Open Problems Column
Edited by William Gasarch

This Issues Column! This issue's Open Problem Column is by P.G. Walsh and is *Integral Points on Elliptic Curves: A Journey into Speculative Number Theory.*

Request for Columns! I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere inbetween, and (2) really important or really unimportant or anywhere inbetween.

Integral Points on Elliptic Curves: A Journey into Speculative Number Theory

P.G. Walsh
University of Ottawa

December 13, 2023

1 Introduction

The subject of elliptic curves is as old and rich as mathematics itself, going back almost 2000 years to the work of Diophantus. Moreover, as a topic of study, it may be among the leaders for the most number of connections to different areas within mathematics and computer science. Notable among these are elliptic curve cryptography, and the proof of Fermat's Last Theorem, however elliptic curves have shown up in many other modern topics, such as random number generators, primality testing, and even post quantum cryptography.

In this article, we turn our attention to the Diophantine nature of elliptic curves. The problem of finding all integer points on an elliptic curve has seen enormous progress over the past fifty or so years, due in large part by the Fields medal winning work of Baker [3], which reduced the problem to a finite search. Since Baker's work, numerous fundamental improvements in both transcendental number theory and Diophantine approximation, along with implementations in computational packages, such as pari, magma and sage, have made it possible to enumerate all integer points on a curve whose coefficients are not too large. Despite all of this progress, many questions concerning integer points on elliptic curves remain completely unsolved.

Simply put, an elliptic curve is a curve of the form

$$y^2 = x^3 + ax + b, \tag{1.1}$$

where a and b are integers. In this article, we will focus entirely on the case that $b = 0$ and $a = -n$ a negative integer, so that the equation becomes

$$y^2 = x^3 - nx. \tag{1.2}$$

The choice of having a negative integer as the coefficient is somewhat arbitrary, as much of what will be discussed can also be done with a positive coefficient.

The type of problems we pursue here include describing the set of integral points on elliptic curves, and as a byproduct, we will be able to derive a heuristic for an upper bound on the number of integral points on a curve. Such bounds were proved by the author [20], and improved by Akhtari [1]. The upper bounds given in those papers include a dependence on various quantities related to the given curve, however it is surely the case that some of the quantities appearing in those upper bounds appear primarily because of the method used. Our computations show that the actual upper bounds depend almost exclusively on the number of prime factors of n.

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ be the factorization of n into primes. Our computations indicate that the number of integral points on (1.2) is highly influenced by the size of t, in that, as t is allowed to get larger, one can find curves with more integral points, although a precise relation between t and the maximal number of integral points, should there be a maximum, eludes us. The current record we have found is the curve having 89 integral points with $n = 3129357$, an integer which is a product of 6 primes. This large number of integral points is related to the large number of associated quartic diophantine equations that are connected to the elliptic curve, a matter that we will see more of in subsequent sections. As the number of such equations is so large, the analysis is extremely cumbersome, and so for the purpose of this article, we will focus only on the case $t = 2$. We point out that the case $t = 1$ has been covered in previous work of this author [21]. We will see that, even for the case $t = 2$, there are numerous cases to consider, and also, that these cases have connections to various well known and popular topics in number theory. We note that the case of n being even was solved completely in a paper by Bennett [4], wherein it was proved that for $n = 2^a p^b$, and p outside a small and explicit finite set, integral points on (1.2) must have $b = 1$. For the remainder of this article, it will be assumed that n has exactly two distinct odd prime factors p and q.

Consequently, this article will be an in depth study of the set of integral points on elliptic curves given by

$$y^2 = x^3 - p^a q^b x, \tag{1.3}$$

where p and q are odd primes. In particular, each pair of positive integers (a, b) will be considered in detail. Though it may not be apparent, covering all such pairs of positive integers will turn out to be a finite process.

Although this article will focus entirely on the dependence on a and b, the number of integral points on the curve does seem to have some dependence on p and q. In particular, for a fixed pair of positive integers a and b, the number of integral points on the curve typically decreases as p and q get large.

It is worth pointing out here that the status of solving the problem of determining the set of integral points on an elliptic curve has seen extraordinary

progress over the past fifty or so years, both in theoretical advances, and in computation. This progress can be viewed as the resolution of Hilbert's tenth problem for elliptic curves in that, given a curve, theoretical advances have allowed for the determination of an upper bound for the size of the coefficients of any integral point, and computational methods combined with implementations in various packages, such as pari, magma, and sage, are able to give a complete list of the integral points with absolute value below that upper bound. The reader is referred to the excellent survey by Gasarch [10] for more on Hilbert's tenth problem and its connections.

Regarding our computations performed on the problems we state, these were primarily done on one node on a pc using magma for varying lengths of time. Some of the problems involved searches of one to three days, but all were quite moderate, and certainly never lasting more than a week (the reader can download our program from https://mysite.science.uottawa.ca/gwalsh/ecprog.txt).

Finally, depending on the context, most of the open problems in this article are phrased in such a way as to suggest what we believe to be the truth (based on our computations), and thus, can also be viewed as conjectures.

2 Primitivity

Integer points on an elliptic curve given by (1.3), with $\max(a, b) \geq 4$, often arise as points derived from points on curves with smaller values of a and b.

Definition Let (x, y) be an integral point on E given by $y^2 = x^3 - p^a q^b x$. If $a \geq 4$ and p^2 divides x, or $b \geq 4$ and q^2 divides x, then (x, y) is an **imprimitive** point on E. Otherwise, (x, y) is a **primitive** point on E.

To see why such a condition is valuable in tracking integral points, suppose that $x = p^2 x_1$ is the x coordinate of a point on a curve $y^2 = x^3 - p^a q^b x$ for which $a \geq 4$. Then p^6 divides the right side of the equation, forcing p^3 to divide y. If $y = p^3 y_1$, then it is easy to verify that (x_1, y_1) satisfies $y_1^2 = x_1^3 - p^{a-4} q^b x_1$.

The notion of primitivity gives a glimpse as to the reason the process of tracking integral points, as a and b get large, is finite. We will see that a combination of some big theorems in number theory, along with the profound ABC conjecture, show that once a and b do become large, all integral points on (1.3) are imprimitive.

3 Small Values of a and b

In the sections below we will give specific details on the set of primitive integral points, and state open problems related to the number of such points. The

amount of detailed analysis we provide will subside as we move from case to case, as the analyses differ only slightly from one case to the next.

3.1 $a = b = 1$

The curve of interest is given by

$$E: \ y^2 = x^3 - pqx, \tag{3.1.1}$$

with p and q distinct odd primes. Let us assume that (x, y) is an integral point on E with $x \neq 0$, $y \geq 0$, and assume that x factors as $x = du^2$ with d a squarefree integer and u a positive integer. As $y^2 = x^3 - pqx = (du^2)(d^2u^4 - pq)$, and d is squarefree, it follows that d divides y, and also that u divides y/d. In particular, if we let $v = y/(du)$, then dividing by du^2 gives

$$dv^2 = d^2u^4 - pq, \tag{3.1.2}$$

and we see that d is necessarily a divisor of pq. Therefore, d must be in the set $\{\pm 1, \pm p, \pm q, \pm pq\}$. We will examine each of these possibilities individually, and deduce the resulting quartic equation that arises in each case.

3.1.1 $d = 1$. In this case, (3.1.2) is the quartic equation $v^2 = u^4 - pq$, which is the same as $u^4 - v^2 = pq$, and as the left side of this equation naturally factors, we may rewrite it as

$$(u^2 - v)(u^2 + v) = pq. \tag{3.1.3}$$

The sum of the two factors on the left side of (3.1.3) is evidently positive, and so each factor appearing therein must also be positive. We deduce that either

$$u^2 - v = p, u^2 + v = q \ \text{ or } \ u^2 - v = 1, u^2 + v = pq,$$

which respectively imply that

$$2u^2 = p + q \ \text{ or } \ 2u^2 = pq + 1,$$

or equivalently, $u = ((p + q)/2)^{1/2}$ and $u = ((pq + 1)/2)^{1/2}$. In particular, it is easily determined if integral points arise for this case, and if they do exist, they can be given explicitly. It is worth noting that there are examples of pairs (p, q) for which integral points on E of both kind described above exist. We invite the reader to verify this for (p, q) equal to either $(7, 193)$ or $(73, 89)$. It is worth pointing out here that Goldbach's Conjecture implies that there are infinitely many pairs of primes (p, q) for which a nonzero integral point exists on the curve (3.1.1).

3.1.2 $d = -1$. In this case, (3.1.2) becomes $u^4 + v^2 = pq$, and an integral point on E corresponds to such a sum with either summand being a fourth power. From the arithmetic in the Gaussian integers, pq is a sum of two squares only

if both p and q are primes that split in the Gaussian integers, i.e. that they are both 1 modulo 4. Furthermore, it is a simple matter to prove that the product of two primes can only have two representations as a sum of two squares. Therefore, there are at most four summands that can give rise to an integral point on E, and thus, there can be at most four points on E with x coordinate having $d = -1$, and explicitly determining these points can be achieved by factoring p and q in the Gaussian integers. We point out that there is an example of (p, q) for which three points on E occur in this way. Namely, with $(p, q) = (73, 89)$, three points (x, y) on E have the property that $x = -u^2$ because of the representations of $73 \cdot 89 = 4^4 + 79^2 = 7^4 + 8^4$.

The above cases were elementary to deal with. Things change quite drastically as we move on to other cases. The diophantine equations that arise involve various types of quartic equations which have been considered by numerous authors, using methods from transcendental number theory, diophantine approximation and algebraic number theory, and the current state-of-the-art remains quite far from what the observed truth seems to be. Our primary goal is to exhibit what the truth is on these problems by way of computational evidence, along with theoretical justification when applicable.

3.1.3 $d = p$. In this case, after division by p, (3.1.2) can be written as

$$v^2 - pu^4 = -q.$$

Upper bounds for the number of solutions to quartic equations were given by the author [20], although the bounds that are given there depend on p and q, and are far from the observed truth. Along those lines, appealing to the overall gist in a separate paper by the author [22], we expect an absolute upper bound of no more than 4 for the number of positive integer solutions to any equation of this type having the right hand side being prime. In fact, one can easily verify that three positive integral solutions (u, v) exist for the cases $(p, q) = (11, 7), (3, 47), (5, 149)$ and $(83, 79)$. We forego a detailed analysis in favour of a summary of what we observe concerning the number of integral points. The interested reader may wish to delve further using the references given above. This brings us to our first open problem.

Open Problem 1. Is there a maximal number of positive integer solutions (x, y) to a quartic equation of the form $x^2 - py^4 = -q$, where the maximum is taken over all pairs of distinct odd primes p and q, and if so, what is that maximum? In particular, is there a pair of distinct prime p, q for which this equation has more than 3 positive integer solutions (x, y)?

3.1.4 $d = -p$. In this case, after division by p, (3.1.2) can be written as

$$v^2 + pu^4 = q,$$

which evidently has a much lower chance of solvability than the previous case. Our computations have failed to find a single pair (p, q) for which 2 positive

integer solutions (x, y) exist, which leads us to our second open problem.

Open Problem 2. For any pair of distinct odd primes p, q, does the equation $x^2 + py^4 = q$ have at most 1 solution in positive integers x and y?

3.1.5 $d = pq$. In this case, after division by p, (3.1.2) can be written as

$$v^2 - pqu^4 = -1,$$

which is an equation that has been extensively studied in the literature. In particular, it was shown by Chen and Voutier [7] that, for $d \geq 3$, the general equation $X^2 - dY^4 = -1$ has at most one solution in positive integers. They showed also that if a solution (X, Y) does exist, then $X + Y^2\sqrt{d}$ is the fundamental unit in the quadratic field $\mathbb{Q}[\sqrt{d}]$, which is an important concept in computational number theory. As for the equation we are considering, we see that there is an upper bound of one positive integer solution for this case.

3.1.6 $d = -pq$. The last case to consider, $d = -pq$, leads to the equation $v^2 + pqu^4 = 1$, which clearly cannot have any positive integer solutions.

We now pull all of these cases together into one statement regarding the number of integral points on any elliptic curve of the form (3.1.1) in the following.

Open Problem 3. Let p and q denote distinct odd primes, and let E be the elliptic curve given by the equation $y^2 = x^3 - pqx$. Determine an upper bound for the number of integral points on E which is independent of p and q.

Toward this problem, we summarize our findings by adding up the various bounds for each of the cases, noting that for the two middle cases, one must swap p and q, giving a total of (conjecturally) at most 15 integral points with nonzero coordinates for any curve given by (3.1.1).

The current record holder for the case $a = b = 1$ is $(p, q) = (73, 89)$, with a total of 8 integral points with nonzero coordinates; 2 with $d = 1$, 3 with $d = -1$, 1 with $d = 73$, 1 with $d = -73$, and 1 with $d = 89$.

3.2 $a = 2, b = 1$

For these values of a and b the curve of interest becomes

$$E: \quad y^2 = x^3 - p^2qx, \tag{3.2.1}$$

where as before, p and q are distinct odd primes. As before, we assume that (x, y) is an integral point E with $x \neq 0$, and let $x = du^2$ with d a squarefree

integer. In this case, with $v = y/(du)$, (3.1.2) becomes

$$dv^2 = d^2u^4 - p^2q, \tag{3.2.2}$$

and so d is therefore a divisor of p^2q. It follows that d is in the set

$$\{\pm 1, \pm p, \pm q, \pm p^2, \pm pq, \pm p^2q\},$$

giving rise to the twelve equations, which we have listed in the following table, along with their respective upper bounds for the number of integral points arising for each case. The two with an asterisk are conjectural. A detailed discussion on the upper bounds follows the table.

d	Equation	Maximum
1	$u^4 - v^2 = p^2q$	2
-1	$u^4 + v^2 = p^2q$	4
p	$u^4 - pv_1^2 = q$	3^*
$-p$	$u^4 + pv_1^2 = q$	1^*
q	$v_1^2 - (u_1^2q)^2q = -1$	1
$-q$	$-v_1^2 - (u_1^2q)^2q = -1$	0
pq	$qu^4 - pv_1^2 = 1$	2
$-pq$	$qu^4 + pv_1^2 = 1$	0
p^2	$u^4 - v^2 = q$	1
$-p^2$	$u^4 + v^2 = q$	1
p^2q	$v^2 - p^2qu^4 = -1$	1
$-p^2q$	$-v^2 - p^2qu^4 = -1$	0

We briefly discuss each of these cases, although it is clear that cases 6, 8 and 12 are not solvable. The first two cases were covered in the previous subsection, and can give rise to at most 2 and 4 points on E respectively. We defer the unsolved cases 3 and 4 to the end of this analysis. Case 5 (and 11) is an equation of the form $X^2 - dY^4 = -1$, which we have already seen can have at most 1 solution by the theorem of Chen and Voutier. Case 7 is covered by a fairly recent result of Akhtari [2], who proved that any equation of the form $aX^4 - bY^2 = 1$ has at most 2 positive integer solutions. Case 9 is clearly only possible if q is of the form $2u^2 - 1$, and can contribute at most 1 point. Case 10 can contribute at most 2 points, and this occurs when q is a sum of 2 fourth powers.

This only leaves cases 3 and 4 to consider, which are analogous to the unsolved problems in the previous subsection. Our computations have failed to find a pair (p, q) with more than 3 positive integer solutions to the equation $X^4 - pY^2 = q$, and more than 1 such solution to the equation $X^4 + pY^2 = q$. This leads us to our next set of open problems.

Open Problem 4 Is there a pair of distinct odd primes p and q for which either the equation $X^4 - pY^2 = q$ has more than 3 positive integer solutions, or the equation $X^4 + pY^2 = q$ has more than 1 positive integer solution?

On the basis of upper bounds of 3 and 1 solution respectively for the equations in Open Problem 4, we can collect the contribution from all of the equations listed above in order to state the main open problem for this subsection. The derived upper bound from these equations is 18 integral points.

Open Problem 5 Prove an absolute upper bound for the number of integer points on any elliptic curve given by an equation of the form $y^2 = x^3 - p^2qx$, which is independent of p and q, where p and q are distinct odd primes.

The record holder for this case is $E: \ y^2 = x^3 - 3^2 \cdot 13x$, which has 10 integral points.

3.3 $a = t, b = 1$

Before moving on to the case $\max(a, b) \geq 2$, we point out that for any $t \geq 1$, one can heuristically produce primes (p, q) for which the curve $y^2 = x^3 - p^tqx$ contains a nonzero integral point with $x = u^2$ for some integer u. To see this, as described in 3.1.1 above, one needs to solve an equation of the form

$$2u^2 = p^t + q$$

in integers u, v, p^t, q with p and q prime. One way to do so is simply to begin by choosing any odd prime power p^t, let $u_0 = \lfloor p^t \rfloor$, and test $2(u_0 + i)^2 - p^t$ for primality for $i \geq 1$.

Despite the fact that one can construct primitive integral points on curves with t large, our computations show that for fixed p and q, there is some positive t_0 for which all curves $y^2 = x^3 - p^tqx$, with $t > t_0$, do not contain primitive integral points. The following is an equivalent formulation.

Open Problem 5a. Let p and q be distinct odd primes, and for $t \geq 1$, let S_t denote the set of primitive integral points on $y^2 = x^3 - p^tqx$. There is an absolute constant $c > 0$, independent of p and q, for which $|\cup_t S_t| < c$.

The value of c in the above open problem may in fact be as small as 11. The pair of primes $(p, q) = (3, 13)$ is currently the record holder with at least this value, as we have failed to find a pair of primes for which the value of c is at least 12.

3.4 $(a, b) = (2, t)$ and $(a, b) = (3, 3)$

We expect by now that the reader can see how one can go through an analysis for each possible pair of fixed positive integers a and b, and so we will forego the details that have been given for the first two cases above. Our computations indicate that the number of integral points starts to decrease quite noticeably as a and b begin to grow.

For $(a, b) = (2, 2)$, the curve $y^2 = x^3 - 7^2 \cdot 23^2 x$ was the only curve found which has 7 integral points. For $(a, b) = (3, 2)$, the curve $y^2 = x^3 - 5^3 \cdot 11^2 x$ was the only curve found containing 6 integral points. For $(a, b) = (3, 3)$, the curves $y^2 = x^3 - 3^3 \cdot 73^3 x$ and $y^2 = x^3 - 5^3 \cdot 31^3 x$ were the only ones found containing 2 integral points (one nonzero integral point).

Despite these findings, we can find arbitrarily many curves which have nonzero integral points in each of the cases listed in the title of this subsection, and we will describe how to do so.

Let us first consider the case $(a, b) = (2, t)$, where t is any positive integer. Let q be any prime satisfying $q \equiv \pm 1 \pmod 8$, so that q splits in the ring R of integers of the field $\mathbb{Q}[\sqrt{2}]$, and let $\alpha \in R$ be an element of norm q. Let u be the unit in R given by $u = 1 + \sqrt{2}$. Then $-q^t$ is the norm of $\alpha^t \cdot u^r$ for any odd integer r, and since R is a unique factorization domain, this explicitly gives integers p and u for which $-q^t = p^2 - 2u^2$ for each choice of r. Select r so that the integer resulting integer p is a prime. Heuristically, this is doable, according to standard conjectures on the distribution of primes (namely, that the probability that an integer n is prime is roughly $1/\log(n)$). By putting $v = (q^t - p^2)/2$, one can verify that $(x, y) = (u^2, uv)$ is a nonzero integral point on the curve $y^2 = x^3 - p^2 q^t x$. Although this construction works extremely well in practice, it is based on heuristics concerning the distribution of primes, and hence proving that this construction always gives a point is quite difficult.

Open Problem 6 Prove that for every positive integer t, there are infinitely many pairs of distinct odd primes p and q for which the elliptic curve $y^2 = x^3 - p^2 q^t x$ contains a nonzero integral point.

The case $(a, b) = (3, 3)$ is quite interesting, and a method which conjecturally gives an infinitude of curves $y^2 = x^3 - p^3 q^3 x$ containing a nonzero integral point will be described below. As in the previous case, the construction will give a point whose x coordinate is a square i.e. $d = 1$. The construction is derived from the following simple observation. Let $f_1(X, Y)$ and $f_2(X, Y)$ denote the bivariate polynomials given by

$$f_1(X, Y) = 4X^4 + 12X^2Y^2 - 3Y^4, \;\; f_2(X, Y) = -4X^4 + 12X^2Y^2 + 3Y^4,$$

and

$$f(X, Y) = 24X^5Y + 18XY^5.$$

Then

$$2f(X,Y)^2 = f_1(X,Y)^3 + f_2(X,Y)^3,$$

and both $f_1(X,Y)$ and $f_2(X,Y)$ are irreducible polynomials in $\mathbb{Z}[X,Y]$. Computationally, one simply searches over values of f_1 and f_2 until two primes p and q are hit. Already with $X = Y = 1$, the pair $(p,q) = (11,13)$ immediately arises, and therefore the curve $y^2 = x^3 - 11^3 \cdot 13^3 x$ has a primitive integral point.

Standard conjectures in analytic number guarantee the existence of infinitely many such prime pairs, and consequently, the corresponding curve given by $y^2 = x^3 - p^3q^3x$ will have a nonzero integral point with x coordinate being the value of $f(X,Y)$ with the same inputs as those which gave p and q. The reader interested in the topic of prime values of irreducible polynomials, a good starting point is p.323 in Serge Lang's textbook Algebra [12]. Admittedly, we are supposing much more than primality of one polynomial here, however, if one regards the primality of each polynomial as independent, then the assertion is not just reasonable, but falls in line with the famous *prime k-tuples conjecture* of Hardy and Littlewood. For this, the reader may wish consult p.66 in Riesel's classic book on primes and factorization [17].

Open Problem 7 Prove that there are infinitely many pairs of distinct primes p and q for which the curve $y^2 = x^3 - p^3q^3x$ contains a nonzero integral point.

It is worth pointing out at this juncture that if $\min(a,b) \geq 3$ and (x,y) is a primitive integral point, then $\gcd(x,pq) = 1$, and thus either $x = u^2$ or $x = -u^2$ for some integer u. This is quite simple to prove using the derived quartic equation $dv^2 = d^2u^4 - p^aq^b$, where $x = du^2$ and d is squarefree dividing pq. This observation reduces the number of derived quartic equations to consider considerably as both a and b grow.

Despite the apparent phenomena of the existence of non-zero integral points on curves of the form $y^2 = x^3 - p^aq^ax$ with $a = 3$, the situation changes sharply for $a \geq 4$, which leads us to the next section.

4 The Diagonal Case and FLT

As is well known, Andrew Wiles used the theory of elliptic curves and modular forms to prove Fermat's Last Theorem [23]. Since then, Wiles' approach has been developed considerably by many authors to solve other Diophantine problems, a subject which is commonly referred to as *modular methods*. Two such results that pertain to the topic at hand are those of Bennett and Skinner [5], and of Bennett, Ellenberg and Ng [6]. In particular, Bennett and Skinner used modular methods to prove, among other things, that for $n \geq 4$, the only nonzero integer solution to the equation

$$2Z^2 = X^n + Y^n$$

is $(X, Y, Z) = (1, 1, 1)$, while Bennett, Ellenberg and Ng proved that for n in that same range, the Diophantine equation

$$Y^2 + Z^4 = X^n$$

has no nonzero solutions (X, Y, Z).

These two theorems imply that if $a = b$ and $a \geq 4$, then the elliptic curve $y^2 = x^3 - p^a q^b x$ has no primitive integral points. To see this, following the arguments given above, a primitive integral point (x, y) would have to have either $x = u^2$, in which case either $2u^2 = p^a + q^a$ or $2u^2 = (pq)^a + 1^a$, or else $x = -u^2$, in which case there would be a positive integer v coprime to u for which $u^4 + v^2 = p^a q^a$. The diophantine results stated just above show that these cases are all impossible to solve. The reader should bear in mind the extremely deep mathematics that underlie these statements, which this author feels is testimony to the state of the art in the area of Diophantine analysis.

5 An Illustrative Example

As our study heads into the space of curves with a and b getting larger, it is a good idea to know what to expect. This can be achieved in multiple ways. One can speculatively do computations to see what patterns arise. There is also a tool for such questions in number theory, which is extremely useful when it applies. It is referred to as the ABC conjecture. We will come back to this tool, and for the time being, look at the results of doing some computations for the specific pair of primes $p = 3$ and $q = 13$. This pair of primes was chosen simply for the reason that there exist primitive integral points for the various pairs (a, b), and it shows quite explicitly, as a and b increase, the general phenomena that has been observed for all elliptic curves of this type.

For these two primes, we searched for primitive integral points on $y^2 = x^3 - p^a q^b x$ with $1 \leq a, b \leq 10$. The results of the search yield such points in the following cases:

$(a, b) = (1, 2)$: 2 points
$(a, b) = (2, 1)$: 9 points
$(a, b) = (2, 2)$: 4 points
$(a, b) = (2, 3)$: 1 point
$(a, b) = (4, 3)$: 1 point
$(a, b) = (5, 2)$: 1 point
$(a, b) = (6, 1)$: 1 point

The main thing to notice is the sharp drop off of primitive points once $\min(a, b) \geq 3$, and the lack of primitive points once this minimum reaches 4.

To illustrate the existence of imprimitive points, we computed the integral points on $y^2 = x^3 - 3^6 \cdot 13^6 x$, and not too surprisingly, the only points on this curve are of the form $(p^2q^2x_1, p^3y_1)$, where (x_1, y_1) is a point on the curve $y^2 = x^3 - 3^2 \cdot 13^2 x$.

6 The ABC Conjecture

Succinctly put, the ABC conjecture is an attempt to capture the essence of a fundamental relationship between the multiplicative structure of two positive integers and that of their sum. Discovered first by Oesterlé [16], and later refined by Masser [14], the ABC conjecture stands as one of the greatest open problems in number theory. Such a relationship was discovered by Mason to hold for polynomials [13], and a substantially weaker form of this relationship has been proven by Stewart and Yu for integers using transcendental number theory [19]. The reader is referred to the website of Nitaj [15] for many aspects of the ABC conjecture, including its applications, numerical examples and references.

The ABC Conjecture Given any $\epsilon > 0$ there is a positive constant $k = k(\epsilon)$, depending only on ϵ with the property that if a, b and c are positive coprime integers satisfying $a + b = c$, then $c < k(\prod_{p|abc} p)^{1+\epsilon}$.

For our purpose, we will make use of a consequence of the ABC conjecture that was proved by Darmon and Granville [8]. This conditional result states that if the ABC conjecture is true, then for any triple of pairwise coprime positive integers R, S, T, there is only a finite number of pairwise coprime triples of pure powers x^r, y^s, z^t (all of r, s, t are > 1) satisfying both

$$Rx^r + Sy^s = Tz^t$$

and

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1.$$

Let's see how this result can be used for the cases $(a, b) = (1, t)$, $(2, t)$, $(3, t)$ and $(4, t)$. Recall equation (3.1.2), which assumes that the x coordinate of a point is of the form $x = du^2$ with d squarefree, and deduces from the curve that there is an integer v which satisfies

$$dv^2 = d^2u^4 - p^aq^b,$$

which, in the cases being considered, is one of $dv^2 = d^2u^4 - p^lq^t$ with $1 \leq l \leq 4$. The primitivity criterion, shows that either $d = \pm 1$ or $d = \pm p$, and so these equations become one of $\pm v^2 = u^4 - p^lq^t$ or $\pm v^2 = pu^4 - q^t$ with $1 \leq l \leq 4$. For each choice of l and equation given, the statement of Darmon and Granville shows that there are no coprime integer solutions for t sufficiently large. The upshot of all of this is, once p and q are chosen, and one of their respective

exponents a or b is kept no larger than 4, while the other exponent is allowed to grow, only a bounded number of primitive integer points will arise, no matter how large that exponent becomes.

Example Let us have a close look at the particular case $(p, q) = (421, 5)$. This example is illuminating because it shows explicitly the general pattern for the number of integral points on elliptic curves of this type. Consider the set of integral points on curves of the form $y^2 = x^3 - pq^t x$, with $1 \leq t \leq 20$. For $t \equiv 0, 2, 3 \pmod 4$, the number of points is constant at 2, 1 and 2 respectively, which means that only imprimitive points lie on those curves with $t > 3$. For $t \equiv 1 \pmod 4$, the situation is a little different. At $t = 1$, the curve has 5 integral points, and then at $t = 5$, 3 new primitive points arise giving a total of 8 integral points on the curve $y^2 = x^3 - 421 \cdot 5^5 x$. Then, at $t = 9$, 1 more primitive point arises for a total of 9 integral points on $y^2 = x^3 - 421 \cdot 5^9 x$, and the total of 9 points remains constant from that point onward ($t = 13$ and $t = 17$). We remark that the primitive point of the curve $y^2 = x^3 - 421 \cdot 5^9 x$ has $d = -1$, which corresponds directly to the fact that one of the representations of $421 \cdot 5^9$ as a sum of two squares has a summand which is a fourth power ($421 \cdot 5^9 = 7933^2 + 166^4$). Further computation on this example failed to find any further primitive points as t increased. Therefore, we conjecture the following to be true, albeit a fairly specific problem.

Open Problem 8 Prove that for any positive integer t, the curve

$$y^2 = x^3 - 421 \cdot 5^t x$$

has at most k integral points, where $k = 2$ if t is even, $k = 1$ if $t \equiv 3 \pmod 4$, and $k = 9$ if both $t \equiv 1 \pmod 4$ and $t \geq 9$.

Our ultimate goal in the use of the ABC conjecture is to get a sense of how many primitive integral points there can be for a fixed pair of distinct odd primes as the exponents are allowed to range over all pairs of positive integers. We have seen that the ABC conjecture implies that the union of all points on curves $y^2 = x^3 - p^a q^b x$, with a and b in the strips determined by $1 \leq a \leq 4,\ 1 \leq b$ and $1 \leq a,\ 1 \leq b \leq 4$ contains a finite set of primitive integral points, and hence there is a positive constant $C = C(p, q)$, depending only on p and q, for which the number of integral points on any one of these curves is bounded by C.

We now look at the remaining set of pairs of positive integers (a, b), which is the set of pairs (a, b) with $\min(a, b) \geq 5$. As noted above, a primitive integral point (x, y) on the curve $y^2 = x^3 - p^a q^b x$ forces $x = \pm u^2$, and we will simply deal with the case $x = u^2$, as the other case is identical. Equation (3.1.2) becomes $v^2 = u^4 - p^a q^b$, which we can rewrite as $v^2 + p^a q^b = u^4$, and primitivity gives that these terms are pairwise coprime. We apply the ABC conjecture with $\epsilon = .05$. We will use the fact that $v < u^2$ and $p^a q^b < u^4$. Lastly, we will use l to represent a prime dividing terms in the product. The ABC conjecture gives

a constant k, depending on this choice of ϵ, for which the following sequence of inequalities hold.

$$u^4 < k(\prod_{l|uvpq} l)^{1.05} < k(uvpq)^{1.05} < k(u^3pq)^{1.05} < k(u^{3.8})^{1.05} = k \cdot u^{3.99}.$$

In other words, the ABC conjecture implies that u is bounded by an absolute constant, and this is for all possible choices of $a, b \geq 5$. We have shown the following result.

Theorem Let p and q be distinct odd primes. Let $\mathcal{E}$ denote the union of all elliptic curves of the form $y^2 = x^3 - p^a q^b x$ with a and b positive integers. The ABC conjecture implies that the number of primitive integral points contained in $\mathcal{E}$ is finite.

Another way to view this result is simply that if one were to fix p and q, then the ABC conjecture shows that if either of a or b is large enough, the curve $y^2 = x^3 - p^a q^b x$ cannot have primitive integral points, and hence that if it were to have an integral point, it must come from a point on a similar curve $y^2 = x^3 - p^{a_1} q^{b_1} x$ with at least one of $a_1 < a$ or $b_1 < b$.

The ABC conjecture gives deep insight into this problem, however our computations go beyond this. To be more specific, the ABC conjecture gives a uniform upper bound for the number of integer points on any curve of the form $y^2 = x^3 - p^a q^b x$ as a and b range over the positive integers, but with p and q fixed. Our computations show that there is an upper bound which is also independent of p and q. The following open problem is intended to summarize our findings, which combines the theoretical truth dictated by the ABC conjecture, together with the findings of our computations.

Open Problem 9 Is there a uniform upper bound for the number of integral points on a curve of the form $y^2 = x^3 - p^a q^b x$ which is independent of p, q, a and b? If so, what is the correct upper bound?

Our computations have failed to find a curve with more than 11 integral points. Moreover, finding primitive integral points on curves with $a \geq 3$ and $b \geq 4$ is not such a simple task. We list below some of the points we have found just to give an idea of how sparse they are.

7 Numerical Examples

It was observed earlier that if $a \geq 3$ and $b \geq 3$, a primitive integral point (x, y) necessarily has the property that the x coordinate is either of the form $x = u^2$ or $x = -u^2$ for some integer u. We refer to the former case as a *Type 1* primitive

point and the latter as a *Type 2* primitive point. We first exhibit a straightforward method to produce curves containing a Type 1 point with $a = 3$ and $b = 4$.

Using methods from Invariant Theory, discussed in the work of Edwards [9], one can sometimes compute polynomial solutions to equations having integer coefficients. For such equations, if there is one solution in integers, then there is a polynomial solution, and hence infinitely many solutions in integers. Now recall that if the equation

$$2u^2 = p^a + q^b$$

has a solution, then (x, y) is a primitive integral point on $y^2 = x^3 - p^a q^b x$, where $x = u^2$, $y = uv$, and $v = (q^b - p^a)/2$. In the case $a = 3$ and $b = 4$, we then wish to find integral solutions to

$$2Z^2 = X^3 + Y^4.$$

It was shown in Edwards [9] how equations of this type are parametrizable provided that at least one integer solution exists. In particular, the work of Edwards shows that because $1 + 1 = 2$, we can find bivariate polynomials f_1, f_2, f_3 satisfying $2f_1^2 = f_2^3 + f_3^4$. Indeed, let

$$f_1(X,Y) = \sum_{i=0}^{12} a_i X^{12-i} Y^i,\ f_2(X,Y) = \sum_{i=0}^{8} b_i^{8-i} Y^i,\ f_3(X,Y) = \sum_{i=0}^{6} c_i X^{6-i} Y^i$$

with

$[a_i] =$

$[1, 0, 66, 88, -693, -3168, -2772, -14256, 13959, 9504, -65934, -29160, -34803]$,

$[b_i] = [1, -8, -28, -168, -42, 840, -252, 1512, 1233]$,

and $[c_i] = [1, 6, -15, 60, 135, 198, -153]$,

then the polynomial equation $2f_1^2 = f_2^3 + f_3^4$ holds. Much to our delight, the polynomials $f_2(X, Y)$ and $f_3(X, Y)$ are irreducible in $\mathbb{Z}[X, Y]$, which conjecturally implies that they will be simultaneously prime infinitely often. In fact, evaluating them at the point $(2, 1)$ gives the two primes $p = 1361$ and $q = 1279$, and we find that $p^3 + q^4 = 2u^2$ with $u = 1157259$. Therefore, $x = u^2$ is the x coordinate of a primitive point on the curve $y^2 = x^3 - p^3 q^4 x$.

The critical aspect to this construction goes back to the sum of the reciprocals of the exponents, as we saw earlier. In the case above, this sum is greater than one, which allows for the parametrization we have given. A similar construction is achievable for exponents $(2, 3, 5)$ because $1/2 + 1/3 + 1/5 > 1$ and a solution exists with $(X, Y, Z) = (1, 1, 1)$. In particular, there are bivariate homogeneous polynomials f_1 of degree 10, f_2 of degree 6, and f_3 of degree 15

which satisfy $2f_3^2 = f_1^3 + f_2^5$. The more motivated reader may wish to work out the details on this. In the meantime, the smallest numerical example found is $(p, q) = (37, 19)$, which means specifically that the curve $y^2 = x^3 - 37^3 \cdot 19^5 x$ contains a primitive integral point.

When the sum of the reciprocals of the exponents is larger than one, an equation as above is referred to as being in the *spherical* case. For exponents $(2, 3, 6)$, the sum of the reciprocals is equal to 1, which is referred to as the *Euclidean* case, and the solvability depends entirely on the solution set of an associated elliptic curve. If the sum is less than one, this is referred to as the *Hyperbolic* case, which has only a finite number of rational solutions, which is a consequence of Faltings' theorem on curves of genus larger than 1. For more about Faltings' theorem, the reader may consider looking at Part E in the textbook of Hindry and Silverman [11].

The case $(2, 3, 6)$ is an easy case to deal with, as it implies integers (X, Y) for which one of the polynomials $f_1(X, Y)$, $f_2(X, Y)$ given in the section above concerning solutions to $2u^2 = p^3 + q^3$ would have to have a value which is of the form p^2. But this is easily seen to be impossible, as $p^2 \equiv 1 \pmod 8$ for any odd prime p, while the values of those polynomials are 5 and 3 modulo 8 respectively.

An extensive search for Type 1 primitive points with $a \geq 3$ and $b \geq 7$ turned up only one example. Namely, the point $(x, y) = (34^2, 35054)$ is a primitive point on $y^2 = x^3 - 3^7 \cdot 5^3 x$. This brings us to our next open problem.

Open Problem 10 Let a and b be positive integers for which $1/a + 1/b \leq 1/2$, and p, q distinct odd primes. Prove that the only Type 1 primitive point on any elliptic curve given by $y^2 = x^3 - p^a q^b x$ is $(x, y) = (34^2, 35054)$ on $y^2 = x^3 - 3^7 \cdot 5^3 x$.

Type 2 primitive points do exist for various pairs (a, b) with $a \geq 3$ and $b \geq 4$, but these appear to be more controlled by the ABC conjecture than by the algebraic methods stemming from Invariant Theory as we saw for Type 1. Primitive points in this case arise from solutions to equations of the form $u^4 + v^2 = p^a q^b$, and once a and b are sufficiently large, the ABC conjecture tells us that integer solutions cannot exist. We provide some examples below, and state an open problem which relates directly to what are known as ABC triples.

$$326^4 + 193525^2 = 41^3 \cdot 29^4$$

$$4892^4 + 3155277^2 = 9769^3 \cdot 5^4$$

$$4084^4 + 8382669^2 = 73^3 \cdot 173^4$$

$$6416^4 + 150205817^2 = 33857^3 \cdot 5^4$$

$$1799^4 + 6800796^2 = 193^3 \cdot 53^4$$

$$44470391025^4 + 7923409608980072275882 = 1009^3 \cdot 257819713^4$$

$$7^4 + 3918^2 = 17^3 \cdot 5^5$$

$$3883^4 + 10635740^2 = 13^3 \cdot 173^5$$

$$965514^4 + 30534726875412 = 577^4 \cdot 613^6$$

$$203130^4 + 393509435932 = 601^4 \cdot 157^6$$

$$(*) \quad 43^4 + 29732^2 = 5^4 \cdot 17^5$$

The reason we put an asterisk in the last example is because it is our current ABC record, which we explain below. The ABC conjecture relates the bitlength of the largest integer appearing in the sum to that of the product of primes dividing the three integers. Thus, the *quality* of a triple a, b, c is measured explicitly by

$$quality(a, b, c) = \frac{\log(\max(|a|, |b|, |c|))}{\log(\prod_{p|abc} p)}$$

The notion of quality gives a very nice interpretation of what the ABC conjecture actual tells us. The essence of the ABC conjecture is simply that for any real number $\alpha > 1$, there exist only a finite number of triples of coprime positive integers (A, B, C) satisfying $C = A + B$ whose quality is larger than α. Consequently, it has become customary to label any triple whose quality is well above 1 as an *ABC triple*. A list of record holders of ABC triples (and their qualities) is available for perusal on a website maintained by Nitaj [15]. We remark finally that the last example above has quality 1.1568, which is not in the top ten of ABC triples, but still considerably away from 1 that it is worth noting.

Open Problem 11
a. Find a Type 2 integral point with exponents a, b satisfying either $a \geq 4, b > 5$, or $a > 4, b \geq 5$.
b. Find a Type 2 integral point with ABC quality larger than 1.1568.

7.1 Finale

Combining our numerical searches for Type 1 and Type 2 integral points, together with the ABC conjecture, we end with the following.

Conjecture Let a and b denote positive integers satisfying $\min(a, b) \geq 5$, and let p and q be distinct odd primes. Then the elliptic curve

$$y^2 = x^3 - p^a q^b x$$

does not contain any primitive integral points.

References

[1] S. Akhtari, Integral points on a certain family of elliptic curves. *J. Théor. Nombres Bordeaux* **27**(2) (2015) 353 - 373.

[2] S. Akhtari, The diophantine equation $aX^4 - bY^2 = 1$, J. Reine Angew. Math **630** (2009), 33 - 57.

[3] A. Baker, The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. London Math. Soc.* **43** (1968), 1 - 9.

[4] M.A. Bennett, Integral points on congruent number curves. *Int. J. Number Theory* **9**(6) (2013) 1619 - 1640.

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

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

[7] J-H. Chen and P.M. Voutier, Complete solution of the diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations, *J. Number Theory* **62** (1997), 71 - 99.

[8] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. Lond. Math. Soc.* **27** (1995), 513 - 543.

[9] J. Edwards, Platonic solids and solutions to $X^2 + Y^3 = DZ^r$, Dissertationes Univ. Utrecht (2004).

[10] W. Gasarch, Hilbert's Tenth Problem: Refinements and Variants, arxiv: 2104.07220v2, 31 May, 2021.

[11] M. Hindry and J.H Silverman, Diophantine Geometry: An Introduction, Springer, Berlin, 2000.

[12] S. Lang, Algebra, 3rd ed., GTM 211, Springer, New York, 1993.

[13] R.C. Mason, Diophantine Equations Over Function Fields. *London Mathematical Society Lecture Note Series* **96** Cambridge University Press. (1984).

[14] D.W. Masser, Note on a conjecture of Szpiro, *Asterisque* **183** (1990), 19 - 23.

[15] A. Nitaj, *https://nitaj.users.lmno.cnrs.fr/abc.html* .

[16] J. Oesterlé, Nouvelles approches du "theoreme" de Fermat. (New approaches to Fermat's last theorem). *Semin. Bourbaki*, 40eme Annee, Vol. 1987/88, Exp. No.694, Asterisque 161/162, 165-186 (1988).

[17] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhäuser, Boston, 2012.

[18] J.H. Silverman, *The Arithmetic of Elliptic Curves* Graduate Texts in Mathematics **106** 2nd Ed. (Springer-Verlag, New York, 2009).

[19] C.L. Stewart and K. Yu, On the abc conjecture. *Math. Ann.* **291** (1991), 225 - 230.

[20] P.G. Walsh, On the number of large integer points on elliptic curves. *Acta Arith.* **138**(4) (2009) 317 - 327.

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

[22] P.G. Walsh, Squares in recurrences using elliptic curves, to appear in *Internat. J. Number Theory*, 2023, 8 pages.

[23] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. Math. **141** (1995), 443 - 551.