MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1585–1593
S 0025-5718(06)01841-2
Article electronically published on March 29, 2006

PRACTICAL SOLUTION OF THE DIOPHANTINE EQUATION $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$

KONSTANTINOS DRAZIOTIS AND DIMITRIOS POULAKIS

ABSTRACT. Let p be an odd prime and a, b positive integers. In this note we prove that the problem of the determination of the integer solutions to the equation $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$ can be easily reduced to the resolution of the unit equation $u + \sqrt{2}v = 1$ over $\mathbb{Q}(\sqrt{2}, \sqrt{p})$. The solutions of the latter equation are given by Wildanger's algorithm.

1. INTRODUCTION

A widely studied class of Diophantine equations consists of elliptic equations. In general, there are two methods for solving elliptic equations: the *Thue approach* and the *elliptic logarithm method*. The Thue approach is the most classical [16, Chapter 27]. Several factorizations over appropriate number fields lead to a finite number of Thue equations. Some methods for the solution of Thue equations has been given in [21] and [12]. The method of the elliptic logarithm was developed independently in [20], [11] and [19]. It is applicable in general, if one knows a full set of generators for the group of rational points on the curve, modulo torsion. Algorithms for finding such generators exist but are not guaranteed to always give an answer [7], [10].

Let E_n be the elliptic curve defined by the equation

$$y^2 = x^3 - n^2 x, \tag{1}$$

where n is an integer ≥ 1. Since the map $\phi : E_n \to E_{c^2 n}$, given by $(x, y) \mapsto (c^2 x, c^3 y)$, is an isomorphism of elliptic curves and the rank of $E_1(\mathbb{Q})$ is zero, then the rank of $E_n(\mathbb{Q})$, where n is a perfect square, is zero. Furthermore, since the rank of $E_2(\mathbb{Q})$ is zero, the rank of $E_{2^{2k+1}}(\mathbb{Q})$, where $k \geq 1$, is zero, and hence for every $m \geq 1$ the rank of $E_{2^m}(\mathbb{Q})$ is zero. In [9, Lemma 1.1] some sufficient conditions on n are listed for the rank of $E_n(\mathbb{Q})$ to be zero. Note that the rank of $E_n(\mathbb{Q})$ is nonzero if and only if n is a congruent number [14, Chapter I]. Recently, in [8], a simple method for the determination of the integer solutions of (1), in the case where $n = p^k$ and p is a prime, is given. Finally, note that in [2, page 203], the integer solutions of (1) with $n \leq 72$ have been calculated by the elliptic logarithm method or by a straightforward application of theorems given in [1] and [6].

In this note, we study the integer solutions of (1) when $n = 2^a p^b$, where p is a prime > 2 and a, b are positive integers not both even. Using the "multiplication

Received by the editor May 27, 2005 and, in revised form, June 18, 2005.
2000 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11D25, 11G05.
The research of the first author was supported by the Hellenic State Scholarships Foundation, I.K.Y.

by 2" on E_n, we reduce the problem of the determination of integer solutions of (1) to the solution of the unit equation $u + \sqrt{2}v = 1$ over $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ which can be solved by Wildanger's algorithm [22]. Our approach goes back to Chabauty [4], [15, page 140]. It has been used in [17] for the computation of an explicit upper bound for the integer solutions of the general elliptic equation over a number field. This result has been improved in [3].

Let $a \geq 3$. If a is even, then we put

$$\Sigma_n = \{p^b(2^{a-2}+1)^2, p^b(2^{a-2}-1)^2, p^b(2^{2(a-1)}+1), 2^{a-1}(p^{2b}+1)\}.$$

Let a be odd. If b is even, then we set

$$\Sigma_n = \{2^{a-2}(p^b+1)^2, p^b(2^{2(a-1)}+1)\}.$$

If b is odd, then we put

$$\Sigma_n = \{2^{a-2}(p^b+1)^2, p^b(2^{2(a-1)}+1), p^b(2^{a-2}+1)^2, p^b(2^{a-2}-1)^2\} \cup \Lambda_n,$$

where $\Lambda_n = \{2^{a-3}25\}$ when $(p,b) = (3,1)$, $\Lambda_n = \{3^{b-1}25\}$ when $(p,a) = (3,3)$ and $\Lambda_n = \emptyset$ otherwise. Finally, for $a = 2$ we put $\Sigma_n = \{2(p^{2b}+1), p^b 5\}$ and for $a = 1$, $\Sigma_n = \{(p^b+1)^2/2, (p^b-1)^2/2\}$.

Theorem 1. *Let $n = 2^a p^b$, where p is a prime > 2 and a, b are positive integers not both even. If $(x,y) \in \mathbb{Z}^2$ is an integer solution to (1) with $x > n$ and $x \notin \Sigma_n$, then there is a unit u of $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ such that $(1-u)/\sqrt{2}$ is also a unit and*

$$x = \frac{(u^2+1)^2 n}{4u(u^2-1)}.$$

The units u and $v = (1-u)/\sqrt{2}$ are a solution of the equation

$$u + \sqrt{2}v = 1$$

over $\mathbb{Q}(\sqrt{2}, \sqrt{p})$. Wildanger's algorithm is an efficient method for the resolution of such equations. It uses Baker's method, the LLL reduction algorithm and means from the geometry of numbers. It is implemented in the Magma Computational Algebraic System [23] and so easily provides the solutions of the above equation. Thus Theorem 1 gives all the solutions of (1) with $x > n$. Since there are no solutions with $x < -n$ and $0 < x < n$, the full set of solutions of (1) can easily be determined. As far as we know, it is the first time that this approach is used for the practical solution of an elliptic equation.

This paper is organized as follows. In Section 2, we give some lemmata which will be needed for the proof of Theorem 1. The proof of Theorem 1 is given in Section 2. Finally, in Section 3, we state a simple algorithm for the solution of (1) and give some examples.

2. Auxiliary lemmata

In this section we give some lemmata which are useful for the proof of Theorem 1.

Lemma 1. *Let $n = 2^a p^b$, where p is a prime > 2 and a, b are positive integers not both even. If (x,y) is an integer solution of (1) with $x > n$ and $x \notin \Sigma_n$, then $n|x$.*

Proof. We have the following cases:

Case 1. $2 \not| x$ and $p \not| x$. Then x, $x - n$, $x + n$ are pairwise prime, and so there are odd positive integers A, B, C satisfying

$$x = A^2, \quad x - n = B^2, \quad x + n = C^2.$$

We have $A^2 - B^2 = n$ and $\gcd(A+B, A-B) = 2$. Since A, B are odd, $8|A^2 - B^2$, and so we get $a \geq 3$. It follows that $(A+B, A-B) = (2^{a-1}p^b, 2), (2^{a-1}, 2p^b), (2p^b, 2^{a-1})$. Thus $A \in \{2^{a-2}p^b + 1, 2^{a-2} + p^b\}$. On the other hand, we have $C^2 - A^2 = n$ and $\gcd(C + A, C - A) = 2$, whence $A \in \{2^{a-2}p^b - 1, 2^{a-2} - p^b, p^b - 2^{a-2}\}$. We deduce that $p = 3$, $n = 24$ and $x = 25$.

Case 2. $2|x$ and $p \not| x$. Thus we can write $x = 2^k z$, where z is an odd integer not divisible by p and $k \geq 1$. If $k > a$, then

$$y^2 = 2^{k+2a} z(z2^{k-a} - p^b)(z2^{k-a} + p^b).$$

The integers z, $z2^{k-a} - p^b$, $z2^{k-a} + p^b$ are odd and pairwise prime. So, k is even and there are positive odd integers A, B, C with

$$z = A^2, \quad z2^{k-a} - p^b = B^2, \quad z2^{k-a} + p^b = C^2.$$

It follows that $C^2 - B^2 = 2p^b$. Since B and C are odd, we get $8|C^2 - B^2$ and so $4|p$, which is a contradiction. If $k < a$, then we obtain, working as in Case 1, that $p = 3$, $k = a - 3 \geq 1$, $b = 1$ and $z = 25$. It follows that $x = 2^{a-3}25$ and a is odd. Suppose next that $k = a$. Then

$$y^2 = 2^{3a} z(z - p^b)(z + p^b).$$

We have $\gcd(z, z \pm p^b) = 1$ and $\gcd(z - p^b, z + p^b) = 2$. If a is even, then there are positive integers A, B, C such that

$$z = A^2, \quad z - p^b = 2B^2, \quad z + p^b = 2C^2.$$

We have $C^2 - B^2 = p^b$ and so $C + B = p^\mu$, $C - B = p^\nu$. If $\nu > 0$, then $p|C$ and hence $p|z$, which is a contradiction. Thus, $C = (p^b + 1)/2$ and so $x = 2^{a-1}(p^{2b} + 1)$. If a is odd, then there are positive integers A, B, C and $i, j \in \{1, 2\}$ with $i + j = 3$ such that

$$z = A^2, \quad z - p^b = 2^i B^2, \quad z + p^b = 2^j C^2.$$

If $(i, j) = (2, 1)$, then $A^2 - (2B)^2 = p^b$, whence $A + 2B = p^r$ and $A - 2B = p^s$ with $b \geq r > s \geq 0$. The case $s > 0$ implies $p|A$, whence $p|z$, which is a contradiction. Thus $s = 0$, and we obtain that $A = (p^b + 1)/2$, whence $x = 2^{a-2}(p^b + 1)^2$. If $(i, j) = (1, 2)$, then we similarly obtain that $x = 2^{a-2}(p^b - 1)^2$.

Case 3. $2 \not| x$ and $p| x$. Then we have $x = p^k z$, where z is an odd integer not divisible by p and $k \geq 1$. If $k > b$, then

$$y^2 = p^{k+2b} z(zp^{k-b} - 2^a)(zp^{k-b} + 2^a).$$

The integers p, z, $zp^{k-b} - 2^a$, $zp^{k-b} + 2^b$ are odd and pairwise prime. So, k is even and there are positive odd integers A, B, C satisfying

$$z = A^2, \quad zp^{k-b} - 2^a = B^2, \quad zp^{k-b} + 2^a = C^2.$$

It follows that $C^2 - B^2 = 2^{a+1}$. The integers B, C are odd and so $8|C^2 - B^2$, whence $a \geq 2$. Since $\gcd(C + B, C - B) = 2$, we get $C = 2^{a-1} + 1$, $B = 2^{a-1} - 1$. Thus, $x = p^b(2^{2(a-1)} + 1)$. If $k < b$, then we deduce, as in Case 1, that $p = 3$, $a = 3$, b odd and $x = 3^{b-1}25$. Finally, let $k = b$. Then

$$y^2 = p^{3b} z(z - 2^a)(z + 2^a).$$

The integers z, $z-2^a$, $z+2^a$ are pairwise prime. If b is even, then there are odd positive integers A, B, C satisfying

$$z = A^2, \quad z - 2^a = B^2, \quad z + 2^a = C^2.$$

So, we deduce, as previously, that $x = p^b(2^{2(a-1)} + 1)$. On the other hand, since $C^2 - A^2 = 2^a$, we obtain that $x = p^b(2^{a-2} - 1)^2$. Thus $2^{2(a-1)} + 1 = (2^{a-2} - 1)^2$, which leads to a contradiction. If b is odd, then p divides either $z - 2^a$ or $z + 2^a$, and we deduce $x = p^b(2^{a-2} \pm 1)^2$ and $a \geq 3$.

From the previous cases we conclude that $n|x$ whenever $x \notin \Sigma_n$.

Lemma 2. *Let $n = 2^a p^b$, where p is a prime > 2 and a, b are positive integers not both even. We have the following cases:*

(a) *$p = 3$ and a, b are odd. Then the integer solutions (x, y) of (1) with $-n < x < 0$ are given by $x = -2^{a-1}3^b$ and $x = -2^a 3^{b-1}$.*

(b) *$p = 7$ and a, b are odd. Then (1) has only one integer solution (x, y) with $-n < x < 0$, given by $x = -2^{a-3}7^b$.*

(c) *$p \equiv 1 \pmod 8$ and a is odd. If (x, y) is an integer solution of (1) with $-n < x < 0$, then $x = -2^k p^l z$, where $k \geq a$, l even, k even if $k > a$ and z is an odd integer, which is a perfect square.*

(d) *$p \equiv 1 \pmod 8$ and a is even. If (x, y) is an integer solution of (1) with $-n < x < 0$, then $x = -2^a p^l z$, where l even and z is an odd integer, which is a perfect square.*

Proof. Let $x = -2^k p^l z$, where z is an odd integer not divisible by p. We distinguish the following cases:

Case 1. $0 \leq k < a$. Suppose that $0 \leq l < b$. Then

$$y^2 = 2^{3k} p^{3l} z(2^{a-k} p^{b-l} - z)(2^{a-k} p^{b-l} + z).$$

The integers p, z, $2^{a-k}p^{b-l} - z$ and $2^{a-k}p^{b-l} + z$ are pairwise prime. Thus, k, l are even, and there are odd positive integers A, B, C satisfying

$$z = A^2, \quad 2^{a-k}p^{b-l} - z = B^2, \quad 2^{a-k}p^{b-l} + z = C^2.$$

It follows that $C^2 - B^2 = 2z$, and since C, B are odd we have $8|C^2 - B^2$. Hence $4|z$, which is a contradiction. If $l > b$, then we similarly obtain a contradiction. Suppose now that $l = b$. Then

$$y^2 = 2^{3k} p^{3b} z(2^{a-k} - z)(2^{a-k} + z).$$

The integers 2, z, $2^{a-k} - z$ and $2^{a-k} + z$ are pairwise prime. Since z, $2^{a-k} - z$ and $2^{a-k} + z$ are odd, we deduce that k is even. If b is even, then there are odd positive integers A, B, C satisfying

$$z = A^2, \quad 2^{a-k} - z = B^2, \quad 2^{a-k} + z = C^2,$$

whence we obtain, as previously, a contradiction. If b is odd, then either $p|2^{a-k} - z$ or $p|2^{a-k} + z$. Suppose that $p|2^{a-k} - z$. Then there are odd positive integers A, B, C such that

$$z = A^2, \quad 2^{a-k} - z = pB^2, \quad 2^{a-k} + z = C^2.$$

Thus $C^2 - A^2 = 2^{a-k}$, whence $(C + A)(C - A) = 2^{a-k}$. Hence $C + A = 2^\mu$, $C - A = 2^\nu$ with $\mu + \nu = a - k$ and $\mu > \nu$, and so we deduce $A = 2^{\mu-1} - 2^{\nu-1}$, $C = 2^{\mu-1} + 2^{\nu-1}$. Since A is odd, we have $\nu = 1$, $\mu = a - k - 1$ and therefore $z = (2^{a-k-2} - 1)^2$. We have $2^{a-k} = C^2 - A^2 \equiv 0 \pmod 8$, whence $a - k \geq 3$. Further, since $B \equiv z \equiv 1 \pmod 8$, we get $p \equiv 7 \pmod 8$. On the other hand, we

have $(2^{a-k-2} - 1)^2 < 2^{a-k}$, whence $a - k \in \{3, 4\}$. If $a - k = 4$, then the equality $16 - z = pB^2$ implies $z = 9$ and $B = 1$. Hence $C^2 = 17$, which is a contradiction. If $a - k = 3$, then a is odd, $p = 7$, $z = 1$, and so $x = -2^{a-3}7^b$. Suppose next that $p|2^{a-k} + z$. Then there are odd positive integers A, B, C such that

$$z = A^2, \quad 2^{a-k} - z = B^2, \quad 2^{a-k} + z = pC^2.$$

We have $2^{a-k} - z = B^2 + z \equiv 2 \pmod 8$, whence $a - k = 1$. Hence $z = B = 1$ and a is odd. It follows that $p = 3$. Therefore $x = -2^{a-1}3^b$.

Case 2. $k > a$. Then $l < b$. So, we have

$$y^2 = p^{3l}2^{k+2a}z(p^{b-l} - 2^{k-a}z)(p^{b-l} + 2^{k-a}z).$$

The integers 2, z, $p^{b-l} - 2^{k-a}z$, $p^{b-l} + 2^{k-a}z$ are odd and pairwise prime. Thus, k, l are even, and there are odd integers A, B, C such that

$$z = A^2, \quad p^{b-l} - 2^{k-a}z = B^2, \quad p^{b-l} + 2^{k-a}z = C^2.$$

If a is odd, then we obtain that 2 and -2 are quadratic residue modulo p, whence we get $p \equiv 1 \pmod 8$. If a is even, then $p^{b-l} = C^2 - (2^{(k-a)/2}A)^2$, whence $C + 2^{(k-a)/2}A = p^\mu$ and $C - 2^{(k-a)/2}A = p^\nu$, where $b - l \geq \mu > \nu \geq 0$. The case $\nu > 0$ implies $p|C$, which is a contradiction. Thus $\nu = 0$ and so $z2^{a-k} = (p^{b-l} - 1)^2/4$. It follows that $p^{b-l} - (p^{b-l} - 1)^2/4 = B^2$, and we get $p = 3$. On the other hand, we have $p \equiv 2^{k-a} + 1 \equiv 1, 5 \pmod 8$, which is a contradiction.

Case 3. $a = k$. Then

$$y^2 = p^{3l}2^{3a}z(p^{b-l} - z)(p^{b-l} + z).$$

We have $\gcd(p^{b-l} - z, p^{b-l} + z) = 2$, and p, z, $p^{b-l} - z$, $p^{b-l} + z$ are pairwise prime. Thus, l is even, and there are positive integers A, B, C such that

$$z = A^2, \quad p^{b-l} - z = 2^s B^2, \quad p^{b-l} + z = 2^t C^2,$$

where s, t are integers ≥ 1 with $s + t = 3$, if a is odd, and $s + t = 2$, if a is even. Suppose that a is even. Then $s = t = 1$, and so 2 and -2 are residue quadratic modulo p, whence we get $p \equiv 1 \pmod 8$. Suppose next that a is odd. If $(s, t) = (2, 1)$, then we deduce that 2 and -2 are residue quadratic modulo p, whence we get $p \equiv 1 \pmod 8$. If $(s, t) = (1, 2)$, then $(2C)^2 - A^2 = p^{b-l}$, whence $2C + A = p^\mu$ and $2C - A = p^\nu$, where $b - l \geq \mu > \nu \geq 0$. The case $\nu > 0$ implies $p|A$, which is a contradiction. Thus $\nu = 0$, and so we obtain $z = (p^{b-l} - 1)^2/4$. Putting this value into the second equality, we get $p = 3$ and $b - l = 1$. Therefore b is odd and $x = -2^a 3^{b-1}$.

Lemma 3. *Let $f(T) = T^4 - 4zT^3 + 2T^2 + 4zT + 1$, where z is an integer ≥ 2. If s is a root of $f(T)$, then the field $K = \mathbb{Q}(s)$ is a totally real Galois extension of degree 4 over $\mathbb{Q}$. Moreover,* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. First, we shall prove that $f(T)$ is irreducible. If $f(T)$ has a linear factor, then there is $s \in \mathbb{Z}$ with $f(s) = 0$. It follows that $s = \pm 1$, which leads to the contradiction $4 = 0$. Suppose now that we have the factorization

$$f(T) = (T^2 + AT + B)(T^2 + CT + D),$$

where $A, B, C, D \in \mathbb{Z}$. Thus

$$A + C = -4z, \tag{2}$$

$$B + AC + D = 2, \tag{3}$$

$$AD + BC = 4z, \tag{4}$$

$$BD = 1. \tag{5}$$

By (5), $(B, D) = (1, 1)$ or $(-1, -1)$. Suppose that $(B, D) = (1, 1)$. Then (3) implies $AC = 0$. If $A = 0$, then (2) gives $C = -4z$ and substituting the values of A and C in (4) we get $z = 0$, which is a contradiction. If $C = 0$, then we obtain a contradiction similarly. Suppose next that $(B, D) = (-1, -1)$. Then (3) gives $AC = 4$. Combining this equality with (2), it follows that $(A, C) = (-1, -4), (-4, -1)$ or $(-2, -2)$. If $(A, C) = (-1, -4)$ or $(-4, -1)$, then (2) implies $-5 = -4z$, which is impossible. If $(A, C) = (-2, -2)$, then (2) gives $z = 1$, which is not the case. Hence, $f(T)$ is irreducible.

The cubic resolvent of $f(T)$ is the polynomial

$$r(T) = T^3 - 2T^2 - (16T^2 + 4)T - 32T^2 + 8 = (T + 2)(T - 2 - 4z)(T - 2 + 4z).$$

Since $r(T)$ splits into linear factors over $\mathbb{Q}$, [13, Proposition 4.11, page 273] implies that the splitting field K of $f(T)$ has Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. So $K/\mathbb{Q}$ is a Galois extension of degree 4. By [5, Proposition 4.1.14], K is either totally real or totally complex. Since $f(1) = 1 - 8zp + 8p^2 + 32p^3z + 16p^4 > 0$ and $f(4p) = (-384z + 400)p^4 < 0$, $f(T)$ has a real root in the interval $(1, 4p)$. Therefore K is totally real.

3. Proof of Theorem 1

We denote by $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$. Let $(x, y) \in \mathbb{Z}^2$ be a solution to (1) such that $x > n$ and $x \notin \Sigma_n$. Let $(s, t) \in \bar{\mathbb{Q}}^2$ be a point on E_n such that $[2](s, t) = (x, y)$ (we denote by $[2](s, t)$ the double of the point (s, t) on the elliptic curve E_n). By [18, page 59], we have

$$s^4 - 4xs^3 + 2n^2s^2 + 4n^2xs + n^4 = 0. \tag{6}$$

Let $K = \mathbb{Q}(s)$. By Lemma 1, $x = nz$, where z is an integer > 1. Thus $s_1 = s/n$ is a root of the equation

$$f(T) = T^4 - 4zT^3 + 2T^2 + 4zT + 1 = 0,$$

and so s_1 is a unit of K. By Lemma 3, K is a totally real Galois extension of degree 4 over $\mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus, the fundamental theorem of Galois theory implies that K contains exactly two distinct real quadratic subfields $\mathbb{Q}(\sqrt{d_i})$ $(i = 1, 2)$, where $d_i \in \mathbb{R}$ and $0 < d_1 < d_2$. By [18, Proposition 1.5(b), page 193], every prime number different from 2 and p is unramified in K. It follows that $(d_1, d_2) \in \{(2, p), (2, 2p), (p, 2p)\}$, and hence $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$.

Now, we put $\sqrt{2}s_2 = 1 - s_1$. The resultant of the polynomials $f(1 - WT)$ and $W^2 - 2$ with respect to W is equal to $16R(T)$, where

$$R(T) = T^8 + (4z - 8z^2)T^6 + (2 - 16z + 20z^2)T^4 + (4z - 8z^2)T^2 + 1.$$

Since $f(1 - \sqrt{2}s_2) = f(s_1) = 0$, we have $R(s_2) = 0$, and hence s_2 is a unit of K. Furthermore, we have

$$s_1 + \sqrt{2}s_2 = 1.$$

Combining this result with (6), we obtain

$$x = \frac{(s^2 + n^2)^2}{4s(s^2 - n^2)},$$

where s/n is a unit of K such that $(1 - s/n)/\sqrt{2}$ is also a unit of K.

4. The algorithm

Theorem 1 and Lemma 2 yield the following algorithm for the solution of (1):

Input: An integer $n = 2^a p^b$, where p is a prime > 2 and a, b are positive integers not both even.
Output: The integer solutions of (1).

(1) If $p \equiv 1 \pmod 8$ and a is odd, then determine the integer solutions (x, y) of (1) with $-n < x < 0$ and $x = -2^k p^l z$, where $k \geq a$, l is even, k is even if $k > a$ and z is an odd integer which is a perfect square. If $p \equiv 1 \pmod 8$ and a is even, then determine the integer solutions (x, y) of (1) with $-n < x < 0$ and $x = -2^a p^l z$, where l is even and z is an odd integer which is a perfect square. If $p \not\equiv 1 \pmod 8$, then go to step (2).
(2) Determine the integer solutions (x, y) of (1) with $x \in \Sigma_n$.
(3) Determine the set U of units u of $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ such that $(1 - u)/\sqrt{2}$ is also a unit.
(4) Determine the integer solutions (x, y) of (1) with

$$x = \frac{(u^2 + 1)^2 n}{4u(u^2 - 1)} \quad \text{and} \quad u \in U.$$

(5) The points $(0, 0)$, $(-n, 0)$, $(n, 0)$ and the integer solutions computed in steps (1), (2) and (4) are all the integer solutions of (1) exept in cases where $p = 3, 7$ and a, b are odd. If $p = 3$ and a, b are odd, then we have in addition the solutions given by $x = -2^{a-1}3^b$ and $x = -2^a 3^{b-1}$. If $p = 7$ and a, b are odd, then there is in addition the solution given by $x = -2^{a-3}7^b$.

Example 1. The integer solutions to the equation E_6 are

$$(x, y) = (0, 0), (\pm 6, 0), (-3, \pm 9), (-2, \pm 8), (12, \pm 36), (18, \pm 72), (294, \pm 5040).$$

Note that the program *mwrank* of J. Cremona implies that the rank of the elliptic curve E_6 over $\mathbb{Q}$ is equal to 1. Let $\theta = \sqrt{2} + \sqrt{3}$. A $\mathbb{Z}$-basis of the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ obtained by the Magma Computational System is given by the elements

$$\omega_0 = 1,\ \omega_1 = \theta,\ \omega_2 = (\theta^2 - 1)/2,\ \omega_3 = (\theta^3 + \theta^2 - \theta - 1)/4.$$

We represent an algebraic integer of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $z = \sum_{i=0}^{3} z_i \omega_i$, where $z_i \in \mathbb{Z}$ $(i = 0, 1, 2, 3)$, by $[z_0, z_1, z_2, z_3]$. Using Magma, we obtain the solutions (u, v) of the unit equation $u + \sqrt{2}v = 1$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which are listed in Table 1.

The solutions of the unit equation yield the following nontrivial solutions for the elliptic equation: $(x, y) = (12, \pm 36), (18, \pm 72), (294, \pm 5040)$. The other solutions are easily obtained.

Example 2. The integer solutions to the equation E_{194} are

$$(x, y) = (0, 0), (\pm 194, 0), (-144, \pm 1560).$$

TABLE 1.

$([89, 280, 43, -126], [63, 196, 30, -88])$	$([0, 1, -1, 0], [0, -1, -1, 1])$
$([-89, 280, 83, -126], [63, -200, -59, 90])$	$([-1, 2, -1, 0], [0, -3, -2, 2])$
$([-9, 0, -13, -14], [7, 0, 9, 10])$	$([1, -2, 1, 0], [0, -1, 1, 0])$
$([10, 31, 5, -14], [7, 20, 3, -9])$	$([0, -1, 1, 0], [0, -3, 0, 1])$
$([9, 0, 27, -14], [7, -4, 18, -8])$	$([0, 1, 1, 0], [0, -3, -1, 1])$
$([5, 18, 3, -8], [4, 9, 1, -4])$	$([1, 2, 1, 0], [0, -1, -1, 0])$
$([-5, 18, 5, -8], [4, -13, -4, 6])$	$([2, -5, -1, 2], [-1, 2, 1, -1])$
$([4, 9, 1, -4], [2, 7, 1, -3])$	$([-1, -4, -1, 2], [-1, -4, -1, 2])$
$([-4, 9, 3, -4], [2, -11, -3, 5])$	$([1, -4, -1, 2], [-1, 0, 0, 0])$
$([-1, 4, 1, -2], [1, -4, -1, 2])$	$([2, -1, 1, 2], [-1, 0, -1, -1])$
$([1, 4, 1, -2], [1, 0, 0, 0])$	$([4, -9, -3, 4], [-2, 7, 2, -3])$
$([2, 5, 1, -2], [1, 2, 0, -1])$	$([-4, -9, -1, 4], [-2, -11, -2, 5])$
$([2, 1, 3, -2], [1, 0, 2, -1])$	$([5, -18, -5, 8], [-4, 9, 3, -4])$
$([2, 1, 3, -2], [1, 0, 2, -1])$	$([-5, -18, -3, 8], [-4, -13, -2, 6])$
$([-1, -2, -1, 0], [0, -3, 0, 2])$	$([-9, 0, -27, 14], [-7, 0, -19, 10])$
$([0, -1, -1, 0], [0, -1, 0, 1])$	$([10, -31, -9, 14], [-7, 20, 6, -9])$
$([0, 1, -1, 0], [0, -1, -1, 1])$	$([9, 0, 13, 14], [-7, -4, -10, -8])$
$([89, -280, -83, 126], [-63, 196, 58, -88])$	$([-89, -280, -43, 126], [-63, -200, -31, 90])$

By the program *mwrank* of J. Cremona, the rank of the elliptic curve E_{194} over $\mathbb{Q}$ is equal to 2. Let $\theta = \sqrt{2} + \sqrt{97}$. Magma gives the following $\mathbb{Z}$-basis of the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{97})$:

$$\omega_0 = 1,\ \omega_1 = \theta,\ \omega_2 = (\theta^2 + 2\theta + 3)/4,\ \omega_3 = (\theta^3 + 87\theta + 190)/380.$$

We represent an algebraic integer of $\mathbb{Q}(\sqrt{2}, \sqrt{97})$, $z = \sum_{i=0}^{3} z_i\omega_i$ with $z_i \in \mathbb{Z}$ $(i = 0, 1, 2, 3)$, by $[z_0, z_1, z_2, z_3]$. Using Magma again we obtain the solutions of the unit equation $u + \sqrt{2}v = 1$ over $\mathbb{Q}(\sqrt{2}, \sqrt{97})$:

$$(u, v) = ([0, 1, 0, -2], [0, -1, 0, 2]),\ ([2, 1, 0, -2], [1, 0, 0, 0]),$$
$$([-2, -1, 0, 2], [-2, -1, 0, 2]),\ ([0, -1, 0, 2], [-1, 0, 0, 0]).$$

None of these solutions gives an integer point (x, y) on E_{97} with $x > 194$. So, the only nontrivial solution obtained by our algorithm is $(-144, \pm 1560)$.

Example 3. The integer solutions to the equation E_{19336} are

$$(x, y) = (0, 0), (\pm 19336, 0), (-3136, \pm 1068480).$$

The rank of E_{19336} is 2. Put $\theta = \sqrt{2} + \sqrt{2417}$. Magma gives the following $\mathbb{Z}$-basis of the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{2417})$:

$$\omega_0 = 1,\ \omega_1 = \theta,\ \omega_2 = (\theta^2 + 2\theta + 3)/4,\ \omega_3 = (\theta^3 + 2407\theta + 4830)/9660.$$

We represent an algebraic integer of $\mathbb{Q}(\sqrt{2}, \sqrt{2417})$, $z = \sum_{i=0}^{3} z_i\omega_i$ with $z_i \in \mathbb{Z}$ $(i = 0, 1, 2, 3)$, by $[z_0, z_1, z_2, z_3]$. The solutions of the unit equation $u + \sqrt{2}v = 1$ over $\mathbb{Q}(\sqrt{2}, \sqrt{2417})$ are

$$(u, v) = ([0, 1, 0, -2], [0, -1, 0, 2]),\ ([2, 1, 0, -2], [1, 0, 0, 0]),$$
$$([-2, -1, 0, 2], [-2, -1, 0, 2]),\ ([0, -1, 0, 2], [-1, 0, 0, 0]).$$

The above solutions do not provide us with a solution (x, y) on E_{19336} having $x > 19336$. Finally the only solution (x, y) with $-19336 < x < 0$ is $(-3136, \pm 1068480)$.

Acknowledgments

The authors wish to thank the referee for several helpful comments.

References

[1] M. A. Bennett and P. G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, *Proc. Amer. Math. Soc.* 127 (1999), no. 12, 3481-3491. MR1625772 (2000b:11025)
[2] A. Bremner, J. H. Silverman and N. Tzanakis, Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$, *J. Number Theory* 80 (2000), 187-208. MR1740510 (2001i:11066)
[3] Y. Bugeaud, On the size of integer solutions of elliptic equations, *Bull. Austral. Math. Soc.* 57 (1998), 199-206. MR1617363 (99h:11027)
[4] C. Chabauty, Démonstration de quelques lemmes de rehaussement, *C. R. Acad. Sci. Paris* 217 (1943), 413-415. MR0011571 (6:185g)
[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, Heidelberg, 1993. MR1228206 (94i:11105)
[6] J. H. E. Cohn, The Diophantine equation $x^4 - Dy^2 = 1$, II, *Acta Arith.* 78 (1997), 403-409. MR1438594 (98e:11033)
[7] J. E. Cremona, *Algorithms for modular elliptic curves,* Cambridge University Press, Cambridge, 1992. MR1201151 (93m:11053)
[8] K. Draziotis, Integral solutions of the equation $Y^2 = X^3 \pm p^k X$, *Math. Comp.* (to appear).
[9] K. Feng and M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero, *J. Number Theory* 109 (2004), 1-26. MR2098473 (2005j:11040)
[10] J. Gebel and H. G. Zimmer, Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$, pp. 61-83 in *Elliptic curves and related topics,* edited by H. Kisilevsky and M. R. Murty, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994. MR1260955 (95c:11070)
[11] J. Gebel, A. Pethö and H. G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.* 68(2) (1994), 171-192. MR1305199 (95i:11020)
[12] G. Hanrot, Resolution effective d'equations diophantiennes: algorithmes et applications, These, Universite Bordeaux 1 (1997).
[13] T. W. Hungerford, *Algebra,* 2nd Edition, Springer-Verlag, New York, Heidelberg, Berlin, 1980. MR0600654 (82a:00006)
[14] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms,* Springer-Verlag, New York, Berlin, Heidelberg, Tokyo 1984. MR0766911 (86c:11040)
[15] S. Lang, *Elliptic curves: Diophantine analysis,* Springer-Verlag, Berlin, Heidelberg, New York, 1978. MR0518817 (81b:10009)
[16] L. J. Mordell, *Diophantine equations,* Academic Press, London and New York, 1969. MR0249355 (40:2600)
[17] D. Poulakis, Integer points on algebraic curves with exceptional units, *J. Austral. Math. Soc.* 63 (1997), 145-164. MR1475559 (98k:11088)
[18] J. H. Silverman, *Arithmetic of Elliptic Curves,* Springer-Verlag, 1986. MR0817210 (87g:11070)
[19] N. Smart, S-integral points on elliptic curves, *Math. Proc. Cambridge Philos. Soc.* 116(3) (1994), 391-399. MR1291748 (95g:11050)
[20] R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* 67(2) (1994), 177-196. MR1291875 (95m:11056)
[21] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equations, *J. Number Theory* 31(2) (1989), 99-132. MR0987566 (90c:11018)
[22] K. Wildanger, Uber das Losen von Einheiten- und Indexformgleichungen in algebraischen Zahlkorpern. *J. Number Theory* 82(2) (2000), 188–224. MR1761620 (2001c:11140)
[23] http://magma.maths.usyd.edu.au/magma/.

Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

E-mail address: drazioti@math.auth.gr

Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

E-mail address: poulakis@math.auth.gr