 1$ defining generically dihedral fields; in each family, these fields are real in one half of the parameter range and of mixed signature in the other. On the other hand, using $\mathbf{Z}[X][X^{-1}, (X^2+1)^{-1}]$ as the Laurent ring one obtains eight families of polynomials which avoid totally real fields, again with some redundancy, and among them several for which neither $X \mapsto 1/X$ nor $X \mapsto -1/X$ induces an automorphism. One interesting family is $X^4+aX^3+X^2+aX-1$ with discriminant $-4a^6-47a^4-112a^2-400$; setting $a=1$ gives a polynomial with full symmetric Galois group defining the field of discriminant −563, and as in the previous section one easily extends this to all $a \equiv \pm 1 \pmod 6$, as well as to all $a \equiv \pm 2 \pmod{21}$. Again, $a=0$ gives a dihedral polynomial (even the field $\mathbf{Q}(\sqrt{\vartheta})$ happens to be the same as above).

5. Discussion

5.1 Larger base rings. We begin by noting that if one wants to study families of fields containing a fixed subfield K_0 other than $\mathbf{Q}$, one can work with Laurent rings of the form $R_0[X][\{g_i^{-1}\}]$, where R_0 is the ring of integers of K_0 or some suitable subring.

The techniques from [19] can be transferred to the determination of the e.u.s of such rings without difficulty as soon as the e.u.s of the base ring R_0 are known. One potentially useful special case of this is the insertion of roots of unity by taking $R_0 = \mathbf{Z}[\zeta_m]$.

5.2 Further treatment of the small family members. When one carries out the procedure sketched in subsection 4.1, one obtains an upper bound for the size E of any exponent vectors attached to e.u.s in fields belonging to the family considered. With modern estimates for linear forms in logarithms, the magnitude of these bounds no longer lives up to the ancient reputation of transcendence theory as being a source of astronomical numbers [38]. When only two logarithms are involved, a typical bound for E would be less than $5{\cdot}10^5$, with three logarithms, bounds of $10^7 \dots 10^8$ are within reach [M. WALDSCHMIDT and P. VOUTIER, pers. comm.]. Of course, they are still far too large to obtain all small and medium solutions by a brute force search. (Indeed one should think twice before even searching blindly up to $E \leq 40$ or so when the unit rank is four or more.)

Several methods are available for covering the range of "medium large" solutions, say for E between 10^2 and the BAKER bound B. Three of these depend on diophantine approximation techniques and require the matrix (4.5) of logarithmic embeddings of the generator units to be known with very high accuracy, roughly to better than one part in B^N, where N is the number of logarithms involved. The "classical" method, preferred by the POHST school, is to combine an N-dimensional continued fraction algorithm with the BAKER-DAVENPORT-ELLISON lemma. B. M. M. DE WEGER suggested a lattice-based approach [43,44], where the main computational effort goes into the LLL basis reduction of an integral lattice (using only integer operations). This method is very easy to implement from scratch and reasonably fast, and has been used extensively, in particular by N. TZANAKIS and DE WEGER [41,42]. [44] contains a (somewhat biased, of course) comparison of both methods. Both do well at excluding solutions in very large ranges for E, but have difficulty in reducing the upper bound on E below a threshold of, very roughly, $20N$. In order to find "medium small" solutions, one can e.g. use algorithms which enumerate short vectors in a lattice, like the FINCKE-POHST algorithm or its variants [9].

Recently, two other methods have been introduced. Y. BILU [2] has pointed out that DE WEGER's lattice basis reduction can be replaced by reductions of bases of suitably chosen 2-dimensional sublattices of an integer lattice, which amount to computing ordinary continued fraction expansions, and then applying the 2-dimensional BAKER-DAVENPORT lemma. The main computational hurdle is that one first needs to invert a quadratic submatrix of the matrix (4.5), and this must be done with rigorous precision control.

A completely different suggestion was made by N. P. SMART [37 and pers. comm.]. It rests on observations of the following kind. Whenever $y \in G$ is *not* exceptional, $y - 1$ lies in some proper ideal I of $\mathbf{Z}[x]$, and we know thus a nontrivial element of the kernel of the group homomorphism $\mathbf{Z}[x]^\times \to (\mathbf{Z}[x]/I)^\times$. Translating this into exponent vectors, where we now need to carry along a component for the torsion part of the unit group as well, we can thus exclude an entire (almost always infinite) subgroup. Also, when we consider an ideal generated by a power of a rational prime p, and thus have approximations to all n embeddings of y into extensions of the p-adic field $\mathbf{Q}_p$ at our disposal, we can conclude that $y - 1$ is a non-unit when we find the product of the embeddings of $y - 1$ to be incongruent to ± 1. Combining information of these two types, one can subject the exponent vectors to a sieving process and, hopefully, exclude all non-e.u.s within a large E range in reasonable time. (Implementing this efficiently is an interesting challenge; the algorithm seems to lend itself well to parallelization.)

SMART's method is obviously a candidate for computing small and not-quite-small solutions in combination with a diophantine approximation method for the medium large solutions, but it is potentially capable of covering that range as well with a single algorithm. Whether this works well in practice remains to be seen. One advantage is that with this method it might be possible to keep track of the $\mathcal{H}$ action, as well as the "higher mesh groups" from [19]. In particular, the exponent vector belonging to the $\jmath$-image of an e.u. which had itself been found and recorded as an exponent vector can be obtained almost for free when the required discrete logarithms have been precomputed; with other methods, matching up the pairs requires extensive sorting or hashing.

There is another potential advantage. When one applies this method to a single field, one usually knows the full group of units, and can sieve y by the more stringent criterion that $y - 1$ modulo any proper ideal must lie in the image of the global units if y is to be exceptional. The two criteria mentioned above are weaker, but do not rely on prior information about units outside G. Moreover, whenever we apply them, the result will depend on a only up to congruence modulo some finite integer. Thus each sieving step provides information about many fields at once — we can sieve on exponents and on the family parameter at the same time.

5.3 Going beyond the subring. We promised an explanation how Heuristics 4.1.4 b) is supposed to be realised. Here it is: Assume that $\overline{G}$ is the full unit group for large enough parameter values. One considers two cases. If the regulator of the field is above a suitably chosen bound, the known regulator of our parametric independent units (the determinant computed from the matrix (4.5)) immediately yields an upper bound on the index of G in $\overline{G}$. This upper bound is polynomial in λ. One can then repeat the argument used for Heuristics 4.1.4 a), being careful to clear denominators from the exponents which occur as coefficients in $|\Lambda_v|$ before computing the lower bound. The gap principle also requires some additional work. One arrives, as before, at an upper bound for λ. This leaves the fields with small regulators, but a simple argument (less simple in the presence of subfields) shows that the discriminants of these fields are bounded, so there are only finitely many of them up to isomorphism. The cutoff point should be chosen large enough to exclude any non-generic solutions in the first case. The number of fields falling under the second case will then be quite formidable; it seems just about tractable (several 10^5) for non-cyclic cubic fields, and fortunately is small enough (only several hundred) for cyclic cubic fields to treat every one of them, as will be discussed in detail in [27].

5.4 How well can one do with ineffective methods? While transcendence theory has made great progress in producing ever sharper estimates for linear forms in logarithms, the diophantine side has not been idle. Thanks mainly to H. P. SCHLICKEWEI, the SCHMIDT Subspace Theorem is now available in p-adic as well as archimedean versions, and in a form which yields explicit bounds on numbers of solutions, although not on the solutions themselves. This is supplemented with general gap principles which yield restrictions already for quite small solutions [SCHLICKEWEI, pers. comm.]. No longer does one have to count blindly all candidates for solutions of small height in all fields of a given signature, as in the early days. However, the exponential dependence of the resulting bounds on n and r is mainly caused by the number of potential large solutions, whose existence cannot be excluded with this type of method.

In our families, the BAKER-type estimates guarantee the absence of large solutions. The price we have to pay is precisely the need to work with families. The ineffective methods are far superior when it comes to considering all fields of a given signature at once.

Still, one is left wondering whether one could not combine both approaches to achieve what neither seems to provide on its own. Specifically, could one perhaps use modern gap principles, maybe in combination with techniques from [19], to show that it is indeed impossible to squeeze more than 24 *small* e.u.s into infinitely many rings of integers of quintic rank three fields in any other way than via our families (4.2)?

5.5 Exponential parameters and overdetermined homomorphisms. There is no difficulty in principle in transferring the reasoning from subsections 4.1 and 5.3 to cases like that considered in 4.3 where the family depends on a single parameter entering as an exponent. (This parameter takes over the rôle of our λ.) When one attempts to proceed to larger degrees, one is soon led to Laurent rings in which several condition polynomials belong themselves to fields with infinitely many units, and possibly to fields of rank larger than one. Take, e.g.,

$$R \;=\; \mathbf{Z}[X][X^{-1},\,(X-1)^{-1},\,(X+1)^{-1},\,(X^2-X-1)^{-1},\,(X^3-X-1)^{-1}]$$

and write α for a root of the last generator polynomial. Then $\mathbf{Z}[\alpha]$ is the ring of integers of the cubic field of discriminant -23, and its units are $\pm\alpha^{\mathbf{Z}}$. The ring R admits homomorphisms into fields of degree as low as 3 and rank as low as 2: The minimal polynomial

$$f \;=\; X^3 + X^2 - 2X - 1$$

of $2\cos(2\pi/7)$ satisfies all five conditions. Clearly this is just a coincidence. The sum of the degrees of the g_i is 8, so we get a family of octic fields depending on two exponential parameters. How about fields of degree 7?

For any choice of values of f at the five points 0, ±1, ϑ, α, one is confronted with eight independent equations for seven unknown coefficients. Thus there is a single linear solvability condition, whose precise shape depends on how the five independent signs were chosen, and which can then be brought into the form

$$sF_\ell + tG_m = u\,, \tag{5.1}$$

with small fixed integers s, t, u. The F_ℓ are again the Fibonacci numbers and the G_m the members of the appropriate linear recurrence attached to α, which is defined by $G_0 = G_2 = 0$, $G_1 = 1$ and, for all $m \in \mathbf{Z}$,

$$G_{m+3} \;=\; G_m \;+\; G_{m+1}\,.$$

Its characteristic polynomial is of course our fifth generator polynomial g_5. One has

$$\alpha^m = G_{m-2} + G_m\alpha + G_{m-1}\alpha^2 .$$

It follows from general (ineffective!) theorems about sums of algebraic numbers which are fixed multiples of members of a finitely generated semigroup [8,14,30] that (5.1) has only finitely many solutions. (Equation (5.1) can be expressed as the vanishing of such a sum.) Thus we do not get an infinite family.

The bad news is that at present no general method is known for solving (5.1). A theorem of MIGNOTTE [20] ensures that such an equation *can* be solved effectively by reduction to a linear form in two logarithms *provided that* each of the two recurrences involved has a unique characteristic root of largest absolute value (and provided that these are multiplicatively independent, as is the case in our example; otherwise one might indeed have an infinity of solutions. This could happen e.g. if one g_i were the reciprocal of another). This applies in our situation for all $m \geq 0$. The quadratic minimal polynomial of ϑ and its reciprocal polynomial each have a single root which is larger than 1 in absolute value, and g_5 has a single real root $1.324\ldots > 1$ and a pair of complex conjugate roots of absolute value less than one. However, MIGNOTTE's theorem fails to be applicable to $m < 0$, when the dominant roots of the reciprocal of g_5 come into play — a complex conjugate pair of roots with the same absolute value. Thus at present we do not know how to effectively determine all members of this finite family in degree 7.

References

[1] A. Baker and G. Wüstholz: Logarithmic forms and group varieties. *J. reine angew. Math.* **442** (1993), 19–62.

[2] Yu. Bilu and G. Hanrot: Solving Thue equations of high degree. Univ. Bordeaux I, Pré-publ. 95-3 (1995), 18pp.

[3] H. Cohen: *A course in computational algebraic number theory.* Berlin *et al.*: Springer-Verlag 1993 (Graduate Texts in Mathematics; 138).

[4] V. Ennola: Cubic number fields with exceptional units. In: A. Pethő *et al.*(ed.), *Computational Number Theory.* Proc. Colloqu. on Computational Number Theory, Debrecen 1989. Berlin *et al.*: W. de Gruyter 1991, 103–128.

[5] P. Erdős, C. L. Stewart and R. Tijdeman: Some diophantine equations with many solutions. *Compositio Math.* **66** (1988), 37–56.

[6] J. H. Evertse: *Upper bounds for the number of solutions of Diophantine equations.* Amsterdam: Stichting Mathematisch Centrum 1983 (Mathematical Centre Tracts; 168).

[7] — : On equations in S-units and the Thue-Mahler equation. *Invent. Math.* **75** (1984), 561–584.

[8] — : On sums of S-units and linear recurrences. *Compositio Math.* **53** (1984), 225–244.

[9] U. Fincke and M. E. Pohst: Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.* **44** (1985), 463–471.

[10] M.-N. Gras: Sur les corps cubiques cycliques dont l'anneau des entiers est monogène. *C. R. Acad. Sci. Paris*, sér. **A 278** (1974), 59–62.

[11] — : Lien entre le groupe des unités et la monogénéité des corps cubiques cycliques. Sém. Théorie des Nombres Besançon 1975–76, *Publ. Math. Fac. Sci. Besançon*, fasc. **1** (1976), 19pp.

[12] K. Győry: Sur l'irréductibilité d'une classe des polynômes I. *Publ. Math. Debrecen* **18** (1971), 289–307.

[13] — : Sur les polynômes à coefficients entiers et de discriminant donné. I: *Acta Arithm.* **23** (1973), 419–426; II: *Publ. Math. Debrecen* **21** (1974), 125–144; III: *ibid.* **23** (1976), 141–165.

[14] M. Laurent: Equations diophantiennes exponentielles. *Invent. Math.* **78** (1984), 299–327.

[15] —, M. Mignotte and Yu. Nesterenko: Formes linéaires en deux logarithmes et déterminants d'interpolation. To appear in *J. Number Theory.*

[16] H. W. Lenstra jr.: Euclidean number fields of large degree. *Invent. Math.* **38** (1977), 237–254.

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

[18] A. Leutbecher and J. Martinet: Lenstra's constant and euclidean number fields. Journées Arithmétiques Metz 1981, *Astérisque* **94** (1982), 87–131.

[19] A. Leutbecher and G. Niklasch: On cliques of exceptional units and Lenstra's construction of Euclidean fields. In: H. P. Schlickewei and E. Wirsing (ed.), *Number Theory.* Proc. Journées Arithmétiques, Ulm 1987. New York *et al.*: Springer-Verlag 1989 (Lecture Notes in Mathematics; 1380), 150–178.

[20] M. Mignotte: Une extension du théorème de Skolem-Mahler. *C. R. Acad. Sci. Paris*, sér. **A 288** (1979), 233–235.

[21] — : Verification of a conjecture of E. Thomas. *J. Number Theory* **44** (1993), 172–177.

[22] T. Nagell: Sur une propriété des unités d'un corps algébrique. *Arkiv f. Matem.* **5**#25 (1964), 343–356.

[23] — : Sur les unités dans les corps biquadratiques primitifs du permier rang. *Arkiv f. Matem.* **7**#27 (1968). 359–394.

[24] — : Quelques problèmes relatifs aux unités algébriques. *Arkiv f. Matem.* **8**#14 (1969), 115–127.

[25] — : Sur un type particulier d'unités algébriques. *Arkiv f. Matem.* **8**#18 (1969), 163–184.

[26] G. Niklasch: The Number Field Database on the World Wide Web server `http://hasse.mathematik.tu-muenchen.de/`. In preparation for the Algorithmic Number Theory Symposium II, Bordeaux 1996.

[27] — : Power bases of invariant orders in cyclic cubic fields. In preparation.

[28] — : Exceptional units and automorphisms. In preparation.

[29] — : Real algebraic units as values of polynomials. In preparation.

[30] H. P. Schlickewei: S-unit equations over number fields. *Invent. Math.* **102** (1990), 95–107.

[31] D. Shanks: The simplest cubic fields. *Math. Comp.* **28** (1974), 1137–1152.

[32] C. L. Siegel: Approximation algebraischer Zahlen. *Math. Zeitschrift* **10** (1921), 173–213. Reprinted in [34], 6–46.

[33] — : Über einige Anwendungen diophantischer Approximationen. *Abh. preuß. Akad. Wiss.*, Phys.-math. Klasse **1929** Nr. 1. Reprinted in [34], 209–266.

[34] K. Chandrasekharan, H. Maaß (ed.): *Carl Ludwig Siegel. Gesammelte Abhandlungen*, Band I. Berlin *et al.*: Springer-Verlag 1966.

[35] J. H. Silverman: *The Arithmetic of Elliptic Curves.* New York *et al.*: Springer-Verlag 1986 (Graduate Texts in Mathematics; 106).

[36] J. H. Silverman: Exceptional units and numbers of small Mahler measure. To appear in *Experimental Math.*

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

[38] C. Smoryński: Some rapidly growing functions. *Math. intelligencer* **2#3** (1980), 149–154.

[39] J.-D. Thérond: Le théorème de l'élément primitif pour un anneau semi-local. *J. Algebra* **105** (1987), 29–39.

[40] E. Thomas: Complete solutions to a family of cubic diophantine equations. *J. Number Theory* **34** (1990), 235–250.

[41] N. Tzanakis and B. M. M. de Weger: On the practical solution of the Thue equation. *J. Number Theory* **31** (1989), 99–132.

[42] — and — : How to explicitly solve a Thue-Mahler equation. *Compositio Math.* **84** (1992), 223–288.

[43] B. M. M. de Weger: Solving exponential diophantine equations using lattice basis reduction algorithms. *J. Number Theory* **26** (1987), 325–367; *ibid.* **31** (1989), 88–89.

[44] — : *Algorithms for diophantine equations.* Amsterdam: Stichting Mathematisch Centrum 1989 (CWI Tract; 65).