BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 67, No. 1, 2019

NUMBER THEORY

Integral points on elliptic curves $y^2 = x(x - 2^m)(x + p)$

by

Tomasz JĘDRZEJAK and Małgorzata WIECZOREK

Presented by Jerzy KACZOROWSKI

Summary. We provide a description of the integral points on elliptic curves $y^2 = x(x-2^m) \times (x+p)$, where p and $p+2^m$ are primes. In particular, we show that for $m = 2$ such a curve has no nontorsion integral point, and for $m = 1$ it has at most one such point (with $y > 0$). Our proofs rely upon numerical computations and a variety of results on quartic and other diophantine equations, combined with an elementary analysis.

1. Introduction. By the famous Siegel Theorem [16], any elliptic curve over $\mathbb{Q}$ has only finitely many integral points. However, searching for integral points leads to considering certain diophantine equations, so it is not easy in general. Many authors have dealt with this problem. For example, Draziotis [8] determined integral points on the curves $y^2 = x^3 \pm p^k x$ (p is a prime) by solving a finite number of quartic elliptic equations, using a reduction through an unramified map. Bennett [2] described integral points in a certain subfamily of congruent number curves using linear forms in logarithms. Yang and Fu [20], combining some properties of quadratic and quartic diophantine equations with an elementary analysis, proved that the elliptic curve $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$ has, under some conditions, only one integral point $(2, 0)$. Alvanos and Draziotis [1] determined all possible integer solution of the equation $y^2 = Ax^4 + B$ by using Lucas sequences.

In this paper, we consider elliptic curves associated to generalized twin primes. Let us recall some information on this topic. It is believed that

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11D25, 11D45.
Key words and phrases: elliptic curves, integral points, rank of elliptic curves, system of Pell equations, Thue equations.
Received 21 March 2018; revised 27 February 2019.
Published online 28 March 2019.

DOI: 10.4064/ba8152-1-2019

there exist infinitely many twin primes (this is the so called Twin Prime Conjecture). More generally, one can expect that (for a fixed positive even integer k) there exist infinitely many primes p such that $p+k$ is also a prime (cf. [9, first part of Conjecture B]). These conjectures are still open. In fact, we seem nowhere close to settling this problem. One well known result is Chen's theorem [5] stating that there are infinitely many primes p such that $p+2$ has at most two prime factors. For the related problem (the so called Bounded Gap Conjecture) Zhang [21] showed that there are bounded gaps between consecutive primes infinitely often. More precisely, he proved that $\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 7\times 10^7$ where p_n denotes the nth prime (note that the Twin Prime Conjecture says that $\liminf_{n\to\infty}(p_{n+1}-p_n)=2$). Next, Maynard [12], by using multidimensional sieve weights, lowered this bound to 600 (and under the assumption of the Elliott–Halberstam conjecture to 12). The Polymath project [14], which extends Maynard's methods, has successfully brought this bound down to 246 unconditionally, and to 6 under the assumption of the generalized Elliott–Halberstam conjecture. Note also that since the Bounded Gap Conjecture is true, there is at least one positive even integer which can be written infinitely often as the difference of two consecutive primes.

Let p, q be odd primes such that $q-p=2^m$, $m\geq 1$. Consider the family of elliptic curves over $\mathbb{Q}$

$$E_{p,m}: y^2 = x(x-2^m)(x+p). \tag{1.1}$$

These curves were considered by Dąbrowski and the second author [7] (note that our notation differs from the one in [7]). The purpose of this paper is to describe the integral points of this family. Note that $E_{p,m}(\mathbb{Q})_{\mathrm{tors}} = E_{p,m}[2] = \{\infty, (0,0), (2^m,0), (-p,0)\}$ (see [13, Main Theorem 1]) and the rank of $E_{p,m}(\mathbb{Q})$ is less than or equal to 2 (see [10, Proposition 4.19]). Moreover, this bound can only be attained for $m=3$ or $m>4$ and certain special primes $q\equiv 1 \pmod 8$. Consequently, we have $E_{p,m}(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}^r$ where $r\in\{0,1,2\}$. We also know that the discriminant of (1.1) equals $2^{2m+4}p^2q^2$ and the reduction at p and q is multiplicative. Summarizing, $E_{p,m}$ has three rational 2-torsion points and its conductor $N_{p,m}$ is 2^epq for some $e\geq 0$. In particular, if $m=4$ and $p\equiv 1 \pmod 4$ then $N_{p,m}=pq$. Note that Bennett [2] considered elliptic curves with three rational 2-torsion points and conductor 2^ap^b.

Suppose that we have a solution of $y^2=x(x-2^m)(x+p)$ in nonzero integers x and y. Then the point (x,y) with (without loss of generality) $y>0$ is nontorsion and we call it a *nontrivial integral point of* $E_{p,m}$ (however, note that the equation (1.1) is not minimal in general). If $E_{p,m}$ has a nontrivial integral point then, by the considerations above, the rank of $E_{p,m}(\mathbb{Q})$ is

in $\{1, 2\}$. However, two nontrivial integral points on $E_{p,m}$ may not be independent. For example, $E_{5,3}$ has rank one and two nontrivial integral points $(-1, 6)$ and $(40, 240)$ (they differ by the torsion point $(0, 0)$).

In this paper, we provide a description of the nontrivial integral points on the elliptic curves $E_{p,m}$ (Theorems 2.1–2.4 below). In particular, we show that $E_{p,2}$ has no nontrivial integral points, and $E_{p,1}$ has at most one such point. Our proofs rely upon computations in Magma [4] and a variety of results on quartic and other Diophantine equations, combined with an elementary analysis.

2. Results. In this section, we state the main results of this paper (the numbers of cases refer to Section 3).

THEOREM 2.1. *There is at most one nontrivial integral point on the curve $E_{p,1}$. If there is one such a point then it arises from case* 3.8. *Furthermore, $p \equiv 1, 7 \pmod 8$ and $p > 416440$.*

In fact, we conjecture that there are no nontrivial integral points on $E_{p,1}$ at all.

THEOREM 2.2. *The curve $E_{p,,2}$ has no nontrivial integral points.*

THEOREM 2.3. *If the curve $E_{p,3}$ has a nontrivial integral point then it must arise from cases* 3.1, 3.8, 3.9 *or* 3.10. *Furthermore, cases* 3.8 *and* 3.9 *can give at most three such points and these cases can only arise if $p \equiv 1 \pmod 8$ and $p > 329080$.*

We conjecture that cases 3.8 and 3.9 never occur for $m = 3$.

In general, we have the following result.

THEOREM 2.4. *If the elliptic curve $E_{p,m}$ has a nontrivial integral point (x, y) then (x, p, m) belongs to the list given below:*

- Case 3.1:
$$x = -(2^{m-2} - 1)^2, \quad p = c^2 + (2^{m-2} - 1)^2,$$
where $m \geq 3$ and c is a positive even integer.
- Case 3.2:
$$x = 2^m a^2, \quad a^2 - (p + 2^m)b^2 = 1, \quad c^2 - 2^m b^2 = 1,$$
where a, b, c are pairwise coprime positive integers such that b, c and $m \geq 3$ are odd, and a is even.
- Case 3.3:
$$x = 2^\alpha a^2, \quad a^2 - (p + 2^m)b^2 = 2^{m-\alpha}, \quad c^2 - 2^\alpha b^2 = 1,$$
where a, b, c are odd pairwise coprime positive integers and $m \geq \alpha + 1 \geq 4$ with odd α.

- Case 3.4:
$$x = 2^\alpha(2^{m-\alpha-2}+1)^2, \quad p = c^2 - 2^\alpha(2^{m-\alpha-2}+1)^2,$$
where $m \geq \alpha+3 \geq 4$ and c is a positive odd integer.
- Case 3.5:
$$x = -2^\alpha(2^{m-\alpha-2}-1)^2, \quad p = c^2 + 2^\alpha(2^{m-\alpha-2}-1)^2,$$
where $m \geq \alpha+3 \geq 4$ and c is a positive odd integer.
- Case 3.6:
$$x = 2^\alpha pa^2, \quad qc^2 - 2^\alpha a^2 = 1, \quad pc^2 - 2^\alpha b^2 = 1,$$
where a, b, c are odd pairwise coprime positive integers and $m \geq \alpha+3 \geq 4$.
- Case 3.7:
$$x = 2^\alpha pa^2, \quad pa^2 - b^2 = 2^{m-\alpha}, \quad c^2 - 2^\alpha a^2 = 1,$$
where a, b, c are odd pairwise coprime positive integers and $m \geq \alpha+1 \geq 4$ with odd α.
- Case 3.8:
$$x = 2^m a^2, \quad a^2 - (p+2^m)b^2 = 1, \quad c^2 - 2^m b^2 = 1,$$
where a, b, c are pairwise coprime positive integers such that a, c and m are odd, and b is even.
- Case 3.9:
$$x = 2^m pa^2, \quad pa^2 - (p+2^m)b^2 = 1, \quad pc^2 - 2^m b^2 = 1,$$
where a, b, c are pairwise coprime positive integers such that b is even and a, c are odd.
- Case 3.10:
$$x = 2^m pa^2, \quad pa^2 - b^2 = 1, \quad c^2 - 2^m a^2 = 1,$$
where a, b, c are pairwise coprime positive integers such that b is even and a, c are odd, and $m \geq 3$ is odd.

3. Case-by-case analysis. For a nontrivial integral point (x, y) on $E_{p,m}$ write $x = 2^\alpha p^\beta x_0$, where α and β are nonnegative integers, and x_0 is coprime to $2p$.

Notice that

$$\gcd(x, x+p) \mid p, \quad \gcd(x-2^m, x+p) \mid q, \quad \gcd(x, x-2^m) = 2^{\min(\alpha,m)}.$$

Furthermore, if $\gcd(x-2^m, x+p) = q$, then $q \nmid x$.

In this section, we consider 32 cases depending on the values of α, β, $\gcd(x-2^m, x+p)$ and $\operatorname{sgn} x$ (we consider positive and negative values of x separately). Throughout, a, b, c denote positive, pairwise coprime integers.

In 22 cases elementary analysis shows that these cases are impossible. We omit the details, and only focus on the remaining ten cases.

3.1. $\alpha = \beta = 0$, $\gcd(x - 2^m, x + p) = 1$, $x < 0$. From

$$x = -a^2, \quad x - 2^m = -b^2, \quad x + p = c^2,$$

we obtain

$$-a^2 - 2^m = -b^2,$$

whence

$$2^m = (b - a)(b + a).$$

Since $a \equiv b \equiv 1 \pmod 2$, this implies that

$$b - a = 2, \quad b + a = 2^{m-1}$$

and further

$$a = 2^{m-2} - 1.$$

We have thus found, for $m \geq 3$, a nontrivial integral point (x, y), where

$$x = -(2^{m-2} - 1)^2,$$

and

$$p = c^2 + (2^{m-2} - 1)^2, \quad q = c^2 + (2^{m-2} + 1)^2,$$

for some positive c. Note that if $m \leq 2$ or $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$, then this case does not occur.

3.2. $\alpha > m$, $\beta = 0$, $\gcd(x - 2^m, x + p) = q$, $x > 0$. We have

$$x = 2^m a^2, \quad x - 2^m = 2^m q b^2, \quad x + p = q c^2, \tag{3.1}$$

where $2 \mid a$ and $2 \nmid bc$. Combining these equations we obtain the following system of three diophantine (quadratic) equations in a, b, c:

$$\begin{cases} a^2 - qb^2 = 1, \\ c^2 - 2^m b^2 = 1, \\ 2^m a^2 - qc^2 = -p. \end{cases} \tag{3.2}$$

Note that the second of these equations comes from subtracting the second condition in (3.1) from the third one. Consequently, any one of these equations depends on the remaining two. Hence in fact we have a system of two Pell-like equations (we can use any two equations from (3.2)). Note also that if this system has a solution (with $b \neq 0$), then $q \equiv 3 \pmod 4$, m is odd, $q \equiv p \pmod 8$ and $\left(\frac{2q}{p}\right) = \left(\frac{-2p}{q}\right) = 1$. Hence in particular $m \geq 3$. Moreover, by [3, Corollary 1.3], this system has at most one solution in positive integers a, b, c. Assume that such a solution exists. Then $(a - c) \times (a + c) = a^2 - c^2 = (q - 2^m)b^2 = pb^2$. Since $\gcd(a - c, a + c) = 1$, we get

$$\begin{cases} a = \frac{pu^2 + v^2}{2}, \\ c = \frac{v^2 - pu^2}{2}, \end{cases} \quad \text{or} \quad \begin{cases} a = \frac{u^2 + pv^2}{2}, \\ c = \frac{pv^2 - u^2}{2}, \end{cases} \tag{3.3}$$

for some relatively prime positive integers u, v such that $b = uv$. Substituting (3.3) into the equation $a^2 - qb^2 = 1$, we deduce that u and v satisfy the Thue equation

$$X^4 - 2(p + 2^{m+1})X^2Y^2 + p^2Y^4 = 4. \tag{3.4}$$

3.3. $0 < \alpha < m$, $\beta = 0$, $\gcd(x - 2^m, x + p) = q$, $x > 0$. We have

$$x = 2^\alpha a^2, \quad x - 2^m = 2^\alpha qb^2, \quad x + p = qc^2,$$

where $2 \nmid abc$. Combining these equations (similar to case 3.2) we obtain the following system of three diophantine equations in a, b, c:

$$\begin{cases} a^2 - qb^2 = 2^{m-\alpha}, \\ c^2 - 2^\alpha b^2 = 1, \\ 2^\alpha a^2 - qc^2 = -p. \end{cases} \tag{3.5}$$

Since each of these equations depends on the remaining ones, in fact we have a system of two Pell-like equations. Assume that (3.5) has a solution with $b \neq 0$. Then α is odd, $\alpha > 1$ and $\left(\frac{2q}{p}\right) = \left(\frac{-2p}{q}\right) = 1$. Hence in particular $m \geq 4$, and so $q \equiv p \pmod{16}$. Moreover, multiplying the second equation in (3.5) by $2^{m-\alpha}$ and subtracting it from the first one, we get

$$a^2 = pb^2 + 2^{m-\alpha}c^2.$$

If $2 \nmid m - \alpha$, then reducing modulo p we obtain $\left(\frac{2}{p}\right) = 1$, so $p \equiv 1, 7 \pmod 8$. Moreover, if $m - \alpha = 1$ then $p \equiv 7 \pmod 8$, and if $m - \alpha > 2$ then $p \equiv 1 \pmod 8$.

3.4. $0 < \alpha < m$, $\beta = 0$, $\gcd(x - 2^m, x + p) = 1$, $x > 0$. The fact that

$$x = 2^\alpha a^2, \quad x - 2^m = 2^\alpha b^2, \quad x + p = c^2,$$

where $2 \nmid abc$, implies that

$$2^\alpha a^2 - 2^m = 2^\alpha b^2,$$

so that

$$2^{m-\alpha} = (a - b)(a + b).$$

We find that

$$a - b = 2, \quad a + b = 2^{m-\alpha-1}.$$

This yields

$$a = 2^{m-\alpha-2} + 1,$$

so

$$x = 2^\alpha(2^{m-\alpha-2} + 1)^2.$$

Hence for $m \geq \alpha + 3 \geq 4$ we have a nontrivial integral point on $E_{p,m}$ with

$$p = c^2 - 2^\alpha(2^{m-\alpha-2} + 1)^2, \quad q = c^2 - 2^\alpha(2^{m-\alpha-2} - 1)^2,$$

for some positive c. In particular, if $2 \nmid \alpha$ and p or q is congruent to 3 or 5 modulo 8, then this case does not occur. The same is true if $\alpha = 1$ and p or q is not congruent to 7 modulo 8, and if $\alpha \geq 3$ and p or q is not congruent to 1 modulo 8.

3.5. $0 < \alpha < m$, $\beta = 0$, $\gcd(x - 2^m, x + p) = 1$, $x < 0$. Similar to the previous case, we have

$$x = -2^\alpha a^2, \quad x - 2^m = -2^\alpha b^2, \quad x + p = c^2,$$

where $2 \nmid abc$. Hence

$$2^{m-\alpha} = (b - a)(b + a)$$

and further

$$b - a = 2, \quad b + a = 2^{m-\alpha-1}.$$

Finally, we obtain

$$a = 2^{m-\alpha-2} - 1, \quad x = -2^\alpha (2^{m-\alpha-2} - 1)^2,$$

where $m \geq \alpha + 3 \geq 4$. Therefore we have a nontrivial integral point on $E_{p,m}$ with

$$p = c^2 + 2^\alpha (2^{m-\alpha-2} - 1)^2, \quad q = c^2 + 2^\alpha (2^{m-\alpha-2} + 1)^2,$$

for some positive c (cf. case 3.1). Notice that for such p and q we have $p \equiv q \equiv 1 \pmod 4$ if $2 \mid \alpha$, and $\left(\frac{-2}{p}\right) = \left(\frac{-2}{q}\right) = 1$ (hence $p, q \equiv 1, 3 \pmod 8$) if $2 \nmid \alpha$. Moreover, $p \equiv q \equiv 1 \pmod 8$ if $\alpha \geq 3$, and $p \equiv q \equiv 3 \pmod 8$ if $\alpha = 1$, and $p \equiv q \equiv 5 \pmod 8$ if $\alpha = 2$.

3.6. $0 < \alpha < m$, $\beta > 0$, $\gcd(x - 2^m, x + p) = q$, $x > 0$. Now

$$x = 2^\alpha p a^2, \quad x - 2^m = 2^\alpha q b^2, \quad x + p = pqc^2,$$

where $2 \nmid abc$. Combining these equations (similar to cases 3.2 or 3.3) we obtain the system of three diophantine equations

$$\begin{cases} pa^2 - qb^2 = 2^{m-\alpha}, \\ pc^2 - 2^\alpha b^2 = 1, \\ 2^\alpha a^2 - qc^2 = -1. \end{cases} \tag{3.6}$$

As each of these equations depends on the other two, in fact we have a system of two Pell-like equations. Assume that this system has a solution. Then combining the second equation in (3.6) with the third one, we get

$$2^{m-\alpha} c^2 = (a - b)(a + b),$$

and consequently $m \geq \alpha + 3 \geq 4$. Moreover, if $\alpha = 1$ then $p \equiv q \equiv 3 \pmod 8$, if $\alpha = 2$ then $p \equiv q \equiv 5 \pmod 8$, and if $\alpha > 2$ then $p \equiv q \equiv 1 \pmod 8$.

3.7. $0 < \alpha < m$, $\beta > 0$, $\gcd(x - 2^m, x + p) = 1$, $x > 0$. Now

$$x = 2^\alpha p a^2, \quad x - 2^m = 2^\alpha b^2, \quad x + p = pc^2,$$

where $2 \nmid abc$. Combining these equations we obtain the system

$$\begin{cases} pa^2 - b^2 = 2^{m-\alpha}, \\ pc^2 - 2^\alpha b^2 = q, \\ 2^\alpha a^2 - c^2 = -1, \end{cases} \tag{3.7}$$

with each equation depending on the other two. Assume that (3.7) has a solution. Then from the third equation we obtain $2 \nmid \alpha$ and $\alpha > 1$, so in particular $m \geq 4$ and $p \equiv q \pmod{16}$. Moreover, multiplying the third equation in (3.7) by $2^{m-\alpha}$ and adding it to the first one, we get

$$qa^2 = b^2 + 2^{m-\alpha} c^2.$$

Therefore, if $2 \nmid m - \alpha$ then reducing modulo q, we obtain $\left(\frac{-2}{q}\right) = 1$, so $q \equiv 1, 3 \pmod 8$. Similarly, if $2 \mid m - \alpha$ then $q \equiv 1 \pmod 4$.

3.8. $\alpha = m$, $\beta = 0$, $\gcd(x - 2^m, x + p) = q$, $x > 0$. Now

$$x = 2^m a^2, \quad x - 2^m = 2^m q b^2, \quad x + p = qc^2,$$

where $2 \nmid ac$ and $2 \mid b$. Combining these equations we obtain the same system as in case 3.2 but now a is odd and b is even. If this system has a nontrivial solution then m is odd and $\left(\frac{2q}{p}\right) = \left(\frac{-2p}{q}\right) = 1$. Moreover, if $q \equiv 5 \pmod 8$ and $m > 1$ then by [19, Theorem 1], the only solution is $(a, b, c) = (1, 0, 1)$ and consequently we get only the torsion point $(2^m, 0)$. Also in general, by [3, Corollary 1.3] this system has at most one solution in positive integers a, b, c. Assume that such a solution exists. Then in much the same way as in case 3.2, we get

$$\begin{cases} a = pu^2 + v^2, \\ c = v^2 - pu^2, \end{cases} \quad \text{or} \quad \begin{cases} a = u^2 + pv^2, \\ c = pv^2 - u^2, \end{cases} \tag{3.8}$$

for some relatively prime positive integers u, v such that $b = 2uv$. Substituting (3.8) into the equation $a^2 - qb^2 = 1$, we deduce that u and v satisfy the Thue equation

$$X^4 - 2(p + 2^{m+1}) X^2 Y^2 + p^2 Y^4 = 1. \tag{3.9}$$

Then substituting $s = X^2 - (p + 2^{m+1}) Y^2$ and $t = Y$ into (3.9), we obtain

$$s^2 - 2^{m+2} q t^4 = 1. \tag{3.10}$$

By [3, Lemma 2.2], the equation (3.10) has at most one solution in positive integers s, t. Therefore for given p and q, in case 3.8 there exists at most one nontrivial integral point on $E_{p,m}$.

Note also that this quartic equation may have a solution but nonetheless our curve may have no nontrivial integral points. For example for $p = 311$

and $m = 1$ the equation $s^2 - 8 \times 313t^4 = 1$ has the solution $(1251, 5)$ but the curve $E_{311,1}$ has no such points (and has rank one). Taking $p = 4799$ and $m = 1$ we obtain another example, and so on.

3.9. $\alpha = m$, $\beta > 0$, $\gcd(x - 2^m, x + p) = q$, $x > 0$. Now

$$x = 2^m pa^2, \quad x - 2^m = 2^m qb^2, \quad x + p = pqc^2,$$

where $2 \nmid ac$ and $2 \mid b$. Combining these equations we obtain the system

$$\begin{cases} pa^2 - qb^2 = 1, \\ pc^2 - 2^m b^2 = 1, \\ 2^m a^2 - qc^2 = -1, \end{cases}$$

with each equation depending on the two others. If the system has a nontrivial solution then $p \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right) = 1$. Moreover, by [6, Lemma 5 and Theorem 2], this system has at most two solutions in positive integers a, b, c. If such a solution exists then the considerations similar to case 3.8 show that the Thue equation

$$pX^4 - 2(p + 2^{m+1})X^2Y^2 + pY^4 = 1 \tag{3.11}$$

has a solution in positive integers.

3.10. $\alpha = m$, $\beta > 0$, $\gcd(x - 2^m, x + p) = 1$, $x > 0$. Now

$$x = 2^m pa^2, \quad x - 2^m = 2^m b^2, \quad x + p = pc^2,$$

where $2 \nmid ac$ and $2 \mid b$. Combining these equations we obtain the system

$$\begin{cases} pa^2 - b^2 = 1, \\ pc^2 - 2^m b^2 = q, \\ 2^m a^2 - c^2 = -1, \end{cases} \tag{3.12}$$

with each equation depending on the other two. If this system has a nontrivial solution then m is odd, and reducing the suitable equations in (3.12) modulo 8, p and q, we get $p \equiv 1 \pmod 4$, $p \equiv q \pmod 8$, and $\left(\frac{2p}{q}\right) = \left(\frac{-2q}{p}\right) = 1$. In particular, $m \geq 3$.

4. Conclusion. As mentioned above, in 22 cases we have no nontrivial integral points on $E_{p,m}$. In the remaining ten cases such a point may exist. In three cases, namely 3.1, 3.4, and 3.5, we have explicit formulas for p and x. In the remaining seven cases we have implicit formulas (via a system of two Pell-like equations). Note that in each such case it is possible (using e.g. the algorithm from [17]) to associate to the system of Pell-like equations a finite family of quartic Thue equations. This was done (without using such an algorithm) to facilitate the analysis in cases 3.2, 3.8 and 3.9. Note also that these cases are different from the others (see Conjecture 6.2). Now we

summarize the analysis from Section 3 by writing sufficient conditions for the nonexistence of such a point in each of these ten cases separately.

PROPOSITION 4.1.

(1) *If* $m \leq 2$ *or* $p \equiv 3 \pmod 4$ *or* $q \equiv 3 \pmod 4$ *then case* 3.1 *does not occur.*
(2) *If* $m = 1$ *or* $2 \,|\, m$ *or* $q \equiv 1 \pmod 4$ *or* $p \not\equiv q \pmod 8$ *or* $\left(\frac{2q}{p}\right) = -1$ *or* $\left(\frac{-2p}{q}\right) = -1$ *then case* 3.2 *does not occur.*
(3) *If* $2 \,|\, \alpha$ *or* $\alpha = 1$ *or* $m \leq 3$ *or* $\left(\frac{2q}{p}\right) = -1$ *or* $\left(\frac{-2p}{q}\right) = -1$, *or* $2 \nmid m - \alpha$ *and* $p \equiv 3, 5 \pmod 8$, *then case* 3.3 *does not occur.*
(4) *If* $m \leq \alpha + 2$, *or* $m \leq 3$, *or* $2 \nmid \alpha$ *and* p *or* $q \equiv 3, 5 \pmod 8$, *or* $\alpha \geq 3$ *and* p *or* $q \not\equiv 1 \pmod 8$, *then case* 3.4 *does not occur.*
(5) *If* $m \leq \alpha + 2$, *or* $m \leq 3$, *or* $2 \nmid \alpha$ *and* p *or* $q \equiv 5, 7 \pmod 8$, *or* $2 \,|\, \alpha$ *and* p *or* $q \equiv 3 \pmod 4$, *or* $\alpha \geq 3$ *and* p *or* $q \not\equiv 1 \pmod 8$, *then case* 3.5 *does not occur.*
(6) *If* $m \leq \alpha + 2$ *or* $m \leq 3$ *then case* 3.6 *does not occur.*
(7) *If* $2 \mid \alpha$, *or* $\alpha = 1$, *or* $m \leq 3$, *or* $2 \nmid m - \alpha$ *and* $q \equiv 5, 7 \pmod 8$, *or* $2 \,|\, m - \alpha$ *and* $q \equiv 3 \pmod 4$, *then case* 3.7 *does not occur.*
(8) *If* $2 \,|\, m$ *or* $\left(\frac{2q}{p}\right) = -1$ *or* $\left(\frac{-2p}{q}\right) = -1$ *then case* 3.8 *does not occur.*
(9) *If* $p \not\equiv 1 \pmod 8$ *or* $\left(\frac{-q}{p}\right) = -1$ *or* $\left(\frac{p}{q}\right) = -1$ *then case* 3.9 *does not occur.*
(10) *If* $m = 1$ *or* $2 \,|\, m$ *or* $p \equiv 3 \pmod 4$ *or* $p \not\equiv q \pmod 8$ *or* $\left(\frac{-2q}{p}\right) = -1$ *or* $\left(\frac{2p}{q}\right) = -1$ *then case* 3.10 *does not occur.*

Proof. This follows from the analysis of these cases made in Section 3. ∎

Below, we show that case 3.9 does not occur for $m = 1$ and for $m \equiv 2 \pmod 4$.

PROPOSITION 4.2. *The diophantine equation* $na^2 - (n+2)b^2 = 1$, *where* $n > 1$, *has no solution in integers.*

Proof. Note that the proof is immediate if n is even. So assume that n is odd and consider the auxiliary Pell equation $x^2 - n(n+2)y^2 = 1$. It is easy to check that $x = n + 1$, $y = 1$ is its fundamental solution. By [18], the equation

$$na^2 - (n+2)b^2 = 1 \tag{4.1}$$

is solvable if and only if the fundamental solution (x, y) of the auxiliary Pell equation is the "square" of the smallest solution (a, b) of (4.1), meaning that $(a\sqrt{n} + b\sqrt{n+2})^2 = x + \sqrt{n(n+2)}y$. Consequently, $n + 1 = x = 2na^2 - 1$, which is impossible. ∎

COROLLARY 4.3. *The system of Pell-like equations*

$$\begin{cases} pa^2 - (p+2)b^2 = 1, \\ pc^2 - 2b^2 = 1, \end{cases}$$

or equivalently the Thue equation $pX^4 - 2(p+4)X^2Y^2 + pY^4 = 1$ *has no solution, and consequently case* 3.9 *does not occur for* $m = 1$.

Proof. This follows immediately from Proposition 4.2 and from the analysis of case 3.9 made in Section 3. ∎

PROPOSITION 4.4. *If* $m \equiv 2 \pmod 4$ *then the Thue equation* $pX^4 - 2(p+2^{m+1})X^2Y^2 + pY^4 = 1$, *where* $p, p+2^m$ *are primes, has no solution in integers. Consequently, case* 3.9 *does not occur for such* m.

Proof. Suppose the proposition were false. Then the congruence $pX^4 - (2p+1)X^2Y^2 + pY^4 \equiv 1 \pmod 5$ has a solution. Note that by the assumption and the Fermat little theorem, $2^m \equiv -1 \pmod 5$ and $p \not\equiv 0, 1 \pmod 5$. Now checking all possible values of X, Y, p modulo 5, we get a contradiction. ∎

Unfortunately, the above methods do not work for other values of m. Also the hypergeometric method and the method of simultaneous Padé approximations do not apply here.

5. Proofs of theorems. In this section, we conclude the proofs of our main results.

Proof of Theorem 2.1. We may assume that $p \equiv 1, 7 \pmod 8$ because for $p \equiv 3, 5 \pmod 8$ we have $\operatorname{rank} E_{p,1}(\mathbb{Q}) = 0$ by [7, Corollary 1]. Now Proposition 4.1, Corollary 4.3, analysis of case 3.8 in Section 3 and computations in Magma prove the theorem. ∎

Proof of Theorem 2.2. Suppose that $E_{p,2}$ has a nontrivial integral point. We may assume that $p \equiv 1 \pmod 4$ because by [7, Corollary 1], $\operatorname{rank} E_{p,2}(\mathbb{Q}) = 0$ for $p \not\equiv 1 \pmod 4$. Then by Proposition 4.1, we are in case 3.9. Now by Proposition 4.4, we get a contradiction, which completes the proof. ∎

Proof of Theorem 2.3. Similar to the above proof, by [7, Corollary 1], we may assume that $p \equiv 1 \pmod 4$. Now the first part of the theorem follows immediately from Proposition 4.1. In Section 3 we showed that case 3.8 gives at most one nontrivial torsion point, and case 3.9 gives at most two such points. Moreover, we may assume that $p \equiv 1 \pmod 8$. Then computations in Magma finish the proof. ∎

Proof of Theorem 2.4. This follows from the analysis made in Section 3. ∎

6. Remarks and problems

REMARK 6.1. Note that all cases from Theorem 2.4 occur for $m \geq 3$ with the possible exception of 3.2, 3.8 and 3.9 (for $m \neq 12$). Indeed, below we write for each such case the minimal (in lexicographic order) triple (m, p, x) where (x, y) is a nontrivial integral point on $E_{p,m}$ (p and $q = p + 2^m$ are primes).

Table 1. Integral points on $E_{p,m}$

Case	m	p	x
3.1	3	5	-1
3.3	4	7	200
3.4	4	7	18
3.5	4	3	-2
3.6	4	3	54
3.7	4	3	24
3.9	12	23593	16331640832
3.10	3	5	40

Numerical computations also suggest the following.

CONJECTURE 6.2. *Cases* 3.2, 3.8 *and* 3.9 *do not occur* (*with the exception of* 3.9 *for* $m = 12$).

CONJECTURE 6.3. *The curve* $E_{p,m}$ *has at most four nontrivial integral points.*

In fact, we found only one example of $E_{p,m}$ with four such points (all other examples we found have at most three integral points): $m = 9$, $p = 89$, $q = 601$, $(x, y) = (-64, 960), (712, 10680), (2312, 99960), (481312, 333771360)$ (these arise from cases 3.5, 3.7, 3.3 and 3.6, respectively).

Under weaker assumptions than Conjecture 6.2 we can prove the following.

PROPOSITION 6.4. *If the system of Pell like equations*

$$\begin{cases} a^2 - (p+2)b^2 = 1, \\ c^2 - 2b^2 = 1, \end{cases}$$

or equivalently the Thue equation $X^4 - 2(p+4)X^2Y^2 + p^2Y^4 = 1$, *where* p, $p+2$ *are primes and* $p \equiv 1, 7 \pmod 8$, *has no nonzero solution, then* $E_{p,1}$ *has no nontrivial integral points.*

Proof. This follows immediately from Theorem 2.1 and from the analysis of case 3.8 made in Section 3. ∎

REMARK 6.5. The above result is nontrivial because by [7, Corollary 2], we have (assuming the Parity Conjecture) $\operatorname{rank} E_{p,m}(\mathbb{Q}) = 1$ for $m = 1$ and $p \equiv 1, 7 \pmod 8$.

Below we explain why the standard tools for solving Thue equations such as linear forms in logarithms (see [15]) and the hypergeometric method (see [11]) do not work for the equations (3.9), i.e., for case 3.8.

REMARK 6.6. There are examples showing that the equation $X^4 - 2(p+4)X^2Y^2 + p^2Y^4 = 1$ may have a nonzero solution if we do not assume that $p+2$ is prime: $(p, X, Y) = (41039, 204, 1)$, $(42193, 204, 1)$, $(684132103, 78472, 3)$. Moreover, if we drop the assumption that p and $p+2$ are primes, a solution of this equation can be easily found. Namely, the form $X^4 - 2(p+4)X^2Y^2 + p^2Y^4 - 1$ is a quadratic in p, and consequently p will be a rational solution if its discriminant $32X^2Y^6 + 4Y^4$ is a perfect square. Hence we want $2(2XY)^2 + 1$ to be a perfect square. Therefore, for any Y, there are infinitely many X's (and infinitely many p's too) which are solutions of these Thue equations. The values of X are members of binary recurrence sequences and the p's grow in a similar way. Therefore, it is reasonable to conjecture that in each such family there are infinitely many primes (for the same reasons why we believe there are infinitely many Mersenne primes, Fibonacci primes etc.). Since there are so many such families of p's, it seems to be at least possible that there is one twin prime among them. Something similar can also be done for the Thue equation $X^4 - 2(p + 2^{m+1})X^2Y^2 + p^2Y^4 = 1$. For both cases, this allows us to show that the twin prime p must be very large. In particular, if $E_{p,1}$ has a nontrivial integral point then p is very large. Anyway, the "purely diophantine" approach (i.e., ignoring the prime pair and congruence conditions) to the equation (3.9) does not work.

A generalization. Let us consider a more general situation. Namely, let p, q be odd primes such that $p^k + 2^m = q^l$ for some positive integers k, l, m, and let $E_{p^k,m}$ be the elliptic curve

$$y^2 = x(x - 2^m)(x + p^k).$$

As before, we have $E_{p^k,m}(\mathbb{Q})_{\mathrm{tors}} = E_{p^k,m}[2] = \{\infty, (0,0), (2^m, 0), (-p^k, 0)\}$, and a point (x, y) on $E_{p^k,m}$ such that $x, y \in \mathbb{Z}$ and $y > 0$ will be called a *nontrivial integral point*. Then we write $x = 2^\alpha p^\beta x_0$, where α and β are nonnegative integers, and x_0 is coprime to $2p$. Note that

$$\gcd(x, x+p^k) = p^{\min(\beta,k)}, \quad \gcd(x-2^m, x+p) \mid q^l, \quad \gcd(x, x-2^m) = 2^{\min(\alpha,m)},$$

and if $\gcd(x - 2^m, x + p) \neq 1$ then $q \nmid x$.

Similarly to Section 3, we have considered 72 cases depending on the values of α, β, $\gcd(x - 2^m, x + p)$ and the sign of x. In 35 cases we have easily obtained a contradiction but the remaining 37 cases cannot be rejected

entirely (obviously as in Proposition 4.1 we can write sufficient conditions for the nonexistence of an integral point in each of these cases). It is possible to formulate a theorem analogous to Theorem 2.4 but it would be very long and involve numerous systems of Pell-like equations. On the other hand, the counterparts of Theorems 2.1 and 2.2 in this general situation are not true. Namely, $E_{p^k,2}$ may have a nontrivial integral point, and $E_{p^k,1}$ may have three nontrivial integral points, as is shown by the following example.

EXAMPLE 6.7. We write selected quadruples (m, p^k, q^l, x) where (x, y) is a nontrivial integral point on $E_{p^k,m}$ $(q^l = p^k + 2^m)$.

Table 2. Integral points on $E_{p^k,m}$

m	p^k	q^l	x
1	3^2	11	$-6, 3, 24$
1	3^4	83	$-6, 27$
2	5	3^2	$-2, 10$
2	5^2	29	$-5, 20$
2	13^2	173	-117
2	5^6	15629	-15125

Acknowledgements. We would like to thank Andrzej Dąbrowski for suggesting the problem and helpful conversations. We also thank Paul Voutier for constructive comments. Last but not least, we would like to thank the anonymous referee for useful suggestions which allowed us to improve the final version of this paper.

References

[1] P. K. Alvanos and K. A. Draziotis, *Integer solutions of the equation* $y^2 = Ax^4 + B$, J. Integer Sequences 18 (2015), no. 4, art. 15.4.4, 14 pp.

[2] M. Bennett, *Integral points on congruent number curves*, Int. J. Number Theory 9 (2013), 1619–1640.

[3] M. Bennett and G. Walsh, *Simultaneous quadratic equations with few or no solutions*, Indag. Math. (N.S.) 11 (2000), 1–12.

[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[5] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973), 157–176.

[6] M. Cipu and M. Mignotte, *On the number of solutions to systems of Pell equations*, J. Number Theory 125 (2007), 356–392.

[7] A. Dąbrowski and M. Wieczorek, *On the equation* $y^2 = x(x - 2^m)(x + q - 2^m)$, J. Number Theory 124 (2007), 364–379.

[8] K. Draziotis, *Integer points on the curve* $y^2 = x^3 \pm p^k x$, Math. Comp. 75 (2006), 1493–1505.

[9] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. 44 (1923), 1–70.
[10] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, Princeton, NJ, 1992.
[11] G. Lettl, A. Pethő and P. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. 351 (1999), 1871–1894.
[12] J. Maynard, *Small gaps between primes*, Ann. of Math. 181 (2015), 383–413.
[13] K. Ono, *Euler's concordant forms*, Acta Arith. 78 (1996), 101–123.
[14] DHJ Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. 1 (2014), art. 12, 83 pp.; Erratum, 2 (2015), art. 15, 2 pp.
[15] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory 34 (1990), 235–250.
[16] C. L. Siegel, *Ueber einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. 1929, no. 1, 70 pp.
[17] L. Szalay, *On the resolution of simultaneous Pell equations*, Ann. Math. Inform. 34 (2007), 77–87.
[18] D. T. Walker, *On the diophantine equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly 74 (1967), 504–513.
[19] P. Walsh, *On two classes of simultaneous Pell equations with no solutions*, Math. Comp. 68 (1999), 385–388.
[20] H. Yang and R. Fu, *The integral points on elliptic curves* $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$, Czechoslovak Math. J. 63 (2013), 375–383.
[21] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. 179 (2014), 1121–1174.

Tomasz Jędrzejak, Małgorzata Wieczorek
Institute of Mathematics
University of Szczecin
Wielkopolska 15
70-451 Szczecin, Poland
E-mail: tjedrzejak@gmail.com
malgorzata.wieczorek@usz.edu.pl