ALGEBRA, LOGIC AND NUMBER THEORY
BANACH CENTER PUBLICATIONS, VOLUME 121
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2020

INTEGRAL POINTS ON ELLIPTIC CURVES ASSOCIATED WITH GENERALIZED TWIN PRIMES

TOMASZ JĘDRZEJAK

University of Szczecin, Institute of Mathematics
Wielkopolska 15, 70-451 Szczecin, Poland
ORCID: 0000-0002-0996-8910 E-mail: tjedrzejak@gmail.com

Abstract. This article is a continuation of our previous paper [Bull. Pol. Acad. Sci. Math. 67 (2019)] concerning elliptic curves $E_{p,m} : y^2 = x(x - 2^m)(x + p)$, where p and $p + 2^m$ are primes. There we proved inter alia that $E_{p,1}$ has at most two non-torsion integral points, and $E_{p,2}$ has no such points. Now by using completely different methods, namely an analysis of local height functions, we try to get upper bounds for the number of integral points and for the number of multiples of such points on our curves for any m. In particular, we show that no even multiples of an integral point on $E_{p,m}$ are also integral, and if $E_{p,m}$ has rank 1 and $p \equiv 3 \pmod 4$ then there are at most twelve non-torsion integral points in the union of the non-identity component and the certain subset of the identity component.

1. Introduction. It is believed that there exist infinitely many twin primes (this is a famous Twin Prime Conjecture). More generally, one expects that (for a fixed positive even integer k) there exist infinitely many primes p such that $p + k$ is also a prime (cf. first part of Conjecture B in [7]). These conjectures are still open and hard to prove. One well known result is Chen's theorem [2] stating that there are infinitely many primes p such that $p + 2$ is a prime or a product of two primes. However, in the related problem (the so called Bounded Gap Conjecture) Zhang [19] showed that there are bounded gaps between consecutive primes infinitely often. More precisely, he proved that $\liminf_{n\to\infty}(p_{n+1} - p_n) \le 7 \times 10^7$ where p_n denotes the nth prime (note that the Twin Prime Conjecture says that $\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$). Nowadays, this bound has been reduced to 246 unconditionally, and to 6 under the assumption of the generalized Elliott–

2010 *Mathematics Subject Classification*: 11G05, 11G50.

Key words and phrases: canonical height, elliptic curves, local heights, multiples of integral points, number of integral points.

The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc121-7

© Instytut Matematyczny PAN, 2020

Halberstam conjecture (see [12]). Consequently, there is at least one positive even integer (less than 247) which can be written infinitely often as the difference of two consecutive primes. We also mention the classical result due to Romanoff [13] that the set of integers of the form $p + 2^m$, where p is a prime and m is a positive integer, has positive lower density in $\mathbb{N}$. On the other hand, there are infinitely many primes p such that $p + 2^m$ is a composite number for any m [17]; one of them is $p = 47867742232066880047611079$ [3].

By the well known Siegel Theorem [14], any elliptic curve E over $\mathbb{Q}$ has only finitely many integral points. However, searching for the number of integral points in families of elliptic curves is not easy in general. Another question related to this subject is to ask which multiples of a non-torsion integral point P may be integral. It is widely expected (for instance, because it is implied by the ABC conjecture) that there is a uniform bound on the number of integers n such that nP is integral. Many authors have dealt with these problems. For example, Ingram [8] proved that there is a uniform constant C and a quantity $M(P)$ bounded above by the global Tamagawa number of E such that nP is integral for at most one value of $n > CM(P)^{16}$. Moreover, he showed that if N is square-free and E is the congruent number curve $y^2 = x^3 - N^2x$ then there is at most one value $n > 1$ such that nP is integral. Subsequently, Fujita and Terai [6] proved that if the congruent number curve has rank one then it contains at most 17 integral points. Next, Fujita and Nara [5] showed that if the Fermat elliptic curve $x^3 + y^3 = m$ (m is cube-free integer) has rank one then it has at most two integral points, and if has rank two then it contains at most six such points. They also proved that the Fermat elliptic curve of rank r has $\leq 3^r - 1$ integral points.

In this paper, we consider elliptic curves associated to the generalized twin primes, i.e., the family of elliptic curves over $\mathbb{Q}$ given by

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

where p, q are odd primes such that $q - p = 2^m$, $m \geq 1$. Such curves were considered for the first time by Dąbrowski and Wieczorek in [4]. Here we give some information concerning this family. Note that $E_{p,m}(\mathbb{Q})_{\mathrm{tors}} = E_{p,m}[2] = \{\infty, (0,0), (2^m, 0), (-p, 0)\}$ (see [11, Main Theorem 1]) and $r_{p,m} := \operatorname{rank} E_{p,m}(\mathbb{Q}) \leq 2$ (see [10, Proposition 4.19]). Moreover, this bound can only be obtained for $m = 3$ or $m > 4$ and certain special primes $q \equiv 1 \pmod 8$. Clearly, $E_{p,m}(\mathbb{R})$ has two connected components: the non-identity component consisting of the points with x-coordinates in the interval $[-p, 0]$, and the identity component consisting of the affine points with x-coordinates $\geq 2^m$ and the point at infinity. Note also that under the assumption of the Parity Conjecture $r_{p,m} = 1$ if ($m = 3$ and $p \equiv 5 \pmod 8$) or $m = 4$ or ($m \geq 5$ and $p \equiv 3, 5, 7 \pmod 8$) (see [4, Corollary 2]). 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 reduction at p and q is multiplicative.

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) is non-torsion and we call it a *non-torsion integral point on* $E_{p,m}$ (however note that equation (1.1) is not minimal in general). If $E_{p,m}$ has a non-torsion integral point then, by the consideration above, we have $\operatorname{rank} E_{p,m}(\mathbb{Q}) \in \{1, 2\}$. Clearly, two non-torsion integral points on $E_{p,m}$ may differ by the torsion point. For example, $E_{5,3}$ has rank one and its non-torsion integral points $(-1, 6)$ and $(40, 240)$ differ by the torsion point $(0, 0)$ (notice that $E_{5,3}$ has only four non-torsion integral points).

2. Results.

In this section, we state the main results of this paper. In [9] we considered the same family, and proved among others that $E_{p,1}$ has at most two non-torsion integral points, and $E_{p,2}$ has no such points. We have also listed all possible integral points as solutions of certain systems of Pell-like equations. The purpose of this paper is to describe the upper bounds for the number of integral points (at least in certain subsets) in this family for $m > 3$. We are also interested in multiples of non-torsion integral points on $E_{p,m}$. For instance, we show that no even multiples of an integral point on $E_{p,m}$ are also integral, and if $E_{p,m}$ has rank 1 and $p \equiv 3 \pmod 4$ then there is at most twelve non-torsion integral points with x-coordinates $\le 2^m 15^2 p$. If moreover Conjecture 1 is true, then this number reduces to eight. Our main method are an analysis of the local height functions and estimations of the Nèron–Tate height on elliptic curves.

Theorem 1. *Let $p \equiv 3 \pmod 4$ or ($p \equiv 1 \pmod 4$ and $m = 3$) or $m \le 2$. Assume that the subgroup Γ of $E_{p,m}(\mathbb{Q})$ which contains $E_{p,m}[2]$ is generated (modulo torsion) by the single non-torsion point $P \in E_{p,m}(\mathbb{Q})$ and (without loss of generality) $x(P) > 0$. Let Q be an integral point in Γ.*

1) *If Q belongs to the non-identity component of $E_{p,m}(\mathbb{R})$ then $Q = nP+T$, where $|n| \le 1$ and $T \in \{(0,0),(-p,0)\}$.*
2) *If Q has x-coordinate in the interval $[2^m, 2^m 15^2 p]$ then $Q = nP + T$, where $|n| \le 3$ and $T \in \{\infty, (2^m, 0)\}$.*

Corollary 1. *Let $p \equiv 3 \pmod 4$ or ($p \equiv 1 \pmod 4$ and $m = 3$) or $m \le 2$. If $E_{p,m}(\mathbb{Q})$ has rank one then there are at most twelve non-torsion integral points with x-coordinate $\le 2^m 15^2 p$.*

Theorem 2. *Assume that P is a non-torsion point in $E_{p,m}(\mathbb{Q})$ and n is an integer. If nP is an integral point then n is odd. Assume moreover that $p \equiv 3 \pmod 4$ or ($p \equiv 1 \pmod 4$ and $m = 3$) or $m \le 2$.*

1) *If nP belongs to the non-identity component then $n = \pm 1$.*
2) *If $x(nP) \in [2^m, 2^m 15^2 p]$ then $n \in \{\pm 1, \pm 3\}$.*

3. Proofs.

In this section, we prove our main results. The proofs split in a natural way into several lemmata. We start with two lemmata concerning multiples of integral points which are of independent interest.

Lemma 1. *If E is an elliptic curve over $\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ is not integral (with respect to a given Weierstrass equation of E) then for any nonzero integer n a point nP is not integral too.*

Proof. See [15, Exercise 9.12]. ∎

Lemma 2. *If $P \in E_{p,m}(\mathbb{Q})$ is a non-torsion point then $x(2P) \notin \mathbb{Z}$. In consequence, nP is not integral for any even n.*

Proof. By Lemma 1 we may assume that $P = (x,y)$, where x, y are nonzero integers. By the duplication formula, we obtain

$$x(2P) = \frac{(x^2 + 2^m p)^2}{4x(x-2^m)(x+p)} .$$

Clearly, if x is odd then $x(2P)$ is not an integer, so assume that $x = 2^{\alpha}x_1$ where x_1 is odd, and α is a positive integer. Substituting, we get

$$x(2P) = \frac{(2^{2\alpha-1}x_1^2 + 2^{m-1}p)^2}{2^{\alpha}x_1(2^{\alpha}x_1 - 2^m)(2^{\alpha}x_1 + p)}\,, \tag{3.1}$$

so if $\alpha \geq m$ then

$$\mathrm{ord}_2((2^{2\alpha-1}x_1^2 + 2^{m-1}p)^2) = 2m-2 < \alpha + m = \mathrm{ord}_2(2^{\alpha}x_1(2^{\alpha}x_1 - 2^m)(2^{\alpha}x_1 + p)),$$

and consequently $x(2P) \notin \mathbb{Z}$, hence we assume that $\alpha < m$, in particular $m > 1$. Now suppose that $x(2P) \in \mathbb{Z}$. Then x_1 divides $(2^{2\alpha-1}x_1^2+2^{m-1}p)^2$, hence any prime factor of x_1 divides $2^{m-1}p$. Thus $x_1 = \pm p^{\beta}$ where $\beta \geq 0$. If $\beta > 1$ then $\mathrm{ord}_p\big((2^{2\alpha-1}x_1^2 + 2^{m-1}p)^2\big) = 2$ but $\mathrm{ord}_p\big(2^{\alpha}x_1(2^{\alpha}x_1 - 2^m)(2^{\alpha}x_1 + p)\big) = 1 + \beta > 2$, so $\beta \leq 1$. The cases $x_1 = 1$ or $-p$ are impossible since they imply $0 < x = 2^{\alpha} < 2^m$ or $x = -2^{\alpha}p < -p$. First consider the case $x_1 = -1$, i.e., $x = -2^{\alpha}$. By [9, Theorem 2.4] we obtain, $\alpha = m-3$ (so in particular $m \geq 4$) and $p - 2^{m-3}$ is a square, say c^2 (c is a positive integer). Hence the denominator of (3.1) equals $2^{2m-6}9(p-2^{m-3}) = 2^{2m-6}(3c)^2$, and the numerator of (3.1) equals $2^{2\mu-2}(2^{2m-6-\mu} + 2^{m-\mu}p)^2 = 2^{2\mu-2}(2^{2m-6-\mu}9 + 2^{m-\mu}c^2)^2$ where $\mu = \min(2m-6, m)$. Since $x(2P) \in \mathbb{Z}$, we have $c = 3$ or $c = 9$. In any case $c = 3c'$ but then the prime $q = p+2^m = 9c'^2+2^{m-3}+2^m = 9(c'^2+2^{m-3})$ which is a contradiction. Now let $x_1 = p$, i.e., $x = 2^{\alpha}p$ ($0 < \alpha < m$). Again by [9, Theorem 2.4] we get $m \geq 4, 3 \leq \alpha \leq m-1$, $2 \nmid \alpha$, and $p = b^2 + 2^{m-\alpha}$, $q = pc^2 - 2^{\alpha}b^2$, $c^2 = 2^{\alpha}+1$ where b, c are positive relatively prime odd integers. In this case the denominator and the numerator of (3.1) are equal to $2^{2\alpha}p^2(p-2^{m-\alpha})(2^{\alpha}+1) = 2^{2\alpha}p^2(bc)^2$ and $2^{2\mu-2}p^2(2^{2\alpha-\mu}p+2^{m-\mu})^2 = 2^{2\mu-2}p^2(2^{2\alpha-\mu}b^2+2^{m-\mu}c^2)^2$ respectively ($\mu = \min(2\alpha, m)$). Since bc divides $2^{2\alpha-\mu}b^2 + 2^{m-\mu}c^2$, we get $b = c = 1$, and consequently $p + 2^m = q = p - 2^{\alpha}$ which is an absurd. Therefore always $x(2P) \notin \mathbb{Z}$, and $nP = 2(kP)$ is not an integral point for $n = 2k$. This finishes the proof. ■

Our next proofs involve estimations of the canonical height and an analysis of local height function. Now we introduce some notation and facts about height functions. Further details may be found for example in Silverman's books [15, 16].

Let E be an elliptic curve over $\mathbb{Q}$. For $P \in E(\mathbb{Q})$ with $x(P) = a/b$ where a and b are relatively prime integers, the *naive height* $h : E(\mathbb{Q}) \to \mathbb{R}$ is defined by $h(P) = \log\max\big(|a|, |b|\big)$ (we put also $h(\infty) = 0$). The *canonical height* (or *Nèron–Tate height*) $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is defined by

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}\,.$$

The canonical height is a quadratic form on $E(\mathbb{Q})$ modulo torsion. In particular, $\widehat{h}(nP) = n^2\widehat{h}(P)$, and $\widehat{h}(P) = 0$ if and only if P is a torsion point. Nèron and Tate (see e.g. [16]) showed that $\widehat{h}$ decomposes into the sum of the local height functions $\widehat{h}_p : E(\mathbb{Q}_p) \to \mathbb{R}$ where p is a place in $\mathbb{Q}$, i.e., p is a prime or infinity. Hence for any $P \in E(\mathbb{Q})$ we have

$$\widehat{h}(P) = \sum_{p\leq\infty} \widehat{h}_p(P).$$

In fact this sum is finite since $\widehat{h}_p(P) = 0$ for any point P and for almost all p. For example, if p is a prime of the good reduction of E then $\widehat{h}_p(P) = 1/2\max\big(0, -v_p(x(P))\big)$ where

$v_p(x) = \operatorname{ord}_p(x)\log p$ and $P \neq \infty$. There are also the (more complicated) formulae for computation of non-archimedean local heights $\widehat{h}_p$ in the other cases (when the reduction at p is not good and a point P is singular after the reduction, see [16, pp. 478–479]). To estimate the archimedean contribution $\widehat{h}_\infty$ to the canonical height we use Tate's series:

$$\widehat{h}_\infty(P) = \frac{1}{2}\log\bigl|x(P)\bigr| + \frac{1}{8}\sum_{k=0}^{\infty}\frac{\log\bigl|z(2^kP)\bigr|}{4^k} - \frac{1}{12}\log|\Delta_E|, \tag{3.2}$$

where z is a certain function depending on the curve E (we omit details but E must be given by the minimal equation) and Δ_E is the discriminant of E.

Lemma 3. *If $p \equiv 3 \pmod 4$ or ($p \equiv 1 \pmod 4$ and $m \le 3$) then*

$$\widehat{h}(P) \le \frac{1}{4}\log(a^2 + 2^m pb^2) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right)$$

for any $P \in E_{p,m}(\mathbb{Q}) \setminus \{\infty\}$, where $x(P) = a/b$ and $\gcd(a,b) = 1$.

Proof. Under our assumptions a global minimal model of $E_{p,m}$ is given by (1.1). We shall consider two cases. In archimedean case we use Tate's series (3.2) where now $z(P) = (1+2^m pt^2)^2$ with $t = 1/x(P)$. Clearly, $E_{p,m}(\mathbb{R})$ has two components, and for any point Q in the identity component $E^0_{p,m}(\mathbb{R})$ we have $1 \le z(Q) \le (1+p2^{-m})^2$. Since $2^kP \in E^0_{p,m}(\mathbb{R})$ (for $k \ge 1$), we get

$$\begin{aligned}\widehat{h}_\infty(P) &\le \frac{1}{2}\log\bigl|x(P)\bigr| + \frac{1}{8}\log\bigl|z(P)\bigr| + \frac{1}{8}\sum_{k=1}^{\infty}\frac{2\log(1+p2^{-m})}{4^k} - \frac{1}{12}\log|\Delta_E| \\ &= \frac{1}{4}\log(x(P)^2 + 2^m p) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right) - \frac{1}{12}\log|\Delta_E|.\end{aligned}$$

Now consider non-archimedean case. Let l be a prime. By [16, p. 478], we obtain

$$\widehat{h}_l(P) \le \frac{1}{2}\max\bigl(0, -v_l(x(P))\bigr) + \frac{1}{12}v_l(\Delta_E).$$

Note that $x(P) = a/b$, and so $\max\bigl(0, -v_l(x(P))\bigr) = v_l(b)$. Since

$$\sum_l v_l(\Delta_E) = \sum_l \log l^{\operatorname{ord}_l(\Delta_E)} = \log\prod_l l^{\operatorname{ord}_l(\Delta_E)} = \log|\Delta_E|,$$

where the above sum is over all (finite) primes, combining the inequalities for local heights, we finally get

$$\widehat{h}(P) \le \frac{1}{4}\log(a^2 + 2^m pb^2) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right),$$

which completes the proof. ∎

Lemma 4. *If $p \equiv 3 \pmod 4$ or ($p \equiv 1 \pmod 4$ and $m = 1, 3$) or ($p \equiv 1 \pmod 8$ and $m = 2$) then for any non-torsion point $P \in E_{p,m}(\mathbb{Q})$ we have*

$$\widehat{h}(P) \ge \frac{1}{16}\log(2^m(p + 2^m)).$$

Proof. See [4, Proposition 7]. ∎

Proof of Theorem 1. We can assume that $m \ge 3$ because by [9, Theorems 2.1, 2,2, 2.3], $E_{p,2}$ has no non-torsion integral points at all, $E_{p,1}$ has no non-torsion integral points in the non-identity component, and at most two such points in the identity component. By assumption, $Q = nP + T$ and $x(Q) = a$ where T is a torsion point, and n, a are integers. Let us first assume that $Q \notin E^0_{p,m}(\mathbb{R})$. Then $a \in [-p, 0]$ and $T \in \big\{(0,0), (-p,0)\big\}$ (since P, $(2^m, 0)$ and ∞ belong to the identity component $E^0_{p,m}(\mathbb{R})$). Therefore by Lemma 3, we get

$$\widehat{h}(P) \le \frac{1}{4}\log(a^2 + 2^m p) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right) \le \frac{1}{4}\log(p^2 + 2^m p) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right).$$

On the other hand, by Lemma 4 and properties of the canonical height, we obtain

$$\widehat{h}(P) = \widehat{h}(nQ + T) = \widehat{h}(nQ) = n^2 \widehat{h}(Q) \ge \frac{n^2}{16}\log(2^m(p + 2^m)).$$

Consequently, after some calculations, we have

$$n^2 \le \frac{4\log p + 16/3\log(p + 2^m) - 4m/3\log 2}{\log(p + 2^m) + m\log 2}.$$

It is not difficult to check (we used Mathematica's [18] command Maximize) that the function on the right side reaches its maximum for $m = 3$ and $p = 5$, hence $n^2 < 3.74$. So $|n| \le 1$, which proves the first part.

Now suppose that $a \in [2^m, 2^m 15^2 p]$. Consequently, $T \in \{\infty, (2^m, 0)\}$. As before by Lemmata 3 and 4, we obtain

$$\frac{n^2}{16}\log(2^m(p + 2^m)) \le \widehat{h}(P) \le \frac{1}{4}\log(2^{2m}p^2 15^4 + 2^m p) + \frac{1}{12}\log\left(1 + \frac{p}{2^m}\right),$$

which implies

$$n^2 \le \frac{4\log(2^{2m}p^2 15^4 + 2^m p) + 4/3\log(1 + p/2^m)}{\log(p + 2^m) + m\log 2}.$$

We checked (by using Mathematica) that the function on the right side reaches its maximum for $m = 3$ and $p = 7$ (and it is circa 15.9519). Therefore $|n| \le 3$, which completes the proof. ∎

Proof of Corollary 1. By Remark 2 we know that there are at most two non-torsion integral points in the non-identity component. If $E_{p,m}(\mathbb{Q})$ has rank 1 then $\Gamma = E_{p,m}(\mathbb{Q})$, and by Theorem 1 and Lemma 2, any non-torsion integral point with x-coordinate in $[2^m, 2^m 15^2 p]$ is contained in the set $\{\pm P,\ \pm P + (2^m, 0),\ \pm 2P + (2^m, 0),\ \pm 3P,\ \pm 3P + (2^m, 0)\}$, and we are done. ∎

Proof of Theorem 2. It follows immediately from Lemma 2 and the proof of Theorem 1. ∎

4. Remarks and conjectures. In this section we make five remarks about our theorems and methods, and state two conjectures. We also discuss numerical computations.

Remark 1. Note that Theorem 1 and Corollary 1 are not 'empty' since for e.g., $m = 4$ or ($m \ge 5$ and $p \equiv 3, 5, 7 \pmod 8$) the root number of $E_{p,m}(\mathbb{Q})$ is -1 so conjecturally $\operatorname{rank} E_{p,m}(\mathbb{Q}) = 1$. In fact, we have many examples of curves $E_{p,m}$ with a positive rank.

Remark 2. Note that by [9, Theorems 2.1–2.4], if $p \equiv 3 \pmod 4$ or $m \le 3$, we have at most two non-torsion integral points in the non-identity component. If they exist, they have x-coordinate -1 (for $m = 3$), and $-2(2^{m-3} - 1)^2$ (for $m \ge 4$).

Remark 3. The bound $2^m 15^2 p$ looks arbitrary, but that is not the whole truth. Indeed, as we showed in [9, Theorem 2.4], any non-torsion integral point in the identity component (with an exception in one case) has x-coordinate of the form $2^\alpha a^2 p^\beta$ where $0 < \alpha \leq m$, $0 \leq \beta \leq 1$, and a is a positive integer. Moreover, almost all integral points (with one exception) that we found numerically have x-coordinates $\leq 2^m 13^2 p$ (see below for details).

Remark 4. In [4, Proposition 7] there are also lower bounds for $\widehat{h}(P)$ for other p and m than in Lemma 4. We are able to compute upper bounds for the canonical height for $p \equiv 1 \pmod 4$ and $m \geq 4$ (cf. Lemma 3) but in this case the equation (1.1) is not minimal. We must use the minimal model, i.e., $y^2 + xy = x^3 + \frac{p-2^m-1}{4}x^2 - 2^{m-4}px$ but we are interested in the integral solutions of (1.1).

Remark 5. Note that the family of the congruent number elliptic curves (considered in [6]) is the family of quadratic twists of one curve $y^2 = x^3 - x$, and the family of Fermat elliptic curves (considered in [5]) is the family of cubic twists of one curve $x^3 + y^3 = 1$. Our two-parameter family $E_{p,m}$ is not a family of quadratic twists nor cubic twists, and perhaps it is harder to estimate the number of integral points in this case.

We have made some numerical calculations in Magma [1]. We were looking for integral points on $E_{p,m}$ for $m \leq 10$ and $p \leq p_{1000} = 7919$ (by using the command IntegralPoints) but for some m and p Magma was not able to answer. We also checked certain bigger m or p, and e.g., we found the integral point

$$(2019550184120871208, 2870000639061829344674420880) \text{ on } E_{178566897581,3}$$

and the integral point $(16331640832, 2087108321525760)$ on $E_{23593,12}$. Among all tested curves $E_{p,m}$ we found only one example of curve with eight non-torsion integral points (all other our examples have at most six integral points): $m = 9$, $p = 89$, $q = 601$, $(x, y) = (-64, \pm 960)$, $(712, \pm 10680)$, $(2312, \pm 99960)$, $(481312, \pm 333771360)$. Note that $E_{89,9}(\mathbb{Q})$ has rank two, and the points $P_1 = (-16/169, -144240/2197)$, $P_2 = (-200/9, 24040/27)$ generate $E_{89,9}(\mathbb{Q})$ modulo torsion. We have also the following relations: $(-64, -960) = P_2 + (2^m, 0)$, $(712, -10680) = P_2 + (-p, 0)$, $(2312, 99960) = P_1 + P_2$, $(481312, -333771360) = P_1 + (0, 0)$. In addition, for all found non-torsion integral points P on the tested $E_{p,m}$ we also checked that $3P$ is not integral. Therefore numerical computations performed in Magma, Theorems 1, 2, Corollary 1, and other reasons mentioned below suggest the following.

Conjecture 1. *If P is a non-torsion point in $E_{p,m}(\mathbb{Q})$ then $3P$ is not integral point.*

Conjecture 2. *The curve $E_{p,m}$ has at most eight non-torsion integral points.*

Notice that if Conjecture 1 is true then from the proof of Corollary 1 we see that if $E_{p,m}(\mathbb{Q})$ has rank one then it has at most 8 non-torsion integral points with x-coordinates $\leq 2^m 15^2 p$ (indeed, $\pm 3P = 3(\pm P)$ and $\pm 3P + (2^m, 0) = 3(\pm P + (2^m, 0))$ are not integral). Similarly, in this case by Theorem 2, we immediately deduce that if nP is a non-torsion integral point and $x(nP) \leq 2^m 15^2 p$ then $n = \pm 1$.

Here we explain why we believe in Conjecture 1. We found the 'triplication' formula, i.e., for a point $P = (x, y)$ on $E_{p,m}$ we have $x(3P) = \frac{xF(x)^2}{G(x)^2}$ where $F(x) = x^4 + 2^{m+1}3px^2 + 2^{m+2}p(p - 2^m)x - 2^{2m}3p^2$, $G(x) = -3x^4 - 4(p - 2^m)x^3 + 2^{m+1}3px^2 + 2^{2m}p^2$. Assume that P is integral (otherwise by Lemma 1, $3P$ is not integral too). Then $x(3P) \in \mathbb{Z} \Leftrightarrow G(x)^2 \mid xF(x)^2 \Leftrightarrow \gcd(G(x)^2, xF(x)^2) = G(x)^2$, but we can prove that for any integer x, the only prime divisors of $\gcd\big(G(x)^2, xF(x)^2\big)$ are 2, p, and $q = p + 2^m$. Since it is reasonable to suppose that for any $x = x(P) \in \mathbb{Z}$ the integer $G(x)$ has (at least one) another prime factor, we think that $x(3P) \notin \mathbb{Z}$.

References

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

[2] 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.

[3] F. Cohen, J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comp. 29 (1975), 79–81.

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

[5] Y. Fujita, T. Nara, *Generators and integral points on twists of the Fermat cubic*, Acta Arith. 168 (2015), 1–16.

[6] Y. Fujita, N. Terai, *Generators and integer points on the elliptic curve $y^2 = x^3 - nx$*, Acta Arith. 160 (2013), 333–348.

[7] G. H. Hardy, 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.

[8] P. Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory 129 (2009), 182–208.

[9] T. Jędrzejak, M. Wieczorek, *Integral points on elliptic curves $y^2 = x(x - 2^m)(x + p)$*, Bull. Pol. Acad. Sci. Math. 67 (2019), 53–67.

[10] A. W. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, NJ, 1992.

[11] K. Ono, *Euler's concordant forms*, Acta Arith. 78 (1996), 101–123.

[12] DHJ Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. 1 (2014), Art. 12; Erratum, ibid. 2 (2015), Art. 15.

[13] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. 109 (1934), 668–678.

[14] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. 1929, no. 1, 41–69.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[16] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[17] M. V. Vassilev-Missana, *Note on extraordinary primes*, Notes Number Theory Discrete Math. 1 (1995), 111–113.

[18] Wolfram Research, Inc., *Mathematica*, Version 9.0, Champaign, IL, 2012.

[19] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) 179 (2014), 1121–1174.