MATHEMATICS OF COMPUTATION
Volume 69, Number 229, Pages 395–405
S 0025-5718(99)01124-2
Article electronically published on May 19, 1999

SOLVING THUE EQUATIONS WITHOUT THE FULL UNIT GROUP

GUILLAUME HANROT

Abstract. The main problem when solving a Thue equation is the computation of the unit group of a certain number field. In this paper we show that the knowledge of a subgroup of finite index is actually sufficient. Two examples linked with the primitive divisor problem for Lucas and Lehmer sequences are given.

1. Introduction

Let P be an irreducible form whose degree is at least three, and a a rational number. We are interested in the solution of the Thue equation:

$$P(X, Y) = a. \tag{1}$$

Despite numerous recent improvements, the algorithmic solution of this equation still relies on the algorithm described in [21].

The method works as follows: the original equation is reduced to a linear unit equation; then one expresses the unit as a product of powers of fundamental units of the associated number field. The coefficients of this decomposition are bounded using Baker's theory of linear forms in logarithms, and the bound is reduced by mean of the continued fractions algorithm or of the LLL lattice basis reduction algorithm. The values within the bound obtained after reduction can be enumerated in several ways.

The "reduction step" and the "enumeration step" have been widely investigated and improved recently; see [2, 3, 14, 19] for details. We shall focus on the initial and "implicit" step, i.e., computing the unit group.

It is well-known [6, 7] that computing a system of fundamental units of a given number field is a hard problem; indeed, it seems to be the major, if not the sole, bottleneck of the method.

We reduce this problem to the problem of computing a system of units which generates a subgroup of maximal rank of the group of units.

Rather than giving yet another account of a general method for solving Thue equations in a slightly more general context, we chose to show two examples which actually occurred during the investigation of the problem of primitive divisors of Lucas and Lehmer sequences. In both cases, it seems almost impossible to obtain

Received by the editor April 7, 1997 and, in revised form March 31, 1998.
1991 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11B37.
Key words and phrases. Diophantine equations, Thue equation, linear recurrence sequences, Lucas sequences, Lehmer sequences, fundamental units.
Partially supported by GDR AMI and GDR Théorie Analytique des Nombres.

a system of fundamental units, whereas obtaining a system of units that generates a subgroup of finite index is extremely easy.

2. Computing a maximal system of units

Computing a system of fundamental units is often a surprisingly difficult task. The currently most popular method, which is due to Hafner and McCurley [9] for quadratic fields and to Buchmann, Cohen, Diaz y Diaz and Olivier [5, 7] for general fields, produces a system of units which is always of maximal rank. Under the assumption of the generalized Riemann hypothesis, it can be proved to be fundamental in decent time.

This system of units can be "certified", i.e., unconditionally proved to be fundamental, but this "certification" process is usually very slow as soon as the invariants of the corresponding number field grow (degree, regulator, ...).

In this context, our adaptation of the method allows one to avoid the certification process, and still to obtain unconditional results where one had to assume the generalized Riemann hypothesis.

In the first example described below, the number field involved is of degree 41, and so it seems hopeless to obtain fundamental units by usual methods; however, our number field is a subfield of a cyclotomic field, and the cyclotomic units give us a system of independent units, which is *a priori* not fundamental.

In the second example, the number field involved can be chosen among 18 different number fields, one of which is of degree 4, another one being of degree 5. But the fundamental units for both of them are very large, and the certification process fails (actually, we stopped the computations after one day, since our method allows us to complete the solution of the corresponding equation in less than 10 minutes).

Note that this method has no analogue for the norm equation, i.e., one still has to determine a complete system of nonassociate solutions of the norm equation modulo the full unit group.

3. Primitive divisors of Lucas and Lehmer sequences

Let α and β be two algebraic numbers such that $\alpha+\beta$ (or $(\alpha+\beta)^2$ in the case of a Lehmer sequence) and $\alpha\beta$ are both rational integers, and α/β is not a root of unity.

The corresponding *Lucas sequence* (u_n) and *Lehmer sequence* (v_n) are defined by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad v_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{for } n \text{ odd}, \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{for } n \text{ even}. \end{cases}$$

A number p is said to be a *primitive divisor* of a Lucas sequence if p divides u_n but p does not divide $(\alpha-\beta)^2 u_2 \dots u_{n-1}$. For a Lehmer sequence, the definition is: p divides u_n but not $(\alpha^2-\beta^2)^2 u_3 \dots u_{n-1}$.

For large values of n, it is known [17, 18] that the n-th term of any Lucas or Lehmer sequence has a primitive divisor. For small values of n, the problem can be reduced to the solution of Thue equations by the use of the following:

Lemma 3.1. *Let $n > 4$, $n \neq 6, 12$. Let $\phi_n(X)$ be the n-th cyclotomic polynomial, $\Phi_n(X,Y) = X^n \phi_n(Y/X)$, and $P^+(n/(n,3))$ the largest prime divisor of $n/(n,3)$. Then u_n has a primitive divisor if and only if $\Phi_n(\alpha,\beta) \neq \pm 1, \pm P^+(n/(n,3))$.*

Proof. See [18, Lemmas 6 and 7]. □

Moreover, one has

$$\Phi_n(\alpha,\beta)=\prod_{j=1,(j,n)=1}^{n/2}(\alpha^2+\beta^2-2\alpha\beta\cos(2j\pi/n)).$$

Since $\alpha+\beta$ (or $(\alpha+\beta)^2$) and $\alpha\beta$ are rational integers, so is $\alpha^2+\beta^2$, and the criterion above reduces to the solution of four Thue equations of degree $\varphi(n)/2$.

Voutier [23] has solved the corresponding equations for $n\le 30$, finding all the sequences for which the n-th term has no primitive divisors. In [3] Bilu and I treated the case $n=67$ as an example, and in [4, 10] a few more examples are given. Voutier [24] has recently solved the primitive divisor problem in the case $\max(\log|\alpha|,\log|\beta|)\le 4$.

The following two sections describe the problem encountered when trying to solve the corresponding Thue equations for $n=83, 4001$, namely that the computation of the full unit group turns out to be very difficult, whereas the computation of a subgroup of finite index is relatively easy.

4. The 83rd term

In this section, we consider the equations

$$\prod_{1\le k\le 41}\left(Y-2\cos\left(\frac{2\pi k}{83}\right)X\right)=\pm 1,\pm 83. \tag{2}$$

4.1. **A preliminary lemma.** The field $\mathbb{Q}\left(\cos(\frac{2\pi}{83})\right)$ has degree 41 over $\mathbb{Q}$, which implies in particular that this field is primitive. Thus, we cannot use the method of [4].

Write the corresponding Thue equations as $F(X,Y)=a$, and put $g(Y)=F(1,Y)$. The classical method for solving a Thue equation relies on the remark that any "large" solution (x,y) should provide a very good rational approximation to one of the real roots of g. Here is an effective version of this remark. In the following lemma, as in all this paper, Log will be the principal branch of the complex logarithm, i.e., $-\pi<\operatorname{Im}\operatorname{Log} z\le\pi$.

Lemma 4.1. *Let (x,y) be an integer solution of (2).*

(i) *If $|x|>1$, then for some $k_0\in\{1,\dots,41\}$ we have*

$$\left|\frac{y}{x}-2\cos\left(\frac{2k_0\pi}{83}\right)\right|\le\frac{3.39\cdot 10^{12}}{|x|^{41}}. \tag{3}$$

(ii) *Let*

$$\psi_k=\begin{cases}2\cos\left(\frac{2\pi k_0}{83}\right)-2\cos\left(\frac{2\pi k}{83}\right), & k\ne k_0,\\ \dfrac{a}{g'\left(2\cos\left(\frac{2\pi k_0}{83}\right)\right)}, & k=k_0,\end{cases}\qquad \rho_k=\begin{cases}1, & k\ne k_0,\\ -40, & k=k_0.\end{cases} \tag{4}$$

Then, if $|x|>2$, we have

$$\left|\operatorname{Log}\frac{y-2\cos\left(\frac{2\pi k}{83}\right)x}{\psi_k x^{\rho_k}}\right|\le\frac{1.65\cdot 10^{16}}{|x|^{41}}. \tag{5}$$

Proof. (i) is just [3, Proposition 2.2.1, (i)].

(ii) Now, if $k \neq k_0$, then

$$\frac{y/x - 2\cos\left(\frac{2\pi k}{83}\right)}{\psi_k} - 1 = \frac{y/x - 2\cos\left(\frac{2\pi k_0}{83}\right)}{\psi_k}.$$

Since $|\psi_k| \geq 4\sin(\pi/83)\sin(2\pi/83)$, we obtain

$$\left|\frac{y/x - 2\cos\left(\frac{2\pi k}{83}\right)}{\psi_k} - 1\right| \leq \frac{2.962 \cdot 10^{14}}{|x|^{41}}. \tag{6}$$

Since $|\mathrm{Log}(u)| \leq 1.39|u-1|$ when $|u-1| \leq 1/2$ (see [21, p.106]), and since for $|x| \geq 3$ one has $2.962 \cdot 10^{14}/|x|^{41} \leq 1/2$, one sees that

$$\left|\mathrm{Log}\frac{y - 2\cos\left(\frac{2\pi k}{83}\right)x}{\psi_k x^{\rho_k}}\right| \leq \frac{4.12 \cdot 10^{14}}{|x|^{41}}.$$

For the case $k = k_0$, since $\prod_{1\leq k\leq 41}(y - 2\cos\left(\frac{2\pi k}{83}\right)x) = a$, write

$$\begin{aligned}
\left|\mathrm{Log}\frac{y - 2\cos\left(\frac{2\pi k_0}{83}\right)x}{\psi_{k_0} x^{\rho_{k_0}}}\right| &= \left|\mathrm{Log}\frac{\prod_{k\neq k_0}\left(2\cos\left(\frac{2\pi k_0}{83}\right) - 2\cos\left(\frac{2\pi k}{83}\right)\right)x^{40}}{\prod_{k\neq k_0} y - 2\cos\left(\frac{2\pi k}{83}\right)x}\right|, \\
&\leq \sum_{k\neq k_0}\left|\mathrm{Log}\frac{\psi_k x}{y - 2\cos\left(\frac{2\pi k}{83}\right)x}\right|, \\
&\leq 40\frac{4.12 \cdot 10^{14}}{|x|^{41}} = \frac{1.65 \cdot 10^{16}}{|x|^{41}}.
\end{aligned}$$

□

4.2. **Reduction to units.** Let M be a complete set of solutions of the norm equations $N_{\mathbb{K}/\mathbb{Q}}(\mu) = \pm 1, \pm 83$ modulo the multiplicative action of the unit group, e.g. $M = \{1, 2 - 2\cos\left(\frac{2\pi}{83}\right)\}$.

The quantity $y - 2\cos\left(\frac{2\pi k}{83}\right)x$, the norm of which is equal to a, can be written $y - 2\cos\left(\frac{2\pi k}{83}\right)x = \mu\eta$, where η is a unit and μ is in M.

At this point one usually requires that a system $\eta_1, \ldots, \eta_r$ of fundamental units be known; the equation is then transformed into an exponential one by writing $\eta = \pm\eta_1^{b_1} \ldots \eta_r^{b_r}$.

One way to avoid the knowledge of the full unit group is to enlarge the set M by considering the set of solutions of the norm equation modulo the multiplicative action of the known subgroup U'; see [15] for instance. We propose here an alternative approach, which we believe is more practical, based on the following remark: for any solution (x, y), there are a unit η in the group U', an element μ of the set M, and an integer b_0, not larger than the index $[U_{\mathbb{K}} : U']$, such that

$$\left(y - 2\cos\left(\frac{2\pi k}{83}\right)x\right)^{b_0} = \mu^{b_0}\eta. \tag{7}$$

Take for U' the group generated by the cyclotomic units

$$\eta_l^{(k)} = \sin(kl\pi/83)/\sin(k\pi/83), \qquad 1 \leq k \leq 41,\ 2 \leq l \leq 41.$$

It is known that under the generalized Riemann hypothesis, one has $U' = U_{\mathbb{K}}$; see [13]. However, this result relies on Odlyzko's effective version of Čebotarev's

theorem, and though more extensive computations have been done since the paper [13] (see [12]), it does not seem that the use of the generalized Riemann hypothesis can be avoided.

Now, there exists an r-tuple $(b_1, \dots, b_r)$ such that $\eta = \eta_1^{b_1} \dots \eta_r^{b_r}$. The next step is to obtain an upper bound for all the b_i.

4.3. **An upper bound for b_0.** The index $[U_{\mathbb{K}} : U']$ can be expressed as the quotient of the regulator of the cyclotomic units by the regulator of the field. Deriving an upper bound for the index thus means finding a lower bound for the regulator of the field. The large degree of the field prevents us from using *ad hoc* techniques such as those described in [16]. We shall instead use the bound given in [8], i.e., $R_{\mathbb{K}} \geq 85.4$. Computing the regulator of the subgroup generated by the cyclotomic units, we find that $b_0 \leq \mathcal{B} := 3.5 \cdot 10^{23}$.

4.4. **An upper bound for b_i.** In view of (7), we can rewrite (5) as

$$\left| \sum_{l=1}^{r} b_l \log |\eta_l^{(k)}| - b_0 \log |\psi_k / \mu^{(k)}| - b_0 \rho_k \log |x| \right| \leq b_0 \frac{1.65 \cdot 10^{16}}{|x|^{41}}.$$

Now let $A = [a_{kl}]_{1 \leq k,l \leq 40}$ be the inverse of the matrix $[\log |\eta_l^{(k)}|]$ (which is invertible, since the units are independent). We obtain

$$\begin{aligned} \left| b_k - b_0 \sum_{l=1}^{r} a_{kl} \rho_l \log |x| - b_0 \sum_{l=1}^{r} a_{kl} \log |\psi_l / \mu^{(l)}| \right| &\leq \max_k \sum_{l=1}^{r} |a_{kl}| \frac{1.65 b_0 \cdot 10^{16}}{|x|^{41}} \\ &\leq \frac{7.24 b_0 \cdot 10^{16}}{|x|^{41}}. \end{aligned} \tag{8}$$

For any choice of k_0, $|\sum_{l=1}^{r} a_{kl} \rho_l| \leq 4.39$, and $\sum_{l=1}^{r} a_{kl} \log |\psi_l / \mu^{(l)}| \leq 2.801$. Since $7.24 b_0 \cdot 10^{16} |x|^{-41} \leq 0.002$ when $|x| \geq 3$, we obtain the bound $|b_k| \leq b_0 (4.39 \log |x| + 2.81)$, valid for $|x| \geq 3$. This implies in particular that

$$1/|x|^{41} \leq 2.5 \cdot 10^{11} \exp(-9.33 \max_{1 \leq k \leq 40} |b_k| / b_0);$$

plugging this estimate into (8), one gets

$$\begin{aligned} &\left| b_k - b_0 \sum_{l=1}^{r} a_{kl} \rho_l \log |x| - b_0 \sum_{l=1}^{r} a_{kl} \log |\psi_l / \mu^{(l)}| \right| \\ &\qquad \leq 1.9 \cdot 10^{28} b_0 \exp(-9.3 \max_{1 \leq k \leq 40} |b_k| / b_0). \end{aligned} \tag{9}$$

Let us now pick $1 \leq k_1 < k_2 \leq 41$, with k_1 and k_2 both different from k_0. It is easy to see that

$$\Psi = \frac{\psi_{k_2}\left(y - 2\cos\left(\frac{2\pi k_1}{83}\right) x\right)}{\psi_{k_1}\left(y - 2\cos\left(\frac{2\pi k_2}{83}\right) x\right)} \tag{10}$$

is different from 1, since the contrary would imply that $y = 2\cos\left(\frac{2\pi k_0}{83}\right) x$.

Since the field is totally real,[1] $\Psi^{b_0} = 1$ can occur only for $\Psi = -1$. However, by (6), for $|x| \geq 3$, one has $|\operatorname{Log} \Psi| \leq 2.26 \cdot 10^{-5}$.

[1] Note that a similar argument applies even if the field is not totally real; one just needs to find an x_0 such that $|\operatorname{Log} \Psi| < 2\pi / \mathcal{B}$ for $|x| \geq x_0$.

Hence, since (10) is not -1, we can use the Baker-Wüstholz theorem [1] for the logarithm of the modulus of the b_0-th power of (10), which is nonzero: it gives a lower bound for the quantity

$$\Lambda = \left| b_0 \log \left| \frac{\psi_{k_2} \mu^{(k_1)}}{\psi_{k_1} \mu^{(k_2)}} \right| + b_1 \log \left| \frac{\eta_1^{(k_1)}}{\eta_1^{(k_2)}} \right| + \cdots + b_r \log \left| \frac{\eta_r^{(k_1)}}{\eta_r^{(k_2)}} \right| \right| \leq \frac{3.3 \cdot 10^{16} b_0}{|x|^{41}},$$

where $\Lambda = |\mathrm{Log}\Psi|$, namely

$$\Lambda \geq \exp(-1.41 \cdot 10^{257} \log \max_i |b_i|).$$

The upper bound can be expressed in terms of $\max_{0 \leq i \leq 41} |b_i|$; the comparison of these two bounds yields $\max_{0 \leq i \leq 41} |b_i| \leq 3.5 \cdot 10^{282}$.

In the sequel, Baker's bound will be denoted by B, whereas the bound on b_0 will still be noted $\mathcal{B}$.

4.5. **Reduction of the bound.** The reduction of Baker's bound is the technique that has been the most extensively studied recently. We apply the method of [2], which is the most efficient, slightly adapted to the present context.

Put $\delta_i = \sum_j a_{ij} \rho_j$, $\lambda_i = \sum_j a_{ij} \log |\psi_j / \mu^{(j)}|$. Let i_0 be such that $|\delta_{i_0}| = \max |\delta_i|$, and define $\overline{\delta}_i = \delta_i \delta_{i_0}^{-1}$, $\overline{\lambda}_i = \overline{\delta}_i \lambda_{i_0} - \lambda_i$. Combining two different conjugates of the inequality (9), namely the ith and the i_0th, we get

$$|b_0 \overline{\lambda}_i - b_i \overline{\delta}_i + b_{i_0}| \leq 3.8 b_0 \cdot 10^{28} \exp(-9.33 \max_{1 \leq i \leq 40} |b_i|/b_0). \tag{11}$$

Note that if we use the extreme sides of the inequality (8), we obtain

$$|b_0 \overline{\lambda}_i - b_i \overline{\delta}_i + b_{i_0}| \leq \frac{1.5 b_0 \cdot 10^{17}}{|x|^{41}}. \tag{12}$$

Now, consider the lattice generated by the columns of the matrix

$$\begin{pmatrix} \lfloor B_0/\mathcal{B} \rfloor & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \lfloor C\overline{\lambda}_{i_1} \rceil & -\lfloor C\overline{\delta}_{i_1} \rceil & C & 0 \\ \lfloor C\overline{\lambda}_{i_2} \rceil & -\lfloor C\overline{\delta}_{i_2} \rceil & 0 & C \end{pmatrix}, \tag{13}$$

with C slightly larger than $\sqrt{\mathcal{B} B_0^3}$, and where for any real x, $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$.

The idea of using a "weight" different from 1 when one has better control on one of the variables goes back to [22]. It allows a slightly better reduction, but the main feature of this trick, though, is that the value of C, and thus the precision needed, is significantly smaller.

Let l be the length of the shortest vector of an LLL-reduced basis.

The reduction process relies on the following:

Lemma 4.2. *Suppose that* $l > \sqrt{20 B_0^2 + 8 B_0 \mathcal{B} + 4 \mathcal{B}^2}$. *Then*

$$\max_{1 \leq i \leq r} |b_i| \leq 0.11 b_0 (\log C + 67.2 - \log(\sqrt{l^2 - 16 B_0^2} - 2B_0 - 2\mathcal{B})).$$

Proof. By [11, (1.12)], we know that for any $(b_0, b_{i_0}, b_{i_1}, b_{i_2}) \in \mathbb{Z}^4$, we have

$$(\lfloor B_0/\mathcal{B} \rfloor b_0)^2 + b_{i_0}^2 + (b_0 \lfloor C\overline{\lambda}_{i_1} \rceil - b_{i_0} \lfloor C\overline{\delta}_{i_1} \rceil + b_{i_1} C)^2 + (b_0 \lfloor C\overline{\lambda}_{i_2} \rceil - b_{i_0} \lfloor C\overline{\delta}_{i_2} \rceil + b_{i_2} C)^2 \geq \frac{l^2}{8}.$$

Now,

$$|b_0\lfloor C\overline{\lambda}_{i_1}\rceil - b_{i_0}\lfloor C\overline{\delta}_{i_1}\rceil + b_{i_1}C - C(b_0\overline{\lambda}_{i_1} - b_{i_0}\overline{\delta}_{i_1} + b_{i_1})| \le (b_0 + b_{i_1})/2$$

and a similar inequality holds for i_2, so that one has, if $l > 4B_0$,

$$\max_{j\in\{i_1,i_2\}} |b_0\overline{\lambda}_{i_1} - b_{i_0}\overline{\delta}_{i_1} + b_{i_1}| \ge \frac{1}{C}\left(\sqrt{\frac{l^2}{16} - B_0^2} - \frac{B_0 + \mathcal{B}}{2}\right).$$

Now one just needs to compare this lower bound with (11). This concludes the proof. □

Two steps of reduction, respectively with $C = 3.9 \cdot 10^{442}$ and $C = 4 \cdot 10^{56}$, give $\max_{1\le i\le r} |b_i| \le 5.2 \cdot 10^{24}$. Further reductions do not significantly improve the bound.

Let B^* be the bound for $\max_{1\le i\le 41} |b_i|$ after reduction.

4.6. **Final enumeration.** There are usually several ways to enumerate all the possible $(r+1)$-tuples:

- straightforward enumeration of all the possibilities; the number of $(r+1)$-tuples to check is $(2B^* + 1)^r\mathcal{B}$,
- intelligent enumeration similar to the one described in [3]; the number of $r+1$-tuples to check is $(2B^* + 1)\mathcal{B}$,
- sieving, as in [22].

However, due to the size of the reduced bound, none of these methods can be applied.

It appears that it is possible to avoid enumerating the b_i by using

Lemma 4.3. *Let l be the length of the shortest vector of an LLL-basis of the lattice (13). Suppose that $l > \sqrt{20B_0^2 + 8B\mathcal{B} + 4\mathcal{B}^2}$. Then any x solution satisfies*

$$|x| \le 10.2\left(\frac{C}{\sqrt{l^2 - 16B^{*2}} - 2B^* - 2\mathcal{B}}\right)^{1/41}.$$

Proof. Similar to that of Lemma 4.2, but uses the upper bound (12) instead of (11) at the last step. □

Instead of the gigantic bound on B, we get the bound $|x| \le 50$. After enumerating[2] the corresponding values of x, we find out that we have proved

Theorem 4.4. *The 83rd term of any Lucas or Lehmer sequence has a primitive divisor.*

Proof. The only solutions of the equation are $(0, \pm 1)$, $(\pm 1, 0)$, $\pm(1, 1)$, $\pm(1, -1)$, $\pm(-1, 2)$, $\pm(1, 2)$, which correspond to pairs (α, β) with α/β a root of unity. □

The total computational time for this example (on a PC Pentium Pro 200MHz), using `pari` version 2.0.2, was 20 minutes.

[2] or appealing to Voutier's result [24]

5. The 4001st term

In this section, we show that the method of [4] can be adapted along the same lines as the method of the previous section. We shall also see that the problem of computing fundamental units can occur even for very modest examples.

We shall consider the equation

$$\prod_{1\le k\le 2000}\left(Y-2\cos\left(\frac{2\pi k}{4001}\right)X\right)=\pm 1,\pm 4001. \tag{14}$$

The field $\mathbb{L}=\mathbb{Q}\left(2\cos\left(\frac{2\pi}{4001}\right)\right)$ is a cyclic extension of $\mathbb{Q}$, with Galois group $G=G(\mathbb{L}/\mathbb{Q})=(\mathbb{Z}/4001\mathbb{Z})^*$. Note that $z\mapsto 3^z$ defines an isomorphism from $\mathbb{Z}/4000\mathbb{Z}$ onto G. We will identify G with $\mathbb{Z}/4000\mathbb{Z}$.

For any divisor l of $[\mathbb{L}:\mathbb{Q}]=4000$, there exists a unique subgroup $l\mathbb{Z}/4000\mathbb{Z}$ of G of order $l'=4000/l$. By Galois theory, the fixed field of this subgroup is the unique subfield $\mathbb{K}$ of $\mathbb{L}$ of degree l. The action of the Galois group $G(\mathbb{L}/\mathbb{K})=\{\tau_1,\dots,\tau_{l'}\}$ on $\mathbb{L}$ is given by

$$\tau_j\left(2\cos\left(\frac{2\pi}{4001}\right)\right)=2\cos\left(\frac{2\pi 3^{jl}}{4001}\right).$$

The minimal polynomial of a generating element of such a subfield can be derived using elementary Galois theory. See [4] for further details and formulae for a generating element of a given subfield.

Using this procedure, one can exhibit the following "small" subfields

- $\mathbb{K}$, generated by a root of $x^4+x^3-1500x^2+23756x-81536$,
- $\mathbb{K}'$, generated by a root of $x^5+x^4-1600x^3-20325x^2+123999x+321199$.

It is rather easy, using `pari`, to compute a system of units of full rank [3] for both these fields; however, the regulator of the first system is around 164000, and the regulator of the second one is slightly less than 900000. It is hopeless to certify such a system of units. This shows, for instance, that the Thue equation $x^4+x^3y-1500x^2y^2+23756xy^3-81536y^4=\pm 1$ requires the method of the previous paragraph to be solved.

5.1. A preliminary lemma.

In the sequel, $\alpha^{(ik)}$ will denote $2\cos\left(\frac{2\pi 3^{4k+i}}{4001}\right)$, for $1\le i\le 4, 1\le k\le 500$. Let (x,y) be an integer solution of (14). Put

$$\varphi^{(i)}=\prod_{1\le k\le 500}\left(y-\alpha^{(ik)}x\right).$$

Note that for $\tau_j\in G(\mathbb{L}/\mathbb{K})$ defined as above, with $l=4$, one has $\tau_j(\alpha^{(ik)})=\alpha^{(i(k+j))}$, which means that $G(\mathbb{L}/\mathbb{K})$ fixes $\varphi^{(i)}$, and, by Galois theory, that $\varphi^{(i)}\in\mathbb{K}$.

The following lemma is an analogue of Lemma 4.1.

Lemma 5.1. (i) *If $|x|>1$, then for some $(i_0,k_0)\in[1,4]\times[1,500]$ we have*

$$\left|\frac{y}{x}-\alpha^{(i_0k_0)}\right|\le\frac{1.77\cdot 10^{602}}{|x|^{2000}}. \tag{15}$$

[3] which is fundamental under the generalized Riemann hypothesis

(ii) *Let*

$$\psi_i = \begin{cases} \displaystyle\prod_{1\le k\le 500} (\alpha^{(ik)} - \alpha^{(i_0k_0)}), & i \ne i_0, \\ \displaystyle a\left(\prod_{\substack{1\le j\le 4\\ j\ne i_0}} \psi_j\right)^{-1}, & i = i_0, \end{cases} \qquad \rho_i = \begin{cases} 500, & i \ne k_0, \\ -1500, & i = k_0. \end{cases} \tag{16}$$

Then, if $|x| > 2$, *we have*

$$\left|\operatorname{Log}\frac{\varphi^{(i)}}{\psi_i x^{\rho_i}}\right| \le \frac{5\cdot 10^{607}}{|x|^{2000}}. \tag{17}$$

5.2. **Reduction to units.** Let θ be a root of the polynomial $x^4 + x^3 - 1500x^2 + 23756x - 81536$. The coefficients of an integral basis of $\mathbb{K}$ with respect to the power basis are given in the following table:

	1	θ	θ^2	θ^3
ν_1	1	0	0	0
ν_2	0	1	0	0
ν_3	$-2/5$	$1/2$	$1/10$	0
ν_4	$-4/25$	$-47/100$	$3/200$	$1/200$

A system of units of finite index of $\mathbb{K}$ is given with respect to the integral basis by the following table:

	η_1	η_2	η_3
ν_1	2579620139	-68133221488165211383	1305916649079360678869
ν_2	-534883224	31300841079878935930	$-32831213498295813 1010$
ν_3	44573602	-16828180003143035894	97359743058696947252
ν_4	89147204	7032960282239282204	80531563055553911358

The prime 4001 is totally ramified in $\mathbb{K}$. The set $M = \{1, 664835\nu_1 - 43952\nu_2 - 4048\nu_3 + 4482\nu_4\}$ is a complete set of nonassociate solutions of the norm equations $N_{\mathbb{K}/\mathbb{Q}}(z) = \pm 1, \pm 4001$.

Just as in the preceding section, we can write $\varphi^{b_0} = \mu^{b_0}\eta$, where η is in the subgroup of the unit group generated by $\{\eta_1, \eta_2, \eta_3\}$.

Using Kant v.1.7, we derive the regulator bound $R_{\mathbb{K}} \ge 44.8$. Note that the bound actually implemented is not that of [16], but a much weaker one, so that it is probably possible to improve on 44.8.

Since the regulator of the unit system $\{\eta_1, \eta_2, \eta_3\}$ is less than 164175, we can assume that $b_0 \le \mathcal{B} := 3664$.

Now put $\eta = \eta_1^{b_1}\eta_2^{b_2}\eta_3^{b_3}$. By arguments similar to those of the preceding section, we derive the upper bound $|b_i| \le 31.7 b_0 \log|x| + 3b_0$, as soon as $|x| \ge 3$, so that $1/|x|^{2000} \le 1.6\cdot 10^{82}\exp(-63\max_{1\le i\le 3}|b_i|/b_0)$.

Now let $1 \le i_1 < i_2 \le 4$, with i_1 and i_2 both different from k_0. One can prove that for at least one choice of (i_1, i_2) the quantity

$$\Psi = \frac{\psi_{i_2}\varphi_{i_1}}{\psi_{i_1}\varphi_{i_2}} \tag{18}$$

is different from 1 (see [4]).

Moreover, for $|x| \geq 3$, by (17), $|\mathrm{Log}\,\Psi| \leq 5.73 \cdot 10^{-347}$, hence $\Psi \neq -1$. Therefore, we can use the Baker-Wüstholz theorem for the logarithm of the modulus of Ψ^{b_0}, which gives us the lower bound

$$\exp(-8.9 \cdot 10^{40} \log \max_i |b_i|) \leq \left| b_0 \log \left| \frac{\psi_{i_2} \mu^{(i_1)}}{\psi_{i_1} \mu^{(i_2)}} \right| + \sum_{1 \leq l \leq 3} b_l \log \left| \frac{\eta_l^{(i_1)}}{\eta_l^{(i_2)}} \right| \right|.$$

The upper bound (17) can be used to derive an upper bound for the same quantity; expressed in terms of $\max_{0 \leq i \leq 3} |b_i|$ the comparison of the two bounds yields $\max_{0 \leq i \leq 3} |b_i| \leq 1.1 \cdot 10^{45}$. The reduction works in a similar way as previously; after two steps one gets $\max_{1 \leq i \leq 3} |b_i| \leq 97000$. Using a lemma similar to 4.3, one finds out that for any solution (x, y), one has $|x| \leq 2$. The corresponding solutions are the same as in Section 4; we have just proved

Theorem 5.2. *The* 4001*st term of any Lucas or Lehmer sequence has a primitive divisor.*

The total computation took 6 minutes and 30 seconds.

6. Comparison with the method using the full unit group

One may have expected the method described in this paper to be significantly slower than the method using the full unit group. This is however not the case.

There is only one computational drawback, which occurs during the reduction step. Usually, one needs only to compute one continued fraction expansion (or reduce one lattice) for each value of k_0. With the present method, the corresponding lattice depends not only on $\overline{\delta}_i$ but also on $\overline{\lambda}_i$. In section 4, this amounts to reducing one lattice per solution of the norm equation, which is (almost) negligible. In section 5, we have to reduce one lattice per pair (i_0, k_0), i.e. 500 times more than by the classical method. However, the computational time is not at all unreasonable, due to the small dimension of these lattices.

One could also argue that the fact that we obtain a very good bound on $|x|$ whereas we obtain a very bad one on B comes mostly from the fact that we are considering very high degree equations. This does not seem to be the case. For the equation $x^4 + x^3y - 1500x^2y^2 + 23756xy^3 - 81536y^4 = \pm 1$, we got, by the same arguments, the bound $|x| \leq 16$.

It is my belief that this adaptation of the classical method is particularly well-suited to the solution of Thue equations appearing when one is trying to find out integral solutions of equations $y^p = f(x)$ by the so-called "Thue descent". In that situation, the Thue equations one needs to solve are indeed often rather complicated, and the corresponding units are often difficult to compute and still more difficult to certify. See for instance [20] for an example.

7. Acknowledgments

I would like to thank Yuri Bilu, Prof. Jean-Marc Deshouillers and Benne de Weger for suggesting improvements and modifications that proved to be worthwile. I also want to thank Prof. Henri Cohen, Claus Fieker and Prof. Michael Pohst for information concerning the computation of unit groups and of regulator bounds, and the referee for his very careful rereading of the manuscript, which allowed me to correct several inaccuracies and to greatly improve the presentation of the paper.

References

1. A. Baker, G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62. MR **94i:**11050
2. M. Bennett, B.M.M. de Weger, On the Diophantine equation $|ax^n - by^n| = 1$, *Math. Comp.* **67** (1998), 413–438. MR **98c:**11024
3. Yu. Bilu, G. Hanrot, Solving Thue equations of high degree, *J. Number Th.* **60** (1996), 373–392. MR **97k:**11040
4. Yu. Bilu, G. Hanrot, Thue equations with composite fields, *Acta Arith.*, to appear.
5. J. Buchmann, A subexponential algorithm for the determination of class groups and regulators of algebraic number fields, Séminaire de Théorie des Nombres de Paris 1988-89, Progr. Math., vol. 94, Birkhaüser, 27–39. MR **92g:**11125
6. H. Cohen "A Course in Computational Algebraic Number Theory", Graduate Texts in Math., Vol. 138, Springer, 1993. MR **94i:**11105
7. H. Cohen, F. Diaz y Diaz, M. Olivier, Subexponential algorithms for class group and unit computations, *J. Symb. Comp.* **24** (1997), 433–441. MR **98m:**11138
8. A. Costa, E. Friedman, Ratios of regulators in totally real extensions of number fields, *J. Number Th.* **37** (1991), 288–297. MR **92j:**11138
9. J. Hafner, K. McCurley, A rigorous subexponential algorithm for computation of class groups, *J. Amer. Math. Soc.* **2** (1989), 837–850. MR **91f:**11090
10. G. Hanrot, "Résolution effective d'équations diophantiennes : algorithmes et applications", Thèse, Université Bordeaux 1, 1997.
11. A. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534. MR **84a:**12002
12. F.J. van der Linden, Class numbers computations of real abelian number fields, *Math. Comp.* **39** (1982), 693–707. MR **84e:**12005
13. J.M. Masley, Class numbers of real cyclic number fields with small conductor, *Compositio Math.* **37** (1978), 297–319. MR **80e:**12005
14. M. Mignotte, B.M.M. de Weger, On the Diophantine equations $x^2+74 = y^5$ and $x^2+76 = y^5$, *Glasgow Math. J.* **38** (1996), 77–85. MR **97b:**11044
15. A. Pethő, Computational methods for the resolution of diophantine equations, *in* R.A. Mollin (ed.), Number Theory: Proc. First Conf. Can. Number Th. Assoc., Banff, 1988, de Gruyter, 1990, 477–492. MR **92c:**11152
16. M. Pohst, K. Wildanger, Tables of unit groups and class groups of quintic fields and a regulator bound, *Math. Comp.* **67** (1998), 361–367. MR **98d:**11163
17. A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, *J. Reine Angew. Math.* **268/269** (1974), 27–33. MR **49:**8961
18. C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer sequences, *Proc. London Math. Soc. (3)* **35** (1977), 425–447. MR **58:**10694
19. N.P. Smart, The solution of triangularly connected decomposable form equation, *Math. Comp.* **64** (1995), 819–840. MR **95f:**11115
20. R. J. Stroeker, B.M.M. de Weger, On elliptic Diophantine equations that defy Thue's method: The case of the Ochoa curve, *Exper. Math.* **2** (1994), 209–220. MR **96c:**11033
21. N. Tzanakis, B.M.M. de Weger, On the practical solution of the Thue Equation, *J. Number Th.* **31** (1989), 99–132. MR **90c:**11018
22. N. Tzanakis, B.M.M. de Weger, How to explicitly solve a Thue-Mahler equation, *Compositio Math.* **84** (1992), 223–288; **89** (1993), 241–242. MR **93k:**11025; MR **95a:**11030
23. P. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.* **64** (1995), 869–888. MR **95f:**11022
24. P. Voutier, Primitive divisors of Lucas and Lehmer sequences, II, *J. Th. Nombres Bordeaux* **8** (1996), 251–275. MR **98h:**11037

Algorithmique Arithmétique Expérimentale, UPRES A CNRS 5465, Université Bordeaux 1, 351, Cours de la Libération, F-33405 Talence Cedex, FRANCE

Current address: LORIA, 615, rue du Jardin Botanique, B.P. 101, F-54600 Villers-lès-Nancy, FRANCE

E-mail address: Guillaume.Hanrot@loria.fr.