International Journal of Number Theory
Vol. 9, No. 6 (2013) 1619–1640
© World Scientific Publishing Company
DOI: 10.1142/S1793042113500474

World Scientific
www.worldscientific.com

INTEGRAL POINTS ON CONGRUENT NUMBER CURVES

MICHAEL A. BENNETT
Department of Mathematics, University of British Columbia
Vancouver, BC, Canada V6T 1Z2
bennett@math.ubc.ca

Received 20 December 2012
Accepted 8 April 2013
Published 10 June 2013

We provide a precise description of the integer points on elliptic curves of the shape $y^2 = x^3 - N^2x$, where $N = 2^ap^b$ for prime p. By way of example, if $p \equiv \pm 3 \pmod 8$ and $p > 29$, we show that all such points necessarily have $y = 0$. Our proofs rely upon lower bounds for linear forms in logarithms, a variety of old and new results on quartic and other Diophantine equations, and a large amount of (non-trivial) computation.

Keywords: Elliptic curves; congruent numbers; integral points.

Mathematics Subject Classification 2010: 11D25, 11G05

1. Introduction

If N is a positive integer, then N is a congruent number, that is, there exists a right triangle with rational sides and area N, precisely when the elliptic curve

$$E_N : y^2 = x^3 - N^2x$$

has infinitely many rational points. In this paper, we will address the question of whether curves of the shape E_N possess *integral* points of infinite order, provided we know they have rational points with this property. We will concentrate on the case when E_N has bad reduction at no more than a single odd prime, i.e. where $N = 2^ap^b$ for a and b non-negative integers and p an odd prime. In this situation, we have a reasonable understanding of whether or not the Mordell–Weil rank of $E_N(\mathbb{Q})$ is positive or not. Additionally, a number of recent papers [10–12, 15, 25–28] have considered precisely this situation. In [11], by way of example, an algorithm is given for solving such Diophantine equations for a, b and p fixed, based upon conversion of the problem to one of solving certain unit equations over biquadratic fields; our Theorem 1.1 makes this essentially a trivial problem. The papers of Draziotis [10] and Walsh [26] consider (in case $a = 0$) the situation more general than that of [11], where b is allowed to vary. The latter sharpens and generalizes the former, providing, given p, precise upper bounds for the number of integers x, y and b for which

$$y^2 = x^3 \pm p^b x,$$

where the paper at hand will vary from [10, 26] is that our emphasis will be more on obtaining a complete classification of all (p, a, b) for which $E_N(\mathbb{Z})$ contains non-torsion points, than on finding bounds for the number of solutions corresponding to a given p. For $a = 0$, this essentially follows from combining the results of [4, 26]. As we shall see, the case $a > 0$ presents a number of interesting subtleties which we feel will make our more general deliberations worthwhile. Indeed, most of the work in this paper will be concerned with treating certain families of Diophantine equations that arise for positive a.

From now on, we will fix p to be an odd prime number, and a and b to be non-negative integers. Since E_N is rationally isomorphic to $E_{m^2 N}$ for each non-zero integer m, and since both E_1 and E_2 have rank 0 over $\mathbb{Q}$ (and $E_N(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ in all cases; see, e.g., [18, Lemma 4.20]), we may suppose, without loss of generality, that b is odd. We are interested in describing the integer solutions (x, y), with, say, $y > 0$ to the Diophantine equation:

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b). \tag{1}$$

Following the terminology of [26], a solution (x, y) (with $y > 0$) to (1) will be called *primitive* if both

$$\min\{\nu_2(x), a\} \leq 1 \quad \text{and} \quad \min\{\nu_p(x), b\} \leq 1$$

and *imprimitive* otherwise. Clearly it suffices to determine all primitive integer solutions. Indeed, imprimitive solutions to (1) necessarily arise from primitive solutions to $u^2 = v(v + 2^c p^d)(v - 2^c p^d)$ with

$$a \equiv c \pmod 2, \quad b \equiv d \pmod 2, \quad 0 \leq c \leq a, \ \ 0 < d \leq b,$$

via multiplication of u and v by suitable powers of 2 and p. We note that primitive solutions to (1) correspond to S-integral points on E_p and E_{2p}, where $S = \{2, p, \infty\}$.

As we search over odd primes p, and integral a and b, we find a number of triples that satisfy (1). For example, we have the following solutions we will deem sporadic; in each case $b = 1$.

p	a	x	p	a	x	p	a	x	p	a	x
3	1	-3	3	3	25	7	3	-7	29	0	284229
3	1	-2	5	0	-4	7	4	-63	41	6	42025
3	1	12	5	0	45	11	1	2178			
3	1	18	5	2	25	17	5	833			
3	1	294	7	1	112	17	7	16337			

(2)

Next, we encounter solutions in a number of families, many of which are, presumably, infinite. Again, in each case, we have $b = 1$. The variables r and s denote integers:

$$r^4 + s^4 = p, \quad a = 1, \quad x = -(2rs)^2, \tag{3}$$

$$r^4 + 6r^2s^2 + s^4 = p, \quad a = 0, \quad x = -(r^2 - s^2)^2, \tag{4}$$

$$r^4 + 12r^2s^2 + 4s^4 = p, \quad a = 1, \quad x = -2(r^2 - 2s^2)^2, \tag{5}$$

$$(2^{a-1})^2 - ps^2 = -1, \quad a \text{ odd}, \quad x = p^2s^2, \tag{6}$$

$$p^2 - 2s^2 = -1, \quad a = 0, \quad x = s^2, \tag{7}$$

$$p^2r^4 - 2s^2 = 1, \quad p \equiv 1 \pmod 8, \quad a = 1, \quad x = 2(pr)^2, \tag{8}$$

$$2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 = ps^2, \quad a \geq 3, \quad x = p(2^{a-2} + 1)^2, \tag{9}$$

$$p^2 \pm 6p + 1 = 8s^2, \quad a = 1, \quad x = \frac{1}{2}(p \pm 1)^2. \tag{10}$$

Our main result is the following.

Theorem 1.1. *The primitive integers solutions to Eq.* (1) *in non-zero integers* (x, y), *non-negative integers* a, b *and odd prime* p *correspond to those in table* (2) *and solutions to Eqs.* (3)–(10). *In particular, all primitive solutions have* $b = 1$.

An almost immediate corollary to this is the following.

Corollary 1.2. *If* $N = 2^a p^b$ *for* a *and* b *non-negative integers, where* $p \equiv \pm 3 \pmod 8$ *is prime and* $p \notin \{3, 5, 11, 29\}$, *then*

$$E_N(\mathbb{Z}) = \{(0, 0), (\pm N, 0)\}.$$

If $p \in \{3, 5, 11, 29\}$, *then all primitive integral solutions to Eq.* (1) *with* $y \neq 0$ *have* $b = 1$ *and* (p, a, x) *in the following set*:

$$\{(3,1,-3), (3,1,-2), (3,1,12), (3,1,18), (3,1,294), (3,3,25),$$
$$(5,0,-4), (5,0,45), (5,2,25), (11,1,2178), (29,0,284229)\}.$$

To obtain Corollary 1.2 from Theorem 1.1, note that solutions to Eqs. (3)–(6), (8) and (9) necessarily have $p \equiv 1 \pmod 8$, while those to (7) have $p \equiv \pm 1 \pmod 8$. The observation that solutions to (10) have $p \equiv 1 \pmod{16}$ or $p \equiv 7 \pmod{16}$, depending on the choice of + or − sign, completes the proof of the corollary.

It is worth commenting at this point that all primes $p \equiv 5, 7 \pmod 8$ are congruent numbers, so that $E_p(\mathbb{Q})$ is infinite for such primes, while the same is true for $2p$ (and hence $E_{2p}(\mathbb{Q})$), when $p \equiv 3, 7 \pmod 8$. This follows from results of Monsky [21] (see also [7, 8, 16]), obtained via careful analysis of mock-Heegner points.

A cursory examination of the families (3)–(10) makes it clear that, given a prime p, determination whether or not there exist non-trivial integer solutions to the corresponding equation (1) is a routine matter, except possibly for families (6),

(8) and (9). To have a solution to Eq. (6), classical work on primitive divisors in recurrence sequences implies that the smallest positive integer solution to $X^2 - pY^2 = -1$ necessarily has $X = 2^{a-1}$. Similarly, for Eq. (8) to be satisfied, the smallest positive integer solution to $X^2 - 2Y^2 = 1$ with $p \mid X$ must have $X = pr^2$ (see Proposition 2.2). In either case, the computational complexity of solving the corresponding equation is essentially equivalent to that of finding a fundamental unit in the related quadratic field. In the case of family (9) (which we will discuss in detail in Sec. 4), lower bounds for linear forms in three complex logarithms enable us to obtain a reasonable bound for a solely in terms of the fundamental unit in $\mathbb{Q}(\sqrt{p})$. With this in mind, by way of example, it is easy to prove the following.

Proposition 1.3. *If* $3 \leq p < 100$ *is prime, then all primitive integral solutions to Eq.* (1) *with* $y \neq 0$ *have* $b = 1$ *and*

$$\begin{aligned}(p, a, x) \in \{&(3,1,-3),(3,1,-2),(3,1,12),(3,1,18),(3,1,294),\\ &(3,3,25),(5,0,-4),(5,0,45),(5,2,25),(7,0,25),(7,1,18),(7,1,112),\\ &(7,3,-7),(7,4,-63),(11,1,2178),(17,1,-16),(17,1,-2),\\ &(17,1,162),(17,1,578),(17,3,153),(17,3,289),(17,5,833),\\ &(17,7,16337),(23,1,242),(29,0,284229),(41,0,-9),(41,0,841),\\ &(41,4,1025),(97,1,-144)\}.\end{aligned}$$

The outline of this paper is as follows. In Sec. 2, we list a number of classical and modern results from the theory of Diophantine equations to which we will appeal in the course of proving Theorem 1.1. Section 3 consists of an elementary (and rather painful) case-by-case analysis required to reduce the problem of solutions to (1) to (2)–(10). On first consideration (and, for that matter, subsequently), the reader might wish to omit much of this section. In Sec. 4, we focus our attentions on a family of Diophantine equations related to (9), applying an assortment of local arguments together with state-of-the-art lower bounds for linear forms in logarithms of algebraic numbers. Sections 5 and 6 consist of heuristics, data and occasional proofs of results pertaining to the sets of primes p for which Eqs. (3)–(10) have solutions.

2. Preliminary Results

We begin by stating some results regarding Diophantine equations that will prove useful in the sequel. The first is essentially an old result of Ljunggren [19] and Mordell [22, 23], but is most readily found as Théorèmes 2.1 and 2.2 of Samuel [24] — the proof is elementary but not easy.

Proposition 2.1. *If* p *is prime and* $\delta \in \{0, 1\}$, *then the only solutions in positive integers to the Diophantine equation*

$$x^4 - 2^{\delta} p y^2 = 1 \qquad (11)$$

are given by

$$(x, y, p, \delta) \in \{(3, 4, 5, 0), (7, 20, 3, 1), (99, 1820, 29, 0)\}.$$

If p is prime, then the only solutions in positive integers to the Diophantine equation

$$4x^4 - py^2 = 1 \tag{12}$$

correspond to

$$(x, y, p) \in \{(1, 1, 3), (2, 3, 7)\}.$$

Continuing with the theme of quartic Diophantine equations, we will have need of Theorem 1.2 of the author and Walsh [6] which we state as the following.

Proposition 2.2. *Let $b, d > 1$ be squarefree integers and suppose that $T + U\sqrt{d}$ denotes the fundamental solution to the Pell equation $X^2 - dY^2 = 1$, and, for $k \geq 1$, that integers T_k and U_k satisfy $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$. Define the* rank of apparition *$\alpha(b)$ of b in $\{T_k\}$ to be the smallest positive integer k for which $b \mid T_k$. If, for all k, b fails to divide T_k, we set $\alpha(b) = \infty$. Then the Diophantine equation*

$$b^2x^4 - dy^2 = 1$$

has at most one solution in positive integers x and y. If such a solution exists, then we necessarily have $bx^2 = T_{\alpha(b)}$.

Next we require Proposition 8.1 of the author and Skinner [5]; it is obtained, basically, by specializing a more general result on solutions to $a^n + b^n = 2c^2$.

Proposition 2.3. *The Diophantine equation*

$$2x^2 - 1 = y^n$$

has only the solutions $(x, y, n) = (1, 1, n)$ and $(x, y, n) = (78, 23, 3)$ in positive integers x, y and n with $n \geq 3$.

We will also appeal to a theorem of the author, Ellenberg and Ng [4].

Proposition 2.4. *There are no solutions in coprime positive integers x, y and z to the equation $x^4 + y^2 = z^n$ with $n \geq 4$. The only solution in positive coprime integers x, y and z to the equation $x^4 + 2y^2 = z^n$ with $n \geq 4$ is given by $(x, y, z, n) = (1, 11, 3, 5)$.*

This is, in essence, a technical appendix to earlier work of Ellenberg [13] who obtained a like result for the first of these equations with $n > 211$ prime.

The final result of which we will have use is a recent theorem of the author, Dahmen, Mignotte and Siksek [3].

Proposition 2.5. *The Diophantine equation*

$$x^{2b} \pm 6x^b + 1 = 8d^2$$

has no solutions in positive integers x, b and d, with $x, b > 1$.

3. Case-by-Case Analysis

A number of the cases we will consider here have been treated in [26]; we include full details in the interest of keeping our exposition reasonably self-contained. Let us begin by supposing we have a solution in non-zero integers x and y, non-negative integer a, odd positive integer b, and odd prime p, to Eq. (1). Write $x = 2^\alpha p^\beta x_1$, where α and β are non-negative integers, and x_1 is coprime to $2p$. Notice that if $\alpha \neq a$, then from (1), α is necessarily even, while $\beta \neq b$ similarly implies that β is even. *A priori*, there are nine cases to consider depending on the sizes of α and β, relative to a and b, respectively. We must also treat positive and negative values of x separately. Since we will restrict our attention to primitive solutions, we may suppose further that

$$\min\{\alpha, a\} \leq 1 \quad \text{and} \quad \min\{\beta, b\} \leq 1. \tag{13}$$

3.1. Case 1: $\alpha < a, \beta < b$

In this situation, from (1) it follows that both α and β are even and hence, from (13), $\alpha = \beta = 0$. There thus exists a positive integer y_1 such that

$$y_1^2 = x_1(x_1 - 2^a p^b)(x_1 + 2^a p^b). \tag{14}$$

If $x_1 < 0$, then there is a positive integer c such that

$$(x_1 - 2^a p^b)(x_1 + 2^a p^b) = -c^2,$$

a contradiction modulo 4. We may thus suppose that $x_1 > 0$, whereby there are positive odd coprime integers c, d and e such that

$$x_1 = c^2, \quad x_1 - 2^a p^b = d^2 \quad \text{and} \quad x_1 + 2^a p^b = e^2 \tag{15}$$

and hence

$$(c - d)(c + d) = 2^a p^b$$

(so that $a \geq 3$). It follows that either

$$c - d = 2 \quad \text{and} \quad c + d = 2^{a-1} p^b \tag{16}$$

or

$$c \pm d = 2^{a-1} \quad \text{and} \quad c \mp d = 2p^b. \tag{17}$$

In the first of these cases,

$$c = 2^{a-2} p^b + 1$$

and so, from the third equation in (15),

$$(2^{a-2} p^b + 1)^2 + 2^a p^b = e^2.$$

Since

$$(2^{a-2} p^b + 1)^2 < (2^{a-2} p^b + 1)^2 + 2^a p^b < (2^{a-2} p^b + 5)^2,$$

it follows, by parity, that

$$(2^{a-2}p^b+1)^2+2^ap^b=(2^{a-2}p^b+3)^2$$

and so

$$2^ap^b=2^ap^b+8,$$

an immediate contradiction.

We thus have (17) and so

$$c=2^{a-2}+p^b.$$

From (15), we have either

$$e-2^{a-2}-p^b=2 \quad \text{and} \quad e+2^{a-2}+p^b=2^{a-1}p^b, \tag{18}$$

or

$$e\pm(2^{a-2}+p^b)=2^{a-1} \quad \text{and} \quad e\mp(2^{a-2}+p^b)=2p^b. \tag{19}$$

In case (18),

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

so that

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

whereby we find the triple $(p,a,x)=(3,3,25)$ (with $b=1$) in (2). On the other hand, if (19) holds, then

$$e=2^{a-2}+p^b=c,$$

contradicting (15).

3.2. Case 2: $\boldsymbol{\alpha>a,\beta>b}$

If $\alpha>a$ and $\beta>b$, again (1) implies that both α and β are even, while (13) yields $a\in\{0,1\}$, $b=1$, and so

$$y_1^2=x_1(2^{\alpha-a}p^{\beta-1}x_1-1)(2^{\alpha-a}p^{\beta-1}x_1+1),$$

for y_1 a positive integer. It follows that $x_1>0$ and so there exist integers c and d with

$$2^{\alpha-a}p^{\beta-1}x_1-1=c^2 \quad \text{and} \quad 2^{\alpha-a}p^{\beta-1}x_1+1=d^2,$$

whereby $d^2-c^2=2$, an immediate contradiction.

3.3. Case 3: $\alpha < a, \beta > b$

Once more α and β are even, whereby $\alpha = 0$, $b = 1$ and hence there is a positive integer y_1 for which

$$y_1^2 = x_1(p^{\beta-1}x_1 - 2^a)(p^{\beta-1}x_1 + 2^a). \tag{20}$$

If $x_1 < 0$, then there necessarily exists an integer c with

$$(p^{\beta-1}x_1 - 2^a)(p^{\beta-1}x_1 + 2^a) = -c^2,$$

a contradiction modulo 4. If, however, $x_1 > 0$, we may find odd positive coprime integers c, d and e for which

$$x_1 = c^2, \quad p^{\beta-1}x_1 - 2^a = d^2 \quad \text{and} \quad p^{\beta-1}x_1 + 2^a = e^2. \tag{21}$$

We thus have

$$(e-d)(e+d) = 2^{a+1}$$

and so

$$d = 2^{a-1} - 1 \quad \text{and} \quad e = 2^{a-1} + 1,$$

whence, from (21) and the fact that $\beta - 1$ is odd,

$$(2^{a-1})^2 - p(p^{(\beta-2)/2}c)^2 = -1. \tag{22}$$

If (u_1, v_1) are the smallest positive integers such that $u_1^2 - pv_1^2 = -1$, then, if we write

$$u_k + v_k\sqrt{p} = (u_1 + v_1\sqrt{p})^k,$$

expanding by the Binomial Theorem yields the expression

$$u_{2j+1} = u_1 \cdot \sum_{i=0}^{j} \binom{2j+1}{2i} u_1^{2(j-i)} v_1^{2i} p^i.$$

Since (22) implies that $p \equiv 1 \pmod 8$, it follows that $\nu_2(u_1) = \nu_2(u_{2j+1})$ for each $j = 0, 1, 2, \ldots$, and thus, from (22), that

$$u_1 = 2^{a-1} \quad \text{and} \quad v_1 = p^{(\beta-2)/2}c.$$

Here $x_1 = c^2$.

If a is even, we can say more. Indeed, if $a = 2k + 2$ is even, then, from (22), we have

$$4 \cdot 2^{4k} + 1 = p(p^{(\beta-2)/2}c)^2$$

and hence one of

$$2^{2k+1} \pm 2^{k+1} + 1 = n^2$$

for some integer n. If $k = 0$, so that $a = 2$, then (22) implies the solution $(p, a, x) = (5, 2, 25)$ to Eq. (1). Otherwise, 2^k exactly divides one of $n - 1$ or $n + 1$, say $n + (-1)^\delta = 2^k \cdot n_1$, where n_1 is an odd positive integer. If $n_1 \geq 3$, then we have

$$n^2 - 1 \geq 3 \cdot 2^k (3 \cdot 2^k - 2) = 2^{2k+1} + 7 \cdot 2^{2k} - 6 \cdot 2^k > 2^{2k+1} + 2^{k+1},$$

a contradiction. We may thus assume that $n_1 = 1$ and so either

$$n^2 - 1 = 2^k (2^k - 2) \quad \text{or} \quad n^2 - 1 = 2^k (2^k + 2).$$

Since

$$2^k (2^k - 2) < 2^{2k+1} - 2^{k+1} + 1,$$

we thus have

$$2^k (2^k + 2) = 2^{2k+1} \pm 2^{k+1}$$

and so

$$2^{k-1} + 1 = 2^k \pm 1,$$

whereby we find that $k = 2$. This leads to the triple $(p, a, x) = (41, 6, 42025)$ in (2). The remaining solutions to (22) correspond to Eq. (6).

3.4. Case 4: $\alpha > a, \beta < b$

Yet again, both α and β are even, so $a \in \{0, 1\}$ and $\beta = 0$. There thus exists a positive integer y_1 such that

$$y_1^2 = x_1 (2^{\alpha - a} x_1 - p^b)(2^{\alpha - a} x_1 + p^b). \tag{23}$$

If $x_1 > 0$, then arguing as previously, we obtain a contradiction modulo 4. We may thus assume $x_1 < 0$ and hence the existence of positive odd coprime integers c, d and e for which

$$x_1 = -c^2, \quad 2^{\alpha - a} x_1 - p^b = -d^2 \quad \text{and} \quad 2^{\alpha - a} x_1 + p^b = e^2. \tag{24}$$

If $a = 0$, then factoring we find that

$$d - 2^{\frac{\alpha}{2}} c = 1, \quad d + 2^{\frac{\alpha}{2}} c = p^b$$

and so

$$d = \frac{p^b + 1}{2} \quad \text{and} \quad 2^\alpha c^2 = \left(\frac{p^b - 1}{2} \right)^2.$$

Substituting these into the final equation of (24), we thus have

$$-p^{2b} + 6p^b - 1 = 4e^2 \geq 4$$

and so $p^b \leq 5$. We check that the only solution with $a = 0$ is thus with $(p, a, x) = (5, 0, -4)$, as in (2).

We now turn our attention to the situation where $a = 1$. In this case, from

$$(d - e)(d + e) = 2^{\alpha} c^2,$$

it follows that there exist positive odd coprime integers f and g such that

$$d \pm e = 2f^2 \quad \text{and} \quad d \mp e = 2^{\alpha-1} g^2,$$

whereby, since $d^2 + e^2 = 2p^b$,

$$f^4 + 2^{2(\alpha-2)} g^4 = p^b. \tag{25}$$

Conversely, a solution to Eq. (25) with f and g odd and coprime and both $\alpha - 1$ and b odd and positive leads to a solution to (23) with $x_1 = -(fg)^2$. Applying Proposition 2.4, we may thus conclude that $b = 1$ in Eq. (25), whereby, since α is even, we are led to (3).

3.5. Case 5: $\alpha = a, \beta < b$

We have $\beta = 0$, $a \in \{0, 1\}$ and so

$$y_1^2 = 2^a x_1 (x_1 - p^b)(x_1 + p^b), \tag{26}$$

for $y_1 \in \mathbb{Z}$. If $a = 0$, then if $x_1 > 0$, we have

$$x_1 = c^2, \quad x_1 - p^b = 2d^2 \quad \text{and} \quad x_1 + p^b = 2e^2,$$

for positive coprime integers c, d and e. Factoring the difference of the second and third equations implies that

$$e - d = 1 \quad \text{and} \quad e + d = p^b,$$

whereby, after a little work,

$$(p^b)^2 - 2c^2 = -1. \tag{27}$$

Applying Proposition 2.3, it follows that $b = 1$ and hence we are led to Eq. (7). Here, $x_1 = c^2$.

If we suppose that $a = 0$, but $x_1 < 0$, then we have

$$x_1 = -c^2, \quad x_1 - p^b = -2d^2 \quad \text{and} \quad x_1 + p^b = 2e^2,$$

for positive coprime integers c, d and e. Adding the second and third equations, we find that $c^2 + e^2 = d^2$ and hence that there exist coprime positive integers f and g such that

$$c = f^2 - g^2, \quad d = f^2 + g^2 \quad \text{and} \quad e = 2fg$$

and so

$$f^4 + 6f^2 g^2 + g^4 = p^b. \tag{28}$$

Conversely, such a solution implies one to (26) with $x_1 = -(f^2 - g^2)^2$. The fact that this equation has no solutions with $b \geq 3$ (and hence that we have a solution to (4)) is an immediate consequence of Proposition 2.4 and the observation that

$$c^4 + (2de)^2 = p^{2b}.$$

Let us next consider the case where $a = 1$. If $x_1 > 0$, from (26) we have that

$$x_1 = c^2, \quad x_1 \pm p^b = 2d^2 \quad \text{and} \quad x_1 \mp p^b = 4e^2$$

for coprime positive c, d and e. We deduce the equalities

$$c - 2e = \pm 1 \quad \text{and} \quad c + 2e = p^b,$$

whereby we find that

$$p^{2b} \pm 6p^b + 1 = 8d^2, \tag{29}$$

with

$$x_1 = \left(\frac{p^b \pm 1}{2}\right)^2.$$

An immediate application of Proposition 2.5 gives, in this case, the desired result.

If $a = 1$ and $x_1 < 0$, then there are positive coprime integers c, d and e with

$$x_1 = -c^2, \quad x_1 - p^b = -2d^2 \quad \text{and} \quad x_1 + p^b = 4e^2, \tag{30}$$

or

$$x_1 = -c^2, \quad x_1 - p^b = -4d^2 \quad \text{and} \quad x_1 + p^b = 2e^2. \tag{31}$$

If we have (30), then $d^2 - c^2 = 2e^2$ and so there exist coprime positive integers f and g with

$$d \pm c = 2f^2 \quad \text{and} \quad d \mp c = 4g^2,$$

whereby

$$c = \pm(f^2 - 2g^2) \quad \text{and} \quad d = f^2 + 2g^2.$$

The fact that $2d^2 - c^2 = p^b$ thus implies that

$$f^4 + 12f^2g^2 + 4g^4 = p^b, \tag{32}$$

with $x_1 = -(f^2 - 2g^2)^2$. This implies

$$c^4 + 2(2de)^2 = p^{2b}$$

and so Proposition 2.4 leads us to conclude that $b = 1$, whereby we have a solution to (5).

Finally, let us suppose that we are in case (31). Then from

$$(2d - c)(2d + c) = p^b,$$

we find that

$$c = \frac{p^b - 1}{2}.$$

Substituting this into the final equation of (31), we thus have

$$-p^{2b} + 6p^b - 1 = 8e^2 \geq 8.$$

It is easy to check that this implies only the solution $(p, a, x) = (3, 1, -2)$ found in (2), again with $b = 1$.

3.6. Case 6: $\alpha = a, \beta > b$

We have that β is even, $b = 1$, $a \in \{0, 1\}$ and so

$$y_1^2 = 2^a x_1 (p^{\beta-1} x_1 - 1)(p^{\beta-1} x_1 + 1),$$

for $y_1 \in \mathbb{Z}$, whereby $x_1 > 0$. Since

$$(p^{\beta-1} x_1 - 1)(p^{\beta-1} x_1 + 1) = 2^a m^2,$$

for some $m \in \mathbb{Z}$, it follows that necessarily $a = 1$, and hence that

$$x_1 = c^2, \quad p^{\beta-1} x_1 \pm 1 = 2d^2 \quad \text{and} \quad p^{\beta-1} x_1 \mp 1 = 4e^2,$$

for c, d and e positive and coprime. We thus have

$$(p^{\beta-1})^2 c^4 - 8(de)^2 = 1. \tag{33}$$

Via Proposition 2.2, it follows that if we define

$$u_k + v_k \sqrt{2} = (3 + 2\sqrt{2})^k,$$

then $p^{\beta-1} c^2 = u_{\alpha(p)}$, where $\alpha(p)$ denotes the rank of apparition of the prime p in this recurrence sequence. Here, $x_1 = c^2$. Since we always have $u_k \equiv 1, 3 \pmod 8$, the same is true for p. If $p \equiv 3 \pmod 8$, then factoring yields the existence of positive integers f and g with f odd, for which

$$p^{\beta-1} c^2 + 1 = 4f^2 \quad \text{and} \quad p^{\beta-1} c^2 - 1 = 2g^2.$$

We thus have that $2f - 1 = (2h + 1)^2$ for some integer h, whence

$$g^2 = 8h^4 + 16h^3 + 16h^2 + 8h + 1.$$

Solving this equation via, say, Magma (see [9]), we find that

$$(|g|, h) \in \{(1, -1), (1, 0), (7, -2), (7, 1)\}.$$

These lead to the solutions $(p, a, x) = (3, 1, 18)$ and $(11, 1, 2178)$ to Eq. (1) (each with $b = 1$), as listed in (2). The cases with $p \equiv 1 \pmod 8$ lead to family (8).

3.7. Case 7: $\alpha < a, \beta = b$

From the fact that $\alpha = 0$, $b = 1$, we deduce the existence of a positive integer y_1 for which

$$y_1^2 = px_1(x_1 - 2^a)(x_1 + 2^a). \tag{34}$$

If $x_1 > 0$, then there are coprime integers c, d and e for which

$$x_1 = c^2, \quad x_1 \pm 2^a = pd^2 \quad \text{and} \quad x_1 \mp 2^a = e^2,$$

whence $c^2 - e^2 = \pm 2^a$ and so $c = 2^{a-2} \pm 1$ (necessarily $a \geq 3$). It follows that either

$$2^{2(a-2)} - 3 \cdot 2^{a-1} + 1 = pd^2, \tag{35}$$

or

$$2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 = pd^2. \tag{36}$$

The latter of these is just Eq. (9); all solutions satisfy

$$x_1 = (2^{a-2} + 1)^2, \quad x = p(2^{a-2} + 1)^2.$$

In case (35), we note the factorizations

$$2^{4k} - 6 \cdot 2^{2k} + 1 = (2^{2k} + 2^{k+1} - 1)(2^{2k} - 2^{k+1} - 1)$$

and

$$2^{4k+2} - 6 \cdot 2^{2k+1} + 1 = (2^{2k+1} + 2^{k+2} + 1)(2^{2k+1} - 2^{k+2} + 1).$$

Since the factors on the right-hand sides of these equations are coprime, and since

$$2^{2k} \pm 2^{k+1} - 1 = (2^k \pm 1)^2 - 2,$$

it follows that a solution to (35) necessarily has a odd, say $a = 2k + 3$ with k positive, and hence either

$$2^{2k+1} + 2^{k+2} + 1 = t^2 \quad \text{or} \quad 2^{2k+1} - 2^{k+2} + 1 = t^2,$$

for t a positive integer. Then 2^{k+1} necessarily divides one of $t \pm 1$. If $t > 1$, it follows that $t \geq 2^{k+1} - 1$ and so

$$2^{2k+1} \pm 2^{k+2} + 1 \geq (2^{k+1} - 1)^2,$$

whereby $k \leq 2$. If $t = 1$, we have $k = 1$. In any case, after a little work, we are led to conclude that the only solutions to (35) are with $a \in \{5, 7\}$, corresponding to $(p, a, x) = (17, 5, 833)$ and $(17, 7, 16337)$ in (2).

If $x_1 < 0$, then we have c, d and e as usual, with

$$x_1 = -c^2, \quad x_1 - 2^a = -p^\delta d^2 \quad \text{and} \quad x_1 + 2^a = p^{1-\delta} e^2,$$

where $\delta \in \{0, 1\}$. If $\delta = 0$, we find that $d^2 - c^2 = 2^a$ and so $c = 2^{a-2} - 1$. Thus

$$-(2^{a-2} - 1)^2 + 2^a = pe^2 \geq 3$$

and hence $3 \leq a \leq 4$. These two possibilities correspond to $(p, a, x) = (7, 3, -7)$ and $(7, 4, -63)$ in (2), respectively. If $\delta = 1$, then from $c^2 + e^2 = 2^a$, it follows that $c = e = a = 1$ and so we obtain the solution $(p, a, x) = (3, 1, -3)$.

3.8. Case 8: $\alpha > a, \beta = b$

As previously, we have α even, $b = 1$, $a \in \{0, 1\}$, and hence a positive integer y_1 with

$$y_1^2 = px_1(2^{\alpha-a}x_1 - 1)(2^{\alpha-a}x_1 + 1),$$

whereby $x_1 > 0$ and hence

$$x_1 = c^2, \quad 2^{\alpha-a}x_1 \pm 1 = pd^2 \quad \text{and} \quad 2^{\alpha-a}x_1 \mp 1 = e^2,$$

for positive c, d and e (so that necessarily $a = 1$). We thus have

$$2^{2(\alpha-1)}c^4 - p(de)^2 = 1, \tag{37}$$

with $x_1 = c^2$. By Proposition 2.1, this implies that $p \in \{3, 7\}$ with corresponding solutions $(2^{\alpha-1}c^2, |de|) = (2, 1)$ and $(8, 3)$, respectively. These lead to the triples $(p, a, x) = (3, 1, 12)$ and $(7, 1, 112)$ found in table (2).

3.9. Case 9: $\alpha = a, \beta = b$

If we have $\alpha = a \in \{0, 1\}$ and $\beta = b = 1$, then there exists an integer y_1 for which

$$2^a\, p\, y_1^2 = x_1^3 - x_1$$

and thus positive integers c and d for which

$$x_1 = c^2 \quad \text{and} \quad x_1^2 - 1 = 2^a pd^2.$$

Thus

$$c^4 - 2^a pd^2 = 1$$

and hence, by Proposition 2.1,

$$(p, a, x) \in \{(5, 0, 45), (3, 1, 294), (29, 0, 284229)\}.$$

4. The Equation $2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 = ps^2$

Our goal in this section is to prove the following result.

Proposition 4.1. *If a, s and p are positive integers for which*

$$2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 = ps^2, \tag{38}$$

with $p > 2$ prime, then either $s = 1$ and (p, a) is one of

$$(17, 3), (41, 4), (113, 5), (353, 6), (1217, 7), (4481, 8), (67073, 10),$$

or $p > 10^6$.

To prove this, we will begin by supposing that there exist positive integers s and a with $a \geq 3$, and a prime p so that Eq. (38) is satisfied. It follows immediately that $p \equiv 17 \pmod{24}$. Further, for such a solution, we have

$$(2^{a-2} + 3)^2 - ps^2 = 8. \tag{39}$$

To our knowledge, there is no especially straightforward characterization of those primes p for which the equation $u^2 - pv^2 = 8$ is solvable in integers u and v. Class group considerations (in particular, if we know whether the ideal lying above 2 in $\mathbb{Q}(\sqrt{p})$ is principal or not) may be used to classify such p, but it is simpler from a computational viewpoint (since we will have need of the data in any case) to observe that if (u, v) is a solution to $u^2-pv^2 = 8$ in positive integers, then u/v is a convergent in the infinite simple continued fraction expansion to $\sqrt{p}$, say $u/v = p_i/q_i$. Since such an expansion is periodic, the values of $p_i^2 - pq_i^2$ lie in a (small) finite set. If this set fails to contain 8 (or, equivalently, -8, since $p \equiv 1 \pmod 8$), then we may exclude p from consideration.

Let us define (U, V) and (m, n) to be the smallest positive integers satisfying

$$U^2 - pV^2 = 1 \quad \text{and} \quad m^2 - pn^2 = 8.$$

It is easy to show that

$$U \equiv 1 \pmod 8 \quad \text{and} \quad V \equiv 0 \pmod 8$$

and moreover that all solutions to $u^2 - pv^2 = 8$ in positive integers u and v satisfy

$$u + v\sqrt{p} = (m \pm n\sqrt{p})(U + V\sqrt{p})^k \tag{40}$$

for some choice of sign and non-negative integer k. It follows that such solutions have $u = u_n, v = v_n$ where u_n and v_n satisfy the recursions

$$u_{n+1} = Uu_n + pVv_n \quad \text{and} \quad v_{n+1} = Vu_n + Uv_n, \tag{41}$$

with initial terms either $(u_1, v_1) = (m, n)$ or $(u_1, v_1) = (m, -n)$. In either case, we may conclude that any solution in positive integers u and v to $u^2 - pv^2 = 8$ necessarily has $u \equiv m \pmod 8$ (and, in many situations, having computed U and V, modulo 2^j for larger values of j). Together with (39), this observation serves to eliminate many possibilities for p. In particular, for $p < 10000$, say, we are left to consider only

$$p = 17, 41, 113, 353, 593, 881, 1217, 1889, 2129, 3089,$$
$$4049, 4481, 5393, 7121, 9137, 9281.$$

Note that the sequence $2^{2(a-2)} + 3 \cdot 2^{a-1} + 1$ is periodic modulo p for each prime (of period $p - 1$ for $p \equiv 1 \pmod 8$). It is thus easy to check to see if a fixed prime p ever divides this sequence. In particular, this serves to eliminate the primes

$$p = 881, 4049, 7121 \text{ and } 9137.$$

For primes that "pass these tests", of which there are precisely 407 up to 10^6 (ranging from 17 to 992561), the situation is more difficult. To begin with, we examine the corresponding values of V more carefully. For each prime $q \mid V$, we necessarily have $U \equiv \pm 1 \pmod q$ and hence, from (41), any solution to $u^2-pv^2 = 8$ has $u \equiv \pm m \pmod q$. From (39), we thus have

$$2^{a-2} \equiv \pm m - 3 \pmod q \tag{42}$$

and even

$$2^{a-2} \equiv m-3 \pmod{q}, \tag{43}$$

if $U \equiv 1 \pmod{q}$.

To illustrate how we can use this information, let us consider the case $q = 5$. First suppose, for a given prime p, we know that

$$V \equiv 0 \pmod{5}, \quad U \equiv 1 \pmod{5} \quad \text{and} \quad m \equiv 3 \pmod{5}.$$

Then it follows from (43) that $2^{a-2} \equiv 0 \pmod{5}$, a contradiction. This serves to eliminate 41 further primes up to $p < 10^6$ (starting with $p = 3089$). Similarly, if we have

$$V \equiv 0 \pmod{5}, \quad U \equiv \pm 1 \pmod{5} \quad \text{and} \quad m \equiv \pm 3 \pmod{5}$$

(the latter two conditions being a consequence of the first congruence for $p \equiv \pm 1 \pmod{5}$), then we deduce that $2^{a-2} \equiv 4 \pmod{5}$ and so $a \equiv 0 \pmod{4}$. In many cases, the fact that

$$2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 \equiv 0 \pmod{p}$$

then leads to a contradiction. For example, if $p = 1889$, the latter congruence implies that

$$a \equiv 173, 303, 645, 775, 1117, 1247, 1589, 1719 \pmod{1888}.$$

Up to 10^6, this argument enables us to eliminate 95 more primes. Analogously, if $5 \mid V$ and $m \equiv \pm 0 \pmod{5}$ or $m \equiv \pm 1 \pmod{5}$, then we have $a \equiv 3 \pmod{4}$ and $a \equiv 1, 2 \pmod{4}$, respectively. These facts take care of 10 and 7 more primes up to 10^6, respectively.

Often, we must work rather harder. For instance, in case $p = 593$, we observe that V is a multiple of 4933, while $U \equiv -1 \pmod{4933}$. From (39), (41) and the fact that $m = 32899$, we thus have

$$2^{a-2} \equiv 1629, 3298 \pmod{4933}$$

and so $a \equiv 2605, 3052 \pmod{4932}$. On the other hand, considering the sequence $2^{2(a-2)} + 3 \cdot 2^{a-1} + 1$ modulo 593 implies that

$$a \equiv 18, 134, 166, 282, 314, 430, 462, 578 \pmod{592}$$

and in particular, that $a \equiv 2 \pmod{4}$, again a contradiction. Similar arguments, combining the knowledge of $2^{2(a-2)} + 3 \cdot 2^{a-1} + 1$ modulo p with information derived from $q \mid V$, for relatively small q, enables us to eliminate all but the following possibilities for p:

$$\begin{gathered} 17, 41, 113, 353, 1217, 4481, 5393, 23873, 67073, \\ 91121, 98849, 126257, 162017, 176417, 303377, \\ 377537, 444449, 620561, 682673, 708497, 873617. \end{gathered} \tag{44}$$

The primes 17, 41, 113, 353, 1217, 4481 and 67073 are each of the form $2^{2(a-2)} + 3 \cdot 2^{a-1} + 1$ for suitable choice of a. For the remaining values of p, either the factorization of the corresponding V or the discrete logarithm problem modulo q is computationally intensive. In any case, for p in (44), we will apply lower bounds for linear forms in logarithms. Writing $\alpha = U + V\sqrt{p}$ and $\beta = m \pm n\sqrt{p}$, from (39) and (40) we have

$$2^{a-1} - \beta\alpha^k = \bar{\beta}\alpha^{-k} - 6,$$

and so

$$\Lambda := |k \log \alpha + \log \beta - (a-1) \log 2| < 3 \cdot 2^{-a+2}. \tag{45}$$

Applying Theorem 2 of Matveev [20], we have that

$$\log \Lambda > -10^{15} \log \alpha \, \log(m + n\sqrt{p}) \, \log((a-1)e), \tag{46}$$

which provides an almost immediate upper bound upon a. A routine application of the lemma of Baker–Davenport [1] treats the remaining values of a.

For prime p in (44), in order to complete the proof of Proposition 4.1, we begin by noting that we have

p	U	V	m	n
17	33	8	5	1
41	2049	320	7	1

For larger values of p in (44), m/n is necessarily a convergent in the infinite simple continued fraction expansion to $\sqrt{p}$, say p_i/q_i, where $U/V = p_j/q_j$ for some $j > i$. We have

p	i	j	p	i	j	p	i	j
113	2	18	91121	34	618	444449	96	1106
353	2	30	98849	18	670	620561	146	818
1217	2	42	126257	48	338	682673	286	734
4481	2	54	162017	66	514	708497	412	894
5593	28	70	176417	66	282	873617	358	894
23873	12	126	303377	80	474			
67073	2	78	377537	272	638			

In general, since we also have that $p_{j-i}^2 - pq_{j-i}^2 = 8$, it follows that $j \geq 2i$. For the values of p in (44), combining inequalities (45) and (46) yields, in every case, an upper bound of the shape $a < 10^{23}$.

5. Calculations and Speculations

Let us denote by $S_3, S_4, \ldots, S_{10}$ the sets of odd primes p satisfying equations of the shape (3), (4), ..., (10), respectively. Further, define $S_{k,N}$ to be the cardinality of

$S_k \cap [1, N]$. Then we have

k	$S_{k,10^4}$	$S_{k,10^6}$	$S_{k,10^8}$	$S_{k,10^{10}}$	$S_{k,10^{12}}$	$S_{k,10^{14}}$	$S_{k,10^{16}}$
3	13	89	611	4915	40590	341872	2966902
4	8	64	453	3481	28525	242469	2097454
5	15	92	640	4949	40698	342349	2965304
6	2	3	3	3	3	3	3
7	3	3	4	4	5	5	5
8	2	3	3	3	3	3	3
9	6	7	10	10	11	11	11
10	6	7	8	8	8	9	9

We suspect that $S_6 = \{17, 257, 65537\}$ and $S_8 = \{17, 577, 665857\}$; they are both likely finite. Obviously, S_6 contains any hitherto unknown Fermat primes. Does it include any non-Fermat primes? For each other choice of k, we would expect S_k to be infinite, though this is not, to our knowledge, currently provable in any case. Certainly S_3, S_4 and S_5 are believed to be infinite, though current sieve technology is not quite advanced enough to demonstrate this (but see [14]). A reasonable generalization of standard heuristics, modeled on the arguments of Bateman and Horn [2], suggests that

$$\sum_{p \in S_k \cap [1,N]} \log p \sim \frac{\Gamma(5/4)^2}{\sqrt{\pi}} C N^{1/2},$$

for $k = 3$ and $k = 5$, while

$$\sum_{p \in S_4 \cap [1,N]} \log p \sim \frac{\Gamma(5/4)^2}{\sqrt{2\pi}} C N^{1/2},$$

where

$$C = \prod_{p \equiv 1 \pmod 8} \left(1 - \frac{3}{p}\right) \prod_{p \equiv 3,5,7 \pmod 8} \left(1 + \frac{1}{p}\right).$$

The corresponding contribution from S_k for $6 \le k \le 10$ are, with some effort, of (provably) lower order.

It is worth observing that the elements of S_9 corresponding to solutions to (9) with $s = 1$ form a subset of $S_4 \cup S_5$. Indeed, if a prime p can be written as $p = 2^{2(a-2)} + 3 \cdot 2^{a-1} + 1$, then, if $a = 2j$ is even, we have that p satisfies (4) with $r = 2^{j-1}$ and $s = 1$. Similarly, if $a = 2j+1$ is odd, p satisfies (5) with $r = 1$ and $s = 2^{j-1}$. We know of no members of S_9 for which $s > 1$. On a related note, if $p = (2^{a-1})^2 + 1$ (i.e. if p satisfies (6) with $s = 1$), then p also satisfies (3) with $r = 2^{(a-1)/2}$ and $s = 1$.

Let us present a heuristic argument that $S_8 = \{17, 577, 665857\}$. We have, defining

$$U_k + V_k \sqrt{2} = (3 + 2\sqrt{2})^k,$$

that $pr^2 = U_{\omega(p)}$. Notice first that standard density arguments suggest (much as for Fermat primes) that the number of primes of the form U_{2^α} is finite; indeed, we expect that it is just the set $3, 17, 577$ and 665857. Similarly, we believe that the set of integers of the form pr^2 in the sequence U_{2^α} is also just $\{3, 17, 577, 665857\}$. Under this hypothesis, we claim that any primes p for which $p \equiv 1 \pmod 4$, with (8) solvable also have $\omega(p) = 2^\alpha$ for some integer α. If this is not the case, we can find a prime $p \equiv 1 \pmod 4$ for which (8) has a solution, and with the property that $\omega(p)$ is divisible by an odd prime factor, say q, and is minimal in this respect. Then, we have, writing $U = U_{\omega(p)/q}$, that

$$pr^2 = U\left(U^{q-1} + \binom{q}{2}U^{q-3}(U^2-1) + \cdots + q(U^2-1)^{(q-1)/2}\right),$$

whereby

$$\gcd(U, pr^2/U) \in \{1, q\}.$$

In the first case, since the definition of $\omega(p)$ precludes the possibility $p \mid U$, it follows that there exists an integer t such that $U = t^2$, whereby

$$t^4 - 2V_{\omega(p)/q}^2 = 1.$$

This equation is easily shown (via Magma, say) to have no solutions in positive integers. It follows that $\gcd(U, pr^2/U) = q$ and hence, since p fails to divide U, there exists a positive integer t such that $U = qt^2$, whence

$$q^2t^4 - 2V_{\omega(p)/q}^2 = 1.$$

From the minimality of $\omega(p)$, we may conclude that either $q \equiv 3 \pmod 4$ or that $\omega(p)/q = 2^\alpha$ for some non-negative integer α. In the first case, the arguments of Case 6 of Sec. 3 imply that either $(q, t, \omega(p)/q) = (3, 1, 1)$ or $(11, 3, 3)$. We therefore have $\omega(p) = 3$ or 33; in neither case is $U_{\omega(p)}$ of the shape pr^2 for $p \equiv 1 \pmod 4$ (U_{33} is divisible by 43, but not by 43^2).

We thus have $\omega(p) = q \cdot 2^\alpha$ and hence, from our assumptions,

$$\omega(p) \in \{2 \cdot 17, 4 \cdot 577, 8 \cdot 665857\}.$$

Note that

$$U_{34} = 17^2 \cdot 25841 \cdot 7153349567063158273.$$

Similarly, we find that U_{2308} is divisible by 609313, but not by 609313^2, and that $U_{2308}/609313$ is not a square. We expect that $U_{5326856}$ is not of the required form either, but are unable to verify this, since the corresponding computation is somewhat more involved (primarily since $U_{5326856}$ has more than 4 million decimal digits).

6. Intersections

Many of the families $(3), (4), \ldots, (10)$ are disjoint, or close to it. In particular, it is not especially difficult to show that

$$S_3 \cap S_4 = S_4 \cap S_5 = S_7 \cap S_8 = \emptyset, \quad S_7 \cap S_{10} = \{7\} \quad \text{and} \quad S_3 \cap S_5 = \{17\}.$$

To see that $S_3 \cap S_4 = \emptyset$, observe that we have

$$r^4 + 6r^2s^2 + s^4 = (r^2+s^2)^2 + (2rs)^2$$

and so if

$$p = r_1^4 + 96r_1^2s_1^2 + 256s_1^4 = r_2^4 + 16s_2^4,$$

say, then

$$r_1^2 + 16s_1^2 = r_2^2 \quad \text{and} \quad 8r_1s_1 = 4s_2^2.$$

There thus exist integers r_3 and s_3 such that

$$r_1 = r_3^2 \quad \text{and} \quad s_1 = 2s_3^2,$$

whence

$$r_3^4 + 64s_3^4 = r_2^2.$$

An easy descent argument shows that this equation (which corresponds to the elliptic curve

$$Y^2 = X^3 - 256X$$

of rank 0) has no solutions in non-zero integers r_3, s_3 and r_2.

An even simpler argument shows that $S_7 \cap S_{10} = \{7\}$. Suppose that we have both

$$p^2 - 2s^2 = -1 \quad \text{and} \quad p^2 \pm 6p + 1 = 8r^2,$$

where $r \geq 1$ and $s \geq 5$ are integers. Then $\pm 3p = 4r^2 - s^2$, so that one of the following cases occurs:

$$\begin{cases} 2r - s = 1 \text{ and } 2r + s = 3p, \text{ or} \\ 2r - s = 3 \text{ and } 2r + s = p, \text{ or} \\ 2r - s = -1 \text{ and } 2r + s = 3p, \text{ or} \\ 2r - s = -3 \text{ and } 2r + s = p. \end{cases} \tag{47}$$

In the first instance, we have $s = (3p-1)/2$ and so

$$p^2 - 2((3p-1)/2)^2 = -1,$$

a contradiction modulo 4. In the second, $p = 2s + 3$, so

$$(2s+3)^2 - 2s^2 = -1$$

whereby $s = -1$ or $s = -5$, contradicting $s \geq 5$. The third leads to

$$p^2 - 2((3p+1)/2)^2 = -1,$$

yet another contradiction, while the fourth gives

$$(2s-3)^2 - 2s^2 = -1$$

and so $s = 5$, $p = 7$ and $r = 1$, whereby $S_7 \cap S_{10} = \{7\}$.

If $S_7 \cap S_8 \neq \emptyset$, then, writing $t_n + u_n\sqrt{2} = (1+\sqrt{2})^n$, it follows that p divides t_n (with n odd) and some t_{2m}. Thus p divides u_{2n} and u_{4m}, and hence $u_{\gcd(2n,4m)}$. Since $\{u_n\}$ is a divisibility sequence, $u_{\gcd(2n,4m)}$ divides u_{2m}, whereby p divides both u_{2m} and t_{2m}, an immediate contradiction.

To show that $S_4 \cap S_5 = \emptyset$ and $S_3 \cap S_5 = \{17\}$ requires rather more work. A nice proof of the latter statement was given by Hoelscher [17]; one shows that if

$$x^4 + y^4 = u^4 + 12u^2v^2 + 4v^4 = p$$

is prime, then we necessarily have

$$\frac{u + (2+\sqrt{2})iv}{x + y\zeta_8} = (1+\sqrt{2})^a \zeta_8^b,$$

for ζ_8 a primitive eighth root of unity. The case $b \equiv 3 \pmod 4$ leads to $p = 17$, while all others yield contradictions. An exactly analogous argument (still working in $\mathbb{Q}(\zeta_8)$) shows that $S_4 \cap S_5 = \emptyset$.

Acknowledgments

The author would like to thank Gary Walsh and Maurice Mignotte for numerous insightful comments. This research was supported in part by a grant from NSERC.

References

[1] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Q. J. Math. (2)* **20** (1969) 129–137.

[2] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962) 363–367.

[3] M. A. Bennett, S. Dahmen, M. Mignotte and S. Siksek, Shifted powers in binary recurrence sequences, preprint.

[4] M. A. Bennett, J. Ellenberg and N. Ng, The Diophantine equation $A^4 + 2^\delta B^2 = C^n$, *Int. J. Number Theory* **6** (2010) 311–338.

[5] M. A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* **56**(1) (2004) 23–54.

[6] M. A. Bennett and P. G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, *Proc. Amer. Math. Soc.* **127** (1999) 3481–3491.

[7] B. J. Birch, Diophantine analysis and modular functions, in *International Colloquium on Algebraic Geometry*, Tata Institute Studies in Mathematics, Vol. 4 (Oxford University Press, London, 1968), pp. 35–42.

[8] ———, Elliptic curves and modular functions, in *Symposia Mathematica*, Indam Rome 1968/1969, Vol. 4 (Academic Press, London, 1970), pp. 27–32.

[9] W. Bosma *et al.*, *Magma* computer algebra system (2005); http://magma.maths.usyd.edu.au/.

[10] K. Draziotis, Integral solutions of the equation $Y^2 = X^3 \pm p^k X$, *Math. Comp.* **75** (2006) 1493–1506.

[11] K. Draziotis and D. Poulakis, Practical solution of the Diophantine equation $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$, *Math. Comp.* **75** (2006) 1585–1593.

[12] ______, Solving the Diophantine equation $y^2 = x(x^2 - n^2)$, *J. Number Theory* **129** (2009) 102–121.

[13] J. Ellenberg, Galois representations attached to Q-curves and the generalized Fermat equation $A^4 + B^2 = C^p$, *Amer. J. Math.* **126**(4) (2004) 763–787.

[14] J. Friedlander and H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Ann. Math.* **148** (1998) 945–1040.

[15] Y. Fujita and N. Terai, Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$, *Tokyo Math. J.* **34** (2011) 367–381.

[16] K. Heegner, Diophantische analysis und modulfunktionen, *Math. Z.* **56** (1952) 227–253.

[17] J. L. Hoelscher, 2008 Western Number Theory Conference problems, (2008); http://www.math.byu.edu/doud/WNTC/problems2008.pdf.

[18] A. W. Knapp, *Elliptic Curves*, Mathematical Notes, Vol. 40 (Princeton University Press, Princeton, NJ, 1992).

[19] W. Ljunggren, The Diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, *J. London Math. Soc.* **41** (1966) 542–544.

[20] E. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II, *Izv. Math.* **64** (2000) 1217–1269.

[21] P. Monsky, Mock Heegner points and congruent numbers, *Math. Z.* **204** (1990) 45–68.

[22] L. J. Mordell, The Diophantine equation $y^2 = Dx^4 + 1$, *J. London Math. Soc.* **39** (1964) 161–164.

[23] ______, The Diophantine equation $y^2 = Dx^4 + 1$, in *1970 Number Theory* (János Bolyai Mathematical Society, Debrecen, 1968), pp. 141–145.

[24] P. Samuel, Résultats élémentaires sur certaines équations diophantiennes, *J. Théorie Nombres Bordeaux* **14** (2002) 629–646.

[25] B. Spearman, Elliptic curves $y^2 = x^3 - px$ of rank two, *Math. J. Okayama Univ.* **49** (2007) 183–184.

[26] P. G. Walsh, The integer solutions to $y^2 = x^3 \pm p^k x$, *Rocky Mountain J. Math.* **38** (2008) 1285–1301.

[27] ______, Maximal ranks and integer points on a family of elliptic curves, *Glas. Math. Ser III* **44** (2009) 83–87.

[28] ______, Maximal ranks and integer points on a family of elliptic curves II, *Rocky Mountain J. Math.* **41** (2011) 311–317.