ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 6, 2010

COMPACT REPRESENTATION OF QUADRATIC INTEGERS AND INTEGER POINTS ON SOME ELLIPTIC CURVES

FILIP NAJMAN

1. Introduction. Let $\mathbf{Q}(\sqrt{d})$ be a real quadratic field. Following [**17**] we define a *compact representation* of an algebraic number $\beta \in \mathbf{Q}(\sqrt{d})$ to be

$$\beta = \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j} \right)^{2^{k-j}}, \tag{1}$$

where $d_j \in \mathbf{Z}$, $\alpha_j = (a_j + b_j\sqrt{d})/2 \in \mathbf{Q}(\sqrt{d})$, $a_j, b_j \in \mathbf{Z}$, $j = 1, \ldots, k$. Bounds on k, α and d_j are given in [**17**], and all depend polynomially on $\log d$. Compact representations are used to store the fundamental unit of the quadratic order O_K. The reason for doing this is that, as is shown in [**15**], there is an infinite set of quadratic orders, such that the binary length of the fundamental unit is exponential in $\log d$. This makes it impossible to create an algorithm for solving the Pell equation with complexity less than exponential. Compact representations are polynomial in $\log d$, and allow faster algorithms for solving the Pell equation.

This representation is a extension of a compact representation as defined in [**2**] from algebraic integers to all elements of $\mathbf{Q}^*(\sqrt{d})$. It is often useful to do modular arithmetic on compact representations, for example for determining the solvability of certain Diophantine equations, as seen in [**14**]. We present an algorithm for computing the value of a quadratic integer represented by a compact representation as defined in [**17**]. In [**2, 14**] there are algorithms for doing modular arithmetic on compact representations as defined in [**2**], but to our knowledge there are no algorithms for doing modular arithmetic on compact representations as defined in [**17**]. The main problem is that the [**2**] representation requires that the partial products

$$\gamma_j = \alpha_j \prod_{i=1}^{j-1} \left(\frac{\alpha_i}{d_i} \right)^{2^{j-i}} \tag{2}$$

Received by the editors on June 11, 2008, and in revised form on June 30, 2008.
DOI:10.1216/RMJ-2010-40-6-1979 Copyright ©2010 Rocky Mountain Mathematics Consortium

be quadratic integers. Using Maurer's methods, we obtain representations that do not satisfy this requirement. On such a representation, using algorithms from [**2, 14**] is not possible.

It is expected that the number of integer points on an elliptic curve E in Weierstrass form depends on the rank of $E(\mathbf{Q})$. More precisely, Lang conjectured that it grows exponentially with the rank (see [**21**]). Since not much is known on the distribution of ranks in parametric families of elliptic curves, this makes it hard to expect to find (or even predict) all integer points on a family of elliptic curves in Weierstrass form. However, for some families of elliptic curves not in Weierstarss form, there are results which give evidence that the number of integer points might not depend on the rank, and that actually the number of points can be the same for all curves in a family. Several such results involve so called $D(n)$-m-tuples.

A set of positive integers $\{a_1, a_2, \dots, a_m\}$ is called a *Diophantine $D(n)$ m-tuple* if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Using our algorithm we shall improve the following results. In [**10**], the following theorem is proved:

Theorem 1. *Let $\{1, 2, c\}$ be a $D(-1)$-triple and E the elliptic curve given by*

$$E_k : y^2 = (x+1)(2x+1)(cx+1). \tag{3}$$

Assume that $c-2$ is square-free and that the rank of E over $\mathbf{Q}$ equals two. Then, the integer points on E are given by

$$\begin{aligned}(x,y) \in \Big\{ &(-1,0), (0,\pm 1), \left(\frac{c-3}{2}, \pm s(c-2)\right), (s(3s-2t), \\ &\pm (t-s)(2s-t)(st-c)), \\ &(s(3s+2t), \pm(t+s)(2s+t)(st+c)) \Big\}\end{aligned} \tag{4}$$

where $s = \sqrt{c-1}$ and $t = \sqrt{2c-1}$.

It is also shown in [**10**] that $c = c_k = 1/8((1+\sqrt{2})^{4k} + (1-\sqrt{2})^{4k} + 6)$, $k \in \mathbf{N}$. It should mentioned that the assumption that $\mathrm{rk}\,(E_k(\mathbf{Q})) = 2$

does not always hold. One example of this is that $\mathrm{rk}\,(E_4(\mathbf{Q})) = 4$. Also $c-2$ does not always have to be square-free. Examples of this are $c_{26}-2$ and $c_{40}-2$. Fujita showed that Theorem 1 holds without the assumptions on the rank and $c-2$ for $k \leq 40$, except for $k \in \{4,7,8,11,12,15,20,24,25,27,30,36,39\}$. We will exclude the cases $k = 4,7,8,11,12,15,20,25,27,30$ and under the extended Riemann hypothesis, also the case $k = 39$.

In [**11**] it is proved

Theorem 2. *Let $k \geq 1$ be an integer, and let E_k be the elliptic curve given by*

$$E_k : y^2 = (F_{2k+1}+1)(F_{2k+3}x+1)(F_{2k+5}x+1). \tag{5}$$

If the rank of E_k over $\mathbf{Q}$ equals one, then the integer points on E_k are given by

$$\begin{aligned}(x,y) \in \{&(0,\pm 1),(4F_{2k+2}F_{2k+3}F_{2k+4},\\ &\pm(2F_{2k+2}F_{2k+3}+1)(2F_{2k+3}^2-1)(2F_{2k+3}F_{2k+4}-1))\}.\end{aligned} \tag{6}$$

Note that $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ is a $D(-1)$-triple.

As in Theorem 1, in Theorem 2 the assumption $\mathrm{rk}\,(E_k(\mathbf{Q})) = 1$ does not always hold. For example, $\mathrm{rk}\,(E_k(\mathbf{Q})) \neq 1$ for $k = 2,3,4,5,7,9,10$. Fujita showed that Theorem 2 holds without the assumption on the rank of E_k for $f \leq k \leq 50$, except for the cases $k \in \{9,20,24,25,32,43\}$. We shall eliminate the cases $k = 9,20,24,25$ and, under the extended Riemann hypothesis, also the case $k = 43$.

In [**5**] it is proved

Theorem 3. *Let E_k be the elliptic curve given by*

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1). \tag{7}$$

If the rank of E_k over $\mathbf{Q}$ equals one or $3 \leq k \leq 1000$, then all integer points on E_k are given by

$$(x,y) \in \{(0,\pm 1),(16k^3-4k, \pm(128k^6-112k^4+20k^2-1))\}. \tag{8}$$

We shall extend this result to $3 \leq k \leq 5000$.

Note that $\{k-1, k+1, 4k\}$ is a $D(1)$-triple. In [**3**] it was proven that this triple extends uniquely to a Diophantine quadruple $\{k-1, k+1, 4k, 16k^3-4k\}$. Note also that in [**5**] it was shown that the statement of Theorem 3 is valid for some subfamilies with ranks 2 and 3, which makes the conjecture that for all $k \geq 3$ all integer points on (7) are given by (8) plausible.

In [**6**] it is proved

Theorem 4. *Let E_k be the elliptic curve given by*

$$E_k : y^2 = (F_{2k}+1)(F_{2k+2}x+1)(F_{2k+4}x+1). \tag{9}$$

If the rank of E_k over $\mathbf{Q}$ equals one or $2 \leq k \leq 50$, then all integer points on E_k are given by

$$\begin{aligned}(x,y) \in \{&(0,\pm 1), (4F_{2k+1}F_{2k+2}F_{2k+3},\\ &\pm (2F_{2k+1}F_{2k+2}-1)(2F_{2k+2}^2+1)(2F_{2k+2}F_{2k+3}+1))\}.\end{aligned} \tag{10}$$

We shall extend this result to $2 \leq k \leq 200$.

Note that $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ is a $D(1)$-triple. In [**4**] it was proven that this triple extends uniquely to a Diophantine quadruple $\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{k+1}F_{2k+2}F_{2k+3}\}$.

2. An algorithm for modular arithmetic on compact representations. We develop an algorithm, which for a given compact representation (1) of a quadratic integer

$$\frac{x+y\sqrt{\Delta}}{2} = \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j}\right)^{2^{k-j}},$$

where $(x+y\sqrt{\Delta})/2$ is the standard representation of the given quadratic integer, and a positive integer n, computes the values x and y modulo n. Our algorithm is a modification of the algorithm described in Theorem 5.7 in [**2**].

Algorithm 1.

mdl:=n$\cdot 2^{k-1}\prod_{i=1}^{k} d_k^2$.

a[1]:=$c_1 \pmod{\text{mdl}}$, b[1]:=$f_1 \pmod{\text{mdl}}$, rem:= 1

For (i=2,i<k−1,++i)

{

xtmp:=(a[i−1]^2+b[i−1]$^2\Delta$) $a_i + 2\Delta$a[i−1]b[i−1]$b_i \pmod{\text{mdl}}$

ytmp:=(a[i−1]^2+b[i−1]$^2\Delta$) $b_i + 2$a[i−1]b[i−1]$a_i \pmod{\text{mdl}}$

rem:=rem^2

divisor:=gcd($4d_{i-1}^2$,xtmp,ytmp)

rem:=$\frac{4d_{i-1}^2 \cdot \text{rem}}{\text{divisor}}$

mdl:=$\frac{\text{mdl}}{\gcd(\text{mdl},\ \text{divisor})}$

a[i]:=$\frac{\text{xtmp}}{\text{divisor}} \pmod{\text{mdl}}$

a[i]:=$\frac{\text{ytmp}}{\text{divisor}} \pmod{\text{mdl}}$

while (gcd(reduction, mdl) > 1)

reduction:=$\frac{\text{rem}}{\gcd(\text{rem},\ \text{mdl})}$

If reduction$\neq 1$

{

mult:=reduction$^{-1} \pmod{\text{mdl}}$

rem:=$\frac{\text{rem}}{\text{reduction}}$

a[i]:=a[i]$\cdot$ mult $\pmod{\text{mdl}}$

b[i]:=b[i]$\cdot$ mult $\pmod{\text{mdl}}$

}

}

This algorithm would be exactly the same algorithm as the one from Theorem 5.7 in [**2**] if all the γ_j, as defined in (2), are quadratic integers. Algorithm 1 takes polynomial time. As in the algorithm from [**2**], we make use of the recursive equation

$$4d_{i-1}^2\gamma_i = \gamma_{i-1}^2\alpha_i. \tag{11}$$

If γ_j is not a quadratic integer, then $4d_{i-1}^2$ does not divide the right

hand side in (11), so we must remember the part that does not divide (*rem* in the algorithm). Also, it may occur that a factor of n is canceled, so we actually get $x \pmod{n'}$ and $y \pmod{n'}$, where n' divides n. To correct this we have Algorithm 2:

Algorithm 2. Algorithm 2 receives as input a compact representation of a quadratic integer P, and a positive integer n. It also uses a version of Algorithm 1, $alg1(P, n, k)$, which receives P and n, and stores the value of n' in k. Also this version prints the obtained values of $x \pmod{n'}$ and $y \pmod{n'}$ if $n' = n$. Algorithm 2 actually finds a multiple of n, n'' such that $alg1(P, n'', k)$ returns $P \pmod{n}$, as wanted.

```
alg1(P,n,k)
pot:=20;
While (k<n)
{
fix:=(n/k)^pot
ko:=k;
fix:=fix · n
fixo:=fix;
alg1(P,fix,k)
if(fixo==fix and ko==k) pot:=pot+20;
}
If (n<k) alg1(P,fix·n/k,k)}
```

Algorithm 2 also runs in polynomial time.

3. The solvability of $ax^2 - by^2 = c$. The main method of improving Theorems 1–4 is going to be, for given $a, b, c \in \mathbf{Z}$, proving the insolubility of a given Diophantine equation of the type

$$ax^2 - by^2 = c, \tag{12}$$

where $a, b, c \in \mathbf{Z}$, one of a, b is greater than one, $\gcd(a, b) =$

$\gcd(ab, c) = 1$ and ab is not a perfect square. For doing this when a, b, c are large, we will need a fast way to solve the Pell equation. Let $R_d = \log \eta_d$, where η_d is the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{d})$. R_d is called the *regulator*. It is shown in [**2**] that, given R_d, there is a polynomial time algorithm for computing a compact representation of $\varepsilon(d) = x_1 + y_1\sqrt{d}$, where $x_1 + y_1\sqrt{d}$ is the fundamental solution of the Pell equation $x^2 - dy^2 = 1$. We use the well-known fact that $\varepsilon(d) = \eta_d^v$, where $v = 1, 2, 3$ or 6. It is always possible to determine the exact value of v, as shown for example in [**14**]. Maurer in [**17**] explicitly shows methods for computing the compact representation. We will use Maurer's methods.

The most time consuming part of solving the Pell equation is computing R_d. We will use two methods for doing this. Both these methods also compute the class group.

The first is the Babystep-Giantstep method of Shanks described in [**20**]. This method has running time complexity of $O(d^{1/4})$, and the result is unconditionally correct. We used the implementation of this algorithm in LiDIA, the `quadratic_order::regulator_shanks()` function.

The second method is the subexponential algorithm first described in [**1**] that gives a multiple of the regulator, mR_d where $m = 1$ under the extended Riemann hypothesis. As explained in [**14**], we can unconditionally compute an odd multiple of the regulator. We used the implementation of this algorithm in PARI, the `quadclassunit` function.

All of our programs were written in C++, using the LiDIA library [**16**].

First we examine the case when $c = 1, 2$. Using the subexponential algorithm we unconditionally compute an odd multiple of the regulator, and then compute a power product that is an odd power of the fundamental solution of the Pell equation.

Theorem 5. *Let m be an odd integer. If $c = 1, 2$, equation* (12) *has a solution in integers if and only if*

$$\left(\frac{2a}{c}\right) \mid v_m + 1 \text{ and } \left(\frac{2b}{c}\right) \mid v_m - 1,$$

where $v_m + u_m\sqrt{ab} = \varepsilon(ab)^m$.

Proof. See [**14**, Theorem 4.2].

Now using Algorithm 2 we can compute the value of v_m, and by Theorem 5 we get an answer to the solvability of (12). We will always use this method if $c = 1, 2$, unless said otherwise. This method was used by the authors of [**14**] to eliminate the exceptional cases and extend the results from [**9**].

If $c \neq 1, 2$, suppose that $ax^2 - by^2 = c$ has a solution. Then, $x^2 - aby^2 = ac$ has a solution, i.e., there exists $x + y\sqrt{ab} \in O_{\mathbf{Q}(\sqrt{ab})}$, such that $N(x + y\sqrt{ab}) = ac$. Then there exists a principal ideal $(x + y\sqrt{ab})$ that has norm ac. It follows that, to show that (12) has no solution, it is sufficient to show that there are no principal ideals of norm ac in $O_{\mathbf{Q}(\sqrt{ab})}$. For checking whether an ideal is principal we again need to compute the regulator and class group. So, we can, as explained in [**22**], find all ideals in $O_{\mathbf{Q}(\sqrt{ab})}$ of norm ac, then, after computing R_{ab}, check whether they are principal. We do this with the function `quadratic_ideal::is_principal()` from LiDIA that is an implementation of the methods described in [**13**]. If none are, (12) is insoluble. We have to test at most $2^{\omega(|c|)}$ ideals. If a, b are small enough ($ab < 10^{35}$) we use the algorithm of Shanks to compute the regulator. If we get that (12) is insoluble and R_{ab} was computed by the algorithm of Shanks, this is unconditional.

4. Improvements of Theorem 1. As shown in [**10**], proving that (4) are the only integer points on (3) is equivalent to proving that the following system has no integer solutions:

$$\begin{aligned} d_2x_1^2 - d_1x_2^2 &= 1, \\ d_3x_1^2 - d_1x_3^2 &= j_2, \\ d_3x_2^2 - d_2x_3^2 &= j_1, \end{aligned} \tag{13}$$

where $c = c_k$, $d_1 = D_1$, $d_2 = 2D_2$, $d_3 = c$, $j_1 = (c-2)/D_1$, $j_2 = (c-1)/D_2$, and D_1 and D_2 are square-free integers dividing $c-2$ and $c-1$ respectively. This system is obtained by eliminating x from the system (4.18) in [**10**].

By examining these equations modulo various primes, it can be shown that all except the following cases can be eliminated:

k	(D_1, D_2)
4	$(407, 17)$
7	$(3, 2),\ (2175243841, 1)$
8	$(470831, 1)$
11	$(248375433167, 2026573)$
12	$(543339719, 1153),\ (543339719, 2306)$
15	$(264489, 5945),\ (1343597439, 5945),\ (2300867879, 1),$ $(43756594946086091, 11890)$
20	$(1, 1330561),\ (c_{20} - 2, 20213),$ $(c_{20} - 2, 2661122),\ (c_{20} - 2, 26894629493)$
24	$(1, 5654885),\ (c_{24} - 2, 7921633),$ $(c_{24} - 2, 11309770),\ (c_{24} - 2, 1345510645)$
25	$(1, 2433376321462076761),\ (c_{25} - 2, 4866752642924153522)$
27	$(1, 985),\ (c_{27} - 2, 1970)$
30	$(1, 93521),\ (1, 161669),\ (1, 15119446549)$ $(c_30 - 2, 187042),\ (c_{30} - 2, 323338),\ (c_{30} - 2, 30238893098)$
36	$(1283229546787304717998403161, 1409409905),$ $(128322954678730471799840315 9, 2818819810)$
39	$(254072969141257218722003304911, 1791421633)$

All these systems are locally solvable. The reason Fujita could not eliminate these systems is because the fundamental solutions of the attached Pell equations are too large. We overcome this problem by using compact representations. Using the methods described in Chapter 3, we are able to eliminate some of the cases.

$$\boxed{k = 4}$$

We get that the first and third equation of (13) have solutions, but the second equation,

$$166465x_1^2 - 407x_3^2 = 9792$$

is not solvable. This can be easily proven using (more powerful) methods from Chapter 3, but we will demonstrate a nice elementary

way of solving the Diophantine equation $ax^2 - by^2 = c$. Suppose $ax^2 - by^2 = c$ has a solution. We can suppose without loss of generality that $c > 0$ (otherwise we multiply the equation with -1).

$$\begin{aligned} ax^2 - by^2 = c \Longrightarrow (\sqrt{a}x + \sqrt{b}y)(\sqrt{a}x - \sqrt{b}y) = c \Longrightarrow (\sqrt{a}x - \sqrt{b}y) \\ = \frac{c}{\sqrt{a}x + \sqrt{b}y} \Longrightarrow \left|\frac{x}{y} - \sqrt{\frac{b}{a}}\right| \\ = \frac{c}{y\sqrt{a}(\sqrt{a}x + \sqrt{b}y)}. \end{aligned}$$

Because $c > 0$, it follows that $\sqrt{a}x > \sqrt{b}y$. Combining this, we get

$$\left|\frac{x}{y} - \sqrt{\frac{b}{a}}\right| < \frac{c}{2y^2\sqrt{ab}}. \tag{14}$$

Theorem 6. *Let α be a real number and c a positive real number. If a rational number p/q satisfies the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2},$$

then

$$\frac{p}{q} = \frac{rp_n \pm sp_{n-1}}{rq_n \pm sq_{n-1}},$$

for some non negative integers n, r, s, such that $rs < 2c$, where p_n/q_n is the nth convergent in the continued fraction of α.

Proof. See [**7**, Theorem 1].

Using this theorem and computing $9792/(2\sqrt{407}(\sqrt{166465} + \sqrt{407})) \approx 0.56679$, it follows that $rs < 1.133$, i.e., for solutions of our equation, we only have to check the following possibilities: $p/q = (p_n/q_n)$, $(p/q) = (p_{n+1} + p_n)/(q_{n+1} + q_n)$ or $p/q = (p_{n+1} - p_n)/(q_{n+1} - q_n)$, where p_n/q_n is the nth convergent in the expansion of $\sqrt{407/166465}$ to a continued fraction.

Lemma 1. *Let $\alpha\beta$ be a positive integer which is not a perfect square, r, u integers and let p_n/q_n denote the nth convergent of the continued*

fraction expansion of $\sqrt{\alpha/\beta} = \sqrt{\alpha\beta}/\beta$, *where* a, b, d *are integers. Let the sequences* (s_n) *and* (t_n) *be defined by* $s_0 = 0$, $t_0 = \beta$, $d = \alpha\beta$ *and*

$$a_n = \left\lfloor \frac{s_n + \sqrt{d}}{t_n} \right\rfloor, \quad s_{n+1} = a_n t_n - s_n, \quad t_{n+1} = \frac{d - s_{n+1}^2}{t_n}. \tag{15}$$

Then

$$\alpha(rq_{n+1} + uq_n)^2 - \beta(rp_{n+1} + up_n)^2 = (-1)^n(u^2 t_{n+1} + 2rus_{n+2} - r^2 t_{n+2}) \tag{16}$$

Proof. See [**8**, Lemma 2].

Since the values s_n and t_n from Lemma 1 are periodic and start repeating after half of a period, it follows that the values of $ap^2 - bq^2$ start repeating after half a period. Thus we only have to check half of the period of the expansion of $\sqrt{407/166465}$ to a continued fraction. The length of the period is 240. After checking that $166465p^2 - 407q^2 \neq 9792$ for all p, q as above, we conclude that $166465x_1^2 - 407x_3^2 = 9792$ has no solutions. We will also use this method for $k = 7, 8$.

We can also examine the minimal value that $ax^2 - by^2$ can obtain. If this is larger than c, the equation is not solvable. Let $\alpha = [a_0, a_1, \ldots]$, $\alpha_i = [a_i, a_{i+1}, \ldots]$ and $\beta_i = q_{i-2}/q_{i-1}$. We see that

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})},$$

and $\alpha_n \in \langle a_n, a_n + 1\rangle$, $\beta_n \in \langle 0, 1\rangle$, from which it follows that

$$\frac{1}{y^2(a_{n+1} + 2)} < \left| \frac{x}{y} - \sqrt{\frac{b}{a}} \right| < \frac{c}{2y^2\sqrt{ab}},$$

and furthermore

$$c > \frac{2\sqrt{ab}}{a_n + 2},$$

where a_n is the largest value that appears in the continued fraction expansion of $\sqrt{b/a}$. Since we only have to remember the largest a_n

and don't have to compute p_n and q_n this method is much faster and can be used on equations with larger coefficients.

We will use this method for the cases $k = 11, 12$ and some of the cases for $k = 15$.

$\boxed{k = 7}$

For the system $(D_1, D_2) = (3, 2)$ we get that the third equation,

$$261029261x_2^2 - x_3^2 = 2175243841$$

is not solvable. For the system $(D_1, D_2) = (2175243841, 1)$, we get that the first equation,

$$2x_1^2 - 2175243841x_3^2 = 1,$$

has no solutions.

$\boxed{k = 8}$

We obtain that the first equation,

$$2x_1^2 - 470831x_2^2 = 1$$

has no solutions.

$\boxed{k = 11}$

We obtain that the first equation,

$$4053146x_1^2 - 248375433167x_2^2 = 1$$

has no solutions. Using the method mentioned above we get that $|4053146x_1^2 - 248375433167x_2^2|$ has to be at least 10. This is the case with the largest coefficients for which we used the continued fraction method. The length of the period was more than 124000000 and the largest a_n that appeared was 222965633.

$\boxed{k = 12}$

For $(D_1, D_2) = (543339719, 1153)$, $(543339719, 2306)$, we obtain that for both systems the first equation is not solvable. These equations are

$$1153x_1^2 - 543339719x_2^2 = 1,$$

and

$$2306x_1^2 - 543339719x_2^2 = 1,$$

respectively.

$$\boxed{k = 15}$$

For all the cases, the first equation is unsolvable. The equations are:

$$\begin{aligned}
(264489, 5945): &\ 11890x_1^2 - 264489x_2^2 = 1,\\
(1343597439, 5945): &\ 11890x_1^2 - 1343597439x_2^2 = 1,\\
(2300867879, 1): &\ 2x_1^2 - 2300867879x_2^2 = 1,\\
(43756594946086091, 11890): &\ 5945x_1^2 - 43756594946086091x_2^2 = 1.
\end{aligned}$$

We also note that the last equation is the first one we were not able to eliminate using the continued fraction method described for $k = 4$. Here we were forced to use the more powerful methods from Section 3.

$$\boxed{k = 20}$$

For the case $(D_1, D_2) = (1, 1330561)$ we will demonstrate another method to prove the insolubility of the second equation

$$52355804823523233317300682758 5x_1^2 - x_3^2 = 3934866933836421878989 44.$$

We compute the regulator $R = 34.90836989050174$. From $\varepsilon(d) = \eta^2 = e^{2R}$ it follows that $u \approx v\sqrt{d} \approx e^{2R}/2$.

Theorem 7. *Let $u + v\sqrt{d}$ be the fundamental solution of the equation $x^2 - dy^2 = 1$. Then for every fundamental solution $a + b\sqrt{d}$ of the equation $x^2 - dy^2 = N$ the following inequalities hold:*

$$0 \le b \le \frac{v\sqrt{N}}{\sqrt{2}(u + \varepsilon)},$$

$$|a| \leq \sqrt{\frac{1}{2}(u+\varepsilon)|N|},$$

where $\varepsilon = \operatorname{sign}(N)$.

Proof. See [**19**, Theorems 108 and 108a].

Using this theorem we obtain a bound on the possible solutions $x_3 < 64189270940628541014374489 7$, which is still too large to check if we run through all the numbers. We now note that

$$523558048235232333173006827585 = 5 \cdot 389 \cdot 4605197 \cdot 1746860020068409.$$

If the equation is soluble, then

$$\begin{aligned} x_3^2 &\equiv -393486693383642187898944 \\ &\equiv 1312874810 \pmod{1746860020068409}, \end{aligned}$$

from which we obtain

$$x_3 \equiv \pm 696660282513640 \pmod{1746860020068409}.$$

Likewise,

$$\begin{aligned} x_3^2 &\equiv 4204250 \pmod{4605197}, \\ x_3 &\equiv \pm 3171874 \pmod{4605197}. \end{aligned}$$

Using the Chinese remainder theorem, we get

$$\begin{gathered} x_3 \equiv 1661420046287125561041, 3112159696733073182126, \\ 4932474827105903739447 \text{ or } 6383214477551851360532 \\ \pmod{804463452383897692157 3}. \end{gathered}$$

So we only have to check x_3 satisfying the above congruences and $x_3 < 64189270940628541014374489 7$. We get that none are solutions to the starting equation. Note that this method can be used effectively only when the regulator is small enough. For the remaining three cases, we get that the equations

$$\begin{aligned} (c_{20}-2, 20213): \quad & 523558048235232333173006827585x_2^2 \\ & - 40426x_3^2 = 1, \\ (c_{20}-2, 2661122): \quad & 1330561x_1^2 \\ & - 523558048235232333173006827583x_2^2 = 1, \\ (c_{20}-2, 26894629493): \quad & 523558048235232333173006827585x_2^2 \\ & - 53789258986x_3^2 = 1, \end{aligned}$$

are insoluble.

$$\boxed{k = 24}$$

For the first case $(D_1, D_2) = (1, 5654885)$, we get that the second equation

$$412561883223160381850384251320232 9x_1^2 - x_3^2 = 1232967869564786370813764736 0$$

is not solvable. For the cases $(c_{24} - 2, 7921633)$ the first equation,

$$15843266x_1^2 - 69722958264714104532714938473119359 9x_2^2 = 1,$$

is not solvable. In the case $(c_{24} - 2, 1345510645)$, the third equation is not solvable,

$$412561883223160381850384251320232 9x_2^2 - 2691021290x_3^2 = 1.$$

All these results were obtained by methods from Section 3.

$$\boxed{k = 25}$$

In the case $(c_{25} - 2, 4866752642924153522)$, the first equation

$$2368528128740923335446826998022500448 5x_2^2 - 2433376321462076761x_3^2 = 1,$$

has no solution.

In the case $(1, 2433376321462076761)$ we get that all three equations have solutions. We examine the equation $4866752642924153522x_1^2 - x_2^2 = 1$, and compute a compact representation of the fundamental solution $u + v\sqrt{d}$. Using Algorithm 2, we test whether u and v are divisible by primes smaller than 100000000. We obtain that u is divisible by 127. In this case we again first used the subexponential algorithm to compute the regulator. We get $R = 43.7221057$. Seeing that the regulator is small, we recompute it using the algorithm of Shanks. This makes the result unconditionally correct.

Theorem 8. *Let $a > 1$, $b > 0$ be square-free positive integers. If (x_1, y_1) is the minimal solution in positive integers of the equation*

$$ax^2 - by^2 = 1,$$

then all solutions of this equation in positive integers are of the form

$$x\sqrt{a} + y\sqrt{b} = (x_1\sqrt{a} + y_1\sqrt{b})^n,$$

where n is a odd positive integer. Furthermore, $x_1|x$ i $y_1|y$.

Proof. See [**18**, Theorem 11.1].

From the above theorem we conclude that 127 divides x_2. Using this, from the first and third equations of the system (13), we get $x_1^2 \equiv 107 \pmod{127}$, $x_3^2 \equiv 88 \pmod{127}$. Then the second equation implies $42 \equiv 38 \pmod{127}$, a contradiction. Hence, the system is unsolvable.

$$\boxed{k = 27}$$

For the case $(1, 985)$, the first and third equations are solvable, so we are forced to examine the second equation. We first compute the regulator with the subexponential algorithm, since the d is large and we expect the algorithm of Shanks to be too slow in this case. We get $R = 47.24760010877535070$, a very small regulator. Seeing this, we redo the computation using Shanks' algorithm, and obtain the same result in less than a second. We now obtain that the second equation,

$$\begin{aligned} &273327940811476617288697287480790195969 01x_1^2 - x_3^2 \\ &\qquad = 277490295240077784049438870538873295 40, \end{aligned}$$

has no solutions. Since we used the algorithm of Shanks, the result is unconditional.

In the second case, $(D_1, D_2) = (c_{27} - 2, 1970)$, the third equation,

$$273327940811476617288697287480790195969 01x_2^2 - 985x_1^2 = 1,$$

has no solution.

$$\boxed{k = 30}$$

In the cases $(D_1, D_2) = (1, 93521),\ (1, 161669),\ (1, 15119446549)$ the second equation is unsolvable. Since the coefficients on the left side are the same for all three equations, all three cases have the same attached quadratic field. The regulator of that quadratic field is $R = 52.53584$, so we can compute it with the algorithm of Shanks implying the unconditional unsolvability of these three cases. The equations are

$$\begin{aligned}1071500192871921052448010061055044341506490001x_1^2 - x_3^2 \\ = 1145732180870522184801285338111273769000 0,\end{aligned}$$

$$\begin{aligned}1071500192871921052448010061055044341506490001x_1^2 - x_3^2 \\ = 6627740586457026717849495333397524210000,\end{aligned}$$

$$\begin{aligned}1071500192871921052448010061055044341506490001x_1^2 - x_3^2 \\ = 7086900895474841712395606690901 0000,\end{aligned}$$

respectively.

In the cases $(c_{30} - 2, 187042)$, $(c_{30} - 2, 323338)$, $(c_{30} - 2, 30238893098)$ the third equation is unsolvable. The equations are

$$2733279408114766172886972874807901959690 1x_2^2 - 985x_3^2 = 1,$$

$$1071500192871921052448010061055044341506490001x_2^2 - 93521x_3^2 = 1,$$

$$\begin{aligned}1071500192871921052448010061055044341506490001x_2^2 \\ - 15119446549x_3^2 = 1,\end{aligned}$$

respectively.

$$\boxed{k = 36}$$

In the case $(D_1, D_2) = (1283229546787304717998403161, 1409409905)$ the first equation,

$$2818819810x_1^2 - 1283229546787304717998403161x_2^2 = 1,$$

is not solvable. We prove this using methods from Section 3.

$$\boxed{k = 39}$$

The first equation is solvable, so we examine the third equation. The coefficients are too large to use the algorithm of Shanks, so we are forced to use the subexponential algorithm. We get

$$R = 5104775786742513766375293263.2217080210$$

after ten days of computation on an Intel Xeon 2.66 GHz. We obtain that the equation

$$\begin{aligned} 38197084998967007648945048789152566022528670450273627282 9x_2^2 \\ - 3582843266x_3^2 = 254072969141257218722003304909 \end{aligned}$$

is unsolvable. Since the right hand side is not 1 or 2 and we used the subexponential algorithm, the correctness of this result depends on the truth of the extended Riemann hypothesis.

Remaining cases. For the system

$$k = 36,\ (1283229546787304717998403159,\ 2818819810)$$

we get that the first and third equation are solvable, while for the second equation the coefficients are too large for the regulator to be computed, even with the subexponential algorithm. For the system $k = 24$, $(c_{24} - 2, 11309770)$ the first and third equation are solvable, while for the second the coefficients are too large for the regulator to be computed.

5. Improvements of Theorem 2. As in Theorem 2, it can be easily shown that (6) are all integer points on (5) if the following system has no solutions:

$$\begin{aligned} d_2x_1^2 - d_1x_2^2 &= j_3, \\ d_3x_1^2 - d_1x_3^2 &= j_2, \\ d_3x_2^2 - d_2x_3^2 &= j_1, \end{aligned} \tag{17}$$

where $a = F_{2k+1}$, $b = F_{2k+3}$, $c = F_{2k+5}$, $d_1 = aD_1$, $d_2 = bD_2$, $d_3 = cD_3$, $j_1 = (c-b)/D_1$, $j_2 = (c-a)/D_2$, $j_3 = (b-a)/D_3$, while D_1, D_2 and D_3 are square-free integers dividing $c-b$, $c-a$ and $b-a$ respectively.

Examining the system modulo various primes, as noted in [**11**], we are able to eliminate all but the following cases:

k	(D_1, D_2, D_3)
9	$(89, 29, 2255)$
20	$(1174889, 144481, 5473)$
24	$(1563, 2, 503450761)$
25	$(98209, 1, 47140601)$
32	$(303955413, 4021, 1762289)$
43	$(3932105689, 22235502640988369, 153088726119)$

Using methods from Section 3, we prove that the following equations are unsolvable

$$k = 9,\ 64621535x_1^2 - 372109x_3^2 = 844$$

$$k = 20,\ 6211325049410x_1^2 - 194538286279349x_3^2 = 6709,$$

$$k = 24,\ 40730022148x_1^2 - 12158173822587x_2^2 = 25,$$

$$k = 25,\ 53316291173x_1^2 - 2000027372566466x_2^2 = 699,$$

$$k = 43,\ 713400599237553863213884440771x_2^2 - 267340577626231378574693576 2x_3^2 = 732449080.$$

The case $k = 9$ can be eliminated using elementary methods, without using compact representations. For the cases $k = 20, 24, 25$, the regulators were computed using the algorithm of Shanks, while for $k = 43$ we had to use the subexponential algorithm, so the result is conditional on the truth of the extended Riemann hypothesis. The computation of this regulator lasted 26 hours. For the case $k = 32$ we obtain that all three equations in (17) are solvable.

6. Improvements of Theorem 3. Here we examine, for a given k, the system

$$\begin{aligned} d_1x_1^2 - d_2x_2^2 &= j_1,\\ d_3x_1^2 - d_2x_3^2 &= j_2,\\ d_1x_3^2 - d_3x_2^2 &= j_3, \end{aligned} \tag{18}$$

where $d_1 = (k+1)\mu_2$, μ_2 is a square-free factor of $3k+1$, $d_2 = (k-1)\mu_1$, μ_1 is a square-free factor of $3k-1$, $(d_3, j_1, j_2) = (4k, 2, (3k+1/\mu_2))$ or $(8k, 1, (3k+1/\mu_2))$ and $j3 = (j_1d_3 - j_2d_1)/d_2$ if d_2 divides $j_1d_3 - j_2d_1$. If $j_1d_3 - j_2d_1$ is not divisible by d_2, we can eliminate the case. We use all the tests as in [**5**], and in addition add the following tests:

If p is an odd prime dividing $d_3j_1 - d_1j_2$ and not dividing $d_1d_2d_3$, $((d_1d_3)/p) = -1$ and $(((d_1j_1)/p) = -1$ or $((d_3j_2)/p) = -1)$ then the system (18) is not solvable.

If p is an odd prime dividing $d_3j_1 - d_2j_3$ and not dividing $d_1d_2d_3$, $((d_2d_3)/p) = -1$ and $(((-d_3j_3)/p) = -1$ or $((-d_2j_1)/p) = -1)$ then the system (18) is not solvable.

If p is an odd prime dividing $j_2d_1 - j_3d_2$ and not dividing $d_1d_2d_3$, $((d_1d_2)/p) = -1$ and $(((-d_2j_2)/p) = -1$ or $((d_1j_3)/p) = -1)$ then the system (18) is not solvable. The proof of these statements can be found in [**14**]. Also, if p is an odd prime dividing j_2 such that $\operatorname{ord}_p j_2$ is even, and $((d_3d_2)/p) \neq 1$ and $(((-d_3j_3)/p) \neq 1$ or $((-d_2j_1)/p) \neq 1)$ then the system (18) is not solvable. If p is an odd prime dividing j_3 such that $\operatorname{ord}_p j_3$ is even, and $((d_3d_1)/p) \neq 1$ and $(((d_1j_1)/p) \neq 1$ or $((d_3j_2)/p) \neq 1$ then the system (18) is not solvable. If a system passes all these tests we test whether each equation has a global solution using methods from Section 3. The only systems that passed the test for $1001 \leq k \leq 5000$ are the following two cases:

$$\begin{aligned} &k = 3192,\ d_1 = 30579361,\ d_2 = 3191,\\ &d_3 = 25536,\ j_1 = 1,\ j_2 = 1,\ j_3 = -9575 \end{aligned}$$

and

$$\begin{aligned} &k = 3836,\ d_1 = 44160033,\ d_2 = 141895,\\ &d_3 = 15344,\ j_1 = 1,\ j_2 = 1,\ j_3 = -311. \end{aligned}$$

$$\boxed{k = 3192}$$

We examine the first equation

$$30579361x_1^2 - 3191x_3^2 = 1.$$

We obtain the fundamental solution of this equation a_0, b_0, i.e., $x_1\sqrt{30579361} + x_3\sqrt{3191} = (a_0\sqrt{30579361} + b_0\sqrt{3191})^n$, where n is odd. We obtain that

$$a_0 \text{ is the 3513 digit integer } 12461\cdots47471$$
$$b_0 \text{ is the 3515 digit integer } 21984\cdots47440$$

By Theorem 8 this implies, since b_0 is even and $b_0|x_2$, that x_2 is even. But then the second equation

$$25536x_3^2 - 3191x_2^2 = 1$$

is not solvable.

$$\boxed{k = 3896}$$

We examine the second equation

$$959a^2 - 141895x_3^2 = 1,$$

where $a = 4x_1$. As in the previous case we find the fundamental solution $a_0\sqrt{959} + b_0\sqrt{141895}$. We compute

$$a_0 = 39721247288713527481462482242253612538898310557311378748119474993962332160268939212034625697057087139084589142727612951351787 2,$$

$$b_0 = 32654920797821606157204990214883810906357055321859983960311747014809614228247888934799231653730139304342594823055931329015 8013.$$

We see that 103 divides b_0, so 103 divides x_1. From the second equation we get $x_1^2 \equiv 34 \pmod{103}$, and from the third equation we get $x_2^2 \equiv 68 \pmod{103}$. But then the first equation gives $2 \equiv 1 \pmod{103}$, a contradiction.

We have proven

Theorem 9. *All integer points on the elliptic curve*

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1)$$

are given by (8) *for* $3 \leq k \leq 5000$.

7. Improvements of Theorem 4. For Theorem 4 we examine, for a given k, the system of equations:

$$\begin{aligned} d_1x_1^2 - d_2x_2^2 &= j_1, \\ d_3x_1^2 - d_2x_3^2 &= j_2, \\ d_1x_3^2 - d_3x_2^2 &= j_3, \end{aligned} \tag{19}$$

where $d_1 = F_{2k+2}D2$, D_2 is a square-free factor of $F_{2k+4} - F_{2k}$, $d_2 = F_{2k}D_1$, D_1 is a square-free factor of F_{2k+4}, $d_3 = F_{2k+4}D_3$, D_3 is a square-free factor of F_{2k+1}, $j_1 = (F_{2k+1})/D_3$, $j_2 = (F_{2k+4} - F_{2k})/D_2$ and $j_3 = (j_1d_3 - j_2d_1)/d_2$ if d_2 divides $j_1d_3 - j_2d_1$. If $j_1d_3 - j_2d_1$ is not divisible by d_2, we can eliminate the case. In fact, the vast majority of the cases was eliminated by this test. The only case that passed all the above tests for $50 \leq k \leq 200$ is the case

$$k = 67, d_1 = 11825896447871834976429068427,$$

$$d_2 = 45170904956503918714087129 37$$

$$d_3 = 338958006034463022366506455179712903059186472 6456,$$

$$j_1 = 66759010,\ j_2 = 26443508352314721186469779407,$$

$$j_3 = -19134702400093278081449423917.$$

We have proven

Theorem 10. *All integer points on the elliptic curve* (9) *are given by* (10) *for* $2 \leq k \leq 200$*, except maybe for* $k = 67$.

Acknowledgments. The author would like to thank Professor Andrej Dujella for introducing him to this problem and for many valuable comments.

REFERENCES

1. Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Sem. Theor. Nombres (1990), 27–41.

2. J. Buchmann, C. Thiel and H.C. Williams, *Short representation of quadratic integers*, Comput. Algebra Number Theory, Math. Appl. **325** (1995) 159–185.

3. A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

4. ———, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc. **127** (1999), 1999–2005.

5. Andrej Dujella, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.

6. ———, *Diophantine m-tuples and elliptic curves*, J.Theor. Nombres Bordeaux **13** (2001), 111–124.

7. ———, *Continued fractions and RSA with small secret exponent*, Tatra Mount. Math. Publ. **29** (2004), 101–112.

8. A. Dujella and B. Jadrijević, *A parametric family of quartic Thue equations*, Acta Arith. **101** (2002), 159–170.

9. A. Dujella and A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.

10. Yasutsugu Fujita, *The $D(1)$-extensions of $D(-1)$-triples $\{1, 2, c\}$ and integer points on the attached elliptic curves*, Acta Arith. **128** (2007), 349–375.

11. ———, *The Hoggatt-Bergum conjecture on $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ and integer points on the attached elliptic curves*, Rocky Mountain J. Math **39** (2009), 1907–1932.

12. A. Grelak and A. Grytzcuk, *On the Diophantine equation $ax^2 - by^2 = c$*, Publ. Math. Debrecen **44** (1994), 291–299.

13. M.J. Jacobson, Jr., *Subexponential class group computation in quadratic orders*, Ph.D. thesis, Tech. Univ. Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 1999.

14. M.J. Jacobson, Jr. and H.C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, Designs, Codes and Cryptography **27** (2002), 93–110.

15. J.C. Lagarias, *On the computational complexity of determining the solvability or un-solvability of the equation $x^2 - dy^2 = -1$*, Trans. Amer. Math. Soc. **260** (1980), 485–507.

16. The LiDIA Group, *LiDIA, a C++ library for computational number theory*, Software, Tech. Univ. Darmstadt, Germany (1997), see `http://www.informatik.tu-darmstadt.de/TI/LiDIA`.

17. Markus Maurer, *Regulator approximation and fundamental unit computation for real quadratic orders*, Ph.D. thesis, Tech. Univ. Darmstadt, Fachbereich Informatik, Darmstadt, Germany, 2000.

18. T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsal. **16** (1954), 105–114.

19. ———, *Introduction on number theory*, Almqvist, Stockholm; Wiley, New York, 1951.

20. Daniel Shanks, *The infrastructure of a real quadratic field and its applications*, Proc. 1972 Boulder Conference on Number Theory, (1973), 217–224.

21. Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

22. Alan Silvester, *Fast and unconditional principal ideal testing*, Masters thesis, University of Calgary, Calgary, Canada, 2006.

Department Of Mathematics, University Of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr