MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1493–1505
S 0025-5718(06)01852-7
Article electronically published on April 6, 2006

INTEGER POINTS ON THE CURVE $Y^2 = X^3 \pm p^k X$

KONSTANTINOS A. DRAZIOTIS

ABSTRACT. We completely solve diophantine equations of the form $Y^2 = X^3 \pm p^k X$, where k is a positive integer, using a reduction to some quartic elliptic equations, which can be solved with well known methods.

1. INTRODUCTION—STATEMENT OF RESULTS

As far as we know, there are three general methods for determining the integer points on a given elliptic curve. First, is the classical method of the reduction of the problem to the solution of a finite number of Thue equations [14, p.246], [27]. Next, is the elliptic logarithm method (ELM). It goes back to an idea of S. Lang [10, p.148] and D. Zagier [31]. They proposed a method for proving the finiteness of S-integer points using elliptic logarithms. Also, this idea was proposed by J. H. Silverman [22, p.262]. S. David gave an effective inequality on linear forms of elliptic logarithms [6] and so J. Gebel, A. Pethö, H. Zimmer [7], N. P. Smart [23] and R. J. Stroeker, N. Tzanakis [24], obtained, independently, a practical method for the determination of the integer points on elliptic curves defined over rational numbers. The ELM requires knowledge of the Mordell-Weil basis of the elliptic curve and is feasible for rank ≤ 8 [25]. Note that ELM has proved to be a source of powerful ideas and can be used to study elliptic diophantine equations. Finally, there is one more method based on properties of solutions to Pell equations and Jacobi symbol manipulations [13], [14], [30].

We are dealing with elliptic curves E, with a 2-torsion rational point. More precisely, our results concern the integer points of curves of the form $Y^2 = X^3 \pm p^k X$, where p is a prime and k is a positive integer. We shall determine the integer points of E solving a finite number of quartic elliptic equations, using a reduction through an unramified map. The ideas in this paper are influenced by a paper of K. R. Coombes and D. R. Grant [5], in which they used a similar reduction to compute the rational points on some families of genus 2 curves.

We introduce the following notation.

(1) If C is an algebraic plane curve defined over $\mathbb{Q}$, then we denote by $C(\mathbb{Z})$ the set of its integer points. Let n be a positive integer. We write $n = \square_1 + \square_2$, when there are integers a, b prime to each other, such that $n = a^2 + b^2$. Also, if d is a positive integer, we denote by $\ell(\sqrt{d})$, the period of the continued fraction of $\sqrt{d}$. If $d = d_1\square$, where d_1 is square-free, we set $ns(d) = d_1$

Received by the editor December 2, 2003 and, in revised form, July 29, 2005.
2000 *Mathematics Subject Classification.* Primary 11D25, 11G05.
Key words and phrases. Elliptic curve, 2-torsion point, unramified morphism, Pell equation.
The research of this author was supported by the Hellenic State Scholarships Foundation-I.K.Y.

(ns: *non-square*). Furthermore, if p is a prime number and a is an integer, $(\frac{a}{p})$ denotes the Legendre symbol.

(2) Let d be an integer which is not a square. Let $\epsilon_d = T_1 + U_1\sqrt{d} > 1$ be the minimal unit of the field $K = \mathbb{Q}(\sqrt{d})$ with $N_K(\epsilon_d) = 1$ and $\epsilon_d^k = T_k + U_k\sqrt{d}$ ($k \geq 1$). We consider the prime number q such that $U_1 = q\Box$, if there is one. We set

$$\Lambda'_{d,\beta} = \{(d^{2\beta+3}U_j, \varepsilon d^{3\beta+3}T_j\sqrt{U_j}) : \varepsilon = \pm 1,\ j = 1, 2, q\},$$

and if $d = p$ is a prime number, then we set

$$\Lambda_{p,\beta} = \{(p^{2\beta+1}U_1, \varepsilon p^{3\beta+1}T_1\sqrt{U_1}) : \varepsilon = \pm 1\}.$$

(3) Let (u_d, v_d) be the fundamental solution, if there is one, of the equation $U^2 - dV^2 = -1$. If $d = p$ is a prime, then we set

$$\Delta_{p^r,\beta} = \{(p^{2\beta+r}v_{p^r}, \varepsilon p^{3\beta+r}u_{p^r}\sqrt{v_{p^r}}) : \varepsilon = \pm 1\}$$

and

$$\Delta'_{p,\beta} = \{(p^{2\beta+1}v_{p,r}, \varepsilon p^{3\beta+2}u_{p,r}\sqrt{v_{p,r}}) : \varepsilon = \pm 1\},$$

where $u_{p,r} + v_{p,r}\sqrt{p} = (u_p + v_p\sqrt{p})^r$ and $r = ns(u_p) > 0$ is an odd integer.

(4) If $r \in \mathbb{Z}_{\geq 0}$ and p is a prime number, then we set

$$\begin{aligned}
\Xi_p^r &= \{(-a^2, \pm ab) : (a, b) \in \mathbb{Z}^2 \text{ with } b^2 + a^4 = p^r\},\\
\Xi_{p,+}^r &= \{(a^2, \pm ab) : (a, b) \in \mathbb{Z}^2 \text{ with } b^2 - a^4 = p^r\},\\
\Xi_{p,-}^r &= \{(a^2, \pm ab) : (a, b) \in \mathbb{Z}^2 \text{ with } b^2 - a^4 = -p^r\}.
\end{aligned}$$

We remark that the sets Ξ_p^r and $\Xi_{p,\pm}^r$ can be determined explicitly. We omit the superscript r when $r = 1$.

Let p be a prime number. We consider the curves

$$E_{p^k} : Y^2 = X(X^2 + p^k) \quad \text{and} \quad E_{-p^k} : Y^2 = X(X^2 - p^k)$$

with $k \in \mathbb{Z}_{\geq 1}$.

Theorem 1.1. (i) *For $\beta > 0$ we have*

$$\begin{aligned}
E_{-p^{4\beta}}(\mathbb{Z}) &= \{(0,0), (\pm p^{2\beta}, 0)\},\\
E_{p^{4\beta}}(\mathbb{Z}) &= \{(0,0)\}.
\end{aligned}$$

(ii) *For $\beta \geq 0$ and $p \geq 3$ we have*

$$\begin{aligned}
E_{-p^{4\beta+1}}(\mathbb{Z}) &\subseteq \{(0,0)\} \cup \Delta_{p,\beta} \cup \Xi_p^{4\beta+1} \cup \Xi_{p,-}^{4\beta+1},\\
E_{p^{4\beta+1}}(\mathbb{Z}) &\subseteq \{(0,0)\} \cup \Xi_{p,+}^{4\beta+1} \cup \Lambda_{p,\beta}.
\end{aligned}$$

Also for $\beta \geq 0$,

$$E_{-2^{4\beta+1}}(\mathbb{Z}) = \{(0,0), (2^{2\beta+1}, \pm 2^{3\beta+1}), (2^{2\beta+1}169, \pm 2^{3\beta+1}3107)\} \cup \Xi_2^{4\beta+1} \cup \Xi_{2,-}^{4\beta+1}.$$

(iii) *If $\beta \geq 0$ and $p \neq 5, 29$, then*

$$E_{-p^{4\beta+2}}(\mathbb{Z}) = \{(0,0), (\pm p^{2\beta+1}, 0)\} \cup \Xi_p^{4\beta+2} \cup \Xi_{p,-}^{4\beta+2}.$$

For $p = 5$ we have

$$E_{-5^{4\beta+2}}(\mathbb{Z}) = \{(0,0), (\pm p^{2\beta+1}, 0), (5^{2\beta}45, \pm 5^{3\beta+2}12)\} \cup \Xi_5^{4\beta+2} \cup \Xi_{5,-}^{4\beta+2},$$

and for $p = 29$,

$$E_{-29^{4\beta+2}}(\mathbb{Z}) = \{(0,0), (\pm p^{2\beta+1}, 0), (29^{2\beta+1}99^2, \pm 29^{3\beta+2}180180)\} \cup \Xi_{29}^{4\beta+2} \cup \Xi_{29,-}^{4\beta+2}.$$

Also, for every p and $\beta \geq 0$ we have

$$E_{p^{4\beta+2}}(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Xi_{p,+}^{4\beta+2} \cup \Delta'_{p,\beta}.$$

(iv) *If $\beta \geq 0$ and $p \geq 3$, then*

$$\begin{aligned} E_{-p^{4\beta+3}}(\mathbb{Z}) &\subseteq \{(0,0)\} \cup \Xi_p^{4\beta+3} \cup \Xi_{p,-}^{4\beta+3} \cup \Delta_{p^3,\beta}, \\ E_{p^{4\beta+3}}(\mathbb{Z}) &\subset \{(0,0)\} \cup \Xi_{p,+}^{4\beta+3} \cup \Lambda'_{p,\beta}. \end{aligned}$$

Also, for $\beta > 0$ we have

$$E_{-2^{4\beta+3}}(\mathbb{Z}) = \{(0,0)\} \cup \Xi_2^{4\beta+3} \cup \Xi_{2,-}^{4\beta+3}.$$

Remark 1.2. (i) In the case (iv), if $p \equiv 3 \pmod 4$, then $\Delta_{p^3,\beta} = \emptyset$, since the negative Pell equation $U^2 - pV^2 = -1$ does not have any solution.

(ii) Let r be an odd integer. Then $p^r \neq \square_1 + \square_2$ if and only if $p \equiv 3 \pmod 4$. Thus $\Xi_p^r = \emptyset$ if and only if $p \equiv 3 \pmod 4$.

(iii) The negative Pell equation $U^2 - pV^2 = -1$ is solvable if and only if the period $\ell(\sqrt{p})$ is odd [21], and in this case the solution is

$$u_p = P_{\ell(\sqrt{p})-1}, \quad v_p = Q_{\ell(\sqrt{p})-1},$$

where P_n/Q_n is nth convergent of $\sqrt{p}$. Also see [9] and [18]. So, if $\ell(\sqrt{p})$ is even, then $\Delta_{p,0} = \emptyset$.

(iv) From [8], if $p \equiv 3 \pmod 8$, then the rank of $E_{-p^2}(\mathbb{Q})$ is equal to zero.

(v) In the case (iii), we see that the ranks of $E_{-5^{4\beta+2}}(\mathbb{Q})$ and $E_{-29^{4\beta+2}}(\mathbb{Q})$ are ≥ 1.

Corollary 1.3. *Let p be an odd prime. Then*

$$E_{-p}(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Xi_p \cup \Big\{ \Big(\frac{p+1}{2}, \pm \frac{p-1}{2}\sqrt{\frac{p+1}{2}} \Big) \Big\} \cup \Delta_{p,0}.$$

If $p \equiv 3 \pmod 4$, then

$$E_{-p}(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Big\{ \Big(\frac{p+1}{2}, \pm \frac{p-1}{2}\sqrt{\frac{p+1}{2}} \Big) \Big\}.$$

Moreover, $E_{-p}(\mathbb{Z}) = \{(0,0)\}$ when $p \equiv 3 \pmod 8$.

Corollary 1.4. *Let p be a prime with $p \equiv 3, 63, 67$ or $79 \pmod{80}$, then*

$$E_p(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Big\{ \Big(\frac{p-1}{2}, \pm \frac{p+1}{2}\sqrt{\frac{p-1}{2}} \Big) \Big\} \cup \Lambda_{p,0}.$$

For the other values of $p \pmod{80}$ with $p \neq 5$, we have

$$E_p(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Big\{ \Big(\frac{p-1}{2}, \pm \frac{p+1}{2}\sqrt{\frac{p-1}{2}} \Big) \Big\}.$$

For $p = 5$, we have

$$E_5(\mathbb{Z}) = \{(0,0), (20, \pm 90)\}.$$

Now we give a brief outline of this work. In Section 2 we reduce the problem of the determination of integer points on an elliptic curve, with a 2-torsion point to the solution of a finite number of quartic elliptic equations. In Section 3 we give some auxiliary results. In Section 4 we obtain the proof of Theorem 1.1, and in Section 5 the proof of the corollaries. Some examples are given in Section 6, where we explicitly compute the integer points on some elliptic curves. In Section 7 we obtain a uniform upper bound for the height of integer points for a class of elliptic curves. Finally, Section 8 is devoted to a generalization of the method for curves of the form $C_k : Y^3 = X(X^3 + k)$, where $k \in \mathbb{Z} - \{0\}$.

2. The reduction to the quartic

We consider the curve E defined by the equation

$$E : Y^2 = (X - \rho)h(X),$$

where $\rho \in \mathbb{Z}$, and

$$h(X) = X^2 + eX + k,$$

where e and k are integers. Let $E^{'}$ be the curve defined by the equation

$$Y^{'2} = X^{'4} + (e + 2\rho)X^{'2} + h(\rho)$$

and the morphism $\Psi : E^{'} \to E$ defined by $\Psi = (X^{'2} + \rho, X^{'}Y^{'})$. Since $h(\rho) \neq 0$, we deduce that Ψ is a finite and unramified map of degree two. Let d be a divisor of $h(\rho)$. We consider the curve

$$W_d : X_2^2 = dX_1^4 + (e + 2\rho)X_1^2 + h(\rho)/d,$$

and we define the sets

$$\Pi_d = \{(\varepsilon_1 A\sqrt{d}, \varepsilon_2 B\sqrt{d}) : (A, B) \in W_d(\mathbb{Z}),\ \varepsilon_1 = \pm 1,\ \varepsilon_2 = \pm 1\}$$

and

$$\mathbb{T} = \{(a, b) \in E(\mathbb{Z}) :\ b = 0\}.$$

Proposition 2.1. *We have $E(\mathbb{Z}) = \mathbb{T} \cup \Psi(E^{'}(\mathbb{Z}) \bigcup_{d|h(\rho)} \Pi_d)$, where d runs in the set of square-free divisors of $h(\rho)$.*

Proof. We denote by $\overline{\mathbb{Q}} \subset \mathbb{C}$ the algebraic closure of $\mathbb{Q}$. Let $(a, b) \in E(\mathbb{Z})$ with $b \neq 0$. Since the morphism Ψ is finite, is onto, so there is a point $(a', b') \in E^{'}(\overline{\mathbb{Q}})$ with $\Psi(a, b) = (a', b')$. Let $K = \mathbb{Q}(a', b^{'})$. Since $a'^2 = a - \rho \in \mathbb{Z}$ and $a'b' = b \in \mathbb{Z}$, we deduce that $[K : \mathbb{Q}] \leq 2$ and a' and b' are algebraic integers. We suppose that $(a', b^{'}) \notin E^{'}(\mathbb{Z})$, which is equivalent to $a' \notin \mathbb{Z}$ and $b' \notin \mathbb{Z}$. So there is a square-free integer $d \neq 0, 1$ such that $K = \mathbb{Q}(\sqrt{d})$. Let $\mathbb{O}_K$ be the ring of integers of K. Since $a^{'2} = a - \rho \in \mathbb{Z}$ and $a' \in \mathbb{O}_K - \mathbb{Z}$, we get that $a' = A\sqrt{d}$, where A is an integer. Thus the equality $a'b' = b$ implies $b' = B\sqrt{d}$, where B is an integer. Replacing a' and b' in the equation of E we obtain that $dB^2 = d^2A^4 + (e + 2\rho)dA^2 + h(\rho)$. So $d|h(\rho)$ and $(A, B) \in W_d$. Therefore, $(a', b') \in \Pi_d$ with $d|h(\rho)$. We conclude that $(a, b) \in \Psi(\Pi_d)$ and $d|h(\rho)$. Finally, if $b = 0$, then $(a, b) \in \mathbb{T}$. □

3. Auxiliary lemmas

Lemma 3.1. *Let m be an integer and C_m be the curve defined by the equation $X_2^2 - X_1^4 = m$. We have the following cases.*

(i) *If $m = p$, where p is a prime number, then*

$$C_p(\mathbb{Z}) \subseteq \Big\{ \Big(\pm\sqrt{\frac{p-1}{2}}, \pm\frac{p+1}{2} \Big) \Big\}.$$

(ii) *If $m = -p$, where p is a prime number, then*

$$C_{-p}(\mathbb{Z}) \subseteq \Big\{ \Big(\pm\sqrt{\frac{p+1}{2}}, \pm\frac{p-1}{2} \Big) \Big\}.$$

Proof. (i) Let $(a,b) \in \mathbb{Z}^2$ with $b^2 - a^4 = p$. Without loss of generality, we can assume that $b > 0$. Since $b + a^2 > b - a^2$, we take

$$b - a^2 = 1, \quad b + a^2 = p,$$

so $b = (1+p)/2$, which implies that $a^2 = (p-1)/2$.

(ii) Let $(a,b) \in \mathbb{Z}^2$ with $a^4 - b^2 = p$, and we assume that $b > 0$, as before. Since $a^2 + b > a^2 - b$, we get

$$a^2 - b = 1, \quad a^2 + b = p,$$

so $b = (p-1)/2$, which implies that $a^2 = (p+1)/2$. □

Let M_d be the curve defined by the equation $Y^2 = dX^4 + 1$, where d is a positive integer, which is not a square. We set $M_d^+ = \{(a,b) \in M_d(\mathbb{Z}) : a > 0,\ b > 0\}$ and $\sigma = |M_d^+|$. Let $\epsilon_d = T_1 + U_1\sqrt{d} > 1$ be the minimal unit of the quadratic number field $K = \mathbb{Q}(\sqrt{d})$, with $N_K(\epsilon_d) = 1$ and $\epsilon_d^k = T_k + U_k\sqrt{d}$ $(k \geq 1)$.

Lemma 3.2. *We have $\sigma \leq 2$. Furthermore, we have*

(i) *If d is a prime number $\neq 5$ and $\not\equiv 3, 63, 67$ and $79 \pmod{80}$, then $\sigma = 0$.*

(ii) *If $\sigma = 1$, then $a^2 = U_1$ or U_2 or U_q, where q is a prime $\equiv 3 \pmod 4$, such that $U_1 = q\square$. Furthermore, if d is prime, then $a^2 = U_1$.*

(iii) *If $\sigma = 2$ and $(a_1,b_1), (a_2,b_2) \in M_d^+$, with $a_1 < a_2$, then $a_1^2 = U_1$ and $a_2^2 = U_2$, except when $d = 1785$ and $4 \cdot 1785$, in which case we have $a_1^2 = U_1$ and $a_2^2 = U_4$.*

Proof. By [12] we have $\sigma \leq 2$. Furthermore, [3] implies that if d is a prime number not equal to 5 and $\not\equiv 3, 63, 67$ and $79 \pmod{80}$, then $\sigma = 0$. For the case $d = 3$ we have $\sigma = 2$. Finally, (ii) and (iii) follow from [26] and [29]. □

Let the curves be $\overline{M}_d : Y^2 = dX^4 - 1$, $\overline{R}_d : dY^2 = X^4 - 1$, and $R_d : dY^2 = X^4 + 1$, where d is a positive integer, not a square.

Lemma 3.3. (i) *If $(a,b) \in \overline{M}_d(\mathbb{Z})$ and $d \geq 3$, then $a = \pm\sqrt{v_d}$ and $b = \pm u_d$.*

(ii) *If $(a,b) \in \overline{R}_p(\mathbb{Z})$, where p is a prime, then $b = 0$ for $p \neq 5$, 29. In the case where $p = 5$, we have $(a,b) = (\pm 1, 0)$, $(3, \pm 4)$, and if $p = 29$, then $(a,b) = (\pm 1, 0)$, $(99, \pm 1820)$.*

(iii) *If $(a,b) \in R_d(\mathbb{Z})$, then $(a,b) = (\pm\sqrt{u_{d,r}}, \pm v_{d,r})$ when r is odd; otherwise, $R_d(\mathbb{Z}) = \emptyset$.*

Proof. For the proofs of (i), (ii) and (iii) see [2], [19], and [4], respectively. □

If a is an integer, p a prime number, and i an integer ≥ 0, then we set $a_i = p^{-i}a$. We remark that $a_0 = a$.

Lemma 3.4. (i) *There is no pair $(a,b) \in \mathbb{Z}^2$ such that $b^2 = \pm pa^4 \pm p^{4\beta-1}$, where $\beta \in \mathbb{Z}_{>0}$.*

(ii) *If $(a,b) \in \mathbb{Z}^2$ with $b^2 = \pm pa^4 \pm p^{4\beta}$ where $\beta \in \mathbb{Z}_{\geq 0}$, then $b_{2\beta}, a_\beta \in \mathbb{Z}$ and satisfy $b_{2\beta}^2 = \pm pa_\beta^4 \pm 1$.*

(iii) *If $(a,b) \in \mathbb{Z}^2$ with $b^2 = \pm pa^4 \pm p^{4\beta+1}$ where $\beta \in \mathbb{Z}_{\geq 0}$, then $b_{2\beta+1}, a_\beta \in \mathbb{Z}$ and satisfy $pb_{2\beta+1}^2 = \pm a_\beta^4 \pm 1$.*

(iv) *If $(a,b) \in \mathbb{Z}^2$ with $b^2 = \pm pa^4 \pm p^{4\beta+2}$ where $\beta \in \mathbb{Z}_{\geq 0}$, then $b_{2\beta+1}, a_{\beta+1} \in \mathbb{Z}$ and satisfy $b_{2\beta+1}^2 = \pm p^3 a_{\beta+1}^4 \pm 1$.*

Proof. (i) Let $a=p^{\alpha}a_0$ and $b=p^{\gamma}b_0$ where a_0b_0 is coprime to p. Then we get

$$p^{2\gamma}b_0^2 \mp p^{4\alpha+1}a_0^4 \mp p^{4\beta-1}=0.$$

So two of the orders at p of the numbers $p^{2\gamma}b_0^2$, $p^{4\alpha+1}a_0^4$, and $p^{4\beta-1}$ are equal. Since the exponents are pairwise distinct mod 4, we get a contradiction.

(ii) From the equality $b^2=\pm pa^4\pm p^{4\beta}$, we deduce that $p|a$ and $p|b$. Since two of the orders at p of $b^2, p^{4\beta}$ and pa^4 are equal, we get that the order at p of b is equal to 2β. Then the result follows.

We obtain (iii) and (iv) similarly. □

4. Proof of Theorem 1.1

We consider the curve

$$E'_{\pm p^k} : Y'^2 = X'^4 \pm p^k$$

and the morphism

$$\Phi : E'_{\pm p^k} \to E_{\pm p^k} \quad \text{with} \quad \Phi=(X'^2, X'Y').$$

We determine the sets $W_d(\mathbb{Z})$ and Π_d where $d\in\{\pm1,\pm p\}$.

(i) We first examine the case of the curve $E_{-p^{4\beta}}$. We consider the equations

$$W_{\pm1} : X_2^2=\pm(X_1^4-p^{4\beta}) \quad \text{and} \quad W_{\pm p} : X_2^2=\pm(pX_1^4-p^{4\beta-1}).$$

From Lemma 3.4(i) we have $W_p(\mathbb{Z})=W_{-p}(\mathbb{Z})=\emptyset$. Further, $\Phi(\Pi_{-1})=\Xi_p^{4\beta}$ and $\Phi(\Pi_1)=\Xi_{p,-}^{4\beta}$. From [14, theorem 2, p.17] we have $\Xi_p^{4\beta}=\{(0,0),(-p^{2\beta},0)\}$ and $\Xi_{p,-}^{4\beta}=\{(\pm p^{2\beta},0)\}$. The result follows from Proposition 2.1.

For the case of the curve $E_{p^{4\beta}}$ we consider the equations

$$W_{\pm1} : X_2^2=\pm(X_1^4+p^{4\beta}) \quad \text{and} \quad W_{\pm p} : X_2^2=\pm(pX_1^4+p^{4\beta-1}).$$

From Lemma 3.4(i) we take $W_p(\mathbb{Z})=W_{-p}(\mathbb{Z})=\emptyset$. Also, $W_{-1}(\mathbb{Z})=\emptyset$ and $\Phi(\Pi_1)=\Xi_{p,+}^{4\beta}$. From [14, theorem 1, p.16] we obtain that if $(u,v)\in\mathbb{Z}^2$, such that $v^2=u^4+p^{4\beta}$, then $u=0$, thus $W_1(\mathbb{Z})=\{(0,\pm p^{2\beta})\}$ and so $\Xi_{p,+}^{4\beta}=\{(0,0)\}$. The result follows from Proposition 2.1.

(ii) We examine first the case of the curve $E_{-p^{4\beta+1}}$. We consider the equations

$$W_{\pm1} : X_2^2=\pm(X_1^4-p^{4\beta+1}) \quad \text{and} \quad W_{\pm p} : X_2^2=\pm(pX_1^4-p^{4\beta}).$$

Reasoning as before, from Lemma 3.4(ii) and Lemma 3.3(i) we get

$$\Pi_p=\{(\varepsilon_1\sqrt{p}p^{\beta}\sqrt{v_p}, \varepsilon_2\sqrt{p}p^{2\beta}u_p) : \varepsilon_1=\pm1,\ \varepsilon_2=\pm1\},$$

which gives

$$\Phi(\Pi_p)=\{(p^{2\beta+1}v_p, \varepsilon p^{3\beta+1}u_p\sqrt{v_p}) : \varepsilon=\pm1\}=\Delta_{p,\beta}.$$

If $(a,b)\in W_{-p}(\mathbb{Z})$, then from Lemma 3.4(ii) we get that the only integer solution of $E_{-p^{4\beta+1}}$ is $(0,0)$. Finally, $\Phi(\Pi_1)=\Xi_{p,-}^{4\beta+1}$ and $\Phi(\Pi_{-1})=\Xi_p^{4\beta+1}$. Now, the result follows from Proposition 2.1.

We now study the curve $E_{p^{4\beta+1}}$. As before, we have that $\Phi(\Pi_1)=\Xi_{p,+}^{4\beta+1}$ and $W_{-1}(\mathbb{Z})=\emptyset$. From Lemma 3.4(ii) and Lemma 3.2 we get

$$\Phi(\Pi_p)=\{(p^{2\beta+1}U_1, \varepsilon p^{3\beta+1}T_1\sqrt{U_1} : \varepsilon=\pm1\}=\Lambda_{p,\beta}.$$

Finally, $W_{-p}(\mathbb{Z})=\emptyset$. The result follows from Proposition 2.1.

For the case of the curve $E_{-2^{4\beta+1}}$ we have

$$W_{\pm1} : X_2^2=\pm(X_1^4-2^{4\beta+1}) \quad \text{and} \quad W_{\pm2} : X_2^2=\pm(2X_1^4-2^{4\beta}).$$

Let $(a,b) \in W_2(\mathbb{Z})$, then from Lemma 3.4(ii) we have

$$\overline{b}^2 = 2\overline{a}^4 + 1,$$

where $a = 2^\beta \overline{a}$ and $b = 2^{2\beta}\overline{b}$. From [11] we have $(\overline{a}, \overline{b}) = (\pm 1, \pm 1)$ or $(\pm 13, \pm 239)$. So $(a,b) = (\pm 2^\beta, \pm 2^{2\beta})$ or $(\pm 2^\beta 13, \pm 239 \cdot 2^{2\beta})$. Finally, $\Phi(\Pi_1) = \Xi_{2,-}^{4\beta+1}$ and $\Phi(\Pi_{-1}) = \Xi_2^{4\beta+1}$.

(iii) First, we examine the case of the curve $E_{-p^{4\beta+2}}$. We consider the equations

$$W_{\pm 1} : X_2^2 = \pm(X_1^4 - p^{4\beta+2}) \quad \text{and} \quad W_{\pm p} : X_2^2 = \pm(pX_1^4 - p^{4\beta+1}).$$

If $(a,b) \in W_p(\mathbb{Z})$, then from Lemma 3.4(iii) we get

$$p\overline{b}^2 = \overline{a}^4 - 1,$$

where $b = p^{2\beta+1}\overline{b}$ and $a = p^\beta \overline{a}$. From Lemma 3.3(ii) there are $\overline{a}$, $\overline{b}$ such that $p\overline{b}^2 = \overline{a}^4 - 1$ only if $p \in \{5, 29\}$. So $\Pi_p = \{(\pm 1, 0)\}$, when $p \neq 5, 29$ and

$$\Pi_5 = \{(\varepsilon_1 3 \cdot 5^\beta \sqrt{5}, \varepsilon_2 4 \cdot 5^{2\beta+1}\sqrt{5}) : \varepsilon_1 = \pm 1, \varepsilon_2 = \pm 1\},$$

$$\Pi_{29} = \{(\varepsilon_1 99 \cdot 29^\beta \sqrt{29}, \varepsilon_2 1820 \cdot 29^{2\beta+1}\sqrt{29}) : \varepsilon_1 = \pm 1, \varepsilon_2 = \pm 1\}.$$

So,

$$\Phi(\Pi_5) = \{(45 \cdot 5^{2\beta}, \pm 12 \cdot 5^{3\beta+2})\}$$

and

$$\Phi(\Pi_{29}) = \{(29^{2\beta+1} \cdot 99^2, \pm 180180 \cdot 29^{3\beta+2})\}.$$

If $(a,b) \in W_{-p}(\mathbb{Z})$, then from Lemma 3.4(iii) we get

$$p\overline{b}^2 = -\overline{a}^4 + 1,$$

where $b = p^{2\beta+1}\overline{b}$ and $a = p^\beta \overline{a}$, so the only integer solution is $\overline{b} = 0$, $\overline{a} = \pm 1$, which gives $b = 0$, $a = \pm p^\beta$. Therefore, $\Pi_{-p} = \{(\sqrt{p}p^\beta, 0)\}$, which through Φ gives the integer points $(\pm p^{2\beta+1}, 0)$ of the curve $E_{-p^{4\beta+2}}$. Finally, $\Phi(\Pi_1) = \Xi_{p,-}^{4\beta+2}$ and $\Phi(\Pi_{-1}) = \Xi_p^{4\beta+2}$.

Now we study the curve $E_{p^{4\beta+2}}$. We have $\Phi(\Pi_1) = \Xi_{p,+}^{4\beta+2}$ and $W_{-1}(\mathbb{Z}) = \emptyset$. From Lemma 3.4(iii) and Lemma 3.3(iii) we take

$$\Pi_p = \{(\varepsilon_1 p^\beta \sqrt{u_{p,r}}\sqrt{p}, \varepsilon_2 p^{2\beta+1} v_{p,r}\sqrt{p}) : \varepsilon_1 = \pm 1,\ \varepsilon_2 = \pm 1\},$$

where $r = ns(u_p)$ is odd. We conclude therefore that $\Phi(\Pi_p) = \Delta'_{p,\beta}$. Finally, $W_{-p}(\mathbb{Z}) = \emptyset$.

(iv) We first study the case of the curve $E_{-p^{4\beta+3}}$. As before, from Lemma 3.4(iv) and Lemma 3.3(i) we get

$$\Phi(\Pi_p) = \{(p^{2\beta+3} v_{p^3}, \varepsilon p^{3\beta+3} u_{p^3}\sqrt{v_{p^3}}) : \varepsilon = \pm 1\} = \Delta_{p^3,\beta}.$$

From Lemma 3.4(iv) we take $\Pi_{-p} = \{(0, \varepsilon p^{2\beta+1}\sqrt{p}) : \varepsilon = \pm 1\}$ which through the morphism Φ gives the point $(0,0)$ on the curve $E_{-p^{4\beta+3}}$. Finally, $\Phi(\Pi_1) = \Xi_{p,-}^{4\beta+3}$ and $\Phi(\Pi_{-1}) = \Xi_p^{4\beta+3}$.

For the case of the curve $E_{p^{4\beta+3}}$ we have $\Phi(\Pi_1) = \Xi_{p,+}^{4\beta+3}$ and $W_{-1}(\mathbb{Z}) = \emptyset$. Also, $\Phi(\Pi_p) = \Lambda_{p,\beta}$. The result follows from Proposition 2.1.

For the case of the curve $E_{-2^{4\beta+3}}$ we consider the equations

$$W_{\pm 1} : X_2^2 = \pm(X_1^4 - 2^{4\beta+3}) \quad \text{and} \quad W_{\pm 2} : X_2^2 = \pm(2X_1^4 - 2^{4\beta}).$$

Let $(a,b)\in W_2(\mathbb{Z})$, then from Lemma 3.4(iv) we have

$$\overline{b}^2 = 8\overline{a}^4 - 1,$$

where $a = 2^{\beta+1}\overline{a}$ and $b = 2^{2\beta+1}\overline{b}$. Since the equation $Y^2 = 8X^4 - 1$ does not have any integer solution, we obtain $W_2(\mathbb{Z}) = \emptyset$. If $(a,b)\in W_{-2}(\mathbb{Z})$, then Lemma 3.4(iv) gives

$$\overline{b}^2 = -8\overline{a}^4 + 1,$$

where $a = 2^{\beta+1}\overline{a}$ and $b = 2^{2\beta+1}\overline{b}$. Noticing that the equation $Y^2 = -8X^4 + 1$ has the unique integer solution, $(X,Y) = (0,\pm 1)$, we get

$$W_{-2}(\mathbb{Z}) = \{(0, \varepsilon 2^{2\beta+1}) : \varepsilon = \pm 1\},$$

so $\Pi_{-2} = \{(0, \varepsilon i 2^{2\beta+1}) : \varepsilon = \pm 1,\ i^2 = -1\}$. Therefore, $\Phi(\Pi_{-2}) = \{(0,0)\}$. Finally, reasoning as before $\Phi(\Pi_1) = \Xi_{2,-}^{4\beta+3}$ and $\Phi(\Pi_{-1}) = \Xi_2^{4\beta+3}$.

5. Proof of Corollaries 1.3 and 1.4

Proof of Corollary 1.3. For $\beta = 0$, Theorem 1.1(ii) gives:

$$E_{-p}(\mathbb{Z}) \subseteq \{(0,0)\} \cup \Delta_{p,0} \cup \Xi_p \cup \Xi_{p,-}.$$

By Lemma 3.1(ii) we have

$$W_1(\mathbb{Z}) \subseteq \Big\{\Big(\pm\sqrt{\frac{p+1}{2}}, \pm\frac{p-1}{2}\Big)\Big\}.$$

Therefore,

$$\Psi(W_1(\mathbb{Z})) = \Xi_{p,-} \subseteq \Big\{\Big(\frac{p+1}{2}, \pm\frac{p-1}{2}\sqrt{\frac{p+1}{2}}\Big)\Big\}.$$

The result follows.

Let $p \equiv 3 \pmod 4$. Then -1 is not a quadratic residue mod p and so the equation $X_2^2 - pX_1^2 = -1$ is not solvable. Thus $\Delta_{p,0} = \emptyset$. Further, by Remark 1.2(ii), we have $\Xi_p = \emptyset$.

If $p \equiv 3 \pmod 8$, then the integer $(p+1)/2$ is not a square and so $E_{-p}(\mathbb{Z}) = \{(0,0)\}$. □

Proof of Corollary 1.4. From Lemma 3.1(i) we have

$$W_1(\mathbb{Z}) \subseteq \Big\{\Big(\pm\sqrt{\frac{p-1}{2}}, \pm\frac{p+1}{2}\Big)\Big\}.$$

So

$$\Xi_{p,+} \subseteq \Big\{\Big(\frac{p-1}{2}, \pm\frac{p+1}{2}\sqrt{\frac{p-1}{2}}\Big)\Big\}.$$

Also, if $p \neq 5$ is a prime number $\not\equiv 3, 63, 67$ and $79 \pmod{80}$, then Lemma 3.2(i) gives $\Lambda_{p,0} = \emptyset$.

From [3] if $p = 5$, then the equation $X_2^2 = 5X_1^4 + 1$, has only the integer solution $(X_1, X_2) = (\pm 2, \pm 9)$, so $W_5(\mathbb{Z}) = \{(\pm 2, \pm 9)\}$. Also, $W_1(\mathbb{Z}) = \emptyset$. Finally, $W_{-5}(\mathbb{Z}) = W_{-1}(\mathbb{Z}) = \emptyset$. So $E_5(\mathbb{Z}) = \{(0,0), (20, \pm 90)\}$. □

6. Examples

(i) In the following tables we give the set $E_{\pm p^k}(\mathbb{Z})$ for some prime numbers p and $k = 1$ or 2. In the last column, using `mwrank` by Cremona, we calculated the rank of the free abelian group $E_{\pm p^k}(\mathbb{Q})$.

$p = 17$	$(0,0), (-1, \pm 4), (-4, \pm 2), (9, \pm 24), (17, \pm 68)$	2
$p = 41$	$(0,0), (-4, \pm 10)$	1
$p = 53$	$(0,0), (1325, \pm 48230)$	1
$p = 97$	$(0,0), (-4, \pm 18), (-9, \pm 12), (49, \pm 336)$	2
$p = 241$	$(0,0), (-4, \pm 30), (121, \pm 1320)$	2
$p = 337$	$(0,0), (-9, \pm 48), (-16, \pm 36), (169, \pm 2184)$	2
$p = 5521$	$(0,0), (-36, \pm 390), (23326225, \pm 112659207180)$	2
$p = 7577$	$(0,0), (-64, \pm 472)$	1
$p = 8101$	$(0,0), (-1, \pm 90), (8101, \pm 729090)$	1
$p = 12101$	$(0,0), (12101, \pm 1331110)$	1

Integer Points of E_{-p}

By Corollary 1.3 and the fact that $|\Xi_p| = |\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 = p\}| \leq 4$, the set $E_{-p}(\mathbb{Z})$ has at most nine elements. As we see in the above table, the curve E_{-17} has exactly nine integer points.

$p = 3$	$(0,0), (1, \pm 2), (3, \pm 6), (12, \pm 42)$	1
$p = 19$	$(0,0), (9, \pm 30)$	1
$p = 83$	$(0,0), (747, \pm 20418)$	1
$p = 163$	$(0,0), (81, \pm 738)$	1
$p = 1459$	$(0,0), (729, \pm 19710)$	1

Integer Points of E_p

$p = 5$	$(0,0), (-4, -6), (\pm 5, 0), (44, \pm 300)$	1
$p = 29$	$(0,0), (\pm 29, 0), (284229, \pm 151531380)$	1

Integer Points of E_{-p^2}

$p = 17$	$(0,0), (68, \pm 578), (144, \pm 1740)$	2
$p = 179$	$(0,0)$	1
$p = 577$	$(0,0), (166464, \pm 67917720)$	2
$p = 1297$	$(0,0), (46692, \pm 10093254)$	2
$p = 1889$	$(0,0)$	2

Integer Points of E_{p^2}

Using the notation of Theorem 1.1, we fix $\beta = 1$ and give a table for the set $E_{\pm p^{4\beta+r}}(\mathbb{Z})$ for various values of r, p. For the first and second example, $r = 1$; the third $r = 2$, and the fourth $r = 3$. Using `mwrank`, we can see that the rank is $\neq 0$ for all the previous curves.

$-p = 53$	$(0,0), (3721925, \pm 7180337710)$
$-p = 5521$	$(0,0), (711016951090225, \pm 18959196686713747963980)$
$p = 17$	$(0,0), (19652, \pm 2839714), (41616, \pm 8548620)$
$-p = 7$	$(0,0)$

Integer Points of $E_{\pm p^{4\beta+r}}$

(ii) Below we give an example concerning elliptic curves of the form $Y^2 = X(X^2+pq)$. We consider the curve of rank 1, $E_{1261} : Y^2 = X^3+1261X$. The curves where E_{1261} is reduced are $W_{\pm 1} : Y'^2 = \pm X'^4 \pm 1261$, $W_{\pm 13} : Y'^2 = \pm 13X'^4 \pm 97$, $W_{\pm 97} : Y'^2 = \pm 97X'^4 \pm 13$ and $W_{\pm 1261} : Y'^2 = \pm 1261X'^4 \pm 1$. The equation $Y'^2 = 13X'^4+97$ does not have any integer solution. Indeed, if there is one (a', b'), then 97 should be a quadratic residue mod 13, which is impossible. So $W_{13}(\mathbb{Z}) = \emptyset$. Also, $W_{97}(\mathbb{Z}) = \emptyset$. If not then there is a point (a', b') such that $b'^2 = \pm 97a'^4 \pm 13$, with $13 \nmid a'$, then 97 should be a quadratic residue (mod 13). If $13|a'$ we conclude that $13|1$, which is impossible. Finally, since $1261 \equiv 13 \pmod{16}$, from [15] we take $W_{1261}(\mathbb{Z}) = \{(0,0)\}$. Also $W_1(\mathbb{Z}) = \emptyset$, so $E_{1261}(\mathbb{Z}) = \{(0,0)\}$.

7. A uniform bound for a class of elliptic curves

In Theorem 7.1 we confirm the Hall-Lang-Stark conjecture [28, Conj. 5.5.5.1, p.74] for a subfamily of the family of elliptic curves with at least one 2-torsion rational point. Now let $\mathcal{F}$ be the of set elliptic curves E defined by the equation

$$Y^2 = (X-\rho)h(X), \quad \rho \in \mathbb{Z},$$

where

$$h(X) = X^2 + eX + k \in \mathbb{Z}[X] \quad \text{and} \quad h(\rho) = \pm 1.$$

We set

$$H = \max\{|a_i| : a_i \text{ is coefficient of } (X-\rho)h(X)\}.$$

Theorem 7.1. *If $E \in \mathcal{F}$ and $(a, b) \in E(\mathbb{Z})$, then*

$$|a| < 11H^2 + 5.$$

Proof. From Proposition 2.1, it suffices to find a polynomial bound for the height of integer points of the curves:

$$W_+ : X_2^2 = X_1^4 + \Delta X_1^2 \pm 1 \quad \text{and} \quad W_- : X_2^2 = -X_1^4 + \Delta X_1^2 \mp 1,$$

where $\Delta = e + 2\rho$. Let $(A, B) \in W_-(\mathbb{Z})$. Then $(2B)^2 + (2A^2 - \Delta)^2 = \Delta^2 \mp 4$, thus $(2B)^2 \leq |\Delta^2 \pm 4|$. We suppose that $A^2 \neq \Delta$, then $A^2 < |A^2(-A^2+\Delta)| = |B^2 \pm 1| < (\Delta^2+8)/4$. But $a = (Ai)^2 + \rho$ where $i = \sqrt{-1}$. So

$$|a| = |(Ai)^2 + \rho| \leq A^2 + |\rho| < (\Delta^2 + 8 + 4|\rho|)/4.$$

If $A^2 = \Delta$, then

$$|a| = |(Ai)^2 + \rho| = |-\Delta + \rho| \leq |\Delta| + |\rho|.$$

If $(A, B) \in W_+(\mathbb{Z})$, then using [16, Theorem 1] we take

$$|a| < \Delta^2 + |\Delta|/2 + 5 + |\rho|.$$

The theorem follows since $|\Delta| \leq 3H$ and $|\rho| \leq H$. To prove that $|\Delta| \leq 3H$ we remark on three things:

(i) We have $|e| \leq 2H$.

(ii) $H = \max\{|e-\rho|, |k-e\rho|, |k\rho|\} \geq 2$. First, we see that $H \neq 0$ since if $H = 0$, then $k = \rho = 0$, which is a contradiction. Now we prove that $H \neq 1$. Indeed, if $H = 1$, then $e - \rho = \pm 1$, $k - e\rho = \pm 1$, and $k\rho = \pm 1$. Combining these equalities, with $h(\rho) = \pm 1$, we get a contradiction. So $H \geq 2$.

(iii) We have $|\Delta| \leq H + 3|\rho|$.

We prove that $3|\rho| \leq 2H$. Assume that $k \neq 0$. Then $|\rho| \leq H/|k|$. It is enough to show that $|k| \geq 3/2$ and since k is integer it is enough to prove that $|k| \geq 2$. If not, then $|k| = 1$. If $k = 1$, then $\rho^2 + e\rho + 1 = \pm 1$, so $\rho^2 + e\rho = 0$ or $\rho^2 + e\rho = -2$. Using $H \geq 2$, all the cases give the desired result. It is similar for the cases $k = -1$ and $k = 0$. Finally, we see that $|\Delta|/2 + |\rho| \leq (1.5 + 1)H < 2H$, which implies $|a| < 11H^2 + 5$. □

8. A generalization of the method

In light of the previous results, we give a generalization of the method provided by Proposition 2.1. Let $k \in \mathbb{Z} - \{0\}$ and C_k, $C_k^{'}$ be the curves defined by equations $Y^3 = X(X^3 + k)$ and $Y^{'3} = X^{'9} + k$, respectively. We consider the morphism $\Psi : C_k^{'} \to C_k$, where $\Psi = (X^{'3}, X^{'}Y^{'})$. Let d be a cube-free integer. We set

$$\begin{aligned} W_{1,d} &= \{(\sqrt[3]{a}, b) : b^3 - da^3 = \frac{k}{d^2}, \text{with } a, b \in \mathbb{Z} \text{ and } d^2 | k\}, \\ W_{2,d} &= \{(\sqrt[3]{a}, b) : b^3 - d^5a^3 = \frac{k}{d}, \text{with } a, b \in \mathbb{Z} \text{ and } d | k\}, \end{aligned}$$

where $\sqrt[3]{a}$ is the real cubic root of the integer a. Furthermore, we set

$$\mathbb{B} = \{(a, b) \in C_k(\mathbb{Z}) : b = 0\}.$$

Proposition 8.1. $C_k(\mathbb{Z}) \subseteq \mathbb{B} \bigcup \Psi(C_k^{'}(\mathbb{Z})) \bigcup_{d^2|k} \Psi(W_{1,d}(\mathbb{Z})) \bigcup_{d|k} \Psi(W_{2,d}(\mathbb{Z}))$.

Proof. Let $(a, b) \in C_k(\mathbb{Z})$ and $b \neq 0$. Since Ψ is a finite map, it is onto. So there is a point $(a^{'}, b^{'}) \in C_k^{'}$ with $\Psi(a, b) = (a^{'}, b^{'})$. We suppose that $(a^{'}, b^{'}) \notin C_k^{'}(\mathbb{Z})$. Then we can choose $a^{'}, b^{'} \notin \mathbb{Z}$. Since $a^{'3} = a$ we take $a^{'} = A\theta$ or $A\theta^2$, where $A \in \mathbb{Z} - \{0\}$ and $\theta = \sqrt[3]{d}$ (the real root) for some cube-free integer $d \neq 0, 1$. But $b^{'} \in \mathbb{Q}(\theta)$, so $b^{'} = b_0 + b_1\theta + b_2\theta^2$ for some $b_j \in \mathbb{Q}$ $(j = 0, 1, 2)$. However, $b^{'3} \in \mathbb{Z}$, so we have $(b_0 + b_1\theta + b_2\theta^2)^3 \in \mathbb{Z}$ and after some calculations we get $b^{'} = b_1\theta$ or $b_2\theta^2$. But $a^{'}b^{'}$ is an integer. So $(a^{'}, b^{'}) = (A\theta, B\theta^2)$ or $(A\theta^2, B\theta)$, with $A, B \in \mathbb{Z}$. If $(a^{'}, b^{'}) = (A\theta, B\theta^2)$, then $(A, B) \in W_{1,d}(\mathbb{Z})$, and if $(a^{'}, b^{'}) = (A\theta^2, B\theta)$, then $(A, B) \in W_{2,d}(\mathbb{Z})$. Finally, if $b = 0$, then $(a, b) \in \mathbb{B}$. □

Let $C_k : Y^3 = X(X^3 + k)$, where k is a positive integer. As an application for the previous proposition, we prove that if k is an odd prime p, then there are at most 12 integer points on the curve C_p. We note that from [1, Theorem 1.4] we have $|W_{2,p}| \leq 10$. Now we prove that $|C_p'(\mathbb{Z})| \leq 2$. Indeed, if $(a, b) \in \mathbb{Z}^2$ is such that $b^3 - a^9 = p$, then $(x-y)(x^2+xy+y^2) = p$, where $(x, y) = (b, a^3)$. If $x^2+xy+y^2 = 1$, then $(2x+y)^2+3y^2 = 4$, which gives $(x, y) = (\pm 1, 0), (0, \pm 1), (-1, 1), (1, -1)$. Since $x - y = p$ and p is an odd prime, we have a contradiction. Now if $x - y = 1$, then $p = 3a^6 + 3a^3 + 1$ which has at most two real roots with respect to a, when p is fixed. From Proposition 8.1 we take $|C_p(\mathbb{Z})| \leq 12$. If we let p to run over such primes which are solutions to the equation $b^3 - p^5a^3 = 1$ for some integers a and b, then the ABC conjecture suggests

$$p^5|a|^3 \ll (|ab|p)^{1+\varepsilon} \ll a^{2(1+\varepsilon)}p^{8/3(1+\varepsilon)},$$

which has finitely many solutions in a and p if $\varepsilon < 1/2$. So the set $\bigcup W_{2,p}$ as p runs over all such primes is finite under the ABC conjecture. Also the Schinzel hypothesis H [20] seems to suggest that there are infinitely many prime numbers p of the form $3a^6 + 3a^3 + 1$.

Finally, Proposition 8.1 provides us with a reduction of the study of integer points on the curve C_k, to the study of a finite number of Thue equations of degree 3, which can be solved with algorithms implemented to many computer algebra systems, such as Kant, Maple, Magma. For instance, when using Maple, if $p = 7$, we have $W_{2,7} = \{(0,0)\}$. Also, $C_7'(\mathbb{Z}) = \{(1,2)\}$, so $C_7(\mathbb{Z}) = \{(0,0),(1,2)\}$.

Acknowledgments

The author is indebted to the referee and Professor D. Poulakis for their very careful reading and very nice suggestions.

References

[1] Bennett, Michael A. On the representation of unity by binary cubic forms. Trans. Amer. Math. Soc. **353** (2001), no. 4, 1507–1534 MR1806730 (2002i:11031)

[2] Chen, Jian Hua; Voutier, Paul, Complete solution of the Diophantine equation $X^2+1 = dY^4$ and a related family of quartic Thue equations. J. Number Theory **62** (1997), no. 1, 71–99. MR1430002 (97m:11039)

[3] Cohn J.H.E., The Diophantine equation $y^2 = Dx^4 + 1$ III. Math. Scand. **42** (1978), 180 - 188. MR0512268 (80a:10031)

[4] ———, The Diophantine equation $x^4 + 1 = Dy^2$. Math. Comp. **66** (1997), no. 219, 1347–1351. MR1415800 (98e:11032)

[5] Coombes, K.R.; Grant D.R., On heterogeneous spaces, J.London. Math.Soc (2) **40** (1989), no.3, 385-397. MR1053609 (91d:11069)

[6] David, Sinnou, Minorations de formes linéaires de logarithmes elliptiques. (French) [Lower bounds for linear forms in elliptic algorithms] Mém. Soc. Math. France (N.S.) No. **62** (1995), iv+143 pp. MR1385175 (98f:11078)

[7] Gebel, J.; Pethö, A.; Zimmer, H. G., Computing integral points on elliptic curves. Acta Arith. **68** (1994), no. 2, 171–192. MR1305199 (95i:11020)

[8] Genocchi, Sur l'impossibilite de quelques egalites doubles, C. R. Acad.Sci. Paris, **78** (1874), 423-436.

[9] Grytczuk, Aleksander; Luca, Florian; Wójtowicz, Marek, The negative Pell equation and Pythagorean triples. Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), no. 6, 91–94. MR1769976 (2001c:11033)

[10] Lang, Serge, Elliptic curves: Diophantine analysis. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 231.Springer-Verlag, Berlin-New York, 1978. xi+261 pp. ISBN: 3-540-08489-4. MR0518817 (81b:10009)

[11] Ljunggren, W., Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Norsk. Vid. Akad. Oslo 1-27 (1942). MR0016375 (8:6f)

[12] ———, Einige Eigenschften der Einheiten reel Quadratischer und rein-bi-quadratischer Zahlkorper. Skr. Norske Vid. Akad. Oslo I, v.1936, no.12.

[13] Luca, F.; Walsh, P. G., A generalization of a theorem of Cohn on the equation $x^3-Ny^2 = \pm 1$. Rocky Mountain J. Math. **31** (2001), no. 2, 503–509. MR1840950 (2002g:11027)

[14] Mordell, L.J., Diophantine Equations. Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York 1969 xi+312 pp. MR0249355 (40:2600)

[15] ———, The Diophantine equation $Y^2 = DX^4 + 1$. J. London Math. Soc. **39** 1964 161–164. MR0162761 (29:65)

[16] Poulakis, Dimitrios, A simple method for solving the Diophantine equation $Y^2 = X^4+aX^3+bX^2+cX+d$. Elem. Math. **54** (1999), no. 1, 32–36. MR1669371 (2000a:11040)

[17] Poulakis, D.; Walsh, G., A note on the Diophantine equation $x^2 - dy^4 = 1$ with prime discriminant, Comptes Rendues Math. Sci. Canada **27** (2005), no. 2, 54–57. MR2142959

[18] Rose H.E., A course in number theory, second edition, Oxford science publications, 1994. ISBN 0-19-852376-9. MR1352868 (96g:11001)

[19] Samuel, Pierre, Résultats élémentaires sur certaines équations diophantiennes. (French) [Elementary results for some Diophantine equations] J. Théor. Nombres Bordeaux **14** (2002), no. 2, 629–646. MR2040698 (2004m:11041)

[20] Schinzel, A.; Sierpiński, W. Sur certaines hypothèses concernant les nombres premiers. (French) Acta Arith. **4** (1958), 185–208; erratum 5 1958 259. MR0106202 (21:4936)

[21] Sierpinski, W., Elementary Theory of Numbers. Polish Scientific Publishers, Warszawa (1987). MR0930670 (89f:11003)

[22] Silverman, J. H., The Arithmetic of Elliptic Curves, Springer-Verlag,1986. MR0817210 (87g:11070)

[23] Smart, N. P., S-integral points on elliptic curves. Math. Proc. Cambridge Philos. Soc. **116** (1994), no. 3, 391–399. MR1291748 (95g:11050)

[24] Stroeker, R. J.; Tzanakis, N., Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. Acta Arith. **67** (1994), no. 2, 177–196. MR1291875 (95m:11056)

[25] Stroeker, Roel J.; Tzanakis, Nikos, On the elliptic logarithm method for elliptic Diophantine equations: reflections and an improvement. Experiment. Math. **8** (1999), no. 2, 135–149. MR1700575 (2000d:11043)

[26] Togbe, A.; Voutier, P. M.; Walsh, P. G., Solving a family of Thue equations with an application to the equation $x^2 - dy^4 = 1$, Acta Arith. **120** (2005), 39–58. MR2189717

[27] Tzanakis N.; B. M. M. de Weger, On the practical solution of the Thue equations, J. Number Theory **31**(2) (1989), 99-132. MR0987566 (90c:11018)

[28] Vojta, Paul, Diophantine approximations and value distribution theory. Lecture Notes in Mathematics, **1239**. Springer-Verlag, Berlin, 1987. x+132 pp. ISBN: 3-540-17551-2. MR0883451 (91k:11049)

[29] Walsh, G., Diophantine equations of the form $aX^4 - bY^2 = \pm 1$. Algebraic number theory and Diophantine analysis, Proceedings of the International Conference in Graz 1998, Walter de Gruyter, Berlin 2000, pp.531-554. MR1770484 (2001h:11034)

[30] Walsh, G., A note on a theorem of Ljunggren and the Diophantine equations $x^2 - kxy^2 + y^4 = 1, 4$. Archiv der Mathematik **73** (1999), no.2, 119-125. MR1703679 (2000i:11048)

[31] Zagier, Don, Large integral points on elliptic curves. Math. Comp. **48** (1987), no. 177, 425–436. MR0866125 (87k:11062)

42 G. Passalidi St., Thessaloniki 54453, Greece
E-mail address: `drazioti@gmail.com`