International Journal of Pure and Applied Mathematics

Volume 21 No. 3 2005, 367-386

ON THE DIOPHANTINE EQUATION $X^4 - DY^4 = \pm Z^2$ AND ITS ASSOCIATED ELLIPTIC CURVE $V^2 = U^3 - DU$

Omar Kihel[1], Claude Levesque[2] §

[1]Department of Mathematics
Brock University
St. Catharines, Ontario, L2S 3A1, CANADA
e-mail: okihel@brocku.ca

[2]Département de Mathématiques et de Statistique
Centre Interuniversitaire en Calcul Mathématique Algébrique (CICMA)
Université Laval
Québec, G1K 7P4, CANADA
e-mail: cl@mat.ulaval.ca

Abstract: We plan to study the Diophantine equations $X^4 - DY^4 = Z^2$ and $x^4 - Dy^4 = -z^2$, where $D \in \mathbf{Z}$. In particular, when $D = p$ or $-p$, where p is a prime, we give a characterization of all the solutions of $X^4 - DY^4 = Z^2$. We conclude with exploiting some links between the title equation and the associated elliptic curve $E : V^2 = U^3 - DU$.

AMS Subject Classification: 11D25, 11G05
Key Words: Diophantine equations, quartic equations, elliptic curves

1. Introduction

The purpose of this paper is to study the Diophantine equations

$$X^4 - DY^4 = Z^2 \tag{1.1}$$

and

$$x^4 - Dy^4 = -z^2, \tag{1.2}$$

where D is assumed throughout this paper to be a *non-zero fourth-power free*

Received: May 5, 2005
© 2005, Academic Publications Ltd.
§Correspondence author

integer. Some results were obtained by Mordell [6] and we know (see chapter 9 of [7]) that Euler and Lagrange studied (1.1) and (1.2) when $D = 2$.

We will describe all types of solutions of (1.1) when $D = p$ (Section 3) and when $D = -p$ (Section 4), p being an odd prime. We will use in Section 5 some properties of the elliptic curve $E : V^2 = U^3 - DU$ that one can associate to (1.1) and (1.2) to characterize the solutions of (1.1). In particular, when P is a point on the elliptic curve E, the values of $3P$ will prove very useful. We will exhibit three possible types of solutions when $D = p$ and four types when $D = -p$. Some examples will show that all these types can occur. We believe that the knowledge of all these types of solutions may later prove useful to study the parity conjecture for the title elliptic curve.

Let us first recall that any positive integral solution X_1, Y_1, Z_1 of (1.1) with $\gcd(X_1, Y_1) = 1$, $D \in \mathbf{Z}$, $D \neq 0$, leads to a new positive solution X_2, Y_2, Z_2 of (1.1), namely,

$$X_2 = |X_1^4 + DY_1^4|, \quad Y_2 = 2X_1Y_1Z_1, \quad Z_2 = \left|Z_1^4 - 4DX_1^4Y_1^4\right|,$$

hence to a new positive solution $\widetilde{X}_2$, $\widetilde{Y}_2$, $\widetilde{Z}_2$ of (1.1) with $\gcd(\widetilde{X}_2, \widetilde{Y}_2) = 1$, namely,

$$\widetilde{X}_2 = \frac{X_2}{\gcd(X_2, Y_2)}, \quad \widetilde{Y}_2 = \frac{Y_2}{\gcd(X_2, Y_2)}, \quad \widetilde{Z}_2 = \frac{Z_2}{(\gcd(X_2, Y_2))^2}. \tag{1.3}$$

Let us explain that this leads to an infinite number of solutions of (1.1). Since Y_1 is coprime to $\gcd(X_2, Y_2) = \gcd(X_2, 2X_1Y_1Z_1)$, we have

$$\widetilde{Y}_2 \;=\; \frac{2X_1Z_1}{\gcd(X_2, Y_2)}Y_1 \;>\; Y_1$$

as soon as $2X_1Z_1 > \gcd(X_2, Y_2)$. Suppose the contrary, i.e. suppose

$$2X_1Z_1 \;=\; \gcd(X_2, Y_2) \;=\; \gcd(X_2, 2X_1Y_1Z_1).$$

Then $2X_1Z_1 \mid X_2 = X_1^4 + DY_1^4 = Z_1^2 + 2DY_1^4$. Hence $2|Z_1$ and $2\not|Y_1$ (otherwise, $2|Y_1$ and $2|X_1$). Therefore, $4 \mid 2X_1Z_1$, $4 \mid Z_1^4 + 2DY_1^4$ and $2|D$. From $X_1^4 - DY_1^4 = Z_1^2$, we get $2|X_1$, so $4|D$. Hence 8 divides $2X_1Z_1$, i.e., $8 \mid Z_1^2 + 2DY_1^4$, whereupon $4|Z_1$. Therefore $16 \mid Z_1^2 = X_1^4 - DY_1^4$ and $16|D$, which contradicts the hypothesis that D is fourth-power free. In conclusion, indeed $\widetilde{Y}_2 > Y_1$.

A solution X, Y, Z of (1.1) is said to be *trivial* if $XY = 0$. As a matter of fact, we are interested in non-trivial solutions (X, Y, Z) with $\gcd(X, Y) = 1$ since solutions of the form (tX, tY, t^2Z) with $t > 1$ offer nothing new.

On the one hand, one knows from [6], or from p. 23 of [7], some values of D for which (1.1) has no solution.

Theorem 1.1. (Lind-Nagell-Pocklington) *If*

$$D = \begin{cases} p & \textit{with} \quad p \equiv 7 \textit{ or } 11 & (\mathrm{mod}\ 16)\,, \\ 2p & \textit{with} \quad p \equiv 3 \textit{ or } 5 & (\mathrm{mod}\ 8)\,, \\ 4p & \textit{with} \quad p \equiv 3,\ 11 \textit{ or } 13 & (\mathrm{mod}\ 16)\,, \\ -p & \textit{with} \quad p \equiv 3,\ 11 \textit{ or } 13 & (\mathrm{mod}\ 16) \end{cases}$$

(*p being a prime*), *then the Diophantine equation*

$$X^4 + DY^4 = Z^2 \qquad (\textit{resp.} \quad X^4 - 4DY^4 = Z^2)$$

has no non-trivial solution with $\gcd(X, Y) = 1$.

On the other hand, there are some obvious values of D for which we can exhibit one solution of (1.1) (hence an infinite number of solutions because of (1.3)). For instance, Churchhouse noticed (see [6]) that if

$$D = -(4a^4 + b^2),$$

then $X = b$, $Y = 2a$, $Z = 8a^4 + b^2$ is a solution of (1.1).

Along the same lines (see p. 25 of [7]), if

$$D = u^2 + uv^2 \neq 0,$$

for some non-zero $u, v \in \mathbf{Z}$, with v odd and $\gcd(u, v) = 1$, then $X = |v^2 + 2u|$, $\quad Y = 2|v|$, $\quad Z = \left|v^4 - 4uv^2 - 4u^2\right|$ is a solution of (1.1).

Another family of examples is given by

$$D = A^4 - B^2 \neq 0,$$

where A, $B \in \mathbf{N}$ with $\gcd(A, B) = 1$, an obvious solution of (1.1) being

$$X = A, \quad Y = 1, \quad Z = B.$$

When

$$D = -r^2 s^4 + 2rt^2 \neq 0,$$

where $r \in \mathbf{Z}\backslash\{0\}$, and where s, $t \in \mathbf{N}$ with $\gcd(s, t) = 1$, one solution of (1.1) is

$$X = t, \quad Y = s, \quad Z = |rs^4 - t^2|.$$

2. Preliminaries and Remarks

In general, it is difficult to know if (1.1) is solvable. Thanks to Mordell [6], we know the following:

- *If the only solution of* $X^4-4abY^4=Z^2$ *is* $Y=0$, *then the only solution of* $ax^4+by^4=z^2$ *is* $xy=0$, *since* $(ax^4-by^4)^2=z^4-4ab(xy)^4$.
- *If the only solution of* $X^4+DY^4=Z^2$ *is* $Y=0$, *then the only solution of* $ax^4+by^4=z^2$ *with* $ab=-4D$ *is* $xy=0$, *since* $(ax^4-by^4)^2=z^4+D(2xy)^4$.

In particular, we have the following result.

Theorem 2.2. (Mordell) *The Diophantine equation* $X^4-DY^4=Z^2$ *has a non-trivial solution if and only if* $x^4+4Dy^4=z^2$ *has a non-trivial solution.*

Proof. This follows from the two identities

$$z^4-D(2xy)^4=(x^4-4Dy^4)^2 \quad \text{and} \quad Z^4+4D(XY)^4=(X^4+DY^4)^2. \tag{2.1}$$

From (2.1), we know that if we have a solution of one of the two equations of Theorem 2.2, we have a solution of the other equation. Does it mean that if we know all the solutions of one of the two equations, we can deduce all the solutions of the other equation as described by (2.1)? The answer is "yes" only if $D=p$ or $-p$, p being a prime, as can be seen from the next proposition.

Proposition 2.3. *Let* $e\in\{1,-1\}$ *and let* D *be a non-zero fourth-power free integer. If* X, Y, Z *is a positive solution in pairwise coprime integers of*

$$X^4-4eDY^4=Z^2, \tag{2.2}$$

then

$$X=z, \quad Y=xy, \quad Z=\left|D_1x^4-eD_2y^4\right|, \tag{2.3}$$

where x, y, $z\in\mathbf{N}$ *with* $\gcd(x,y)=1$ *is a solution of*

$$D_1x^4+eD_2y^4=z^2 \quad \text{or} \quad D_1x^4+eD_2y^4=ez^2, \tag{2.4}$$

with $D=D_1D_2$ *and* $\gcd(D_1,D_2)=1$. *Conversely, if* $D=D_1D_2$ *with* $\gcd(D_1,D_2)=1$ *and if* x, y, z *is a positive solution in pairwise coprime integers of any equation in* (2.4), *then the integers* X, Y, Z *defined in* (2.3) *provide a positive solution of* (2.2) *with* $\gcd(X,Y)=1$.

Proof. When $e=1$, it is understood that (2.4) reduces to one equation.

(i) Let X, Y, Z be a positive solution in pairwise coprime integers of (2.2). Since the equation $X^4 - Z^2 = (X^2 + Z)(X^2 - Z) = 4eDY^4$ implies

$$\text{either} \quad \begin{cases} X^2 \pm Z &= 2eD_1A^4, \\ X^2 \mp Z &= 2D_2B^4, \end{cases} \quad \text{or} \quad \begin{cases} X^2 \pm Z &= 2D_1A^4, \\ X^2 \mp Z &= 2eD_2B^4, \end{cases}$$

where $D = D_1D_2$ and $Y = AB$ with $\text{GCD}(D_1, D_2) = gcd(A, B) = 1$, we obtain

$D_1A^4 + eD_2B^4 = eX^2$ or $D_1A^4 + eD_2B^4 = X^2$, $Y = AB$, $Z = D_1A^4 - eD_2B^4$.

(ii) Conversely, consider pairwise coprime positive integers x, y, z which satisfy either $D_1x^4 + eD_2y^4 = z^2$ or $D_1x^4 + eD_2y^4 = ez^2$ where $D = D_1D_2$ with $\text{GCD}(D_1, D_2) = 1$. Proceeding as on p. 22 of [7], we have

$$\text{either} \quad D_1x^4 + eD_2y^4 = \left(\frac{z^2}{x^2}\right)x^2 \quad \text{or} \quad D_1x^4 + eD_2y^4 = e\left(\frac{z^2}{x^2}\right)x^2$$

with $\dfrac{z^2}{x^2} \in \mathbf{Q}$. Hence we respectively obtain

$$\text{either} \quad D_1x^4 - \left(\frac{z^2}{x^2}\right)x^2 + eD_2y^4 = 0 \quad \text{or} \quad D_1x^4 - e\left(\frac{z^2}{x^2}\right)x^2 + eD_2y^4 = 0,$$

so there exists $v \in \mathbf{Q}$ such that $\left(\dfrac{z^2}{x^2}\right)^2 - 4eD_1D_2y^4 = v^2$ (as a discriminant), i.e.,

$$z^4 - 4eD(xy)^4 = (x^2v)^2$$

with $x^2v \in \mathbf{N}$ and $\text{GCD}(z, xy) = 1$. In practice, $x^2v = D_1x^4 - eD_2y^4$, i.e., $v = D_1x^2 + eD_2\dfrac{y^4}{x^2}$. □

For the sequel, it may help to note that if $D = p$ or $-p$ (p being a prime), we have the following property for a non-trivial integral solution X, Y, Z: $\text{GCD}(X, Y) = 1$ if and only if X, Y, Z are pairwise coprime integers.

3. On the Solutions of $X^4 - pY^4 = Z^2$

Let us investigate some values of p for which we can characterize the non-trivial solutions (when they exist) of $X^4 - pY^4 = Z^2$. First, a general result.

Proposition 3.1. *Let p be an odd prime. Suppose there exists a positive solution X, Y, Z of*

$$X^4 - pY^4 = Z^2 \tag{3.1}$$

in pairwise coprime integers. Then it has one of the following three types:

Type A. $X = a^4 + pb^4,\ Y = 2abc,\ Z = \left|c^4 - 4pa^4b^4\right|,$ *where* a, b, c, *with* c *odd are pairwise coprime integers which verify*

$$a^4 - pb^4 = ec^2 \ \text{ with } \ e = 1 \text{ or } -1. \tag{3.2}$$

Type B. $X = \frac{1}{2}\left(a^4 + pb^4\right),\ Y = 2abc,\ Z = \left|4c^4 - pa^4b^4\right|,$ *where* a, b, c *with* a, b *odd are pairwise coprime integers which verify*

$$a^4 - pb^4 = e(2c)^2 \ \text{ with } \ e = 1 \text{ or } -1. \tag{3.3}$$

Type C. $X = c,\ Y = ab,\ Z = |c^2 - pb^4| = \frac{1}{2}\left|a^4 - pb^4\right| = |a^4 - c^2|,$ *where* a, b, c *with* a, b *odd are pairwise coprime integers which verify*

$$a^4 + pb^4 = 2c^2. \tag{3.4}$$

Proof. (1) Suppose Y is even, so X and Z are odd. Hence $\text{GCD}(X^2 - Z,\ X^2 + Z) = 2,$ whereupon

$$\text{either } \begin{cases} X^2 \pm Z &= 8pw^4, \\ X^2 \mp Z &= 2c^4, \\ Y &= 2wc \ (c \ \text{ odd}), \end{cases} \quad \text{or} \quad \begin{cases} X^2 \pm Z &= 2pw^4, \\ X^2 \mp Z &= 8c^4, \\ Y &= 2wc \ (w \ \text{odd}), \end{cases} \tag{3.5}$$

with $\text{GCD}(w, c) = 1.$

(i) The first system of equations of (3.5) leads to

$$X^2 = c^4 + 4pw^4, \quad \text{i.e.,} \quad (X - c^2)(X + c^2) = 4pw^4.$$

Since $\text{GCD}(X + c^2,\ X - c^2) = 2,$ we obtain

$$X \pm c^2 = 2pb^4, \quad X \mp c^2 = 2a^4,$$

where $w = ab$ with $\text{GCD}(a, b) = 1.$ Hence $a^4 - pb^4 = \mp c^2$ and we have a solution of Type A:

$$X = a^4 + pb^4, \quad Y = 2abc, \quad Z = \left|c^4 - 4pa^4b^4\right|.$$

(ii) The latter system of equations in (3.5) leads to $X^2 = pw^4 + 4c^4,$ i.e., to $(X - 2c^2)(X + 2c^2) = pw^4$ with $\text{GCD}(X - 2c^2,\ X + 2c^2) = 1,$ hence to

$$X \pm 2c^2 = pb^4, \quad X \mp 2c^2 = a^4,$$

where $w = ab$ with $\text{GCD}(a, b) = 1$ and $2 \nmid ab$, from which we deduce $a^4 - pb^4 = \mp(2c)^2$, so we have a solution of Type B:

$$X = \frac{1}{2}(a^4 + pb^4), \quad Y = 2abc\,, \quad Z = \left|4c^4 - pa^4b^4\right|.$$

(2) Suppose that Y is odd, so either Z is even (and $2 \nmid X$) or X is even (and $2 \nmid Z$). Then $(X^2 + Z)(X^2 - Z) = pY^4$, whereupon

$$X^2 \pm Z = pb^4, \quad X^2 \mp Z = a^4, \quad Y = ab\,,$$

with $\text{GCD}(a, b) = 1$ and $2 \nmid ab$. Hence $a^4 + pb^4 = 2X^2$ and we have a solution of Type C:

$$Y = ab\,, \quad Z = \frac{1}{2}\left|a^4 - pb^4\right|. \qquad \square$$

In fact, Types A and B take care of the possibility of Y even (and $2 \nmid XZ$) and Type C takes care of the possibility of Y odd (and $2|XZ$). Note that each time (a, b, c) verifies $a^4 - pb^4 = c^2$, then $(X, Y, Z) = (a^4 + pb^4, 2abc, |c^4 - 4pa^4b^4|)$ verifies $X^4 - pY^4 = Z^2$ This leads to the following theorem.

Theorem 3.2. *Let p be an odd prime. Suppose that the set S of positive solutions of*

$$X^4 - pY^4 = Z^2 \tag{3.6}$$

in pairwise coprime integers is non empty. Then S is infinite and we have the following:

(i) *Let $p \equiv 1 \pmod{16}$. Then the solutions are of Type A or of Type B, or of Type C (with X odd) and Type A with $e = 1$ always occurs. Moreover, at least one of the following types also occurs: Type A with $e = -1$, or Type B with $e = 1$ or -1, or Type C. Finally, Type C occurs if and only if Type B with $e = 1$ occurs.*

(ii) *Let $p \equiv 5 \pmod{16}$. Then they are of Type A with $e = 1$, or of Type B with $e = -1$, and both possibilities occur.*

(iii) *Let $p \equiv 7$ or $15 \pmod{16}$. Then they are of Type A with $e = 1$, or of Type C (with X even), and both possibilities occur.*

(iv) *Let $p \equiv 9 \pmod{16}$. Then they are of Type A with $e = 1$ or -1, and both possibilities occur.*

Proof. We explained in Section 2 that because of (1.3), S is infinite.

(i) Let $p \equiv 1 \pmod{16}$. It is easy to show that X is never even, so last proposition gives the result. If Type A with $e = -1$, Type B and Type C never occur, then a descent argument gives that a solution of (3.6) of Type A with $e = 1$ and with the smallest Y involves a solution of (3.2) with again $e = 1$ such that $b < Y$. This is a contradiction.

Suppose that Type C occurs. Then (3.4) holds for some a, b, c with a, b odd. Reading (3.4) (mod 16) forces c to be odd, whereupon the integer $Z = \frac{1}{2}\left|a^4 - pb^4\right| = c^2 - pb^4$ in Type C is even. So we have the equality $X^4 - pY^4 = Z^2$ with Z even, which is of the form (3.3) with $e = 1$. Hence we have Type B with $e = 1$.

Conversely, suppose that Type B occurs with $e = 1$. Then we have (3.3) with $e = 1$ for some integers a, b, c with a, b odd: $a^4 - pb^4 = 4c^2$. Therefore $a^4 - 4c^2 = (a^2 + 2c)(a^2 - 2c) = pb^4$, whereupon

$$\begin{cases} a^2 \pm 2c &= b_1^4, \\ a^2 \mp 2c &= pb_2^4. \end{cases}$$

Hence $b_1^4 + pb_2^2 = 2a^2$, i.e., we have (3.4) which leads to a solution of Type C.

Let us prove that Type A with $e = 1$ always occurs. By hypothesis, there exists a non-trivial solution X_1, Y_1, Z_1 of (3.1). If Z_1 is odd, we have a solution in integers X_1, Y_1, Z_1 of (3.2) which generates a solution X, Y, Z of Type A with $e = 1$. If Z_1 is even, then we have a solution of (3.3) which can be used to obtain a solution X, Y, Z of Type B with $e = 1$, where $Z = 4Z_1^4 - pX_1Y_1^4$ is odd, so we can conclude as before.

(ii) Let $p \equiv 5 \pmod{16}$. Looking at all the possible congruences modulo 16, we conclude that Y is even. Moreover, it is impossible to have $e = -1$ in (3.2) since c is odd. It is also impossible to have $e = 1$ in (3.3). A descent argument as above gives that Type B must occur.

(iii) Let $p \equiv 7$ or $15 \pmod{16}$. It is easy to see that Z must be odd. Moreover, if Y is even, Type A with $e = -1$ never occurs, and Type B never occurs because (3.3) is impossible with $e \in \{1, -1\}$. If X is even, we have Type C. A descent argument gives that Type C must occur.

(iv) Let $p \equiv 9 \pmod{16}$. Here Y is even, because the contrary implies $Y^4 \equiv 1 \pmod{16}$, $Z^2 \equiv X^4 - 9 \equiv -9$ or $-8 \pmod{16}$, which is impossible. So X and Z are odd and Type C never occurs. Moreover, Type B never occurs, since (3.3) is impossible. Again a descent argument can be used to conclude that Type A with $e = -1$ must occur. □

Examples. Here are some types of solutions of $X^4 - pY^4 = Z^2$.

(mod 16)	p	a	b	c	X	Y	Z	Types
$p \equiv 1$	17	1	1	3	3	1	8	C
	17	1	1	4	9	4	47	B $(e=-1)$
	17	3	1	4	49	24	353	B $(e=1)$
	17	2	1	1	33	4	1087	A $(e=-1)$
	17	9	4	47	10913	3384	109334207	A $(e=1)$
$p \equiv 5$	5	1	1	1	3	2	1	B $(e=-1)$
	5	3	2	1	161	12	25919	A $(e=1)$
$p \equiv 7$	7	1	1	2	2	1	3	C
	7	2	1	3	23	12	367	A $(e=1)$
$p \equiv 9$	41	2	1	5	57	20	1999	A $(e=-1)$
	41	57	20	1999	17116001	4557720	261021442247999	A $(e=1)$
$p \equiv 15$	31	1	1	4	4	1	15	C
	31	4	1	15	287	120	18881	A $(e=1)$

4. On the Solutions of $X^4 + pY^4 = Z^2$

Now let us concentrate on $X^4 + pY^4 = Z^2$. Let us recall from [6] that if the prime p is congruent to 1 (mod 8) and if 2 is not a quartic residue modulo p, then the only solutions of (4.1) are the trivial ones. First a general result.

Proposition 4.1. *Let p be an odd prime. Suppose there exists a positive solution of*

$$X^4 + pY^4 = Z^2 \tag{4.1}$$

in pairwise coprime integers. Then it has one of the following four types:

Type a. $X = \left|a^4 - pb^4\right|, \quad Y = 2abc, \quad Z = c^4 + 4pa^4b^4,$ *where a, b, c with c odd are pairwise coprime integers which verify*

$$a^4 + pb^4 = c^2. \tag{4.2}$$

Type b. $X = \frac{1}{2}\left|a^4 - pb^4\right|, \quad Y = 2abc, \quad Z = 4c^4 + pa^4b^4,$ *where a, b, c with a, b odd are pairwise coprime integers which verify*

$$a^4 + pb^4 = (2c)^2. \tag{4.3}$$

Type c. $X = c, \quad Y = 2ab, \quad Z = -c^2 + 2pb^4 = 4a^4 + pb^4 = 8a^4 + c^2,$ *where a, b, c with b, c odd are pairwise coprime integers which verify*

$$4a^4 - pb^4 = -c^2. \tag{4.4}$$

Type d. $X = c\,, \quad Y = ab\,, \quad Z = ec^2 + pb^4 = \frac{1}{2}(a^4 + pb^4) = |a^4 - ec^2|$, *where* a, b, c *with* a, b *odd are pairwise coprime integers which verify*

$$a^4 - pb^4 = 2ec^2 \quad \textit{with} \quad e = 1 \textit{ or } -1. \tag{4.5}$$

Proof. (1) Suppose Y is even, so X and Z are odd. Hence $\gcd(Z+X^2,\, Z-X^2) = 2$, whereupon

$$\text{either } \begin{cases} Z \pm X^2 &= 8pw^4\,, \\ Z \mp X^2 &= 2c^4\,, \\ Y &= 2wc \ (c \text{ odd})\,, \end{cases} \quad \text{or } \begin{cases} Z \pm X^2 &= 2pw^4\,, \\ Z \mp X^2 &= 8c^4\,, \\ Y &= 2wc \ (w \text{ odd})\,, \end{cases} \tag{4.6}$$

with $\gcd(w, c) = 1$.

(i) The former system of equations leads to

$$c^4 - 4pw^4 = \mp X^2. \tag{4.7}$$

Considering (4.7) modulo 4, we conclude that the minus sign can never occur. Hence $c^4 - X^2 = 4pw^4$, i.e.,

$$c^2 \mp X = 2a^4, \quad c^2 \pm X = 2pb^4$$

where $w = ab$ with $\gcd(a, b) = 1$. Hence $a^4 + pb^4 = c^2$ and we have a solution of Type a:

$$X = \left|a^4 - pb^4\right|\,, \quad Y = 2abc\,, \quad Z = c^4 + 4pa^4b^4.$$

(ii) The second system in (4.6) gives

$$4c^4 - pw^4 = \mp X^2. \tag{4.8}$$

Suppose first $4c^4 - pw^4 = X^2$, so $(2c^2 + X)(2c^2 - X) = pw^4$. Then

$$2c^2 \pm X = a^4, \quad 2c^2 \mp X = pb^4$$

with $w = ab$, $2 \nmid ab$ and $\gcd(a, b) = 1$. Hence $a^4 + pb^4 = (2c)^2$ and we have a solution of Type b. Next suppose $4c^4 - pw^4 = -X^2$. Then we have a solution of Type c:

$$X = c_1\,, \quad Y = 2cw\,, \quad Z = 4c^4 + pw^4. \tag{4.9}$$

(2) Suppose Y is odd. Now

$$Z \pm X^2 = a^4, \quad Z \mp X^2 = pb^4, \tag{4.10}$$

with $Y = ab$, $2 \not| ab$ and $\text{GCD}(a, b) = 1$. This gives

$$a^4 - pb^4 = \pm 2X^2 \tag{4.11}$$

and we have a solution of Type d. □

We can again note that each time (a, b, c) verifies $a^4 + pb^4 = c^2$, then $(X, Y, Z) = (|a^4 - pb^4|, 2abc, c^4 + 4pa^4b^4)$ verifies $X^4 + pY^4 = Z^2$. This leads to the following theorem.

Theorem 4.2. *Let p be an odd prime. Suppose that the set S of positive solutions of*

$$X^4 + pY^4 = Z^2 \tag{4.12}$$

in pairwise coprime integers is non empty. Then S is infinite and we have the following:

(i) *Let $p \equiv 3$ or 15 (mod 16). Then the solutions are of Type a or of Type b (with X, Z odd) or of Type d (with $e = -1$ when $p \equiv 3$ (mod 16) and with $e = 1$ when $p \equiv 15$ (mod 16)). Moreover, all three types occur.*

(ii) *Let $p \equiv 5$ or 13 (mod 16). Then they are of Type a, or of Type c, and both types occur.*

(iii) *Let $p \equiv 1$ (mod 8). Then they are of Type a, or of Type c, or of Type d. Moreover, Type c or Type d occurs and Type a always occurs.*

Proof. Iterations of (1.3) lead to an infinite set S.

(i) Let $p \equiv 3$ (mod 16). Let Y be even, so we obtain (4.6). This leads first to Type a or to Type b (with X, Z odd), and the minus sign cannot occur in (4.8). Next let Y be odd. We then obtain (4.10) and (4.11), and the plus sign in (4.11) cannot occur. When $p \equiv 15$ (mod 16), the proof is the same except that $e = 1$.

Let us show that Type b occurs if and only if Type d occurs. If Type b occurs, then $(a^2 + 2c)(a^2 - 2c) = -pb^4$, and as for Theorem 3.2, we have (4.5), i.e., Type d. If Type d occurs, then we have (4.5), c odd, Z even, so we have Type b. A descent argument gives the last statement: it is obvious that Type a always occurs; moreover, a solution (a, b, c) of Type a comes from a solution (a_1, b_1, c_1) verifying $a_1^4 + pb_1^4 = c_1^2$ with $b_1 < b$, so we cannot have only Type a solutions.

(ii) Let $p \equiv 5$ or 13 (mod 16), so Y has to be even. Then we consider (4.6) and we see that the plus sign cannot occur in (4.8). A descent argument secures the rest.

(iii) Let $p \equiv 1 \pmod 8$. Let Y be even, so we obtain (4.6). We saw that (4.7) is impossible with the minus sign and that the plus sign corresponds to a solution of Type a. Next we can have (4.8), but (4.8) is impossible with the plus sign, and we get (4.9). If Y is odd, then we obtain (4.10), (4.11) and Type d. A descent argument secures the rest. □

Examples. Here are some types of solutions of $X^4 + pY^4 = Z^2$.

(mod 16)	p	a	b	c	X	Y	Z	Types
$p \equiv 1$	113	3	1	4	4	3	97	d $(e=-1)$
	113	2	1	7	7	4	177	c
	113	4	3	97	8897	2328	98233729	a
$p \equiv 3$	3	1	1	1	1	1	2	d $(e=-1)$
	3	1	1	1	1	2	7	b
	3	1	2	7	47	28	2593	a
$p \equiv 5$	5	1	1	1	1	2	9	c
	5	1	2	9	79	36	6881	a
$p \equiv 9$	73	3	1	2	2	3	77	d $(e=-1)$
	73	2	1	3	3	4	137	c
	73	2	3	77	5897	924	35531473	a
$p \equiv 13$	13	1	1	3	3	2	17	c
	13	3	2	17	127	204	150913	a
$p \equiv 15$	31	3	1	5	5	3	56	d $(e=1)$
	31	3	1	5	943	840	402799	b
	31	5	3	36	1886	1680	16111996	a

5. On the Associated Elliptic Curve $V^2 = U^3 - DU$

Suppose that $(X, Y, Z) = (a, b, c)$ $(b \neq 0)$ is a non-trivial (positive) solution of

$$X^4 - DY^4 = eZ^2 \quad \text{with} \quad e \in \{1, -1\}. \tag{5.1}$$

Then it is well known that $P = (U, V)$ with

$$U = \frac{ea^2}{b^2} \quad \text{and} \quad V = \frac{ac}{b^3} \tag{5.2}$$

is a rational point of the associated elliptic curve

$$E : V^2 = U^3 - DU. \tag{5.3}$$

Conversely, suppose that $P = (U, V) = \left(\frac{ea^2}{b^2}, \frac{ac}{b^3}\right)$ is a rational point of (5.3). Then it is direct to verify that (a, b, c) is a non-trivial solution of (5.1). Moreover, the duplication formula (see p. 59 of [8]) gives

$$2P = \left(\frac{A^2}{B^2}, \frac{AC}{B^3}\right) \quad \text{with} \quad \begin{cases} A = a^4 + Db^4, \\ B = 2abc, \\ C = c^4 - 4Da^4b^4, \end{cases}$$

where $A^4 - DB^4 = C^2$. Then (see p. 59 of [8]) the first component of $3P = P + 2P$ is

$$x(3P) \quad = \quad \left(\frac{ACb^3 - acB^3}{Bb(A^2b^2 - ea^2B^2)}\right)^2 - \frac{A^2b^2 + ea^2B^2}{B^2b^2},$$

i.e.,

$$x(3P) = \frac{A^2C^2b^6 - 2ACB^3acb^3 + a^2c^2B^6 + eA^4B^2b^4a^2 + a^4b^2A^2B^4 - A^6b^6 - ea^6B^6}{B^2b^2(A^2b^2 - ea^2B^2)^2}. \quad (5.4)$$

We claim that

$$x(3P) = \frac{eb^2c^2A^2B^4 - 2b^3cAB^3Ca + eB^2C^2a^2b^4}{B^2b^2(A^2b^2 - ea^2B^2)^2} = e\frac{(ABc - eabC)^2}{(A^2b^2 - ea^2B^2)^2}. \quad (5.5)$$

To see it, just replace in (5.5) and in (5.6) each C^2 by $(A^4 - DB^4)$ and each c^2 by $e\left(a^4 - Db^4\right)$. After similar calculations for the second component of $3P$, we deduce that

$$3P = \left(\frac{eF^2}{G^2}, \frac{FH}{G^3}\right)$$

with

$$\begin{cases} F = ABc - eabC, \\ G = A^2b^2 - ea^2B^2, \\ H = -Cc(eA^2b^2 + a^2B^2) - 2ABab(DB^2b^2 - eA^2a^2). \end{cases} \quad (5.6)$$

The duplication formula (5.4) explains now the well known fact that the solution X_2, Y_2, Z_2 of (1.1) which is exhibited in (1.3) comes from taking the double of

$$P = \left(\frac{eX_1^2}{Y_1^2}, \frac{X_1Z_1}{Y_1^3}\right)$$

and implies that the rank of E is ≥ 1. The proof that $\text{rank}(E) \geq 1$ is obvious: if $Y^2 \neq 1$, then the first component $x(P)$ of P is not in $\mathbf{Z}$, so P is not a torsion point of E because of the Lutz-Nagell Theorem ([8], p. 221); if $Y_1^2 = 1$, then

$$x(2P) = \left(\frac{X_1^4 + D}{2X_1Z_1}\right)^2 \notin \mathbf{Z}$$

(the argument being the same as the one following (1.3)), so $2P$ is not a torsion point.

We also have that $\widetilde{P} = (\widetilde{U}, \widetilde{V})$, with

$$\widetilde{U} = \frac{-Db^2}{a^2} \quad \left(\text{resp. } \widetilde{U} = \frac{Db^2}{a^2}\right) \quad \text{and} \quad \widetilde{V} = \frac{Dbc}{a^3}, \tag{5.7}$$

where $a \neq 0$, is a rational point of (5.3): $\widetilde{V}^2 = \widetilde{U}^3 - D\widetilde{U}$. One verifies that $P - \widetilde{P} = (0, 0)$, where $(0, 0)$ is a rational point of E of order 2.

Elliptic curves, in particular, the values of $2P$ and $3P$, will prove useful in the proof of the following theorem.

Theorem 5.1. *Let p be an odd prime. Suppose there is a positive solution in pairwise coprime integers of $X^4 - pY^4 = Z^2$ of a given type. Then that type of solution occurs infinitely often.*

Proof. The proof is divided in three parts.

(1) The result is true for Type A with $e = 1$; it suffices to look at $2P$ and to remark that in (5.4) the integers A, B and C are pairwise coprime integers with C odd.

Let us assume that we have a solution X, Y, Z of Type A with $e = -1$, whereupon there are integers a, b, c such that $a^4 - pb^4 = -c^2$ with c odd. Then

$$P = \left(-\frac{a^2}{b^2}, \frac{ac}{b^3}\right)$$

is a rational point of infinite order of the elliptic curve E defined in (5.3). Now by (5.7),

$$3P = \left(-\frac{F^2}{G^2}, \frac{FH}{G^3}\right)$$

with $F^4 - pG^4 = -H^2$. From Theorem 3.2, we know that $p \equiv 1$ or $9 \pmod{16}$; this implies that a is even and b is odd. Hence $2 \not| A$, $2 \not| C$, $2 | B$, $2 | F$, $2 \not| G$ and, most importantly, $2 \not| H$. Then $\widetilde{F}^4 - p\widetilde{G}^4 = \widetilde{H}^2$ with

$$\widetilde{F} = \frac{F}{\text{GCD}(F, G)}, \quad \widetilde{G} = \frac{G}{\text{GCD}(F, G)}, \quad \widetilde{H} = \frac{H}{(\text{GCD}(F, G))^2},$$

and we have $\text{GCD}(\widetilde{F}, \widetilde{G}) = 1$ and $2 \not| \widetilde{H}$.

(2) Suppose now there exists a solution of Type B. We have to remember that if $e = -1$ (resp. $e = 1$), then by Theorem 3.2, we have $p \equiv 1$ or $5 \pmod{16}$ (resp. $p \equiv 1 \pmod{16}$). Suppose that $a^4 - pb^4 = ec^2$ with c even. Consider

$$3P = \left(e\frac{F^2}{G^2}, \frac{FH}{G^3} \right),$$

where $F^4 - pG^4 = eH^2$ with F, G, H as defined in (5.7). Then $\widetilde{F}^4 - p\widetilde{G}^4 = e\widetilde{H}^2$ with $\widetilde{F}$, $\widetilde{G}$, $\widetilde{H}$ as above. So it suffices to prove that $\widetilde{H}$ is even. Since c is even, we have a and b odd, whereupon $2 \| A$ (2 divides exactly A, since $p \equiv 1$ or $5 \pmod{16}$). Moreover $4|B$, $4\|C$, $4\|F$, $4\|G$, so $4\|\text{GCD}(F, G)$. Since $32|H$, we conclude $2|\widetilde{H}$.

(3) Suppose finally that we have a solution of Type C. By Theorem 3.2(i), if $p \equiv 1 \pmod{16}$), then Type C occurs if and only if Type B with $e = 1$ occurs. So we can suppose $p \equiv 7$ or $15 \pmod{16}$). In part 2 of the proof of Proposition 3.1, we saw that if Y is odd in $X^4 - pY^4 = Z^2$, then we have a solution of Type C and vice-versa. So it suffices to prove that if (a, b, c) is a solution of $X^4 - pY^4 = Z^2$ with b odd, then this occurs infinitely often. Consider again

$$3P = \left(\frac{F^2}{G^2}, \frac{FH}{G^3} \right)$$

and $\widetilde{F}^4 - p\widetilde{G}^4 = \widetilde{H}^2$ with $\widetilde{F}$, $\widetilde{G}$, $\widetilde{H}$ defined as before. Since $p \equiv 7$ or $15 \pmod{16}$, we have $2|a$, $2 \not| b$. Therefore, $2 \not| A$, $2|B$, $2 \not| G$ and $\widetilde{G}$ is odd. □

Scolie 5.2. *If there is a positive solution of the Diophantine equation*

$$R^4 + pS^4 = 2T^2$$

where R, S, T with R, S odd are pairwise coprime integers, then there are infinitely many ones.

Proof. See part (3) of the last proof. □

Theorem 5.3. *Let p be an odd prime. Suppose there is a positive solution in pairwise coprime integers of $X^4 + pY^4 = Z^2$ of a given Type. Then that Type of solution occurs infinitely often.*

Proof. (1) For Type a (resp. Type b), the proof is similar to what was done in part (1) (resp. part (2)) of the preceding proof.

(2) Suppose now that for some fixed $e \in \{1, -1\}$, (a, b, c) is a solution of Type d, so b is odd. Consider again $3P$ and $\widetilde{F}$, $\widetilde{G}$, $\widetilde{H}$ defined as before. From part (2) of the proof of Proposition 4.1, we know that it suffices to show that $\widetilde{G}$

is odd. If a is even, then G (hence $\widetilde{G}$) is odd. If a is odd, then c is even (since b is odd) and $2 \,\|\, G = (c^2 - 2pb^4)b^2 - ea^2(2abc)^2$ while $4|F$, whereupon $\widetilde{G}$ is odd, as required.

(3) Suppose that a Type c solution of $X^4 + pY^4 = Z^2$ is given by

$$X = c, \quad Y = 2ab, \quad Z = -c^2 + 2pb^4 = 4a^4 + pb^4,$$

where a, b, c with b, c odd are pairwise coprime integers which verify

$$4a^4 - pb^4 = -c^2.$$

Then $P = (U, V)$ with $U = -\dfrac{4a^2}{b^2}$, $V = \dfrac{4ac}{b^3}$ is a rational point on the elliptic curve

$$E' : V^2 = U^3 - 4pU.$$

Then on the one hand,

$$2P = \left(\frac{A^2}{B^2}, \frac{AC}{B^3}\right) \quad \text{with} \quad \begin{cases} A = 16a^4 + 4pb^4, \\ B = 8abc, \\ C = 16c^4 - 256pa^4b^4, \end{cases}$$

where $A^4 - 4pB^4 = C^2$, and on the other hand,

$$3P = \left(-\frac{F^2}{G^2}, \frac{FH}{G^3}\right)$$

with

$$\begin{cases} F = 2ABc + 2abC, \\ G = A^2b^2 + 4a^2B^2, \\ H = -2Cc(-A^2b^2 + 4a^2B^2) - 4ABab(4pB^2b^2 + 4A^2a^2). \end{cases}$$

Since b and c are odd, we have $4\|A$, $8|B$ and $16\|C$. Then $32|F$, $16\|G$ and $512||H$. After simplifying the powers of 2 in F, G and H, we obtain

$$\frac{F^2}{G^2} = \frac{4F_1^2}{G_1^2} \quad \text{and} \quad \frac{FH}{G^3} = \frac{4F_1H_1}{G_1^3},$$

with G_1, H_1 odd. Hence

$$3P = \left(-\frac{4F_1^2}{G_1^2}, \frac{4F_1H_1}{G_1^3}\right)$$

is a rational point on E, with $\text{GCD}(F_1, G_1)^2 \,|H_1$, whereupon

$$\left(\frac{4F_1H_1}{G_1^3}\right)^2 = \left(-\frac{4F_1^2}{G_1^2}\right)^3 - 4p\left(-\frac{4F_1^2}{G_1^2}\right), \quad \text{i.e.,} \quad 4F_1^4 - pG_1^4 = -H_1^2.$$

Let

$$\widetilde{F} = \frac{F_1}{\text{GCD}(F_1, G_1)}, \quad \widetilde{G} = \frac{G_1}{\text{GCD}(F_1, G_1)}, \quad \widetilde{H} = \frac{H_1}{(\text{GCD}(F_1, G_1))^2}.$$

Then $4\widetilde{F}^4 - p\widetilde{G}^4 = -\widetilde{H}^2$, where $\widetilde{F}$, $\widetilde{G}$, $\widetilde{H}$ with $\widetilde{G}$, $\widetilde{H}$ odd are pairwise coprime integers. We conclude that $X = \widetilde{H}$, $Y = 2\widetilde{F}\widetilde{G}$ and $Z = 4\widetilde{F}^4 + p\widetilde{G}^4$ is a new solution of Type c of $X^4 + pY^4 = Z^2$. Note that $\dfrac{A}{B} \in \mathbf{Q}\backslash\mathbf{Z}$, since $8 \not| 4pb^4$, whereupon by the theorem of Lutz-Nagell, $2P$ is not a torsion point, i.e., P is a point of infinite order. □

Scolie 5.4. (1) *If there is a positive solution of the Diophantine equation*

$$R^4 - pS^4 = 2eT^2 \quad \textit{with} \quad e \in \{1, -1\}$$

where R, S, T with R, S odd are pairwise coprime integers, then there are infinitely many ones.

(2) If there is a positive solution of the Diophantine equation

$$4R^4 - pS^4 = -T^2\,,$$

where R, S, T with S, T odd are pairwise coprime integers, then there are infinitely many ones.

6. Concluding Remarks

On the one hand, A. Bremner and J.W.S. Cassels [1] proved that for all primes $p \equiv 5 \pmod 8$ less than 1000, the rank of the elliptic curve $E : Y^2 = X^3 + pX$ is 1 and exhibited an explicit generator of the group of rational points of E. On the other hand, P. Monsky [5] obtained the following remarkable result: using modular functions, he constructed a rational point of infinite order on $E_2 : V^2 = U^3 + DU$ when

$$D = \begin{cases} p \quad \text{or} \quad p^3, & p \text{ being a prime } \equiv 3, 5 \pmod{16}\,, \\ -p \quad \text{or} \quad -p^3, & p \text{ being a prime } \equiv 5, 7 \pmod{16}\,. \end{cases}$$

The following theorem summarizes what is known in the litterature about the rank of certain elliptic curves ([8], [3], [4]).

Theorem 6.1. *Let p be an odd prime. Consider the elliptic curves*

$$E_1 : V^2 = U^3 - pU \quad \text{and} \quad E_2 : V^2 = U^3 + pU.$$

(i) Then the rank r of E_1 over $\mathbf{Q}$ satisfies

$$\begin{cases} r = 1 & \text{if } p = 2, \\ r = 0 & \text{if } p \equiv 3,\ 11 \text{ or } 13 \pmod{16}, \\ r \leq 1 & \text{if } p \equiv 5,\ 7,\ 9 \text{ or } 15 \pmod{16}, \\ r \leq 2 & \text{if } p \equiv 1 \pmod{16}. \end{cases}$$

Moreover, the parity conjecture (stating that the root number of E_1 is equal to $(-1)^r$) implies that $r = 1$ for $p \equiv 5,\ 7,\ 9$ or $15 \pmod{16}$ and that $r = 0$ or 2 for $p \equiv 1 \pmod{16}$.

(ii) The rank r of E_2 over $\mathbf{Q}$ satisfies

$$\begin{cases} r = 0 & \text{if } p = 2 \text{ or if } p \equiv 7 \text{ or } 11 \pmod{16}, \\ r \leq 1 & \text{if } p \equiv 3,\ 5,\ 13 \text{ or } 15 \pmod{16}, \\ r \leq 2 & \text{if } p \equiv 1 \pmod{8}. \end{cases}$$

If $p \equiv 1 \pmod 8$, the parity conjecture implies that $r = 0$ or 2. Moreover, if $p \equiv 1 \pmod 8$ and if 2 is not a quartic residue modulo p, then $r = 0$.

It is worth mentioning that (in Chapter X of his book [8]) J. Silverman made a nice study of the value of the sum of the rank r of $E_2 : V^2 = U^3 + pU$ and of the dimension d over $\mathbf{Z}/2\mathbf{Z}$ of the 2-torsion of the Shafarevich-Tate group of E_2. For $p \equiv 3,\ 5,\ 13$ or $15 \pmod{16}$, he obtained $r + d = 1$, and for $p \equiv 1 \pmod 8$, he obtained $r + d = 2$.

Let p be an odd prime. Consider first the Diophantine equation $X^4 - pY^4 = Z^2$ and its associated elliptic curve $E_1 : V^2 = U^3 - pU$. We know from Section 3.6 of [4] that if there exist non-zero integers a, b, c such that $a^4 - pb^4 = ec^2$, so $p = \left(\frac{a}{b}\right)^4 - e\left(\frac{c}{b^2}\right)^2$, then this criterion secures $\operatorname{rank}(E_1) \geq 1$. This property of a prime p to be written as $p = r^4 - es^2$ may look trivial , but it has the drastic impact that the rank of E_1 will be ≥ 1. If in particular, $p = R^4 + S^2$ with R, $S \in \mathbf{N}$, which happens infinitely often thanks to the deep results of Friedlander and Iwaniec [2], then $\operatorname{rank}(E_1) \geq 1$ infinitely often. In the same

vein, we deduce from Proposition 3.1 the following equivalences:

$$\begin{cases} \text{Type A occurs} & \iff & p = r^4 - es^2 & \text{with } r, s \in \mathbf{Q}, \\ \text{Type B occurs} & \iff & p = r^4 - es^2 & \text{with } r, s \in \mathbf{Q}, \\ \text{Type C occurs} & \iff & p = -r^4 + 2s^2 & \text{with } r, s \in \mathbf{Q}. \end{cases}$$

So we just exhibited conditions on the prime p under which $\text{rank}(E_1) \geq 1$.

When we consider the Diophantine equation $X^4 + pY^4 = Z^2$ and the associated elliptic curve $E_2 : V^2 = U^3 + pU$, we deduce from Proposition 4.1 the following equivalences:

$$\begin{cases} \text{Type a occurs} & \iff & p = -r^4 + s^2 & \text{with } r, s \in \mathbf{Q}, \\ \text{Type b occurs} & \iff & p = -r^4 + s^2 & \text{with } r, s \in \mathbf{Q}, \\ \text{Type c occurs} & \iff & p = 4r^4 + s^2 & \text{with } r, s \in \mathbf{Q}, \\ \text{Type d occurs} & \iff & p = r^4 - 2es^2 & \text{with } r, s \in \mathbf{Q}. \end{cases}$$

Again we have conditions on the prime p under which $\text{rank}(E_2) \geq 1$. As a matter of fact, the criterion $p = 4r^4 + s^2$ with $r,\ s \in \mathbf{Q}$ was found by J.S. Milne (p. 363 of [4]) when $p \equiv 5 \pmod 8$.

It should now be clear that when $p \equiv 5$, 7, 9 or 15 (mod 16), the parity conjecture implies $\text{rank}(E_1) = 1$ and $p \in \mathcal{A}_1$, where

$$\mathcal{A}_1 = \{r^4 + s^2,\ r^4 - s^2,\ -r^4 + 2s^2 \mid r, s \in \mathbf{Q}\}.$$

Moreover, when $p \equiv 3$, 5, 13 or 15 (mod 16), the parity conjecture implies $\text{rank}(E_2) = 1$ and $p \in \mathcal{A}_2$, where

$$\mathcal{A}_2 = \{-r^4 + s^2,\ 4r^4 + s^2,\ r^4 + 2s^2,\ r^4 - 2s^2 \mid r, s \in \mathbf{Q}\}.$$

7. Acknowledgements

Both authors benefitted from research grants from NSERC.

References

[1] A. Bremner, J.W.S. Cassels, On the equation $Y^2 = X(X^2 + p)$, *Math. of Comp.*, **42**, No. 165 (1984), 257-264

[2] J. Friedlander, H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Ann. of Math. 2*, **148**, No. 3 (1998), 945-1040.

[3] A.W. Knapp, *Elliptic Curves*, Mathematical Notes, Princeton University Press, xvi+427.

[4] J.S. Milne, *Elliptic Curves*, Lecture Notes, Department of Mathematics of University of Michigan.

[5] P. Monsky, Three constructions of rational points on $Y^2 = X^3 \pm NX$, *Math. Z.*, **209**, No. 3 (1992), 445-462; Errata in *Math. Z.*, **212**, No. 1 (1993), 141.

[6] L.J. Mordell, The Diophantine equation $x^4 + my^4 = z^2$, *Quat. J. Math. Oxford*, **18** (1967), 1-6.

[7] L.J. Mordell, *Diophantine Equations*, Academic Press (1969), xii+312.

[8] J.S. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., **106** (1992), xii+400.