Twisted Extensions of Fermat's Last Theorem

by

Carmen Anthony Bruni

A thesis submitted in partial fulfillment of the requirements for
the degree of

Doctor of Philosophy

in

The Faculty of Graduate and Postdoctoral Studies
(Mathematics)

The University of British Columbia
(Vancouver)

April 2015

Abstract

Let $x, y, z, p, n, \alpha \in \mathbb{Z}$ with $\alpha \geq 1$, p and $n \geq 5$ primes. In 2011, Michael Bennett, Florian Luca and Jamie Mulholland showed that the equation $x^3+y^3 = p^\alpha z^n$ has no pairwise coprime nonzero integer solutions provided $p \geq 5, n \geq p^{2p}$ and $p \notin S$ where S is the set of primes q for which there exists an elliptic curve of conductor $N_E \in \{18q, 36q, 72q\}$ with at least one nontrivial rational 2-torsion point. In this thesis, I will present a solution that extends the result to include a subset of the primes in S; those $q \in S$ for which all curves with conductor $N_E \in \{18q, 36q, 72q\}$ with nontrivial rational 2-torsion have discriminants not of the form ℓ^2 or $-3m^2$ with $\ell, m \in \mathbb{Z}$. Using a similar approach, I will classify certain integer solutions to the equation $x^5 + y^5 = p^\alpha z^n$ which in part generalizes work done from Billerey and Dieulefait in 2009. I will also discuss limitations of the methods for these equations and as they extend to further prime exponents.

Preface

This dissertation is original, unpublished, independent work by the author, Carmen Anthony Bruni.

Table of Contents

List of Tables

Acknowledgements

My sincerest and utmost thanks to my supervisor Professor Michael Bennett for all of his patience and dedication to me as a Ph.D. student. I cannot express in words how much it has meant to have someone who has believed in me as much as you have over the years. Your guidance and help has made this project possible. I am very thankful to have a supervisor with your vision and expertise in the field.

To my supervisory committee Professors Greg Martin and Vinayak Vatsal, thank you so much for always being available for advice and for teaching. It has been great having a committee with such a kind and generous open door policy. Your guidance has always been appreciated over the years!

I would also like to thank many professors I have had discussions with including Professors Nils Bruin, Samir Siksek and Michael Stoll. A thank you as well to the many people who reply to MathOverflow posts.

I would also like to thank the faculty and staff at the University of British Columbia, especially all the support staff in Math 121. Over the years I have spoken to just about everyone in that room and their knowledge of the hidden working of a university is so invaluable. The University of British Columbia is very blessed to have such a great room of people.

A big thank you goes out to all of my friends and family back at home who have supported me over the years. I would like to especially thank my parents for supporting me over these last 10 years both emotionally and mentally with the highs and lows that come with a graduate degree. Without such a loving and supportive family cast I'm not sure how this would have been possible.

To my fiancée Jessica. I cannot put into words how much your love and support has meant to me over these last 5 years of my degree. Thank you so much for always being there to help me. Thank you for picking me up when I was down and reminding me to stay healthy when I was too busy to remember. Thanks for helping me to explore Vancouver and

reminding me that there is so much more to life than mathematics. Thank you for being there in the past and thank you in advance for being there in the future.

To my friends from Waterloo, especially Vince and Vicki Chan and Faisal al-Faisal. Over the last 10 years you have been my go to people for help and advice for all things math related. Thank you for being a part of my life. This project could not have been successful without such a great group of core friends.

To my friends here at the University of British Columbia, thank you for everything. I could state the names of about half the math graduate students by now over the last 5 years here but let me just keep it short and say that you know who you are and thank you so much for helping me to keep my sanity intact. A big thank you especially to my office mates in Math 201 and to the MER wiki team for always being there when the stress of graduate school was too much for me to handle alone.

Finally I would like to acknowledge that this project was funded in part by both a CGS-M scholarship and a Four Year Fellowship from the University of British Columbia for which I am thankful for.

Dedication

Per mia nonna Giuseppina Mattina e mia zia Carmela Mattina. Il vostro amore e il duro lavoro ha reso possibile questa tesi. Che tu possa riposare in pace con il comfort di Dio.

Chapter 1

Introduction

1.1 The History of the Problem

A *Diophantine equation* is a polynomial defined over $\mathbb{Z}[x_1, .., x_n]$ where we seek out integer (or rational) n-tuples satisfying the polynomial. These equations are named after Diophantus of Alexandria who lived during the third century A.D. His book Arithmetica contains such equations which he solved for using positive rational numbers. For a more thorough view of the history of Diophantus, see [Sch98][1].

Throughout the last 2600 years of number theory, a great deal of mathematics has been created to solve Diophantine equations. Some of the earliest attempts at solving Diophantine equations date back to Pythagoreas. He was particularly interested in the equation $x^2 + y^2 = z^2$. This equation is the Pythagorean theorem for right angled triangles, which geometrically says that sum of the squares of the perpendicular sides of a triangle equals the square of its hypotenuse. A question one can ask is "Which right angled triangles have all integer side lengths?" With a bit of effort, we can come up with a few simple examples, the most well known being $(3, 4, 5)$ and $(5, 12, 13)$ and then notice that integer multiples of these will also work such as $(6, 12, 15)$ or $(2500, 6000, 6500)$. In light of this, we call a solution *primitive* if there is no common multiple between the three variables. Simplifying our question, we now ask "Can we find all such primitive solutions?" This question at first might seem ill posed - what happens if there are infinitely many? One cannot list all solutions if there are infinitely many. In this case, what we can hope to find is a parameterized family of solutions, that is, equations for the variables that depend on parameters in such a way that if we replace the parameters with integers, we get solutions to our original equation and that these solutions form a comprehensive list. It is said that Pythagoreas was the first to attempt

[1] An English translation can be found on the author's personal webpage at ⟨http://www-irma.u-strasbg.fr/~schappa/NSch/Publications_files/Dioph.pdf⟩.

such a parameterization and came up with the following [Itō87]

$$(x, y, z) = (2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$$

for a (positive) integer n. This parameterization gives an infinite family of solutions, but not a complete list. The full parameterization is possible and is given by

$$(x, y, z) = (s^2 - t^2, 2st, s^2 + t^2)$$

where s and t are integers. This was first given in Euclid Elements [Euc02, Book 10 Proposition 29].

From here, it seems like a simple switch would be to turn all the squares into cubes, that is to examine the equation $x^3 + y^3 = z^3$. Thinking about this geometrically, we are asking can we write the volume of a cube as the sum of two volumes of cubes. There are some trivial such examples of this problem, namely when one of the cubes has 0 length so we further say that a solution to a Diophantine equation is *trivial* if $xyz = 0$, that is, if at least one of the components is zero. Now as before, we ask "Can we classify all non-trivial primitive solutions to this equation?" This question can be resolved in the affirmative. It is known that no such solutions exist, the first proof of which was given formally by Leonhard Euler in 1770. He used the method of infinite descent, the same method that Pierre de Fermat used to solve the case of $x^4 + y^4 = z^4$ in the 1600s [Bal60, p.242]. Fermat seldom formally published any of his proofs however stories say that whenever asked for a proof, he could always produce one [Bal60, p.242].

This brings us to our title character, Pierre de Fermat. In the margin of his copy of Diophantus' *Arithmetica*[2], he wrote down, after translating to modern language, that the equation $x^n + y^n = z^n$ had no non-trivial primitive solutions and claimed he had a remarkable proof of this fact for which the margin was too narrow to contain. Since that time, mathematicians have sought out a solution to this problem. This quest as we will see took many years before being completed.

Years later, in 1847, Gabriel Lamé announced a proof of Fermat's Last Theorem using the idea of cyclotomic numbers [Dev90, p.278]. Let $p \geq 5$ be a prime number and let ζ_p be a primitive pth root of unity, that is, a strictly complex solution to $x^p - 1$. Lamé argues that

[2]The term "Diophantine equation" originates from the name Diophantus.

if (x, y, z) is a solution to Fermat's Last Theorem with exponent p a prime, then

$$z^p = x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$$

and then one argues that each $(x + \zeta_p^i y)$ is a pth power times a unit. Argue similarly for $x^p + (-z)^p$ and then use these two pieces of information to derive a contradiction (see [BS66, Chapter 3] for the full and complete argument). The problem with this proof is that three years earlier, Ernst Kummer showed that the ring $\mathbb{Z}[\zeta_{23}]$ fails to be a unique factorization domain. In one sentence, the elements of this ring do not behave like integers in the sense that elements do not necessarily decompose into a product of prime elements uniquely, contrary to how the Fundamental Theorem of Arithmetic works for the integers. This failure prevents each factor in the product above from necessarily being a pth power as Lamé assumes. Kummer in 1847 found a way around this. He introduced the idea of using ideals to attempt to solve this problem. Over prime ideals, unique factorization does occur as we know it and much of the theory of integers carries through. The concept of the class number, the size of the group of fractional ideals modulo the principal fractional ideals, has its roots here. He shows that if the prime p does not divide the order of this finite group, then the Fermat equation for exponent p has only trivial solutions. These primes are called regular primes and Kummer showed that the only primes less than 100 that are not regular are $37, 59$ and 67.

Seeing just how close Kummer was to a proof, it seemed that a solution would soon surface. Sadly this is not the case. The next big step towards solving Fermat's Last Theorem is due to Louis Mordell. In 1922, Mordell noticed that when dealing with a Diophantine equation, there were no known examples of equations of genus (an algebraic invariant of the equation) bigger than or equal to 2 where the number of rational points was infinite [Dev90, p.286]. He conjectured that if one considers an equation with genus strictly bigger than 1, then the equation in question must only have finitely many primitive integer solutions. It was not until 1983 when Gerd Faltings proved that indeed this is true [Fal83]. For his work, he was awarded the Fields Medal in 1986.

Now Plücker's formula says that for $n \geq 4$, the genus of the curve $x^n + y^n = z^n$ is at least 2. Hence, we know that each such curve has only finitely many primitive integer points. Unfortunately, Faltings' theorem is not effective meaning that while you know that there are only finitely many solutions, the theorem does not give you an algorithm on how to find them. The statement that we wish to prove is that the equation $x^n + y^n = z^n$ has only trivial primitive solutions and up to this point in time, we are close, but still far away.

This brings us to the work of Andrew Wiles in 1993-1994. Our brief detour in history ends now and I will begin to outline the proof that Wiles used to prove Fermat's Last Theorem. This will involve techniques using elliptic curves and modular forms so we begin first by giving a review of relevant topics.

1.2 Elliptic Curves

The information in this chapter is a summary of some of the notation in this thesis and is not meant to be an inclusive rehashing of elliptic curves. For a few excellent references, see [Kna92], [Sil09], [Was08].

An elliptic curve E defined over a field K is a nonsingular curve of the form

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with each $a_i \in K$. This is known as the Weierstrass form of an elliptic curve. In this form, we recall that there is a point at infinity given in projective coordinates by $[0 : 1 : 0] \in E$ and this is the only point that lies on the curve with $z = 0$. For this reason, we typically work with the elliptic curve in the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

recalling that we have an extra point given above which we call the point at infinity and denote it by 0_E or 0 if the context is clear. For such forms we have the following invariants

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = \frac{b_2b_6 - b_4^2}{4} \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6.
\end{aligned}$$

We also define the discriminant of an elliptic curve as follows

$$\begin{aligned}\Delta &= \frac{c_4^3 - c_6^2}{1728} \\ &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\ &= -a_1^4 a_2 a_3^2 + a_1^5 a_3 a_4 - a_1^6 a_6 - 8a_1^2 a_2^2 a_3^2 + a_1^3 a_3^3 + 8a_1^3 a_2 a_3 a_4 + a_1^4 a_4^2 - 12a_1^4 a_2 a_6 - 16a_2^3 a_3^2 \\ &\quad + 36a_1 a_2 a_3^3 + 16a_1 a_2^2 a_3 a_4 - 30a_1^2 a_3^2 a_4 + 8a_1^2 a_2 a_4^2 - 48a_1^2 a_2^2 a_6 + 36a_1^3 a_3 a_6 - 27a_3^4 \\ &\quad + 72a_2 a_3^2 a_4 + 16a_2^2 a_4^2 - 96a_1 a_3 a_4^2 - 64a_2^3 a_6 + 144a_1 a_2 a_3 a_6 + 72a_1^2 a_4 a_6 - 64a_4^3 - 216a_3^2 a_6 \\ &\quad + 288a_2 a_4 a_6 - 432a_6^2.\end{aligned}$$

Throughout this thesis, we will be interested in rational elliptic curves with rational two torsion. Translating so that this torsion point occurs at $(x, y) = (0, 0)$ shifts the above equation to one of the form

$$E : y^2 = x^3 + a_2 x^2 + a_4 x$$

and in this case, the invariants become

$$\begin{aligned}b_2 &= 4a_2 \\ b_4 &= 2a_4 \\ b_6 &= 0 \\ b_8 &= -a_4^2 \\ c_4 &= 16a_2^2 - 48a_4 \\ c_6 &= -64a_2^3 + 288a_2 a_4 \\ \Delta &= 16a_2^2 a_4^2 - 64a_4^3 = 16a_4^2(a_2^2 - 4a_4).\end{aligned}$$

Definition 1.2.1. Two elliptic curves E_1 and E_2 are said to be isomorphic over K if there is an admissible change of variables between them given by

$$\begin{aligned}&\phi : E_1 \to E_2 \\ &(x, y) \mapsto (u^2 x' + r, u^3 y' + s u^2 x' + t)\end{aligned}$$

where $u, r, s, t \in K$ and $u \neq 0$. More generally, there are rational function in both directions defined for all points such that their composition in both directions gives the identity function.

In the case where $K = \mathbb{Q}$, we can perform an admissible change of variables so that the coefficients are integers. We assume this throughout whenever we define an elliptic over $\mathbb{Q}$ we have coefficients in $\mathbb{Z}$. Performing the above admissible change of variables also changes the discriminant by at most a twelfth power. There is a model of our equation such that the discriminant is smallest possible and we shall call such a model a minimal model and such a

discriminant a minimal discriminant denoted by $\Delta_{\min}$.

One thing we will also want to do is change the field of definition from $\mathbb{Q}$ to a finite field $\mathbb{F}_p$ where p is a prime. In doing so, we define the following types of reduction.

Definition 1.2.2. We say that an elliptic curve has

1. Good reduction at p if $p \nmid \Delta_{\min}$.
2. Bad multiplicative reduction at p if $p \mid \Delta_{\min}$ and $p \nmid c_4$ (the equation of the reduced curve has a node - a double root).
3. Bad additive reduction at p if $p \mid \Delta_{\min}$ and $p \mid c_4$ (the equation of the reduced curve has a cusp - a triple root).

On an elliptic curve, we have a group law. Any two points on an elliptic curve give rise to a third. Take the line joining the two points (or the tangent line if the two points are the same). This line intersects the curve at a third point (or at the point at infinity).

Definition 1.2.3. An isogeny over a field K between two elliptic curves defined over K is a morphism defined over K (in the sense of algebraic varieties; briefly, a rational map that is defined everywhere) that preserves the base point (the point at infinity). Two elliptic curves are said to be isogenous if there is a nonzero isogeny between them.

Isogenies are group homomorphisms between two elliptic curves (see [Sil09, p.71 Theorem 4.8]). Each isogeny induces a map called the pullback

$$\begin{aligned} \phi^* : \overline{K}(E_2) &\to \overline{K}(E_1) \\ F &\mapsto F \circ \phi \end{aligned}$$

where $\overline{K}(E_i)$ is the field of rational functions $F(x,y) = f(x,y)/g(x,y)$ such that f and g have the same homogeneous degree, $g(x,y) \notin I(E_i)$ and two functions f_1/g_1 and f_2/g_2 are identified if $f_1 g_2 - f_2 g_1 \in I(E_i)$ and $I(E_i)$ is given by

$$I(E_i) = \{F \in \overline{K}[x,y] : F(x,y) = 0 \text{ for all } (x,y) \in E_i\}.$$

Definition 1.2.4. The degree of an isogeny is

$$\deg \phi = \begin{cases} 0 & \text{if } F = 0 \\ [\overline{K}(E_1) : \phi^* \overline{K}(E_2)] & \text{otherwise.} \end{cases}$$

A p-isogeny is a degree p isogeny.

When the field extension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is separable, we have that $\deg\phi = \#\ker\phi$ (a reminder that this holds when $\mathrm{char}K = 0$). To be more concrete, if $\phi : E_1 \to E_2$ is an isogeny defined over a field K and E_1, E_2 are elliptic curves defined over K, as outlined in [Was08, p.387], we can define rational functions f_1 and f_2 defined over $K[x]$ such that

$$(x_2, y_2) = \phi((x_1, y_1)) = (f_1(x_1), y_1 f_2(x_1))$$

holds for all but finitely many points $(x_1, y_1) \in E_1$ We proceed to write $f_1(x) = \frac{p(x)}{q(x)}$ and then we could have defined the degree of ϕ as

$$\deg(\phi) = \max\{\deg(p(x)), \deg(q(x))\}.$$

The first definition has the benefit of being more general but the downfall of being far more abstract and often harder to work with in practice. To see the connection between definitions, let $\pi : E \to E/\{\pm 1\} \cong \mathbb{P}^1$ be the map given by $\pi((x, y)) = x$ [Sil07, Chapter 6]. Consider the following commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1 & \xrightarrow[f_1]{} & \mathbb{P}^1 \end{array}$$

Now the bottom map in the diagram is the function f_1 with the exception of the point at infinity. Now, as degrees are multiplicative, we have

$$\deg(\pi)\deg(\phi) = \deg(\pi \circ \phi) = \deg(f_1 \circ \pi) = \deg(f_1)\deg(\pi)$$

and so $\deg(f_1) = \deg(\phi)$ and $\deg(f_1)$ is the degree in terms of algebraic geometry (just as we defined it above for elliptic curves). Analyzing the bottom map, it is now easy to see that the degree in the abstract sense is the same as the second definition above.

There is one more invariant we will need and that's the conductor of an elliptic curve. This value measures arithmetic information about our elliptic curve in ways similar to how the discriminant measures arithmetic information. This is an isogeny invariant. For simplicity, I will give the definition only over $\mathbb{Q}$ and direct the reader to [Sil94] for a more general treatment.

Definition 1.2.5. The conductor of an elliptic curve $E/\mathbb{Q}$ is the integer

$$N = \prod_p p^{f_p}$$

where the product is over all primes and

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The value δ_p is sometimes called the wild part of the conductor.

The exact definition of δ_p is a bit clunky and takes us astray from our real goal which is to compute the conductor. I will however mention a formula due to Ogg and in the characteristic 2 case by Saito which helps compute this value. Again since this is not entirely relevant to the overall discussion I will only state the theorem.

Theorem 1.2.6 (Ogg-Saito Formula)**.** *[Ogg67][Sai88] Let $E/\mathbb{Q}$ be an elliptic curve. Then the exponent f_p of the prime p in the conductor is given by*

$$f_p = v_p(\Delta_{\min}) - c_p + 1$$

where c_p is the number of components (without counting multiplicities) of the singular fibre of the Néron minimal model for E at p.

Again to go into details on the latter part will take us too far astray though I direct the interested reader for details on Néron models or conductors to either [Mil06] or [Sil94]. For now, I note that $f_p \leq v_p(\Delta_{\min})$ is a consequence of the above theorem so the conductor divides the minimal discriminant. It should be noted that $\delta_p = 0$ whenever $p \geq 5$ as is given by the following upper bound due to a result of Lockhart-Rosen-Silverman [LS93] and Brumer-Kramer [BK94].

Theorem 1.2.7. *[Sil94, p.385] Let $K/\mathbb{Q}_p$ be a local field with normalized valuation v_K (so that $v_K(p)$ is the ramification index of $K/\mathbb{Q}_P$) and let E/K be an elliptic curve. Then the exponent of the conductor of E/K is bounded by*

$$f \leq 2 + 3v_K(3) + 6v_K(2)$$

and this bound is best possible, that is, some elliptic curve E/K attains the aforementioned bound.

Despite all these technicalities, the actual value of the conductor can be computed very simply using an algorithm due to Tate [Tat75]. In fact, since then the work has been reduced even further to simply checking congruence conditions of the coefficients in most cases

[Pap93][3] or the simplified formulas when your curve has rational two torsion [Mul06]. For a given fixed elliptic curve, the value can be computed either in MAGMA [BCP97] or Sage [S+14].

Summarizing the above, we see that for an elliptic curve over the rationals we have for $p \geq 5$ and $E/\mathbb{Q}$ an elliptic curve with conductor $N = \prod_p p^{f_p}$

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has bad reduction at } p. \end{cases}$$

Further, we must have that $v_2(N) \leq 8$, $v_3(N) \leq 5$. We say that the curve is semi-stable if the conductor is square free, that is, our elliptic curve has only good or multiplicative reduction.

Ideally we would like to apply Tate's algorithm to general elliptic curves where the coefficients depend on solutions to Diophantine equations. However computer algebra software currently cannot perform this task abstractly. One way to compute these values is through the following lemma.

Lemma 1.2.8. *[BCDY14] Suppose E and E' are elliptic curves given by the equations*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

where a_i and a'_i lie in a discrete valuation ring $\mathcal{O}$ with valuation v and uniformizer π. Suppose that

$$\max\{v(\Delta_E), v(\Delta_{E'})\} \leq 12k$$

for some positive integer k. Suppose further that $v(a_i - a'_i) \geq ik$ for $i \in \{1, 2, 3, 4, 6\}$. Then

1. *If the reduction type of E' is not $I^*_{m'}$ for $m' > 2$, then the reduction type of E is the same as the reduction type of E'. In this case $v(N_E) = v(N_{E'})$.*

2. *If the reduction type of E' is $I^*_{m'}$ for $m' > 2$, then the reduction type of E is I^*_m for some $m > 2$.*

3. *In particular, E has good reduction if and only if E' has good reduction.*

This gives us a way to compute the conductor of abstract elliptic curves by looking at all possible residue classes of the parameters modulo prime powers. Since we will need this

[3]Errata in [Pap93]: In the column labeled *Equation non minimale* of table IV, the first column should read $[4, 6, \geq 12]$ not $[4, 6, 12]$.

notation for our next example and throughout the paper, we define now for any integers M and Q, the radical of M excluding Q to be

$$\mathrm{rad}_Q(M) := \prod_{\substack{p \nmid Q \\ p \mid M}} p$$

where the product runs over primes p. Succinctly, these are the primes dividing M that do not share a prime divisor with Q.

Example 1.2.9. Let $a^p+b^p = c^p$ for some prime $p \geq 5$ and some nontrivial primitive solution (a, b, c). We assume that $2 \mid b$ and that $a \equiv -1 \pmod 4$. Let $y^2 = x^3 + (b^p - a^p)x^2 - a^p b^p x$ be an elliptic curve associated to this solution. We wish to compute the conductor N of this elliptic curve. The discriminant and c_4 invariant of this elliptic curve are given by

$$\Delta = 2^4(abc)^{2p}, \qquad c_4 = 16(c^{2p} - a^p b^p).$$

In fact, using [Kna92, p.291], we can show that the above model is guaranteed to be minimal at all primes except possibly at 2. To show this, notice that the discriminant shares primes with $\mathrm{rad}_2(abc)$. Thus, we are only concerned about the minimality with these primes. For each of these primes, notice that these primes cannot divide c_4 since (a, b, c) was a primitive solution. Thus, the equation is minimal at all primes outside of 2. It turns out that the equation is not minimal at 2 and the actual minimal discriminant is given by $\Delta_{\min} = 2^{-8}(abc)^{2p}$ but we will not use this fact here.

For the odd primes, we see that the above equation has bad reduction at the primes dividing $\mathrm{rad}_2(abc)$. As these primes do not divide c_4, we see from [Sil09, p.45] that these primes have bad multiplicative reduction. Thus, we have that $\mathrm{rad}_2(abc) \mid N$. For the prime 2, we use the tables in [Mul06] since our curve has rational two torsion to see that the conductor is $N = 2\mathrm{rad}_2(abc)$ and in fact a minimal model at 2 is given by

$$y^2 + xy = x^3 + \left(\frac{b^p - a^p - 1}{4}\right)x^2 - \left(\frac{a^p b^p}{4}\right)x.$$

We note that the tables there would also give the conductor in all cases.

The last major piece of discussion for elliptic curves is the trace of Frobenius. Let $E/\mathbb{Q}$ be an elliptic curve and ℓ a prime of good reduction. The value

$$a_\ell(E) = \ell + 1 - |E(\mathbb{F}_\ell)|$$

is called the trace of Frobenius for the elliptic curve E. Traces, from a linear algebra viewpoint, correspond to the sum of entries on the diagonal of a matrix. In the form written

above, we see no direct relationship to linear algebra. In its simplest form, one can see that this is the trace of a matrix as follows. Let $q = p^n$ be a prime for this section and define the Frobenius map $\phi_q \in G_{\mathbb{F}_q} := \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ as

$$\phi_q((x, y)) = (x^q, y^q).$$

An important fact is that this map has degree q [Sil09, p.25]. We will be most interested in the case when $q = p$ and so we drop the $q = p^n$ notation.

Now, let ℓ be an odd prime for simplicity and suppose that $p \nmid \ell N_E$. Then p is a prime of good reduction and so we can consider E defined over $\mathbb{F}_p$. Now, ϕ_p acts on the ℓ torsion group, denoted by $E[\ell] = \{P \in E(\overline{\mathbb{F}}_p) : [\ell]P = 0\}$ and $[\ell]P = P + P + ... + P$ a total of ℓ times. If we pick a basis for $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ [Sil09, p.86], say P and Q, then we have $\phi_p(P) = aP + bQ$ and $\phi_p(Q) = cP + dQ$. Then we have that

$$(\phi_p)_\ell = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and it is here that we see that $\mathrm{Trace}((\phi_p)_\ell) \equiv a_p \pmod{\ell}$ and $\det((\phi_p)_\ell) \equiv p \pmod{\ell}$ [Was08, p.102]. In fact the above holds with p replaced by arbitrary prime powers q and ℓ replaced by any integer m with $\gcd(m, q) = 1$. The above is enough for us to get what we want, however I would like to delve a bit deeper into Galois representations in order to bring to surface some of the underlying ideas.

Let $E/\mathbb{Q}$ be an elliptic curve. We define the representation attached to an elliptic curve as follows. First let $\mathrm{Ta}_\ell(E) = \varprojlim E[\ell^n]$ denote the ℓ-adic Tate module where the projection maps are multiplication by ℓ. Now, notice that any σ inside the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on any $E[\ell^n]$ and in fact takes ℓ^n-torsion points to ℓ^n-torsion points. Hence, this σ induces an element of $\mathrm{Aut}(\mathrm{Ta}_\ell(E))$. By picking a compatible basis for each $E[\ell^n]$, that is a collection $\{(P_n, Q_n)\}_{n \in \mathbb{Z}^+}$ such that $\ell P_{n+1} = P_n$ and $\ell Q_{n+1} = Q_n$, we can get an isomorphism from $\mathrm{Ta}_\ell(E)$ to two copies of the ℓ-adic integers denoted by $\mathbb{Z}_\ell^2$. This naturally sits inside $\mathbb{Q}_\ell^2$ and so combining all this gives a representation:

$$G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{Ta}_\ell(E)) \cong \mathrm{Aut}(\mathbb{Z}_\ell^2) \hookrightarrow \mathrm{Aut}(\mathbb{Q}_\ell^2) \cong \mathrm{GL}_2(\mathbb{Q}_\ell).$$

This map $\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is called the representation associated to the elliptic curve E. We will also use the same symbol to denote the action from $G_{\mathbb{Q}}$ to $\mathrm{Aut}(\mathrm{Ta}_\ell(E))$. Next, we need the following definition.

Definition 1.2.10. We say $\rho_{E,\ell}$ is unramified at p if

$$I_{\mathfrak{p}} := \{\sigma \in D_{\mathfrak{p}} : \sigma(x) \equiv x \pmod{p} \forall x \in \bar{\mathbb{Z}}\} \subseteq \ker(\rho)$$

for any maximal ideal $\mathfrak{p} \in \bar{\mathbb{Z}}$ over p where $D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ is the decomposition group and $I_{\mathfrak{p}}$ is called the inertia group.

The decomposition group above is of particular importance to us. As the decomposition group sits inside $G_{\mathbb{Q}}$, it has a natural action on $\mathrm{Aut}(E[\ell^n])$ and hence on $\mathrm{Aut}(\mathrm{Ta}_\ell(E))$. Let $p \nmid \ell N_E$ be another prime where N_E is the conductor of E. Then we also have an isomorphism from $E[\ell^n]$ to $\bar{E}[\ell^n]$ where $\bar{E}$ is the reduction of E at the good prime of reduction p as both are isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. This also induces an isomorphism from $\mathrm{Aut}(\mathrm{Ta}_\ell(E))$ to $\mathrm{Aut}(\mathrm{Ta}_\ell(\bar{E}))$.

Each $\sigma \in D_{\mathfrak{p}}$ can act on each number ring $\overline{\mathbb{Z}}/\mathfrak{p}$ via $\sigma(\alpha + \mathfrak{p}) = \sigma(\alpha) + \mathfrak{p}$ since σ fixes $\mathfrak{p}$. As $\overline{\mathbb{Z}}/\mathfrak{p}$ and $\overline{\mathbb{F}_p}$ are both algebraic closures of $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, they are isomorphic[4]. Thus, we can map $\psi : D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ and this map is a surjection [DS05, p.377]. Let ϕ_p be the Frobenius element of $G_{\mathbb{F}_p}$ which is a generator of this group. Then any preimage of ϕ_p in $D_{\mathfrak{p}}$ is denoted by $\mathrm{Frob}_{\mathfrak{p}}$ and is called an absolute Frobenius element over $\mathfrak{p}$. Notice that this element is only well defined up to the kernel of ψ which is equal to $I_{\mathfrak{p}}$. Thus, whenever the representation $\rho_{E,\ell}$ is unramified , we see that $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ is a value that is equal for any preimage choice of ϕ_p. Similarly to the above, the group $G_{\mathbb{F}_p}$ also acts on $\bar{E}[\ell^n]$ and hence on $\mathrm{Aut}(\mathrm{Ta}_\ell(\bar{E}))$ by a map we shall denote via $\bar{\rho}_{\bar{E},\ell}$. Combining all these actions gives the following commutative diagram

$$\begin{array}{ccc} D_{\mathfrak{p}} & \longrightarrow & E[\ell^n] \\ \psi \downarrow & & \downarrow \cong \\ G_{\mathbb{F}_p} & \longrightarrow & \bar{E}[\ell^n] \end{array}$$

which induces the following commutative diagram

$$\begin{array}{ccc} D_{\mathfrak{p}} & \xrightarrow{\rho_{E,\ell}} & \mathrm{Aut}(\mathrm{Ta}_\ell(E)) \\ \psi \downarrow & & \downarrow \cong \\ G_{\mathbb{F}_p} & \xrightarrow{\bar{\rho}_{\bar{E},\ell}} & \mathrm{Aut}(\mathrm{Ta}_\ell(\bar{E})) \end{array}$$

From the diagrams, since the right most map is an isomorphism, we must have that $\ker(\psi) = I_{\mathfrak{p}} \subseteq \ker(\rho_{E,\ell})$ and so the representation is unramified for all primes $p \nmid \ell N_E$. As

[4]Alternatively let $\mathfrak{p}$ be the kernel of the reduction map from $\overline{\mathbb{Z}}$ to $\overline{\mathbb{F}}_p$.

the map is commutative, we see that $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})) = \mathrm{tr}(\bar{\rho}_{E,\ell}(\phi_p))$. To evaluate the latter, we use the Weil pairing. Let (P, Q) be a basis for $\mathrm{Aut}(\mathrm{Ta}_\ell(\bar{E}))$. The isogeny theorem [Sil09, p.91] tells us that this $\bar{\rho}_{E,\ell}(\phi_p) =: \phi_{p,\ell}$ must come from an isogeny on $\bar{E}$ which we also denote by ϕ_p. This map is given by $\phi_p(X, Y) = (X^p, Y^p)$ for points in $\bar{E}$. Next we use the Weil pairing [Sil09, p.92-99] on $E[\ell^n]$ to see that

$$\begin{aligned}
e_{\ell^n}(P,Q)^{\deg(\phi_p)} &= e_{\ell^n}([\deg(\phi_p)]P, Q) && \text{by bilinearity of } e_\ell \\
&= e_{\ell^n}(\hat{\phi}_{p,\ell}\phi_{p,\ell}P, Q) && \text{by definition of dual} \\
&= e_{\ell^n}(\phi_{p,\ell}P, \phi_{p,\ell}Q) && \text{by property of Weil Pairing} \\
&= e_{\ell^n}(aP + bQ, cP + dQ) && \text{provided } \phi_{p,\ell} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ on the basis } (P, Q) \\
&= e_{\ell^n}(P,Q)^{ad-bc} && \text{since Weil pairing is bilinear and alternating} \\
&= e_{\ell^n}(P,Q)^{\det(\phi_{p,\ell})} && \text{by definition from above.}
\end{aligned}$$

This means that $\deg(\phi_p) \equiv \det(\phi_{p,\ell}) \pmod{\ell^n}$ for any positive integer n. Thus in particular, we have that $\deg(\phi_p) = \det(\phi_{p,\ell})$ and in particular that $\det(\phi_{p,\ell})$ is an integer. One can also show that this ϕ_p acting on $\bar{E}$ has degree p and so $\det(\phi_{p,\ell}) = p$. Now, it is immediate that for any two by two matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we have

$$\mathrm{tr}(M) = a + d = 1 + (ad - bc) - ((1 - a)(1 - d) - bc) = 1 + \det(M) - \det(I - M).$$

Thus, we have

$$\begin{aligned}
\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})) &= \mathrm{tr}(\bar{\rho}_{E,\ell}(\phi_p)) \\
&= 1 + \det(\bar{\rho}_{E,\ell}(\phi_p)) - \det(I - \bar{\rho}_{E,\ell}(\phi_p)) \\
&= 1 + p - \#E(\mathbb{F}_p)
\end{aligned}$$

with the last equality following from using the same argument above to see that

$$\deg([1] - \phi_p) = \det(I - \bar{\rho}_{E,\ell}(\phi_p))$$

and as the map $[1] - \phi_p$ is separable by [DS05, p.320], we get that

$$\deg([1] - \phi_p) = \deg_{\mathrm{sep}}([1] - \phi_p) = \ker([1] - \phi_p) = \#E(\mathbb{F}_p).$$

Though the proof of the exact equality above is a bit scant, it is clear at the very least that defining the trace of Frobenius in this manner does indeed give an integer despite *a priori* that it is only clear that you get an element in $\mathbb{Z}_\ell$ and not necessarily in $\mathbb{Z}$.

A final note is that isogenous elliptic curves do in fact have equal trace of Frobenius values [Kna92, p.366], a statement which can be stated as isogenous elliptic curves have equal L-series.

1.3 Modular Forms

The other key objects in the Modularity Theorem, the theorem for which these attacks on Diophantine equations is based, are modular forms. These are functions on the complex upper half plane $\mathbb{H}$ and so are, by nature, analytic objects. In the previous section, we saw a treatment of elliptic curves that was very algebraic in nature. This joining of analysis and algebra is one of the components that makes the Modularity Theorem such an incredible feat of mathematics. We begin by describing a modular form.

Definition 1.3.1. Let $\mathrm{SL}_2(\mathbb{Z}) = \left\{ M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) : \det(M) = 1 \right\}$. Then a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$ where

$$\Gamma(N) = \left\{ M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : M \cong \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Definition 1.3.2. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k with respect to Γ if

1. f is weight-k invariant under Γ, meaning $f[\gamma]_k = f$ for all $\gamma \in \Gamma$ where

$$f[\gamma]_k(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau))$$

   and $j\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tau \right) := c\tau + d.$

2. $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ (that is, f is holomorphic at all cusps, points in $\mathbb{Q} \cup \{\infty\}$).

The first condition above gives modular forms a periodicity property as mentioned below. The second condition above actually gives us other important arithmetic information given by Laurent series. As a congruence subgroup $\Gamma \supset \Gamma(N)$ contains $\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}$, there must be some minimal positive integer h such that $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \Gamma$. For this h, we have that $f(\tau + h) = f(\tau)$ by the weight-k invariance. The theory of Fourier series thus applies here and we see that

our f has a Fourier series expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q_h^n \qquad q_h = e^{2\pi i \tau / h}$$

The notation here should be reminiscent of the trace of Frobenius for elliptic curves. This is no accident and we shall explore this in the next section. If in addition to the above definition of a modular form, we have that $a_0(f[\alpha]_k) = 0$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then say that our modular form f is a cusp form. This is equivalent to f being holomorphic at ∞ and the Fourier series expansion of f satisfies $|a_n(f)| \leq Cn^r$ for some constants C and r [DS05, p.200]. Our particular interest will be with weight 2 modular forms over the congruence subgroup

$$\Gamma_1(N) = \left\{ M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : M \cong \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N \right\}$$

where the $*$ denotes an arbitrary element. For future reference, another often used congruence subgroup is

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) = \left\{ M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : M \cong \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod N \right\}.$$

To define a newform, we will first need to describe the space of oldforms. An oldform colloquially is a form that comes from a lower level than the one you are currently considering. For example, if $M \mid N$ is a proper divisor (that is, $M \neq N$) then $\mathcal{S}_k(\Gamma_1(M)) \subseteq \mathcal{S}_k(\Gamma_1(N))$ and so the modular forms in $\mathcal{S}_k(\Gamma_1(N))$ coming from this subset are old in the sense that if we were listing all modular forms by the size of the level, we already knew they existed.

More precisely, there are two main ways to embed the lower subspace into the bigger one. We have described one way above. For the second way, suppose that $d \mid (N/M)$ is any divisor. Then taking

$$f[\alpha_d]_k(\tau) := \det(\alpha_d)^{k-1} f(\alpha_d \tau) j(\alpha_d, \tau)^{-k} = d^{k-1} f(d\tau)$$

where $\alpha_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$, we see that this embeds a modular form $f \in \mathcal{S}_k(\Gamma_1(M))$ into $\mathcal{S}_k(\Gamma_1(Md))$ which is a subset of $\mathcal{S}_k(\Gamma_1(N))$. This prompts the following definition for the map i_d, which combines the above methods

$$\begin{aligned} i_d : \mathcal{S}_k(\Gamma_1(Nd^{-1})) \times \mathcal{S}_k(\Gamma_1(Nd^{-1})) &\to \mathcal{S}_k(\Gamma_1(N)) \\ (f, g) &\mapsto f + g[\alpha_d]_k. \end{aligned}$$

Thus, we define the space of oldforms to be the following sum of vector spaces

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} := \sum_{p|N} i_p(\mathcal{S}_k(\Gamma_1(Np^{-1})) \times \mathcal{S}_k(\Gamma_1(Np^{-1}))).$$

To define the space of newforms, we need to figure out a complementary space to the space of oldforms. This can be done by using the Petersson inner product. For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and cusp forms $f, g \in \mathcal{S}_k(\Gamma)$, we define an inner product by

$$\langle f, g \rangle := \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\Im(\tau)^k \, d\mu(\tau)$$

where $d\mu(\tau) = \frac{dx\,dy}{y^2}$ is the hyperbolic measure and $V_\Gamma = \int_{X(\Gamma)} d\mu(\tau)$. This measure is $\mathrm{GL}_2^+(\mathbb{Q})$ invariant and the integrand above is continuous, bounded and Γ-invariant. The space of newforms is then defined to be the orthogonal complement of $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ inside $\mathcal{S}_k(\Gamma_1(N))$. Symbolically

$$\mathcal{S}_k(\Gamma_1(N))^{\text{new}} := (\mathcal{S}_k(\Gamma_1(N))^{\text{old}})^\perp.$$

By a newform, we actually mean an element of the space of newforms that is normalized so that the first Fourier coefficient satisfies $a_1(f) = 1$ and that it is an eigenvector for all the Hecke operators T_n and $\langle d \rangle$ (such an element is also called an eigenform). To be brief, the Hecke operators for $f \in \mathcal{S}_k(\Gamma_1(N))$ can be defined by

$$\langle d \rangle f := f \left[\begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \right]_k$$

where $\delta \equiv d \pmod N$ for $d \in \mathbb{Z}$, $\begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N)$ and

$$T_p f := \begin{cases} \displaystyle\sum_{j=0}^{p-1} f \left[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix} \right]_k & \text{if } p \mid N \\ \displaystyle\sum_{j=0}^{p-1} f \left[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix} \right]_k + f \left[\begin{bmatrix} m & n \\ N & p \end{bmatrix} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \right]_k & \text{if } p \nmid N \end{cases}$$

where $mp - nN = 1$. For the second Hecke operator, we can define T_n to be the multiplicative extension of T_p under the additional rule that $T_{p^r} := T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}$.

We have introduced newforms in full generality above however we will be mainly interested in weight two newforms for $\Gamma_0(N)$, that is for the space $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$. This is due to their connection with elliptic curves as we shall soon see. So from here on out, a newform will

refer to a normalized eigenform of $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$. The primary properties of a newform that we will need is that a newform is a q-expansion $f := q + \sum_{n\geq 2} a_n(f)q^n$, that is, a cusp form normalized so that the first coefficient is 1, with the additional property that adjoining all the coefficients to $\mathbb{Q}$ via $K_f = \mathbb{Q}(a_2(f), a_3(f), ...)$ forms a number field that is a finite and totally real extension of $\mathbb{Q}$ [DS05, p.234] and in fact, each of the $a_i(f)$ are algebraic integers. We call the $a_i(f)$ the Fourier coefficients of f. These coefficients satisfy $|a_\ell(f)| \leq 2\sqrt{\ell}$ for prime ℓ. This was Ramanujan's conjecture and was proven by Deligne as a consequence of the Weil Conjectures [Del74] [Del80]. Another important fact is that there are no newforms of level $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60$ which can easily be checked in MAGMA (see [HK98] or [Mar05] for a formula).

1.4 A Modern Approach to Fermat's Last Theorem

Let's first start out by examining the Fermat curve $x^3 + y^3 = z^3$. I want to give a modern proof as to why this curve has no non-trivial rational points via elliptic curves. This will introduce some of the terminology necessary to understanding the ideas behind Wiles' approach to Fermat's Last Theorem. Under the change of coordinates $z \mapsto (y + z/3)$, we see that this curve becomes $x^3 - y^2z - yz^2/3 - z^3/27 = 0$. Homogenizing under $z = 1$ and then performing a change of coordinates to minimal Weierstrass form, we see that this curve is an elliptic curve with form $y^2 = x^3 - 432$. This curve has conductor 27. A check on the Cremona tables [Cre] reveals that the Mordell-Weil Group $E(\mathbb{Q})$ has rank 0 and torsion subgroup of order 3 corresponding to the point $(x, y) = (12, \pm 36)$ and the point at infinity. These points correspond to the points $(1/3, 0)$, $(1/3, -1/3)$ and the point at infinity on the second curve mentioned above and these lastly correspond to the points $(1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)$ on the Fermat curve. Any other point on the Fermat curve would correspond to another rational point on the curve $y^2 = x^3 - 432$ which is impossible and we have thus shown that there are only trivial solutions to the Fermat curve $x^3 + y^3 = z^3$.

The case $n = 3$ above gives an indication of how elliptic curves can be used in the study of Diophantine equations. I now present a solution to Fermat's Last Theorem based on the method derived by Wiles. These notes are a slightly modified version of the notes produced by Samir Siksek in [Coh07b].

In the background of the following will be the Modularity Theorem. This is a statement that rational elliptic curves are in a bijection with rational modular forms. How the proof of Fermat's Last Theorem will work is that we start with a hypothesized nontrivial primitive solution to our Diophantine equation $x^n + y^n = z^n$ say $(x, y, z) = (a, b, c)$. Next, we take this solution and associate to it an elliptic curve called a Frey-Hellegouarch curve. Mapping

the curve under the bijection to modular forms, this form has a few special properties which allow it to conform to the hypothesis of Ribet's level lowering theorem. Level lowering finds an equivalent modular form, in the sense of having a congruence condition between the coefficients modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_f}$, at a lower level that does not depend on (a, b, c). This level is equal to 2 and this is a contradiction since there are no newforms of level 2. We will make all of the above precise in this section. For now, we begin by stating the Modularity Theorem.

Theorem 1.4.1. *(The Modularity Theorem for Elliptic Curves [Wil95] [TW95] [BCDT01]) Let $N \geq 1$ be an integer. Then there is a one to one correspondence $f \mapsto E_f$ between rational weight 2 newforms of level N, that is, normalized eigenforms of $f \in \mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ with rational coefficients and isogeny classes of elliptic curves E defined over $\mathbb{Q}$ and of conductor N. Under this correspondence, for all primes $\ell \nmid N$, $a_\ell(f) = a_\ell(E_f)$.*

As a sanity check, notice that $a_i(f) \in \mathcal{O}_{K_f}$ and since they are rational, we have in fact that $a_i(f) \in \mathbb{Z}$ so the terms above are indeed well defined. This is the amazing merger of two really different mathematical objects unifying them into one statement. One can think of this as a dictionary between languages, swapping between terminologies wherever thinking of the objects in one context is easier than the other.

Definition 1.4.2. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Let f be a weight 2 newform of level N' not necessarily equal to N. We will say that E arises modulo p from f (written $E \sim_p f$) if there exists a prime ideal $\mathfrak{p}$ of K_f above p such that $a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{p}}$ for all but finitely many primes ℓ. If F is an elliptic curve of conductor N', then we also write $E \sim_p F$ to mean $E \sim_p f$ where $F = E_f$ and the f coming from the Modularity Theorem.

It should be noted here that under the second interpretation, we have that $\sim_p$ forms an equivalence relation on elliptic curves. This property implies the following theorem that we will need now and in the subsequent chapters.

Theorem 1.4.3. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Let f be a weight 2 newform of level N' not necessarily equal to N. Assume that $E \sim_p f$. There exists a prime ideal $\mathfrak{p}$ of K_f above p such that for all prime numbers ℓ, we have*

1. *If $\ell \nmid pNN'$, then $a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{p}}$, that is $p \mid N_{K_f/\mathbb{Q}}(a_\ell(f) - a_\ell(E))$.*
2. *If $\ell \,||\, N$ but $\ell \nmid pN'$, then $a_\ell(f) \equiv \pm(\ell + 1) \pmod{\mathfrak{p}}$, that is $p \mid N_{K_f/\mathbb{Q}}(a_\ell(f) \pm (\ell + 1))$.*

where $N_{K_f/\mathbb{Q}}$ denotes the norm map here and throughout this article.

The following is an improvement of the above theorem due to Kraus and Oesterlé [KO92] that will help us remove the cumbersome fact that the above depends on $\ell \nmid p$. The annoyance

comes from the fact that p will usually be an unknown exponent and so having conditions that depend on this exponent is an inconvenience that we can do away with in the special case that the newform is rational (and so corresponds to an elliptic curve).

Theorem 1.4.4. *(Kraus and Oesterlé [KO92]) Let E and F be elliptic curves defined over $\mathbb{Q}$ with conductors N and N' and assume that $E \sim_p F$ as defined above. Then for all prime numbers ℓ, we have*

1. *If $\ell \nmid NN'$, then $a_\ell(E) \equiv a_\ell(F) \pmod{p}$.*
2. *If $\ell \mid\mid N$ but $\ell \nmid N'$, then $a_\ell(F) \equiv \pm(\ell + 1) \pmod{p}$.*

Next we introduce the Level Lowering Theorem of Ribet. This is a simplified modification to suit our specific needs. It turns out that in our situation, we can reduce the general Level Lowering Theorem into the following much easier to state theorem that avoids potential issues at p.

Definition 1.4.5. Define for p a prime number

$$N_p := \frac{N}{\prod\limits_{\substack{q \mid\mid N \\ p \mid v_q(\Delta_{\min})}} q}$$

where the product runs over primes q and $v_q(\Delta_{\min})$ is the q-adic valuation of $\Delta_{\min}$ formally defined as

$$v_q(n) = \begin{cases} \max\{k \in \mathbb{N} : q^k \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0. \end{cases}$$

Reworded, this means $v_q(N) = 1$ and $p \mid v_q(\Delta_{\min})$. This N_p will be the conductor of the level lowered curve. Finally we can state the following.

Theorem 1.4.6. *(Ribet's Level Lowering Theorem) [Rib90] Let E be an elliptic curve defined over $\mathbb{Q}$ and let $p \geq 5$ be a prime number. Assume that there does not exist a p-isogeny (that is, an isogeny of degree p) defined over $\mathbb{Q}$ from E to some other elliptic curve and let N_p be as above. Then there exists a newform f of level N_p such that $E \sim_p f$.*

This theorem in its original form is a statement about modular forms. The Modularity Theorem allows us to pass back and forth from elliptic curves to modular forms. See [Rib90], [Rib94] for the original phrasing. In order to apply Ribet's Level Lowering Theorem, we need to know when a curve has no p-isogeny. It turns out that this work was done by Barry Mazur and is collected in the following theorem. It should be noted that this statement was

actually worded originally as a statement about the irreducibility of the mod p representation associated to an elliptic curve.

Theorem 1.4.7. *(Mazur [Maz78]) Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Then E does not have any p-isogeny if at least one of the following conditions holds:*

1. *$p \geq 17$ and $j(E) \notin \mathbb{Z}[\frac{1}{2}]$*
2. *$p \geq 11$ and N is square free (that is, E is semi-stable).*
3. *$p \geq 5$, N is square free, and $\#E(\mathbb{Q})[2] = 4$.*

The last ingredient in the proof of Fermat's Last Theorem are Frey-Hellegouarch curves. These are elliptic curves that are associated to solutions to Diophantine equations, more specifically, the coefficients of the elliptic curve should be related to the solution of a Diophantine equation. In addition, the minimal discriminant $\Delta_{\min}$ should be able to be written as the product of two factors. One factor should not depend on the solution of the Diophantine equation and the other should be a pth power (that could depend on the solution). We write $\Delta_{\min} = C_0 D^p$. For the primes $p \mid D$, we should also have that E has multiplicative reduction.

We now have enough terminology to give a "black box" proof of Fermat's Last Theorem.

Theorem 1.4.8. *Let $p \geq 5$ be a prime number. The equation $x^p + y^p + z^p = 0$ has no nontrivial primitive solutions.*

Proof. Let (a, b, c) be a nontrivial primitive solution to our equation (that is, a, b, c are pairwise coprime and $abc \neq 0$). Local considerations at 2 show abc is even and so without loss of generality, we can suppose (by changing coordinates if necessary) that b is divisible by 2. Further, suppose $a \equiv -1 \pmod 4$ by possibly modifying the solution to $(-a, -b, -c)$ if necessary[5]. Let E be the following associated Frey-Hellegouarch curve

$$y^2 = x(x - a^p)(x + b^p) = x^3 + (b^p - a^p)x^2 - a^p b^p x$$

Computing the minimal discriminant and the conductor using Tate's algorithm as was done in Example 1.2.9 and computing the N_p value desired in Ribet's Level Lowering Theorem, we have

$$\Delta_{min} = 2^{-8}(abc)^{2p} \qquad N = 2\mathrm{rad}_2(abc) \qquad N_p = 2$$

[5]These conditions, while seemingly not used directly, give a simplification of $v_2(N)$ in the application of Tate's algorithm.

It is here where we need that we have a nontrivial solution for otherwise our curve above has discriminant zero and hence its associated defining equation has repeated roots. Before applying Ribet's theorem, we need to check that E has no p-isogenies. By construction, this curve has full rational 2-torsion and since N is squarefree, we can apply Mazur's Theorem (Theorem 1.4.7) which shows that E has no p-isogenies. By Ribet's Theorem (Theorem 1.4.6), we have that there is a newform of level $N_p = 2$ such that $E \sim_p f$. Notice that there are no newforms at level 2 and so we have a contradiction and thus no solution (a, b, c) can exist. ■

This concludes the proof of Fermat's Last Theorem, omitting the proofs of some very big hammers that we used above. There are a few other theorems that can be important in trying to apply the Modularity Theorem and that are used throughout this thesis. I will include these here. Remember that one of the key ingredients was the absence of p-isogenies. The following theorems can help to determine whether they exist.

Theorem 1.4.9. *Let $E/\mathbb{Q}$ be an elliptic curve such that its pth division polynomial is irreducible. Then E has no p-isogenies.*

Proof. Let P be a point on E. If the pth division polynomial is irreducible, then the denominator of the point $[p]P$ is irreducible. Thus, there are no rational points of order p. By [Sil09, p.72], the kernel of a p-isogeny has size p. This is a contradiction since the isogeny composed with its dual isogeny is the map $[p]$ which as we have shown has no kernel (so if ψ has kernel of size p, then $[p] = \tilde{\psi} \circ \psi$ has kernel of size at least p which is a contradiction). ■

Theorem 1.4.10. *(Diamond-Kramer) [DK95] Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. If $v_2(N) = 3, 5,$ or 7, then E does not have any p-isogeny for p an odd prime.*

In the cases where we can reduce to a curve with complex multiplication, the following result might aid in further simplifying.

Theorem 1.4.11. *Let E and F be two elliptic curves defined over $\mathbb{Q}$. Assume that F has complex multiplication by some imaginary quadratic field K and that $E \sim_p F$ for some prime p. Then*

1. *(Halberstadt-Kraus via Momose)[HK98] [Mom84] If $p = 11$ or $p \geq 17$ and p splits in L, then the conductors of E and F are equal.*

2. *(Darmon-Merel)[DM97] If $p \geq 5$, p is inert, and E has a $\mathbb{Q}$-rational subgroup of order 2 or 3, then $j(E) \in \mathbb{Z}[\frac{1}{p}]$. If in addition, $p^2 \nmid N$ and $p \nmid N'$, where N is the conductor of E and N' is the conductor of F, then we have $j(E) \in \mathbb{Z}$.*

Next, the following theorem whose proof can be found in [Coh07b, p.510] follows mainly as a result of Theorem 1.4.4 and can help with bounding the exponent.

Theorem 1.4.12. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let $t \in \mathbb{Z}$ be an integer dividing the rational torsion subgroup of E. Let f be a newform of level N'. Lastly, let ℓ be a prime number such that $\ell^2 \nmid N$ and $\ell \nmid N'$. Define*

$$S_\ell = \{a \in \mathbb{Z} : -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell} \quad \textit{and} \quad a \equiv \ell + 1 \pmod{t}\},$$

$$\delta_f = \begin{cases} \ell & \textit{if } f \textit{ is not rational} \\ 1 & \textit{if } f \textit{ is rational,} \end{cases}$$

$$B_\ell(f) = \delta_f \mathcal{N}_f((\ell+1)^2 - a_\ell(f)) \prod_{a \in S_\ell} \mathcal{N}_f(a - a_\ell(f))$$

where $\mathcal{N}_f$ denotes the norm on $K_f/\mathbb{Q}$. If $E \sim_p f$ then $p \mid B_\ell(f)$.

An important question is when the above theorem can give you a bound on the exponent, that is, when $B_\ell(f) \neq 0$ for at least some values of ℓ. This occurs whenever your newform f is one of the following:

1. Irrational.
2. Rational, t is prime or equal to 4 and for every elliptic curve F isogenous to E_f, we have $t \nmid \#E_{\text{tor}}(\mathbb{Q})$.
3. Rational, $t = 4$ and for every elliptic curve F isogenous to E_f, we have F does not have full 2 torsion.

In these cases, then in fact $B_\ell(f)$ is nonzero for infinitely many values of ℓ.

1.5 Where Do Frey-Hellegouarch Curves Come From?

There still leaves one quite important question and that is "Where do Frey-Hellegouarch curves come from?" I will try to give an idea of where certain curves come from by motivating the construction of the curves used in this thesis. An excellent source of this information can be found in [Kra99]. I will give a brief summary.

First we discuss the Frey-Hellegouarch curve used in Fermat's Last Theorem, namely

$$y^2 = x(x - a^p)(x + b^p).$$

This curve was first noticed by Yves Hellegouarch [Hel75] while examining points of finite order on elliptic curves. He was one of the first people to take a solution to a Diophantine equation and associate to it an elliptic curve. In 1986, Gerhard Frey [Fre86] looked at the same curve and noticed that it would have some strange properties should it exist (see [Fre09]

for a recent recanting of this idea). This was later formalized by Kenneth Ribet [Rib90]. He proved a theorem that is now known as Ribet's Level Lowering theorem. This associates to a modular form at a level containing a large pth power, a modular form at a much smaller level (essentially removing the pth power). His result would lead to a proof of Fermat's Last Theorem if one could prove that there was a correspondence between elliptic curves and modular forms. This was known as the Taniyama-Shimura-Weil Conjecture. In 1995, Andrew Wiles [Wil95] proved that this conjecture was true for semi-stable elliptic curves and this was enough to close the proof. This conjecture is now known as the Modularity Theorem and has since been proven to be true [Wil95] [TW95] [BCDT01].

Many of the other Frey-Hellegouarch curves are based on the above Frey-Hellegouarch curve. For a Frey-Hellegouarch curve of the form

$$Y^2 = X(X - A)(X + B) = X^3 + (B - A)X^2 - ABX,$$

we saw at the beginning of this section that $\Delta = 2^4 A^2 B^2 (B + A)^2$. In the situation above, we let $A = a^p$ and $B = b^p$. Then since $a^p + b^p = c^p$ we could make the replacement and see that the discriminant has a large pth power dividing it. Remember that to use the above method we need the following:

1. The Frey-Hellegouarch curve should depend on our solution to a Diophantine equation.
2. The minimal discriminant $\Delta_{\min}$ should be of the form CD^p where C does not depend on the solution to a Diophantine equation.
3. For the primes $p \mid D$, we should also have that E has multiplicative reduction.

Let's try the technique on the Diophantine equation $x^3 + y^3 = Cz^p$. We consider factoring the left hand side over $\mathbb{Q}(\zeta_3)$ (or equivalently over $\mathbb{Q}(\sqrt{-3})$) where $\zeta_3 = \frac{-1-\sqrt{-3}}{2}$ is a third root of unity. This gives us

$$x^3 + y^3 = (x + y)(x^2 + xy + y^2) = (x + y)(x + \zeta_3 y)(x + \zeta_3^2 y) = Cz^p$$

Now these factors are coprime [BS66, p.157] and the class number of $\mathbb{Q}(\zeta_3)$ is 1 which allows us to write $x + \zeta_3^j y = c_j z_j^p$ for $j \in \{0, 1, 2\}$ where $c_0 c_1 c_2 = C$ are coprime factors and $z_0 z_1 z_2 = z$. Now, if we can find factors γ_0, γ_1 and γ_2 such that

$$(x + y)\gamma_0 + (x + \zeta_3 y)\gamma_1 + (x + \zeta_3^2 y)\gamma_2 = 0$$

then substituting the above yields

$$c_0 z_0^p \gamma_0 + c_1 z_1^p \gamma_1 + c_2 z_2^p \gamma_2 = 0$$

and this should remind us of the original Frey-Hellegouarch curve we used above. Thus, we search for values of γ_j that make the above work and then see if we get a Frey-Hellegouarch curve. The above equation can be solved provided the following system is satisfied

$$\gamma_0 + \gamma_1 + \gamma_2 = 0$$
$$\gamma_0 + \zeta_3\gamma_1 + \zeta_3^2\gamma_2 = 0$$

Since $1 + \zeta_3 + \zeta_3^2$ and $\zeta_3^3 = 1$, we see that $\gamma_0 = 1$, $\gamma_1 = \zeta_3$ and $\gamma_2 = \zeta_3^2$ gives an admissible solution. Inserting this information and letting

$$A := (x + \zeta_3 y)\gamma_1 = \zeta_3(x + \zeta_3 y) \qquad B := (x + \zeta_3^2 y)\gamma_2 = \zeta_3^2(x + \zeta_3^2 y)$$

we have that the above Frey-Hellegouarch curve becomes

$$Y^2 = X^3 + (B - A)X^2 - ABX = X^3 + ((\zeta_3^2 - \zeta_3)(x - y))X^2 - \frac{x^3 + y^3}{x + y}X.$$

Since $\zeta_3^2 - \zeta_3 = -2\zeta_3 - 1 = \sqrt{-3}$, the above elliptic curve is not rational. However, we can perform a quadratic twist over $\mathbb{Q}(\sqrt{-3})$ by $(-3)^{1/4}$. This is done by sending $(X, Y) \mapsto (X, (-3)^{1/4})$, multiplying through by $(-3)^{3/2}$ and then relabeling $-3Y$ as $\tilde{Y}$ and $(-3)^{1/2}X$ as $\tilde{X}$. Performing these operations gives us the curve defined by

$$\begin{aligned}
(-3)^{1/2}Y^2 &= X^3 + (-3)^{1/2}(x - y)X^2 - \frac{x^3 + y^3}{x + y}X \\
(-3)^2Y^2 &= (-3)^{3/2}X^3 + (-3)^2(x - y)X^2 - (-3)^{3/2}\frac{x^3 + y^3}{x + y}X \\
(-3Y)^2 &= ((-3)^{1/2}X)^3 - 3(x - y)((-3)^{1/2}X)^2 + 3\frac{x^3 + y^3}{x + y}((-3)^{1/2}X) \\
\tilde{Y}^2 &= \tilde{X}^3 - 3(x - y)\tilde{X}^2 + 3\left(\frac{x^3 + y^3}{x + y}\right)\tilde{X}
\end{aligned}$$

or, if we like, we can shift the above curve so that the 2-torsion point is at $y - x$ via $\tilde{X} \mapsto \tilde{X} + x - y$ and get the curve

$$\tilde{Y}^2 = \tilde{X}^3 + 3xy\tilde{X} + x^3 - y^3$$

It is this curve used in [BLM11] and [Mul06] and we will use this curve later in this thesis. We can perform the same computation with $x^5 + y^5 = Cz^p$. Let's factor the left hand side over the totally real field $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ (or equivalently over $\mathbb{Q}(\sqrt{5})$). Denote by $\alpha = \zeta_5 + \zeta_5^{-1} = \frac{-1+\sqrt{5}}{2}$ (so here we choose the primitive fifth root so that this works) and $\bar{\alpha} = \frac{-1-\sqrt{5}}{2}$. Then factoring

gives

$$x^5+y^5=(x+y)(x^4-x^3y+x^2y^2-xy^3+y^4)=(x+y)(x^2+\alpha xy+y^2)(x^2+\bar{\alpha}xy+y^2)=Cz^p.$$

Similar to the above, we solve

$$(x+y)^2\gamma_0+(x^2+\alpha xy+y^2)\gamma_1+(x^2+\bar{\alpha}xy+y^2)\gamma_2=0$$

where the square on the linear term above aids with the algebra. A solution to the above is given by

$$\gamma_0=1 \qquad \gamma_1=\bar{\alpha} \qquad \gamma_2=\alpha.$$

Setting

$$A:=\bar{\alpha}(x^2+\alpha xy+y^2) \qquad B:=\alpha(x^2+\bar{\alpha}xy+y^2)$$

and substituting into our Frey-Hellegouarch curve gives

$$\begin{aligned} Y^2=X^3+(B-A)X^2-ABX &= X^3+(\alpha-\bar{\alpha})(x^2+y^2)X^2-\alpha\bar{\alpha}\frac{x^5+y^5}{x+y}X. \\ &= X^3+\sqrt{5}(x^2+y^2)X^2+\frac{x^5+y^5}{x+y}X. \end{aligned}$$

As before, twisting at $5^{1/4}$ yields

$$\tilde{Y}^2=\tilde{X}^3+5(x^2+y^2)\tilde{X}^2+5\left(\frac{x^5+y^5}{x+y}\right)\tilde{X}.$$

To extend this idea further, [Fre10, Chapter 3] has used a technique similar to the case with signature $(5,5,p)$ above. He exploits the fact that $\mathbb{Q}(\zeta_5+\zeta_5^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_5)$ and generalizes this idea to curves with signature (r,r,p). He then further uses Hilbert modularity to get his correspondence between elliptic curves over a totally real field and Hilbert modular forms as was proven by Khare and Wintenberger [KW09a] [KW09b]. This thesis does not go into details of the methods of Hilbert modularity however I did want to mention that this would be a source for more interesting problems in the future.

At this time, I would like to record some more results in the same spirit as those mentioned above here for use later.

1.6 Ternary Fermat-Type Diophantine Equations

Here I describe the kinds of arguments necessary to completely solve certain types of Fermat equations. These arguments will also be used in the following chapters. Please note that some of the notation used here involving variables is used only for the scope of this section. To start, we will solve the Diophantine equation

$$Ax^p + By^p + z^p = 0 \tag{1.1}$$

where $p \geq 5$ is prime and Ax, By and z are non-zero pairwise coprime integers and $R := AB = 2^a 5^b$. We start by assuming that (x, y, z, p) is a solution to the equation defined by 1.1. Without loss of generality, we may suppose that $v_q(R) < p$ for all primes q since otherwise we have via the coprime condition that one of A or B is divisible by q^p and so can be brought into the corresponding x^p or y^p term. Without loss of generality, we may also assume that $By^p \equiv 0 \pmod 2$ and that $Ax^p \equiv -1 \pmod 4$. We can associate to this curve a corresponding Frey-Hellegouarch curve given by

$$E : Y^2 = X(X - Ax^p)(X + By^p)$$

Using Tate's algorithm (see [Coh07b, p.542], [Sil94, p.364-368], [Pap93], [Mul06]), we see that this curve has minimal discriminant

$$\Delta_{\min} = \begin{cases} 2^4 R^2 (xyz)^{2p} & \text{if } 16 \nmid By^p \\ 2^{-8} R^2 (xyz)^{2p} & \text{if } 16 \mid By^p \end{cases}$$

and conductor $N = 2^\alpha \mathrm{rad}_2(Rxyz)$ where α is given by

$$\alpha = \begin{cases} 1 & \text{if } v_2(R) = 0,\ 1 \leq v_2(R) \leq 4 \text{ and } y \text{ is even, or } v_2(R) \geq 5 \\ 0 & \text{if } v_2(R) = 4 \text{ and } y \text{ is odd} \\ 3 & \text{if } 2 \leq v_2(R) \leq 3 \text{ and } y \text{ is odd} \\ 5 & \text{if } v_2(R) = 1 \text{ and } y \text{ is odd.} \end{cases}$$

Next we want to apply Ribet's Theorem first verifying that our curve has no p-isogenies. When α above equals 0 or 1, we can use Theorem 1.4.7 by noting that $p \geq 5$, N is square free and 4 divides $|E_{\mathrm{tor}}(\mathbb{Q})|$ (since it is factored into linear terms). When α equals 3 or 5, we can use Theorem 1.4.10 to see that E has no p-isogenies for any odd prime p. Hence, we can apply level lowering and find a newform $f \in S_2^{\mathrm{new}}(\Gamma_0(N_p))$ where $N_p = 2^\alpha \mathrm{rad}_2(R)$. As $R = 2^a 5^b$ we have that $\mathrm{rad}_2(R) = 1$ or 5.

Now, if $\alpha = 0$ or 1, we have that $N_p \in \{1, 2, 5, 10\}$ which is a contradiction since there are no newforms at these levels. Thus, we may suppose that y is odd. If $\alpha = 3$ and $b = 0$ then $N_p = 8$ and that is also a contradiction since there are no newforms at level 8. If $\alpha = 3$ but $b \geq 1$ then we reduce to a curve of level $N_p = 40$ of which there is one such isogeny class. This gives an obstruction which the method cannot overcome. These obstructions are often the difficulty when solving problems with this method.

The last case is when $\alpha = 5$. This occurs when $a = 1$. If $b = 0$, then $N_p = 32$ and there is one curve at level 32. A look at the Cremona tables shows us that this curve has complex multiplication by $\mathbb{Z}[i]$. Now we use Theorem 1.4.11. Note that the j-invariant for the Frey-Hellegouarch curve above is given by

$$j(E) = \frac{2^8(z^{2p} - x^p y^p)^3}{(xyz)^p}.$$

To start, we may suppose that $p \neq 5$ or 13 since these cases were done by Dénes [Dén52] on the equation $x^p + y^p = 2z^p$. We proceed in cases.

Case 1: p is inert in $\mathbb{Z}[i]$. This occurs when $p \equiv 3 \pmod 4$. Recall that here x, y, z are all odd. Notice that if q is a prime divisor of one of these three terms, then as x, y, z are pairwise coprime, the prime q cannot divide the numerator. So the j-invariant is not an integer. As p is not 2 and we have already considered the case $p = 5$, we know that $p \nmid N_p$ and $p^2 \nmid N$ so this contradicts Theorem 1.4.11 unless xyz has no prime divisors. This would mean that $|xyz| = 1$.

Case 2: p splits in $\mathbb{Z}[i]$. This occurs when $p \equiv 1 \pmod 4$. In this case Theorem 1.4.11 immediately tells us that $N = N_p$ and so we must have that $2^\alpha \mathrm{rad}_2(Rxyz) = 2^\alpha \mathrm{rad}_2(R)$. This means that $|xyz| = 1$.

In either case above, we see that $|xyz| = 1$. Since $a = 1$ and $b = 0$, we want to find a solution to $x^p + 2y^p + z^p = 0$ with $|xyz| = 1$ and this can be given only by $(A, B, x, y, z, p) = (1, 2, -1, 1, -1, p)$. This completes the proof when $b = 0$.

If $b \geq 1$, then we go to level $N_p = 160$. By an exponent bound computation, we see that $B_3(f)$ is nonzero and divisible only by the primes 2 and 3 for each of the three newforms of level 160. As all primes outside of $\ell = 2$ or $\ell = 5$ satisfy Theorem 1.4.12, we see that this means that p divides a product of twos and threes, a contradiction since $p \geq 5$. This gives us the following theorem originally proven by Kraus in generality [Kra97].

Theorem 1.6.1. *(Kraus) The equation $Ax^p + By^p + z^p = 0$ with $AB = 2^a 5^b$ and $p \geq 5$ has no nontrivial solutions with Ax, By and z are non-zero pairwise coprime integers when either*

$b = 0$, $a = 0$, $a = 1$ *or* $a \geq 4$ *except for the one given by* $(A, B, x, y, z, p) = (1, 2, -1, 1, -1, p)$.

Using similar techniques, Bennett and Skinner [BS04] also proved the following

Theorem 1.6.2. *(Bennett and Skinner) [BS04] Let* $C \in \{1, 2, 5, 10\}$ *and* $n \geq 4$ *be an integer. Then the equation*

$$x^n + y^n = Cz^2$$

has no solutions in pairwise coprime integers (x, y, z) *with* $x > y$ *unless* $C = 2$ *and*

$$(n, x, y, z) \in \{(5, 3, -1, \pm 11), (4, 1, -1, \pm 1)\}.$$

Notice that this theorem also solves the cases when $C = 2^a$, $C = 5^b$ or $C = 2^a 5^b$ since if C is not squarefree, we can write C as $k^\delta m^2$ with δ either 0 or 1 and $k = 1, 2, 5$ or 10 thereby reducing it to a case in the above theorem. Similarly, we have

Theorem 1.6.3. *(Bennett and Skinner) [BS04] [Coh07b, p.507] Let* $p \geq 7$ *be prime and* $a \geq 2$ *or* $a = 0$. *Then the equation*

$$x^p + 2^a y^p = z^2$$

has no solutions in pairwise coprime integers (x, y, z) *with* $|xy| > 1$ *and when* $|xy| = 1$, *then the only solutions are* $(x, y, z) = (1, 1, \pm 3)$.

Theorem 1.6.4. *(Bennett and Skinner) [BS04] Let* $p \geq 7$ *be prime and* $a \geq 6$ *or* $a = 0$. *Then the equation*

$$x^p + 2^a y^p = 5z^2$$

has no solutions in pairwise coprime integers (x, y, z) *with* $|xy| > 1$.

Note that in the above theorem, $a = 0$ was a specific case of Theorem 1.6.2. Lastly, we have

Theorem 1.6.5. *(Bennett and Skinner) [BS04] Let* $p \geq 7$ *be prime,* $a \geq 6$ *and* $b \geq 0$. *Then the equation*

$$Ax^p + By^p = z^2$$

with $AB = 2^a 5^b$ *has no nontrivial solutions with* Ax, By *and* z *are non-zero pairwise coprime integers.*

Extending the techniques above even further, we have the following results first proven by Bennett, Vatsal, and Yasdani [BVY04].

Theorem 1.6.6. *(Bennett, Vatsal, Yasdani) [BVY04] Let $C \in \{1, 2, 5\}$ and $p \geq 7$ a prime and b a nonnegative integer. Then the equation*

$$x^p + y^p = C^b z^3$$

has no solutions in coprime integers x, y, z with $|xy| > 1$.

Theorem 1.6.7. *(Bennett, Vatsal, Yasdani) [BVY04] Let $p \geq 7$ a prime and b a positive integer. Then the equation*

$$x^p + 5^b y^p = z^3$$

has no solutions in coprime integers x, y, z with $|xy| > 1$.

1.7 Results From This Thesis

After solving Fermat's Last Theorem, what other similar types of problems can now be solved? With the armamentarium of techniques at our disposal, there have since been a multitude of generalizations of this method to approach many different types of Diophantine equations, see for example any of [BS04], [BVY04], [BLM11], [Bil07], [BD10], [DG95], [Ell04], [Kra97], [Kra98], [Sik03]. Some of these results were discussed in the previous section and will be used later on.

In this thesis, we will look at twisted extensions of Fermat's theorem, in particular, those of the form $x^q + y^q = p^\alpha z^n$ for $x, y, z, p, r, n \in \mathbb{Z}$ with p prime, $q \in \{3, 5\}$, $\alpha \geq 1$ and $n \geq 5$ prime. Here I mention that work on the equations when $\alpha = 0$ have been done by many mathematicians, including the works of [Kra98] ($17 \leq n < 10^4$ prime), [Bru00] ($n = 4, 5$), [Dah08] ($n = 5, 7, 11, 13$) and [CS09] (infinitely many n, including a set of primes of Dirichlet density 28219/44928) on the equation $x^3 + y^3 = z^n$ and an unpublished note by Darmon and Kraus on the equation $x^5 + y^5 = (2z)^n$ for n prime. A full classification in these cases has not currently been discovered, though not as a result of a lack of interest.

For this equation, we will discuss in Chapter 2 a classification of elliptic curves with a nontrivial rational two torsion point and conductor with three distinct primes (with one of them being 2). From here in Chapter 3, I will present some auxiliary results on Diophantine equations to aid with our classification. Then we specify to two particular cases, curves with conductor in the set $\mathcal{S}_{3,p} = \{18p, 36p, 72p\}$ and those curves with conductor in $\mathcal{S}_{5,p} = \{50p, 200p, 400p\}$. In Chapters 4 and 5, I prove a classification on the type of primes such that we have an elliptic curve with conductor in $S_{q,p}$ and a nontrivial rational two torsion point. We denote such primes with the notation S_q. In Chapter 6, I generalize the results from

[BLM11] first to the equation $x^5 + y^5 = p^\alpha z^n$ for the complement of the primes p classified in Chapter 5, that is, for primes where all curves with conductor in the set $\mathcal{S}_{5,p}$ do not have an elliptic curve with a nontrivial rational two torsion point. Finally, in Chapter 7, I take both this new result and the result from the [BLM11] paper one step further and extend the result to a subset of the primes in S_q. In this final extension I show a specific subset of $\mathcal{S}_{q,p}$ that the prime p must avoid in order to be in my classification. The main theorems in this thesis are given by the following. For the purposes of stating the theorems now, I will delay the definition of $\mathcal{P}_{b,q}$ and $\mathcal{P}_{g,q}$ until Chapter 7 but mention now that these two sets are subsets of S_q.

Theorem 1.7.1. *Suppose that $p \geq 5$ and that $p \notin S_5$. Let $\alpha \geq 1$ be an integer. Then the equation*

$$x^5 + y^5 = p^\alpha z^n$$

has no solutions in coprime nonzero integers x, y, z and prime n satisfying $n \geq p^{13p}$

Theorem 1.7.2. *Let $q \in \{3, 5\}$ and let $p \in \mathcal{P}_{g,q} \subseteq S_q$. Then $p \in \mathcal{P}_{b,q}$ if and only if every elliptic curve with conductor in $\mathcal{S}_{q,p}$ with non-trivial rational two torsion has discriminant not of the form $\Delta_{Q,q,m} := \left(\frac{-1}{q}\right)qm^2$ for all integers m.*

Theorem 1.7.3. *Let $q \in \{3, 5\}$ and suppose that p is a prime such that $p \notin S_q$ or that $p \in \mathcal{P}_{b,q} \subseteq S_q$. Then the equation $x^q + y^q = p^\alpha z^n$ has no nontrivial coprime integer solutions (x, y, z) where $\alpha \geq 1$ and $n \geq C_q(p)$ a prime. Furthermore, if the prime p avoids the lists in Tables 7.1 and 7.3 (hence residing in Table 7.5) when $q = 3$ or in Tables 7.2 and 7.4 (hence residing in Table 7.6) when $q = 5$, then we have that $p \notin S_q$ or that $p \in \mathcal{P}_{b,q} \subseteq S_q$.*

Chapter 2

Classification of Elliptic Curves With Nontrivial Rational Two Torsion

2.1 On the $\mathbb{Q}$-Isomorphism Classes of Elliptic Curves With Nontrivial Rational 2-Torsion and Conductor $2^L q^M p^N$

Let E be an elliptic curve over $\mathbb{Q}$ with rational two torsion and conductor $2^L q^M p^N$ (here, we use q first because we are interested in the case when $q = 5$). We know via Theorem 1.2.7 that the conductor of any such elliptic curve cannot be divisible by 2^9, 3^6, or ℓ^3 where $\ell \geq 5$ is a prime. Further, by [Mul06, p. 13], we know that any elliptic curve over $\mathbb{Q}$ with rational two torsion is such that 3^3 does not divide the conductor. Thus we can assume here that $0 \leq L \leq 8$ and $0 \leq M, N \leq 2$. We may also assume that E has a model given by

$$E : y^2 = x^3 + ax^2 + bx.$$

For such a curve, we have that the discriminant is given by

$$\Delta = 2^4 b^2 (a^2 - 4b).$$

From [Mul06, p.13-14], we see that the discriminant above and the conductor must share odd primes and so we have that

$$b^2(a^2 - 4b) = \pm 2^\lambda q^\mu p^\nu$$

for some non-negative integers λ, μ, ν. Hence, we must have that

$$b = \pm 2^i q^j p^k$$

for some i, j, k satisfying $0 \leq 2i \leq \lambda$, $0 \leq 2j \leq \mu$ and $0 \leq 2k \leq \nu$. Using this, we have that

$$a^2 = 2^{i+2}q^j p^k \pm 2^{\lambda-2i}q^{\mu-2j}p^{\nu-2k}.$$

Now, break this down into 27 cases based on the trichotomies depending on if $i+2 > \lambda-2i$, $i+2 < \lambda-2i$ or $i+2 = \lambda-2i$ (and similarly with i replaced by j or k and λ replaced by μ or ν) we can create a table of $\mathbb{Q}$-isomorphism classes of curves. I will demonstrate one such case here and for the rest I refer the interested reader to the appendix in [Mul06] though the reader should be warned that there are numerous typos in the proof found there. Let's suppose that $i+2 > \lambda-2i$, $j = \mu-2j$ and $k < \nu-2k$. Factoring gives

$$a^2 = 2^{\lambda-2i}q^j p^k(2^{3i-\lambda+2} \pm p^{\nu-3k}).$$

Set $d := 2^{3i-\lambda+2} \pm p^{\nu-3k}$. Since *a priori* we do not know if $q \mid d$, we have that $q^{(j+\epsilon)/2} \mid a$ where $j \equiv \epsilon \pmod 2$. Rewriting the above equation, we have

$$3^\epsilon \left(\frac{a}{2^{\lambda/2-i}q^{(j+\epsilon)/2}p^{k/2}}\right)^2 - 2^{3i-\lambda+2} = \pm p^{\nu-2k}$$

with $\ell := 3i-\lambda+2 \geq 1$ and $n := \nu-2k \geq 1$. Then depending on ϵ, we have a solution to one of the following equations

$$d^2 - 2^\ell = \pm p^n \qquad \text{or} \qquad 3d^2 - 2^\ell = \pm p^n$$

if $\epsilon = 0$ in the first case or $\epsilon = 1$ in the second case. Either way, a model for our elliptic curve can be given by

$$y^2 = x^3 + 2^{\lambda/2-i}q^{(j+\epsilon)/2}p^{k/2}dx^2 + 2^i q^j p^k x.$$

Now, by the division algorithm, we can write

$$\lambda/2 - i = 2q_1 + r_1 \qquad \frac{j+\epsilon}{2} = 2q_2 + r_2 \qquad k/2 = 2q_3 + r_3$$

where $r_1, r_2, r_3 \in \{0, 1\}$. Rewriting the elliptic curve gives

$$y^2 = x^3 + 2^{2q_1+r_1}q^{2q_2+r_2}p^{2q_3+r_3}dx^2 + 2^{\ell-2+4q_1+2r_1}q^{4q_2+2r_2-\epsilon}p^{4q_2+2r_3}x.$$

If $\ell = 1$ and $r_1 = 0$, then the change of variables

$$(X, Y) = \left(\frac{x}{2^{2(q_1-1)}q^{2(q_2+(r_2-1)\epsilon)}p^{2q_3}}, \frac{y}{2^{3(q_1-1)}q^{3(q_2+(r_2-1)\epsilon)}p^{3q_3}}\right)$$

gives the $\mathbb{Q}$-isomorphic curve

$$Y^2 = X^3 + 2^2 q^{2\epsilon+(1-2\epsilon)r_2} p^{r_3} dX^2 + 2^3 q^{3\epsilon+2(1-2\epsilon)r_2} p^{2r_2} X$$

If $(\ell, r_1) \neq (1,0)$ (and so either $\ell > 1$ or $r_1 > 0$), we have that the change of variables

$$(X, Y) = \left(\frac{x}{2^{2q_1} q^{2(q_2+(r_2-1)\epsilon)} p^{2q_3}}, \frac{y}{2^{3q_1} q^{3(q_2+(r_2-1)\epsilon)} p^{3q_3}} \right)$$

gives the $\mathbb{Q}$-isomorphic curve

$$Y^2 = X^3 + 2^{r_1} q^{2\epsilon+(1-2\epsilon)r_2} p^{r_3} dX^2 + 2^{\ell+2r_1-2} q^{3\epsilon+2(1-2\epsilon)r_2} p^{2r_2} X.$$

Note that when $\epsilon = 0$, the curve above corresponds to case 4 in the tables below. When $\epsilon = 1$, then the curve above corresponds to case 8 in the table below. To see this easily, plug in for the cases of $r_2 \in \{0, 1\}$ and $\epsilon \in \{0, 1\}$. Modifying the above argument 26 times gives the following theorem.

Theorem 2.1.1. *(Modified from [Mul06, p. 270-271, 309-310]) Suppose E is an elliptic curve with rational two torsion and conductor $2^L q^M p^N$. Without loss of generality, E can take the form*

$$E : y^2 = x^3 + a_2 x^2 + a_4 x.$$

Further assume that $a_4 > 0$. Then, there exists an integer d and non-negative integers ℓ, m, n satisfying one of the equations in the second column below and the corresponding curve E is given by a_2 and a_4 given in the third and fourth columns where $r_1, r_2, r_3 \in \{0, 1\}$ except in cases 1 through 9 (for both tables below) where if $\ell = 1$, then $r_1 \in \{1, 2\}$ and the sign in the Diophantine equation matches that of the sign in the discriminant Δ.

	Equation	a_2	a_4	Δ
1	$d^2 - 2^\ell q^m p^n = \pm 1$	$2^{r_1} q^{r_2} p^{r_3} d$	$2^{\ell+2r_1-2} q^{m+2r_2} p^{n+2r_3}$	$\pm 2^{2\ell+6r_1} q^{2m+6r_2} p^{2n+6r_3}$
2	$d^2 - 2^\ell q^m = \pm p^n$	$2^{r_1} q^{r_2} p^{r_3} d$	$2^{\ell+2r_1-2} q^{m+2r_2} p^{2r_3}$	$\pm 2^{2\ell+6r_1} q^{2m+6r_2} p^{n+6r_3}$
3	$d^2 - 2^\ell p^n = \pm q^m$	$2^{r_1} q^{r_2} p^{r_3} d$	$2^{\ell+2r_1-2} q^{2r_2} p^{n+2r_3}$	$\pm 2^{2\ell+6r_1} q^{m+6r_2} p^{2n+6r_3}$
4	$d^2 - 2^\ell = \pm q^m p^n$	$2^{r_1} q^{r_2} p^{r_3} d$	$2^{\ell+2r_1-2} q^{2r_2} p^{2r_3}$	$\pm 2^{2\ell+6r_1} q^{m+6r_2} p^{n+6r_3}$
5	$pd^2 - 2^\ell q^m = \pm 1$	$2^{r_1} q^{r_2} p^{r_3+1} d$	$2^{\ell+2r_1-2} q^{m+2r_2} p^{2r_3+1}$	$\pm 2^{2\ell+6r_1} q^{2m+6r_2} p^{6r_3+3}$
6	$pd^2 - 2^\ell = \pm q^m$	$2^{r_1} q^{r_2} p^{r_3+1} d$	$2^{\ell+2r_1-2} q^{2r_2} p^{2r_3+1}$	$\pm 2^{2\ell+6r_1} q^{m+6r_2} p^{6r_3+3}$
7	$qd^2 - 2^\ell p^n = \pm 1$	$2^{r_1} q^{r_2+1} p^{r_3} d$	$2^{\ell+2r_1-2} q^{2r_2+1} p^{n+2r_3}$	$\pm 2^{2\ell+6r_1} q^{6r_2+3} p^{2n+6r_3}$
8	$qd^2 - 2^\ell = \pm p^n$	$2^{r_1} q^{r_2+1} p^{r_3} d$	$2^{\ell+2r_1-2} q^{2r_2+1} p^{2r_3}$	$\pm 2^{2\ell+6r_1} q^{6r_2+3} p^{n+6r_3}$
9	$qpd^2 - 2^\ell = \pm 1$	$2^{r_1} q^{r_2+1} p^{r_3+1} d$	$2^{\ell+2r_1-2} q^{2r_2+1} p^{2r_3+1}$	$\pm 2^{2\ell+6r_1} q^{6r_2+3} p^{6r_3+3}$
10	$d^2 - q^m p^n = \pm 2^\ell$	$2^{r_1+1} q^{r_2} p^{r_3} d$	$2^{2r_1} q^{m+2r_2} p^{n+2r_3}$	$\pm 2^{\ell+6r_1+6} q^{2m+6r_2} p^{2n+6r_3}$
11	$d^2 - q^m = \pm 2^\ell p^n$	$2^{r_1+1} q^{r_2} p^{r_3} d$	$2^{2r_1} q^{m+2r_2} p^{2r_3}$	$\pm 2^{\ell+6r_1+6} q^{2m+6r_2} p^{n+6r_3}$
12	$d^2 - p^n = \pm 2^\ell q^m$	$2^{r_1+1} q^{r_2} p^{r_3} d$	$2^{2r_1} q^{2r_2} p^{n+2r_3}$	$\pm 2^{\ell+6r_1+6} q^{m+6r_2} p^{2n+6r_3}$
13	$d^2 - 1 = \pm 2^\ell q^m p^n$	$2^{r_1+1} q^{r_2} p^{r_3} d$	$2^{2r_1} q^{2r_2} p^{2r_3}$	$\pm 2^{\ell+6r_1+6} q^{m+6r_2} p^{n+6r_3}$
14	$pd^2 - q^m = \pm 2^\ell$	$2^{r_1+1} q^{r_2} p^{r_3+1} d$	$2^{2r_1} q^{m+2r_2} p^{2r_3+1}$	$\pm 2^{\ell+6r_1+6} q^{2m+6r_2} p^{6r_3+3}$
15	$pd^2 - 1 = \pm 2^\ell q^m$	$2^{r_1+1} q^{r_2} p^{r_3+1} d$	$2^{2r_1} q^{2r_2} p^{2r_3+1}$	$\pm 2^{\ell+6r_1+6} q^{m+6r_2} p^{6r_3+3}$
16	$qd^2 - p^n = \pm 2^\ell$	$2^{r_1+1} q^{r_2+1} p^{r_3} d$	$2^{2r_1} q^{2r_2+1} p^{n+2r_3}$	$\pm 2^{\ell+6r_1+6} q^{6r_2+3} p^{2n+6r_3}$
17	$qd^2 - 1 = \pm 2^\ell p^n$	$2^{r_1+1} q^{r_2+1} p^{r_3} d$	$2^{2r_1} q^{2r_2+1} p^{2r_3}$	$\pm 2^{\ell+6r_1+6} q^{6r_2+3} p^{n+6r_3}$
18	$qpd^2 - 1 = \pm 2^\ell$	$2^{r_1+1} q^{r_2+1} p^{r_3+1} d$	$2^{2r_1} q^{2r_2+1} p^{2r_3+1}$	$\pm 2^{\ell+6r_1+6} q^{6r_2+3} p^{6r_3+3}$
19	$2d^2 - q^m p^n = \pm 1$	$2^{r_1+2} q^{r_2} p^{r_3} d$	$2^{2r_1+1} q^{m+2r_2} p^{n+2r_3}$	$\pm 2^{6r_1+9} q^{2m+6r_2} p^{2n+6r_3}$
20	$2d^2 - q^m = \pm p^n$	$2^{r_1+2} q^{r_2} p^{r_3} d$	$2^{2r_1+1} q^{m+2r_2} p^{2r_3}$	$\pm 2^{6r_1+9} q^{2m+6r_2} p^{n+6r_3}$
21	$2d^2 - p^n = \pm q^m$	$2^{r_1+2} q^{r_2} p^{r_3} d$	$2^{2r_1+1} q^{2r_2} p^{n+2r_3}$	$\pm 2^{6r_1+9} q^{m+6r_2} p^{2n+6r_3}$
22	$2d^2 - 1 = \pm q^m p^n$	$2^{r_1+2} q^{r_2} p^{r_3} d$	$2^{2r_1+1} q^{2r_2} p^{2r_3}$	$\pm 2^{6r_1+9} q^{m+6r_2} p^{n+6r_3}$
23	$2pd^2 - q^m = \pm 1$	$2^{r_1+2} q^{r_2} p^{r_3+1} d$	$2^{2r_1+1} q^{m+2r_2} p^{2r_3+1}$	$\pm 2^{6r_1+9} q^{2m+6r_2} p^{6r_3+3}$
24	$2pd^2 - 1 = \pm q^m$	$2^{r_1+2} q^{r_2} p^{r_3+1} d$	$2^{2r_1+1} q^{2r_2} p^{2r_3+1}$	$\pm 2^{6r_1+9} q^{m+6r_2} p^{6r_3+3}$
25	$2qd^2 - p^n = \pm 1$	$2^{r_1+2} q^{r_2+1} p^{r_3} d$	$2^{2r_1+1} q^{2r_2+1} p^{n+2r_3}$	$\pm 2^{6r_1+9} q^{6r_2+3} p^{2n+6r_3}$
26	$2qd^2 - 1 = \pm p^n$	$2^{r_1+2} q^{r_2+1} p^{r_3} d$	$2^{2r_1+1} q^{2r_2+1} p^{2r_3}$	$\pm 2^{6r_1+9} q^{6r_2+3} p^{n+6r_3}$
27	$2qpd^2 - 1 = \pm 1$	$2^{r_1+2} q^{r_2+1} p^{r_3+1} d$	$2^{2r_1+1} q^{2r_2+1} p^{2r_3+1}$	$\pm 2^{6r_1+9} q^{6r_2+3} p^{6r_3+3}$

Table 2.1: Elliptic curves of conductor $2^L q^M p^N$ when $a_4 > 0$

When $a_4 < 0$, we have

	Equation	a_2	a_4	Δ
2	$d^2+2^\ell q^m=p^n$	$2^{r_1}q^{r_2}p^{r_3}d$	$-2^{\ell+2r_1-2}q^{m+2r_2}p^{2r_3}$	$2^{2\ell+6r_1}q^{2m+6r_2}p^{n+6r_3}$
3	$d^2+2^lp^n=q^m$	$2^{r_1}q^{r_2}p^{r_3}d$	$-2^{\ell+2r_1-2}q^{2r_2}p^{n+2r_3}$	$2^{2\ell+6r_1}q^{m+6r_2}p^{2n+6r_3}$
4	$d^2+2^l=q^mp^n$	$2^{r_1}q^{r_2}p^{r_3}d$	$-2^{\ell+2r_1-2}q^{2r_2}p^{2r_3}$	$2^{2\ell+6r_1}q^{m+6r_2}p^{n+6r_3}$
6	$pd^2+2^l=q^m$	$2^{r_1}q^{r_2}p^{r_3+1}d$	$-2^{\ell+2r_1-2}q^{2r_2}p^{2r_3+1}$	$2^{2\ell+6r_1}q^{m+6r_2}p^{6r_3+3}$
8	$qd^2+2^l=p^n$	$2^{r_1}q^{r_2+1}p^{r_3}d$	$-2^{\ell+2r_1-2}q^{2r_2+1}p^{2r_3}$	$2^{2\ell+6r_1}q^{6r_2+3}p^{n+6r_3}$
10	$d^2+q^mp^n=2^\ell$	$2^{r_1+1}q^{r_2}p^{r_3}d$	$-2^{2r_1}q^{m+2r_2}p^{n+2r_3}$	$2^{\ell+6r_1+6}q^{2m+6r_2}p^{2n+6r_3}$
11	$d^2+q^m=2^\ell p^n$	$2^{r_1+1}q^{r_2}p^{r_3}d$	$-2^{2r_1}q^{m+2r_2}p^{2r_3}$	$2^{\ell+6r_1+6}q^{2m+6r_2}p^{n+6r_3}$
12	$d^2+p^n=2^\ell q^m$	$2^{r_1+1}q^{r_2}p^{r_3}d$	$-2^{2r_1}q^{2r_2}p^{n+2r_3}$	$2^{\ell+6r_1+6}q^{m+6r_2}p^{2n+6r_3}$
13	$d^2+1=2^\ell q^mp^n$	$2^{r_1+1}q^{r_2}p^{r_3}d$	$-2^{2r_1}q^{2r_2}p^{2r_3}$	$2^{\ell+6r_1+6}q^{m+6r_2}p^{n+6r_3}$
14	$pd^2+q^m=2^\ell$	$2^{r_1+1}q^{r_2}p^{r_3+1}d$	$-2^{2r_1}q^{m+2r_2}p^{2r_3+1}$	$2^{\ell+6r_1+6}q^{2m+6r_2}p^{6r_3+3}$
15	$pd^2+1=2^\ell q^m$	$2^{r_1+1}q^{r_2}p^{r_3+1}d$	$-2^{2r_1}q^{2r_2}p^{2r_3+1}$	$2^{\ell+6r_1+6}q^{m+6r_2}p^{6r_3+3}$
16	$qd^2+p^n=2^\ell$	$2^{r_1+1}q^{r_2+1}p^{r_3}d$	$-2^{2r_1}q^{2r_2+1}p^{n+2r_3}$	$2^{\ell+6r_1+6}q^{6r_2+3}p^{2n+6r_3}$
17	$qd^2+1=2^\ell p^n$	$2^{r_1+1}q^{r_2+1}p^{r_3}d$	$-2^{2r_1}q^{2r_2+1}p^{2r_3}$	$2^{\ell+6r_1+6}q^{6r_2+3}p^{n+6r_3}$
18	$qpd^2+1=2^\ell$	$2^{r_1+1}q^{r_2+1}p^{r_3+1}d$	$-2^{2r_1}q^{2r_2+1}p^{2r_3+1}$	$2^{\ell+6r_1+6}q^{6r_2+3}p^{6r_3+3}$
20	$2d^2+q^m=p^n$	$2^{r_1+2}q^{r_2}p^{r_3}d$	$-2^{2r_1+1}q^{m+2r_2}p^{2r_3}$	$2^{6r_1+9}q^{2m+6r_2}p^{n+6r_3}$
21	$2d^2+p^n=q^m$	$2^{r_1+2}q^{r_2}p^{r_3}d$	$-2^{2r_1+1}q^{2r_2}p^{n+2r_3}$	$2^{6r_1+9}q^{m+6r_2}p^{2n+6r_3}$
22	$2d^2+1=q^mp^n$	$2^{r_1+2}q^{r_2}p^{r_3}d$	$-2^{2r_1+1}q^{2r_2}p^{2r_3}$	$2^{6r_1+9}q^{m+6r_2}p^{n+6r_3}$
24	$2pd^2+1=q^m$	$2^{r_1+2}q^{r_2}p^{r_3+1}d$	$-2^{2r_1+1}q^{2r_2}p^{2r_3+1}$	$2^{6r_1+9}q^{m+6r_2}p^{6r_3+3}$
26	$2qd^2+1=p^n$	$2^{r_1+2}q^{r_2+1}p^{r_3}d$	$-2^{2r_1+1}q^{2r_2+1}p^{2r_3}$	$2^{6r_1+9}q^{6r_2+3}p^{n+6r_3}$

Table 2.2: Elliptic curves of conductor $2^Lq^Mp^N$ when $a_4<0$

To avoid redundancies in the lists above, in the right hand side of the equations above, we do allow the exponent of primes on the right to be 0 *and otherwise, the exponents of the Diophantine equations are at least* 1. *The numbering in the second list is kept to reflect the first list.*

In our case, we are interested for application purposes in the case when $q=5$. Our goal will be to solve the above Diophantine equations in general. Then, after simplification, ideally we would be able to remove many of the conditions on the exponents to reveal a short and succinct list of potential elliptic curves.

2.2 Elliptic Curves With Nontrivial Rational Two Torsion and Conductor $2^aq^bp^c$

In what follows, let E be an elliptic curve of conductor $2^aq^bp^c$ with nontrivial rational two torsion where p and q are distinct odd primes. By Theorem 1.2.7, we need only to consider

values of the exponents of the conductor where

$$0 \leq a \leq 8 \qquad 0 \leq b, c \leq 2$$

The work on curves of conductor $2^a 3^b p^c$ has been done already and is summarized in [Mul06, Chapter 3]. In what follows, we assume that $p, q \geq 3$ are distinct primes and further that $1 \leq b, c \leq 2$. We will create a list of all such curves below satisfying this criteria sorted by conductor. From this list, we will focus on the curves of conductor $50p, 200p$ and $400p$ and use tricks of Diophantine equations to simplify these results to get a succinct list of primes p with an elliptic curve with nontrivial rational two torsion and conductor $50p, 200p$ or $400p$.

Before we begin, we discuss some notes on the notation.

1. We are looking for curves of conductor $2^a q^b p^c$ with nontrivial rational two torsion. The idea here is to find integers ℓ, m, n so that the curves we find fit into some appropriate row of the tables in Section 2.1.

2. We require that $m \geq 1$ when $b = 1$ and we can allow $m = 0$ when $b = 2$ (because then $r_2 = 1$), which is equivalent to asking for $m \geq 2 - b$ for $b = 1, 2$.

3. The function $\psi(t)$ returns the square root value congruent to 1 modulo 4 or the positive value if t is even.

4. Some cases that were present in the tables above are not below. These omitted cases are the ones with associated Diophantine equations that cannot be solved as seen by looking at local conditions, for example by reducing modulo a power of 2 or modulo p or q.

5. The tables below give minimal models at the primes that divide the conductor except when 4 does not divide the conductor. In that case, one can obtain a minimal model as stated in [Mul06, p. 13].

6. Curves denoted by E and E' are related by a twist by $\sqrt{-1}$.

7. Curves beginning with the same letter are linked by a degree 2 isogeny as in [Coh07a, p. 532-533] or a composition of two such isogenies as in [Mul06, p.31].

8. The lettering used here was inspired by [Mul06]. It is unfortunate that the lettering here does not correspond in any way to either the lettering used there or in [Cre] but for us, the notation is self contained and so we proceed with this in mind.

Theorem 2.2.1. *The elliptic curves E defined over $\mathbb{Q}$ of conductor $q^b p$ and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2^6 q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot q^{b-1}\psi(2^6 q^m p^n + 1)$	$2^4 q^{m+2(b-1)} p^n$	$2^{12} q^{2m+6(b-1)} p^{2n}$
A2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 q^m p^n + 1)$	$q^{2(b-1)}$	$2^{12} q^{m+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

2. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2^6 q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot q^{b-1}\psi(2^6 q^m + p^n)$	$2^4 q^{m+2(b-1)}$	$2^{12} q^{2m+6(b-1)} p^n$
B2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 q^m + p^n)$	$q^{2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

3. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2^6 q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot q^{b-1}\psi(2^6 q^m - p^n)$	$2^4 q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$
C2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 q^m - p^n)$	$-q^{2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

4. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $p^n - 2^6 q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot q^{b-1}\psi(p^n - 2^6 q^m)$	$-2^4 q^{m+2(b-1)}$	$2^{12} q^{2m+6(b-1)} p^n$
D2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 2^6 q^m$	$q^{2(b-1)} p^n$	$-2^{12} q^{m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

5. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2^6 p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot q^{b-1}\psi(2^6 p^n + q^m)$	$2^4 q^{2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$
E2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 p^n + q^m)$	$q^{m+2(b-1)}$	$2^{12} q^{2m+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

6. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^6 p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$*,* m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot q^{b-1}\psi(2^6 p^n - q^m)$	$2^4 q^{2(b-1)} p^n$	$-2^{12} q^{m+6(b-1)} p^{2n}$
F2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 p^n - q^m)$	$-q^{m+2(b-1)}$	$2^{12} q^{2m+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

7. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 2^6 p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot q^{b-1}\psi(q^m - 2^6 p^n)$	$-2^4 q^{2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$
G2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m - 2^6 p^n)$	$q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

8. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^6 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot q^{b-1}\psi(2^6 + q^m p^n)$	$2^4 q^{2(b-1)}$	$2^{12} q^{m+6(b-1)} p^n$
H2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 + q^m p^n)$	$q^{m+2(b-1)} p^n$	$2^{12} q^{2m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

9. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^6 - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot q^{b-1}\psi(2^6 - q^m p^n)$	$2^4 q^{2(b-1)}$	$-2^{12} q^{m+6(b-1)} p^n$
I2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^6 - q^m p^n)$	$-q^{m+2(b-1)} p^n$	$2^{12} q^{2m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

10. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m p^n - 2^6$ *is a square,* $8 \mid (3q+5)(q-1)$*,* $8 \mid (3p+5)(p-1)$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot q^{b-1}\psi(q^m p^n - 2^6)$	$-2^4 q^{2(b-1)}$	$2^{12} q^{m+6(b-1)} p^n$
J2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m p^n - 2^6)$	$q^{m+2(b-1)} p^n$	$-2^{12} q^{2m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

In the case that $b = 2$*, we furthermore could have one of the following conditions satisfied:*

11. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^6 p^n + 1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
K1	$q^{s+1}\psi(\frac{2^6 p^n + 1}{q})$	$2^4 q^{2s+1} p^n$	$2^{12} q^{6s+3} p^{2n}$
K2	$-2 \cdot q^{s+1}\psi(\frac{2^6 p^n + 1}{q})$	q^{2s+1}	$2^{12} q^{6s+3} p^n$

12. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^6 p^n - 1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot q^{s+1}\psi(\frac{2^6 p^n - 1}{q})$	$2^4 q^{2s+1} p^n$	$-2^{12} q^{6s+3} p^{2n}$
L2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^6 p^n - 1}{q})$	$-q^{2s+1}$	$2^{12} q^{6s+3} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

13. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^6 + p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot q^{s+1}\psi(\frac{2^6 + p^n}{q})$	$2^4 q^{2s+1}$	$2^{12} q^{6s+3} p^n$
M2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^6 + p^n}{q})$	$q^{2s+1} p^n$	$2^{12} q^{6s+3} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

14. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^6 - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot q^{s+1}\psi(\frac{2^6 - p^n}{q})$	$2^4 q^{2s+1}$	$-2^{12} q^{6s+3} p^n$
N2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^6 - p^n}{q})$	$-q^{2s+1} p^n$	$2^{12} q^{6s+3} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

15. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{p^n - 2^6}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot q^{s+1}\psi(\frac{p^n-2^6}{q})$	$-2^4 q^{2s+1}$	$2^{12}q^{6s+3}p^n$
O2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{p^n-2^6}{q})$	$q^{2s+1}p^n$	$-2^{12}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

Theorem 2.2.2. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2q^b p$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 7$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^\ell q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m p^n + 1)$	$2^{\ell-2}q^{m+2(b-1)}p^n$	$2^{2\ell}q^{2m+6(b-1)}p^{2n}$
A2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m p^n + 1)$	$q^{2(b-1)}$	$2^{\ell+6}q^{m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

2. *There exist integers* $\ell \geq 7$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^\ell q^m + p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m + p^n)$	$2^{\ell-2}q^{m+2(b-1)}$	$2^{2\ell}q^{2m+6(b-1)}p^n$
B2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m + p^n)$	$q^{2(b-1)}p^n$	$2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

3. *There exist integers* $\ell \geq 7$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^\ell q^m - p^n$ *is a square,* $p \equiv 7 \pmod 8$, n *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m - p^n)$	$2^{\ell-2}q^{m+2(b-1)}$	$-2^{2\ell}q^{2m+6(b-1)}p^n$
C2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

4. *There exist integers $\ell \geq 7$, $m \geq 2-b$ and $n \geq 1$ such that $p^n - 2^\ell q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot q^{b-1}\psi(p^n - 2^\ell q^m)$	$-2^{\ell-2}q^{m+2(b-1)}$	$2^{2\ell}q^{2m+6(b-1)}p^n$
D2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 2^\ell q^m)$	$q^{2(b-1)}p^n$	$-2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

5. *There exist integers $\ell \geq 7$, $m \geq 2-b$ and $n \geq 1$ such that $2^\ell p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot q^{b-1}\psi(2^\ell p^n + q^m)$	$2^{\ell-2}q^{2(b-1)}p^n$	$2^{2\ell}q^{m+6(b-1)}p^{2n}$
E2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell p^n + q^m)$	$q^{m+2(b-1)}$	$2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

6. *There exist integers $\ell \geq 7$, $m \geq 2-b$ and $n \geq 1$ such that $2^\ell p^n - q^m$ is a square, $q \equiv 7 \pmod 8$, m odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot q^{b-1}\psi(2^\ell p^n - q^m)$	$2^{\ell-2}q^{2(b-1)}p^n$	$-2^{2\ell}q^{m+6(b-1)}p^{2n}$
F2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell p^n - q^m)$	$-q^{m+2(b-1)}$	$2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

7. *There exist integers $\ell \geq 7$, $m \geq 2-b$ and $n \geq 1$ such that $q^m - 2^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot q^{b-1}\psi(q^m - 2^\ell p^n)$	$-2^{\ell-2}q^{2(b-1)}p^n$	$2^{2\ell}q^{m+6(b-1)}p^{2n}$
G2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m - 2^\ell p^n)$	$q^{m+2(b-1)}$	$-2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

8. *There exist integers $\ell \geq 7$, $m \geq 2-b$ and $n \geq 1$ such that $2^\ell + q^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot q^{b-1}\psi(2^\ell + q^m p^n)$	$2^{\ell-2}q^{2(b-1)}$	$2^{2\ell}q^{m+6(b-1)}p^n$
H2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell + q^m p^n)$	$q^{m+2(b-1)}p^n$	$2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

9. *There exist integers* $\ell \geq 7$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot q^{b-1}\psi(2^\ell - q^m p^n)$	$2^{\ell-2}q^{2(b-1)}$	$-2^{2\ell}q^{m+6(b-1)}p^n$
I2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell - q^m p^n)$	$-q^{m+2(b-1)}p^n$	$2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

10. *There exist integers* $\ell \geq 7$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot q^{b-1}\psi(q^m p^n - 2^\ell)$	$-2^{\ell-2}q^{2(b-1)}$	$2^{2\ell}q^{m+6(b-1)}p^n$
J2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m p^n - 2^\ell)$	$q^{m+2(b-1)}p^n$	$-2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

In the case that $b = 2$, *we furthermore could have one of the following conditions satisfied:*

11. *there exist integers* $\ell \geq 7$, $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^\ell p^n + 1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
K1	$q^{s+1}\psi(\frac{2^\ell p^n+1}{q})$	$2^{\ell-2}q^{2s+1}p^n$	$2^{2\ell}q^{6s+3}p^{2n}$
K2	$-2 \cdot q^{s+1}\psi(\frac{2^\ell p^n+1}{q})$	q^{2s+1}	$2^{\ell+6}q^{6s+3}p^n$

12. *there exist integers* $\ell \geq 7$, $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^\ell p^n - 1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell p^n-1}{q})$	$2^{\ell-2}q^{2s+1}p^n$	$-2^{2\ell}q^{6s+3}p^{2n}$
L2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell p^n-1}{q})$	$-q^{2s+1}$	$2^{\ell+6}q^{6s+3}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

13. *there exist integers* $\ell \geq 7$, $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^\ell + p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell+p^n}{q})$	$2^{\ell-2}q^{2s+1}$	$2^{2\ell}q^{6s+3}p^n$
M2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell+p^n}{q})$	$q^{2s+1}p^n$	$2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

14. *there exist integers* $\ell \geq 7$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell-p^n}{q})$	$2^{\ell-2}q^{2s+1}$	$-2^{2\ell}q^{6s+3}p^n$
N2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell-p^n}{q})$	$-q^{2s+1}p^n$	$2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

15. *there exist integers* $\ell \geq 7$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n - 2^\ell}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot q^{s+1}\psi(\frac{p^n-2^\ell}{q})$	$-2^{\ell-2}q^{2s+1}$	$2^{2\ell}q^{6s+3}p^n$
O2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{p^n-2^\ell}{q})$	$q^{2s+1}p^n$	$-2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

Theorem 2.2.3. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* 2^2q^bp *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4q^m + p^n$ *is a square,* $q^m \equiv -1 \pmod 4$*,* n *odd and* $p \equiv 5 \pmod 8$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{m+2(b-1)}$	$2^4q^{2m+6(b-1)}p^n$
A2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{2(b-1)}p^n$	$2^8q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

2. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4q^m - p^n$ *is a square,* $q^m \equiv -1 \pmod 4$*,* n *odd and* $p \equiv 3 \pmod 8$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot q^{b-1}\psi(4q^m - p^n)$	$q^{m+2(b-1)}$	$-2^4 q^{2m+6(b-1)} p^n$
B2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^8 q^{m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

3. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $p^n - 4q^m$ *is a square,* $q^m \equiv 1 \pmod 4$, n *odd and* $p \equiv 5 \pmod 8$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot q^{b-1}\psi(p^n - 4q^m)$	$-q^{m+2(b-1)}$	$2^4 q^{2m+6(b-1)} p^n$
C2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 4q^m)$	$q^{2(b-1)}p^n$	$-2^8 q^{m+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

4. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n + q^m$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$q^{b-1}\psi(4p^n + q^m)$	$q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)} p^{2n}$
D2	$-2 \cdot q^{b-1}\psi(4p^n + q^m)$	$q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)} p^n$

5. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n - q^m$ *is a square,* $q \equiv 3 \pmod 8$, $p^n \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot q^{b-1}\psi(4p^n - q^m)$	$q^{2(b-1)}p^n$	$-2^4 q^{m+6(b-1)} p^{2n}$
E2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4p^n - q^m)$	$-q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

6. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 4p^n$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$q^{b-1}\psi(q^m - 4p^n)$	$-q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)} p^{2n}$
F2	$-2 \cdot q^{b-1}\psi(q^m - 4p^n)$	$q^{m+2(b-1)}$	$-2^8 q^{2m+6(b-1)} p^n$

7. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m p^n - 4$ *is a square,* $p, q \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$q^{b-1}\psi(q^m p^n - 4)$	$-q^{2(b-1)}$	$2^4 q^{m+6(b-1)} p^n$
G2	$-2 \cdot q^{b-1}\psi(q^m p^n - 4)$	$q^{m+2(b-1)} p^n$	$-2^{10} q^{2m+6(b-1)} p^{2n}$

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

8. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n+1}{q}$ is a square, $p^n \equiv 3 \pmod 4$, $q \equiv 5 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
H1	$q^{s+1}\psi(\frac{4p^n+1}{q})$	$q^{2s+1} p^n$	$2^4 q^{6s+3} p^{2n}$
H2	$-2 \cdot q^{s+1}\psi(\frac{4p^n+1}{q})$	q^{2s+1}	$2^8 q^{6s+3} p^n$

9. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{q}$ is a square, $p^n \equiv 1 \pmod 4$, $q \equiv 3 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$q^{2s+1} p^n$	$-2^4 q^{6s+3} p^{2n}$
I2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$-q^{2s+1}$	$2^8 q^{6s+3} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{s+1} modulo 4.

10. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4+p^n}{q}$ is a square, $q \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot q^{s+1}\psi(\frac{4+p^n}{q})$	q^{2s+1}	$2^4 q^{6s+3} p^n$
J2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{4+p^n}{q})$	$q^{2s+1} p^n$	$2^8 q^{6s+3} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{s+1} modulo 4.

11. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-4}{q}$ is a square, $q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
L1	$q^{s+1}\psi(\frac{p^n-4}{q})$	$-q^{2s+1}$	$2^4 q^{6s+3} p^n$
L2	$-2 \cdot q^{s+1}\psi(\frac{p^n-4}{q})$	$q^{2s+1} p^n$	$-2^8 q^{6s+3} p^{2n}$

Theorem 2.2.4. *The elliptic curves E defined over $\mathbb{Q}$ of conductor 2^3q^bp and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $\ell \in \{4,5\}$, $m \geq 2-b$ and $n \geq 1$ such that $2^\ell q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m p^n + 1)$	$2^{\ell-2}q^{m+2(b-1)}p^n$	$2^{2\ell}q^{2m+6(b-1)}p^{2n}$
A2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m p^n + 1)$	$q^{2(b-1)}$	$2^{\ell+6}q^{m+6(b-1)}p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

2. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $4q^m+p^n$ is a square, $q^m \equiv 1 \pmod 4$, n odd and $p \equiv 5 \pmod 8$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$-\epsilon \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{m+2(b-1)}$	$2^4q^{2m+6(b-1)}p^n$
B2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{2(b-1)}p^n$	$2^8q^{m+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

3. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $4q^m-p^n$ is a square, $q^m \equiv 1 \pmod 4$, n odd and $p \equiv 3 \pmod 8$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$-\epsilon \cdot q^{b-1}\psi(4q^m - p^n)$	$q^{m+2(b-1)}$	$-2^4q^{2m+6(b-1)}p^n$
C2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^8q^{m+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

4. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $p^n - 4q^m$ is a square, $q^m \equiv -1 \pmod 4$, n odd and $p \equiv 5 \pmod 8$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$-\epsilon \cdot q^{b-1}\psi(p^n - 4q^m)$	$-q^{m+2(b-1)}$	$2^4q^{2m+6(b-1)}p^n$
D2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 4q^m)$	$q^{2(b-1)}p^n$	$-2^8q^{m+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

5. *There exist integers* $\ell \in \{4,5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^\ell q^m + p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m + p^n)$	$2^{\ell-2}q^{m+2(b-1)}$	$2^{2\ell}q^{2m+6(b-1)}p^n$
E2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m + p^n)$	$q^{2(b-1)}p^n$	$2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

6. *There exist integers* $\ell \in \{4,5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^\ell q^m - p^n$ *is a square,* $p \equiv 7 \pmod 8$, n *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot q^{b-1}\psi(2^\ell q^m - p^n)$	$2^{\ell-2}q^{m+2(b-1)}$	$-2^{2\ell}q^{2m+6(b-1)}p^n$
F2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

7. *There exist integers* $\ell \in \{4,5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $p^n - 2^\ell q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot q^{b-1}\psi(p^n - 2^\ell q^m)$	$-2^{\ell-2}q^{m+2(b-1)}$	$2^{2\ell}q^{2m+6(b-1)}p^n$
G2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 2^\ell q^m)$	$q^{2(b-1)}p^n$	$-2^{\ell+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

8. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n + q^m$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$-q^{b-1}\psi(4p^n + q^m)$	$q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)}p^{2n}$
H2	$2 \cdot q^{b-1}\psi(4p^n + q^m)$	$q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)}p^n$

9. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n - q^m$ *is a square,* $q \equiv 3 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$-\epsilon \cdot q^{b-1}\psi(4p^n - q^m)$	$q^{2(b-1)}p^n$	$-2^4 q^{m+6(b-1)}p^{2n}$
I2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(4p^n - q^m)$	$-q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

10. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 4p^n$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
J1	$-q^{b-1}\psi(q^m - 4p^n)$	$-q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)}p^{2n}$
J2	$2 \cdot q^{b-1}\psi(q^m - 4p^n)$	$q^{m+2(b-1)}$	$-2^8 q^{2m+6(b-1)}p^n$

11. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^\ell p^n + q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot q^{b-1}\psi(2^\ell p^n + q^m)$	$2^{\ell-2}q^{2(b-1)}p^n$	$2^{2\ell}q^{m+6(b-1)}p^{2n}$
K2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell p^n + q^m)$	$q^{m+2(b-1)}$	$2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

12. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^\ell p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$, m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot q^{b-1}\psi(2^\ell p^n - q^m)$	$2^{\ell-2}q^{2(b-1)}p^n$	$-2^{2\ell}q^{m+6(b-1)}p^{2n}$
L2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell p^n - q^m)$	$-q^{m+2(b-1)}$	$2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

13. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 2^\ell p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot q^{b-1}\psi(q^m - 2^\ell p^n)$	$-2^{\ell-2}q^{2(b-1)}p^n$	$2^{2\ell}q^{m+6(b-1)}p^{2n}$
M2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m - 2^\ell p^n)$	$q^{m+2(b-1)}$	$-2^{\ell+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

14. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
N1	$-\epsilon \cdot q^{b-1}\psi(4 + q^m p^n)$	$q^{2(b-1)}$	$2^4 q^{m+6(b-1)}p^n$
N2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(4 + q^m p^n)$	$q^{m+2(b-1)}p^n$	$2^8 q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

15. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^\ell + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot q^{b-1}\psi(2^\ell + q^m p^n)$	$2^{\ell-2}q^{2(b-1)}$	$2^{2\ell}q^{m+6(b-1)}p^n$
O2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell + q^m p^n)$	$q^{m+2(b-1)}p^n$	$2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

16. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot q^{b-1}\psi(2^\ell - q^m p^n)$	$2^{\ell-2}q^{2(b-1)}$	$-2^{2\ell}q^{m+6(b-1)}p^n$
P2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(2^\ell - q^m p^n)$	$-q^{m+2(b-1)}p^n$	$2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

17. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
Q1	$\epsilon \cdot q^{b-1}\psi(q^m p^n - 2^\ell)$	$-2^{\ell-2}q^{2(b-1)}$	$2^{2\ell}q^{m+6(b-1)}p^n$
Q2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m p^n - 2^\ell)$	$q^{m+2(b-1)}p^n$	$-2^{\ell+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

In the case that $b = 2$*, we furthermore could have one of the following conditions satisfied:*

18. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{4p^n+1}{q}$ *is a square,* $p^n \equiv 1 \pmod 4$*,* $q \equiv 5 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
R1	$-q^{s+1}\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^n$	$2^4 q^{6s+3}p^{2n}$
R2	$2 \cdot q^{s+1}\psi(\frac{4p^n+1}{q})$	q^{2s+1}	$2^8 q^{6s+3}p^n$

19. *there exist integers* $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{4p^n-1}{q}$ *is a square,* $p^n \equiv 3 \pmod 4$*,* $q \equiv 3 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
S1	$-\epsilon \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$q^{2s+1}p^n$	$-2^4q^{6s+3}p^{2n}$
S2	$\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$-q^{2s+1}$	$2^8q^{6s+3}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

20. *there exist integers* $\ell \in \{4,5\}$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n+1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
T1	$q^{s+1}\psi(\frac{2^\ell p^n+1}{q})$	$2^{\ell-2}q^{2s+1}p^n$	$2^{2\ell}q^{6s+3}p^{2n}$
T2	$-2 \cdot q^{s+1}\psi(\frac{2^\ell p^n+1}{q})$	q^{2s+1}	$2^{\ell+6}q^{6s+3}p^n$

21. *there exist integers* $\ell \in \{4,5\}$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n-1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
U1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell p^n-1}{q})$	$2^{\ell-2}q^{2s+1}p^n$	$-2^{2\ell}q^{6s+3}p^{2n}$
U2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell p^n-1}{q})$	$-q^{2s+1}$	$2^{\ell+6}q^{6s+3}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

22. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{4+p^n}{q}$ *is a square,* $q \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
V1	$-q^{s+1}\psi(\frac{4+p^n}{q})$	q^{2s+1}	$2^4q^{6s+3}p^n$
V2	$2 \cdot q^{s+1}\psi(\frac{4+p^n}{q})$	$q^{2s+1}p^n$	$2^8q^{6s+3}p^{2n}$

23. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-4}{q}$ *is a square,* $q \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
W1	$-\epsilon \cdot q^{s+1}\psi(\frac{p^n-4}{q})$	$-q^{2s+1}$	$2^4q^{6s+3}p^n$
W2	$\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{p^n-4}{q})$	$q^{2s+1}p^n$	$-2^8q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

24. *there exist integers* $\ell \in \{4,5\}$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
X1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell+p^n}{q})$	$2^{\ell-2}q^{2s+1}$	$2^{2\ell}q^{6s+3}p^n$
X2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell+p^n}{q})$	$q^{2s+1}p^n$	$2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

25. *there exist integers* $\ell \in \{4, 5\}$, $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^\ell - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Y1	$\epsilon \cdot q^{s+1}\psi(\frac{2^\ell-p^n}{q})$	$2^{\ell-2}q^{2s+1}$	$-2^{2\ell}q^{6s+3}p^n$
Y2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^\ell-p^n}{q})$	$-q^{2s+1}p^n$	$2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

26. *there exist integers* $\ell \in \{4, 5\}$, $n \geq 1$ *and* $s \in \{0, 1\}$ *such that* $\frac{p^n - 2^\ell}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Z1	$\epsilon \cdot q^{s+1}\psi(\frac{p^n-2^\ell}{q})$	$-2^{\ell-2}q^{2s+1}$	$2^{2\ell}q^{6s+3}p^n$
Z2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{p^n-2^\ell}{q})$	$q^{2s+1}p^n$	$-2^{\ell+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

Theorem 2.2.5. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* 2^4q^bp *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 4$, $m \geq 2 - b$ *and* $n \geq 1$ *such that* $2^l q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$-\epsilon \cdot q^{b-1}\psi(2^l q^m p^n + 1)$	$2^{l-2}q^{m+2(b-1)}p^n$	$2^{2l}q^{2m+6(b-1)}p^{2n}$
A2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l q^m p^n + 1)$	$q^{2(b-1)}$	$2^{l+6}q^{m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

2. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4q^m + p^n$ *is a square,* $q^m \equiv 1 \pmod 4$, *n even or* $p \equiv 1 \pmod 4$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{m+2(b-1)}$	$2^4q^{2m+6(b-1)}p^n$
B2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m + p^n)$	$q^{2(b-1)}p^n$	$2^8q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{m+b-1} *modulo* 4.

3. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4q^m - p^n$ *is a square,* $q^m \equiv 1 \pmod 4$*,* n *odd and* $p \equiv 3 \pmod 8$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot q^{b-1}\psi(4q^m - p^n)$	$q^{m+2(b-1)}$	$-2^4 q^{2m+6(b-1)}p^n$
C2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^8 q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{m+b-1} *modulo* 4.

4. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $p^n - 4q^m$ *is a square,* $q^m \equiv -1 \pmod 4$*,* n *even or* $p \equiv 1 \pmod 4$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot q^{b-1}\psi(p^n - 4q^m)$	$-q^{m+2(b-1)}$	$2^4 q^{2m+6(b-1)}p^n$
D2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 4q^m)$	$q^{2(b-1)}p^n$	$-2^8 q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{m+b-1} *modulo* 4.

5. *There exist integers* $\ell \geq 4$*,* $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^l q^m + p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$-\epsilon \cdot q^{b-1}\psi(2^l q^m + p^n)$	$2^{l-2}q^{m+2(b-1)}$	$2^{2l}q^{2m+6(b-1)}p^n$
E2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l q^m + p^n)$	$q^{2(b-1)}p^n$	$2^{l+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

6. *There exist integers* $\ell \geq 4$*,* $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^l q^m - p^n$ *is a square,* $p \equiv 7 \pmod 8$*,* n *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$-\epsilon \cdot q^{b-1}\psi(2^l q^m - p^n)$	$2^{l-2}q^{m+2(b-1)}$	$-2^{2l}q^{2m+6(b-1)}p^n$
F2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^{l+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

7. *There exist integers* $\ell \geq 4$*,* $m \geq 2-b$ *and* $n \geq 1$ *such that* $p^n - 2^l q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$-\epsilon \cdot q^{b-1}\psi(p^n - 2^l q^m)$	$-2^{l-2}q^{m+2(b-1)}$	$2^{2l}q^{2m+6(b-1)}p^n$
G2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(p^n - 2^l q^m)$	$q^{2(b-1)}p^n$	$-2^{l+6}q^{m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

8. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n + q^m$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$q^{b-1}\psi(4p^n + q^m)$	$q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)}p^{2n}$
H2	$-2 \cdot q^{b-1}\psi(4p^n + q^m)$	$q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)}p^n$

9. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4p^n - q^m$ *is a square,* $q \equiv 3 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot q^{b-1}\psi(4p^n - q^m)$	$q^{2(b-1)}p^n$	$-2^4 q^{m+6(b-1)}p^{2n}$
I2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4p^n - q^m)$	$-q^{m+2(b-1)}$	$2^8 q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{b-1}p^n$ *modulo* 4.

10. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 4p^n$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
J1	$q^{b-1}\psi(q^m - 4p^n)$	$-q^{2(b-1)}p^n$	$2^4 q^{m+6(b-1)}p^{2n}$
J2	$-2 \cdot q^{b-1}\psi(q^m - 4p^n)$	$q^{m+2(b-1)}$	$-2^8 q^{2m+6(b-1)}p^n$

11. *There exist integers* $\ell \geq 4$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^l p^n + q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
K1	$-\epsilon \cdot q^{b-1}\psi(2^l p^n + q^m)$	$2^{l-2}q^{2(b-1)}p^n$	$2^{2l}q^{m+6(b-1)}p^{2n}$
K2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l p^n + q^m)$	$q^{m+2(b-1)}$	$2^{l+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

12. *There exist integers* $\ell \geq 4$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^l p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$, m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
L1	$-\epsilon \cdot q^{b-1}\psi(2^l p^n - q^m)$	$2^{l-2}q^{2(b-1)}p^n$	$-2^{2l}q^{m+6(b-1)}p^{2n}$
L2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l p^n - q^m)$	$-q^{m+2(b-1)}$	$2^{l+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

13. *There exist integers* $\ell \geq 4$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m - 2^l p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
M1	$-\epsilon \cdot q^{b-1}\psi(q^m - 2^l p^n)$	$-2^{l-2}q^{2(b-1)}p^n$	$2^{2l}q^{m+6(b-1)}p^{2n}$
M2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m - 2^l p^n)$	$q^{m+2(b-1)}$	$-2^{l+6}q^{2m+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

14. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $4 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot q^{b-1}\psi(4 + q^m p^n)$	$q^{2(b-1)}$	$2^4 q^{m+6(b-1)}p^n$
N2	$-\epsilon \cdot 2 \cdot q^{b-1}\psi(4 + q^m p^n)$	$q^{m+2(b-1)}p^n$	$2^8 q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

15. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $q^m p^n - 4$ *is a square,* $p \equiv 1 \pmod 4$, $q \equiv 1 \pmod 4$ *if* $m \geq 1$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
O1	$-\epsilon \cdot q^{b-1}\psi(q^m p^n - 4)$	$-q^{2(b-1)}$	$2^4 q^{m+6(b-1)}p^n$
O2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(q^m p^n - 4)$	$q^{m+2(b-1)}p^n$	$-2^{10} q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

16. *There exist integers* $\ell \geq 4$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^l + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
P1	$-\epsilon \cdot q^{b-1}\psi(2^l + q^m p^n)$	$2^{l-2}q^{2(b-1)}$	$2^{2l}q^{m+6(b-1)}p^n$
P2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l + q^m p^n)$	$q^{m+2(b-1)}p^n$	$2^{l+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{b-1} *modulo* 4.

17. *There exist integers $\ell \geq 4$, $m \geq 2-b$ and $n \geq 1$ such that $2^l - q^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
Q1	$-\epsilon \cdot q^{b-1}\psi(2^l - q^m p^n)$	$2^{l-2}q^{2(b-1)}$	$-2^{2l}q^{m+6(b-1)}p^n$
Q2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(2^l - q^m p^n)$	$-q^{m+2(b-1)}p^n$	$2^{l+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

18. *There exist integers $\ell \geq 4$, $m \geq 2-b$ and $n \geq 1$ such that $q^l p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
R1	$-\epsilon \cdot q^{b-1}\psi(q^l p^n - 2^m)$	$-2^{l-2}q^{2(b-1)}$	$2^{2l}q^{m+6(b-1)}p^n$
R2	$\epsilon \cdot 2 \cdot q^{b-1}\psi(q^l p^n - 2^m)$	$q^{m+2(b-1)}p^n$	$-2^{l+6}q^{2m+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of q^{b-1} modulo 4.

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

19. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n+1}{q}$ is a square, $p^n \equiv 1 \pmod 4$, $q \equiv 5 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
S1	$q^{s+1}\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^n$	$2^4 q^{6s+3}p^{2n}$
S2	$-2 \cdot q^{s+1}\psi(\frac{4p^n+1}{q})$	q^{2s+1}	$2^8 q^{6s+3}p^n$

20. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{q}$ is a square, $p^n \equiv 3 \pmod 4$, $q \equiv 3 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
T1	$\epsilon \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$q^{2s+1}p^n$	$-2^4 q^{6s+3}p^{2n}$
T2	$-\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{4p^n-1}{q})$	$-q^{2s+1}$	$2^8 q^{6s+3}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of $q^s p^n$ modulo 4.

21. *there exist integers $\ell \geq 4$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^l p^n+1}{q}$ is a square, $q \equiv 1 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
U1	$-q^{s+1}\psi(\frac{2^l p^n+1}{q})$	$2^{l-2}q^{2s+1}p^n$	$2^{2l}q^{6s+3}p^{2n}$
U2	$2\cdot q^{s+1}\psi(\frac{2^l p^n+1}{q})$	q^{2s+1}	$2^{l+6}q^{6s+3}p^n$

22. *there exist integers* $\ell \geq 4$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l p^n-1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
V1	$-\epsilon\cdot q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$2^{l-2}q^{2s+1}p^n$	$-2^{2l}q^{6s+3}p^{2n}$
V2	$\epsilon\cdot 2\cdot q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$-q^{2s+1}$	$2^{l+6}q^{6s+3}p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

23. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{4+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
W1	$\epsilon q^{s+1}\psi(\frac{4+p^n}{q})$	q^{2s+1}	$2^4 q^{6s+3}p^n$
W2	$-\epsilon 2\cdot q^{s+1}\psi(\frac{4+p^n}{q})$	$q^{2s+1}p^n$	$2^8 q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^s *modulo* 4.

24. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-4}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
X1	$\epsilon\cdot q^{s+1}\psi(\frac{p^n-4}{q})$	$-q^{2s+1}$	$2^4 q^{6s+3}p^n$
X2	$-\epsilon\cdot 2\cdot q^{s+1}\psi(\frac{p^n-4}{q})$	$q^{2s+1}p^n$	$-2^8 q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $-q^s$ *modulo* 4.

25. *there exist integers* $\ell \geq 4$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Y1	$-\epsilon\cdot q^{s+1}\psi(\frac{2^l+p^n}{q})$	$2^{l-2}q^{2s+1}$	$2^{2l}q^{6s+3}p^n$
Y2	$\epsilon\cdot 2\cdot q^{s+1}\psi(\frac{2^l+p^n}{q})$	$q^{2s+1}p^n$	$2^{l+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

26. *there exist integers* $\ell \geq 4$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Z1	$-\epsilon \cdot q^{s+1}\psi(\frac{2^l-p^n}{q})$	$2^{l-2}q^{2s+1}$	$-2^{2l}q^{6s+3}p^n$
Z2	$\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{2^l-p^n}{q})$	$-q^{2s+1}p^n$	$2^{l+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

27. *there exist integers* $\ell \geq 4$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n - 2^l}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
AA1	$-\epsilon \cdot q^{s+1}\psi(\frac{p^n-2^l}{q})$	$-2^{l-2}q^{2s+1}$	$2^{2l}q^{6s+3}p^n$
AA2	$\epsilon \cdot 2 \cdot q^{s+1}\psi(\frac{p^n-2^l}{q})$	$q^{2s+1}p^n$	$-2^{l+6}q^{6s+3}p^{2n}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q^{s+1} *modulo* 4.

Theorem 2.2.6. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* 2^5q^bp *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $8q^mp^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$q^{b-1}\psi(8q^mp^n+1)$	$2q^{m+2(b-1)}p^n$	$2^6q^{2m+6(b-1)}p^{2n}$
A2	$-2 \cdot q^{b-1}\psi(8q^mp^n+1)$	$q^{2(b-1)}$	$2^9q^{m+6(b-1)}p^n$
A1′	$-q^{b-1}\psi(8q^mp^n+1)$	$2q^{m+2(b-1)}p^n$	$2^6q^{2m+6(b-1)}p^{2n}$
A2′	$2 \cdot q^{b-1}\psi(8q^mp^n+1)$	$q^{2(b-1)}$	$2^9q^{m+6(b-1)}p^n$

2. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $8q^m + p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$q^{b-1}\psi(8q^m+p^n)$	$2q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
B2	$-2 \cdot q^{b-1}\psi(8q^m+p^n)$	$q^{2(b-1)}p^n$	$2^9q^{m+6(b-1)}p^{2n}$
B1′	$-q^{b-1}\psi(8q^m+p^n)$	$2q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
B2′	$2 \cdot q^{b-1}\psi(8q^m+p^n)$	$q^{2(b-1)}p^n$	$2^9q^{m+6(b-1)}p^{2n}$

3. *There exist integers* $m \geq 2-b$ *and* $n \geq 1$ *such that* $8q^m - p^n$ *is a square,* $p \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$q^{b-1}\psi(8q^m - p^n)$	$2q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)}p^n$
C2	$-2 \cdot q^{b-1}\psi(8q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^9 q^{m+6(b-1)}p^{2n}$
C1′	$-q^{b-1}\psi(8q^m - p^n)$	$2q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)}p^n$
C2′	$2 \cdot q^{b-1}\psi(8q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^9 q^{m+6(b-1)}p^{2n}$

4. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $p^n - 8q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$q^{b-1}\psi(p^n - 8q^m$	$-2q^{m+2(b-1)}$	$2^6 q^{2m+6(b-1)}p^n$
D2	$-2 \cdot q^{b-1}\psi(p^n - 8q^m$	$q^{2(b-1)}p^n$	$-2^9 q^{m+6(b-1)}p^{2n}$
D1′	$-q^{b-1}\psi(p^n - 8q^m$	$-2q^{m+2(b-1)}$	$2^6 q^{2m+6(b-1)}p^n$
D2′	$2 \cdot q^{b-1}\psi(p^n - 8q^m$	$q^{2(b-1)}p^n$	$-2^9 q^{m+6(b-1)}p^{2n}$

5. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $8p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$q^{b-1}\psi(8p^n + q^m)$	$2q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
E2	$-2 \cdot q^{b-1}\psi(8p^n + q^m)$	$q^{m+2(b-1)}$	$2^9 q^{2m+6(b-1)}p^n$
E1′	$-q^{b-1}\psi(8p^n + q^m)$	$2q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
E2′	$2 \cdot q^{b-1}\psi(8p^n + q^m)$	$q^{m+2(b-1)}$	$2^9 q^{2m+6(b-1)}p^n$

6. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $8p^n - q^m$ is a square, $q \equiv 7 \pmod 8$, m odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$q^{b-1}\psi(8p^n - q^m)$	$2q^{2(b-1)}p^n$	$-2^6 q^{m+6(b-1)}p^{2n}$
F2	$-2 \cdot q^{b-1}\psi(8p^n - q^m)$	$-q^{m+2(b-1)}$	$2^9 q^{2m+6(b-1)}p^n$
F1′	$-q^{b-1}\psi(8p^n - q^m)$	$2q^{2(b-1)}p^n$	$-2^6 q^{m+6(b-1)}p^{2n}$
F2′	$2 \cdot q^{b-1}\psi(8p^n - q^m)$	$-q^{m+2(b-1)}$	$2^9 q^{2m+6(b-1)}p^n$

7. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m - 8p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$q^{b-1}\psi(q^m - 8p^n)$	$-2q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
G2	$-2 \cdot q^{b-1}\psi(q^m - 8p^n)$	$q^{m+2(b-1)}$	$-2^9 q^{2m+6(b-1)}p^n$
G1′	$-q^{b-1}\psi(q^m - 8p^n)$	$-2q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
G2′	$2 \cdot q^{b-1}\psi(q^m - 8p^n)$	$q^{m+2(b-1)}$	$-2^9 q^{2m+6(b-1)}p^n$

8. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $8+q^m p^n$ is a square, $p \equiv 1,7 \pmod 8$, $q \equiv 1,7 \pmod 8$ if $m>0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$q^{b-1}\psi(8+q^m p^n)$	$2q^{2(b-1)}$	$2^6 q^{m+6(b-1)} p^n$
H2	$-2\cdot q^{b-1}\psi(8+q^m p^n)$	$q^{m+2(b-1)} p^n$	$2^9 q^{2m+6(b-1)} p^{2n}$
H1′	$-q^{b-1}\psi(8+q^m p^n)$	$2q^{2(b-1)}$	$2^6 q^{m+6(b-1)} p^n$
H2′	$2\cdot q^{b-1}\psi(8+q^m p^n)$	$q^{m+2(b-1)} p^n$	$2^9 q^{2m+6(b-1)} p^{2n}$

9. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m p^n - 8$ is a square, $p \equiv 1,3 \pmod 8$, $q \equiv 1,3 \pmod 8$ if $m>0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$q^{b-1}\psi(q^m p^n-8)$	$-2q^{2(b-1)}$	$2^6 q^{m+6(b-1)} p^n$
I2	$-2\cdot q^{b-1}\psi(q^m p^n-8)$	$q^{m+2(b-1)} p^n$	$-2^9 q^{2m+6(b-1)} p^{2n}$
I1′	$-q^{b-1}\psi(q^m p^n-8)$	$-2q^{2(b-1)}$	$2^6 q^{m+6(b-1)} p^n$
I2′	$2\cdot q^{b-1}\psi(q^m p^n-8)$	$q^{m+2(b-1)} p^n$	$-2^9 q^{2m+6(b-1)} p^{2n}$

10. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
J1	$2q^{b-1}\psi(q^m p^n+1)$	$q^{m+2(b-1)} p^n$	$2^6 q^{2m+6(b-1)} p^{2n}$
J2	$-4\cdot q^{b-1}\psi(q^m p^n+1)$	$4q^{2(b-1)}$	$2^{12} q^{m+6(b-1)} p^n$
J1′	$-2q^{b-1}\psi(q^m p^n+1)$	$q^{m+2(b-1)} p^n$	$2^6 q^{2m+6(b-1)} p^{2n}$
J2′	$4\cdot q^{b-1}\psi(q^m p^n+1)$	$4q^{2(b-1)}$	$2^{12} q^{m+6(b-1)} p^n$

11. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m p^n - 1$ is a square, $p \equiv 1 \pmod 4$ if $n>0$, $q \equiv 1 \pmod 4$ if $m>0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
K1	$2q^{b-1}\psi(q^m p^n-1)$	$q^{2(b-1)}$	$2^6 q^{2m+6(b-1)} p^{2n}$
K2	$-4\cdot q^{b-1}\psi(q^m p^n-1)$	$4q^{m+2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^n$
K1′	$-2q^{b-1}\psi(q^m p^n-1)$	$q^{2(b-1)}$	$2^6 q^{2m+6(b-1)} p^{2n}$
K2′	$4\cdot q^{b-1}\psi(q^m p^n-1)$	$4q^{m+2(b-1)} p^n$	$2^{12} q^{m+6(b-1)} p^n$

12. There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
L1	$2q^{b-1}\psi(q^m+p^n)$	$q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
L2	$-4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{m+2(b-1)}$	$2^{12}q^{2m+6(b-1)}p^n$
L1′	$-2q^{b-1}\psi(q^m+p^n)$	$q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
L2′	$4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{m+2(b-1)}$	$2^{12}q^{2m+6(b-1)}p^n$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
M1	$2q^{b-1}\psi(q^m+p^n)$	$q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
M2	$-4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$
M1′	$-2q^{b-1}\psi(q^m+p^n)$	$q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
M2′	$4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$

13. There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
N1	$2q^{b-1}\psi(q^m-p^n)$	$-q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
N2	$-4\cdot q^{b-1}\psi(q^m-p^n)$	$4q^{m+2(b-1)}$	$-2^{12}q^{2m+6(b-1)}p^n$
N1′	$-2q^{b-1}\psi(q^m-p^n)$	$-q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
N2′	$4\cdot q^{b-1}\psi(q^m-p^n)$	$4q^{m+2(b-1)}$	$-2^{12}q^{2m+6(b-1)}p^n$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
O1	$2q^{b-1}\psi(q^m-p^n)$	$q^{m+2(b-1)}$	$-2^6q^{2m+6(b-1)}p^n$
O2	$-4\cdot q^{b-1}\psi(q^m-p^n)$	$-4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$
O1′	$-2q^{b-1}\psi(q^m-p^n)$	$q^{m+2(b-1)}$	$-2^6q^{2m+6(b-1)}p^n$
O2′	$4\cdot q^{b-1}\psi(q^m-p^n)$	$-4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$

14. There exist integers $m \geq 2-b$ and $n \geq 1$ such that $p^n - q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
P1	$2q^{b-1}\psi(p^n - q^m)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
P2	$-4 \cdot q^{b-1}\psi(p^n - q^m)$	$4q^{m+2(b-1)}$	$-2^{12}q^{2m+6(b-1)}p^n$
P1′	$-2q^{b-1}\psi(p^n - q^m)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)}p^{2n}$
P2′	$4 \cdot q^{b-1}\psi(p^n - q^m)$	$4q^{m+2(b-1)}$	$-2^{12}q^{2m+6(b-1)}p^n$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
Q1	$2q^{b-1}\psi(p^n - q^m)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)}p^n$
Q2	$-4 \cdot q^{b-1}\psi(p^n - q^m)$	$-4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$
Q1′	$-2q^{b-1}\psi(p^n - q^m)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)}p^n$
Q2′	$4 \cdot q^{b-1}\psi(p^n - q^m)$	$-4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

15. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{8p^n+1}{q}$ is a square, $q \equiv 1 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
R1	$q^{s+1}\psi(\frac{8p^n+1}{q})$	$2q^{2s+1}p^n$	$2^6 q^{6s+3}p^{2n}$
R2	$-2 \cdot q^{s+1}\psi(\frac{8p^n+1}{q})$	q^{2s+1}	$2^9 q^{6s+3}p^n$
R1′	$-q^{s+1}\psi(\frac{8p^n+1}{q})$	$2q^{2s+1}p^n$	$2^6 q^{6s+3}p^{2n}$
R2′	$2 \cdot q^{s+1}\psi(\frac{8p^n+1}{q})$	q^{2s+1}	$2^9 q^{6s+3}p^n$

16. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{8p^n-1}{q}$ is a square, $q \equiv 7 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
S1	$q^{s+1}\psi(\frac{8p^n-1}{q})$	$2q^{2s+1}p^n$	$-2^6 q^{6s+3}p^{2n}$
S2	$-2 \cdot q^{s+1}\psi(\frac{8p^n-1}{q})$	$-q^{2s+1}$	$2^9 q^{6s+3}p^n$
S1′	$-q^{s+1}\psi(\frac{8p^n-1}{q})$	$2q^{2s+1}p^n$	$-2^6 q^{6s+3}p^{2n}$
S2′	$2 \cdot q^{s+1}\psi(\frac{8p^n-1}{q})$	$-q^{2s+1}$	$2^9 q^{6s+3}p^n$

17. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{8+p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
T1	$q^{s+1}\psi(\frac{8+p^n}{q})$	$2q^{2s+1}$	$2^6q^{6s+3}p^n$
T2	$-2\cdot q^{s+1}\psi(\frac{8+p^n}{q})$	$q^{2s+1}p^n$	$2^9q^{6s+3}p^{2n}$
T1′	$-q^{s+1}\psi(\frac{8+p^n}{q})$	$2q^{2s+1}$	$2^6q^{6s+3}p^n$
T2′	$2\cdot q^{s+1}\psi(\frac{8+p^n}{q})$	$q^{2s+1}p^n$	$2^9q^{6s+3}p^{2n}$

18. *there exist integers* $n\geq 1$ *and* $s\in\{0,1\}$ *such that* $\frac{8-p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
U1	$q^{s+1}\psi(\frac{8-p^n}{q})$	$2q^{2s+1}$	$-2^6q^{6s+3}p^n$
U2	$-2\cdot q^{s+1}\psi(\frac{8-p^n}{q})$	$-q^{2s+1}p^n$	$2^9q^{6s+3}p^{2n}$
U1′	$-q^{s+1}\psi(\frac{8-p^n}{q})$	$2q^{2s+1}$	$-2^6q^{6s+3}p^n$
U2′	$2\cdot q^{s+1}\psi(\frac{8-p^n}{q})$	$-q^{2s+1}p^n$	$2^9q^{6s+3}p^{2n}$

19. *there exist integers* $n\geq 1$ *and* $s\in\{0,1\}$ *such that* $\frac{p^n-8}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
V1	$q^{s+1}\psi(\frac{p^n-8}{q})$	$-2q^{2s+1}$	$2^6q^{6s+3}p^n$
V2	$-2\cdot q^{s+1}\psi(\frac{p^n-8}{q})$	$q^{2s+1}p^n$	$-2^9q^{6s+3}p^{2n}$
V1′	$-q^{s+1}\psi(\frac{p^n-8}{q})$	$-2q^{2s+1}$	$2^6q^{6s+3}p^n$
V2′	$2\cdot q^{s+1}\psi(\frac{p^n-8}{q})$	$q^{2s+1}p^n$	$-2^9q^{6s+3}p^{2n}$

20. *there exist integers* $n\geq 1$ *and* $s\in\{0,1\}$ *such that* $\frac{p^n+1}{q}$ *is a square,* $q\equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
W1	$q^{s+1}\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^n$	$2^6q^{6s+3}p^{2n}$
W2	$-2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}$	$2^{12}q^{6s+3}p^n$
W1′	$-q^{s+1}\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^n$	$2^6q^{6s+3}p^{2n}$
W2′	$2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}$	$2^{12}q^{6s+3}p^n$

21. *there exist integers* $n\geq 1$ *and* $s\in\{0,1\}$ *such that* $\frac{p^n+1}{q}$ *is a square,* $q\equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
X1	$q^{s+1}\psi(\frac{p^n+1}{q})$	q^{2s+1}	$2^6q^{6s+3}p^n$
X2	$-2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^n$	$2^{12}q^{6s+3}p^{2n}$
X1′	$-q^{s+1}\psi(\frac{p^n+1}{q})$	q^{2s+1}	$2^6q^{6s+3}p^n$
X2′	$2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^n$	$2^{12}q^{6s+3}p^{2n}$

22. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-1}{q}$ *is a square,* $q \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Y1	$q^{s+1}\psi(\frac{p^n-1}{q})$	$-q^{2s+1}$	$2^6q^{6s+3}p^n$
Y2	$-2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^n$	$-2^{12}q^{6s+3}p^{2n}$
Y1′	$-q^{s+1}\psi(\frac{p^n-1}{q})$	$-q^{2s+1}$	$2^6q^{6s+3}p^n$
Y2′	$2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^n$	$-2^{12}q^{6s+3}p^{2n}$

23. *there exist integers* $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-1}{q}$ *is a square,* $q \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
Z1	$q^{s+1}\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^n$	$-2^6q^{6s+3}p^{2n}$
Z2	$-2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}$	$2^{12}q^{6s+3}p^n$
Z1′	$-q^{s+1}\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^n$	$-2^6q^{6s+3}p^{2n}$
Z2′	$2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}$	$2^{12}q^{6s+3}p^n$

Theorem 2.2.7. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* 2^6q^bp *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 3$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^lq^mp^n+1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$2q^{b-1}\psi(2^lq^mp^n+1)$	$2^lq^{m+2(b-1)}p^n$	$2^{2l+6}q^{2m+6(b-1)}p^{2n}$
A2	$-4\cdot q^{b-1}\psi(2^lq^mp^n+1)$	$4q^{2(b-1)}$	$2^{l+12}q^{m+6(b-1)}p^n$
A1′	$-2q^{b-1}\psi(2^lq^mp^n+1)$	$2^lq^{m+2(b-1)}p^n$	$2^{2l+6}q^{2m+6(b-1)}p^{2n}$
A2′	$4\cdot q^{b-1}\psi(2^lq^mp^n+1)$	$4q^{2(b-1)}$	$2^{l+12}q^{m+6(b-1)}p^n$

2. *There exist integers* $\ell \geq 2$, $m \geq 2-b$ *and* $n \geq 1$ *such that* $2^lq^m+p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$2q^{b-1}\psi(2^lq^m+p^n)$	$2^lq^{m+2(b-1)}$	$2^{2l+6}q^{2m+6(b-1)}p^n$
B2	$-4\cdot q^{b-1}\psi(2^lq^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{l+12}q^{m+6(b-1)}p^{2n}$
B1′	$-2q^{b-1}\psi(2^lq^m+p^n)$	$2^lq^{m+2(b-1)}$	$2^{2l+6}q^{2m+6(b-1)}p^n$
B2′	$4\cdot q^{b-1}\psi(2^lq^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{l+12}q^{m+6(b-1)}p^{2n}$

3. *There exist integers $\ell \geq 2$, $m \geq 2-b$ and $n \geq 1$ such that $2^l q^m - p^n$ is a square, n odd, $p \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$2q^{b-1}\psi(2^l q^m - p^n)$	$2^l q^{m+2(b-1)}$	$-2^{2l+6}q^{2m+6(b-1)}p^n$
C2	$-4 \cdot q^{b-1}\psi(2^l q^m - p^n)$	$-4q^{2(b-1)}p^n$	$2^{l+12}q^{m+6(b-1)}p^{2n}$
C1′	$-2q^{b-1}\psi(2^l q^m - p^n)$	$2^l q^{m+2(b-1)}$	$-2^{2l+6}q^{2m+6(b-1)}p^n$
C2′	$4 \cdot q^{b-1}\psi(2^l q^m - p^n)$	$-4q^{2(b-1)}p^n$	$2^{l+12}q^{m+6(b-1)}p^{2n}$

4. *There exist integers $\ell \geq 2$, $m \geq 2-b$ and $n \geq 1$ such that $p^n - 2^l q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$2q^{b-1}\psi(p^n - 2^l q^m$	$-2^l q^{m+2(b-1)}$	$2^{2l+6}q^{2m+6(b-1)}p^n$
D2	$-4 \cdot q^{b-1}\psi(p^n - 2^l q^m$	$4q^{2(b-1)}p^n$	$-2^{l+12}q^{m+6(b-1)}p^{2n}$
D1′	$-2q^{b-1}\psi(p^n - 2^l q^m$	$-2^l q^{m+2(b-1)}$	$2^{2l+6}q^{2m+6(b-1)}p^n$
D2′	$4 \cdot q^{b-1}\psi(p^n - 2^l q^m$	$4q^{2(b-1)}p^n$	$-2^{l+12}q^{m+6(b-1)}p^{2n}$

5. *There exist integers $\ell \geq 2$, $m \geq 2-b$ and $n \geq 1$ such that $2^l p^n + q^m$ is a square, $q \equiv 5 \pmod 8$ when $l = 2$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$2q^{b-1}\psi(2^l p^n + q^m)$	$2^l q^{2(b-1)}p^n$	$2^{2l+6}q^{m+6(b-1)}p^{2n}$
E2	$-4 \cdot q^{b-1}\psi(2^l p^n + q^m)$	$4q^{m+2(b-1)}$	$2^{l+12}q^{2m+6(b-1)}p^n$
E1′	$-2q^{b-1}\psi(2^l p^n + q^m)$	$2^l q^{2(b-1)}p^n$	$2^{2l+6}q^{m+6(b-1)}p^{2n}$
E2′	$4 \cdot q^{b-1}\psi(2^l p^n + q^m)$	$4q^{m+2(b-1)}$	$2^{l+12}q^{2m+6(b-1)}p^n$

6. *There exist integers $\ell \geq 2$, $m \geq 2-b$ and $n \geq 1$ such that $2^l p^n - q^m$ is a square, $q \equiv 7 \pmod 8$ when $l \geq 3$ or $q \equiv 3 \pmod 8$ if $l = 2$, m odd, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$2q^{b-1}\psi(2^l p^n - q^m)$	$2^l q^{2(b-1)}p^n$	$-2^{2l+6}q^{m+6(b-1)}p^{2n}$
F2	$-4 \cdot q^{b-1}\psi(2^l p^n - q^m)$	$-4q^{m+2(b-1)}$	$2^{l+12}q^{2m+6(b-1)}p^n$
F1′	$-2q^{b-1}\psi(2^l p^n - q^m)$	$2^l q^{2(b-1)}p^n$	$-2^{2l+6}q^{m+6(b-1)}p^{2n}$
F2′	$4 \cdot q^{b-1}\psi(2^l p^n - q^m)$	$-4q^{m+2(b-1)}$	$2^{l+12}q^{2m+6(b-1)}p^n$

7. *There exist integers $\ell \geq 2$, $m \geq 2-b$ and $n \geq 1$ such that $q^m - 2^l p^n$ is a square, $q \equiv 5 \pmod 8$ when $l = 2$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$2q^{b-1}\psi(q^m - 2^l p^n)$	$-2^l q^{2(b-1)} p^n$	$2^{2l+6} q^{m+6(b-1)} p^{2n}$
G2	$-4 \cdot q^{b-1}\psi(q^m - 2^l p^n)$	$4q^{m+2(b-1)}$	$-2^{l+12} q^{2m+6(b-1)} p^n$
G1′	$-2q^{b-1}\psi(q^m - 2^l p^n)$	$-2^l q^{2(b-1)} p^n$	$2^{2l+6} q^{m+6(b-1)} p^{2n}$
G2′	$4 \cdot q^{b-1}\psi(q^m - 2^l p^n)$	$4q^{m+2(b-1)}$	$-2^{l+12} q^{2m+6(b-1)} p^n$

8. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^l + q^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$2q^{b-1}\psi(2^l + q^m p^n)$	$2^l q^{2(b-1)}$	$2^{2l+6} q^{m+6(b-1)} p^n$
H2	$-4 \cdot q^{b-1}\psi(2^l + q^m p^n)$	$4q^{m+2(b-1)} p^n$	$2^{l+12} q^{2m+6(b-1)} p^{2n}$
H1′	$-2q^{b-1}\psi(2^l + q^m p^n)$	$2^l q^{2(b-1)}$	$2^{2l+6} q^{m+6(b-1)} p^n$
H2′	$4 \cdot q^{b-1}\psi(2^l + q^m p^n)$	$4q^{m+2(b-1)} p^n$	$2^{l+12} q^{2m+6(b-1)} p^{2n}$

9. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^l - q^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$2q^{b-1}\psi(2^l - q^m p^n)$	$2^l q^{2(b-1)}$	$-2^{2l+6} q^{m+6(b-1)} p^n$
I2	$-4 \cdot q^{b-1}\psi(2^l - q^m p^n)$	$-4q^{m+2(b-1)} p^n$	$2^{l+12} q^{2m+6(b-1)} p^{2n}$
I1′	$-2q^{b-1}\psi(2^l - q^m p^n)$	$2^l q^{2(b-1)}$	$-2^{2l+6} q^{m+6(b-1)} p^n$
I2′	$4 \cdot q^{b-1}\psi(2^l - q^m p^n)$	$-4q^{m+2(b-1)} p^n$	$2^{l+12} q^{2m+6(b-1)} p^{2n}$

10. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $q^m p^n - 2^l$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$2q^{b-1}\psi(q^m p^n - 2^l)$	$-2^l q^{2(b-1)}$	$2^{2l+6} q^{m+6(b-1)} p^n$
J2	$-4 \cdot q^{b-1}\psi(q^m p^n - 2^l)$	$4q^{m+2(b-1)} p^n$	$-2^{l+12} q^{2m+6(b-1)} p^{2n}$
J1′	$-2q^{b-1}\psi(q^m p^n - 2^l)$	$-2^l q^{2(b-1)}$	$2^{2l+6} q^{m+6(b-1)} p^n$
J2′	$4 \cdot q^{b-1}\psi(q^m p^n - 2^l)$	$4q^{m+2(b-1)} p^n$	$-2^{l+12} q^{2m+6(b-1)} p^{2n}$

11. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
K1	$2q^{b-1}\psi(q^mp^n+1)$	$q^{2(b-1)}$	$2^6q^{2m+6(b-1)}p^{2n}$
K2	$-4\cdot q^{b-1}\psi(q^mp^n+1)$	$4q^{m+2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^n$
K1′	$-2q^{b-1}\psi(q^mp^n+1)$	$q^{2(b-1)}$	$2^6q^{2m+6(b-1)}p^{2n}$
K2′	$4\cdot q^{b-1}\psi(q^mp^n+1)$	$4q^{m+2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^n$

12. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that q^mp^n-1 is a square, $p \equiv 1 \pmod 4$, $q \equiv 1 \pmod 4$ if $m > 0$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
L1	$2q^{b-1}\psi(q^mp^n-1)$	$q^{m+2(b-1)}p^n$	$2^6q^{2m+6(b-1)}p^{2n}$
L2	$-4\cdot q^{b-1}\psi(q^mp^n-1)$	$4q^{2(b-1)}$	$2^{12}q^{m+6(b-1)}p^n$
L1′	$-2q^{b-1}\psi(q^mp^n-1)$	$q^{m+2(b-1)}p^n$	$2^6q^{2m+6(b-1)}p^{2n}$
L2′	$4\cdot q^{b-1}\psi(q^mp^n-1)$	$4q^{2(b-1)}$	$2^{12}q^{m+6(b-1)}p^n$

13. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that q^m+p^n is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

    (a) *m is even or $q \equiv 1 \pmod 4$;*

	a_2	a_4	Δ
M1	$2q^{b-1}\psi(q^m+p^n)$	$q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
M2	$-4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$
M1′	$-2q^{b-1}\psi(q^m+p^n)$	$q^{m+2(b-1)}$	$2^6q^{2m+6(b-1)}p^n$
M2′	$4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{2(b-1)}p^n$	$2^{12}q^{m+6(b-1)}p^{2n}$

    (b) *m is odd and $q \equiv 3 \pmod 4$;*

	a_2	a_4	Δ
N1	$2q^{b-1}\psi(q^m+p^n)$	$q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
N2	$-4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{m+2(b-1)}$	$2^{12}q^{2m+6(b-1)}p^n$
N1′	$-2q^{b-1}\psi(q^m+p^n)$	$q^{2(b-1)}p^n$	$2^6q^{m+6(b-1)}p^{2n}$
N2′	$4\cdot q^{b-1}\psi(q^m+p^n)$	$4q^{m+2(b-1)}$	$2^{12}q^{2m+6(b-1)}p^n$

14. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that q^m-p^n is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

    (a) *m is even or $q \equiv 1 \pmod 4$;*

	a_2	a_4	Δ
O1	$2q^{b-1}\psi(q^m - p^n)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)} p^n$
O2	$-4 \cdot q^{b-1}\psi(q^m - p^n)$	$-4q^{2(b-1)}p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$
O1′	$-2q^{b-1}\psi(q^m - p^n)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)} p^n$
O2′	$4 \cdot q^{b-1}\psi(q^m - p^n)$	$-4q^{2(b-1)}p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
P1	$2q^{b-1}\psi(q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)} p^{2n}$
P2	$-4 \cdot q^{b-1}\psi(q^m - p^n)$	$4q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$
P1′	$-2q^{b-1}\psi(q^m - p^n)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)} p^{2n}$
P2′	$4 \cdot q^{b-1}\psi(q^m - p^n)$	$4q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$

15. *There exist integers $m \geq 2 - b$ and $n \geq 1$ such that $p^n - q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
Q1	$2q^{b-1}\psi(p^n - q^m)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)} p^n$
Q2	$-4 \cdot q^{b-1}\psi(p^n - q^m)$	$-4q^{2(b-1)}p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$
Q1′	$-2q^{b-1}\psi(p^n - q^m)$	$q^{m+2(b-1)}$	$-2^6 q^{2m+6(b-1)} p^n$
Q2′	$4 \cdot q^{b-1}\psi(p^n - q^m)$	$-4q^{2(b-1)}p^n$	$2^{12} q^{m+6(b-1)} p^{2n}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
R1	$2q^{b-1}\psi(p^n - q^m)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)} p^{2n}$
R2	$-4 \cdot q^{b-1}\psi(p^n - q^m)$	$4q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$
R1′	$-2q^{b-1}\psi(p^n - q^m)$	$-q^{2(b-1)}p^n$	$2^6 q^{m+6(b-1)} p^{2n}$
R2′	$4 \cdot q^{b-1}\psi(p^n - q^m)$	$4q^{m+2(b-1)}$	$-2^{12} q^{2m+6(b-1)} p^n$

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

16. *there exist integers $\ell \geq 2$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^l p^n + 1}{q}$ is a square, $q \equiv 1 \pmod 4$ when $l = 2$ or $q \equiv 1 \pmod 8$ when $l \geq 3$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
S1	$2q^{s+1}\psi(\frac{2^l p^n+1}{q})$	$2^l q^{2s+1} p^n$	$2^{2l+6} q^{6s+3} p^{2n}$
S2	$-4 \cdot q^{s+1}\psi(\frac{2^l p^n+1}{q})$	$4q^{2s+1}$	$2^{l+12} q^{6s+3} p^n$
S1′	$-2q^{s+1}\psi(\frac{2^l p^n+1}{q})$	$2^l q^{2s+1} p^n$	$2^{2l+6} q^{6s+3} p^{2n}$
S2′	$4 \cdot q^{s+1}\psi(\frac{2^l p^n+1}{q})$	$4q^{2s+1}$	$2^{l+12} q^{6s+3} p^n$

17. *there exist integers* $\ell \geq 2$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l p^n-1}{q}$ *is a square,* $q \equiv 3 \pmod 4$ *when* $l = 2$ *or* $q \equiv 7 \pmod 8$ *when* $l \geq 3$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
T1	$2q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$2^l q^{2s+1} p^n$	$-2^{2l+6} q^{6s+3} p^{2n}$
T2	$-4 \cdot q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$-4q^{2s+1}$	$2^{l+12} q^{6s+3} p^n$
T1′	$-2q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$2^l q^{2s+1} p^n$	$-2^{2l+6} q^{6s+3} p^{2n}$
T2′	$4 \cdot q^{s+1}\psi(\frac{2^l p^n-1}{q})$	$-4q^{2s+1}$	$2^{l+12} q^{6s+3} p^n$

18. *there exist integers* $\ell \geq 2$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
U1	$2q^{s+1}\psi(\frac{2^l+p^n}{q})$	$2^l q^{2s+1}$	$2^{2l+6} q^{6s+3} p^n$
U2	$-4 \cdot q^{s+1}\psi(\frac{2^l+p^n}{q})$	$4q^{2s+1} p^n$	$2^{l+12} q^{6s+3} p^{2n}$
U1′	$-2q^{s+1}\psi(\frac{2^l+p^n}{q})$	$2^l q^{2s+1}$	$2^{2l+6} q^{6s+3} p^n$
U2′	$4 \cdot q^{s+1}\psi(\frac{2^l+p^n}{q})$	$4q^{2s+1} p^n$	$2^{l+12} q^{6s+3} p^{2n}$

19. *there exist integers* $\ell \geq 2$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{2^l-p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
V1	$2q^{s+1}\psi(\frac{2^l-p^n}{q})$	$2^l q^{2s+1}$	$-2^{2l+6} q^{6s+3} p^n$
V2	$-4 \cdot q^{s+1}\psi(\frac{2^l-p^n}{q})$	$-4q^{2s+1} p^n$	$2^{l+12} q^{6s+3} p^{2n}$
V1′	$-2q^{s+1}\psi(\frac{2^l-p^n}{q})$	$2^l q^{2s+1}$	$-2^{2l+6} q^{6s+3} p^n$
V2′	$4 \cdot q^{s+1}\psi(\frac{2^l-p^n}{q})$	$-4q^{2s+1} p^n$	$2^{l+12} q^{6s+3} p^{2n}$

20. *there exist integers* $\ell \geq 2$, $n \geq 1$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-2^l}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following curves:*

	a_2	a_4	Δ
W1	$2q^{s+1}\psi(\frac{p^n-2^l}{q})$	$-2^l q^{2s+1}$	$2^{2l+6}q^{6s+3}p^n$
W2	$-4\cdot q^{s+1}\psi(\frac{p^n-2^l}{q})$	$4q^{2s+1}p^n$	$-2^{l+12}q^{6s+3}p^{2n}$
W1′	$-2q^{s+1}\psi(\frac{p^n-2^l}{q})$	$-2^l q^{2s+1}$	$2^{2l+6}q^{6s+3}p^n$
W2′	$4\cdot q^{s+1}\psi(\frac{p^n-2^l}{q})$	$4q^{2s+1}p^n$	$-2^{l+12}q^{6s+3}p^{2n}$

21. there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{q}$ is a square, $q \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:

	a_2	a_4	Δ
X1	$q^{s+1}\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^n$	$2^6 q^{6s+3}p^{2n}$
X2	$-2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}$	$2^{12}q^{6s+3}p^n$
X1′	$-q^{s+1}\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^n$	$2^6 q^{6s+3}p^{2n}$
X2′	$2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}$	$2^{12}q^{6s+3}p^n$

22. there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{q}$ is a square, $q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:

	a_2	a_4	Δ
Y1	$q^{s+1}\psi(\frac{p^n+1}{q})$	q^{2s+1}	$2^6 q^{6s+3}p^n$
Y2	$-2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^n$	$2^{12}q^{6s+3}p^{2n}$
Y1′	$-q^{s+1}\psi(\frac{p^n+1}{q})$	q^{2s+1}	$2^6 q^{6s+3}p^n$
Y2′	$2\cdot q^{s+1}\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^n$	$2^{12}q^{6s+3}p^{2n}$

23. there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{q}$ is a square, $q \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:

	a_2	a_4	Δ
Z1	$q^{s+1}\psi(\frac{p^n-1}{q})$	$-q^{2s+1}$	$2^6 q^{6s+3}p^n$
Z2	$-2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^n$	$-2^{12}q^{6s+3}p^{2n}$
Z1′	$-q^{s+1}\psi(\frac{p^n-1}{q})$	$-q^{2s+1}$	$2^6 q^{6s+3}p^n$
Z2′	$2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^n$	$-2^{12}q^{6s+3}p^{2n}$

24. there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{q}$ is a square, $q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:

	a_2	a_4	Δ
AA1	$q^{s+1}\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^n$	$-2^6 q^{6s+3}p^{2n}$
AA2	$-2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}$	$2^{12}q^{6s+3}p^n$
AA1′	$-q^{s+1}\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^n$	$-2^6 q^{6s+3}p^{2n}$
AA2′	$2\cdot q^{s+1}\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}$	$2^{12}q^{6s+3}p^n$

Theorem 2.2.8. *The elliptic curves E defined over $\mathbb{Q}$ of conductor 2^7q^bp and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2q^mp^n - 1$ is a square, $p, q \equiv 1 \pmod 4$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
A1	$2^{t+1}q^{b-1}\psi(2q^mp^n-1)$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{8+6t}q^{2m+6(b-1)}p^{2n}$
A2	$-2^{2-t}\cdot q^{b-1}\psi(2q^mp^n-1)$	$-2^{2-2t}q^{2(b-1)}$	$2^{13-6t}q^{m+6(b-1)}p^n$
A1′	$-2^{t+1}q^{b-1}\psi(2q^mp^n-1)$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{8+6t}q^{2m+6(b-1)}p^{2n}$
A2′	$2^{2-t}\cdot q^{b-1}\psi(2q^mp^n-1)$	$-2^{2-2t}q^{2(b-1)}$	$2^{13-6t}q^{m+6(b-1)}p^n$

2. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2q^m+p^n$ is a square, $p \equiv 3 \pmod 4$, n odd, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
B1	$2^{t+1}q^{b-1}\psi(2q^m+p^n)$	$2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{2m+6(b-1)}p^n$
B2	$-2^{2-t}\cdot q^{b-1}\psi(2q^m+p^n)$	$2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{m+6(b-1)}p^{2n}$
B1′	$-2^{t+1}q^{b-1}\psi(2q^m+p^n)$	$2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{2m+6(b-1)}p^n$
B2′	$2^{2-t}\cdot q^{b-1}\psi(2q^m+p^n)$	$2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{m+6(b-1)}p^{2n}$

3. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2q^m-p^n$ is a square, n is even or $p \equiv 1 \pmod 4$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
C1	$2^{t+1}q^{b-1}\psi(2q^m-p^n)$	$2^{1+2t}q^{m+2(b-1)}$	$-2^{8+6t}q^{2m+6(b-1)}p^n$
C2	$-2^{2-t}\cdot q^{b-1}\psi(2q^m-p^n)$	$-2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{m+6(b-1)}p^{2n}$
C1′	$-2^{t+1}q^{b-1}\psi(2q^m-p^n)$	$2^{1+2t}q^{m+2(b-1)}$	$-2^{8+6t}q^{2m+6(b-1)}p^n$
C2′	$2^{2-t}\cdot q^{b-1}\psi(2q^m-p^n)$	$-2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{m+6(b-1)}p^{2n}$

4. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that p^n-2q^m is a square, $p \equiv 3 \pmod 4$, n odd, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
D1	$2^{t+1}q^{b-1}\psi(p^n-2q^m)$	$-2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{2m+6(b-1)}p^n$
D2	$-2^{2-t}\cdot q^{b-1}\psi(p^n-2q^m)$	$2^{2-2t}q^{2(b-1)}p^n$	$-2^{13-6t}q^{m+6(b-1)}p^{2n}$
D1′	$-2^{t+1}q^{b-1}\psi(p^n-2q^m)$	$-2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{2m+6(b-1)}p^n$
D2′	$2^{2-t}\cdot q^{b-1}\psi(p^n-2q^m)$	$2^{2-2t}q^{2(b-1)}p^n$	$-2^{13-6t}q^{m+6(b-1)}p^{2n}$

5. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2p^n + q^m$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
E1	$2^{t+1}q^{b-1}\psi(2p^n+q^m)$	$2^{1+2t}q^{2(b-1)}p^n$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
E2	$-2^{2-t}\cdot q^{b-1}\psi(2p^n+q^m)$	$2^{2-2t}q^{m+2(b-1)}$	$2^{13-6t}q^{2m+6(b-1)}p^n$
E1′	$-2^{t+1}q^{b-1}\psi(2p^n+q^m)$	$2^{1+2t}q^{2(b-1)}p^n$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
E2′	$2^{2-t}\cdot q^{b-1}\psi(2p^n+q^m)$	$2^{2-2t}q^{m+2(b-1)}$	$2^{13-6t}q^{2m+6(b-1)}p^n$

6. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2p^n - q^m$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
F1	$2^{t+1}q^{b-1}\psi(2p^n-q^m)$	$2^{1+2t}q^{2(b-1)}p^n$	$-2^{8+6t}q^{m+6(b-1)}p^{2n}$
F2	$-2^{2-t}\cdot q^{b-1}\psi(2p^n-q^m)$	$-2^{2-2t}q^{m+2(b-1)}$	$2^{13-6t}q^{2m+6(b-1)}p^n$
F1′	$-2^{t+1}q^{b-1}\psi(2p^n-q^m)$	$2^{1+2t}q^{2(b-1)}p^n$	$-2^{8+6t}q^{m+6(b-1)}p^{2n}$
F2′	$2^{2-t}\cdot q^{b-1}\psi(2p^n-q^m)$	$-2^{2-2t}q^{m+2(b-1)}$	$2^{13-6t}q^{2m+6(b-1)}p^n$

7. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^m - 2p^n$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
G1	$2^{t+1}q^{b-1}\psi(q^m-2p^n)$	$-2^{1+2t}q^{2(b-1)}p^n$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
G2	$-2^{2-t}\cdot q^{b-1}\psi(q^m-2p^n)$	$2^{2-2t}q^{m+2(b-1)}$	$-2^{13-6t}q^{2m+6(b-1)}p^n$
G1′	$-2^{t+1}q^{b-1}\psi(q^m-2p^n)$	$-2^{1+2t}q^{2(b-1)}p^n$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
G2′	$2^{2-t}\cdot q^{b-1}\psi(q^m-2p^n)$	$2^{2-2t}q^{m+2(b-1)}$	$-2^{13-6t}q^{2m+6(b-1)}p^n$

8. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $2+q^mp^n$ is a square, $p \equiv 1$ or $7 \pmod 8$, $q \equiv 1$ or $7 \pmod 8$ if $m > 0$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
H1	$2^{t+1}q^{b-1}\psi(2+q^mp^n)$	$2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
H2	$-2^{2-t}\cdot q^{b-1}\psi(2+q^mp^n)$	$2^{2-2t}q^{m+2(b-1)}p^n$	$2^{13-6t}q^{2m+6(b-1)}p^n$
H1′	$-2^{t+1}q^{b-1}\psi(2+q^mp^n)$	$2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
H2′	$2^{2-t}\cdot q^{b-1}\psi(2+q^mp^n)$	$2^{2-2t}q^{m+2(b-1)}p^n$	$2^{13-6t}q^{2m+6(b-1)}p^n$

9. *There exist integers $m \geq 2-b$ and $n \geq 1$ such that $q^mp^n - 2$ is a square, $p \equiv 1$ or $3 \pmod 8$, $q \equiv 1$ or $3 \pmod 8$ if $m > 0$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves:*

	a_2	a_4	Δ
I1	$2^{t+1}q^{b-1}\psi(q^mp^n-2)$	$-2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
I2	$-2^{2-t}\cdot q^{b-1}\psi(q^mp^n-2)$	$2^{2-2t}q^{m+2(b-1)}p^n$	$-2^{13-6t}q^{2m+6(b-1)}p^n$
I1′	$-2^{t+1}q^{b-1}\psi(q^mp^n-2)$	$-2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{m+6(b-1)}p^{2n}$
I2′	$2^{2-t}\cdot q^{b-1}\psi(q^mp^n-2)$	$2^{2-2t}q^{m+2(b-1)}p^n$	$-2^{13-6t}q^{2m+6(b-1)}p^n$

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

10. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{2p^n+1}{q}$ is a square, $q \equiv 3 \pmod 4$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
J1	$2^{t+1}q^{s+1}\psi(\frac{2p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$2^{8+6t}q^{6s+3}p^{2n}$
J2	$-2^{2-t}\cdot q^{s+1}\psi(\frac{2p^n+1}{q})$	$2^{2-2t}q^{2s+1}$	$2^{13-6t}q^{6s+3}p^n$
J1′	$-2^{t+1}q^{s+1}\psi(\frac{2p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$2^{8+6t}q^{6s+3}p^{2n}$
J2′	$2^{2-t}\cdot q^{s+1}\psi(\frac{2p^n+1}{q})$	$2^{2-2t}q^{2s+1}$	$2^{13-6t}q^{6s+3}p^n$

11. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{2p^n-1}{q}$ is a square, $q \equiv 1 \pmod 4$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
K1	$2^{t+1}q^{s+1}\psi(\frac{2p^n-1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$-2^{8+6t}q^{6s+3}p^{2n}$
K2	$-2^{2-t}\cdot q^{s+1}\psi(\frac{2p^n-1}{q})$	$-2^{2-2t}q^{2s+1}$	$2^{13-6t}q^{6s+3}p^n$
K1′	$-2^{t+1}q^{s+1}\psi(\frac{2p^n-1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$-2^{8+6t}q^{6s+3}p^{2n}$
K2′	$2^{2-t}\cdot q^{s+1}\psi(\frac{2p^n-1}{q})$	$-2^{2-2t}q^{2s+1}$	$2^{13-6t}q^{6s+3}p^n$

12. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{2+p^n}{q}$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
L1	$2^{t+1}q^{b-1}\psi(\frac{2+p^n}{q})$	$2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{6s+3}p^n$
L2	$-2^{2-t}\cdot q^{b-1}\psi(\frac{2+p^n}{q})$	$2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{6s+3}p^{2n}$
L1′	$-2^{t+1}q^{b-1}\psi(\frac{2+p^n}{q})$	$2^{1+2t}q^{2(b-1)}$	$2^{8+6t}q^{6s+3}p^n$
L2′	$2^{2-t}\cdot q^{b-1}\psi(\frac{2+p^n}{q})$	$2^{2-2t}q^{2(b-1)}p^n$	$2^{13-6t}q^{6s+3}p^{2n}$

13. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-2}{q}$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following curves:*

	a_2	a_4	Δ
$M1$	$2^{t+1}q^{b-1}\psi(\frac{p^n-2}{q})$	$-2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{6s+3}p^n$
$M2$	$-2^{2-t}\cdot q^{b-1}\psi(\frac{p^n-2}{q})$	$2^{2-2t}q^{2(b-1)}p^n$	$-2^{13-6t}q^{6s+3}p^{2n}$
$M1'$	$-2^{t+1}q^{b-1}\psi(\frac{p^n-2}{q})$	$-2^{1+2t}q^{m+2(b-1)}$	$2^{8+6t}q^{6s+3}p^n$
$M2'$	$2^{2-t}\cdot q^{b-1}\psi(\frac{p^n-2}{q})$	$2^{2-2t}q^{2(b-1)}p^n$	$-2^{13-6t}q^{6s+3}p^{2n}$

Theorem 2.2.9. *The elliptic curves E defined over $\mathbb{Q}$ of conductor 2^8q^bp and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^mp^n+1}{2}$ is a square, $p, q \equiv 1, 7 \pmod 8$, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$A1$	$2^{t+2}q^{b-1}\psi(\frac{q^mp^n+1}{2})$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{9+6t}q^{2m+6(b-1)}p^{2n}$
$A2$	$-2^{3-t}q^{b-1}\psi(\frac{q^mp^n+1}{2})$	$-2^{3-2t}q^{2(b-1)}$	$2^{15-6t}q^{m+6(b-1)}p^n$
$A1'$	$-2^{t+2}q^{b-1}\psi(\frac{q^mp^n+1}{2})$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{9+6t}q^{2m+6(b-1)}p^{2n}$
$A2'$	$2^{3-t}q^{b-1}\psi(\frac{q^mp^n+1}{2})$	$-2^{3-2t}q^{2(b-1)}$	$2^{15-6t}q^{m+6(b-1)}p^n$

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^mp^n-1}{2}$ is a square, $p, q \equiv 1, 3 \pmod 8$, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$B1$	$2^{t+2}q^{b-1}\psi(\frac{q^mp^n-1}{2})$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{9+6t}q^{2m+6(b-1)}p^{2n}$
$B2$	$-2^{3-t}q^{b-1}\psi(\frac{q^mp^n-1}{2})$	$-2^{3-2t}q^{2(b-1)}$	$2^{15-6t}q^{m+6(b-1)}p^n$
$B1'$	$-2^{t+2}q^{b-1}\psi(\frac{q^mp^n-1}{2})$	$2^{1+2t}q^{m+2(b-1)}p^n$	$-2^{9+6t}q^{2m+6(b-1)}p^{2n}$
$B2'$	$2^{3-t}q^{b-1}\psi(\frac{q^mp^n-1}{2})$	$-2^{3-2t}q^{2(b-1)}$	$2^{15-6t}q^{m+6(b-1)}p^n$

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m+p^n}{2}$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$C1$	$2^{t+2}q^{b-1}\psi(\frac{q^m+p^n}{2})$	$2^{1+2t}q^{m+2(b-1)}$	$2^{9+6t}q^{2m+6(b-1)}p^n$
$C2$	$-2^{3-t}q^{b-1}\psi(\frac{q^m+p^n}{2})$	$2^{3-2t}q^{2(b-1)}p^n$	$2^{15-6t}q^{m+6(b-1)}p^{2n}$
$C1'$	$-2^{t+2}q^{b-1}\psi(\frac{q^m+p^n}{2})$	$2^{1+2t}q^{m+2(b-1)}$	$2^{9+6t}q^{2m+6(b-1)}p^n$
$C2'$	$2^{3-t}q^{b-1}\psi(\frac{q^m+p^n}{2})$	$2^{3-2t}q^{2(b-1)}p^n$	$2^{15-6t}q^{m+6(b-1)}p^{2n}$

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m-p^n}{2}$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$2^{t+2}q^{b-1}\psi(\frac{q^m-p^n}{2})$	$2^{1+2t}q^{m+2(b-1)}$	$-2^{9+6t}q^{2m+6(b-1)}p^n$
D2	$-2^{3-t}q^{b-1}\psi(\frac{q^m-p^n}{2})$	$-2^{3-2t}q^{2(b-1)}p^n$	$2^{15-6t}q^{m+6(b-1)}p^{2n}$
D1′	$-2^{t+2}q^{b-1}\psi(\frac{q^m-p^n}{2})$	$2^{1+2t}q^{m+2(b-1)}$	$-2^{9+6t}q^{2m+6(b-1)}p^n$
D2′	$2^{3-t}q^{b-1}\psi(\frac{q^m-p^n}{2})$	$-2^{3-2t}q^{2(b-1)}p^n$	$2^{15-6t}q^{m+6(b-1)}p^{2n}$

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n-q^m}{2}$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$2^{t+2}q^{b-1}\psi(\frac{p^n-q^m}{2})$	$2^{1+2t}q^{2(b-1)}p^n$	$-2^{9+6t}q^{m+6(b-1)}p^{2n}$
E2	$-2^{3-t}q^{b-1}\psi(\frac{p^n-q^m}{2})$	$-2^{3-2t}q^{m+2(b-1)}$	$2^{15-6t}q^{2m+6(b-1)}p^n$
E1′	$-2^{t+2}q^{b-1}\psi(\frac{p^n-q^m}{2})$	$2^{1+2t}q^{2(b-1)}p^n$	$-2^{9+6t}q^{m+6(b-1)}p^{2n}$
E2′	$2^{3-t}q^{b-1}\psi(\frac{p^n-q^m}{2})$	$-2^{3-2t}q^{m+2(b-1)}$	$2^{15-6t}q^{2m+6(b-1)}p^n$

In the case that $b = 2$, we furthermore could have one of the following conditions satisfied:

6. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n+1}{2q}$ is a square, $p^n \equiv 1 \pmod 4$, $s,t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$2^{9+6t}q^{6s+3}p^{2n}$
F2	$-2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{3-2t}q^{2s+1}$	$2^{15-6t}q^{6s+3}p^n$
F1′	$-2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$2^{9+6t}q^{6s+3}p^{2n}$
F2′	$2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{3-2t}q^{2s+1}$	$2^{15-6t}q^{6s+3}p^n$

7. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n-1}{2q}$ is a square, $p^n \equiv 3 \pmod 4$, $s,t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$-2^{9+6t}q^{6s+3}p^{2n}$
G2	$-2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$-2^{3-2t}q^{2s+1}$	$2^{15-6t}q^{6s+3}p^n$
G1′	$-2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^n$	$-2^{9+6t}q^{6s+3}p^{2n}$
G2′	$2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$-2^{3-2t}q^{2s+1}$	$2^{15-6t}q^{6s+3}p^n$

Theorem 2.2.10. *The elliptic curves E defined over $\mathbb{Q}$ of conductor q^2p^2 and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^6 q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$\epsilon \cdot qp\psi(2^6 q^m p^n + 1)$	$2^4 q^{m+2} p^{n+2}$	$2^{12} q^{2m+6} p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 q^m p^n + 1)$	$q^2 p^2$	$2^{12} q^{m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^6 q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$\epsilon \cdot qp\psi(2^6 q^m + p^n)$	$2^4 q^{m+2} p^2$	$2^{12} q^{2m+6} p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 q^m + p^n)$	$q^2 p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^6 q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$\epsilon \cdot qp\psi(2^\ell q^m - p^n)$	$2^4 q^{m+2} p^2$	$-2^{12} q^{2m+6} p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 q^m - p^n)$	$-q^2 p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - 2^6 q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$\epsilon \cdot qp\psi(p^n - 2^6 q^m)$	$-2^4 q^{m+2} p^2$	$2^{12} q^{2m+6} p^{n+6}$
D2	$-\epsilon \cdot 2 \cdot qp\psi(p^n - 2^6 q^m)$	$q^2 p^{n+2}$	$-2^{12} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^6 p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$\epsilon \cdot qp\psi(2^6 p^n + q^m)$	$2^4 q^2 p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$
E2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 p^n + q^m)$	$q^{m+2} p^2$	$2^{12} q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

6. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $2^6 p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$*,* m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$\epsilon \cdot qp\psi(2^6 p^n - q^m)$	$2^4 q^2 p^{n+2}$	$-2^{12} q^{m+6} p^{2n+6}$
F2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 p^n - q^m)$	$-q^{m+2} p^2$	$2^{12} q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

7. *There exist integers* $\ell \geq 7$*,* $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 2^6 p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$\epsilon \cdot qp\psi(q^m - 2^6 p^n)$	$-2^4 q^2 p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$
G2	$-\epsilon \cdot 2 \cdot qp\psi(q^m - 2^6 p^n)$	$q^{m+2} p^2$	$-2^{12} q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

8. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $2^6 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$\epsilon \cdot qp\psi(2^6 + q^m p^n)$	$2^4 q^2 p^2$	$2^{12} q^{m+6} p^{n+6}$
H2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 + q^m p^n)$	$q^{m+2} p^{n+2}$	$2^{12} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

9. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $2^6 - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$\epsilon \cdot qp\psi(2^6 - q^m p^n)$	$2^4 q^2 p^2$	$-2^{12} q^{m+6} p^{n+6}$
I2	$-\epsilon \cdot 2 \cdot qp\psi(2^6 - q^m p^n)$	$-q^{m+2} p^{n+2}$	$2^{12} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

10. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 2^6$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$\epsilon \cdot qp\psi(q^m p^n - 2^6)$	$-2^4 q^2 p^2$	$2^{12} q^{m+6} p^{n+6}$
J2	$-\epsilon \cdot 2 \cdot qp\psi(q^m p^n - 2^6)$	$q^{m+2} p^{n+2}$	$-2^{12} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

11. *There exist integers* $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{2^6 q^m + 1}{p}$ *is a square,* $p \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^6 q^m + 1}{p})$	$2^4 q^{m+2} p^{2r+1}$	$2^{12} q^{2m+6} p^{6r+3}$
K2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^6 q^m + 1}{p})$	$q^2 p^{2r+1}$	$2^{12} q^{m+6} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

12. *There exist integers* $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{2^6 q^m - 1}{p}$ *is a square,* $p \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^6 q^m - 1}{p})$	$2^4 q^{m+2} p^{2r+1}$	$-2^{12} q^{2m+6} p^{6r+3}$
L2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^6 q^m - 1}{p})$	$-q^2 p^{2r+1}$	$2^{12} q^{m+6} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

13. *There exist integers* $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{2^6 + q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^6 + q^m}{p})$	$2^4 q^2 p^{2r+1}$	$2^{12} q^{m+6} p^{6r+3}$
M2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^6 + q^m}{p})$	$q^{m+2} p^{2r+1}$	$2^{12} q^{2m+6} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

14. *There exist integers* $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{2^6 - q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^6 - q^m}{p})$	$2^4 q^2 p^{2r+1}$	$-2^{12} q^{m+6} p^{6r+3}$
N2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^6 - q^m}{p})$	$-q^{m+2} p^{2r+1}$	$2^{12} q^{2m+6} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

15. *There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-2^6}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
O1	$\epsilon \cdot qp^{r+1}\psi(\frac{q^m-2^6}{p})$	$-2^4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$
O2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-2^6}{p})$	$q^{m+2}p^{2r+1}$	$-2^{12}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp^{r+1} modulo 4.

16. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^6p^n+1}{q}$ is a square, $q \equiv 1 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
P1	$\epsilon \cdot q^{s+1}p\psi(\frac{2^6p^n+1}{q})$	$2^4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$
P2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^6p^n+1}{q})$	$q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

17. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^6p^n-1}{q}$ is a square, $q \equiv 7 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Q1	$\epsilon \cdot q^{s+1}p\psi(\frac{2^6p^n-1}{q})$	$2^4q^{2s+1}p^{n+2}$	$-2^{12}q^{6s+3}p^{2n+6}$
Q2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^6p^n-1}{q})$	$-q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $q^{s+1}p$ modulo 4.

18. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^6+p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
R1	$\epsilon \cdot q^{s+1}p\psi(\frac{2^6+p^n}{q})$	$2^4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
R2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^6+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $q^{s+1}p$ modulo 4.

19. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^6-p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
S1	$\epsilon \cdot q^{s+1}p\psi(\frac{2^6-p^n}{q})$	$2^4q^{2s+1}p^2$	$-2^{12}q^{6s+3}p^{n+6}$
S2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^6-p^n}{q})$	$-q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

20. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-2^6}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
T1	$\epsilon \cdot q^{s+1}p\psi(\frac{p^n-2^6}{q})$	$-2^4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
T2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{p^n-2^6}{q})$	$q^{2s+1}p^{n+2}$	$-2^{12}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

21. *There exist integers* $r, s \in \{0,1\}$ *such that* $\frac{2^6+1}{qp}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
U1	$\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^6+1}{qp})$	$2^4q^{2s+1}p^{2r+1}$	$2^{12}q^{6s+3}p^{6r+3}$
U2	$-\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^6+1}{qp})$	$q^{2s+1}p^{2r+1}$	$2^{12}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

22. *There exist integers* $r, s \in \{0,1\}$ *such that* $\frac{2^6-1}{qp}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
V1	$\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^6-1}{qp})$	$2^4q^{2s+1}p^{2r+1}$	$-2^{12}q^{6s+3}p^{6r+3}$
V2	$-\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^6-1}{qp})$	$-q^{2s+1}p^{2r+1}$	$2^{12}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

Theorem 2.2.11. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2q^2p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$\epsilon \cdot qp\psi(2^\ell q^m p^n + 1)$	$2^{\ell-2}q^{m+2}p^{n+2}$	$2^{2\ell}q^{2m+6}p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m p^n + 1)$	q^2p^2	$2^{\ell+6}q^{m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

2. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$\epsilon \cdot qp\psi(2^\ell q^m + p^n)$	$2^{\ell-2}q^{m+2}p^2$	$2^{2\ell}q^{2m+6}p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m + p^n)$	q^2p^{n+2}	$2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

3. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$\epsilon \cdot qp\psi(2^\ell q^m - p^n)$	$2^{\ell-2}q^{m+2}p^2$	$-2^{2\ell}q^{2m+6}p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m - p^n)$	$-q^2p^{n+2}$	$2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

4. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $p^n - 2^\ell q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$\epsilon \cdot qp\psi(p^n - 2^\ell q^m)$	$-2^{\ell-2}q^{m+2}p^2$	$2^{2\ell}q^{2m+6}p^{n+6}$
D2	$-\epsilon \cdot 2 \cdot qp\psi(p^n - 2^\ell q^m)$	q^2p^{n+2}	$-2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

5. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $2^\ell p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$\epsilon \cdot qp\psi(2^\ell p^n + q^m)$	$2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
E2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n + q^m)$	$q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

6. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $2^\ell p^n - q^m$ is a square, $q \equiv 7 \pmod 8$, m odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$\epsilon \cdot qp\psi(2^\ell p^n - q^m)$	$2^{\ell-2}q^2p^{n+2}$	$-2^{2\ell}q^{m+6}p^{2n+6}$
F2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n - q^m)$	$-q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

7. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 2^\ell p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$\epsilon \cdot qp\psi(q^m - 2^\ell p^n)$	$-2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
G2	$-\epsilon \cdot 2 \cdot qp\psi(q^m - 2^\ell p^n)$	$q^{m+2}p^2$	$-2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

8. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$\epsilon \cdot qp\psi(2^\ell + q^m p^n)$	$2^{\ell-2}q^2p^2$	$2^{2\ell}q^{m+6}p^{n+6}$
H2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell + q^m p^n)$	$q^{m+2}p^{n+2}$	$2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

9. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$\epsilon \cdot qp\psi(2^\ell - q^m p^n)$	$2^{\ell-2}q^2p^2$	$-2^{2\ell}q^{m+6}p^{n+6}$
I2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell - q^m p^n)$	$-q^{m+2}p^{n+2}$	$2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

10. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$\epsilon \cdot qp\psi(q^m p^n - 2^\ell)$	$-2^{\ell-2}q^2p^2$	$2^{2\ell}q^{m+6}p^{n+6}$
J2	$-\epsilon \cdot 2 \cdot qp\psi(q^m p^n - 2^\ell)$	$q^{m+2}p^{n+2}$	$-2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

11. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{2^\ell q^m + 1}{p}$ *is a square,* $p \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$2^{2\ell}q^{2m+6}p^{6r+3}$
K2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	q^2p^{2r+1}	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

12. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell q^m-1}{p}$ *is a square,* $p \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$-2^{2\ell}q^{2m+6}p^{6r+3}$
L2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$-q^2p^{2r+1}$	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

13. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell+q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
M2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

14. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell-q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$-2^{2\ell}q^{m+6}p^{6r+3}$
N2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$-q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

15. *There exist integers* $\ell \geq 7$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{q^m-2^\ell}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
O1	$\epsilon \cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$-2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
O2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$q^{m+2}p^{2r+1}$	$-2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

16. *There exist integers* $\ell \geq 7$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n+1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
P1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell p^n+1}{q})$	$2^{\ell-2} q^{2s+1} p^{n+2}$	$2^{2\ell} q^{6s+3} p^{2n+6}$
P2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell p^n+1}{q})$	$q^{2s+1} p^2$	$2^{\ell+6} q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

17. *There exist integers* $\ell \geq 7$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n-1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Q1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell p^n-1}{q})$	$2^{\ell-2} q^{2s+1} p^{n+2}$	$-2^{2\ell} q^{6s+3} p^{2n+6}$
Q2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell p^n-1}{q})$	$-q^{2s+1} p^2$	$2^{\ell+6} q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

18. *There exist integers* $\ell \geq 7$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell + p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
R1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell + p^n}{q})$	$2^{\ell-2} q^{2s+1} p^2$	$2^{2\ell} q^{6s+3} p^{n+6}$
R2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell + p^n}{q})$	$q^{2s+1} p^{n+2}$	$2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

19. *There exist integers* $\ell \geq 7$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
S1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell - p^n}{q})$	$2^{\ell-2} q^{2s+1} p^2$	$-2^{2\ell} q^{6s+3} p^{n+6}$
S2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell - p^n}{q})$	$-q^{2s+1} p^{n+2}$	$2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

20. *There exist integers* $\ell \geq 7$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n - 2^\ell}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
T1	$\epsilon \cdot q^{s+1} p \psi(\frac{p^n - 2^\ell}{q})$	$-2^{\ell-2} q^{2s+1} p^2$	$2^{2\ell} q^{6s+3} p^{n+6}$
T2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{p^n - 2^\ell}{q})$	$q^{2s+1} p^{n+2}$	$-2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

21. *There exist integers* $\ell \geq 7$ *and* $r, s \in \{0, 1\}$ *such that* $\frac{2^\ell+1}{qp}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
U1	$\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$2^{\ell-2}q^{2s+1}p^{2r+1}$	$2^{2\ell}q^{6s+3}p^{6r+3}$
U2	$-\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$q^{2s+1}p^{2r+1}$	$2^{\ell+6}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

22. *There exist integers* $\ell \geq 7$ *and* $r, s \in \{0, 1\}$ *such that* $\frac{2^\ell-1}{qp}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
V1	$\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$2^{\ell-2}q^{2s+1}p^{2r+1}$	$-2^{2\ell}q^{6s+3}p^{6r+3}$
V2	$-\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$-q^{2s+1}p^{2r+1}$	$2^{\ell+6}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

Theorem 2.2.12. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2^2q^2p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4q^m + p^n$ *is a square,* $q^m \equiv -1 \pmod 4$*,* $p \equiv 5 \pmod 8$*,* n *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$\epsilon \cdot qp\psi(4q^m + p^n)$	$q^{m+2}p^2$	$2^4q^{2m+6}p^{n+6}$
A2	$-\epsilon \cdot 2 \cdot qp\psi(4q^m + p^n)$	q^2p^{n+2}	$2^8q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

2. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4q^m - p^n$ *is a square,* $q^m \equiv -1 \pmod 4$*,* $p \equiv 3 \pmod 8$*,* n *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$\epsilon \cdot qp\psi(4q^m - p^n)$	$q^{m+2}p^2$	$-2^4q^{2m+6}p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot qp\psi(4q^m - p^n)$	$-q^2p^{n+2}$	$2^8q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - 4q^m$ is a square, $q^m \equiv 1 \pmod 4$, $p \equiv 5 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$\epsilon \cdot qp\psi(p^n - 4q^m)$	$-q^{m+2}p^2$	$2^4 q^{2m+6} p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot qp\psi(p^n - 4q^m)$	$q^2 p^{n+2}$	$-2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4p^n + q^m$ is a square, $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$\epsilon \cdot qp\psi(4p^n + q^m)$	$q^2 p^{n+2}$	$2^4 q^{m+6} p^{2n+6}$
D2	$-\epsilon \cdot 2 \cdot qp\psi(4p^n + q^m)$	$q^{m+2}p^2$	$2^8 q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4p^n - q^m$ is a square, $q \equiv 3 \pmod 8$, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$\epsilon \cdot qp\psi(4p^n - q^m)$	$q^2 p^{n+2}$	$-2^4 q^{m+6} p^{2n+6}$
E2	$-\epsilon \cdot 2 \cdot qp\psi(4p^n - q^m)$	$-q^{m+2}p^2$	$2^8 q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

6. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - 4p^n$ is a square, $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$\epsilon \cdot qp\psi(q^m - 4p^n)$	$-q^2 p^{n+2}$	$2^4 q^{m+6} p^{2n+6}$
F2	$-\epsilon \cdot 2 \cdot qp\psi(q^m - 4p^n)$	$q^{m+2}p^2$	$-2^8 q^{2m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

7. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m p^n - 4$ is a square, $p, q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$qp\psi(q^m p^n - 4)$	$-q^2 p^2$	$2^4 q^{m+6} p^{n+6}$
G2	$-2 \cdot qp\psi(q^m p^n - 4)$	$q^{m+2} p^{n+2}$	$-2^8 q^{2m+6} p^{2n+6}$

8. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4q^m+1}{p}$ *is a square,* $p \equiv 5 \pmod 8$, $q^m \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$\epsilon \cdot qp^{r+1}\psi(\frac{4q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^4q^{2m+6}p^{6r+3}$
H2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4q^m+1}{p})$	q^2p^{2r+1}	$2^8q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

9. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4q^m-1}{p}$ *is a square,* $p \equiv 3 \pmod 8$, $q^m \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$\epsilon \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^4q^{2m+6}p^{6r+3}$
I2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$-q^2p^{2r+1}$	$2^8q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

10. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4+q^m}{p}$ *is a square,* $p \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$\epsilon \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	q^2p^{2r+1}	$2^4q^{m+6}p^{6r+3}$
J2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

11. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{q^m-4}{p}$ *is a square,* $p \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$\epsilon \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$-q^2p^{2r+1}$	$2^4q^{m+6}p^{6r+3}$
K2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$q^{m+2}p^{2r+1}$	$-2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

12. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4p^n+1}{q}$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$\epsilon \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^4q^{6s+3}p^{2n+6}$
L2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^2$	$2^8q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

13. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4p^n-1}{q}$ *is a square,* $q \equiv 3 \pmod 8$*,* $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$\epsilon \cdot q^{s+1}p\psi(\frac{4p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^4q^{6s+3}p^{2n+6}$
M2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4p^n-1}{q})$	$-q^{2s+1}p^2$	$2^8q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

14. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4+p^n}{q}$ *is a square,* $q \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$\epsilon \cdot q^{s+1}p\psi(\frac{4+p^n}{q})$	$q^{2s+1}p^2$	$2^4q^{6s+3}p^{n+6}$
N2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^8q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

15. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-4}{q}$ *is a square,* $q \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
O1	$\epsilon \cdot q^{s+1}p\psi(\frac{p^n-4}{q})$	$-q^{2s+1}p^2$	$2^4q^{6s+3}p^{n+6}$
O2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{p^n-4}{q})$	$q^{2s+1}p^{n+2}$	$-2^8q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

Theorem 2.2.13. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2^3q^2p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \in \{4,5\}$*,* $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$\epsilon \cdot qp\psi(2^\ell q^m p^n + 1)$	$2^{\ell-2}q^{m+2}p^{n+2}$	$2^{2\ell}q^{2m+6}p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m p^n + 1)$	q^2p^2	$2^{\ell+6}q^{m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4q^m + p^n$ is a square, $q^m \equiv 1 \pmod 4$, $p \equiv 5 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$-\epsilon \cdot qp\psi(4q^m + p^n)$	$q^{m+2}p^2$	$2^4 q^{2m+6} p^{n+6}$
B2	$\epsilon \cdot 2 \cdot qp\psi(4q^m + p^n)$	$q^2 p^{n+2}$	$2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4q^m - p^n$ is a square, $q^m \equiv 1 \pmod 4$, $p \equiv 3 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$-\epsilon \cdot qp\psi(4q^m - p^n)$	$q^{m+2}p^2$	$-2^4 q^{2m+6} p^{n+6}$
C2	$\epsilon \cdot 2 \cdot qp\psi(4q^m - p^n)$	$-q^2 p^{n+2}$	$2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - 4q^m$ is a square, $q^m \equiv -1 \pmod 4$, $p \equiv 5 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$-\epsilon \cdot qp\psi(p^n - 4q^m)$	$-q^{m+2}p^2$	$2^4 q^{2m+6} p^{n+6}$
D2	$\epsilon \cdot 2 \cdot qp\psi(p^n - 4q^m)$	$q^2 p^{n+2}$	$-2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

5. *There exist integers $\ell \in \{4, 5\}$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$\epsilon \cdot qp\psi(2^\ell q^m + p^n)$	$2^{\ell-2} q^{m+2} p^2$	$2^{2\ell} q^{2m+6} p^{n+6}$
E2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m + p^n)$	$q^2 p^{n+2}$	$2^{\ell+6} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

6. *There exist integers $\ell \in \{4, 5\}$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$\epsilon \cdot qp\psi(2^\ell q^m - p^n)$	$2^{\ell-2} q^{m+2} p^2$	$-2^{2\ell} q^{2m+6} p^{n+6}$
F2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m - p^n)$	$-q^2 p^{n+2}$	$2^{\ell+6} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

7. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $p^n - 2^\ell q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$\epsilon \cdot qp\psi(p^n - 2^\ell q^m)$	$-2^{\ell-2}q^{m+2}p^2$	$2^{2\ell}q^{2m+6}p^{n+6}$
G2	$-\epsilon \cdot 2 \cdot qp\psi(p^n - 2^\ell q^m)$	q^2p^{n+2}	$-2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4[1].

8. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4p^n + q^m$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$-\epsilon \cdot qp\psi(4p^n + q^m)$	q^2p^{n+2}	$2^4q^{m+6}p^{2n+6}$
H2	$\epsilon \cdot 2 \cdot qp\psi(4p^n + q^m)$	$q^{m+2}p^2$	$2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

9. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4p^n - q^m$ *is a square,* $q \equiv 3 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$-\epsilon \cdot qp\psi(4p^n - q^m)$	q^2p^{n+2}	$-2^4q^{m+6}p^{2n+6}$
I2	$\epsilon \cdot 2 \cdot qp\psi(4p^n - q^m)$	$-q^{m+2}p^2$	$2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

10. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 4p^n$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$-\epsilon \cdot qp\psi(q^m - 4p^n)$	$-q^2p^{n+2}$	$2^4q^{m+6}p^{2n+6}$
J2	$\epsilon \cdot 2 \cdot qp\psi(q^m - 4p^n)$	$q^{m+2}p^2$	$-2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

11. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell p^n + q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

[1] Note the typo in [Mul06, p.113]

	a_2	a_4	Δ
K1	$\epsilon \cdot qp\psi(2^\ell p^n + q^m)$	$2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
K2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n + q^m)$	$q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

12. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$, m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$\epsilon \cdot qp\psi(2^\ell p^n - q^m)$	$2^{\ell-2}q^2p^{n+2}$	$-2^{2\ell}q^{m+6}p^{2n+6}$
L2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n - q^m)$	$-q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

13. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 2^\ell p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$\epsilon \cdot qp\psi(q^m - 2^\ell p^n)$	$-2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
M2	$-\epsilon \cdot 2 \cdot qp\psi(q^m - 2^\ell p^n)$	$q^{m+2}p^2$	$-2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

14. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$-\epsilon \cdot qp\psi(4 + q^m p^n)$	q^2p^2	$2^4q^{m+6}p^{n+6}$
N2	$\epsilon \cdot 2 \cdot qp\psi(4 + q^m p^n)$	$q^{m+2}p^{n+2}$	$2^8q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

15. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
O1	$\epsilon \cdot qp\psi(2^\ell + q^m p^n)$	$2^{\ell-2}q^2p^2$	$2^{2\ell}q^{m+6}p^{n+6}$
O2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell + q^m p^n)$	$q^{m+2}p^{n+2}$	$2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

16. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
P1	$\epsilon \cdot qp\psi(2^\ell - q^m p^n)$	$2^{\ell-2}q^2p^2$	$-2^{2\ell}q^{m+6}p^{n+6}$
P2	$-\epsilon \cdot 2 \cdot qp\psi(2^\ell - q^m p^n)$	$-q^{m+2}p^{n+2}$	$2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

17. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Q1	$\epsilon \cdot qp\psi(q^m p^n - 2^\ell)$	$-2^{\ell-2}q^2p^2$	$2^{2\ell}q^{m+6}p^{n+6}$
Q2	$-\epsilon \cdot 2 \cdot qp\psi(q^m p^n - 2^\ell)$	$q^{m+2}p^{n+2}$	$-2^{\ell+6}q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

18. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4q^m+1}{p}$ *is a square,* $p \equiv 5 \pmod 8$, $q^m \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
R1	$-qp^{r+1}\psi(\frac{4q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^4q^{2m+6}p^{6r+3}$
R2	$2 \cdot qp^{r+1}\psi(\frac{4q^m+1}{p})$	q^2p^{2r+1}	$2^8q^{m+6}p^{6r+3}$

19. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4q^m-1}{p}$ *is a square,* $p \equiv 3 \pmod 8$, $q^m \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
S1	$-\epsilon \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^4q^{2m+6}p^{6r+3}$
S2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$-q^2p^{2r+1}$	$2^8q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

20. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell q^m+1}{p}$ *is a square,* $p \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
T1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$2^{2\ell}q^{2m+6}p^{6r+3}$
T2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	q^2p^{2r+1}	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

21. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell q^m - 1}{p}$ *is a square,* $p \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
U1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$-2^{2\ell}q^{2m+6}p^{6r+3}$
U2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$-q^2p^{2r+1}$	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

22. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4+q^m}{p}$ *is a square,* $p \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
V1	$-\epsilon \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	q^2p^{2r+1}	$2^4q^{m+6}p^{6r+3}$
V2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

23. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{q^m-4}{p}$ *is a square,* $p \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
W1	$-\epsilon \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$-q^2p^{2r+1}$	$2^4q^{m+6}p^{6r+3}$
W2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$q^{m+2}p^{2r+1}$	$-2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

24. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell+q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
X1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
X2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

25. *There exist integers* $\ell \in \{4,5\}$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell-q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Y1	$\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell - q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$-2^{2\ell}q^{m+6}p^{6r+3}$
Y2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell - q^m}{p})$	$-q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

26. *There exist integers* $\ell \in \{4, 5\}$, $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{q^m - 2^\ell}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Z1	$\epsilon \cdot qp^{r+1}\psi(\frac{q^m - 2^\ell}{p})$	$-2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
Z2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m - 2^\ell}{p})$	$q^{m+2}p^{2r+1}$	$-2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

27. *There exist integers* $n \geq 0$ *and* $s \in \{0, 1\}$ *such that* $\frac{4p^n+1}{q}$ *is a square,* $q \equiv 5 \pmod 8$, $p^n \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AA1	$-\epsilon \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^4q^{6s+3}p^{2n+6}$
AA2	$\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^2$	$2^8q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

28. *There exist integers* $n \geq 0$ *and* $s \in \{0, 1\}$ *such that* $\frac{4p^n-1}{q}$ *is a square,* $q \equiv 3 \pmod 8$, $p^n \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves* [2]

	a_2	a_4	Δ
AB1	$-\epsilon \cdot q^{s+1}p\psi(\frac{4p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^4q^{6s+3}p^{2n+6}$
AB2	$\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4p^n-1}{q})$	$-q^{2s+1}p^2$	$2^8q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

29. *There exist integers* $\ell \in \{4, 5\}$, $n \geq 0$ *and* $s \in \{0, 1\}$ *such that* $\frac{2^\ell p^n+1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AC1	$\epsilon \cdot q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$2^{\ell-2}q^{2s+1}p^{n+2}$	$2^{2\ell}q^{6s+3}p^{2n+6}$
AC2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$q^{2s+1}p^2$	$2^{\ell+6}q^{6s+3}p^{n+6}$

[2] Typo in [Mul06, p. 116] the two a_2 values there are reversed. Also there are two Z curves.

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

30. *There exist integers* $\ell \in \{4,5\}$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n - 1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AD1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell p^n - 1}{q})$	$2^{\ell-2} q^{2s+1} p^{n+2}$	$-2^{2\ell} q^{6s+3} p^{2n+6}$
AD2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell p^n - 1}{q})$	$-q^{2s+1} p^2$	$2^{\ell+6} q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

31. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4+p^n}{q}$ *is a square,* $q \equiv 1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AE1	$-\epsilon \cdot q^{s+1} p \psi(\frac{4+p^n}{q})$	$q^{2s+1} p^2$	$2^4 q^{6s+3} p^{n+6}$
AE2	$\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{4+p^n}{q})$	$q^{2s+1} p^{n+2}$	$2^8 q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

32. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n - 4}{q}$ *is a square,* $q \equiv 3 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
AF1	$-\epsilon \cdot q^{s+1} p \psi(\frac{p^n - 4}{q})$	$-q^{2s+1} p^2$	$2^4 q^{6s+3} p^{n+6}$
AF2	$\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{p^n - 4}{q})$	$q^{2s+1} p^{n+2}$	$-2^8 q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

33. *There exist integers* $\ell \in \{4,5\}$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell + p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AG1	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell + p^n}{q})$	$2^{\ell-2} q^{2s+1} p^2$	$2^{2\ell} q^{6s+3} p^{n+6}$
AG2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell + p^n}{q})$	$q^{2s+1} p^{n+2}$	$2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

34. *There exist integers* $\ell \in \{4,5\}$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell - p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AH1$	$\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell - p^n}{q})$	$2^{\ell-2} q^{2s+1} p^2$	$-2^{2\ell} q^{6s+3} p^{n+6}$
$AH2$	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell - p^n}{q})$	$-q^{2s+1} p^{n+2}$	$2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

35. *There exist integers* $\ell \in \{4, 5\}$, $n \geq 0$ *and* $s \in \{0, 1\}$ *such that* $\frac{p^n - 2^\ell}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AI1$	$\epsilon \cdot q^{s+1} p \psi(\frac{p^n - 2^\ell}{q})$	$-2^{\ell-2} q^{2s+1} p^2$	$2^{2\ell} q^{6s+3} p^{n+6}$
$AI2$	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{p^n - 2^\ell}{q})$	$q^{2s+1} p^{n+2}$	$-2^{\ell+6} q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

36. *We have* $\ell = 5$, $p, q \in \{3, 11\}$ *distinct,* $r, s \in \{0, 1\}$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AJ1$	$\epsilon \cdot q^{s+1} p^{r+1} \psi(\frac{2^5 + 1}{qp})$	$2^3 q^{2s+1} p^{2r+1}$	$2^{10} q^{6s+3} p^{6r+3}$
$AJ2$	$-\epsilon \cdot 2 \cdot q^{s+1} p^{r+1} \psi(\frac{2^5 + 1}{qp})$	$q^{2s+1} p^{2r+1}$	$2^{11} q^{6s+3} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

37. *We have* $\ell = 4$, $p, q \in \{3, 5\}$ *distinct,* $r, s \in \{0, 1\}$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AK1$	$\epsilon \cdot q^{s+1} p^{r+1} \psi(\frac{2^4 - 1}{qp})$	$4q^{2s+1} p^{2r+1}$	$-2^8 q^{6s+3} p^{6r+3}$
$AK2$	$-\epsilon \cdot 2 \cdot q^{s+1} p^{r+1} \psi(\frac{2^4 - 1}{qp})$	$-q^{2s+1} p^{2r+1}$	$2^{10} q^{6s+3} p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

Theorem 2.2.14. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2^4 q^2 p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$-\epsilon \cdot qp\psi(2^\ell q^m p^n + 1)$	$2^{\ell-2} q^{m+2} p^{n+2}$	$2^{2\ell} q^{2m+6} p^{2n+6}$
A2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m p^n + 1)$	$q^2 p^2$	$2^{\ell+6} q^{m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

2. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4q^m + p^n$ *is a square,* $q^m \equiv 1 \pmod 4$*,* n *even or* $p \equiv 1 \pmod 4$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$\epsilon \cdot qp\psi(4q^m + p^n)$	$q^{m+2} p^2$	$2^4 q^{2m+6} p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot qp\psi(4q^m + p^n)$	$q^2 p^{n+2}$	$2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{m+1}p$ *modulo* 4.

3. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4q^m - p^n$ *is a square,* $q^m \equiv 1 \pmod 4$*,* n *odd and* $p \equiv 3 \pmod 8$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$\epsilon \cdot qp\psi(4q^m - p^n)$	$q^{m+2} p^2$	$-2^4 q^{2m+6} p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot qp\psi(4q^m - p^n)$	$-q^2 p^{n+2}$	$2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{m+1}p$ *modulo* 4.

4. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $p^n - 4q^m$ *is a square,* $q^m \equiv -1 \pmod 4$*,* n *even or* $p \equiv 1 \pmod 4$*, and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$\epsilon \cdot qp\psi(p^n - 4q^m)$	$-q^{m+2} p^2$	$2^4 q^{2m+6} p^{n+6}$
D2	$-\epsilon \cdot 2 \cdot qp\psi(p^n - 4q^m)$	$q^2 p^{n+2}$	$-2^8 q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{m+1}p$ *modulo* 4.

5. *There exist integers* $\ell \geq 4$*,* $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell q^m + p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$-\epsilon \cdot qp\psi(2^\ell q^m + p^n)$	$2^{\ell-2} q^{m+2} p^2$	$2^{2\ell} q^{2m+6} p^{n+6}$
E2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m + p^n)$	$q^2 p^{n+2}$	$2^{\ell+6} q^{m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

6. *There exist integers $\ell \geq 4$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$-\epsilon \cdot qp\psi(2^\ell q^m - p^n)$	$2^{\ell-2}q^{m+2}p^2$	$-2^{2\ell}q^{2m+6}p^{n+6}$
F2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell q^m - p^n)$	$-q^2p^{n+2}$	$2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

7. *There exist integers $\ell \geq 4$, $m \geq 0$ and $n \geq 0$ such that $p^n - 2^\ell q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$-\epsilon \cdot qp\psi(p^n - 2^\ell q^m)$	$-2^{\ell-2}q^{m+2}p^2$	$2^{2\ell}q^{2m+6}p^{n+6}$
G2	$\epsilon \cdot 2 \cdot qp\psi(p^n - 2^\ell q^m)$	q^2p^{n+2}	$-2^{\ell+6}q^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

8. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4p^n + q^m$ is a square, $q \equiv 5 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$\epsilon \cdot qp\psi(4p^n + q^m)$	q^2p^{n+2}	$2^4q^{m+6}p^{2n+6}$
H2	$-\epsilon \cdot 2 \cdot qp\psi(4p^n + q^m)$	$q^{m+2}p^2$	$2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{n+1} modulo 4.

9. *There exist integers $m \geq 0$ and $n \geq 0$ such that $4p^n - q^m$ is a square, $q \equiv 3 \pmod 8$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$\epsilon \cdot qp\psi(4p^n - q^m)$	q^2p^{n+2}	$-2^4q^{m+6}p^{2n+6}$
I2	$-\epsilon \cdot 2 \cdot qp\psi(4p^n - q^m)$	$-q^{m+2}p^2$	$2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp^{n+1} modulo 4.

10. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - 4p^n$ is a square, $q \equiv 5 \pmod 8$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$\epsilon \cdot qp\psi(q^m - 4p^n)$	$-q^2p^{n+2}$	$2^4q^{m+6}p^{2n+6}$
J2	$-\epsilon \cdot 2 \cdot qp\psi(q^m - 4p^n)$	$q^{m+2}p^2$	$-2^8q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $-p^{n+1}$ *modulo* 4.

11. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell p^n + q^m$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$-\epsilon \cdot qp\psi(2^\ell p^n + q^m)$	$2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
K2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n + q^m)$	$q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

12. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell p^n - q^m$ *is a square,* $q \equiv 7 \pmod 8$, m *odd and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$-\epsilon \cdot qp\psi(2^\ell p^n - q^m)$	$2^{\ell-2}q^2p^{n+2}$	$-2^{2\ell}q^{m+6}p^{2n+6}$
L2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell p^n - q^m)$	$-q^{m+2}p^2$	$2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

13. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 2^\ell p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$-\epsilon \cdot qp\psi(q^m - 2^\ell p^n)$	$-2^{\ell-2}q^2p^{n+2}$	$2^{2\ell}q^{m+6}p^{2n+6}$
M2	$\epsilon \cdot 2 \cdot qp\psi(q^m - 2^\ell p^n)$	$q^{m+2}p^2$	$-2^{\ell+6}q^{2m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

14. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $4 + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$\epsilon \cdot qp\psi(4 + q^m p^n)$	q^2p^2	$2^4q^{m+6}p^{n+6}$
N2	$-\epsilon \cdot 2 \cdot qp\psi(4 + q^m p^n)$	$q^{m+2}p^{n+2}$	$2^8q^{2m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

15. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 4$ *is a square,* $p \equiv 1 \pmod 4$ *if* $n \geq 1$, $q \equiv 1 \pmod 4$ *if* $m \geq 1$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
O1	$-\epsilon qp\psi(q^m p^n - 4)$	$-q^2p^2$	$2^4 q^{m+6} p^{n+6}$
O2	$\epsilon \cdot 2 \cdot qp\psi(q^m p^n - 4)$	$q^{m+2}p^{n+2}$	$-2^8 q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

16. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
P1	$-\epsilon \cdot qp\psi(2^\ell + q^m p^n)$	$2^{\ell-2}q^2p^2$	$2^{2\ell} q^{m+6} p^{n+6}$
P2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell + q^m p^n)$	$q^{m+2}p^{n+2}$	$2^{\ell+6} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

17. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Q1	$-\epsilon \cdot qp\psi(2^\ell - q^m p^n)$	$2^{\ell-2}q^2p^2$	$-2^{2\ell} q^{m+6} p^{n+6}$
Q2	$\epsilon \cdot 2 \cdot qp\psi(2^\ell - q^m p^n)$	$-q^{m+2}p^{n+2}$	$2^{\ell+6} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

18. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
R1	$-\epsilon \cdot qp\psi(q^m p^n - 2^\ell)$	$-2^{\ell-2}q^2p^2$	$2^{2\ell} q^{m+6} p^{n+6}$
R2	$\epsilon \cdot 2 \cdot qp\psi(q^m p^n - 2^\ell)$	$q^{m+2}p^{n+2}$	$-2^{\ell+6} q^{2m+6} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp *modulo* 4.

19. *There exist integers* $m \geq 0$ *and* $r \in \{0, 1\}$ *such that* $\frac{4q^m+1}{p}$ *is a square,* $p \equiv 5 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves* [3]

	a_2	a_4	Δ
S1	$\epsilon \cdot qp^{r+1}\psi(\frac{4q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^4 q^{2m+6} p^{6r+3}$
S2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4q^m+1}{p})$	q^2p^{2r+1}	$2^8 q^{m+6} p^{6r+3}$

[3] Typo in [Mul06, p. 120], the 2^m should be removed.

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{m+1}p^r$ *modulo* 4.

20. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4q^m-1}{p}$ *is a square,* $p \equiv 3 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves* [4]

	a_2	a_4	Δ
T1	$\epsilon \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^4q^{2m+6}p^{6r+3}$
T2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4q^m-1}{p})$	$-q^2p^{2r+1}$	$2^8q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{m+1}p^r$ *modulo* 4.

21. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell q^m+1}{p}$ *is a square,* $p \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves* [5]

	a_2	a_4	Δ
U1	$-\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$2^{2\ell}q^{2m+6}p^{6r+3}$
U2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	q^2p^{2r+1}	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* q *modulo* 4.

22. *There exist integers* $\ell \geq 4$, $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{2^\ell q^m-1}{p}$ *is a square,* $p \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves* [6]

	a_2	a_4	Δ
V1	$-\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$2^{\ell-2}q^{m+2}p^{2r+1}$	$-2^{2\ell}q^{2m+6}p^{6r+3}$
V2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$-q^2p^{2r+1}$	$2^{\ell+6}q^{m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^{r+1} *modulo* 4.

23. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{4+q^m}{p}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
W1	$\epsilon \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	q^2p^{2r+1}	$2^4q^{m+6}p^{6r+3}$
W2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{4+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* qp^r *modulo* 4.

[4] Typo in [Mul06, p. 121], the 2^m should be removed.
[5] Typo in [Mul06, p. 121], the 2^m should be 2^{m-2}.
[6] Typo in [Mul06, p. 121], the 2^m should be 2^{m-2}.

24. *There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-4}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
X1	$\epsilon \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$-q^2p^{2r+1}$	$2^4q^{m+6}p^{6r+3}$
X2	$-\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-4}{p})$	$q^{m+2}p^{2r+1}$	$-2^8q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of $-qp^r$ modulo 4.

25. *There exist integers $\ell \geq 4$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{2^\ell+q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Y1	$-\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
Y2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp^{r+1} modulo 4.

26. *There exist integers $\ell \geq 4$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{2^\ell-q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Z1	$-\epsilon \cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$2^{\ell-2}q^2p^{2r+1}$	$-2^{2\ell}q^{m+6}p^{6r+3}$
Z2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$-q^{m+2}p^{2r+1}$	$2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp^{r+1} modulo 4.

27. *There exist integers $\ell \geq 4$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-2^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AA1	$-\epsilon \cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$-2^{\ell-2}q^2p^{2r+1}$	$2^{2\ell}q^{m+6}p^{6r+3}$
AA2	$\epsilon \cdot 2 \cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$q^{m+2}p^{2r+1}$	$-2^{\ell+6}q^{2m+6}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of qp^{r+1} modulo 4.

28. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{4p^n+1}{q}$ is a square, $q \equiv 5 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AB1	$\epsilon \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^4q^{6s+3}p^{2n+6}$
AB2	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{4p^n+1}{q})$	$q^{2s+1}p^2$	$2^8q^{6s+3}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^s p^{n+1}$ *modulo* 4.

29. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4p^n-1}{q}$ *is a square,* $q \equiv 3 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AC1	$\epsilon \cdot q^{s+1} p \psi(\frac{4p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^4 q^{6s+3} p^{2n+6}$
AC2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{4p^n-1}{q})$	$-q^{2s+1}p^2$	$2^8 q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^s p^{n+1}$ *modulo* 4.

30. *There exist integers* $\ell \geq 4$*,* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n+1}{q}$ *is a square,* $q \equiv 1 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AD1	$-\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell p^n+1}{q})$	$2^{\ell-2} q^{2s+1} p^{n+2}$	$2^{2\ell} q^{6s+3} p^{2n+6}$
AD2	$\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell p^n+1}{q})$	$q^{2s+1}p^2$	$2^{\ell+6} q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* p *modulo* 4.

31. *There exist integers* $\ell \geq 4$*,* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell p^n-1}{q}$ *is a square,* $q \equiv 7 \pmod 8$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AE1	$-\epsilon \cdot q^{s+1} p \psi(\frac{2^\ell p^n-1}{q})$	$2^{\ell-2} q^{2s+1} p^{n+2}$	$-2^{2\ell} q^{6s+3} p^{2n+6}$
AE2	$\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{2^\ell p^n-1}{q})$	$-q^{2s+1}p^2$	$2^{\ell+6} q^{6s+3} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

32. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{4+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
AF1	$\epsilon \cdot q^{s+1} p \psi(\frac{4+p^n}{q})$	$q^{2s+1}p^2$	$2^4 q^{6s+3} p^{n+6}$
AF2	$-\epsilon \cdot 2 \cdot q^{s+1} p \psi(\frac{4+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^8 q^{6s+3} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^s p$ *modulo* 4.

33. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-4}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AG1$	$\epsilon \cdot q^{s+1}p\psi(\frac{p^n-4}{q})$	$-q^{2s+1}p^2$	$2^4q^{6s+3}p^{n+6}$
$AG2$	$-\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{p^n-4}{q})$	$q^{2s+1}p^{n+2}$	$-2^8q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $-q^sp$ *modulo* 4.

34. *There exist integers* $\ell \geq 4$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell+p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$AH1$	$-\epsilon \cdot q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$2^{\ell-2}q^{2s+1}p^2$	$2^{2\ell}q^{6s+3}p^{n+6}$
$AH2$	$\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^{\ell+6}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

35. *There exist integers* $\ell \geq 4$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{2^\ell-p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AI1$	$-\epsilon \cdot q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$2^{\ell-2}q^{2s+1}p^2$	$-2^{2\ell}q^{6s+3}p^{n+6}$
$AI2$	$\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$-q^{2s+1}p^{n+2}$	$2^{\ell+6}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

36. *There exist integers* $\ell \geq 4$, $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-2^\ell}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AJ1$	$-\epsilon \cdot q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$-2^{\ell-2}q^{2s+1}p^2$	$2^{2\ell}q^{6s+3}p^{n+6}$
$AJ2$	$\epsilon \cdot 2 \cdot q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$q^{2s+1}p^{n+2}$	$-2^{\ell+6}q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

37. *There exist integers* $\ell \geq 4$ *and* $r, s \in \{0,1\}$ *such that* $\frac{2^\ell+1}{qp}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AK1$	$-\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$2^{\ell-2}q^{2s+1}p^{2r+1}$	$2^{2\ell}q^{6s+3}p^{6r+3}$
$AK2$	$\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$q^{2s+1}p^{2r+1}$	$2^{\ell+6}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p^{r+1}$ *modulo* 4.

38. *There exist integers $\ell \geq 4$ and $r, s \in \{0, 1\}$ such that $\frac{2^\ell - 1}{qp}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
AL1	$-\epsilon \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$2^{\ell-2}q^{2s+1}p^{2r+1}$	$-2^{2\ell}q^{6s+3}p^{6r+3}$
AL2	$\epsilon \cdot 2 \cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$-q^{2s+1}p^{2r+1}$	$2^{\ell+6}q^{6s+3}p^{6r+3}$

where $\epsilon \in \{\pm 1\}$ is the residue of $q^{s+1}p^{r+1}$ modulo 4.

Theorem 2.2.15. *The elliptic curves E defined over $\mathbb{Q}$ of conductor $2^5q^2p^2$ and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $\ell \geq 7$, $m \geq 0$ and $n \geq 0$ such that $8q^mp^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$qp\psi(8q^mp^n + 1)$	$2q^{m+2}p^{n+2}$	$2^6q^{2m+6}p^{2n+6}$
A2	$-2 \cdot qp\psi(8q^mp^n + 1)$	q^2p^2	$2^9q^{m+6}p^{n+6}$
A1′	$-qp\psi(8q^mp^n + 1)$	$2q^{m+2}p^{n+2}$	$2^6q^{2m+6}p^{2n+6}$
A2′	$2 \cdot qp\psi(8q^mp^n + 1)$	q^2p^2	$2^9q^{m+6}p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of qp modulo 4.

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $8q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$qp\psi(8q^m + p^n)$	$2q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
B2	$-2 \cdot qp\psi(8q^m + p^n)$	q^2p^{n+2}	$2^9q^{m+6}p^{2n+6}$
B1′	$-qp\psi(8q^m + p^n)$	$2q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
B2′	$2 \cdot qp\psi(8q^m + p^n)$	q^2p^{n+2}	$2^9q^{m+6}p^{2n+6}$

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $8q^m - p^n$ is a square, $p \equiv 7 \pmod 8$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$qp\psi(8q^m - p^n)$	$2q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
C2	$-2 \cdot qp\psi(8q^m - p^n)$	$-q^2p^{n+2}$	$2^9q^{m+6}p^{2n+6}$
C1′	$-qp\psi(8q^m - p^n)$	$2q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
C2′	$2 \cdot qp\psi(8q^m - p^n)$	$-q^2p^{n+2}$	$2^9q^{m+6}p^{2n+6}$

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - 8q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$qp\psi(p^n - 8q^m)$	$-2q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
D2	$-2 \cdot qp\psi(p^n - 8q^m)$	q^2p^{n+2}	$-2^9q^{m+6}p^{2n+6}$
D1′	$-qp\psi(p^n - 8q^m)$	$-2q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
D2′	$2 \cdot qp\psi(p^n - 8q^m)$	q^2p^{n+2}	$-2^9q^{m+6}p^{2n+6}$

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $8p^n + q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$qp\psi(8p^n + q^m)$	$2q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
E2	$-2 \cdot qp\psi(8p^n + q^m)$	$q^{m+2}p^2$	$2^9q^{2m+6}p^{n+6}$
E1′	$-qp\psi(8p^n + q^m)$	$2q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
E2′	$2 \cdot qp\psi(8p^n + q^m)$	$q^{m+2}p^2$	$2^9q^{2m+6}p^{n+6}$

6. *There exist integers $m \geq 0$ and $n \geq 0$ such that $8p^n - q^m$ is a square, $q \equiv 7 \pmod 8$, m odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$qp\psi(8p^n - q^m)$	$2q^2p^{n+2}$	$-2^6q^{m+6}p^{2n+6}$
F2	$-2 \cdot qp\psi(8p^n - q^m)$	$-q^{m+2}p^2$	$2^9q^{2m+6}p^{n+6}$
F1′	$-qp\psi(8p^n - q^m)$	$2q^2p^{n+2}$	$-2^6q^{m+6}p^{2n+6}$
F2′	$2 \cdot qp\psi(8p^n - q^m)$	$-q^{m+2}p^2$	$2^9q^{2m+6}p^{n+6}$

7. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - 8p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$qp\psi(q^m - 8p^n)$	$-2q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
G2	$-2 \cdot qp\psi(q^m - 8p^n)$	$q^{m+2}p^2$	$-2^9q^{2m+6}p^{n+6}$
G1′	$-qp\psi(q^m - 8p^n)$	$-2q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
G2′	$2 \cdot qp\psi(q^m - 8p^n)$	$q^{m+2}p^2$	$-2^9q^{2m+6}p^{n+6}$

8. *There exist integers $m \geq 0$ and $n \geq 0$ such that $8 + q^mp^n$ is a square, $p \equiv 1, 7 \pmod 8$ if $n > 0$, $q \equiv 1, 7 \pmod 8$ if $m > 0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$qp\psi(8+q^mp^n)$	$2q^2p^2$	$2^6q^{m+6}p^{n+6}$
H2	$-2\cdot qp\psi(8+q^mp^n)$	$q^{m+2}p^{n+2}$	$2^9q^{2m+6}p^{2n+6}$
H1′	$-qp\psi(8+q^mp^n)$	$2q^2p^2$	$2^6q^{m+6}p^{n+6}$
H2′	$2\cdot qp\psi(8+q^mp^n)$	$q^{m+2}p^{n+2}$	$2^9q^{2m+6}p^{2n+6}$

9. *There exist integers $m\geq 0$ and $n\geq 0$ such that q^mp^n-8 is a square, $p\equiv 1,3 \pmod 8$ if $n>0$, $q\equiv 1,3 \pmod 8$ if $m>0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$qp\psi(q^mp^n-8)$	$-2q^2p^2$	$2^6q^{m+6}p^{n+6}$
I2	$-2\cdot qp\psi(q^mp^n-8)$	$q^{m+2}p^{n+2}$	$-2^9q^{2m+6}p^{2n+6}$
I1′	$-qp\psi(q^mp^n-8)$	$-2q^2p^2$	$2^6q^{m+6}p^{n+6}$
I2′	$2\cdot qp\psi(q^mp^n-8)$	$q^{m+2}p^{n+2}$	$-2^9q^{2m+6}p^{2n+6}$

10. *There exist integers $m\geq 0$ and $n\geq 0$ such that q^mp^n+1 is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$2qp\psi(q^mp^n+1)$	$q^{m+2}p^{n+2}$	$2^6q^{2m+6}p^{2n+6}$
J2	$-4\cdot qp\psi(q^mp^n+1)$	$4q^2p^2$	$2^{12}q^{m+6}p^{n+6}$
J1′	$-2qp\psi(q^mp^n+1)$	$q^{m+2}p^{n+2}$	$2^6q^{2m+6}p^{2n+6}$
J2′	$4\cdot qp\psi(q^mp^n+1)$	$4q^2p^2$	$2^{12}q^{m+6}p^{n+6}$

11. *There exist integers $m\geq 0$ and $n\geq 0$ such that q^mp^n-1 is a square, $p\equiv 1 \pmod 4$ if $n>0$, $q\equiv 1 \pmod 4$ if $m>0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$2qp\psi(q^mp^n-1)$	q^2p^2	$2^6q^{2m+6}p^{2n+6}$
K2	$-4\cdot qp\psi(q^mp^n-1)$	$4q^{m+2}p^{n+2}$	$2^{12}q^{m+6}p^{n+6}$
K1′	$-2qp\psi(q^mp^n-1)$	q^2p^2	$2^6q^{2m+6}p^{2n+6}$
K2′	$4\cdot qp\psi(q^mp^n-1)$	$4q^{m+2}p^{n+2}$	$2^{12}q^{m+6}p^{n+6}$

12. *There exist integers $m\geq 0$ and $n\geq 0$ such that q^m+p^n is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

    (a) m is even or $q\equiv 1 \pmod 4$;

	a_2	a_4	Δ
L1	$2qp\psi(q^m+p^n)$	q^2p^{n+2}	$2^6q^{m+6}p^{2n+6}$
L2	$-4\cdot qp\psi(q^m+p^n)$	$4q^{m+2}p^2$	$2^{12}q^{2m+6}p^{n+6}$
L1′	$-2qp\psi(q^m+p^n)$	q^2p^{n+2}	$2^6q^{m+6}p^{2n+6}$
L2′	$4\cdot qp\psi(q^m+p^n)$	$4q^{m+2}p^2$	$2^{12}q^{2m+6}p^{n+6}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
M1	$2qp\psi(q^m+p^n)$	$q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
M2	$-4\cdot qp\psi(q^m+p^n)$	$4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$
M1′	$-2qp\psi(q^m+p^n)$	$q^{m+2}p^2$	$2^6q^{2m+6}p^{n+6}$
M2′	$4\cdot qp\psi(q^m+p^n)$	$4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$

13. There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
N1	$2qp\psi(q^m-p^n)$	$-q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
N2	$-4\cdot qp\psi(q^m-p^n)$	$4q^{m+2}$	$-2^{12}q^{2m+6}p^{n+2}$
N1′	$-2qp\psi(q^m-p^n)$	$-q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
N2′	$4\cdot qp\psi(q^m-p^n)$	$4q^{m+2}$	$-2^{12}q^{2m+6}p^{n+2}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
O1	$2qp\psi(q^m-p^n)$	$q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
O2	$-4\cdot qp\psi(q^m-p^n)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$
O1′	$-2qp\psi(q^m-p^n)$	$q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
O2′	$4\cdot qp\psi(q^m-p^n)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$

14. There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
P1	$2qp\psi(p^n-q^m)$	$-q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
P2	$-4\cdot qp\psi(p^n-q^m)$	$4q^{m+2}p^2$	$-2^{12}q^{2m+6}p^{n+6}$
P1′	$-2qp\psi(p^n-q^m)$	$-q^2p^{n+2}$	$2^6q^{m+6}p^{2n+6}$
P2′	$4\cdot qp\psi(p^n-q^m)$	$4q^{m+2}p^2$	$-2^{12}q^{2m+6}p^{n+6}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
Q1	$2qp\psi(p^n - q^m)$	$q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
Q2	$-4 \cdot qp\psi(p^n - q^m)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$
Q1′	$-2qp\psi(p^n - q^m)$	$q^{m+2}p^2$	$-2^6q^{2m+6}p^{n+6}$
Q2′	$4 \cdot qp\psi(p^n - q^m)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$

15. *There exist integers $m \geq 0$ and $r \in \{0, 1\}$ such that $\frac{8q^m+1}{p}$ is a square, $p \equiv 1 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
R1	$qp^{r+1}\psi(\frac{8q^m+1}{p})$	$2q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
R2	$-2 \cdot qp^{r+1}\psi(\frac{8q^m+1}{p})$	q^2p^{2r+1}	$2^9q^{m+6}p^{6r+3}$
R1′	$-qp^{r+1}\psi(\frac{8q^m+1}{p})$	$2q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
R2′	$2 \cdot qp^{r+1}\psi(\frac{8q^m+1}{p})$	q^2p^{2r+1}	$2^9q^{m+6}p^{6r+3}$

16. *There exist integers $m \geq 0$ and $r \in \{0, 1\}$ such that $\frac{8q^m-1}{p}$ is a square, $p \equiv 7 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
S1	$qp^{r+1}\psi(\frac{8q^m-1}{p})$	$2q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
S2	$-2 \cdot qp^{r+1}\psi(\frac{8q^m-1}{p})$	$-q^2p^{2r+1}$	$2^9q^{m+6}p^{6r+3}$
S1′	$-qp^{r+1}\psi(\frac{8q^m-1}{p})$	$2q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
S2′	$2 \cdot qp^{r+1}\psi(\frac{8q^m-1}{p})$	$-q^2p^{2r+1}$	$2^9q^{m+6}p^{6r+3}$

17. *There exist integers $m \geq 0$ and $r \in \{0, 1\}$ such that $\frac{8+q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
T1	$qp^{r+1}\psi(\frac{8+q^m}{p})$	$2q^2p^{2r+1}$	$2^6q^{m+6}p^{6r+3}$
T2	$-2 \cdot qp^{r+1}\psi(\frac{8+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^9q^{2m+6}p^{6r+3}$
T1′	$-qp^{r+1}\psi(\frac{8+q^m}{p})$	$2q^2p^{2r+1}$	$2^6q^{m+6}p^{6r+3}$
T2′	$2 \cdot qp^{r+1}\psi(\frac{8+q^m}{p})$	$q^{m+2}p^{2r+1}$	$2^9q^{2m+6}p^{6r+3}$

18. *There exist integers $m \geq 0$ and $r \in \{0, 1\}$ such that $\frac{8-q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
U1	$qp^{r+1}\psi(\frac{8-q^m}{p})$	$2q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
U2	$-2\cdot qp^{r+1}\psi(\frac{8-q^m}{p})$	$-q^{m+2}p^{2r+1}$	$2^9q^{2m+6}p^{6r+3}$
U1′	$-qp^{r+1}\psi(\frac{8-q^m}{p})$	$2q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
U2′	$2\cdot qp^{r+1}\psi(\frac{8-q^m}{p})$	$-q^{m+2}p^{2r+1}$	$2^9q^{2m+6}p^{6r+3}$

19. *There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-8}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
V1	$qp^{r+1}\psi(\frac{q^m-8}{p})$	$-2q^2p^{2r+1}$	$2^6q^{m+6}p^{6r+3}$
V2	$-2\cdot qp^{r+1}\psi(\frac{q^m-8}{p})$	$q^{m+2}p^{2r+1}$	$-2^9q^{2m+6}p^{6r+3}$
V1′	$-qp^{r+1}\psi(\frac{q^m-8}{p})$	$-2q^2p^{2r+1}$	$2^6q^{m+6}p^{6r+3}$
V2′	$2\cdot qp^{r+1}\psi(\frac{q^m-8}{p})$	$q^{m+2}p^{2r+1}$	$-2^9q^{2m+6}p^{6r+3}$

20. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{8p^n+1}{q}$ is a square, $q \equiv 1 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
W1	$q^{s+1}p\psi(\frac{8p^n+1}{q})$	$2q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
W2	$-2\cdot q^{s+1}p\psi(\frac{8p^n+1}{q})$	$q^{2s+1}p^2$	$2^9q^{6s+3}p^{n+6}$
W1′	$-q^{s+1}p\psi(\frac{8p^n+1}{q})$	$2q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
W2′	$2\cdot q^{s+1}p\psi(\frac{8p^n+1}{q})$	$q^{2s+1}p^2$	$2^9q^{6s+3}p^{n+6}$

21. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{8p^n-1}{q}$ is a square, $q \equiv 7 \pmod 8$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
X1	$q^{s+1}p\psi(\frac{8p^n-1}{q})$	$2q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
X2	$-2\cdot q^{s+1}p\psi(\frac{8p^n-1}{q})$	$-q^{2s+1}p^2$	$2^9q^{6s+3}p^{n+6}$
X1′	$-q^{s+1}p\psi(\frac{8p^n-1}{q})$	$2q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
X2′	$2\cdot q^{s+1}p\psi(\frac{8p^n-1}{q})$	$-q^{2s+1}p^2$	$2^9q^{6s+3}p^{n+6}$

22. *There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{8+p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
Y1	$q^{s+1}p\psi(\frac{8+p^n}{q})$	$2q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
Y2	$-2\cdot q^{s+1}p\psi(\frac{8+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^9q^{6s+3}p^{2n+6}$
Y1′	$-q^{s+1}p\psi(\frac{8+p^n}{q})$	$2q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
Y2′	$2\cdot q^{s+1}p\psi(\frac{8+p^n}{q})$	$q^{2s+1}p^{n+2}$	$2^9q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

23. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{8-p^n}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$Z1$	$q^{s+1}p\psi(\frac{8-p^n}{q})$	$2q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$Z2$	$-2\cdot q^{s+1}p\psi(\frac{8-p^n}{q})$	$-q^{2s+1}p^{n+2}$	$2^9q^{6s+3}p^{2n+6}$
$Z1'$	$-q^{s+1}p\psi(\frac{8-p^n}{q})$	$2q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$Z2'$	$2\cdot q^{s+1}p\psi(\frac{8-p^n}{q})$	$-q^{2s+1}p^{n+2}$	$2^9q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

24. *There exist integers* $n \geq 0$ *and* $s \in \{0,1\}$ *such that* $\frac{p^n-8}{q}$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AA1$	$q^{s+1}p\psi(\frac{p^n-8}{q})$	$-2q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
$AA2$	$-2\cdot q^{s+1}p\psi(\frac{p^n-8}{q})$	$q^{2s+1}p^{n+2}$	$-2^9q^{6s+3}p^{2n+6}$
$AA1'$	$-q^{s+1}p\psi(\frac{p^n-8}{q})$	$-2q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
$AA2'$	$2\cdot q^{s+1}p\psi(\frac{p^n-8}{q})$	$q^{2s+1}p^{n+2}$	$-2^9q^{6s+3}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ *is the residue of* $q^{s+1}p$ *modulo* 4.

25. *There exist integers* $m \geq 0$ *and* $r \in \{0,1\}$ *such that* $\frac{q^m+1}{p}$ *is a square,* $q^m \equiv -1 \pmod 4$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

(a) $p \equiv 1 \pmod 4$*;*

	a_2	a_4	Δ
$AB1$	$2qp^{r+1}\psi(\frac{q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
$AB2$	$-4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$
$AB1'$	$-2qp^{r+1}\psi(\frac{q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
$AB2'$	$4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$

(b) $p \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
$AC1$	$2qp^{r+1}\psi(\frac{q^m+1}{p})$	q^2p^{2r+1}	$2^6q^{m+6}p^{6r+3}$
$AC2$	$-4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$
$AC1'$	$-2qp^{r+1}\psi(\frac{q^m+1}{p})$	q^2p^{2r+1}	$2^6q^{m+6}p^{6r+3}$
$AC2'$	$4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$

26. There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-1}{p}$ is a square, $q^m \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
AD1	$2qp^{r+1}\psi(\frac{q^m-1}{p})$	$-q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
AD2	$-4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$
AD1′	$-2qp^{r+1}\psi(\frac{q^m-1}{p})$	$-q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
AD2′	$4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$

(b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
AE1	$2qp^{r+1}\psi(\frac{q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
AE2	$-4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$
AE1′	$-2qp^{r+1}\psi(\frac{q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
AE2′	$4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$

27. There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{q}$ is a square, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
AF1	$2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
AF2	$-4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
AF1′	$-2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
AF2′	$4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

(b) $q \equiv -1 \pmod 4$;

	a_2	a_4	Δ
AG1	$2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
AG2	$-4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$
AG1′	$-2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
AG2′	$4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

28. There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{q}$ is a square, $p^n \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
$AH1$	$2q^{s+1}p\psi(\frac{p^n-1}{q})$	$-q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$AH2$	$-4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$
$AH1'$	$-2q^{s+1}p\psi(\frac{p^n-1}{q})$	$-q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$AH2'$	$4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

(b) $q \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
$AI1$	$2q^{s+1}p\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
$AI2$	$-4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
$AI1'$	$-2q^{s+1}p\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
$AI2'$	$4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

29. *There exist integers* $r, s \in \{0, 1\}$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

(a) $qp \equiv 1 \pmod 4$*;*

	a_2	a_4	Δ
$AJ1$	0	$-q^{2s+1}p^{2r+1}$	$2^6q^{6s+3}p^{6r+3}$
$AJ2$	0	$4q^{2s+1}p^{2r+1}$	$-2^{12}q^{6s+3}p^{6r+3}$

(b) $qp \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
$AK1$	0	$q^{2s+1}p^{2r+1}$	$-2^6q^{6s+3}p^{6r+3}$
$AK2$	0	$-4q^{2s+1}p^{2r+1}$	$2^{12}q^{6s+3}p^{6r+3}$

Theorem 2.2.16. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2^6q^2p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $\ell \geq 3$*,* $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell q^m p^n + 1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$A1$	$2qp\psi(2^\ell q^m p^n + 1)$	$2^\ell q^{m+2}p^{n+2}$	$2^{2\ell+6}q^{2m+6}p^{2n+6}$
$A2$	$-4qp\psi(2^\ell q^m p^n + 1)$	$4q^2p^2$	$2^{\ell+12}q^{m+6}p^{n+6}$
$A1'$	$-2qp\psi(2^\ell q^m p^n + 1)$	$2^\ell q^{m+2}p^{n+2}$	$2^{2\ell+6}q^{2m+6}p^{2n+6}$
$A2'$	$4qp\psi(2^\ell q^m p^n + 1)$	$4q^2p^2$	$2^{\ell+12}q^{m+6}p^{n+6}$

2. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$2qp\psi(2^\ell q^m + p^n)$	$2^\ell q^{m+2} p^2$	$2^{2\ell+6} q^{2m+6} p^{n+6}$
B2	$-4qp\psi(2^\ell q^m + p^n)$	$4q^2 p^{n+2}$	$2^{\ell+12} q^{m+6} p^{2n+6}$
B1′	$-2qp\psi(2^\ell q^m + p^n)$	$2^\ell q^{m+2} p^2$	$2^{2\ell+6} q^{2m+6} p^{n+6}$
B2′	$4qp\psi(2^\ell q^m + p^n)$	$4q^2 p^{n+2}$	$2^{\ell+12} q^{m+6} p^{2n+6}$

3. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m - p^n$ is a square, $p \equiv 3 \pmod 4$, n odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$2qp\psi(2^\ell q^m - p^n)$	$2^\ell q^{m+2} p^2$	$-2^{2\ell+6} q^{2m+6} p^{n+6}$
C2	$-4qp\psi(2^\ell q^m - p^n)$	$-4q^2 p^{n+2}$	$2^{\ell+12} q^{m+6} p^{2n+6}$
C1′	$-2qp\psi(2^\ell q^m - p^n)$	$2^\ell q^{m+2} p^2$	$-2^{2\ell+6} q^{2m+6} p^{n+6}$
C2′	$4qp\psi(2^\ell q^m - p^n)$	$-4q^2 p^{n+2}$	$2^{\ell+12} q^{m+6} p^{2n+6}$

4. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $p^n - 2^\ell q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$2qp\psi(p^n - 2^\ell q^m)$	$-2^\ell q^{m+2} p^2$	$2^{2\ell+6} q^{2m+6} p^{n+6}$
D2	$-4qp\psi(p^n - 2^\ell q^m)$	$4q^2 p^{n+2}$	$-2^{\ell+12} q^{m+6} p^{2n+6}$
D1′	$-2qp\psi(p^n - 2^\ell q^m)$	$-2^\ell q^{m+2} p^2$	$2^{2\ell+6} q^{2m+6} p^{n+6}$
D2′	$4qp\psi(p^n - 2^\ell q^m)$	$4q^2 p^{n+2}$	$-2^{\ell+12} q^{m+6} p^{2n+6}$

5. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^\ell p^n + q^m$ is a square, $q \equiv 5 \pmod 8$ if $\ell = 2$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$2qp\psi(2^\ell p^n + q^m)$	$2^\ell q^2 p^{n+2}$	$2^{2\ell+6} q^{m+6} p^{2n+6}$
E2	$-4 \cdot qp\psi(2^\ell p^n + q^m)$	$4q^{m+2} p^2$	$2^{\ell+12} q^{2m+6} p^{n+6}$
E1′	$-2qp\psi(2^\ell p^n + q^m)$	$2^\ell q^2 p^{n+2}$	$2^{2\ell+6} q^{m+6} p^{2n+6}$
E2′	$4 \cdot qp\psi(2^\ell p^n + q^m)$	$4q^{m+2} p^2$	$2^{\ell+12} q^{2m+6} p^{n+6}$

6. *There exist integers $\ell \geq 2$, $m \geq 0$ and $n \geq 0$ such that $2^\ell p^n - q^m$ is a square, $q \equiv 7 \pmod 8$ when $\ell \geq 3$ or $q \equiv 3 \pmod 8$ if $\ell = 2$, m odd and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$2qp\psi(2^\ell p^n - q^m)$	$2^\ell q^2 p^{n+2}$	$-2^{2\ell+6} q^{m+6} p^{2n+6}$
F2	$-4 \cdot qp\psi(2^\ell p^n - q^m)$	$-4q^{m+2}p^2$	$2^{\ell+12} q^{2m+6} p^{n+6}$
F1′	$-2qp\psi(2^\ell p^n - q^m)$	$2^\ell q^2 p^{n+2}$	$-2^{2\ell+6} q^{m+6} p^{2n+6}$
F2′	$4 \cdot qp\psi(2^\ell p^n - q^m)$	$-4q^{m+2}p^2$	$2^{\ell+12} q^{2m+6} p^{n+6}$

7. *There exist integers* $\ell \geq 2$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m - 2^\ell p^n$ *is a square,* $q \equiv 5 \pmod 8$ *if* $\ell = 2$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$2qp\psi(q^m - 2^\ell p^n)$	$-2^\ell q^2 p^{n+2}$	$2^{2\ell+6} q^{m+6} p^{2n+6}$
G2	$-4 \cdot qp\psi(q^m - 2^\ell p^n)$	$4q^{m+2}p^2$	$-2^{\ell+12} q^{2m+6} p^{n+6}$
G1′	$-2qp\psi(q^m - 2^\ell p^n)$	$-2^\ell q^2 p^{n+2}$	$2^{2\ell+6} q^{m+6} p^{2n+6}$
G2′	$4 \cdot qp\psi(q^m - 2^\ell p^n)$	$4q^{m+2}p^2$	$-2^{\ell+12} q^{2m+6} p^{n+6}$

8. *There exist integers* $\ell \geq 2$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell + q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$2qp\psi(2^\ell + q^m p^n)$	$2^\ell q^2 p^2$	$2^{2\ell+6} q^{m+6} p^{n+6}$
H2	$-4 \cdot qp\psi(2^\ell + q^m p^n)$	$4q^{m+2}p^{n+2}$	$2^{\ell+12} q^{2m+6} p^{2n+6}$
H1′	$-2qp\psi(2^\ell + q^m p^n)$	$2^\ell q^2 p^2$	$2^{2\ell+6} q^{m+6} p^{n+6}$
H2′	$4 \cdot qp\psi(2^\ell + q^m p^n)$	$4q^{m+2}p^{n+2}$	$2^{\ell+12} q^{2m+6} p^{2n+6}$

9. *There exist integers* $\ell \geq 2$, $m \geq 0$ *and* $n \geq 0$ *such that* $2^\ell - q^m p^n$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$2qp\psi(2^\ell - q^m p^n)$	$2^\ell q^2 p^2$	$-2^{2\ell+6} q^{m+6} p^{n+6}$
I2	$-4 \cdot qp\psi(2^\ell - q^m p^n)$	$-4q^{m+2}p^{n+2}$	$2^{\ell+12} q^{2m+6} p^{2n+6}$
I1′	$-2qp\psi(2^\ell - q^m p^n)$	$2^\ell q^2 p^2$	$-2^{2\ell+6} q^{m+6} p^{n+6}$
I2′	$4 \cdot qp\psi(2^\ell - q^m p^n)$	$-4q^{m+2}p^{n+2}$	$2^{\ell+12} q^{2m+6} p^{2n+6}$

10. *There exist integers* $\ell \geq 2$, $m \geq 0$ *and* $n \geq 0$ *such that* $q^m p^n - 2^\ell$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$2qp\psi(q^m p^n - 2^\ell)$	$-2^\ell q^2 p^2$	$2^{2\ell+6} q^{m+6} p^{n+6}$
J2	$-4 \cdot qp\psi(q^m p^n - 2^\ell)$	$4q^{m+2}p^{n+2}$	$-2^{\ell+12} q^{2m+6} p^{2n+6}$
J1′	$-2qp\psi(q^m p^n - 2^\ell)$	$-2^\ell q^2 p^2$	$2^{2\ell+6} q^{m+6} p^{n+6}$
J2′	$4 \cdot qp\psi(q^m p^n - 2^\ell)$	$4q^{m+2}p^{n+2}$	$-2^{\ell+12} q^{2m+6} p^{2n+6}$

11. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$2qp\psi(q^m p^n + 1)$	q^2p^2	$2^6 q^{2m+6} p^{2n+6}$
K2	$-4 \cdot qp\psi(q^m p^n + 1)$	$4q^{m+2}p^{n+2}$	$2^{12} q^{m+6} p^{n+6}$
K1′	$-2qp\psi(q^m p^n + 1)$	q^2p^2	$2^6 q^{2m+6} p^{2n+6}$
K2′	$4 \cdot qp\psi(q^m p^n + 1)$	$4q^{m+2}p^{n+2}$	$2^{12} q^{m+6} p^{n+6}$

12. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m p^n - 1$ is a square, $p \equiv 1 \pmod 4$ if $n > 0$, $q \equiv 1 \pmod 4$ if $m > 0$, and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$2qp\psi(q^m p^n - 1)$	$q^{m+2}p^{n+2}$	$2^6 q^{2m+6} p^{2n+6}$
L2	$-4 \cdot qp\psi(q^m p^n - 1)$	$4q^2p^2$	$2^{12} q^{m+6} p^{n+6}$
L1′	$-2qp\psi(q^m p^n - 1)$	$q^{m+2}p^{n+2}$	$2^6 q^{2m+6} p^{2n+6}$
L2′	$4 \cdot qp\psi(q^m p^n - 1)$	$4q^2p^2$	$2^{12} q^{m+6} p^{n+6}$

13. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

    (a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
M1	$2qp\psi(q^m + p^n)$	$q^{m+2}p^2$	$2^6 q^{2m+6} p^{n+6}$
M2	$-4 \cdot qp\psi(q^m + p^n)$	$4q^2p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$
M1′	$-2qp\psi(q^m + p^n)$	$q^{m+2}p^2$	$2^6 q^{2m+6} p^{n+6}$
M2′	$4 \cdot qp\psi(q^m + p^n)$	$4q^2p^{n+2}$	$2^{12} q^{m+6} p^{2n+6}$

    (b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
N1	$2qp\psi(q^m + p^n)$	q^2p^{n+2}	$2^6 q^{m+6} p^{2n+6}$
N2	$-4 \cdot qp\psi(q^m + p^n)$	$4q^{m+2}p^2$	$2^{12} q^{2m+6} p^{n+6}$
N1′	$-2qp\psi(q^m + p^n)$	q^2p^{n+2}	$2^6 q^{m+6} p^{2n+6}$
N2′	$4 \cdot qp\psi(q^m + p^n)$	$4q^{m+2}p^2$	$2^{12} q^{2m+6} p^{n+6}$

14. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
O1	$2qp\psi(q^m - p^n)$	$q^{m+2}p^2$	$-2^6 q^{2m+6}p^{n+6}$
O2	$-4 \cdot qp\psi(q^m - p^n)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$
O1′	$-2qp\psi(q^m - p^n)$	$q^{m+2}p^2$	$-2^6 q^{2m+6}p^{n+6}$
O2′	$4 \cdot qp\psi(q^m - p^n)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
P1	$2qp\psi(q^m - p^n)$	$-q^2p^{n+2}$	$2^6 q^{m+6}p^{2n+6}$
P2	$-4 \cdot qp\psi(q^m - p^n)$	$4q^{m+2}p^2$	$-2^{12}q^{2m+6}p^{n+6}$
P1′	$-2qp\psi(q^m - p^n)$	$-q^2p^{n+2}$	$2^6 q^{m+6}p^{2n+6}$
P2′	$4 \cdot qp\psi(q^m - p^n)$	$4q^{m+2}p^2$	$-2^{12}q^{2m+6}p^{n+6}$

15. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - q^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

(a) m is even or $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
Q1	$2qp\psi(p^n - q^m)$	$q^{m+2}p^2$	$-2^6 q^{2m+6}p^{n+6}$
Q2	$-4 \cdot qp\psi(p^n - q^m)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$
Q1′	$-2qp\psi(p^n - q^m)$	$q^{m+2}p^2$	$-2^6 q^{2m+6}p^{n+6}$
Q2′	$4 \cdot qp\psi(p^n - q^m)$	$-4q^2p^{n+2}$	$2^{12}q^{m+6}p^{2n+6}$

(b) m is odd and $q \equiv 3 \pmod 4$;

	a_2	a_4	Δ
R1	$2qp\psi(p^n - q^m)$	$-q^2p^{n+2}$	$2^6 q^{m+6}p^{2n+6}$
R2	$-4 \cdot qp\psi(p^n - q^m)$	$4q^{m+2}$	$-2^{12}q^{2m+6}p^{n+6}$
R1′	$-2qp\psi(p^n - q^m)$	$-q^2p^{n+2}$	$2^6 q^{m+6}p^{2n+6}$
R2′	$4 \cdot qp\psi(p^n - q^m)$	$4q^{m+2}$	$-2^{12}q^{2m+6}p^{n+6}$

16. *There exist integers $\ell \geq 2$, $m \geq 0$ and $r \in \{0, 1\}$ such that $\frac{2^\ell q^m + 1}{p}$ is a square, $p \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
S1	$2qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$2^\ell q^{m+2}p^{2r+1}$	$2^{2\ell+6}q^{2m+6}p^{6r+3}$
S2	$-4 \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{\ell+12}q^{m+6}p^{6r+3}$
S1′	$-2qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$2^\ell q^{m+2}p^{2r+1}$	$2^{2\ell+6}q^{2m+6}p^{6r+3}$
S2′	$4 \cdot qp^{r+1}\psi(\frac{2^\ell q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{\ell+12}q^{m+6}p^{6r+3}$

17. *There exist integers $\ell \geq 2$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{2^\ell q^m - 1}{p}$ is a square, $p \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
T1	$2qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$2^\ell q^{m+2}p^{2r+1}$	$-2^{2\ell+6}q^{2m+6}p^{6r+3}$
T2	$-4\cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{\ell+12}q^{m+6}p^{6r+3}$
T1′	$-2qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$2^\ell q^{m+2}p^{2r+1}$	$-2^{2\ell+6}q^{2m+6}p^{6r+3}$
T2′	$4\cdot qp^{r+1}\psi(\frac{2^\ell q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{\ell+12}q^{m+6}p^{6r+3}$

18. *There exist integers $\ell \geq 2$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{2^\ell + q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
U1	$2qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$2^\ell q^2p^{2r+1}$	$2^{2\ell+6}q^{m+6}p^{6r+3}$
U2	$-4\cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$4q^{m+2}p^{2r+1}$	$2^{\ell+12}q^{2m+6}p^{6r+3}$
U1′	$-2qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$2^\ell q^2p^{2r+1}$	$2^{2\ell+6}q^{m+6}p^{6r+3}$
U2′	$4\cdot qp^{r+1}\psi(\frac{2^\ell+q^m}{p})$	$4q^{m+2}p^{2r+1}$	$2^{\ell+12}q^{2m+6}p^{6r+3}$

19. *There exist integers $\ell \geq 2$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{2^\ell - q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
V1	$2qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$2^\ell q^2p^{2r+1}$	$-2^{2\ell+6}q^{m+6}p^{6r+3}$
V2	$-4\cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$-4q^{m+2}p^{2r+1}$	$2^{\ell+12}q^{2m+6}p^{6r+3}$
V1′	$-2qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$2^\ell q^2p^{2r+1}$	$-2^{2\ell+6}q^{m+6}p^{6r+3}$
V2′	$4\cdot qp^{r+1}\psi(\frac{2^\ell-q^m}{p})$	$-4q^{m+2}p^{2r+1}$	$2^{\ell+12}q^{2m+6}p^{6r+3}$

20. *There exist integers $\ell \geq 2$, $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m - 2^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
W1	$2qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$-2^\ell q^2p^{2r+1}$	$2^{2\ell+6}q^{m+6}p^{6r+3}$
W2	$-4\cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$4q^{m+2}p^{2r+1}$	$-2^{\ell+12}q^{2m+6}p^{6r+3}$
W1′	$-2qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$-2^\ell q^2p^{2r+1}$	$2^{2\ell+6}q^{m+6}p^{6r+3}$
W2′	$4\cdot qp^{r+1}\psi(\frac{q^m-2^\ell}{p})$	$4q^{m+2}p^{2r+1}$	$-2^{\ell+12}q^{2m+6}p^{6r+3}$

21. *There exist integers $\ell \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^\ell p^n + 1}{q}$ is a square, $q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
X1	$2q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$2^\ell q^{2s+1}p^{n+2}$	$2^{2\ell+6}q^{6s+3}p^{2n+6}$
X2	$-4\cdot q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{\ell+12}q^{6s+3}p^{n+6}$
X1′	$-2q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$2^\ell q^{2s+1}p^{n+2}$	$2^{2\ell+6}q^{6s+3}p^{2n+6}$
X2′	$4\cdot q^{s+1}p\psi(\frac{2^\ell p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{\ell+12}q^{6s+3}p^{n+6}$

22. There exist integers $\ell \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^\ell p^n-1}{q}$ is a square, $q \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

	a_2	a_4	Δ
Y1	$2q^{s+1}p\psi(\frac{2^\ell p^n-1}{q})$	$2^\ell q^{2s+1}p^{n+2}$	$-2^{2\ell+6}q^{6s+3}p^{2n+6}$
Y2	$-4\cdot q^{s+1}p\psi(\frac{2^\ell p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{\ell+12}q^{6s+3}p^{n+6}$
Y1′	$-2q^{s+1}p\psi(\frac{2^\ell p^n-1}{q})$	$2^\ell q^{2s+1}p^{n+2}$	$-2^{2\ell+6}q^{6s+3}p^{2n+6}$
Y2′	$4\cdot q^{s+1}p\psi(\frac{2^\ell p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{\ell+12}q^{6s+3}p^{n+6}$

23. There exist integers $\ell \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^\ell+p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

	a_2	a_4	Δ
Z1	$2q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$2^\ell q^{2s+1}p^2$	$2^{2\ell+6}q^{6s+3}p^{n+6}$
Z2	$-4\cdot q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$4q^{2s+1}p^{n+2}$	$2^{\ell+12}q^{6s+3}p^{2n+6}$
Z1′	$-2q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$2^\ell q^{2s+1}p^2$	$2^{2\ell+6}q^{6s+3}p^{n+6}$
Z2′	$4\cdot q^{s+1}p\psi(\frac{2^\ell+p^n}{q})$	$4q^{2s+1}p^{n+2}$	$2^{\ell+12}q^{6s+3}p^{2n+6}$

24. There exist integers $\ell \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^\ell-p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve

	a_2	a_4	Δ
AA1	$2q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$2^\ell q^{2s+1}p^2$	$-2^{2\ell+6}q^{6s+3}p^{n+6}$
AA2	$-4\cdot q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$-4q^{2s+1}p^{n+2}$	$2^{\ell+12}q^{6s+3}p^{2n+6}$
AA1′	$-2q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$2^\ell q^{2s+1}p^2$	$-2^{2\ell+6}q^{6s+3}p^{n+6}$
AA2′	$4\cdot q^{s+1}p\psi(\frac{2^\ell-p^n}{q})$	$-4q^{2s+1}p^{n+2}$	$2^{\ell+12}q^{6s+3}p^{2n+6}$

25. There exist integers $\ell \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n-2^\ell}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve

	a_2	a_4	Δ
$AB1$	$2q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$-2^\ell q^{2s+1}p^2$	$2^{2\ell+6}q^{6s+3}p^{n+6}$
$AB2$	$-4\cdot q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$4q^{2s+1}p^{n+2}$	$-2^{\ell+12}q^{6s+3}p^{2n+6}$
$AB1'$	$-2q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$-2^\ell q^{2s+1}p^2$	$2^{2\ell+6}q^{6s+3}p^{n+6}$
$AB2'$	$4\cdot q^{s+1}p\psi(\frac{p^n-2^\ell}{q})$	$4q^{2s+1}p^{n+2}$	$-2^{\ell+12}q^{6s+3}p^{2n+6}$

26. *There exist integers $\ell \geq 2$ and $r, s \in \{0,1\}$ such that $\frac{2^\ell+1}{qp}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AC1$	$2q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$2^\ell q^{2s+1}p^{2r+1}$	$2^{2\ell+6}q^{6s+3}p^{6r+3}$
$AC2$	$-4\cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$4q^{2s+1}p^{2r+1}$	$2^{\ell+12}q^{6s+3}p^{6r+3}$
$AC1'$	$-2q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$2^\ell q^{2s+1}p^{2r+1}$	$2^{2\ell+6}q^{6s+3}p^{6r+3}$
$AC2'$	$4\cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell+1}{qp})$	$4q^{2s+1}p^{2r+1}$	$2^{\ell+12}q^{6s+3}p^{6r+3}$

27. *There exist integers $\ell \geq 2$ and $r, s \in \{0,1\}$ such that $\frac{2^\ell-1}{qp}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
$AD1$	$2q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$2^\ell q^{2s+1}p^{2r+1}$	$-2^{2\ell+6}q^{6s+3}p^{6r+3}$
$AD2$	$-4\cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$-4q^{2s+1}p^{2r+1}$	$2^{\ell+12}q^{6s+3}p^{6r+3}$
$AD1'$	$-2q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$2^\ell q^{2s+1}p^{2r+1}$	$-2^{2\ell+6}q^{6s+3}p^{6r+3}$
$AD2'$	$4\cdot q^{s+1}p^{r+1}\psi(\frac{2^\ell-1}{qp})$	$-4q^{2s+1}p^{2r+1}$	$2^{\ell+12}q^{6s+3}p^{6r+3}$

28. *There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m+1}{p}$ is a square, $q^m \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

(a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
$AE1$	$2qp^{r+1}\psi(\frac{q^m+1}{p})$	q^2p^{2r+1}	$2^6q^{m+6}p^{6r+3}$
$AE2$	$-4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$
$AE1'$	$-2qp^{r+1}\psi(\frac{q^m+1}{p})$	q^2p^{2r+1}	$2^6q^{m+6}p^{6r+3}$
$AE2'$	$4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$

(b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
$AF1$	$2qp^{r+1}\psi(\frac{q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
$AF2$	$-4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$
$AF1'$	$-2qp^{r+1}\psi(\frac{q^m+1}{p})$	$q^{m+2}p^{2r+1}$	$2^6q^{2m+6}p^{6r+3}$
$AF2'$	$4\cdot qp^{r+1}\psi(\frac{q^m+1}{p})$	$4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$

29. There exist integers $m \geq 0$ and $r \in \{0,1\}$ such that $\frac{q^m-1}{p}$ is a square, $q^m \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
$AG1$	$2qp^{r+1}\psi(\frac{q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
$AG2$	$-4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$
$AG1'$	$-2qp^{r+1}\psi(\frac{q^m-1}{p})$	$q^{m+2}p^{2r+1}$	$-2^6q^{2m+6}p^{6r+3}$
$AG2'$	$4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$-4q^2p^{2r+1}$	$2^{12}q^{m+6}p^{6r+3}$

(b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
$AH1$	$2qp^{r+1}\psi(\frac{q^m-1}{p})$	$-q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
$AH2$	$-4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$
$AH1'$	$-2qp^{r+1}\psi(\frac{q^m-1}{p})$	$-q^2p^{2r+1}$	$-2^6q^{m+6}p^{6r+3}$
$AH2'$	$4\cdot qp^{r+1}\psi(\frac{q^m-1}{p})$	$4q^{m+2}p^{2r+1}$	$2^{12}q^{2m+6}p^{6r+3}$

30. There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{q}$ is a square, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
$AI1$	$2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
$AI2$	$-4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$
$AI1'$	$-2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^2$	$2^6q^{6s+3}p^{n+6}$
$AI2'$	$4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

(b) $q \equiv -1 \pmod 4$;

	a_2	a_4	Δ
$AJ1$	$2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
$AJ2$	$-4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
$AJ1'$	$-2q^{s+1}p\psi(\frac{p^n+1}{q})$	$q^{2s+1}p^{n+2}$	$2^6q^{6s+3}p^{2n+6}$
$AJ2'$	$4\cdot q^{s+1}p\psi(\frac{p^n+1}{q})$	$4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

31. There exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{q}$ is a square, $p^n \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves

(a) $q \equiv 1 \pmod 4$;

	a_2	a_4	Δ
$AK1$	$2q^{s+1}p\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
$AK2$	$-4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$
$AK1'$	$-2q^{s+1}p\psi(\frac{p^n-1}{q})$	$q^{2s+1}p^{n+2}$	$-2^6q^{6s+3}p^{2n+6}$
$AK2'$	$4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$-4q^{2s+1}p^2$	$2^{12}q^{6s+3}p^{n+6}$

(b) $q \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
$AL1$	$2q^{s+1}p\psi(\frac{p^n-1}{q})$	$-q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$AL2$	$-4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$
$AL1'$	$-2q^{s+1}p\psi(\frac{p^n-1}{q})$	$-q^{2s+1}p^2$	$-2^6q^{6s+3}p^{n+6}$
$AL2'$	$4\cdot q^{s+1}p\psi(\frac{p^n-1}{q})$	$4q^{2s+1}p^{n+2}$	$2^{12}q^{6s+3}p^{2n+6}$

32. There exist integers $r, s \in \{0,1\}$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curve*

(a) $qp \equiv 1 \pmod 4$*;*

	a_2	a_4	Δ
$AM1$	0	$q^{2s+1}p^{2r+1}$	$-2^6q^{6s+3}p^{6r+3}$
$AM2$	0	$-4q^{2s+1}p^{2r+1}$	$2^{12}q^{6s+3}p^{6r+3}$

(b) $qp \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
$AN1$	0	$-q^{2s+1}p^{2r+1}$	$2^6q^{6s+3}p^{6r+3}$
$AN2$	0	$4q^{2s+1}p^{2r+1}$	$-2^{12}q^{6s+3}p^{6r+3}$

Theorem 2.2.17. *The elliptic curves* E *defined over* $\mathbb{Q}$ *of conductor* $2^7q^2p^2$ *and having at least one rational point of order* 2 *are the ones such that one of the following conditions is satisfied:*

1. *There exist integers* $m \geq 0$ *and* $n \geq 0$ *such that* $2q^mp^n - 1$ *is a square,* $p, q \equiv 1 \pmod 4$*,* $t \in \{0,1\}$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
$A1$	$2^{t+1}qp\psi(2q^mp^n-1)$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{8+6t}q^{2m+6}p^{2n+6}$
$A2$	$-2^{2-t}\cdot qp\psi(2q^mp^n-1)$	$-2^{2-2t}q^2p^2$	$2^{13-6t}q^{m+6}p^{n+6}$
$A1'$	$-2^{t+1}qp\psi(2q^mp^n-1)$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{8+6t}q^{2m+6}p^{2n+6}$
$A2'$	$2^{2-t}\cdot qp\psi(2q^mp^n-1)$	$-2^{2-2t}q^2p^2$	$2^{13-6t}q^{m+6}p^{n+6}$

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m + p^n$ is a square, $p \equiv 3 \pmod 4$, n odd, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$2^{t+1}qp\psi(2q^m + p^n)$	$2^{1+2t}q^{m+2}p^2$	$2^{8+6t}q^{2m+6}p^{n+6}$
B2	$-2^{2-t}qp\psi(2q^m + p^n)$	$2^{2-2t}q^2p^{n+2}$	$2^{13-6t}q^{m+6}p^{2n+6}$
B1′	$-2^{t+1}qp\psi(2q^m + p^n)$	$2^{1+2t}q^{m+2}p^2$	$2^{8+6t}q^{2m+6}p^{n+6}$
B2′	$2^{2-t}qp\psi(2q^m + p^n)$	$2^{2-2t}q^2p^{n+2}$	$2^{13-6t}q^{m+6}p^{2n+6}$

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2^\ell q^m - p^n$ is a square, either n even or $p \equiv 1 \pmod 4$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$2^{t+1}qp\psi(2q^m - p^n)$	$2^{1+2t}q^{m+2}p^2$	$-2^{8+6t}q^{2m+6}p^{n+6}$
C2	$-2^{2-t}qp\psi(2q^m - p^n)$	$-2^{2-2t}q^2p^{n+2}$	$2^{13-6t}q^{m+6}p^{2n+6}$
C1′	$-2^{t+1}qp\psi(2q^m - p^n)$	$2^{1+2t}q^{m+2}p^2$	$-2^{8+6t}q^{2m+6}p^{n+6}$
C2′	$2^{2-t}qp\psi(2q^m - p^n)$	$-2^{2-2t}q^2p^{n+2}$	$2^{13-6t}q^{m+6}p^{2n+6}$

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $p^n - 2^\ell q^m$ is a square, $p \equiv 3 \pmod 4$, n odd, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$2^{t+1}qp\psi(p^n - 2q^m)$	$-2^{1+2t}q^{m+2}p^2$	$2^{8+6t}q^{2m+6}p^{n+6}$
D2	$-2^{2-t}qp\psi(p^n - 2q^m)$	$2^{2-2t}q^2p^{n+2}$	$-2^{13-6t}q^{m+6}p^{2n+6}$
D1′	$-2^{t+1}qp\psi(p^n - 2q^m)$	$-2^{1+2t}q^{m+2}p^2$	$2^{8+6t}q^{2m+6}p^{n+6}$
D2′	$2^{2-t}qp\psi(p^n - 2q^m)$	$2^{2-2t}q^2p^{n+2}$	$-2^{13-6t}q^{m+6}p^{2n+6}$

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2p^n + q^m$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$2^{t+1}qp\psi(2p^n + q^m)$	$2^{1+2t}q^2p^{n+2}$	$2^{8+6t}q^{m+6}p^{2n+6}$
E2	$-2^{2-t} \cdot qp\psi(2p^n + q^m)$	$2^{2-2t}q^{m+2}p^2$	$2^{13-6t}q^{2m+6}p^{n+6}$
E1′	$-2^{t+1}qp\psi(2p^n + q^m)$	$2^{1+2t}q^2p^{n+2}$	$2^{8+6t}q^{m+6}p^{2n+6}$
E2′	$2^{2-t} \cdot qp\psi(2p^n + q^m)$	$2^{2-2t}q^{m+2}p^2$	$2^{13-6t}q^{2m+6}p^{n+6}$

6. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2p^n - q^m$ is a square, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$2^{t+1}qp\psi(2p^n - q^m)$	$2^{1+2t}q^2p^{n+2}$	$-2^{8+6t}q^{m+6}p^{2n+6}$
F2	$-2^{2-t} \cdot qp\psi(2p^n - q^m)$	$-2^{2-2t}q^{m+2}p^2$	$2^{13-6t}q^{2m+6}p^{n+6}$
F1′	$-2^{t+1}qp\psi(2p^n - q^m)$	$2^{1+2t}q^2p^{n+2}$	$-2^{8+6t}q^{m+6}p^{2n+6}$
F2′	$2^{2-t} \cdot qp\psi(2p^n - q^m)$	$-2^{2-2t}q^{m+2}p^2$	$2^{13-6t}q^{2m+6}p^{n+6}$

7. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^m - 2p^n$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$2^{t+1}qp\psi(q^m - 2p^n)$	$-2^{1+2t}q^2p^{n+2}$	$2^{8+6t}q^{m+6}p^{2n+6}$
G2	$-2^{2-t} \cdot qp\psi(q^m - 2p^n)$	$2^{2-2t}q^{m+2}p^2$	$-2^{13-6t}q^{2m+6}p^{n+6}$
G1′	$-2^{t+1}qp\psi(q^m - 2p^n)$	$-2^{1+2t}q^2p^{n+2}$	$2^{8+6t}q^{m+6}p^{2n+6}$
G2′	$2^{2-t} \cdot qp\psi(q^m - 2p^n)$	$2^{2-2t}q^{m+2}p^2$	$-2^{13-6t}q^{2m+6}p^{n+6}$

8. *There exist integers $m \geq 0$ and $n \geq 0$ such that $2+q^mp^n$ is a square, $p \equiv 1$ or $7 \pmod 8$ if $n > 0$, $q \equiv 1$ or $7 \pmod 8$ if $m > 0$, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$2^{t+1}qp\psi(2^\ell + q^mp^n)$	$2^{1+2t}q^2p^2$	$2^{8+6t}q^{m+6}p^{n+6}$
H2	$-2^{2-t} \cdot qp\psi(2^\ell + q^mp^n)$	$2^{2-2t}q^{m+2}p^{n+2}$	$2^{13-6t}q^{2m+6}p^{2n+6}$
H1′	$-2^{t+1}qp\psi(2^\ell + q^mp^n)$	$2^{1+2t}q^2p^2$	$2^{8+6t}q^{m+6}p^{n+6}$
H2′	$2^{2-t} \cdot qp\psi(2^\ell + q^mp^n)$	$2^{2-2t}q^{m+2}p^{n+2}$	$2^{13-6t}q^{2m+6}p^{2n+6}$

9. *There exist integers $m \geq 0$ and $n \geq 0$ such that $q^mp^n - 2$ is a square, $p \equiv 1$ or $3 \pmod 8$, $q \equiv 1$ or $3 \pmod 8$ if $m > 0$, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$2^{t+1}qp\psi(q^mp^n - 2^\ell)$	$-2^{1+2t}q^2p^2$	$2^{8+6t}q^{m+6}p^{n+6}$
I2	$-2^{2-t} \cdot qp\psi(q^mp^n - 2^\ell)$	$2^{2-2t}q^{m+2}p^{n+2}$	$-2^{13-6t}q^{2m+6}p^{2n+6}$
I1′	$-2^{t+1}qp\psi(q^mp^n - 2^\ell)$	$-2^{1+2t}q^2p^2$	$2^{8+6t}q^{m+6}p^{n+6}$
I2′	$2^{2-t} \cdot qp\psi(q^mp^n - 2^\ell)$	$2^{2-2t}q^{m+2}p^{n+2}$	$-2^{13-6t}q^{2m+6}p^{2n+6}$

10. *There exist integers $m \geq 0$ and $r, t \in \{0, 1\}$ such that $\frac{2q^m+1}{p}$ is a square, $p \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	$2^{t+1}qp^{r+1}\psi(\frac{2q^m+1}{p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$2^{8+6t}q^{2m+6}p^{6r+3}$
J2	$-2^{2-2t}\cdot qp^{r+1}\psi(\frac{2q^m+1}{p})$	$2^{2-2t}q^2p^{2r+1}$	$2^{13-6t}q^{m+6}p^{6r+3}$
J1′	$-2^{t+1}qp^{r+1}\psi(\frac{2q^m+1}{p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$2^{8+6t}q^{2m+6}p^{6r+3}$
J2′	$2^{2-2t}\cdot qp^{r+1}\psi(\frac{2q^m+1}{p})$	$2^{2-2t}q^2p^{2r+1}$	$2^{13-6t}q^{m+6}p^{6r+3}$

11. *There exist integers $m \geq 0$ and $r, t \in \{0, 1\}$ such that $\frac{2q^m-1}{p}$ is a square, $p \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
K1	$2^{t+1}qp^{r+1}\psi(\frac{2q^m-1}{p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$-2^{8+6t}q^{2m+6}p^{6r+3}$
K2	$-2^{2-2t}\cdot qp^{r+1}\psi(\frac{2q^m-1}{p})$	$-2^{2-2t}q^2p^{2r+1}$	$2^{13-6t}q^{m+6}p^{6r+3}$
K1′	$-2^{t+1}qp^{r+1}\psi(\frac{2q^m-1}{p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$-2^{8+6t}q^{2m+6}p^{6r+3}$
K2′	$2^{2-2t}\cdot qp^{r+1}\psi(\frac{2q^m-1}{p})$	$-2^{2-2t}q^2p^{2r+1}$	$2^{13-6t}q^{m+6}p^{6r+3}$

12. *There exist integers $m \geq 0$ and $r, t \in \{0, 1\}$ such that $\frac{2+q^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
L1	$2^{t+1}qp^{r+1}\psi(\frac{2+q^m}{p})$	$2^{1+2t}q^2p^{2r+1}$	$2^{8+6t}q^{m+6}p^{6r+3}$
L2	$-2^{2-2t}\cdot qp^{r+1}\psi(\frac{2+q^m}{p})$	$2^{2-2t}q^{m+2}p^{2r+1}$	$2^{13-6t}q^{2m+6}p^{6r+3}$
L1′	$-2^{t+1}qp^{r+1}\psi(\frac{2+q^m}{p})$	$2^{1+2t}q^2p^{2r+1}$	$2^{8+6t}q^{m+6}p^{6r+3}$
L2′	$2^{2-2t}\cdot qp^{r+1}\psi(\frac{2+q^m}{p})$	$2^{2-2t}q^{m+2}p^{2r+1}$	$2^{13-6t}q^{2m+6}p^{6r+3}$

13. *There exist integers $m \geq 0$ and $r, t \in \{0, 1\}$ such that $\frac{q^m-2}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
M1	$2^{t+1}qp^{r+1}\psi(\frac{q^m-2}{p})$	$-2^{1+2t}q^2p^{2r+1}$	$2^{8+6t}q^{m+6}p^{6r+3}$
M2	$-2^{2-2t}\cdot qp^{r+1}\psi(\frac{q^m-2}{p})$	$2^{2-2t}q^{m+2}p^{2r+1}$	$-2^{13-6t}q^{2m+6}p^{6r+3}$
M1′	$-2^{t+1}qp^{r+1}\psi(\frac{q^m-2}{p})$	$-2^{1+2t}q^2p^{2r+1}$	$2^{8+6t}q^{m+6}p^{6r+3}$
M2′	$2^{2-2t}\cdot qp^{r+1}\psi(\frac{q^m-2}{p})$	$2^{2-2t}q^{m+2}p^{2r+1}$	$-2^{13-6t}q^{2m+6}p^{6r+3}$

14. *There exist integers $n \geq 0$ and $s, t \in \{0, 1\}$ such that $\frac{2p^n+1}{q}$ is a square, $q \equiv 3 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
N1	$2^{t+1}q^{s+1}p\psi(\frac{2p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$2^{8+6t}q^{6s+3}p^{2n+6}$
N2	$-2^{2-2t}\cdot q^{s+1}p\psi(\frac{2p^n+1}{q})$	$2^{2-2t}q^{2s+1}p^2$	$2^{13-6t}q^{6s+3}p^{n+6}$
N1′	$-2^{t+1}q^{s+1}p\psi(\frac{2p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$2^{8+6t}q^{6s+3}p^{2n+6}$
N2′	$2^{2-2t}\cdot q^{s+1}p\psi(\frac{2p^n+1}{q})$	$2^{2-2t}q^{2s+1}p^2$	$2^{13-6t}q^{6s+3}p^{n+6}$

15. *There exist integers $n \geq 0$ and $s, t \in \{0,1\}$ such that $\frac{2p^n-1}{q}$ is a square, $q \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
O1	$\epsilon \cdot q^{s+1} p\psi(\frac{2p^n-1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$-2^{8+6t}q^{6s+3}p^{2n+6}$
O2	$-2^{2-2t} \cdot q^{s+1} p\psi(\frac{2p^n-1}{q})$	$-2^{2-2t}q^{2s+1}p^2$	$2^{13-6t}q^{6s+3}p^{n+6}$
O1′	$-\epsilon \cdot q^{s+1} p\psi(\frac{2p^n-1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$-2^{8+6t}q^{6s+3}p^{2n+6}$
O2′	$2^{2-2t} \cdot q^{s+1} p\psi(\frac{2p^n-1}{q})$	$-2^{2-2t}q^{2s+1}p^2$	$2^{13-6t}q^{6s+3}p^{n+6}$

16. *There exist integers $n \geq 0$ and $s, t \in \{0,1\}$ such that $\frac{2+p^n}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
P1	$2^{t+1}q^{s+1}p\psi(\frac{2+p^n}{q})$	$2^{1+2t}q^{2s+1}p^2$	$2^{8+6t}q^{6s+3}p^{n+6}$
P2	$-2^{2-2t} \cdot q^{s+1} p\psi(\frac{2+p^n}{q})$	$2^{2-2t}q^{2s+1}p^{n+2}$	$2^{13-6t}q^{6s+3}p^{2n+6}$
P1′	$-2^{t+1}q^{s+1}p\psi(\frac{2+p^n}{q})$	$2^{1+2t}q^{2s+1}p^2$	$2^{8+6t}q^{6s+3}p^{n+6}$
P2′	$2^{2-2t} \cdot q^{s+1} p\psi(\frac{2+p^n}{q})$	$2^{2-2t}q^{2s+1}p^{n+2}$	$2^{13-6t}q^{6s+3}p^{2n+6}$

17. *There exist integers $n \geq 0$ and $s, t \in \{0,1\}$ such that $\frac{p^n-2}{q}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curve*

	a_2	a_4	Δ
Q1	$2^{t+1}q^{s+1}p\psi(\frac{p^n-2}{q})$	$-2^{1+2t}q^{2s+1}p^2$	$2^{8+6t}q^{6s+3}p^{n+6}$
Q2	$-2^{2-2t} \cdot q^{s+1} p\psi(\frac{p^n-2}{q})$	$2^{2-2t}q^{2s+1}p^{n+2}$	$-2^{13-6t}q^{6s+3}p^{2n+6}$
Q1′	$-2^{t+1}q^{s+1}p\psi(\frac{p^n-2}{q})$	$-2^{1+2t}q^{2s+1}p^2$	$2^{8+6t}q^{6s+3}p^{n+6}$
Q2′	$2^{2-2t} \cdot q^{s+1} p\psi(\frac{p^n-2}{q})$	$2^{2-2t}q^{2s+1}p^{n+2}$	$-2^{13-6t}q^{6s+3}p^{2n+6}$

Theorem 2.2.18. *The elliptic curves E defined over $\mathbb{Q}$ of conductor $2^8q^2p^2$ and having at least one rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m p^n+1}{2}$ is a square, $p, q \equiv 1, 7 \pmod 8$, $t \in \{0,1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
A1	$2^{t+2}qp\psi(\frac{q^m p^n+1}{2})$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{9+6t}q^{2m+6}p^{2n+6}$
A2	$-2^{3-t}qp\psi(\frac{q^m p^n+1}{2})$	$-2^{3-2t}q^2p^2$	$2^{15-6t}q^{m+6}p^{n+6}$
A1′	$-2^{t+2}qp\psi(\frac{q^m p^n+1}{2})$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{9+6t}q^{2m+6}p^{2n+6}$
A2′	$2^{3-t}qp\psi(\frac{q^m p^n+1}{2})$	$-2^{3-2t}q^2p^2$	$2^{15-6t}q^{m+6}p^{n+6}$

2. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m p^n - 1}{2}$ is a square, $p, q \equiv 1, 3 \pmod 8$, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
B1	$2^{t+2}qp\psi(\frac{q^m p^n - 1}{2})$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{9+6t}q^{2m+6}p^{2n+6}$
B2	$-2^{3-t}qp\psi(\frac{q^m p^n - 1}{2})$	$-2^{3-2t}q^2p^2$	$2^{15-6t}q^{m+6}p^{n+6}$
B1′	$-2^{t+2}qp\psi(\frac{q^m p^n - 1}{2})$	$2^{1+2t}q^{m+2}p^{n+2}$	$-2^{9+6t}q^{2m+6}p^{2n+6}$
B2′	$2^{3-t}qp\psi(\frac{q^m p^n - 1}{2})$	$-2^{3-2t}q^2p^2$	$2^{15-6t}q^{m+6}p^{n+6}$

3. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m + p^n}{2}$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
C1	$2^{t+2}qp\psi(\frac{q^m + p^n}{2})$	$2^{1+2t}q^{m+2}p^2$	$2^{9+6t}q^{2m+6}p^{n+6}$
C2	$-2^{3-t}qp\psi(\frac{q^m + p^n}{2})$	$2^{3-2t}q^2p^{n+2}$	$2^{15-6t}q^{m+6}p^{2n+6}$
C1′	$-2^{t+2}qp\psi(\frac{q^m + p^n}{2})$	$2^{1+2t}q^{m+2}p^2$	$2^{9+6t}q^{2m+6}p^{n+6}$
C2′	$2^{3-t}qp\psi(\frac{q^m + p^n}{2})$	$2^{3-2t}q^2p^{n+2}$	$2^{15-6t}q^{m+6}p^{2n+6}$

4. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m - p^n}{2}$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
D1	$2^{t+2}qp\psi(\frac{q^m - p^n}{2})$	$2^{1+2t}q^{m+2}p^2$	$-2^{9+6t}q^{2m+6}p^{n+6}$
D2	$-2^{3-t}qp\psi(\frac{q^m - p^n}{2})$	$-2^{3-2t}q^2p^{n+2}$	$2^{15-6t}q^{m+6}p^{2n+6}$
D1′	$-2^{t+2}qp\psi(\frac{q^m - p^n}{2})$	$2^{1+2t}q^{m+2}p^2$	$-2^{9+6t}q^{2m+6}p^{n+6}$
D2′	$2^{3-t}qp\psi(\frac{q^m - p^n}{2})$	$-2^{3-2t}q^2p^{n+2}$	$2^{15-6t}q^{m+6}p^{2n+6}$

5. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n - q^m}{2}$ is a square, $t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
E1	$2^{t+2}qp\psi(\frac{p^n - q^m}{2})$	$2^{1+2t}q^2p^{n+2}$	$-2^{9+6t}q^{m+6}p^{2n+6}$
E2	$-2^{3-t}qp\psi(\frac{p^n - q^m}{2})$	$-2^{3-2t}q^{m+2}p^2$	$2^{15-6t}q^{2m+6}p^{n+6}$
E1′	$-2^{t+2}qp\psi(\frac{p^n - q^m}{2})$	$2^{1+2t}q^2p^{n+2}$	$-2^{9+6t}q^{m+6}p^{2n+6}$
E2′	$2^{3-t}qp\psi(\frac{p^n - q^m}{2})$	$-2^{3-2t}q^{m+2}p^2$	$2^{15-6t}q^{2m+6}p^{n+6}$

6. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m + 1}{2p}$ is a square, $q^m \equiv 1 \pmod 4$, $r, t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
F1	$2^{t+2}qp^{r+1}\psi(\frac{q^m+1}{2p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$2^{9+6t}q^{2m+6}p^{6r+3}$
F2	$-2^{3-t}qp^{r+1}\psi(\frac{q^m+1}{2p})$	$2^{3-2t}q^2p^{2r+1}$	$2^{15-6t}q^{m+6}p^{6r+3}$
F1′	$-2^{t+2}qp^{r+1}\psi(\frac{q^m+1}{2p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$2^{9+6t}q^{2m+6}p^{6r+3}$
F2′	$2^{3-t}qp^{r+1}\psi(\frac{q^m+1}{2p})$	$2^{3-2t}q^2p^{2r+1}$	$2^{15-6t}q^{m+6}p^{6r+3}$

7. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{q^m-1}{2p}$ is a square, $q^m \equiv 3 \pmod 4$, $r, t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
G1	$2^{t+2}qp^{r+1}\psi(\frac{q^m-1}{2p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$-2^{9+6t}q^{2m+6}p^{6r+3}$
G2	$-2^{3-t}qp^{r+1}\psi(\frac{q^m-1}{2p})$	$-2^{3-2t}q^2p^{2r+1}$	$2^{15-6t}q^{m+6}p^{6r+3}$
G1′	$-2^{t+2}qp^{r+1}\psi(\frac{q^m-1}{2p})$	$2^{1+2t}q^{m+2}p^{2r+1}$	$-2^{9+6t}q^{2m+6}p^{6r+3}$
G2′	$2^{3-t}qp^{r+1}\psi(\frac{q^m-1}{2p})$	$-2^{3-2t}q^2p^{2r+1}$	$2^{15-6t}q^{m+6}p^{6r+3}$

8. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n+1}{2q}$ is a square, $p^n \equiv 1 \pmod 4$, $s, t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
H1	$2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$2^{9+6t}q^{6s+3}p^{2n+6}$
H2	$-2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{3-2t}q^{2s+1}p^2$	$2^{15-6t}q^{6s+3}p^{n+6}$
H1′	$-2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$2^{9+6t}q^{6s+3}p^{2n+6}$
H2′	$2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{3-2t}q^{2s+1}p^2$	$2^{15-6t}q^{6s+3}p^{n+6}$

9. *There exist integers $m \geq 0$ and $n \geq 0$ such that $\frac{p^n-1}{2q}$ is a square, $p^n \equiv 3 \pmod 4$, $s, t \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
I1	$2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$-2^{9+6t}q^{6s+3}p^{2n+6}$
I2	$-2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$-2^{3-2t}q^{2s+1}p^2$	$2^{15-6t}q^{6s+3}p^{n+6}$
I1′	$-2^{t+2}q^{s+1}p\psi(\frac{p^n+1}{q})$	$2^{1+2t}q^{2s+1}p^{n+2}$	$-2^{9+6t}q^{6s+3}p^{2n+6}$
I2′	$2^{3-t}q^{s+1}p\psi(\frac{p^n+1}{q})$	$-2^{3-2t}q^{2s+1}p^2$	$2^{15-6t}q^{6s+3}p^{n+6}$

10. *There exist integers $r, s \in \{0, 1\}$ and E is $\mathbb{Q}$-isomorphic to one of the following elliptic curves*

	a_2	a_4	Δ
J1	0	$2q^{2s+1}p^{2r+1}$	$-2^9q^{6s+3}p^{6r+3}$
J2	0	$-8q^{2s+1}p^{2r+1}$	$2^{15}q^{6s+3}p^{6r+3}$

	a_2	a_4	Δ
K1	0	$-2q^{2s+1}p^{2r+1}$	$2^9q^{6s+3}p^{6r+3}$
K2	0	$8q^{2s+1}p^{2r+1}$	$-2^{15}q^{6s+3}p^{6r+3}$

Proof. The proof of this is completely analogous to [Mul06, p.146-149]. I will include the details here in the interest of correcting a few typos in the proof and to provide a reference for the reader.

We organize the curves from Theorem 2.1.1. Let A.I represent the curves labeled form 1 to 9 in the two tables. Similarly, let A.II represent the curves labeled from 10 to 18 in the tables and let A.III be the curves labeled from 19 to 27. Using the tables from [Mul06, p.15-16], we can easily compute the conductors of these curves just based on the valuations of the values of a_2, a_4, and Δ. Keeping the notation from Theorem 2.1.1 (in particular, that $\ell \geq 1$ unless it appears on the right hand side of an equation), we see that

	A.I	A.II	A.III
$v_2(a_2)$	r_1	$= r_1 + 1$ if $\ell \geq 1$ $> r_1 + 1$ if $\ell = 0$	$\geq r_1 + 2$
$v_2(a_4)$	$\ell + 2r_1 - 2$	$2r_1$	$2r_1 + 1$
$v_2(\Delta)$	$2\ell + 6r_1$	$\ell + 6r_1 + 6$	$6r_1 + 9$

In the first row, the greater sign in the second column comes from the fact that in this case, we can conclude that d must be even and so we get at least one additional exponent of 2 coming from the d value in a_2. Similarly, we do not know the exact contribution of $v_2(d)$ in the last column for a_2 and so we have a greater than or equal to sign to account for this. The conductor computations yield for the curves in A.I that

$$v_2(N) = \begin{cases} 0 & \text{if } r_1 = 0, \ell = 6, a \equiv 1 \pmod 4 \\ 1 & \text{if } r_1 = 0, \ell \geq 7, a \equiv 1 \pmod 4 \\ 2 & \text{if } r_1 = 0, \ell = 2, a \equiv 1 \pmod 4, b \equiv -1 \pmod 4 \\ 3 & \text{if } r_1 = 0, \ell = 2, a \equiv -1 \pmod 4, b \equiv 1 \pmod 4 \\ & \text{or } r_1 = 0, \ell = 4, 5, a \equiv 1 \pmod 4 \\ 4 & \text{if } r_1 = 0, \ell = 2, a \equiv b \equiv \pm 1 \pmod 4 \\ & \text{or } r_1 = 0, \ell \geq 4, a \equiv -1 \pmod 4 \\ 5 & \text{if } r_1 = 0, \ell = 3 \\ 6 & \text{if } r_1 = 1, \ell \geq 2 \\ 7 & \text{if } r_1 = 1, 2, \ell = 1. \end{cases}$$

For the curves in A.II, the conductor is

$$v_2(N) = \begin{cases} 0 & \text{if } r_1 = 0, \ell = 6, \frac{a}{2} \equiv -1 \pmod 4 \\ 1 & \text{if } r_1 = 0, \ell \geq 7, \frac{a}{2} \equiv -1 \pmod 4 \\ 2 & \text{if } r_1 = 0, \ell = 2, a - b \equiv 9 \pmod{16} \\ 3 & \text{if } r_1 = 0, \ell = 2, a - b \equiv 5 \pmod{16} \\ & \text{or } r_1 = 0, \ell = 4, 5, \frac{a}{2} \equiv -1 \pmod 4 \\ 4 & \text{if } r_1 = 0, \ell = 2, a - b \equiv 1, 13 \pmod{16} \\ & \text{or } r_1 = 0, \ell \geq 4, \frac{a}{2} \equiv 1 \pmod 4 \\ 5 & \text{if } r_1 = 0, \ell = 0, b \equiv -1 \pmod 4 \\ & \text{or } r_1 = 0, \ell = 3 \\ & \text{or } r_1 = 1, \ell = 0, \frac{b}{4} \equiv 1 \pmod 4 \\ 6 & \text{if } r_1 = 0, \ell = 0, b \equiv 1 \pmod 4 \\ & \text{or } r_1 = 1, \ell = 0, \frac{b}{4} \equiv -1 \pmod 4 \\ & \text{or } r_1 = 1, \ell \geq 1, \frac{b}{4} \equiv 1 \pmod 4 \\ 7 & \text{if } r_1 = 0, \ell = 1 \\ & \text{or } r_1 = 1, \ell \geq 1, \frac{b}{4} \equiv -1 \pmod 4. \end{cases}$$

Lastly, for the curves in A.III, we have

$$v_2(N) = 8.$$

To compute $v_q(N)$, consider the condition

(*) q appears as a coefficient of d^2 in the associated Diophantine Equation from the tables in Theorem 2.1.1.

Then, we have

$$v_q(N) = \begin{cases} 0 & \text{if (*) does not hold and } r_2 = 0 \text{ and } m = 0 \\ 1 & \text{if (*) does not hold and } r_2 = 0 \text{ and } m \neq 0 \\ 2 & \text{if } r_2 = 1 \text{ or (*) holds.} \end{cases}$$

Similarly, let

(**) p appears as a coefficient of d^2 in the associated Diophantine Equation from the tables in Theorem 2.1.1.

Then, we have

$$v_p(N) = \begin{cases} 0 & \text{if (**) does not hold and } r_3 = 0 \text{ and } n = 0 \\ 1 & \text{if (**) does not hold and } r_3 = 0 \text{ and } n \neq 0 \\ 2 & \text{if } r_3 = 1 \text{ or (**) holds.} \end{cases}$$

There is a key fact to point out in the above proof. To compute the conductor above, we used the tables from [Mul06, p.15-16]. In these tables, there is a different table when $q = 3$ and for $q \geq 5$. However, for our purposes, the only rows we are concerned with are the p and q-adic valuations of a_2 and a_4, the supplementary conditions and the conductor exponent. Looking only at these rows, we see that the $q = 3$ and the $q = 5$ cases coincide. From these tables it also easy to see that the above values for $v_q(N)$ and $v_p(N)$ are indeed correct. It is this fact here that shows us that the theorem from chapter 3 of [Mul06] can be generalized almost verbatim and give us the result stated above. ■

Having finished the classification in this case, we proceed to specialize the above information in terms of setting $q = 3$ and $q = 5$. Most of the work for $q = 3$ was done in [Mul06] but as we will see, we will need to reorganize this data in a way that is suitable for this work. One thing we would like to now do is look at the table in Theorem 2.1.1 and solve the listed Diophantine equations. It will turn out that for the most part we will not make use of the fact that we are dealing with primes p and q, but rather we will attempt to solve the equations in greater generality. Doing this will require a range of techniques common to Diophantine equations including some recently developed results.

Chapter 3

Diophantine Equations

The goal of this chapter is to take the Diophantine equations that arose in Theorem 2.1.1 and try to classify all integer solution to these equations. Throughout the course of solving these equations, we will require different techniques to solve equations with smaller exponents and equations with larger exponents. This is because modularity methods, the technique that will end up being our primary tool, require that exponents be suitably large in order to be applied. Thus, we will take a small detour and discuss integer, rational and $\{2, 5, \infty\}$-solutions to the equations $y^2 = x^q \pm 2^\alpha 5^\beta$ for $q \in \{3, 5\}$. In our case we will find that our treatment of $q = 5$ will require a lot more work than was needed in the case $y^2 = x^5 \pm 2^\alpha 3^\beta$ as in [Mul06]. There were complications with finding all rational solution to this equation and so we reduce ourselves to finding integer solutions to these equations via Thue-Mahler equations and an algorithm of [TdW92] with corrections in [TdW93] implemented by [Ham11]. All of the computer programs used in this section were implemented in MAGMA [BCP97].

3.1 S-Integer Solutions to $y^2 = x^3 \pm 2^\alpha 5^\beta$

The goal of this section is to find all integer solutions to $y^2 = x^3 \pm 2^\alpha 5^\beta$. In order to achieve this goal, it suffices to compute all S-integer solutions to $y^2 = x^3 \pm 2^\alpha 5^\beta$ for $S = \{2, 5, \infty\}$ and where $0 \leq \alpha, \beta \leq 6$. For this we use MAGMA to find the S-integer points and then use this data to create the following theorems using their built in calculator. An explanation of this method can be found in [Mul06].

The major idea here is to use bounds from Baker on linear forms in complex logarithms [Bak67] [Bak68] or the more recent updated work due to Matveev [Mat00]. In practice these bounds can still be difficult to work with. In his 1987 thesis, de Weger [dW89] found a way to lower the bound obtained via the LLL algorithm [LLL82]. Very briefly, let $P_1, ..., P_r$ be

generators for the free part of $E(\mathbb{Q})$. Then any $P \in E(\mathbb{Q})$ can be written of the form

$$P = T + n_1 P_1 + ... + n_r P_r$$

where T is an element of the torsion subgroup of $E(\mathbb{Q})$. For a point $(x, y) \in E(\mathbb{Q})$, one can show similar to [Sil09, p. 292] that

$$|x|_p^{-1/2} \leq C_2 e^{-C_3 \max\{|n_i|\}^2}$$

where C_2, C_3 are constants depending on the elliptic curve, the generators P_i and S and $p \in S$ is such that $|x|_p = \max\{|x|_q : q \in S\}$. Finding a lower bound on this $|x|_p$ would in turn find a lower bound on $\max\{|n_i|\}$ and thus would restrict the possible values of P. These lower bounds can be obtained when $p = \infty$ in [Dav95] and in certain cases when the rank of $E(\mathbb{Q})$ is bounded by at most 2 as in [RU96]. Fortunately, our elliptic curves of the form $y^2 = x^3 \pm 2^\alpha 5^\beta$ all have ranks bounded by at most 2. Hence we can apply these results and we get the following tables as computed by MAGMA [BCP97].

Theorem 3.1.1. *The integer points on*

$$y^2 = x^3 + 2^\alpha 5^\beta$$

with x-coordinate p^A, $p \neq 2, 5$, $A \geq 1$ and $\alpha, \beta \geq 0$ integers are given by

$$(\alpha, \beta, x, y) = (5, 5, 41, \pm 411).$$

Theorem 3.1.2. *The integer points on*

$$y^2 = x^3 + 2^\alpha 5^\beta$$

with x-coordinate $2^A p^B$, $p \neq 2, 5$, $B \geq 1$ and $A, \alpha, \beta \geq 0$ integers are given by

α	β	x	y	n
$0+6n$	1	$2^{2n-4}\cdot 41$	$\pm 2^{3n-6}\cdot 299$	$n\geq 2$
$0+6n$	4	$2^{2n+1}\cdot 3$	$\pm 2^{3n}\cdot 29$	$n\geq 0$
$1+6n$	0	$2^{2n-2}\cdot 17$	$\pm 2^{3n-3}\cdot 71$	$n\geq 1$
$1+6n$	1	$2^{2n-2}\cdot 3^2$	$\pm 2^{3n-3}\cdot 37$	$n\geq 1$
$2+6n$	2	$2^{2n+3}\cdot 3$	$\pm 2^{3n}\cdot 118$	$n\geq 0$
$2+6n$	3	$-2^{2n-2}\cdot 31$	$\pm 2^{3n-3}\cdot 47$	$n\geq 1$
$3+6n$	0	$-2^{2n-2}\cdot 7$	$\pm 2^{3n-3}\cdot 13$	$n\geq 1$
$3+6n$	0	$2^{2n+1}\cdot 23$	$\pm 2^{3n}\cdot 312$	$n\geq 0$
$3+6n$	1	$2^{2n+1}\cdot 3$	$\pm 2^{3n}\cdot 16$	$n\geq 0$
$3+6n$	3	$-2^{2n+1}\cdot 3$	$\pm 2^{3n}\cdot 28$	$n\geq 0$
$3+6n$	4	$-2^{2n+1}\cdot 7$	$\pm 2^{3n}\cdot 88$	$n\geq 0$
$4+6n$	1	$2^{2n+2}\cdot 11$	$\pm 2^{3n}\cdot 292$	$n\geq 0$
$5+6n$	5	$2^{2n}\cdot 41$	$\pm 2^{3n}\cdot 411$	$n\geq 0$

Table 3.1: Integer solutions to $y^2=x^3+2^\alpha 5^\beta$ with x-coordinate $2^A p^B$, $p\neq 2,5$, $B\geq 1$ and $A,\alpha,\beta\geq 0$.

Theorem 3.1.3. *The integer points on*

$$y^2=x^3+2^\alpha 5^\beta$$

with x-coordinate $5^A p^B$, $p\neq 2,5$, $B\geq 1$ and $A,\alpha,\beta\geq 0$ integers are given by

α	β	x	y	m
0	$4+6m$	$5^{2m+2}\cdot 3$	$\pm 5^{3m+2}\cdot 26$	$m\geq 0$
3	$3+6m$	$5^{2m+1}\cdot 13$	$\pm 5^{3m+2}\cdot 21$	$m\geq 0$
5	$3+6m$	$-5^{2m+1}\cdot 3$	$\pm 5^{3m+2}$	$m\geq 0$
5	$5+6m$	$5^{2m}\cdot 41$	$\pm 5^{3m}\cdot 411$	$m\geq 0$

Table 3.2: Integer solutions to $y^2=x^3+2^\alpha 5^\beta$ with x-coordinate $5^A p^B$, $p\neq 2,5$, $B\geq 1$ and $A,\alpha,\beta\geq 0$.

Theorem 3.1.4. *The integer points on*

$$y^2=x^3+2^\alpha 5^\beta$$

with x-coordinate $2^A 5^B p^C$, $p\neq 2,5$, $C\geq 1$ and $A,B,\alpha,\beta\geq 0$ integers are given by

α	β	x	y	n	m
$0+6n$	$1+6m$	$2^{2n-4}\cdot 5^{2m}\cdot 41$	$\pm 2^{3n-6}\cdot 5^{3m}\cdot 299$	$n\geq 2$	$m\geq 0$
$0+6n$	$4+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m}\cdot 29$	$n\geq 0$	$m\geq 0$
$0+6n$	$4+6m$	$2^{2n}\cdot 5^{2m+2}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m+2}\cdot 26$	$n\geq 0$	$m\geq 0$
$1+6n$	$0+6m$	$2^{2n-2}\cdot 5^{2m}\cdot 17$	$\pm 2^{3n-3}\cdot 5^{3m}\cdot 71$	$n\geq 1$	$m\geq 0$
$1+6n$	$1+6m$	$2^{2n-2}\cdot 5^{2m}\cdot 3^2$	$\pm 2^{3n-3}\cdot 5^{3m}\cdot 37$	$n\geq 1$	$m\geq 0$
$2+6n$	$2+6m$	$2^{2n+3}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m}\cdot 118$	$n\geq 0$	$m\geq 0$
$2+6n$	$2+6m$	$-2^{2n-2}\cdot 5^{2m+1}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m+1}\cdot 11$	$n\geq 1$	$m\geq 0$
$2+6n$	$3+6m$	$-2^{2n-2}\cdot 5^{2m}\cdot 31$	$\pm 2^{3n-3}\cdot 5^{3m}\cdot 47$	$n\geq 1$	$m\geq 0$
$3+6n$	$0+6m$	$-2^{2n-2}\cdot 5^{2m}\cdot 7$	$\pm 2^{3n-3}\cdot 5^{3m}\cdot 13$	$n\geq 1$	$m\geq 0$
$3+6n$	$0+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 23$	$\pm 2^{3n}\cdot 5^{3m}\cdot 312$	$n\geq 0$	$m\geq 0$
$3+6n$	$1+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m}\cdot 16$	$n\geq 0$	$m\geq 0$
$3+6n$	$3+6m$	$-2^{2n+1}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m}\cdot 28$	$n\geq 0$	$m\geq 0$
$3+6n$	$3+6m$	$2^{2n}\cdot 5^{2m+1}\cdot 13$	$\pm 2^{3n}\cdot 5^{3m+2}\cdot 21$	$n\geq 0$	$m\geq 0$
$3+6n$	$4+6m$	$-2^{2n+1}\cdot 5^{2m}\cdot 7$	$\pm 2^{3n}\cdot 5^{3m}\cdot 88$	$n\geq 0$	$m\geq 0$
$4+6n$	$1+6m$	$2^{2n+2}\cdot 5^{2m}\cdot 11$	$\pm 2^{3n}\cdot 5^{3m}\cdot 292$	$n\geq 0$	$m\geq 0$
$4+6n$	$1+6m$	$2^{2n+2}\cdot 5^{2m-1}\cdot 11$	$\pm 2^{3n}\cdot 5^{3m-3}\cdot 3927$	$n\geq 0$	$m\geq 1$
$5+6n$	$3+6m$	$-2^{2n}\cdot 5^{2m+1}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m+2}$	$n\geq 0$	$m\geq 0$
$5+6n$	$5+6m$	$2^{2n}\cdot 5^{2m}\cdot 41$	$\pm 2^{3n}\cdot 5^{3m}\cdot 411$	$n\geq 0$	$m\geq 0$

Table 3.3: Integer solutions to $y^2 = x^3 + 2^\alpha 5^\beta$ with x-coordinate $2^A 5^B p^C$, $p \neq 2, 5$, $C \geq 1$ and $A, B, \alpha, \beta \geq 0$.

Theorem 3.1.5. *The integer points on*

$$y^2 = x^3 - 2^\alpha 5^\beta$$

with x-coordinate p^A, $p \neq 2, 5$, $A \geq 1$ and $\alpha, \beta \geq 0$ integers are given by

α	β	x	y
1	0	3	± 5
1	4	11	± 9
3	2	9	± 23
5	2	41	± 261

Table 3.4: Integer solutions to $y^2 = x^3 - 2^\alpha 5^\beta$ with x-coordinate p^A, $p \neq 2, 5$, $A \geq 1$ and $\alpha, \beta \geq 0$.

Theorem 3.1.6. *The integer points on*

$$y^2 = x^3 - 2^\alpha 5^\beta$$

with x-coordinate $2^A p^B$, $p \neq 2, 5$, $B \geq 1$ and $A, \alpha, \beta \geq 0$ integers are given by

α	β	x	y	n
$1+6n$	0	$2^{2n} \cdot 3$	$\pm 2^{3n} \cdot 5$	$n \geq 0$
$1+6n$	4	$2^{2n} \cdot 11$	$\pm 2^{3n} \cdot 9$	$n \geq 0$
$2+6n$	1	$2^{2n+1} \cdot 3$	$\pm 2^{3n+1} \cdot 7$	$n \geq 0$
$2+6n$	2	$2^{2n+1} \cdot 17$	$\pm 2^{3n+1} \cdot 99$	$n \geq 0$
$3+6n$	1	$2^{2n+1} \cdot 7$	$\pm 2^{3n+2} \cdot 13$	$n \geq 0$
$3+6n$	2	$2^{2n+1} \cdot 3$	$\pm 2^{3n+2}$	$n \geq 0$
$3+6n$	2	$2^{2n} \cdot 9$	$\pm 2^{3n} \cdot 23$	$n \geq 0$
$5+6n$	2	$2^{2n} \cdot 41$	$\pm 2^{3n} \cdot 261$	$n \geq 0$

Table 3.5: Integer solutions to $y^2 = x^3 - 2^\alpha 5^\beta$ with x-coordinate $2^A p^B$, $p \neq 2, 5$, $B \geq 1$ and $A, \alpha, \beta \geq 0$.

Theorem 3.1.7. *The integer points on*

$$y^2 = x^3 - 2^\alpha 5^\beta$$

with x-coordinate $5^A p^B$, $p \neq 2, 5$, $B \geq 1$ and $A, \alpha, \beta \geq 0$ integers are given by

α	β	x	y	m
1	$0+6m$	$5^{2m} \cdot 3$	$\pm 5^{3m} \cdot 5$	$m \geq 0$
1	$4+6m$	$5^{2m} \cdot 11$	$\pm 5^{3m} \cdot 9$	$m \geq 0$
3	$2+6m$	$5^{2m} \cdot 9$	$\pm 5^{3m} \cdot 23$	$m \geq 0$
5	$2+6m$	$5^{2m} \cdot 41$	$\pm 5^{3m} \cdot 261$	$m \geq 0$

Table 3.6: Integer solutions to $y^2 = x^3 - 2^\alpha 5^\beta$ with x-coordinate $5^A p^B$, $p \neq 2, 5$, $B \geq 1$ and $A, \alpha, \beta \geq 0$.

Theorem 3.1.8. *The integer points on*

$$y^2 = x^3 - 2^\alpha 5^\beta$$

with x-coordinate $2^A 5^B p^C$, $p \neq 2, 5$, $C \geq 1$ and $A, B, \alpha, \beta \geq 0$ integers are given by

α	β	x	y	n	m
$0+6n$	$2+6m$	$2^{2n-4}\cdot 5^{2m+1}\cdot 13$	$\pm 2^{3n-6}\cdot 5^{3m+1}\cdot 83$	$n\geq 2$	$m\geq 0$
$1+6n$	$0+6m$	$2^{2n}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n}\cdot 5^{3m}\cdot 5$	$n\geq 0$	$m\geq 0$
$1+6n$	$4+6m$	$2^{2n}\cdot 5^{2m}\cdot 11$	$\pm 2^{3n}\cdot 5^{3m}\cdot 9$	$n\geq 0$	$m\geq 0$
$2+6n$	$1+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n+1}\cdot 5^{3m}\cdot 7$	$n\geq 0$	$m\geq 0$
$2+6n$	$2+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 17$	$\pm 2^{3n+1}\cdot 5^{3m}\cdot 99$	$n\geq 0$	$m\geq 0$
$2+6n$	$2+6m$	$2^{2n-2}\cdot 5^{2m+1}\cdot 37$	$\pm 2^{3n-3}\cdot 5^{3m+1}\cdot 503$	$n\geq 1$	$m\geq 0$
$3+6n$	$1+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 7$	$\pm 2^{3n+2}\cdot 5^{3m}\cdot 13$	$n\geq 0$	$m\geq 0$
$3+6n$	$2+6m$	$2^{2n+1}\cdot 5^{2m}\cdot 3$	$\pm 2^{3n+2}\cdot 5^{3m}$	$n\geq 0$	$m\geq 0$
$3+6n$	$2+6m$	$2^{2n}\cdot 5^{2m}\cdot 9$	$\pm 2^{3n}\cdot 5^{3m}\cdot 23$	$n\geq 0$	$m\geq 0$
$4+6n$	$4+6m$	$2^{2n-2}\cdot 5^{2m+2}\cdot 17$	$\pm 2^{3n-3}\cdot 5^{3m+2}\cdot 349$	$n\geq 1$	$m\geq 0$
$5+6n$	$2+6m$	$2^{2n}\cdot 5^{2m}\cdot 41$	$\pm 2^{3n}\cdot 5^{3m}\cdot 261$	$n\geq 0$	$m\geq 0$

Table 3.7: Integer solutions to $y^2 = x^3 - 2^\alpha 5^\beta$ with x-coordinate $2^A 5^B p^C$, $p \neq 2, 5$, $C \geq 1$ and $A, B, \alpha, \beta \geq 0$.

3.2 Integer and Rational Solutions to $y^2 = x^5 \pm 2^\alpha 5^\beta$

The goal of this section is to compute solutions to $y^2 = x^5 \pm 2^\alpha 5^\beta$ for $\alpha, \beta \geq 0$. This equation is much more difficult to solve in comparison to the curve $y^2 = x^5 \pm 2^\alpha 3^\beta$ as was considered by my predecessor in [Mul06]. To proceed to solve this question, we will begin with attempting to solve this equation using Chabauty's method. Chabauty's method as implemented here depends on two key factors. One is knowledge of the Mordell-Weil group attached to the hyperelliptic curve and the other is ensuring that the aforementioned group has rank strictly less than the genus of our curves, which in our case is 2. Failing this, we apply the techniques of Elliptic Curve Chabauty to a covering of the remaining curves. This method however also suffers from the Mordell-Weil group computations being difficult in certain cases. I will then briefly mention the work of Gallegos-Ruiz [GR11] on S-integral solutions to Diophantine equations which is a continuation of the work of [BMS+08]. In particular, I will discuss how one verifies the ranks of certain genus 2 curves and then outline how an approach using these papers would proceed. Upon exhausting these techniques, we will use the work of [Ham11] on Thue-Mahler equations to help solve the remaining cases.

3.2.1 Chabauty's Method

We begin by using Chabauty's method [Cha41] to figure out the rational solutions to the equation $y^2 = x^5 \pm 2^\alpha 5^\beta$ where $(x, y) \in \mathbb{Q}^2$ and $\alpha, \beta \in \mathbb{Z}^+$. A hypothesized set of solutions is given as follows by searching for points with small heights.

Conjecture 3.2.1. *Rational solutions to* $y^2 = x^5 + 2^\alpha 5^\beta$ *with integers* $0 \leq \alpha, \beta \leq 9$ *are given by*

1. *If* $\alpha, \beta \in 2\mathbb{Z}$, *then* $(x, y) = (0, \pm 2^{\alpha/2} 5^{\beta/2})$ *is a set of solutions.*
2. *If* $\alpha, \beta \in 5\mathbb{Z}$, *then* $(x, y) = (-2^{\alpha/5} 5^{\beta/5}, 0)$ *is a set of solutions.*
3. *In addition to the above solutions, we have solutions given by*

α	β	$2^\alpha 5^\beta$	(x, y)
0	1	5	$(-1, \pm 2)$
1	0	2	$(-1, \pm 1)$
1	1	10	$(-1, \pm 3)$
1	2	50	$(-1, \pm 7)$
1	5	6250	$(15, \pm 875), (\frac{-15}{4}, \pm \frac{2375}{32})$
2	0	4	$(2, \pm 6)$
2	4	2500	$(5, \pm 75)$
2	5	12500	$(5, \pm 125)$
3	0	8	$(1, \pm 3)$
4	1	80	$(-1, \pm 9)$
5	0	32	$(2, \pm 8)$
6	2	1600	$(-4, \pm 24)$
6	4	40000	$(20, \pm 1800)$
8	1	1280	$(4, \pm 48), (-4, \pm 16)$
8	3	3200	$(-4, \pm 176)$
8	5	800000	$(20, \pm 2000)$

Table 3.8: Rational solutions to $y^2 = x^5 + 2^\alpha 5^\beta$.

Conjecture 3.2.2. *Rational solutions to* $y^2 = x^5 - 2^\alpha 5^\beta$ *with integers* $0 \leq \alpha, \beta \leq 9$ *are given by*

1. *If* $\alpha, \beta \in 5\mathbb{Z}$, *then* $(x, y) = (2^{\alpha/5} 5^{\beta/5}, 0)$ *is a set of solutions.*
2. *In addition to the above solutions, we have solutions given by*

α	β	$2^\alpha 5^\beta$	(x, y)
0	4	625	$(5, \pm 50)$
1	3	250	$(11, \pm 401)$
2	2	100	$(5, \pm 55)$
2	4	2500	$(5, \pm 25)$
4	0	16	$(2, \pm 4)$
4	3	2000	$(6, \pm 76), (14, \pm 732)$
4	4	10000	$(10, \pm 300)$
4	8	6250000	$(25, \pm 1875), (50, \pm 17500)$
5	0	32	$(6, \pm 88)$

Table 3.9: Rational solutions to $y^2 = x^5 - 2^\alpha 5^\beta$.

Despite inabilities to prove these conjectures, we will be able to prove the following theorem about the integer solutions to the above curves.

Theorem 3.2.3. *All integer solutions to $y^2 = x^5 \pm 2^\alpha 5^\beta$ are given by taking the above integer solutions when ($0 \leq \alpha, \beta \leq 9$ and if $\alpha, \beta \geq 10$, additional integer solutions are given by translations via the following. Take $r_\alpha \equiv \alpha \pmod{10}$ for $r_\alpha \in \{0, 1, ..., 9\}$ and similarly for r_β. Then take any integer solution (x, y) for $C = 2^{r_\alpha} 5^{r_\beta}$ above and notice that*

$$(X, Y) := (x \cdot 2^{(\alpha - r_\alpha)/5} \cdot 5^{(\beta - r_\beta)/5}, y \cdot 2^{(\alpha - r_\alpha)/2} \cdot 5^{(\beta - r_\beta)/2})$$

is a solution to $Y^2 = X^5 \pm 2^\alpha 5^\beta$.

As a final note, notice that in all of the x-coordinates above, only the primes $2, 3, 5, 7$ and 11 divide the numerator of the x-coordinate of a solution to $y^2 = x^5 \pm 2^\alpha 5^\beta$.

To prove this theorem, we will use a myriad of techniques. The first of which is Chabauty's method. The key to Chabauty's method is to notice that the rational points on a hyperelliptic curve can be embedded into its Jacobian. It can be shown that the set of rational points on the Jacobian form a finitely generated abelian group known as the Mordell-Weil group. When one can show that the Mordell-Weil group has rank strictly less than the genus, then Chabauty's method can give us a way to determine the rational points on our curve. One can associate to the curve a p-adic power series and use Strassman's Theorem to give an upper bound on the number of p-adic solutions to the power series in terms of its coefficients. This corresponds to an upper bound on the number of rational solutions to the original equation and if the bound can be obtained, one can conclude that these are all the rational points on your curve. Given that the prime above can be any prime outside of a finite set, there are many such options one can use to find these upper bounds. In fact, one can also

use information at many different primes to also help obtain tight bounds on the number of solutions. For an excellent primer I refer the reader to [Mul06]. I will include some of the finer details missing from that excerpt here in this thesis as well as present Chabauty's method from the viewpoint of differentials as in [Col85]. For a different viewpoint see [CF96].

Let C be a hyperelliptic curve defined by

$$C : y^2 = f(x)$$

where $\text{disc}(f) \neq 0$ over a number field K. It does no harm for the reader to think of K as $\mathbb{Q}$ since that is where our main application will be.

An important concept for us will be the Jacobian of a hyperelliptic curve, denoted by J throughout. For an in depth discussion of the Jacobian, I refer the reader to the primer in [Mul06, Chapter 5]. For us, we will need a few crucial facts about the Jacobian that I will outline here. Firstly, if C/K is a curve and $C(K) \neq \emptyset$ then we have that

$$J(K) \cong \text{Div}^0(C/K)/\text{Prin}(C/K)$$

where the $\text{Div}^0(C/K)$ is the set of rational degree zero divisors and $\text{Prin}(C/K)$ is the set of principal divisors over C (elements corresponding to $\text{div}\,(f)$ for some $f \in k(C)^*$). In fact, one can define a map called the Abel-Jacobi map associated to $P_0 \in C(K)$ defined by

$$\begin{aligned} C &\to J \\ P &\mapsto [P - P_0]. \end{aligned}$$

The hyperelliptic curve has an invariant called the genus and is given by $g = \left\lfloor \frac{\deg(f)-1}{2} \right\rfloor$ [HS00, p.86-87] (this follows from the Riemann-Hurwitz formula [DS05, p.66]). Let Ω be the space of regular differentials. The Riemann-Roch Theorem [Sil09, p.35] states that this space is a K-vector space and has dimension g. In fact, a basis for this space, as shown in [DR11, p.55-56] can be given by

$$\left\{ \frac{dx}{y}, \frac{xdx}{y}, ..., \frac{x^{g-1}dx}{y} \right\}.$$

Further, letting p be an odd prime not dividing the discriminant of f, we have a bilinear pairing given by

$$\begin{aligned} \Omega \times J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ \langle \omega, \sum_i [P_i - Q_i] \rangle &\mapsto \sum_i \int_{Q_i}^{P_i} \omega. \end{aligned}$$

This pairing has the properties that it is $\mathbb{Q}_p$ linear on the left, $\mathbb{Z}$-linear on the right and that the kernel on the right is the torsion subgroup of $J(\mathbb{Q}_p)$ [Sik13]. The key assumption that the rank r of the Jacobian $J(\mathbb{Q}) \leq g-1$ will come into play in the following proposition.

Proposition 3.2.4. *With the notation as above and assuming that $r \leq g-1$, there exists a differential ω called an annihilating differential such that*

$$\langle \omega, D \rangle = 0$$

holds for all $D \in J(\mathbb{Q})$.

The proof of the above is relatively straightforward as well. Since the dimension of Ω is g and the rank of $J(\mathbb{Q}_p)$ is $g-1$, one can simply take each of the basis elements ω_g, take an arbitrary $\sum_{i=1}^{r} n_i R_i \in J(\mathbb{Q}_p)$ and solve the linear system created from these values. An explicit example of this method can be found in [MP12]. I will say a few words about this integral. These integrals above are called tiny integrals and can be evaluated like normal integrals. Use a power series representation to write $1/y$ subject to $y^2 = f(x)$ as an element of $\mathbb{Z}_p[[x]]$ and then integrate term by term substituting the endpoints into the x-coordinate by the Fundamental Theorem of Calculus. Fix some point say $P_0 \in C(\mathbb{Q})$. Then using the Abel-Jacobi map, we see that if another point $P \in C(\mathbb{Q})$ were to exist, then $[P - P_0] \in J(\mathbb{Q})$ implies that $\int_{P_0}^{P} \omega = 0$ where ω is an annihilating differential. The integral becomes a power series in $\mathbb{Z}_p[[x]]$ and thus our problem reduces to finding a root of a polynomial in this ring. At first glance this problem may seem harder, however a theorem of Strassman can help us.

Theorem 3.2.5. *(Strassman's Theorem) Suppose that*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}_p[[x]]$$

where $\mathbb{Z}_p$ is the p-adic integers. Further suppose that $\lim_{i \to \infty} a_i = 0$. Let $k = \min_i v_p(a_i)$ and let $N = \max\{i : v_p(a_i) = k\}$. Then the number of roots of $f(x)$ in $\mathbb{Z}_p$ is at most N.

The last ingredient in this method is to show that all known points form all the possible neighbourhoods where potential points on $C(\mathbb{Q})$ can live. This can be accomplished by a Mordell-Weil Sieve. Suppose that our curve $C/\mathbb{Q}$ has rank 1 and that $J(\mathbb{Q}) = \langle D \rangle$. Then with the Abel-Jacobi map, we have that if $P \in C(\mathbb{Q})$, then $[P - P_0] = nD$ for any fixed P_0. We would like to know what possible values of n there are. Use the known points of $C(\mathbb{Q})$ to give an initial set of these n values and then for different values of p, compute the order of the reduced divisor $\bar{D} \in J(\mathbb{F}_p)$. Doing this for multiple values of p can help narrow the possible values of n and these can be translated to find a small collection of neighbourhoods where points of $C(\mathbb{Q})$ can live. When we can show that all points must live in the neighbourhoods

as discovered from Chabauty's method, we are done after including possible torsion points of $J(\mathbb{Q})$.

With the above approach in mind, I will divide our curves into groups of curves with rank 0, 1, ≥ 2 and those whose rank we cannot determine. The strategy for determining the Mordell-Weil rank of Jacobians is to use descent arguments to get an upper bound on the rank and then attempt to find linearly independent points on the Jacobian to establish this rank. There is no currently known algorithm to compute this number exactly and this fact causes many problems for us in determining the exact structure of these Mordell-Weil groups.

Case 1: Known rank 0 curves

Of the 100 cases of curves with a positive sign, there are 36 which can by proven to have rank exactly 0. These correspond to

$$\begin{aligned}(\alpha,\beta) \in \{&(0,0),(0,2),(0,3),(0,5),(0,7),(0,8),(1,3),(1,8),(2,2),(2,3),(2,7),(2,8),(3,2),\\ &(3,3),(3,7),(3,8),(4,0),(4,2),(4,5),(4,7),(5,2),(5,7),(6,0),(6,3),(6,5),(6,8),\\ &(7,2),(7,7),(8,0),(8,4),(8,5),(8,9),(9,0),(9,2),(9,5),(9,7)\}\end{aligned}$$

and with a negative sign, we see that there are 28 cases given by

$$\begin{aligned}(\alpha,\beta) \in \{&(1,0),(1,5),(2,0),(2,1),(2,5),(2,6),(3,2),(3,3),(3,7),(3,8),(4,1),(4,6),(5,2),\\ &(5,7),(6,1),(6,4),(6,6),(6,9),(7,2),(7,7),(8,0),(8,4),(8,5),(8,9),(9,0),(9,2),\\ &(9,5),(9,7)\}.\end{aligned}$$

Of these curves, we can run the commands for each (α,β) in the above list

```
_<x> := PolynomialRing(Rationals());
C := HyperellipticCurve(x^5+2^a * 5^b);
Chabauty0(Jacobian(C));
```

and find that rational points occur on the following curves in the positive case

α	β	$2^\alpha 5^\beta$	(x, y)
0	0	1	$(-1, 0)$
0	0	1	$(0, \pm 1)$
0	2	25	$(0, \pm 5)$
0	5	3125	$(-5, 0)$
0	8	390625	$(0, \pm 625)$
2	2	100	$(0, \pm 10)$
2	8	1562500	$(0, \pm 1250)$
4	0	16	$(0, \pm 4)$
4	2	400	$(0, \pm 20)$
6	0	64	$(0, \pm 8)$
6	8	25000000	$(0, \pm 5000)$
8	0	256	$(0, \pm 16)$
8	4	160000	$(0, \pm 400)$
8	5	800000	$(20, \pm 2000)$

Table 3.10: Rational solutions to $y^2 = x^5 + 2^\alpha 5^\beta$ for rank 0 curves

and in the negative case none of the curves have any rational points other than the point at infinity.

Case 2: Known rank 1 curves

In this case, we discuss the situation where we know the generator of a curve with rank 1. The following list of coordinates give rise to such curves in the positive sign case

$$(\alpha, \beta) \in \{(0,1), (0,4), (1,1), (1,4), (1,6), (2,0), (2,1), (2,4), (2,5), (3,0), (3,1), (3,4), (4,1), (4,4), (5,0), (5,1), (5,4), (6,1), (6,4), (7,0), (7,1), (7,4), (8,2), (8,3), (9,1)\}$$

and in the negative sign case, we have

$$(\alpha, \beta) \in \{(0,0), (0,2), (1,4), (2,2), (3,0), (3,1), (4,0), (4,2), (5,0), (5,1), (6,0), (6,2), (8,2)\}.$$

There are also curves where the computation for the given model of our hyperelliptic curves above go beyond what MAGMA can do. To handle these cases, we can change the model to use smaller coefficients and this helps limit the search space to something more manageable. There were six other cases in the positive sign setting given by

$$(\alpha, \beta) \in \{(0,6), (2,6), (3,5), (5,5), (7,5), (8,7)\}$$

and ten others in the negative sign setting given by

$$(\alpha, \beta) \in \{(0,5),(0,7),(0,8),(2,8),(4,7),(6,5),(7,0),(7,5),(8,8),(9,1)\}$$

where we can use the trick of changing the model to help us compute the Mordell-Weil group of the Jacobian by reducing the size of the coefficients involved. It will turn out that we can verify a generator in each of these cases as well.

To determine the Jacobian in these cases, we use MAGMA. To illustrate the methods used above, I will show them explicitly using the curves $y^2 = x^5 + 5$ and $y^2 = x^5 + 5^6$. To begin with the first curve, we set up the polynomial ring, the hyperelliptic curve and the Jacobian.

```
> _<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(x^5 + 5);
> J := Jacobian(C);
> J;
Jacobian of Hyperelliptic Curve defined by y^2 = x^5 + 5 over Rational Field
```

We would like to know what the rank of this Jacobian is and for this we can use "RankBounds".

```
> RankBounds(J);
1 1
```

There is also a command called "RankBound" which just gives the upper bound. From this we see that the lower and upper bounds of the Jacobian is indeed 1. Thus our curve has rank 1. Next, we search for rational point on our curve up to some bound. We use the LLL algorithm [LLL82] to help determine a basis of this group.

```
> ratPoints := RationalPoints(J:Bound:=5000);
> B := ReducedBasis(ratPoints);
> B;
[ (x + 1, 2, 1) ]
```

The point $P = (x + 1, 2, 1)$ is on the Jacobian and MAGMA suggests that this could be a possible generator. Remember that this point is in the Mumford representation (for more details, see [Mul06]). To determine if this is the generator, we need to check the following. Suppose that this was not the generator. Then there would be some point P_0 such that $P = mP_0$ for some integer m. However, this m is an integer at least of size 2 and so using

the canonical height of the Jacobian (denoted by $\hat{h}$) [HS00, p. 199] [Sto02b, Chapter 6], we see that

$$\hat{h}(P) = \hat{h}(mP_0) = m^2\hat{h}(P_0) \leq 4\hat{h}(P_0).$$

This gives us that $\hat{h}(P_0) \leq \frac{1}{4}\hat{h}(P)$ which in turn gives us a way to bound how far we need to check for rational points. The command RationalPoints(J:Bound:=N) will look for rational points up to naive height N on the associated Kummer Surface to our Jacobian (for more details, see [CF96]). We can compute the maximum difference between the canonical height and naive height using MAGMA and thus, to verify the bound, we need to check for rational points up to the bound

$$\exp\left(\frac{\hat{h}(P)}{4} + HC\right)$$

where HC is the height constant, this maximal height difference between canonical and naive heights. For more details see [Sto99] [Sto02b]. Computing gives us that

```
> P := B[1];
> HC := HeightConstant(J:Effort:=2);
> hP := Height(P);
> boundToCheck := Exp(hP/4 + HC);
> boundToCheck;
11.199450436960278217068726 4455
```

As we have already checked up to 5000, we have successfully determined that P is a generator. In some cases, the computations are too large to be performed. For example, consider the curve $y^2 = x^5 + 5^6$:

```
> C1 := HyperellipticCurve(x^5 + 5^6);
> J1 := Jacobian(C1);
> ratPoints1 := RationalPoints(J1:Bound:=15000);
> B1 := ReducedBasis(ratPoints1);
> B1;
[ (x^2 - 105/16*x - 525/16, 2205/64*x - 575/64, 2) ]
> HC1 := HeightConstant(J1:Effort:=2);
> hPoint := Height(B1[1]);
> Exp(hPoint/4+HC1);
57732.571188196237992879296620 9
```

This computation just exceeds what MAGMA can do (the max bound rational points will allow is 46340). We can reduce our model and perform this computation again. MAGMA has a command that will give us a smaller model (though this is not an exact science - sometimes other models can do better).

```
> C2, mapC1toC2 := ReducedMinimalWeierstrassModel(C1);
> C2;
Hyperelliptic Curve defined by y^2 = 5*x^5 + 25 over Rational Field
> J2 := Jacobian(C2);
> ratPoints2 := RationalPoints(J2:Bound:=1000);
> B2 := ReducedBasis(ratPoints2);
> HC2 := HeightConstant(J2: Effort:=2);
> hPoint2 := Height(B2[1]);
> Exp(hPoint2/4+HC2);
595.98630637802534312831604667
```

This computation is manageable. In our specific setting, we can also find a different model by hand by using say $(x, y) \mapsto (2x, 2^2y)$ or $(x, y) \mapsto (5x, 5^2y)$ (or a combination of these maps) provided that the power of $\alpha, \beta \geq 4$.

Next, we can execute Chabauty's method on all these curves that we have computed a Mordell-Weil basis for their respective Jacobians and come up with the following set of solutions to the curves $y^2 = x^5 \pm 2^\alpha 5^\beta$. To use the following command, we need to tell MAGMA which prime specifically to check. This method returns the number of points that are roots of the equation over $\mathbb{Z}_p[[x]]$ discussed earlier modulo a prime power of p and taking the cardinality of this set returns a bound on half the number of non-Weierstrass points. By definition, Weierstrass points are the points $(x, 0)$ and the point at infinity. We also need to check the torsion subgroup for any other points not coming from the free part of $J(\mathbb{Q})$. In our example $y^2 = x^5 + 5$, we have

```
// Recall C := HyperellipticCurve(x^5 + 5)
> RationalPoints(C:Bound:=1000000);
{@ (1 : 0 : 0), (-1 : -2 : 1), (-1 : 2 : 1) @}
> TorsionSubgroup(J);
Abelian Group of order 1
Mapping from: Abelian Group of order 1 to JacHyp:
J given by a rule [no inverse]
```

We can see that we do not have any points coming from the torsion subgroup and we only have one non-Weierstrass point given by $(-1, \pm 2)$. Since we know two non-Weierstrass points on our curve, we are done if our Chabauty method returns the value 1.

```
//Recall  P := B[1];
> #Chabauty(P,7);
2
```

```
> #Chabauty(P,11);
5
> #Chabauty(P,13);
1
```

We reach our bound using the prime $p = 13$. Thus we can conclude that the number of rational points on $y^2 = x^5 + 5$ is exactly 2 given by (-1 ± 2). We repeat this computation on all the curves $y^2 = x^5 + 2^\alpha 5^\beta$ that have rank 1 to illustrate this method. The column denoted by p denotes the prime used in Chabauty.

α	β	$C(\mathbb{Q})\backslash\infty$	p
0	1	$(-1, \pm 2)$	13
0	4	$(0, \pm 25)$	11
0	6	$(0, \pm 125)$	7
1	1	$(-1, \pm 3)$	11
1	4		11
1	6		11
2	0	$(0, \pm 2), (2, \pm 6)$	19
2	1		29
2	4	$(0, \pm 50), (5, \pm 75)$	61
2	5	$(5, \pm 125)$	19
2	6	$(0, \pm 250)$	11
3	0	$(1, \pm 3)$	13
3	1		11
3	4		31
3	5		17
4	1	$(1, \pm 9)$	19

α	β	$C(\mathbb{Q})\backslash\infty$	p
4	4	$(0, \pm 100)$	11
5	0	$(-2, 0), (2, \pm 8)$	109
5	1		17
5	4		19
5	5	$(-10, 0)$	11
6	1		17
6	4	$(0, \pm 200), (20, -1800)$	229
7	0		11
7	1		29
7	4		59
7	5		11
8	2	$(0, \pm 80)$	11
8	3	$(-4, \pm 176)$	11
8	7		17
9	1		19

Table 3.11: Rational points on $y^2 = x^5 + 2^\alpha 5^\beta$ for known rank 1 curves.

In the later versions of MAGMA, we can also perform Chabauty, the Mordell-Weil sieving and the torsion computation without explicitly giving the primes needed to check. This can be done using

```
> Chabauty(P); //Recall P is the generator of J.
{ (-1 : -2 : 1), (1 : 0 : 0), (-1 : 2 : 1) }
{ 3, 19, 29, 59, 79 }
[ 5, 2, 3, 2 ]
```

The first line is the list of rational points. The next two are Mordell-Weil sieving data which we will not discuss here. This helps to take care of ghost solutions as in [Mul06, p.191] and [BC06, p.63-92]. Using this command, we do likewise for the curve $y^2 = x^5 - 2^\alpha 5^\beta$ and see that

α	β	$C(\mathbb{Q})\backslash\infty$
0	0	$(1, 0)$
0	2	
0	5	$(5, 0)$
0	7	
0	8	
1	4	
2	2	$(5, \pm 55)$
2	8	
3	0	
3	1	
4	0	$(2, \pm 4)$
4	2	

α	β	$C(\mathbb{Q})\backslash\infty$
4	5	
4	7	
5	0	$(2, 0), (6, \pm 88)$
5	1	
6	0	
6	2	
6	5	
7	0	
7	5	
8	2	
8	8	
9	1	

Table 3.12: Rational points on $y^2 = x^5 - 2^\alpha 5^\beta$ for known rank 1 curves.

3.2.2 Elliptic Curve Chabauty

We now address the question of what happens when Chabauty's method cannot be applied either because the rank of $J(\mathbb{Q})$ is greater than 1 or because we cannot specifically compute the exact size of the rank. In this case, there are some more advanced techniques that one can try to use (see also [Mul06], [Sto98] and [Sto02a] for other tricks, but the ones mentioned there do not work here). The first of which is Elliptic Curve Chabauty. The idea behind this method is to pass our curves to a covering collection of curves that map down to elliptic curves over a relatively small number field K. Over this number field, we try to find all points where the x component is rational. These give a superset of all the rational points on our elliptic curve. One can then map these points back to the original curve and verify whether or not they are rational points for our original curve. For more details, see [Bru02] and [Bru03].

Our first step is to get this covering collection. A common way to do this is to use a

2-cover descent. The main idea here is to write our hyperelliiptic curve C/K as

$$C : y^2 = f(x) = g(x)h(x) = f_n \prod_{i=1}^{\deg(f)} (x - \theta_i)$$

where $h(x)$ is monic (for us it will be a monic linear term), $g(x)$ is of even degree and $g(x), h(x) \in L[x]$ for some finite extension L of K and f_n is the coefficient of x^n in $f(x)$. For our applications here our $f(x)$ is a degree five monic polynomial and so we make this simplifying assumption. For more details on any of these methods in full generality, the reader is encouraged to see [BS08], [BS09] and [BS10].

Define $H_K := \{\delta \in A^*/A^{*2} : N_{A/K}(\delta) \in k^{*2}\}$ where $A = K[x]/f(x) = K[\theta]$ for $\theta = \theta_1$. For $\delta \in H_K$, we can write down the cover given by

$$D_\delta = \begin{cases} y_1^2 & = \delta_1(x - \theta_1) \\ & \vdots \\ y_5^2 & = \delta_5(x - \theta_5) \\ y & = y_1 ... y_5 \\ 1 & = \delta_1 ... \delta_5 \end{cases}$$

where here we are thinking of $\delta_1, ..., \delta_5$ as conjugates of δ and hence we think of $y_1, ..., y_5$ as conjugates as well. Condensing the above map and relabeling gives

$$E_\gamma : \gamma y_1^2 = g(x)$$
$$E_\gamma' : (1/\gamma) y_2^2 = h(x)$$

where this γ is associated to the δ from above as follows. Suppose that $\delta \in A$ and let $L[\Theta] = L[x]/h(x)$. Define the map

$$j : A \to L[\Theta]$$
$$\theta \mapsto \Theta$$

and extend the above map in the natural way. Then, we have that $\gamma = N_{L[\Theta]/L}(j(\delta))$. Denote this γ by $\gamma(\delta)$ to remind ourselves of the association. The question now arises "How many of these such δ (and consequently $\gamma(\delta)$) values do we have to consider?" The smallest such set we can hope to obtain by purely local means is given by the fake 2-Selmer group. This is

defined as follows. The map from $A \to A \otimes_K K_v$ gives a commutative diagram

$$\begin{array}{ccc} C(K) & \xrightarrow{\mu_K} & H_K \\ \downarrow & & \downarrow \rho_{K_v} \\ C(K_v) & \xrightarrow[\mu_{K_v}]{} & H_{K_v} \end{array}$$

From here, we define the fake 2-Selmer group as

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C/K) = \{\delta \in H_K : \rho_{K_v} \in \mu_{K_v}(C(K_v)) \text{ for all places } v \in K\}.$$

This group was first introduced by Poonen and Schaefer [PS97]. It is related to the Selmer group by being equal to a quotient of the Selmer group. For more details on this, see [SvL13]. With all this terminology now introduced, we can note that there is an algorithm for computing the fake 2-Selmer group and this has been implemented in MAGMA. Proceeding with the computation gives

```
> P<x> := PolynomialRing(Rationals());
< poly := x^5 + 2*5^5;
> C := HyperellipticCurve(poly);
> Hk,AtoHk := TwoCoverDescent(C);
> Hk := [d @@ AtoHk : d in Hk];
> Hk;
[
    1,
    -1/5*theta - 1
]
> K<w> := NumberField(poly);
> HK := [Evaluate(P!d, w) : d in Hk];
> HK;
[
    1,
    1/5*(-w - 5)
]
```

This means that every rational point on our curve C leads to a rational point with the same $\mathbb{Q}$-rational x-coordinate on one of the two genus 1 curves given by

$$E_1 : y^2 = g(x)$$
$$E_2 : y^2 = -1/5(w+5)g(x)$$

where $g(x) := \frac{x^5+2\cdot 5^5}{x-w}$. We load this now into MAGMA

```
> PK<X> := PolynomialRing(K);
> g := ExactQuotient(Evaluate(PK!poly,X), X - w);
```

We will run Elliptic Curve Chabauty on each elliptic curve. To do this, we iterate over all values of "HK" and use MAGMA's built-in capabilities. First we set up our elliptic curve.

```
> for d in HK do
for> C2 := HyperellipticCurve(d*g);
for> E, mE := EllipticCurve(C2, RationalPoints(C2:Bound:=20)[1]);
```

Here we might need some user intervention depending on if we cannot find any small rational points. If you know a rational point on the curve, for example infinity when $d = 1$ and $x = 15$ when $d = -1/5(w + 5)$, then you can use the command

```
for> Rep(Points(C2, Infinity()))
```

instead of searching for rational points. With the elliptic curve built, we can now attempt to compute the rank. This command can take a bit of time depending on the curve. For the purposes of showing sample output, I will assume that $d = -1/5(w + 5)$ and that we use the point at $x = 15$.

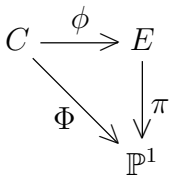
```
for> E, mE := EllipticCurve(C2, Rep(Points(C2, 15)));
for> bounds, gens := MordellWeilShaInformation(E);
for> end for;


Torsion Subgroup = Z/2
The 2-Selmer group has rank 3
Found a point of infinite order.
Found 2 independent points.
After 2-descent:
    2 <= Rank(E) <= 2
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)
```

It is here that we should note we need the rank above to be exact. If we cannot compute the exact rank of E then we cannot guarantee that the next steps are valid. Here we know $\text{rank}(E) = 2$ and so we can continue to apply Elliptic Curve Chabauty since this rank is less than the degree of the number field extension (which is 5). Next, we set up an abstract representation of the Mordell-Weil group of E.

```
> T, mapTtoE := TorsionSubgroup(E);
> A := AbelianGroup(Invariants(T) cat [0 : g in gens]);
> gensE := [mapTtoE(T.j) : j in [1..Ngens(T)]] cat gens;
> MWmap := map<A -> E | a :-> &+[e[i]*gensE[i] : i in [1..#e]]
    where e := Eltseq(a)>;
> MWmap;
Mapping from: GrpAb: A to CrvEll: E given by a rule [no inverse]
```

Some notes on the above code. The code "T.j" refers to the elements of T (and in particular the generators). The symbols "& +" will take the map on each of the generators and put them together to form an element in E. Elliptic Curve Chabauty requires a representation of the Mordell-Weil group and a map from E to $\mathbb{P}^1$. The major idea is the following. Let C/K be an algebraic curve where K is a number field. Suppose that C covers an elliptic curve E defined over L where L is a finite extension of K. Next, consider following commutative diagram



where Φ is defined over K and ϕ, π are defined over L. The map ϕ is the aforementioned cover of E. From this map, we can see that

$$\Phi(C(K)) \subseteq \phi(E(L)) \cap \mathbb{P}^1(K)$$

The right most set can sometimes be bounded using p-adic methods. One such situation is when $\text{rank}(E) \leq [L : K]$. The details of this method can be found in [Bru02] and [Bru03]. If the bound is sharp, then we have found all rational points on C. For our purposes, MAGMA has the built in functionality and so we will not go into the details. We compute the necessary values as follows.

```
> P1 := ProjectiveSpace(Rationals(), 1);
> piC2toP1 := map<C2 -> P1 | [FunctionField(C2).1,1]>;
> piE := Inverse(mE)*piC2toP1;
> set, n := Chabauty(MW, piE);
> set, n;
{
    0,
    $.1 + $.2 - $.3,
    $.1 + $.2 - 3*$.3,
```

```
    -2*$.3
}
396902628105984000
```

Lastly, we need to verify that the output is valid. This is the case if the index of A in $E(K)$ is finite and coprime to n as computed in the above code. This can be done using the "Saturation" command.

```
> primes := PrimeDivisors(n);
> p := 1;
> omitPrimes := [];
> while(p lt (Max(primes)+1)) do
while> p := NextPrime(p);
while> if not(p in primes) then
while|if> omitPrimes := Append(omitPrimes,p);
while|if> end if;
while> end while;
> sat := Saturation(gens, Max(primes) :
    TorsionFree, OmitPrimes := omitPrimes);
> sat eq gens;
True
```

The "Saturation" command takes in rational points on E and an integer n and returns a sequence of points generating a subgroup of $E(\mathbb{Q})$ such that the given points are contained in the subgroup and that the subgroup is p-saturated for all primes p up to n excluding those given by the optional "OmitPrimes" parameter. Recall that a subgroup S is p-saturated in a group G if there is no intermediate subgroup H for which the index in S is finite and divisible by p. This is the exact condition we wish to verify. If "TorsionFree" is specified above to be true, then the torsion points are omitted from the result. Checking this to be equal to the generators is enough.

If this last check of equality with the generators turns out to be false, then use the saturated group in place of the original generators (in our case given by "gens") and repeat the computation. Check that the new second value does not have new prime divisors or else repeat the saturation step with the new primes and loop until you get an equality.

Translating back to the curve C, we see that the rational points on C corresponding to $d = -1/5(w + 5)$ are given by

```
> xCoords := {piE(MW(s)) : s in set};
> ptsOnC := &join{Points(C, pt[2] eq 0 select Infinity() else pt[1]/pt[2]) :
```

```
pt in xCoords};
> xCoords; ptsOnC;
{ (15 : 1), (-5 : 1) }
{@ (15 : 875 : 1), (15 : -875 : 1) @}
```

We can repeat this[1] for the point $d = 1$ and see that

$$C(\mathbb{Q}) = \{\infty, (15, -875), (15, 875), (-15/4, -2375/32), (-15, 2375/32)\}.$$

We can run this method on the remaining curves and we can verify the rational points on $y^2 = x^5 \pm 2^\alpha 5^\beta$ for the curves

α	β	$\pm$	$2^\alpha 5^\beta$	(x, y)
0	1	$-$	5	None
0	3	$-$	125	None
0	4	$-$	625	$(5, \pm 50)$
0	6	$-$	15625	None
0	9	$+$	1953125	None
0	9	$-$	1953125	None
1	5	$+$	6250	$(15, \pm 875)$, $(\frac{-15}{4}, \pm\frac{2375}{32})$
2	9	$+$	7812500	None
3	5	$-$	25000	None
5	3	$+$	4000	None
5	3	$-$	4000	None
5	4	$-$	20000	None
5	6	$+$	500000	None

α	β	$\pm$	$2^\alpha 5^\beta$	(x, y)
5	6	$-$	500000	None
5	8	$+$	12500000	None
5	8	$-$	12500000	None
5	9	$+$	62500000	None
5	9	$-$	62500000	None
6	6	$+$	1000000	None
8	3	$-$	32000	None
8	7	$+$	20000000	None
8	7	$-$	20000000	None
8	8	$-$	100000000	None
9	4	$+$	320000	None
9	4	$-$	320000	None
9	6	$+$	8000000	None

Table 3.13: Rational solutions to $y^2 = x^5 \pm 2^\alpha 5^\beta$ solved using Elliptic Curve Chabauty.

3.2.3 S-integer Points

Yet another technique we can attempt to use is that of finding S-integer points on hyperelliptic curves based on [GR11] and [BMS+08]. Currently, the code is not yet fully implemented in MAGMA. In lieu of applying this method by hand, we note that the calculation is made substantially easier if one already knows the Mordell-Weil group exactly and so I will give some examples of how one verifies this in practice for higher ranked curves.

[1] In reality, we get an error in this case caused by a MAGMA programming error. However in the version I used, we can use a different model of our curve using the command "MinimalReducedWeierstrassModel(C)" and come up with the other two points in the same manner.

Contrary to the rank 1 case where we could do a simple computation involving the height constant and one fourth the value of the presumed generator, when we consider ranks 2 or higher we need to use more sophisticated machinery [Sto02b]. The main idea here is to compute a value called the covering radius ϱ (or at least an upper bound on it). Once we have this value, we use an upper bound similar to that in the rank 1 case to check that there are no more rational points on the Jacobian of naive height at most

$$\exp\left(\varrho^2 + HC\right)$$

where again HC is the height constant. We illustrate this method using the curves $y^2 = x^5 - 2^4 5^3$ and $y^2 = x^5 - 2^4 5^9$. First we proceed with the second curve which has rank 2 as given by

```
> _<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(x^5 - 2^4*5^9);
> C1, mapCtoC1 := ReducedMinimalWeierstrassModel(C); C1;
Hyperelliptic Curve defined by y^2 = -5*x^6 + 50*x over Rational Field
> J1 := Jacobian(C1);
> B := ReducedBasis(RationalPoints(Jacobian(C1):Bound:=8000));
> B;
[ (x^2 + x + 18/7, 9/7*x + 12/7, 2),
    (x^2 + 17/3*x + 32/3, 1/9*x + 712/9, 2) ]
```

Then to compute the covering radius, we use the formula found in [Sto02b, p. 178] as given by

$$\varrho^2 = \frac{\hat{h}(P_1)\hat{h}(P_2)\hat{h}(P_1 \pm P_2)}{4\mathrm{Reg}(P_1, P_2)}$$

where Reg denotes the regulator and the sign above is chosen to give the smaller value of $\hat{h}(P_1 \pm P_2)$. If we use the height pairing matrix $M = (\langle P_i, P_j \rangle)_{1 \le i,j \le 2}$ where

$$\langle P_i, P_j \rangle = \frac{\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2)}{2}$$

we can also see that

$$\varrho^2 = \frac{\langle P_1, P_1 \rangle \langle P_2, P_2 \rangle (\langle P_1, P_1 \rangle + \langle P_2, P_2 \rangle + 2|\langle P_1, P_2 \rangle|)}{4 \det(M)}$$

valid since $\hat{h}(P_1 + P_2) - \hat{h}(P_1 - P_2) = 2(\hat{h}(P_1) + \hat{h}(P_2))$. This gives

```
> H1 := HeightPairingMatrix(B);
> H1;
```

```
[5.702031324165132672505938145 58 0.607244504928574524217534640890]
[0.607244504928574524217534640890 8.219599880703018591771463200 80]
> rsq := H1[1,1]*H1[2,2]*(H1[1,1]+H1[2,2]-2*Abs(H1[1,2])
/(4*Determinant(H1));
> rsq;
3.201977697600176347378944785 8
> HC := HeightConstant(J1 : Effort := 2);
> Exp(HC + rsq);
7604.25353647160094586160852567
```

This confirms that our generators for $J(\mathbb{Q})$ are given by

$$(x^2 + x + 18/7, 9x/7 + 12/7, 2), (x^2 + 17x/3 + 32/3, x/9 + 712/9, 2).$$

If we pull back, we see that the generators are

```
> C5 := HyperellipticCurve(x^5 - 2^4*5^9);
> C10, mapping := ReducedMinimalWeierstrassModel(C5);
> basOrig := [Pullback(mapping,b) : b in B];
> basOrig;
[ (x^2 - 175/9*x + 8750/9, 1225/27*x - 16250/27, 2),
    (x^2 - 425/16*x + 1875/8, -47525/64*x + 314375/32, 2) ]
```

With rank 3 and higher, there is no exact formula like in the $r = 2$ case. However MAGMA is still capable of computing this. We perform this computation for our only rank 3 curve given by $y^2 = x^5 - 2^4 5^3$. As always, we produce potential candidates for our generators.

```
> _<x> := PolynomialRing(Rationals());
> C2 := HyperellipticCurve(x^5 - 2^4*5^3);
> C3, mapC2toC3 := ReducedMinimalWeierstrassModel(C2); C3;
Hyperelliptic Curve defined by y^2 = 2*x^5 - 125 over Rational Field
> J3 := Jacobian(C3);
//Can take a while
> B3 := ReducedBasis(RationalPoints(Jacobian(C3):Bound:=24500));
> B3;
 [(x - 3, 19, 1), (x - 7, 183, 1), (x^2 + 1/2*x + 3/2, 19/2*x + 5/2, 2) ]
```

Next, we compute the covering radius. This is done by using the height pairing matrix as before, creating a lattice from the matrix and then computing the covering radius.

```
> H3 := HeightPairingMatrix(B3);
```

```
> L3 := LatticeWithGram(H3);
> r3 := CoveringRadius(L3);
Runtime error in 'CoveringRadius': Argument 1 must be over Z or Q
```

The problem with this code is that the height pairing matrix is over a real field of precision 30. In order to compute the covering radius, we must tell MAGMA to think of "H3" as a rational matrix. To do this, we truncate the entries at a few different values for n and then we compute the covering radius. Note that the command "CoveringRadius" runs in time approximately factorial in the size of the matrix and so is really only feasible for small values of the size of the matrix.

```
> seq := [];
> n := 8; //Vary for precision
>for a in [1,2,3] do
> for b in [1,2,3] do
//Trick to round values multiply by power of 10, floor, then divide.
>  seq := Append(seq,Floor((10^n)*H[a][b])/10^n);
> end for;
>end for;
> H3 := Matrix(RationalField(),3,3,seq);
> L3 := LatticeWithGram(H3);
> r3 := CoveringRadius(L3);
> r3;
2.27285021881299
```

If we vary the n values from say 1 to 10, we can see that $\varrho^2 \leq 2.3$. This gives

```
> HC := HeightConstant(Jacobian(C):Effort:=2);
> Exp(2.3^2 + HC);
24116.31544471309173573622204 27
```

and we have already verified past this bound so our basis is given by

$$(x-3, 19, 1), (x-7, 183, 1), (x^2 + x/2 + 3/2, 19x/2 + 5/2, 2).$$

Now that one has these points, one could in principle use the techniques of [GR11] to find the S-integral points on this curve. In order to use this technique, one need only two more facts, namely a bound on the number of S-integral points of the curve and a variant of the Mordell-Weil Sieve capable of searching up to the bounds. I will not do this here because the Mordell-Weil Sieving code still requires some in depth user knowledge before executing

properly which the author has yet to obtain. I will however state that there is no reason that this technique could not be done if the user had enough knowledge of the code (or enough time to write his or her own). We will see in the section on Thue-Mahler equations that work has already been done to classify the integer points on these two curves and that will be enough for our purposes.

3.2.4 Other Techniques

We can also use elliptic curves in the rare case that the polynomial on the right factors. For example, for

$$y^2 = x^5 - 2^5 5^5 = (x - 10)(x^4 + 10x^3 + 100x^2 + 1000x + 10000),$$

we have that the factors on the right are coprime and hence we can use techniques for finding $\{2, 5\infty\}$-integral points on the elliptic curve

$$y^2 = x^4 + 10x^3 + 100x^2 + 1000x + 10000.$$

We use MAGMA via the command

```
//The following command includes integral points
> SIntegralQuarticPoints([1,10,100,1000,10000], [2,5]);
[
    [ 30, -1100 ],
    [ -10, -100 ],
    [ -55/4, 2525/16 ],
    [ 0, 100 ]
]
```

A quick check shows that none of these points leads to a $\{2, 5, \infty\}$-integer point on $y^2 = x^5 - 2^5 5^5$. Thus the only such point must come when $y = 0$ and hence $x = 10$. This gives us that the only $\{2, 5\}$-integer points on this curve is the point $(x, y) = (10, 0)$.

3.2.5 Integer Points Via Thue-Mahler Equations

When the previous methods fail one can always try to simplify the search by trying to find integer solutions to your equations. The goal of this section is to compute integer solutions to $y^2 = x^5 \pm 2^\alpha 5^\beta$ with $\alpha, \beta \geq 0$. Our primary tools will be techniques from algebraic number theory as well as reductions to Thue-Mahler equations, that is, equations of the form

$$f(x, y) = cp_1^{z_1} ... p_n^{z_n}$$

where $f(x, y)$ is an irreducible binary form in $\mathbb{Z}[x, y]$ of degree at least 3. From here, we apply an algorithm of [TdW92] as implemented by [Ham11] to solve these equations. Throughout we assume that $xy \neq 0$ as these solutions are easy to obtain. In this case, we know that the greatest common divisor of x and y has only powers of 2 and 5. Thus, removing all the powers of 2 and 5 in x and y, let

$$y = 2^{y_1}5^{y_2}\hat{y}$$
$$x = 2^{x_1}5^{x_2}\hat{x}.$$

Plugging this into our equation, we have

$$2^{2y_1}5^{2y_2}\hat{y}^2 = 2^{5x_1}5^{5x_2}\hat{x}^5 \pm 2^A5^B.$$

Notice that two of the powers of 2 must be equal and the third must be a larger power of the smaller two. This leads to the following cases:

1. $2y_1 = 5x_1$ and $2y_2 = 5x_2$
2. $2y_1 = 5x_1$ and $2y_2 = B$
3. $2y_1 = 5x_1$ and $5x_2 = B$
4. $2y_1 = A$ and $2y_2 = 5x_2$
5. $2y_1 = A$ and $2y_2 = B$
6. $2y_1 = A$ and $5x_2 = B$
7. $5x_1 = A$ and $2y_2 = 5x_2$
8. $5x_1 = A$ and $2y_2 = B$
9. $5x_1 = A$ and $5x_2 = B$.

We proceed case by case. Note in all the cases below, the class number is coprime to 5 and so factoring in the ring of integers will be permitted.

1. $2y_1 = 5x_1$ and $2y_2 = 5x_2$.

   This case is equivalent to $\gcd(x, y) = 1$. For the duration of this case, to easy notation, we suppose that we have a solution to $y^2 = x^5 \pm 2^\alpha 5^\beta$ with $\gcd(x, y) = 1$. The work for the equation with a negative sign has been done as a consequence of the following.

   Theorem 3.2.6. *[GLT08] (Goins, Luca, Togbe) The only solutions to $y^2 = x^5 - 2^\alpha 5^\beta$ for $\gcd(x, y) = 1$ and α, β non-negative integers are given by $(x, y, \alpha, \beta) = (11, \pm 401, 1, 3)$ or $(x, y, \alpha, \beta) = (1, 0, 0, 0)$.*

This was done using work on Lucas sequences and S-integral points on elliptic curves. For the rest of this section, we attempt to apply a myriad of techniques to the equation $y^2 = x^5 + 2^\alpha 5^\beta$ with $\gcd(x, y) = 1$ to come up with a full solution set to the above problem. We attempt to solve this first by factoring.

Case 1: Suppose that $\alpha = 2a$ and $\beta = 2b$ for some non-negative integers a and b. Then we have $(y - 2^a 5^b)(y + 2^a 5^b) = x^5$. Now, let $d = \gcd(y - 2^a 5^b, y + 2^a 5^b)$. Adding the two values shows that $d \mid 2y$. Now if $d \mid y$, then $d \mid 2^\alpha 5^\beta$ and so $d \mid x$, contradicting the coprimality of x and y. If $d = 2$ then we know that $2 \nmid y$ from the above argument and so we must have that $a = 0$ when $d = 2$. The argument to follow only works when $d = 1$ and so we assume that $a \neq 0$. The case where $a = 0$ was solved earlier using Chabauty's method. Unique factorization tells us that

$$y - 2^a 5^b = M^5 \qquad \text{and} \qquad y + 2^a 5^b = N^5$$

and so subtracting gives $N^5 + (-M)^5 = 2^a 5^b$. Using Theorem 1.6.2 (valid since the right hand side is a square), we have that the only solution to $x^5 + y^5 = Cz^2$ for $C \in \{1, 2, 5, 10\}$ with $x > y$ is given by $C = 2$ and $(n, x, y, z) = (5, 3, -1, \pm 11)$. Since here z is a power of 2 and 5 in our situation, we have a contradiction. Summarizing gives

Lemma 3.2.7. *There are no solutions to $y^2 = x^5 + 2^\alpha 5^\beta$ with α, β even non-negative integers with $\alpha > 0$ and x, y coprime integers.*

This technique worked because we could factor in a unique factorization domain. We now attempt to try this over the ring $\mathbb{Z}(\sqrt{2})$ which is also a unique factorization domain.

Case 2: We assume now that $\alpha = 2a + 1$ and $\beta = 2b$. Performing a factorization in $\mathbb{Z}[\sqrt{2}]$ gives us $(y - 2^a 5^b \sqrt{2})(y + 2^a 5^b \sqrt{2}) = x^5$. Again, let $d = \gcd(y - 2^a 5^b \sqrt{2}, y + 2^a 5^b \sqrt{2})$ for $d \in \mathbb{Z}[\sqrt{2}]$. Adding the two values shows that $d \mid 2y$. Now if $d \mid y$, then $d \mid 2^\alpha 5^\beta$ and so $d \mid x$ thus $d = 1$. If $d = 2$ then as $d \mid 2^a 5^b \sqrt{2}$, we have that $d \mid y$ and the above again shows that $d \mid x$, a contradiction. Unique factorization tells us that

$$y + 2^a 5^b \sqrt{2} = (1 + \sqrt{2})^k (m + n\sqrt{2})^5 \tag{3.1}$$

where $m, n \in \mathbb{Z}$, $1 + \sqrt{2}$ is a fundamental unit for $\mathbb{Z}[\sqrt{2}]$ and we have absorbed roots of unity into the 5th power. We may suppose without loss of generality that $0 \leq k \leq 4$ since we can absorb all the 5th powers into the $(m + n\sqrt{2})^5$ term if necessary. Using the first equation above, we can expand and compare coefficients of $\sqrt{2}$ to get a set of

equations for each value of k given by $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ given by

$$\begin{aligned}
k=0 \qquad & f_0(m,n) := n(5m^4 + 20m^2n^2 + 4n^4) \\
k=1 \qquad & f_1(m,n) := m^5 + 5m^4n + 20m^3n^2 + 20m^2n^3 + 20mn^4 + 4n^5 \\
k=2 \qquad & f_2(m,n) := 2m^5 + 15m^4n + 40m^3n^2 + 60m^2n^3 + 40mn^4 + 12n^5 \\
k=3 \qquad & f_3(m,n) := 5m^5 + 35m^4n + 100m^3n^2 + 140m^2n^3 + 100mn^4 + 28n^5 \\
k=4 \qquad & f_4(m,n) := 12m^5 + 85m^4n + 240m^3n^2 + 340m^2n^3 + 240mn^4 + 68n^5.
\end{aligned}$$

To solve this, we use the Thue-Mahler solver. The program takes as an input an irreducible binary form of degree at least 3, a parameter and a set of primes given by a tuple $([c_0, ..., c_n], [p_1, ..., p_k], A)$ where

$$c_0X^N + c_1X^{N-1}Y + ... + c_NY^N = \pm Ap_1^{\delta_1} \cdots p_k^{\delta_k}$$

and outputs coprime integers X, Y with $\gcd(c_0, Y) = 1$ satisfying the above equation. First, let's see why solving for solutions with $\gcd(X, Y) = 1$ is not an issue. Notice that for a solution (m_0, n_0) to our Thue-Mahler equation above implies that $\gcd(m_0, n_0) \mid y$ by Equation 3.1. As $\gcd(m_0, n_0) \mid 2^a5^b$, we must also have that $\gcd(m_0, n_0) \mid x$ as well. So $\gcd(m_0, n_0) \mid \gcd(x, y) = 1$ showing that $\gcd(m_0, n_0) = 1$ since we assumed that x and y were coprime. Thus solving the Thue-Mahler equation for coprime m and n is sufficient.

For our purposes, the restriction that $\gcd(c_0, Y) = 1$ is unwanted so to deal with this, we solve the following set of related Thue-Mahler equations $g_j(m,n) = \pm 2^{\delta_1}5^{\delta_2}$ where $g_j(m,n)$ are given by [Ham11, p.6]

$$\begin{aligned}
k=0 \qquad & g_1(m,n) := 5m^4 + 20m^2n^2 + 4n^4 \\
k=0 \qquad & g_2(m,n) := m^4 + 100m^2n^2 + 500n^2 \\
k=1 \qquad & g_3(m,n) := m^5 + 5m^4n + 20m^3n^2 + 20m^2n^3 + 20mn^4 + 4n^5 \\
k=2 \qquad & g_4(m,n) := 2m^5 + 15m^4n + 40m^3n^2 + 60m^2n^3 + 40mn^4 + 12n^5 \\
k=2 \qquad & g_5(m,n) := m^5 + 15m^4n + 80m^3n^2 + 240m^2n^3 + 320mn^4 + 192n^5 \\
k=3 \qquad & g_6(m,n) := 5m^5 + 35m^4n + 100m^3n^2 + 140m^2n^3 + 100mn^4 + 28n^5 \\
k=3 \qquad & g_7(m,n) := m^5 + 35m^4n + 500m^3n^2 + 3500m^2n^3 + 12500mn^4 + 17500n^5 \\
k=4 \qquad & g_8(m,n) := 12m^5 + 85m^4n + 240m^3n^2 + 340m^2n^3 + 240mn^4 + 68n^5 \\
k=4 \qquad & g_9(m,n) := 6m^5 + 85m^4n + 480m^3n^2 + 1360m^2n^3 + 1920mn^4 + 1088n^5 \\
k=4 \qquad & g_{10}(m,n) := 3m^5 + 85m^4n + 960m^3n^2 + 5440m^2n^3 + 15360mn^4 + 17408n^5.
\end{aligned}$$

To give an idea of the above collection and where they come from, take the case with $k = 0$ above. To go to the second $k = 0$ case, multiply every term by 5^3 and then relabel $m_{\text{new}} = 5m$. Each time you do this you will find solutions with $d \mid y$ where d is the base of the number we are multiplying by. For example, solving with $j = 9$ above, we see that we will find solutions to our original Thue-Mahler equation with $2 \mid n$ and solving with $j = 10$ above, we see that we will find solutions to our original Thue-Mahler equation with $4 \mid n$. Solving the above sets of equations gives the following solutions.

j	Solutions to $g_j(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$ in the form $(m, n, \delta_1, \delta_2)$
1	$(1,0,0,1), (-1,0,0,1)$
2	$(1,0,0,0), (-1,0,0,0)$
3	$(1,0,0,0), (-1,0,0,0)$
4	$(-1,1,0,1), (1,-1,0,1)$
5	$(-2,1,4,1), (2,-1,4,1), (1,0,0,0), (-1,0,0,0)$
6	$(-1,1,1,0), (1,-1,1,0)$
7	$(-1,0,0,0), (1,0,0,0), (-5,1,1,4), (5,-1,1,4)$
8	$(-1,1,0,0), (1,-1,0,0), (-2,1,2,0), (2,-1,2,0)$
9	$(2,-1,4,0), (-2,1,4,0), (-4,1,6,0), (4,-1,6,0)$
10	$(4,-1,8,0), (-4,1,8,0), (-8,1,10,0), (8,-1,10,0)$

Table 3.14: Solutions to $g_j(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m,0)$.

Notice that in the cases of $j = 4$ and $j = 6$ above, we get only one more additional solution to our original equation with $\gcd(c_0, Y) > 1$ and these come when $Y = 0$. To satisfy $\gcd(X,Y) = 1$, we have that only $(m,n) = (\pm 1, 0)$ are added solutions given from this reduction process. Our $k = 0$ situation above does not give us a valid solution since the coefficient of $\sqrt{2}$ on the left is nonzero. Thus our final list of solutions for $f_k(m,n) = 2^{\alpha} 5^{\beta}$ is as follows:

k	Solutions to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ in the form (m,n,δ_1,δ_2)	Corresponding (x,y,α,β)
0	None	None
1	$(1,0,0,0)$	$(-1,1,1,0)$
2	$(-1,1,0,1)$	$(-1,-7,1,2)$
2	$(1,0,0,0)$	$(1,3,3,0)$
3	$(1,-1,1,0)$	$(1,-3,3,0)$
3	$(1,0,0,0)$	$(-1,7,1,2)$
4	$(-1,1,0,0)$	$(-1,-1,1,0)$
4	$(-2,1,2,0)$	$(2,-8,5,0)$

Table 3.15: Solutions to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m,0)$.

To compute the last column above, we plug back in (m,n) into the Equation 3.1 and solve for the corresponding variables. Notice that the last solution, we obtain a solution with $\gcd(x,y) > 1$. Notice that finding solutions with $\gcd(m,n) = 1$ does not necessarily guarantee finding solutions with $\gcd(x,y) = 1$ but it does ensure that we find all such solutions with $\gcd(x,y) = 1$. Summarizing the above, we get the following

Lemma 3.2.8. *Solutions to $y^2 = x^5 + 2^\alpha 5^\beta$ with α, β non-negative integers with α odd and β even and x, y coprime integers are given by the following*

$$(x,y,\alpha,\beta) \in \{(-1,\pm 1,1,0),(-1,\pm 7,1,2),(1,\pm 3,3,0)\}$$

Case 3: We assume now that $\alpha = 2a$ and $\beta = 2b+1$. Notice that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain, however $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is. Performing a factorization in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ gives us $(y - 2^a5^b\sqrt{5})(y + 2^a5^b\sqrt{5}) = x^5$. Again, let $d = \gcd(y - 2^a5^b\sqrt{5}, y + 2^a5^b\sqrt{5})$ for $d \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Adding the two values shows that $d \mid 2y$. Now if $d \mid y$, then $d \mid 2^\alpha 5^\beta$ and so $d \mid x$ thus $d = 1$. If $d = 2$ then we know from above that $d \nmid y$ and so $\alpha = 0$ and y is odd. Thus x is even and modulo 8, we have that

$$y^2 = x^5 + 2^\alpha 5^\beta \equiv 0 + 5^{2b+1} \equiv 5 \pmod 8$$

which is a contradiction since odd squares modulo 8 are congruent to 1. Thus we have that $d = 1$ and so unique factorization tells us that

$$y + 2^a5^b\sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^k \left(\frac{m+n\sqrt{5}}{2}\right)^5 \tag{3.2}$$

where $m, n \in \mathbb{Z}$, $\frac{1+\sqrt{5}}{2}$ is a fundamental unit for $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and we have absorbed roots of unity into the 5th power. As before, we may suppose without loss of generality that $0 \leq k \leq 4$.

In contrast to the previous situation where we had leading coefficients that might have shared prime divisors with the n value, we do not have coefficients that are no longer necessarily integers. To simplify this we'll multiply through to eliminate the denominators (notice that our set of primes already contains 2 so this introduces no additional concerns). This can give us additional solutions depending on how big the power of 2 is. Evaluating the powers of the fundamental unit, we see that

$$\left\{\frac{1+\sqrt{5}}{2}\right\}_{k=0}^{k=4} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}, 2+\sqrt{5}, \frac{7+3\sqrt{5}}{2}\right\}.$$

From this, we see when $k = 0, 3$, then we can multiply by 2^5 to clear denominators and in the other three k cases, we multiply by 2^6 to clear denominators. This gives the following quintic forms $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ after expanding and comparing coefficients of $\sqrt{5}$.

$$\begin{aligned}
k=0 \qquad & g_0(m,n) := 2^5 f_0(m,n)/(5n) := m^4 + 10m^2n^2 + 5n^4 \\
k=1 \qquad & g_1(m,n) := 2^6 f_1(m,n) := m^5 + 5m^4n + 50m^3n^2 + 50m^2n^3 + 125mn^4 + 25n^5 \\
k=2 \qquad & g_2(m,n) := 2^6 f_2(m,n) := m^5 + 15m^4n + 50m^3n^2 + 150m^2n^3 + 125mn^4 + 75n^5 \\
k=3 \qquad & g_3(m,n) := 2^5 f_3(m,n) := m^5 + 10m^4n + 50m^3n^2 + 100m^2n^3 + 125mn^4 + 50n^5 \\
k=4 \qquad & g_4(m,n) := 2^6 f_4(m,n) := 3m^5 + 35m^4n + 150m^3n^2 + 350m^2n^3 \\
& \qquad\qquad\qquad\qquad + 375mn^4 + 175n^5.
\end{aligned}$$

Solving using the Thue-Mahler solver, we have

j	Solutions to $g_j(m,n) = \pm 2^{\delta_1}5^{\delta_2}$ in the form $(m, n, \delta_1, \delta_2)$
0	$(-1,0,0,1), (1,0,0,1), (1,-1,4,1), (-1,1,4,1), (1,1,4,1)(-1,-1,4,1)$
1	$(-1,0,0,0), (1,0,0,0), (0,1,0,2), (0,-1,0,2), (1,1,8,0), (-1,-1,8,0)$
2	$(-1,0,0,0), (1,0,0,0), (-1,1,6,0), (1,-1,6,0), (-5,1,7,2), (5,-1,7,2)$
3	$(-1,0,0,0), (1,0,0,0), (0,-1,1,2), (0,1,1,2)$
4	$(1,-1,5,0), (-1,1,5,0), (3,-1,8,0), (-3,1,8,0), (-5,1,5,2), (5,-1,5,2)$

Table 3.16: Solutions to $g_j(m,n) = \pm 2^{\delta_1}5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m,0)$.

Now, notice that in the $k = 0, 3$ cases, there are no solutions with the power of 2 at least 5. In the other three cases, there are solutions with the power of 2 at least 6 and the parity of m and n are the same. In these cases, we get two solutions given by

$$m + n\sqrt{5} \qquad \text{and} \qquad \frac{m + n\sqrt{5}}{2}$$

Call solutions relating to the first equation to be type 1 and those of the second type 2. This gives the following table of solutions.

k	Type	Sol'ns to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ of form $(m, n, \delta_1, \delta_2)$	Corresponding (x, y, α, β)
0	1	$(-1, 1, 4, 1)$	$(-4, -176, 8, 3)$
0	1	$(1, 1, 4, 1)$	$(-4, 176, 8, 3)$
1	1	$(1, 1, 8, 0)$	$(288, 4, 14, 1)$
1	2	$(1, 1, 8, 0)$	$(1, 9, 4, 1)$
2	1	$(-1, 1, 6, 0)$	$(-4, 64, 10, 1)$
2	2	$(-1, 1, 6, 0)$	$(-1, -2, 0, 1)$
2	1	$(-5, 1, 7, 2)$	$(20, -4000, 12, 5)$
2	2	$(-5, 1, 7, 2)$	$(5, -125, 2, 5)$
3	1	$(1, 0, 0, 0)$	$(-1, 2, 0, 1)$
3	1	$(0, 1, 1, 2)$	$(5, 125, 2, 5)$
4	1	$(-1, 1, 5, 0)$	$(-4, 16, 8, 1)$
4	1	$(-3, 1, 8, 0)$	$(4, 128, 14, 5)$
4	2	$(-3, 1, 8, 0)$	$(1, -9, 4, 1)$
4	1	$(-5, 1, 5, 2)$	$(20, 2000, 8, 5)$

Table 3.17: Solutions to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m, 0)$.

Lemma 3.2.9. *Solutions to $y^2 = x^5 + 2^\alpha 5^\beta$ with α, β non-negative integers with α even and β odd and x, y coprime integers are given by the following*

$$(x, y, \alpha, \beta) \in \{(-1, \pm 2, 0, 1), (-1, \pm 9, 4, 1)\}.$$

Case 4: We assume now that $\alpha = 2a + 1$ and $\beta = 2b + 1$. Notice that both x and y must be odd since the power of 2 is nonzero. Now we have a bigger issue to deal with. The class group of $\mathbb{Q}(\sqrt{10})$ has order 2 so we have to argue using ideals in the ring of

integers $\mathcal{O}_{\mathbb{Q}(\sqrt{10})} = \mathbb{Z}[\sqrt{10}]$. Factoring into ideals gives

$$\langle y - 2^a 5^b \sqrt{10} \rangle \langle y + 2^a 5^b \sqrt{10} \rangle = \langle x \rangle^5$$

Now suppose there exists a proper prime ideal $\mathfrak{p}$ containing both ideals on the right. Notice that summing the two generators shows that $2y \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime either $2 \in \mathfrak{p}$ or $y \in \mathfrak{p}$. If $2 \in \mathfrak{p}$, Then notice that $\mathfrak{p}$ must also contain x^5 and hence must contain x. As x is odd, we get that $1 = \gcd(x, 2) \in \mathfrak{p}$ which is a contradiction. Now suppose that $y \in \mathfrak{p}$. Then again as $\mathfrak{p} = \langle y - 2^a 5^b \sqrt{5} \rangle$, we see that $x \in \mathfrak{p}$ and hence $1 = \gcd(x, y) \in \mathfrak{p}$ which is again a contradiction. Thus the two ideals are coprime. Hence we can factor as

$$\langle y - 2^a 5^b \sqrt{10} \rangle = I^5$$

for some ideal I. Now the class group of $\mathbb{Z}[\sqrt{10}]$ is of size 2 so we must have that I is principal since 2 and 5 are coprime. Thus, setting $I = (m + n\sqrt{10})$, we have that

$$y - 2^a 5^b \sqrt{10} = (3 + \sqrt{10})^k (m + n\sqrt{10})^5$$

for $k \in \{0, 1, 2, 3, 4\}$ where $3 + \sqrt{10}$ is a fundamental unit and we use the usual trick of absorbing roots of unity to the 5th power. As in case 2, we can expand the equation above and compare coefficients of $\sqrt{10}$ to get a set of equations for each value of k given by $f_k(m, n) = 2^{\delta_1} 5^{\delta_2}$ given by

$$\begin{aligned}
k = 0 \qquad & f_0(m,n) := 5n(m^4 + 20m^2n^2 + 20n^4) \\
k = 1 \qquad & f_1(m,n) := m^5 + 15m^4n + 100m^3n^2 + 300m^2n^3 + 500mn^4 + 300n^5 \\
k = 2 \qquad & f_2(m,n) := 6m^5 + 95m^4n + 600m^3n^2 + 1900m^2n^3 + 3000mn^4 + 1900n^5 \\
k = 3 \qquad & f_3(m,n) := 37m^5 + 585m^4n + 3700m^3n^2 + 11700m^2n^3 \\
& \qquad + 18500mn^4 + 11700n^5 \\
k = 4 \qquad & f_4(m,n) := 228m^5 + 3605m^4n + 22800m^3n^2 + 72100m^2n^3 \\
& \qquad + 114000mn^4 + 72100n^5.
\end{aligned}$$

Again we mimic case 2. We need to account for the cases when the leading coefficient shares a divisor with an element of $\{2, 5\}$. To do this, we solve the following set of

related Thue-Mahler equations $g_j(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$ where $g_j(m,n)$ are given by

$$
\begin{aligned}
k = 0 \qquad & g_1(m,n) := m^4 + 20m^2n^2 + 20n^4 \\
k = 1 \qquad & g_2(m,n) := m^5 + 15m^4n + 100m^3n^2 + 300m^2n^3 + 500mn^4 + 300n^5 \\
k = 2 \qquad & g_3(m,n) := 6m^5 + 95m^4n + 600m^3n^2 + 1900m^2n^3 + 3000mn^4 + 1900n^5 \\
k = 2 \qquad & g_4(m,n) := 3m^5 + 95m^4n + 1200m^3n^2 + 7600m^2n^3 + 24000mn^4 + 30400n^5 \\
k = 3 \qquad & g_5(m,n) := 37m^5 + 585m^4n + 3700m^3n^2 + 11700m^2n^3 + 18500mn^4 + 11700n^5 \\
k = 4 \qquad & g_6(m,n) := 228m^5 + 3605m^4n + 22800m^3n^2 + 72100m^2n^3 \\
& \qquad + 114000mn^4 + 72100n^5 \\
k = 4 \qquad & g_7(m,n) := 114m^5 + 3605m^4n + 45600m^3n^2 + 288400m^2n^3 \\
& \qquad + 912000mn^4 + 1153600n^5 \\
k = 4 \qquad & g_8(m,n) := 57m^5 + 3605m^4n + 91200m^3n^2 + 1153600m^2n^3 \\
& \qquad + 7296000mn^4 + 18457600n^5.
\end{aligned}
$$

Solving the above sets of equations gives the following solutions.

j	Solutions to $g_j(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$ in the form $(m, n, \delta_1, \delta_2)$
1	$(1,0,0,0), (-1,0,0,0)$
2	$(1,0,0,0), (-1,0,0,0)$
3	$(-5,1,0,2), (5,-1,0,2)$
4	$(-5,1,4,2), (5,-1,4,2), (-10,1,4,2), (10,-1,4,2)$
5	$(-5,2,0,2), (5,-2,0,2), (5,-1,5,2), (-5,1,5,2)$
6	$(3,-1,0,0), (-3,1,0,0)$
7	$(6,-1,4,0), (-6,1,4,0)$
8	$(12,-1,8,0), (-12,1,8,0)$

Table 3.18: Solutions to $g_j(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m,0)$.

Here we see we gain additional solutions when we allow $\gcd(c_0, Y) > 1$ only in the case when $k = 2$ and this gives the solutions $(-5,2,5,2)$ and $(5,-2,5,2)$ with the second solution corresponding to a negative sign in $f_k(m,n) = \pm 2^{\delta_1} 5^{\delta_2}$. Thus our final list of solutions for $f_k(m,n) = 2^{\alpha} 5^{\beta}$ is as follows:

k	Solutions to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ in the form (m,n,δ_1,δ_2)	Corresponding (x,y,α,β)
0	None	None
1	$(1,0,0,0)$	$(-1,3,1,1)$
2	$(-5,1,0,2)$	$(15,-875,1,5)$
2	$(-5,2,5,2)$	$(-15,-2375,11,5)$
3	$(-5,2,0,2)$	$(15,875,1,5)$
3	$(5,-1,5,2)$	$(-15,2375,11,5)$
4	$(-3,1,0,0)$	$(-1,-3,1,1)$

Table 3.19: Solutions to $f_k(m,n) = 2^{\delta_1}5^{\delta_2}$ with $\gcd(m,n) = 1$ and n coprime to the coefficient of $g_j(m,0)$.

Summarizing the above, we get the following

Lemma 3.2.10. *The only solution to $y^2 = x^5 + 2^\alpha 5^\beta$ with α, β non-negative integers with α and β odd and x, y coprime integers is given by $(x,y,\alpha,\beta) = (-1,\pm 3,1,1)$.*

Thus, collecting all the above lemmas gives rise to the solutions with the powers of 2 and 5 in x and y are equal as

$$\begin{aligned}(x,y,\pm,A,B) \in \{&(2^{(A-1)/5}5^{B/5}, \pm 2^{(A-1)/2}5^{B/2}, +, 1+10A_1, 10B_1),\\ &(2^{(A-3)/5}5^{B/5}, \pm 2^{(A-3)/2}5^{B/2}(3), +, 3+10A_1, 10B_1),\\ &(-2^{(A-1)/5}5^{(B-1)/5}, \pm 2^{(A-1)/2}5^{(B-1)/2}(3), +, 1+10A_1, 1+10B_1),\\ &(-2^{(A-1)/5}5^{(B-2)/5}, \pm 2^{(A-1)/2}5^{(B-2)/2}(7), +, 1+10A_1, 2+10B_1),\\ &(-2^{(A-4)/5}5^{(B-1)/5}, \pm 2^{(A-4)/2}5^{(B-1)/2}(9), +, 4+10A_1, 1+10B_1),\\ &(2^{(A-1)/5}5^{(B-3)/5}(11), \pm 2^{(A-1)/2}5^{(B-3)/2}(401), -, 1+10A_1, 3+10B_1)\}.\end{aligned}$$

2. $2y_1 = 5x_1$ and $2y_2 = B$. Cancelling out the equal terms and relabelling terms

$$\hat{y}^2 = 5^{\hat{x_2}}\hat{x}^5 \pm 2^{\hat{A}}.$$

We have solved the case where $5 \mid x_2$ via Chabauty methods so without loss of generality, we may suppose that $x_2 > 0$. Modulo 5 considerations shows us that A is even. Thus, bringing over and factoring gives

$$(\hat{y} - 2^{A/2})(\hat{y} + 2^{A/2}) = 5^{\hat{x_2}}\hat{x}^5$$

or that

$$(\hat{y} - 2^{A/2}i)(\hat{y} + 2^{A/2}i) = 5^{\hat{x_2}}\hat{x}^5$$

As the terms are coprime in each case, we have that

$$\begin{cases} \hat{y} \mp 2^{A/2} = 5^{\hat{x_2}} K^5 \\ \hat{y} \pm 2^{A/2} = L^5 \end{cases}$$

where $K, L \in \mathbb{Z}$ or we have that

$$\hat{y} + 2^{A/2} i = \gamma^{\hat{x_2}} \alpha^5$$

where $\alpha = (a + bi) \in \mathbb{Z}[i]$ and $\gamma = 1 \pm 2i$. Without loss of generality again, we may assume that $\gamma = 1 + 2i$ since if $\alpha = a + bi$ is a solution to

$$2^{A/2} i = \Im((1 + 2i)^{\hat{x_2}} \alpha^5)$$

then we have that $\alpha_0 = -a + bi$ is a solution to

$$2^{A/2} i = \Im((1 - 2i)^{\hat{x_2}} \alpha_0^5).$$

In the first case, we get the Thue-Mahler equations corresponding to

$$5^s x^5 - y^5 = \pm 2^r \qquad \text{for } s \in \{0, ..4\} \text{ and where } \gcd(y, 5) = 1.$$

where we also note that $\gcd(y, 5) = 1$ or we get a Thue-Mahler equation corresponding to one of the following curves (denote the left hand sides by g_0, g_1, g_2 and g_3 respectively)

$$\begin{aligned} 2y^5 + 5y^4 x - 20y^3 x^2 - 10y^2 x^3 + 10yx^4 + x^5 &= \pm 2^r \\ 4y^5 - 15y^4 x - 40y^3 x^2 + 30y^2 x^3 + 20yx^4 - 3x^5 &= \pm 2^r \\ -2y^5 - 55y^4 x + 20y^3 x^2 + 110y^2 x^3 - 10yx^4 - 11x^5 &= \pm 2^r \\ -24y^5 - 35y^4 x + 240y^3 x^2 + 70y^2 x^3 - 120yx^4 - 7x^5 &= \pm 2^r. \end{aligned}$$

We enter these cases into the Thue-Mahler equation solver and come up with the following solutions

$$\begin{aligned} 5^s (0)^5 - (1)^5 &= -2^0 \\ 5^s (0)^5 - (-1)^5 &= 2^0 \\ 5^1 (1)^5 - (1)^5 &= 2^2 \\ 5^1 (-1)^5 - (-1)^5 &= -2^2 \end{aligned}$$

and for the other 4 equations (where below we keep the same sign for $\pm$ when we make

a choice)[2] solutions to $g_0(x,y) = \pm 2^r$ are given by

$$(x, y, r, \pm) \in \{(\pm 1, 0, 0, \pm), (-1, 1, 2, -), (1, -1, 2, +), (0, \pm 1, 1, \pm)\}.$$

Solutions to $g_1(x,y) = \pm 2^r$

$$(x, y, r, \pm) \in \{(0, \pm 1, 2, \pm), (-1, -1, 2, +), (1, 1, 2, -)\}.$$

Solutions to $g_2(x,y) = \pm 2^r$

$$(x, y, r, \pm) \in \{(0, \pm 1, 1, \pm)\}.$$

There are no solutions to $g_3(x,y) = \pm 2^r$.

Transferring back to the original equation gives rise to the solutions

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{(A-1)/5}5^{B/5}, \pm 2^{(A-1)/2}5^{B/2}, +, 1 + 10A_1, 10B_1),\\ &(2^{(A-3)/5}5^{B/5}, \pm 2^{(A-3)/2}5^{B/2}(3), +, 3 + 10A_1, 10B_1),\\ &(-2^{(A-2)/5}5^{(B+1)/5}, \pm 2^{(A-2)/2}5^{B/2}(3), +, 2 + 10A_1, 4 + 10B_1),\\ &(-2^{(A-2)/5}5^{(B+3)/5}, \pm 2^{(A-2)/2}5^{B/2}(11), -, 2 + 10A_1, 2 + 10B_1),\\ &(-2^{(A-2)/5}5^{(B+1)/5}, \pm 2^{(A-2)/2}5^{B/2}, -, 2 + 10A_1, 4 + 10B_1),\\ &(2^{(A-4)/5}5^{(B+2)/5}, \pm 2^{(A-4)/2}5^{B/2}(3), -, 4 + 10A_1, 8 + 10B_1)\}.\end{aligned}$$

3. $2y_1 = 5x_1$ and $5x_2 = B$. Canceling out the equal terms and relabeling terms

$$5^{\hat{y_2}}\hat{y}^2 = \hat{x}^5 \pm 2^{\hat{A}}.$$

If $\hat{y_2}$ is even, then we get the equation

$$Y^2 = X^5 \pm 2^{\hat{A}}.$$

Otherwise, if $\hat{y_2}$ is odd, multiplying through by 5^5 gives the equation

$$Y^2 = X^5 \pm 2^{\hat{A}}5^5.$$

Here we can use the results from Chabauty and Elliptic Curve Chabauty methods to

[2]Notice that above we reversed the roles of x and y. This is since the Thue-Mahler equation solver has the additional constraint that it only returns solutions with $\gcd(c_0, y) = 1$ where c_0 is the coefficient of x^5. In the form above, we note that any solution must necessarily have $\gcd(c_0, y) = 1$.

see that the only solutions to $Y^2 = X^5 \pm 2^{\hat{A}}$ with $\hat{A} \leq 9$ are given by

$$\begin{aligned}(X, Y, \hat{A}, \pm) \in \{&(-1, 0, 0, +), (0, \pm 1, 0, +), (1, 0, 0, -), (-1, \pm 1, 1, +), (0, \pm 2, 2, +),\\ &(2, \pm 6, 2, +), (1, \pm 3, 3, +), (0, \pm 4, 4, +), (2, \pm 4, 4, -), (-2, 0, 5, +),\\ &(2, \pm 8, 5, +), (2, 0, 5, -), (6, \pm 88, 5, -), (0, \pm 8, 6, +), (0, \pm 16, 8, +)\}\end{aligned}$$

and the only solutions to $Y^2 = X^5 \pm 2^{\hat{A}} 5^5$ with $\hat{A} \leq 9$ are given by

$$\begin{aligned}(X, Y, \hat{A}, \pm) \in \{&(-5, 0, 0, +), (5, 0, 0, -), (15, \pm 875, 1, +), (-15/4, \pm 2375/32, 1, +),\\ &(5, \pm 125, 2, +), (-10, 0, 5, +), (10, 0, 5, -), (20, \pm 2000, 8, +)\}.\end{aligned}$$

Of the above solutions, in this case, we only consider the ones where $2 \nmid \gcd(x, y)$ (otherwise we violate the condition that $2y_1 = 5x_1$). The remaining 5 cases give rise to the solutions

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{(A-1)/5} 5^{B/5}, \pm 2^{(A-1)/2} 5^{B/2}, +, 1 + 10A_1, 10B_1),\\ &(2^{(A-3)/5} 5^{B/5}, \pm 2^{(A-3)/2} 5^{B/2}(3), +, 3 + 10A_1, 10B_1),\\ &(2^{(A-1)/5} 5^{B/5}(3), \pm 2^{(A-1)/2} 5^{(1+B)/2}(7), +, 1 + 10A_1, 5 + 10B_1),\\ &(2^{(A-1)/5} 5^{B/5}(3), \pm 2^{(A-1)/2} 5^{(1+B)/2}(19), +, 11 + 10A_1, 5 + 10B_1),\\ &(2^{(A-2)/5} 5^{B/5}, \pm 2^{(A-2)/2} 5^{(1+B)/2}, +, 2 + 10A_1, 5 + 10B_1)\}.\end{aligned}$$

4. $2y_1 = A$ and $2y_2 = 5x_2$. Canceling out the equal terms and relabeling terms

$$\hat{y}^2 = 2^{\hat{x_1}} \hat{x}^5 \pm 5^{\hat{B}}.$$

In the case where $\hat{y}^2 = 2^{\hat{x_1}} \hat{x}^5 - 5^{\hat{B}}$, if $x_1 \geq 2$, then reducing modulo 4 shows us that $\hat{y}^2 = 2^{\hat{x_1}} \hat{x}^5 - 5^{\hat{B}}$ has no solutions. Thus we are left only with the case

$$\hat{y}^2 = 2\hat{x}^5 - 5^{\hat{B}}$$

with $\gcd(\hat{x}, \hat{y}) = 1$. Here we may use [AMLST09] to see that the only solutions to this equation are given by

$$(\hat{x}, \hat{y}, \hat{B}) \in \{(3, \pm 19, 3), (7, \pm 183, 3)\}$$

and these translate to

$$(x, y, \pm, A, B) \in \{(2^{(A+1)/5}5^{(B-3)/5}(3), \pm 2^{A/2}5^{(B-3)/2}(19), -, 4 + 10A_1, 3 + 10B_1),$$
$$(2^{(A+1)/5}5^{(B-3)/5}(7), \pm 2^{A/2}5^{(B-3)/2}(3)(61), -, 4 + 10A_1, 3 + 10B_1))\}.$$

We finish this case off by considering when $\hat{y}^2 = 2^{\hat{x_1}}\hat{x}^5 + 5^{\hat{B}}$. Notice here that reducing modulo 4 yields that $\hat{x_1} \geq 2$. Considerations modulo 8 thus reveal that $\hat{B}$ is odd when $\hat{y}^2 = 4\hat{x}^5 + 5^{\hat{B}}$ and that $\hat{B}$ is even when $\hat{y}^2 = 2^{\hat{x_1}}\hat{x}^5 + 5^{\hat{B}}$ for $\hat{x_1} \geq 3$.

For the case where $\hat{y}^2 = 4\hat{x}^5 + 5^{\hat{B}}$ with $\hat{B}$ is odd, we may factor over the ring of integers of $\mathbb{Q}(\sqrt{5})$ (namely $\mathbb{Z}[(1 + \sqrt{5})/2]$) to see that

$$(\hat{y} - 5^{(\hat{B}-1)/2}\sqrt{5})(\hat{y} + 5^{(\hat{B}-1)/2}\sqrt{5}) = 4\hat{x}^5.$$

The greatest common divisor of the terms on the left is 2 and so we have that

$$\frac{\hat{y} + 5^{(\hat{B}-1)/2}\sqrt{5}}{2} = \epsilon^k \left(\frac{a + b\sqrt{5}}{2}\right)^5$$

where $\epsilon = (1+\sqrt{5})/2$. Expanding and simplifying gives a subset of the cases considered in case 1. In particular, we are looking for solutions there with 2^{4+k} in the Thue-Mahler equation. This gives desired solutions when $k = 0, 4$ (see the table from the first case in this section) and in these cases, we have the solutions given by

$$(a, b, k, \hat{y}, \hat{B}) \in \{(-1, 1, 0, 11, 3), (1, 1, 0, -11, 3), (-1, 1, 4, 1, 1), (-5, 1, 4, 125, 5)\}$$

and also solutions coming just from units as given by

$$(a, b, k, \hat{y}, \hat{B}) \in \{(1, 0, 1, 1, 1), (1, 0, 3, 3, 1)\}.$$

When we translate these solutions to the equation $\hat{y}^2 = 4\hat{x}^5 + 5^{\hat{B}}$, we get

$$(\hat{x}, \hat{y}, \hat{B}) \in \{(-1, \pm 11, 3), (-1, \pm 1, 1), (5, \pm 125, 5), (1, \pm 3, 1)\}.$$

In this case, we need that $2y_1 = A$ and $2y_2 = 5x_2$ which eliminates the third solution above. Summarizing, we get the solutions to the original equation given by

$$(x, y, \pm, A, B) \in \{(2^{(A+2)/5}5^{(B-1)/5}, \pm 2^{A/2}5^{(B-1)/2}(3), +, 8 + 10A_1, 1 + 10B_1),$$
$$(2^{(A+2)/5}5^{(B-1)/5}, \pm 2^{A/2}5^{(B-1)/2}, +, 8 + 10A_1, 1 + 10B_1),$$
$$(2^{(A+2)/5}5^{(B-3)/5}, \pm 2^{A/2}5^{(B-3)/2}(11), +, 8 + 10A_1, 3 + 10B_1)\}.$$

For the case where $\hat{y}^2 = 2^{\hat{x_1}}\hat{x}^5 + 5^{\hat{B}}$ for $\hat{x_1} \geq 3$ and $\hat{B}$ is even, we isolate and factor over $\mathbb{Z}$ to see that

$$(\hat{y} - 5^{\hat{B}/2})(\hat{y} + 5^{\hat{B}/2}) = 2^{\hat{x_1}}\hat{x}^5.$$

The left hand side has only a common factor of 2. This gives rise to the pair of equations

$$\begin{cases} \hat{y} \mp 5^{\hat{B}/2} = 2K^5 \\ \hat{y} \pm 5^{\hat{B}/2} = 2^{\hat{x_1}-1}L^5. \end{cases}$$

Subtracting yields $\pm 5^{\hat{B}/2} = 2^{\hat{x_1}-2}L^5 - K^5$. We solve this using our Thue-Mahler solver to see that the only solutions with $KL \neq 0$ are given when $K, L \in \{\pm 1\}$. This gives

$$(\hat{y}, \hat{B}, \hat{x_1}, K, L) \in \{(\pm 3, 0, 3, 1, 1), (\pm 3, 0, 4, -1, 1)\}.$$

Translating to the general solution of our equation gives

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{(A+3)/5}5^{B/5}, \pm 2^{A/2}5^{B/2}(3), +, 2 + 10A_1, 10B_1), \\ &(2^{(A+4)/5}5^{(B-2)/5}, \pm 2^{A/2}5^{(B-2)/2}(3), +, 6 + 10A_1, 2 + 10B_1)\}.\end{aligned}$$

Summarizing, this case gives the following solutions:

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{A/5}5^{B/5}, \pm 2^{A/2}5^{B/2}(3), +, 2 + 10A_1, 10B_1), \\ &(2^{(A+1)/5}5^{B/5}, \pm 2^{A/2}5^{B/2}, -, 4 + 10A_1, 10B_1), \\ &(2^{(A+4)/5}5^{(B-2)/5}, \pm 2^{A/2}5^{(B-2)/2}(3), +, 6 + 10A_1, 2 + 10B_1), \\ &(2^{(A+2)/5}5^{(B-1)/5}, \pm 2^{A/2}5^{(B-1)/2}(3), +, 8 + 10A_1, 1 + 10B_1), \\ &(2^{(A+2)/5}5^{(B-1)/5}, \pm 2^{A/2}5^{(B-1)/2}, +, 8 + 10A_1, 1 + 10B_1), \\ &(2^{(A+2)/5}5^{(B-3)/5}, \pm 2^{A/2}5^{(B-3)/2}(11), +, 8 + 10A_1, 3 + 10B_1), \\ &(2^{(A+1)/5}5^{(B-3)/5}(3), \pm 2^{A/2}5^{(B-3)/2}(19), -, 4 + 10A_1, 3 + 10B_1), \\ &(2^{(A+1)/5}5^{(B-3)/5}(7), \pm 2^{A/2}5^{(B-3)/2}(3)(61), -, 4 + 10A_1, 3 + 10B_1)\}.\end{aligned}$$

5. $2y_1 = A$ and $2y_2 = B$. Canceling out the equal terms and relabeling terms

$$\hat{y}^2 = 2^{\hat{x_1}}5^{\hat{x_2}}\hat{x}^5 \pm 1.$$

In this case, again if $x_1 > 1$, then we see that the -1 case gives a contradiction via modulo 4 considerations. This leaves us with

$$\hat{y}^2 = 2 \cdot 5^{\hat{x_2}}\hat{x}^5 - 1$$

and the positive 1 case which we defer until later. Factoring gives

$$(\hat{y}+i)(\hat{y}-i) = 2 \cdot 5^{\hat{x_2}} \hat{x}^5.$$

As the two terms on the left are coprime outside of 2, we see that

$$\hat{y}+i = (1 \pm i)(1 \pm 2i)^{\hat{x_2}}(a+bi)^5.$$

We use the Thue-Mahler equation solver on these equations and see that the only solutions come when $\hat{x_2} = 0, 1$ or 2 giving solutions as

$$(\hat{x}, \hat{y}, \hat{x_1}, \hat{x_2}) \in \{(0, \pm 1, 1, 0), (1, \pm 3, 1, 1), (1, \pm 7, 1, 2)\}.$$

These in turn give rise to solutions to the original equation of the form

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{(A+1)/5}5^{B/5}, \pm 2^{A/2}5^{B/2}, -, 4+10A_1, 10B_1),\\ &(2^{(A+1)/5}5^{(B+1)/5}(3), \pm 2^{A/2}5^{B/2}, -, 4+10A_1, 4+10B_1),\\ &(2^{(A+1)/5}5^{(B+2)/5}(7), \pm 2^{A/2}5^{B/2}, -, 4+10A_1, 8+10B_1)\}.\end{aligned}$$

Now, to handle the case where

$$\hat{y}^2 = 2^{\hat{x_1}}5^{\hat{x_2}}\hat{x}^5 + 1$$

we first note that if $\hat{x_1} \leq 2$, we have that modulo 8 considerations give a contradiction. Hence $\hat{x_1} \geq 3$. Factoring gives

$$(\hat{y}+1)(\hat{y}-1) = 2^{\hat{x_1}}5^{\hat{x_2}}\hat{x}^5.$$

The left hand side is coprime outside of 2 and hence we have one of

$$\begin{cases} \hat{y} \mp 1 &= 2^{\hat{x_1}-1}5^{\hat{x_2}}K^5 \\ \hat{y} \pm 1 &= 2L^5 \end{cases} \qquad \begin{cases} \hat{y} \mp 1 &= 2 \cdot 5^{\hat{x_2}}K^5 \\ \hat{y} \pm 1 &= 2^{\hat{x_1}-1}L^5. \end{cases}$$

Subtracting the equations and dividing by 2 in each case gives

$$\mp 1 = 2^{\hat{x_1}-2}5^{\hat{x_2}}K^5 - L^5 \qquad \mp 1 = 5^{\hat{x_2}}K^5 - 2^{\hat{x_1}-2}L^5.$$

Both of these can be solved using the Thue-Mahler equation solver. The solutions with

$KL \neq 0$ are given by

$$(\hat{x_1}, \hat{x_2}, K, L) \in \{(3, 0, 1, 1), (3, 0, -1, -1)\}$$

in the first case and in the second case by

$$(\hat{x_1}, \hat{x_2}, K, L) \in \{(3, 0, 1, 1), (3, 0, -1, -1), (4, 1, 1, 1), (4, 1, -1, -1)\}.$$

Converting to solutions of the original equation gives

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{A/5}5^{B/5}, \pm 2^{A/2}5^{B/2}(3), +, 2 + 10A_1, 10B_1),\\ &(2^{(A+4)/5}5^{(B+1)/5}(9), \pm 2^{A/2}5^{B/2}, +, 6 + 10A_1, 4 + 10B_1)\}\end{aligned}$$

Collecting all the solutions in this case yields the following list:

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{A/5}5^{B/5}, \pm 2^{A/2}5^{B/2}(3), +, 2 + 10A_1, 10B_1),\\ &(2^{(A+1)/5}5^{B/5}, \pm 2^{A/2}5^{B/2}, -, 4 + 10A_1, 10B_1),\\ &(2^{(A+4)/5}5^{(B+1)/5}(9), \pm 2^{A/2}5^{B/2}, +, 6 + 10A_1, 4 + 10B_1),\\ &(2^{(A+1)/5}5^{(B+1)/5}(3), \pm 2^{A/2}5^{B/2}, -, 4 + 10A_1, 4 + 10B_1),\\ &(2^{(A+1)/5}5^{(B+2)/5}(7), \pm 2^{A/2}5^{B/2}, -, 4 + 10A_1, 8 + 10B_1)\}.\end{aligned}$$

6. $2y_1 = A$ and $5x_2 = B$. Canceling out the equal terms and relabeling terms

$$5^{\hat{y_2}}\hat{y}^2 = 2^{\hat{x_1}}\hat{x}^5 \pm 1.$$

We can reduce this to exactly case (iii), which we solved using Chabauty and Elliptic Curve Chabauty techniques, by removing the power of 5 on the left hand side by multiplying through by 5^5 if $\hat{y_2}$ is odd and a suitable power of 2 which gives rise to the equations

$$Y^2 = X^5 \pm 2^{\hat{A}} \quad \text{or} \quad Y^2 = X^5 \pm 2^{\hat{A}}5^5.$$

Here we are interested in the cases where $2 \mid \gcd(X, Y)$ and thus are left with the list given by

$$(X, Y, \hat{A}, \pm) \in \{(2, \pm 6, 2, +), (2, \pm 4, 4, -), (2, \pm 8, 5, +), (6, \pm 88, 5, -)\}$$

for the first equation and for the second equation,

$$(X, Y, \hat{A}, \pm) \in \{(20, \pm 2000, 8, +)\}.$$

The cases where $(X, Y, \hat{A}, \pm) = (2, \pm 8, 5, +)$ or $(6, \pm 88, 5, -)$ are inadmissible since the power of 2 in Y^2 does not match the value of $\hat{A}$. This leaves us only three solutions which in terms of our original equation are given by

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{A/5}5^{B/5}, \pm 2^{A/2}5^{B/2}(3), +, 2 + 10A_1, 10B_1),\\ &(2^{(A+1)/5}5^{B/5}, \pm 2^{A/2}5^{B/2}, -, 4 + 10A_1, 10B_1),\\ &(2^{(A+2)/5}5^{B/5}, \pm 2^{(A+12)/2}5^{(B+1)/2}, +, 8 + 10A_1, 5 + 10B_1)\}.\end{aligned}$$

7. $5x_1 = A$ and $2y_2 = 5x_2$. In this case, we have

$$2^{\hat{y_1}}\hat{y}^2 = \hat{x}^5 \pm 5^{\hat{B}}.$$

We can proceed similar to case 3. If $\hat{y_1}$ is even, then we look at solutions to the equation

$$Y^2 = X^5 \pm 5^{\hat{B}}$$

and if $\hat{y_1}$ is odd, multiply through by 2^5 and look at solutions to the equation

$$Y^2 = X^5 \pm 2^5 5^{\hat{B}}.$$

Using Chabauty and Elliptic Curve Chabauty, we have the solutions given in the case of $Y^2 = X^5 \pm 5^{\hat{B}}$ by

$$\begin{aligned}(X, Y, \hat{B}, \pm) \in \{&(-1, 0, 0, +), (0, \pm 1, 0, +), (1, 0, 0, -), (-1, \pm 2, 1, +), (0, \pm 5, 2, +),\\ &(0, \pm 25, 4, +), (5, \pm 50, 4, -), (-5, 0, 5, +),\\ &(5, 0, 5, -), (0, \pm 125, 6, +), (0, \pm 625, 8, +)\}\end{aligned}$$

and in the second case by

$$\begin{aligned}(X, Y, \hat{B}, \pm) \in \{&(-2, 0, 0, +), (2, \pm 8, 0, +), (2, 0, 0, -),\\ &(6, \pm 88, 0, +), (-10, 0, 5, +), (10, 0, 5, -)\}.\end{aligned}$$

In the first case, there are only two solutions with non-zero entries and these are given by

$$(X, Y, C, \pm) \in \{(-1, \pm 2, 1, +), (5, \pm 50, 4, -)\}$$

The second solution above does not satisfy $2y_2 = 5x_2$ (it satisfies $2y_2 = B$). The remaining case corresponds to the solution given by

$$(x, y, \pm, A, B) \in \{(-2^{A/5}5^{(B-1)/5}, \pm 2^{(2+A)/2}5^{(B-1)/2}, +, 10A_1, 1 + 10B_1)\}$$

In the second case, we see that the only solutions correspond to when $\hat{B} = 0$. These are precisely the solutions discussed in case (ix) below and are given by

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(2^{A/5}5^{B/5}(3), \pm 2^{(1+A)/2}5^{B/2}(11), -, 5 + 5A_1, 10B_1),\\ &(2^{A/5}5^{B/5}, \pm 2^{(1+A)/2}5^{B/2}, +, 5 + 5A_1, 10B_1)\}.\end{aligned}$$

Hence all solutions in this case are given by

$$\begin{aligned}(x, y, \pm, A, B) \in \{&(-2^{A/5}5^{(B-1)/5}, \pm 2^{(2+A)/2}5^{(B-1)/2}, +, 10A_1, 1 + 10B_1),\\ &(2^{A/5}5^{B/5}(3), \pm 2^{(1+A)/2}5^{B/2}(11), -, 5 + 5A_1, 10B_1),\\ &(2^{A/5}5^{B/5}, \pm 2^{(1+A)/2}5^{B/2}, +, 5 + 5A_1, 10B_1)\}.\end{aligned}$$

8. $5x_1 = A$ and $2y_2 = B$. In this case, we have

$$2^{\hat{y_1}}\hat{y}^2 = 5^{\hat{x_2}}\hat{x}^5 \pm 1.$$

In the case where $\hat{x_2} > 0$, we see that modulo 5, we must have that

$$\hat{y}^2 = \pm 2^{\hat{y_1}}$$

which is a contradiction unless $\hat{y_1}$ is even. When this is even, this case gives rise to solutions of

$$Y^2 = X^5 \pm 5^C$$

for some constant $0 \leq C \leq 9$. These solutions were discussed in case (vii) above and solved by Chabauty and Elliptic Curve Chabauty techniques. There are only two solutions with non-zero entries and these are given by

$$(X, Y, C, \pm) \in \{(-1, \pm 2, 1, +), (5, \pm 50, 4, -)\}.$$

The case when $C = 1$ above does not correspond to a solution in this case as it is too small. Hence we are given solutions only by the second case above which corresponds to

$$(x, y, \pm, A, B) \in \{(2^{A/5}5^{(1+B)/5}, \pm 2^{(2+A)/2}5^{B/2}, -, 10A_1, 4 + 10B_1)\}.$$

If $\hat{x_2} = 0$, then we see as in case (ix) below that the solutions are given by

$$(x, y, \pm, A, B) \in \{(2^{A/5}5^{B/5}(3), \pm 2^{(1+A)/2}5^{B/2}(11), -, 5 + 5A_1, 10B_1),$$
$$(2^{A/5}5^{B/5}, \pm 2^{(1+A)/2}5^{B/2}, +, 5 + 5A_1, 10B_1)\}.$$

Hence all solutions in this case are given by

$$(x, y, \pm, A, B) \in \{(2^{A/5}5^{(1+B)/5}, \pm 2^{(2+A)/2}5^{B/2}, -, 10A_1, 4 + 10B_1),$$
$$(2^{A/5}5^{B/5}(3), \pm 2^{(1+A)/2}5^{B/2}(11), -, 5 + 5A_1, 10B_1),$$
$$(2^{A/5}5^{B/5}, \pm 2^{(1+A)/2}5^{B/2}, +, 5 + 5A_1, 10B_1)\}.$$

9. $5x_1 = A$ and $5x_2 = B$. In this case, we have

$$2^{\hat{y_1}}5^{\hat{y_2}}\hat{y}^2 = \hat{x}^5 \pm 1.$$

By work done by Bennett and Skinner as stated in Theorem 1.6.2, this gives rise to a solution to

$$X^5 + Y^5 = CZ^2$$

with $C \in \{1, 2, 5, 10\}$. In their work, they show that this case has no solutions when $y = \pm 1$ except for

$$(X, Y, Z, C) \in \{(3, -1, \pm 11, 2), (1, -1, 0, C), (-1, 1, 0, C), (1, 1, 1, 2)\}.$$

We drop the cases where $z = 0$ as these have been considered already. Translating back to the original problem, we have that

$$(x, y, \pm, A, B) = \{(2^{A/5}5^{B/5}(3), \pm 2^{(1+A)/2}5^{B/2}(11), -, 5 + 5A_1, 10B_1),$$
$$(2^{A/5}5^{B/5}, \pm 2^{(1+A)/2}5^{B/2}, +, 5 + 5A_1, 10B_1)\}$$

are the solutions that arise from this case.

We finish off with a theorem that will be used heavily later.

Theorem 3.2.11. *Let $d, \ell, m \geq 0$ be integers and let $p \neq 5$ be an odd prime number. Then solutions to the equations*

$$d^2 = 2^\ell 5^m p^5 \pm 1 \quad d^2 = \pm 2^\ell p^5 \pm 5^m \quad d^2 = \pm 2^\ell 5^m \pm p^5$$
$$d^2 = 2^\ell \pm 5^m p^5 \quad 5d^2 = \pm 2^\ell \pm p^5 \quad 5d^2 = \pm 2^\ell p^5 \pm 1$$

are given by

$$19^2 = 2 \cdot 3^5 - 5^3 \qquad (183)^2 = 2 \cdot 7^5 - 5^3$$
$$401^2 = -2 \cdot 5^3 + 11^5 \qquad 5(7)^2 = 3^5 + 2$$
$$5(19)^2 = -3^5 + 2^{11}.$$

In particular, the equations

$$d^2 = 2^\ell 5^m p^5 \pm 1 \qquad d^2 = 2^\ell \pm 5^m p^5 \qquad 5d^2 = \pm 2^\ell p^5 \pm 1$$

have no solutions.

3.3 Other Results

The following are results used from Wilfrid Ivorra [Ivo04][p.38-45]. Define

$$f(n) := \begin{cases} 18 + 2\log_2 n & \text{if } n < 2^{96} \\ 435 + 10\log_2 n & \text{if } n \geq 2^{96}. \end{cases}$$

Theorem 3.3.1. *Solutions to $d^2 - 1 = 2^\ell p^n$ with $d \geq 1$ and $d, \ell, n \in \mathbb{Z}$ nonnegative integers are given by*

1. *$n = 0$ and $(d, \ell, p) = (3, 3, p)$.*
2. *$n = 1$ and $(d, \ell, p) \in \{(2, 0, 3), (5, 3, 3), (7, 4, 3), (9, 4, 5), (2p - 1, \ell, 2^{\ell-2} + 1), (2p + 1, \ell, 2^{\ell-2} - 1)\}$ with $\ell \geq 5$ in the last two cases.*
3. *$n = 2$ and $(d, \ell, p) = (17, 5, 3)$.*

Theorem 3.3.2. *Solutions to $d^2 + 1 = 2^\ell p^n$ with $d \geq 1$ and $d, \ell, n \in \mathbb{Z}$ nonnegative integers are given by*

1. *$n = 0$ and $(d, \ell, p) = (1, 1, p)$.*
2. *$n = 1$ and $(d, \ell, p) \in \{(5, 1, 13), (d, 0, 1), (d, 1, 1)\}$.*
3. *$n = 2$ and $(d, \ell, p) = (d, 1, p)$ with $p \equiv 1 \pmod 4$ and $p \neq 13$.*
4. *$n = 4$ and $(d, \ell, p) = (239, 1, 13)$.*

Theorem 3.3.3. *Solutions to $d^2 + 2^\ell = p^n$ with $d \geq 1$ and $d, \ell, n \in \mathbb{Z}$ nonnegative integers are given by*

1. $n = 1$ *and* $\ell < \log_2 p$.

2. $n = 2$ *and* $(d, \ell, p) \in \{(3, 4, 5), (1, 3, 3), (p-2, \ell, 2^{\ell-2}+1)\}$ *where in the last case,* $\ell \geq 5$.

3. $n = 3$ *and* $(d, \ell, p) \in \{(5, 1, 3), (11, 2, 5)\}$.

4. $n = 4$ *and* $(d, \ell, p) = (7, 5, 3)$.

Theorem 3.3.4. *Solutions to* $d^2 - 2^\ell = p^n$ *with* $d \geq 1$ *and* $d, \ell, n \in \mathbb{Z}$ *nonnegative integers are given by*

1. $n = 0$ *and* ℓ *odd.*

2. $n = 1$ *and* $\ell < f(p)$.

3. $n = 2$ *and* $(d, \ell, p) = (p + 2, \ell, 2^{\ell-2} - 1)$ *with* $\ell \geq 4$.

4. $n = 3$ *and* $(d, \ell, p) = (71, 7, 17)$.

Theorem 3.3.5. *Solutions to* $d^2 + p^n = 2^\ell$ *with* $d \geq 1$ *and* $d, \ell, n \in \mathbb{Z}$ *nonnegative integers are given by*

1. $n = 0$ *and* $(d, \ell, p) = (1, 1, p)$.

2. $n = 1$ *and* $\ell < f(p)$.

3. $n = 3$ *and* $(d, \ell, p) \in \{(13, 9, 7)\}$.

Theorem 3.3.6. *Solutions to* $2d^2 + 1 = p^n$ *with* $d \geq 1$ *and* $d, n \in \mathbb{Z}$ *nonnegative integers are given by*

1. $n = 1$.

2. $n = 2$.

3. $n = 5$ *and* $(d, p) = (11, 3)$.

Theorem 3.3.7. *Solutions to* $2d^2 - 1 = p^n$ *with* $d \geq 1$ *and* $d, n \in \mathbb{Z}$ *nonnegative integers are given by*

1. $n = 0$ *and* $d = 1$.

2. $n = 1$.

3. $n = 2$.

4. $n = 3$ *and* $(d, p) = (78, 23)$.

This final result on Catalan's conjecture is due to Mihăilescu [Mih04].

Theorem 3.3.8. *(Mihăilescu's Theorem) The only solution to the Diophantine equation* $x^m - y^n = 1$ *in positive integers* x, y, n, m *with* $n, m \geq 2$ *is given by* $3^2 - 2^3 = 1$.

3.4 Diophantine Equations Relating to Elliptic Curves

In this section, we solve the following Diophantine equations where $d \geq 1$, $\ell, m, n \geq 0$, $p \neq 2, 5$ and we do not have $(+, -)$ in the two $\pm$ signs:

1. $d^2 - 2^\ell 5^m p^n = \pm 1$
2. $d^2 \pm 2^\ell p^n = \pm 5^m$
3. $d^2 \pm 2^\ell 5^m = \pm p^n$
4. $d^2 \pm 2^\ell = \pm 5^m p^n$
5. $5d^2 \pm 2^\ell = \pm p^n$
6. $5d^2 \pm 2^\ell p^n = \pm 1$.

This will help simplify the classification of primes such that there is an elliptic curve with rational two torsion and conductor in the set $50p, 200p$ and $400p$. Throughout let $P_{\min}(n)$ denote the minimum prime dividing n.

Theorem 3.4.1. *Let $p \neq 2, 5$ be a prime number with $\ell, m, n \geq 0$ and $d \geq 1$.*

1. *Solutions to $d^2 - 2^\ell 5^m p^n = 1$ are given by*
   - *(a) $n = 0$ and $(d, \ell, m) \in \{(3, 3, 0), (9, 4, 1)\}$.*
   - *(b) $n = 1$ and*
     - *a) $p = 3$ and $(d, \ell, m) \in \{(2, 0, 0), (5, 3, 0), (7, 4, 0), (4, 0, 1), (11, 3, 1), (49, 5, 2)\}$.*
     - *b) $(d, \ell, m, p) \in \{(2p - 1, \ell, 0, 2^{\ell-2} + 1), (2p + 1, \ell, 0, 2^{\ell-2} - 1)\}$ with $\ell \geq 5$.*
     - *c) $(d, \ell, m, p) \in \{(2^{\ell-1} + 1, \ell, m, \frac{2^{\ell-2}+1}{5^m})\}$ with $m \geq 1$ and $\ell \geq 4$ even.*
     - *d) $(d, \ell, m, p) \in \{(p + 1, 0, m, 5^m - 2), (p - 1, 0, m, 5^m + 2)\}$ with $m \geq 1$.*
     - *e) $(d, \ell, m, p) \in \{(4p - 1, 3, m, \frac{5^m+1}{2})\}$ with $m \geq 1$.*
     - *f) $(d, \ell, m, p) \in \{(2p - 1, \ell, m, 2^{\ell-2}5^m + 1), (2p + 1, \ell, m, 2^{\ell-2}5^m - 1)\}$ with $m \geq 1$ and $\ell \geq 3$.*
     - *g) $(d, \ell, m, p) = (2 \cdot 5^m - 1, 4, m, \frac{5^m-1}{4})$ and m odd.*
   - *(c) $n = 2$ and $(d, \ell, m, p) \in \{(17, 5, 2, 3), (19, 3, 1, 3), (99, 3, 2, 7)\}$.*
   - *(d) $n = 3$ and $(d, \ell, m, p) = (26, 0, 2, 3)$.*
   - *(e) $n = 4$ and $(d, \ell, m, p) = (161, 6, 1, 3)$.*
   - *(f) $P_{\min}(n) \geq 7$, $d = 2 \cdot 5^m - 1$ and $4p^n = 5^m - 1$ with m odd and $\ell = 4$.*
2. *Solutions to $d^2 - 2^\ell 5^m p^n = -1$ with $\ell, m, n \geq 0$ and $d \geq 1$ are given by*

(a) $m = 0$ *and*

i. $p \geq 5$ *and* $(d, \ell, n) = (1, 1, 0)$.

ii. $p = 13$ *and* $(d, \ell, n) \in \{(5, 1, 1), (239, 1, 4)\}$.

iii. $p \neq 13, p \equiv 1 \pmod 4$ *and* $(\ell, n) = (1, 2)$.

iv. $(\ell, n) \in \{(0, 1), (1, 1)\}$

(b) $n = 0$ *and* $(d, \ell, m) \in \{(2, 0, 1), (3, 1, 1), (7, 1, 2)\}$.

(c) $m, n \geq 1$, $\ell = 0, 1$ *and* $p \equiv 1 \pmod 4$.

1. (a) **Case 1:** $m = 0$ **or** $n = 0$**.** This is done in Ivorra's thesis (see Theorem 3.3.1). Note that the $(d, \ell, n, p) = (9, 4, 1, 5)$ solution above is given as $(d, \ell, m, n, p) = (9, 4, 1, 0, p)$. Thus throughout, we assume that $m > 0$ and that $n > 0$.

Case 2: $p = 3$ This case was done in [Mul06] Gives the solutions

$$(d, \ell, m, n) \in \{(161, 6, 1, 4), (9, 4, 1, 0), (26, 0, 2, 3), (49, 5, 2, 1), \\ (4, 0, 1, 1), (19, 3, 1, 2), (11, 3, 1, 1)\}$$

and a potential solution given from $5 \cdot 3^\ell = 2^{m-2} + 1$ with $\ell \geq 1$ and $m \geq 5$. For this case, modulo 5 shows us that $2^{m-2} \equiv -1 \pmod 5$ and so $m \equiv 0 \pmod 4$. Modulo 3 gives $2^{m-2} \equiv -1 \pmod 3$ and so m is odd which gives a contradiction. Thus this last case does not occur and the other cases are listed in the statement. Hence throughout we suppose that $p \geq 7$.

Case 3: $\ell = 0$**.** Here we have that $d^2 - 1 = 5^m p^n$. As d is even, we have that modulo 4, we see that $p \equiv 3 \pmod 4$ and that n is odd. Factoring the left hand side gives $(d - 1)(d + 1) = 5^m p^n$ which gives

$$d \pm 1 = 5^m$$
$$d \mp 1 = p^n$$

where the signs above match up[3] In either case, taking the difference gives

$$\pm 2 = 5^m - p^n.$$

As we have already shown that n is odd, we begin breaking this into mini cases.

[3] A positive sign for the first term means you must use a negative sign in the second term. This convention will be consistent throughout the paper, especially in this section.

Case 3a: $n = 1$**.** This gives $p = 5^m \mp 2$ and $d = p \pm 1$ where again the signs match up.

Case 3b: $3 \mid n$**.** This gives $(p^{n/3})^3 = 5^m \mp 2$. If m is even, then looking at this as an integer solution to an elliptic curve of the form $y^2 = x^3 \pm 2$. We use Theorem 3.1.4 to show that this has no solution for x prime when we have $y^2 = x^3 + 2$ and Theorem 3.1.8 to see when $y^2 = x^3 - 2$ that the solutions are given by $(x, y) = (3, \pm 5)$ (a solution we have already found). Now, assume that m is odd. Since we know that $p \geq 7$ a quick check locally at 3 shows that

$$(p^{n/3})^3 = 5^m \mp 2 \equiv 2 \mp 2 \pmod 3$$

so $p^n \equiv 0 \pmod 3$ or $p^n \equiv 1 \pmod 3$. The first case gives $p = 3$, a case we have already considered above, and so we must have that $(p^{n/3})^3 = 5^m + 2$ with m odd. Multiplying by 5^3 gives $(5p^{n/3})^3 = (5^{(m+3)/2})^2 + 2 \cdot 5^3$, that is, a solution to $y^2 = x^3 - 250$. A check with Theorem 3.1.8 shows that there are no $\{2, 5, \infty\}$ solutions.

Case 3c: $P_{\min}(n) \geq 5$**.** This gives $p^n = 5^m \mp 2$. If we think of this as a solution $(x, y, z) = (1, \mp 1, p)$ to $5^m x^n + 2y^n = z^n$ for a prime $n \geq 3$, then we can use Theorem 1.6.1 to show that we have no solutions.

Case 4: $\ell = 1$**.** Here we have locally at 8 that

$$d^2 \equiv 1 + 2^\ell 5^m p^n \equiv \begin{cases} 3 \pmod 8 & \text{if either } n \text{ is even or } p \equiv 1, 5 \pmod 8 \\ 7 \pmod 8 & \text{if } n \text{ is odd and } p \equiv 3, 7 \pmod 8 \end{cases}$$

holding since $2 \cdot 5^m \equiv 2 \pmod 8$ always. This is a contradiction since odd squares modulo 8 are congruent to 1.

Case 5: $\ell = 2$**.** If $\ell = 2$, then notice that $4 \cdot 5^m \equiv 4 \pmod 8$ and that $4p^n \equiv 4 \pmod 8$. Hence we have that $1 + 2^l 5^m p^n \equiv 5 \pmod 8$ always, a contradiction.

Case 6: $\ell \geq 6$**,** $P_{\min}(n) \geq 7$**.** If $\ell \geq 6$, then using Theorem 1.6.4, we see that there are no solutions in this case.

Case 7: $3 \mid n$**.** Here, we have the equation $d^2 = 2^\ell 5^m (p^{n/3})^3 + 1$. Let $\ell = 3L + \lambda$ and $m = 3M + \mu$ where $\lambda, \mu \in \{0, 1, 2\}$ and L, M are nonnegative integers. Rewriting the equation gives

$$d^2 = 2^\lambda 5^\mu (2^L 5^M p^{n/3})^3 + 1.$$

Multiplying through by $2^{2\lambda}$ and $5^{2\mu}$ gives

$$(2^\lambda 5^\mu d)^2 = (2^{L+\lambda}5^{M+\mu}p^{n/3})^3 + 2^{2\lambda}5^{2\mu}$$

Thus it suffices to look up all $\{2,5,\infty\}$-integer points on elliptic curves with the above form. This is done in Section 3.1. A quick check on the tables shows that the only entry that has an x-coordinate of the form $x = 2^{L+\lambda}5^{M+\mu}p^{n/3}$ and the constant term of the form $2^{2\lambda}5^{2\mu}$ corresponds to the solution

$$(25 \cdot 26)^2 = (25 \cdot 3)^3 + 2^0 \cdot 5^4.$$

This corresponds to

$$(d, \ell, m, n, p) = (26, 0, 2, 3, 3)$$

which is a solution we already have found since $p = 3$.

Case 8: $5 \mid n$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

Case 9: $\ell \geq 3$**,** $m, n \geq 1$ **and one of** $2 \mid n$ **or** $\ell = 3, 4, 5$ **with** $P_{\min}(n) \geq 7$ **or** $n = 1$. We rearrange the equation to $d^2 - 1 = 2^\ell 5^m p^n$ and factor the left hand side to see that

$$(d-1)(d+1) = d^2 - 1 = 2^\ell 5^m p^n.$$

This leads to the following possible situations

$$\begin{cases} d \mp 1 = 2^{\ell-1} \\ d \pm 1 = 2 \cdot 5^m p^n \end{cases} \quad \begin{cases} d \mp 1 = 2^{\ell-1} p^n \\ d \pm 1 = 2 \cdot 5^m \end{cases} \quad \begin{cases} d \mp 1 = 2^{\ell-1} 5^m \\ d \pm 1 = 2 \cdot p^n \end{cases} \quad \begin{cases} d \mp 1 = 2^{\ell-1} 5^m p^n \\ d \pm 1 = 2. \end{cases}$$

The last case has no such solutions as m and p are positive. Eliminating d in each of the first 3 cases gives the equations

i. $\pm 1 = 5^m p^n - 2^{\ell-2}$.

ii. $\pm 1 = 5^m - 2^{\ell-2} p^n$.

iii. $\pm 1 = p^n - 2^{\ell-2} 5^m$.

Now we divide into subcases

Case 9a: n **is even.**

i. For this case, rewrite the equation as $2^{\ell-2} \pm 1 = 5^m (p^{n/2})^2$. Using Theorem 1.6.2, we get a contradiction when $\ell \geq 6$. Hence, we have that $\ell = 3, 4, 5$.

In these cases, the only solution with $n \geq 2$ even is given by $(p, \ell, m, d, n) = (3, 5, 0, 17, 2)$.

ii. For this case, rewrite the equation as $2^{\ell-2}p^n = 5^m \mp 1$ which gives a solution to the equation $Cz^2 = x^m + y^m$ where $C \in \{1, 2\}$ (possible grouping extra powers of 2 inside z). Theorem 1.6.2 implies that $m < 4$. Since $m > 0$, and n is even, a quick check of the 3 possible values of n shows that we have $n = 1$ in all admissible cases, contradicting this case.

iii. For this case, if $p^n = 2^{\ell-2}5^m - 1$, then if $\ell - 2 \geq 3$, we have that $p^n \equiv -1 \pmod 8$, a contradiction since n is even. If $\ell = 4$, then we get that $p^n \equiv 3 \pmod 8$ which is also a contradiction. This leaves the case when $\ell = 3$. In this case, a result of Cohn [Coh96] shows us that we have no solutions when $m > 2$. For $m \leq 2$, we get solutions given by

$$(d, \ell, m, n, p) \in \{(19, 3, 1, 2, 3), (99, 3, 2, 2, 7)\}.$$

Now, if $p^n = 2^{\ell-2}5^m + 1$, we move the 1 to the other side and factor to see that

$$(p^{n/2} - 1)(p^{n/2} + 1) = 2^{\ell-2}5^m.$$

Since the greatest common divisor on the left is 2, we see that when $\ell = 3$ we have a contradiction. Thus $\ell \geq 4$ and further, we are in one of the following cases

$$\begin{cases} p^{n/2} \mp 1 = 2 \cdot 5^m \\ p^{n/2} \pm 1 = 2^{\ell-3} \end{cases} \qquad \begin{cases} p^{n/2} - 1 = 2 \\ p^{n/2} + 1 = 2^{\ell-3}5^m. \end{cases}$$

In the second case, it is clear that the only solution comes when $(d, \ell, m, n, p) = (17, 5, 0, 2, 3)$. In the first case, eliminating the p factor gives $5^m - 2^{\ell-4} = \pm 1$ and Mihăilescu's Theorem (Theorem 3.3.8) implies that either $m = 1$ and $\ell = 6$ or that $m = 0$ and $\ell = 5$. In these cases, we have the solutions given by

$$(d, \ell, m, n, p) \in \{(161, 6, 1, 4, 3), (17, 5, 0, 2, 3)\}.$$

Case 9b: $\ell = 3, 4, 5$ and $P_{\min}(n) \geq 7$.

i. For this case, plugging in $\ell = 3, 4, 5$ immediately shows that there are no solutions with $n \geq 3$.

ii. In this case, notice that $\pm 1 = 5^m - 2p^n$ can be handled by Theorem 1.6.1 to show that the only solution to this equation is given by $-1 = 5^0 - 2p^0$. When $\ell = 4$ or 5, if $-1 = 5^m - 2^\ell p^n$, then we have modulo 4 that $-1 \equiv 1 \pmod 4$

which is a contradiction. So we may suppose that we are in the case where $1 = 5^m - 4p^n$ or $1 = 5^m - 8p^n$. For the latter note that modulo 8, we have that $1 \equiv 5^m \pmod 8$ and so we get that m is even. Factoring gives $8p^n = (5^{m/2} - 1)(5^{m/2} + 1)$ where the factors on the right have a greatest common divisor of 2 and so we have one of the following cases

$$\begin{cases} 5^{m/2} \pm 1 = 2p^n \\ 5^{m/2} \mp 1 = 4 \end{cases} \qquad \begin{cases} 5^{m/2} \pm 1 = 4p^n \\ 5^{m/2} \mp 1 = 2. \end{cases}$$

Subtracting pairwise shows that either $\pm 1 = p^n - 3$ or $\pm 1 = 2p^n - 1$ giving that either p is even, a contradiction or that $n = 0$ in the latter case which also leads to a contradiction.

This leaves the case $1 = 5^m - 4p^n$. Modulo 8 gives $5 \equiv 5^m \pmod 8$ and this shows that m is odd. This leaves the situation mentioned in the statement.

iii. As above, notice that $\pm 1 = p^n - 2 \cdot 5^m$ can be handled by Theorem 1.6.1 to show that the only solutions to this equation are given when $P_{\min}(n) < 5$. The equation $\pm 1 = p^n - 4 \cdot 5^m$ can be made to look like a solution to $x^n + y^n = Cz^2$ with $C = 1$ or 5. Thus by Theorem 1.6.2, we see that this has no solutions. Lastly, the equation $\pm 1 = p^n - 8 \cdot 5^m$ can be made to look like $x^n + y^n = 5^m z^3$ which also has no solutions via Theorem 1.6.6.

Case 9c: $n = 1$**.**

i. In this case, we have that $\pm 1 = 5^m p - 2^{\ell-2}$. Modulo 5 considerations gives $\mp 1 = 2^{\ell-2} \pmod 5$ and this shows that ℓ is even. In the -1 case, we have that $5^m p = (2^{(\ell-2)/2} - 1)(2^{(\ell-2)/2} + 1)$ and so factoring gives $2^{(\ell-2)/2} \pm 1 = 5^m$ and $2^{(\ell-2)/2} \mp 1 = 5^m$ which leads to $p = 5^m \mp 2$. The other case gives $p = \frac{2^{\ell-2}+1}{5^m}$ and $d = 2^{\ell-1} + 1$.

ii. In the case where $1 = 5^m - 2^{\ell-2}p$, if $\ell = 3$, then modulo 4 considerations gives $1 \equiv 1 + 2 \pmod 4$ a contradiction. If $\ell = 4$, then we get solutions given by $p = \frac{5^m - 1}{4}$. Lastly, if $\ell \geq 5$, then modulo 8 considerations show that m is even. Rearranging the equation and factoring gives

$$2^{\ell-2}p = (5^{m/2} - 1)(5^{m/2} + 1).$$

This gives the cases

$$\begin{cases} 5^{m/2} \pm 1 = 2p \\ 5^{m/2} \mp 1 = 2^{\ell-3} \end{cases} \qquad \begin{cases} 5^{m/2} \pm 1 = 2^{\ell-3}p \\ 5^{m/2} \mp 1 = 2. \end{cases}$$

Considerations modulo 4 reduce the above to

$$\begin{cases} 5^{m/2}+1=2p \\ 5^{m/2}-1=2^{\ell-3} \end{cases} \qquad \begin{cases} 5^{m/2}-1=2^{\ell-3}p \\ 5^{m/2}+1=2. \end{cases}$$

The second case above is impossible since $m>0$. In the remaining case, we see that the second equation reads $1=5^{m/2}-2^{\ell-3}$ and so by Mihăilescu's Theorem (Theorem 3.3.8) we have that $m=2$, $\ell=5$ and $p=3$.

In the case where $-1=5^m-2^{\ell-2}p$, if $\ell\geq 4$, then we get a contradiction by considerations modulo 4. If $\ell=3$, then we get the solutions given by $p=\frac{5^m+1}{2}$, $d=4p-1$.

iii. Here we have $p=2^{\ell-2}5^m\pm 1$ with $d=2p\mp 1$.

(b) **Case 1:** $m=0$ **or** $n=0$**.** This is done in Ivorra's thesis (see Theorem 3.3.2) to give the solutions as stated.

Case 2: $\ell\geq 3$ Modulo 8 gives $d^2\equiv -1 \pmod 8$ which has no solutions.

Case 3: $\ell=2$. Locally at 8, we have

$$-1+2^\ell 5^m p^n \equiv -1+4\cdot 5^m p^n \equiv 3 \pmod 8,$$

a contradiction. Thus there is no solution when $\ell=2$.

Case 4: $\ell\leq 1$. There is little we can say in this case other than that solutions do in fact exist.

Theorem 3.4.2. *Let $p\neq 2,5$ be a prime number with $\ell,m,n\geq 0$ and $d\geq 1$.*

1. *Solutions to $d^2-2^\ell p^n=5^m$ are given by*

   (a) $n=0$ *and* $(d,\ell,m,p)\in\{(3,3,0,p),(3,2,1,p)\}$.

   (b) $n=1$ *and*

   a) $m=0$ *with* $(d,\ell,p)\in\{(2,0,3),(5,3,3),(7,4,3),(2p-1,\ell,2^{\ell-2}+1),(2p+1,\ell,2^{\ell-2}-1)\}$ *with* $\ell\geq 5$ *in the last two cases.*

   b) $m>0$, $\ell=0$ *and* $p\equiv 3 \pmod 4$.

   c) $m>0$ *is odd,* $\ell=2$ *and* $p=\frac{d^2-5^m}{4}$.

   d) $m>0$ *even,* $\ell=3$ *and* $p=\frac{5^{m/2}+1}{2}$.

e) $m > 0$ *even,* $\ell \geq 3$ *and* $p = 2^{\ell-2} \pm 5^{m/2}$ *with* $d = 2^{\ell-1} \pm 5^{m/2}$ *and both signs the same.*

(c) $n = 2$ *and*

i. $(d, \ell, m, p) = (\frac{5^m+1}{2}, 2, m, \frac{5^m-1}{4})$ *and* m *is odd.*

ii. $(d, \ell, m, p) \in \{(17, 5, 0, 3)\}$.

(d) $2 \parallel n$ *and* $4p^{n/2} = 5^m - 1$ *with* m *odd,* $\ell = 2$ *and either* $n = 2$ *or* $P_{\min}(n/2) \geq 7$.

(e) $n = 3$ *and* $(d, \ell, m, p) \in \{(29, 3, 4, 3), (59, 7, 2, 3), (73, 2, 1, 11)\}$.

(f) $n = 4$ *and* $(d, \ell, m, p) = (129, 4, 3, 11)$.

(g) $P_{\min}(n) \geq 7$, $m \geq 1$ *and*

a $\ell = 0$ *with* $p \equiv 3 \pmod 4$.

b $\ell = 2$ *with* $p^n = \frac{d^2-5^m}{4}$ *and* m *odd.*

c $\ell = 3$ *with* $p^n = \frac{5^{m/2}+1}{2}$ *and* m *even.*

d $\ell \in \{4, 5\}$ *with* $p^n = 2^{\ell-2} \pm 5^{m/2}$ *and* m *even.*

2. *Solutions to* $d^2 + 2^\ell p^n = 5^m$ *are given by*

(a) $n = 0$ *and* $(d, \ell, m, p) \in \{(11, 2, 3, p), (3, 4, 2, p)\}$.

(b) $n = 1$ *and*

a) $(d, \ell, m, p) = (23, 5, 4, 3)$.

b) $p = 5^m - d^2$ *and* $\ell = 0$.

c) $p = \frac{5^m-d^2}{4}$ *and* $\ell = 2$.

d) $(d, \ell, m, p) = (\pm(5^{m/2} - 2^{\ell-1}), \ell, m, 5^{m/2} - 2^{\ell-2})$ $\ell \geq 3$ *and* $m \geq 2$ *even.*

e) $p = \frac{5^{m/2}-1}{4}$, $d = 5^{m/2} - 2$ *and* $\ell = 4$ *with* $m \geq 2$ *even.*

(c) $n \geq 2$ *is even and* $\ell = 0$ *with* m *even and* $p^n = 2 \cdot 5^{m/2} - 1$.

(d) $n \geq 2$ *is even and* $\ell \in \{0, 2\}$ *with* m *odd.*

(e) $n = 2$ *and* $(d, \ell, m, p) = (117, 4, 6, 11)$.

(f) $P_{\min}(n) \geq 7$ *and* $0 \leq \ell \leq 5$ *and* $m \geq 1$.

3. *Solutions to* $d^2 + 5^m = 2^\ell p^n$ *are*

(a) $n = 0$ *and* $(d, \ell, m, p) = (1, 1, 0, p)$.

(b) $n = 1$, $\ell = 0$ *and* $p \equiv 1 \pmod 4$.

(c) $n = 1$ *and* $\ell = 1$.

(d) $n = 2$, $\ell = 0$, $p = \frac{5^m+1}{2}$, $d = p - 1$.

(e) $n = 2$, $\ell = 1$ *and* $m = 0$ *with* $p \equiv 1 \pmod 4$ *and* $p \neq 13$.

(f) $n = 3$ *and* $(d, \ell, m, p) \in \{(7, 1, 1, 3), (99, 1, 2, 17)\}$.

(g) $n = 4$ *and* $(d, \ell, m, p) = (239, 1, 0, 13)$.

(h) $n = 5$ *and* $(d, \ell, m, p) \in \{(19, 1, 3, 3), (183, 1, 3, 7)\}$.

Proof. 1. **Case 1:** $n = 0$ **or** $m = 0$**.** This is done in Ivorra's thesis. If $n = 0$, we look up Theorem 3.3.4 for solutions to $d^2 - 2^\ell = 5^m$. This gives solutions when $m = 0$ or $m = 1$. When $m = 0$, we use Mihăilescu's Theorem (Theorem 3.3.8) to get the only solution of $(d, \ell, m) = (3, 3, 0)$. When $m = 1$, we see that ℓ must be even via modulo 5 considerations and so the left hand side factors to give the equations

$$\begin{cases} d - 2^{\ell/2} = 1 \\ d + 2^{\ell/2} = 5. \end{cases}$$

Subtracting these two equations gives $2^{\ell/2+1} = 4$ and so $\ell = 2$. This gives another solution given by $(d, \ell, m) = (3, 2, 1)$.

When $m = 0$ and $n > 0$, via Theorem 3.3.1 (recalling that $p \neq 5$), we get the solutions mentioned in the theorem. For the duration of this proof, we suppose that $m, n > 0$.

Case 2: $3 \mid n$**.** If $\ell \equiv 0 \pmod 3$ then $(x, y) = (2^{\ell/3} p^{n/3}, d)$ is a solution to $y^2 = x^3 + 5^m$. Using Theorem 3.1.2, we have that the only solution of this shape that arises is when $(x, y) = (6, \pm 29)$ and this gives $(d, \ell, m, n, p) = (29, 3, 4, 3, 3)$.

If $\ell \equiv 1 \pmod 3$ then $(x, y) = (2^{(\ell+2)/3} p^{n/3}, 2d)$ is a solution to $y^2 = x^3 + 2^2 5^m$. Using Theorem 3.1.2, we have that the only solution of this shape that arises is when $(x, y) = (24, \pm 118)$ and this gives $(d, \ell, m, n, p) = (59, 7, 2, 3, 3)$.

If $\ell \equiv 2 \pmod 3$ then $(x, y) = (2^{(\ell+4)/3} p^{n/3}, 4d)$ is a solution to $y^2 = x^3 + 2^4 5^m$. Using Theorem 3.1.2, we have that the only solution of this shape that arises is when $(x, y) = (44, \pm 292)$ and this gives $(d, \ell, m, n, p) = (73, 2, 1, 3, 11)$.

Case 3: $5 \mid n$. Checking with Theorem 3.2.11, we see that this case gives no solutions.

Case 4: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$. Using the modular method of Theorem 1.6.5, we can show that this equation has no solutions.

Case 5: n **even.** We break this into subcases.

Case 5a: $\ell = 0$**.** In this case, we have $d^2 - p^n = 5^m$. Notice that d must be even since p is odd and so considerations modulo 4 give $-1 \equiv 1 \pmod 4$, a contradiction.

Case 5b: $\ell = 1$**.** In this case, we have $d^2 - 2p^n = 5^m$. Considerations modulo 5 give $d^2 \equiv 2p^n \pmod 5$. Since n is even, we know that 2 must be a square modulo 5, a contradiction.

Case 5c: $\ell = 2$**.** Local considerations at 8 give us that

$$d^2 = 2^\ell p^n + 5^m \equiv 4 + 5^m \pmod 8$$

and this value is either 1 or 5 depending on if m is odd or even. If m is even, then we get $d^2 \equiv 5 \pmod 8$ which is a contradiction. Hence m is odd. Thus, let $m = 2k + 1$ and $j = n/2$. Factoring gives

$$5^m = d^2 - 4p^{2j} = (d - 2p^j)(d + 2p^j).$$

As $\gcd(d - 2p^j, d + 2p^j) = 1$, we have that

$$\begin{aligned} d + 2p^j &= 5^m \\ d - 2p^j &= 1. \end{aligned}$$

Subtracting these two equations gives $4p^j = 5^m - 1$. If $4 \mid n$, then j is also even and hence the above gives rise to a solution to $z^2 = x^m + y^m$. By Theorem 1.6.2, we know that this implies that $m < 4$. Checking values of $m = 1$ and $m = 3$ shows that $m = 3$ gives rise to $p = 31$ and $j = 1$ contradicting that j was even.

If $2 \parallel n$, then we get $4p^{n/2} = 5^m - 1$. Modulo 8 considerations shows that m is odd.

Case 5d: $\ell \geq 3$**.** Local considerations at 8 give us that

$$1 \equiv d^2 = 2^\ell p^n + 5^m \equiv 5^m \pmod 8$$

and so, we see that m must be even. Now, considerations at 3 show us that

$$d^2 = 2^\ell p^n + 5^m \equiv 2^\ell + 1 \pmod 3.$$

Thus, ℓ has to be odd (as 2 is a quadratic non-residue modulo 3). Next, modulo 5 gives

$$d^2 = 2^\ell p^n \equiv 2 \cdot (2^{(\ell-1)/2} p^{n/2})^2 \pmod 5$$

and so once again, we see that 2 is a square modulo 5 which is a contradiction.

Case 6: $n = 1$ **or** $P_{\min}(n) \geq 7$**.** When $\ell = 0$, d is even and so modulo 4 considerations show that $p \equiv 3 \pmod 4$. When $\ell = 1$, we see that $d^2 - 2p^n = 5^m$. Reducing modulo 4 yields that $d^2 \equiv 3 \pmod 4$ and this is a contradiction. When $\ell = 2$, then we have $d^2 = 5^m + 4p^n \equiv 5^m + 4 \pmod 8$ showing that m is odd since 5 is not a square modulo 8. Lastly, if $\ell \geq 3$, then m is even by reducing modulo 8 and thus we can factor giving $(d - 5^{m/2})(d + 5^{m/2}) = 2^\ell p^n$. This gives the following cases

$$\begin{cases} d - 5^{m/2} = 2 \\ d + 5^{m/2} = 2^{\ell-1} p^n \end{cases} \qquad \begin{cases} d \mp 5^{m/2} = 2p^n \\ d \pm 5^{m/2} = 2^{\ell-1}. \end{cases}$$

In the first case, eliminating d yields $5^{m/2} = 2^{\ell-2} p^n - 1$. When $\ell = 3$, This gives $p^n = \frac{5^{m/2}+1}{2}$ which is a potential solution. When $\ell \geq 4$, modulo 4 considerations give a contradiction. In the second case, eliminating gives $\pm 5^{m/2} = 2^{\ell-2} - p^n$. The case when $\ell = 3$ is solved via Theorem 1.6.1 and the other cases are included in the theorem.

2. **Case 1:** $m = 0$ **or** $n = 0$ If $m = 0$ then we immediately see we have no solution since d is positive. If $n = 0$, then from Ivorra's thesis (see Theorem 3.3.3), we see that the only solutions are given by

$$(d, \ell, m) \in \{(3, 4, 2), (11, 2, 3)\}.$$

From now on, assume that $m > 0$ and $n > 0$.

Case 2: $3 \mid n$

If $\ell \equiv 0 \pmod 3$ then $(x, y) = (-2^{\ell/3} p^{n/3}, d)$ is a solution to $y^2 = x^3 + 5^m$.

If $\ell \equiv 1 \pmod 3$ then $(x, y) = (-2^{(\ell+2)/3} p^{n/3}, 2d)$ is a solution to $y^2 = x^3 + 2^2 5^m$.

If $\ell \equiv 2 \pmod 3$ then $(x, y) = (-2^{(\ell+4)/3} p^{n/3}, 4d)$ is a solution to $y^2 = x^3 + 2^4 5^m$.

Using Theorem 3.1.2, we see that all the solutions which have a negative x-coordinate are not integer solutions (there is one $\{2, 5, \infty\}$-integer solution with constant term $2^{2+6n} \cdot 5^3$ but this does not translate to a solution) and so these cases do not give a solution.

Case 3: $5 \mid n$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

Case 4: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$**.** This is shown to have no solutions via Theorem 1.6.5.

Case 5: n **even.** We break this up into subcases

Case 5a: ℓ **odd.** Here modulo 5 considerations gives $d^2 = -2^\ell p^n \pmod 5$. Since $-2 \equiv 3 \pmod 5$ is a non-quadratic residue, this gives a contradiction and hence no solutions for this case.

Case 5b: ℓ **even**. If $\ell = 0$, then if m is even, we can factor to get that

$$d \mp 5^{m/2} = -1$$
$$d \pm 5^{m/2} = p^n$$

and eliminating d yields $2 \cdot 5^{m/2} = p^n - 1$ which is included in the theorem. If $\ell = 2$, then modulo 8 considerations shows that m is odd. In this situation, there are many possible solutions.

Now, if $\ell \geq 4$, modulo 8 considerations gives m even. Isolating and factoring gives the cases

$$\begin{cases} d - 5^{m/2} = -2 \\ d + 5^{m/2} = 2^{\ell-1}p^n \end{cases} \qquad \begin{cases} d - 5^{m/2} = -2^{\ell-1} \\ d + 5^{m/2} = 2p^n \end{cases} \qquad \begin{cases} d - 5^{m/2} = -2p^n \\ d + 5^{m/2} = 2^{\ell-1}. \end{cases}$$

Eliminating for d in the first case gives $5^{m/2} = 2^{\ell-2}p^n + 1$ and in the last two cases gives $5^{m/2} = p^n + 2^{\ell-2}$.

In the case where $5^{m/2} = 2^{\ell-2}p^n + 1 = (2^{(\ell-2)/2}p^{n/2})^2 + 1$, we have no solutions via Mihăilescu's Theorem (Theorem 3.3.8).

In the case where $5^{m/2} = p^n + 2^{\ell-2}$, when $\ell = 4$, we get the only admissible solution via [Coh03] to be $(d, \ell, n, m, p) = (117, 4, 2, 6, 11)$. When $\ell \geq 6$, we get that by looking modulo 8, we see that $m/2$ is also even. Hence factoring gives

$$(5^{m/4} - p^{n/2})(5^{m/4} + p^{n/2}) = 2^{\ell-2}$$

which in turn gives the cases

$$\begin{cases} 5^{m/4} - p^{n/2} = 2 \\ 5^{m/4} + p^{n/2} = 2^{\ell-3}. \end{cases}$$

Eliminating for p gives $5^{m/4} = 2^{\ell-4} - 1$ and so $1 = 2^{\ell-4} - 5^{m/4}$. Mihăilescu's Theorem (Theorem 3.3.8) implies that $\ell - 4 = 0$ (since ℓ is even) and this gives a contradiction. Thus there are no solutions in this case.

Case 6: $n = 1$**.** If $\ell = 0$, then we can only say $p = 5^m - d^2$. If $\ell = 1$ then modulo 4 considerations gives $d^2 \equiv 5^m - 2p \equiv 1 - 2 \equiv -1 \pmod 4$ which is a contradiction. When $\ell = 2$, then we can only say that $d^2 = 5^m - 4p$. When $\ell \geq 3$, modulo 8 considerations show that m is even. Just as in the case 5b above, we can factor to give $(d - 5^{m/2})(d + 5^{m/2}) = 2^\ell p$ leading to

$$\begin{cases} d - 5^{m/2} = -2 \\ d + 5^{m/2} = 2^{\ell-1}p \end{cases} \qquad \begin{cases} d - 5^{m/2} = -2^{\ell-1} \\ d + 5^{m/2} = 2p \end{cases} \qquad \begin{cases} d - 5^{m/2} = -2p \\ d + 5^{m/2} = 2^{\ell-1}. \end{cases}$$

Eliminating for d in the first case gives $5^{m/2} = 2^{\ell-2}p + 1$ and in the last two cases gives $5^{m/2} = p + 2^{\ell-2}$. The second case gives $p = 5^{m/2} - 2^{\ell-2}$. The first case needs to be broken into more cases. When $\ell = 3$, we get a contradiction by looking modulo 4. When $\ell = 4$, we get $p = \frac{5^{m/2}-1}{4}$ and we can say nothing more. When $\ell \geq 5$, modulo 8 considerations give $m/2$ is even and so factoring gives $(5^{m/4} - 1)(5^{m/4} + 1) = 2^{\ell-2}p$. This leads to

$$\begin{cases} 5^{m/4} \mp 1 = 2p \\ 5^{m/4} \pm 1 = 2^{\ell-3}. \end{cases}$$

Looking at the second equation, Mihăilescu's Theorem (Theorem 3.3.8) implies that of the equations

$$5^{m/4} + 1 = 2^{\ell-3}$$
$$5^{m/4} - 1 = 2^{\ell-3}$$

only the second admits a solution given by $m = 4$ and $\ell = 5$. This gives $p = 3$ in the first equation and thus the solution given by

$$(d, \ell, n, m, p) = (23, 5, 1, 4, 3).$$

This completes this case.

3. **Case 1:** $m = 0$ **or** $n = 0$ If $m = 0$, then Theorem 3.3.2 shows that either $(d, \ell, n, p) = (1, 1, 0, p)$, $p = 13$ and $(d, \ell, n) \in \{(5, 1, 1), (239, 1, 4)\}$ or that $p \equiv 1 \pmod 4$, $p \neq 13$ and $(\ell, n) \in \{(0, 1), (1, 1), (1, 2)\}$.

   If $n = 0$ and $m > 0$, then a check with Theorem 3.3.5 shows that $m = 1$ and $\ell < 435 + 10 \log_2(5) \leq 500$. Checking with MAGMA for squares of the form $2^\ell - 5$ quickly yields no results for $\ell \in \{1, 2, ..., 500\}$ (we could also refer to [Coh03] to see this has no solutions). Thus, throughout suppose that $n > 0$ and $m > 0$.

   Case 2: $\ell \geq 3$

   Here, we have

$$d^2 = -5^m + 2^l p^n \equiv \begin{cases} -5 \pmod 8 & \text{if } m \equiv 1 \pmod 2 \\ -1 \pmod 8 & \text{if } m \equiv 0 \pmod 2 \end{cases}$$

   which is a contradiction since -1 and -5 are not squares modulo 8.

   Case 3: $\ell = 2$

   If $\ell = 2$, then

$$\begin{aligned} d^2 = -5^m + 2^l p^n &\equiv \begin{cases} -5 \pmod 8 & \text{if } m \equiv 1 \pmod 2 \\ -1 \pmod 8 & \text{if } m \equiv 0 \pmod 2 \end{cases} + \begin{cases} 4p \pmod 8 & \text{if } n \equiv 1 \pmod 2 \\ 4 \pmod 8 & \text{if } n \equiv 0 \pmod 2 \end{cases} \\ &\equiv \begin{cases} -1 \pmod 8 & \text{if } m \equiv 1 \pmod 2 \\ 3 \pmod 8 & \text{if } m \equiv 0 \pmod 2. \end{cases} \end{aligned}$$

   Since $4p \equiv 4 \pmod 8$ for any odd prime. Again we have a contradiction since neither -1 nor 3 are squares modulo 8.

   Case 4: $\ell = 1$

   When $n \geq 3$, the solutions are given by theorems 1 and 3 of [AMLST09] (valid since $\gcd(d, p) = 1$ resulting from $p \neq 5$) to be

$$(d, \ell, m, n, p) \in \{(7, 1, 1, 3, 3), (99, 1, 2, 3, 17), (239, 1, 0, 4, 13), (19, 1, 3, 5, 3), (183, 1, 3, 5, 7)\}.$$

   If $n = 2$, then since $m > 0$, we have that modulo 5 considerations give $d^2 \equiv 2p^2 \pmod 5$ which is a contradiction since 2 is a quadratic non-residue.

If $\ell = 1$ and $n = 1$, there are many solutions. If $\ell = 1$ and $n = 0$, then the equation becomes $d^2 + 5^m = 2$ which only has the solution $d = 1$ and $m = 0$.

Case 5: $\ell = 0$

When $\ell = 0$, the solutions are given by theorem 1 of [PR11] when $n \geq 3$ and there are no such solutions. When $n = 2$, we have $5^m = p^2 - d^2 = (p-d)(p+d)$. Since d is even, we know that $\gcd(p-d, p+d) = \gcd(p-d, 2p) = 1$ and so this gives the equations

$$\begin{cases} p - d = 1 \\ p + d = 5^m \end{cases}$$

and hence $p = \frac{5^m+1}{2}$, a case included in the theorem. When $n = 1$, this gives $p = d^2+5^m$. Hence d is even and so $p \equiv 1 \pmod 4$.

■

Theorem 3.4.3. *Let $p \neq 2, 5$ be a prime number with $\ell, m, n \geq 0$ and $d \geq 1$.*

1. *Solutions to $d^2 - 2^\ell 5^m = p^n$ are given by*
   - *(a) $n = 0$ and $(d, \ell, m) \in \{(3, 3, 0), (9, 4, 1)\}$.*
   - *(b) $n = 1$, $m = 0$ and $\ell < 435 + 10 \log_2(p)$.*
   - *(c) $n = 1$ and $m > 0$.*
   - *(d) $n = 2$ and*
     - *a) $(d, \ell, p) = (p + 2, \ell, 2^{\ell-2} - 1)$ with $\ell \geq 4$.*
     - *b) $p = 2^{\ell-2} - 5^m$, $d = 2^{\ell-1} - p$ and $\ell \geq 3$.*
     - *c) $p = 5^m - 2^{\ell-2}$, $d = 2^{\ell-1} + p$ and $\ell \geq 3$.*
     - *d) $p = 2^{\ell-2} \cdot 5^m - 1$, $d = p + 2$ and $\ell \geq 3$.*
     - *e) $(d, \ell, m, p) = (13, 5, 1, 3)$.*
   - *(e) $2 \parallel n$, m is odd, $\ell = 4$ and p satisfies $p^{n/2} = 5^m - 4$.*
   - *(f) $n = 3$ and $(d, \ell, m, p) \in \{(299, 12, 1, 41), (71, 7, 0, 17), (411, 5, 5, 41)\}$.*
   - *(g) $n = 4$ and $(d, \ell, m, p) \in \{(41, 6, 2, 3), (11, 3, 1, 3), (51, 3, 2, 7), (129, 4, 3, 11)\}$.*
   - *(h) $n = 6$ and $(d, \ell, m, p) = (37, 7, 1, 3)$.*
   - *(i) $P_{\min}(n) \geq 7$ and $0 \leq \ell \leq 5$ and $m \geq 1$.*
2. *Solutions to $d^2 + p^n = 2^\ell 5^m$ are given by*

(a) $n = 0$ *and* $(d, \ell, m, p) \in \{(1, 1, 0, p), (13, 9, 3, 7)\}$.

(b) $n = 1$.

(c) $2 \mid n$ *and* $\ell = 0, 1$.

(d) $n = 3$ *and* $(d, \ell, m, p) \in \{(47, 8, 3, 31), (17, 9, 0, 7)\}$.

(e) $P_{\min}(n) \geq 7$ *and* $0 \leq \ell \leq 5$ *and* $m \geq 1$.

3. *Solutions to* $d^2 + 2^\ell 5^m = p^n$ *are given by*

(a) $n = 1$ *so* $p = d^2 + 2^\ell 5^m$.

(b) $n = 2$ *and*

a) $(d, \ell, m, p) = (p - 1, 0, m, \frac{5^m+1}{2})$.

b) $(d, \ell, m, p) = (\pm(p - 2^{\ell-1}), \ell, m, 5^m + 2^{\ell-2})$ *and* $\ell \geq 3$.

c) $(d, \ell, m, p) = (p - 2, \ell, m, 2^{\ell-2} \cdot 5^m + 1)$ *and* $\ell \geq 3$.

(c) $n = 3$ *and* $(d, \ell, m, p) \in \{(9, 1, 4, 11), (261, 5, 2, 41)\}$.

(d) $n = 4$ *and* $(d, \ell, m, p) = (1, 4, 1, 3)$.

(e) $n = 5$ *and* $(d, \ell, m, p) = (401, 1, 3, 11)$.

(f) $n = 6$ *and* $(d, \ell, m, p) = (23, 3, 2, 3)$.

(g) $n = 8$ *and* $(d, \ell, m, p) = (79, 6, 1, 3)$.

Proof. 1. **Case 1:** $m = 0$ **or** $n = 0$**.** When $m = 0$, we have via Theorem 3.3.4 that

(a) $n = 0$.

(b) $n = 1$ and $\ell < f(p) < 435 + 10 \log_2(p)$.

(c) $n = 2$ and $(d, \ell, p) = (p + 2, \ell, 2^{\ell-2} - 1)$ with $\ell \geq 4$.

(d) $n = 3$ and $(d, \ell, p) = (71, 7, 17)$.

If both $m = 0$ and $n = 0$, then Mihăilescu's Theorem (Theorem 3.3.8) implies that $\ell = 3$ and $d = 3$ is the only solution to $d^2 - 2^\ell = 1$.

If only $n = 0$, then we get two solutions via Theorem 3.3.1, namely

$$(d, \ell, m) \in \{(3, 3, 0), (9, 4, 1)\}$$

and the first one is discussed above. Thus throughout, suppose that $m, n > 0$.

Case 2: $3 \mid n$**.** Our equation is set up in the form $d^2 = (p^{n/3})^3 + 2^\ell 5^m$. Thus we want solutions to $y^2 = x^3 + 2^\alpha 5^\beta$ with the x coordinate a positive prime. A check on Theorem 3.1.4 reveals that these solutions are given by

$$(d, \ell, m, n, p) \in \{(299, 12, 1, 3, 41), (71, 7, 0, 3, 17), (37, 7, 1, 6, 3), (411, 5, 5, 3, 41)\}.$$

Case 3: $5 \mid n$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

Case 4: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$**.** Using the modular method of Theorem 1.6.5, we can show that this equation has no solutions.

Case 5: n **is even.** Suppose n is even, so $n = 2k$. Then if $\ell = 0$, we have

$$\begin{aligned} d^2 = p^{2k} + 5^m &\equiv 1 + \begin{cases} 5 & \text{if } m \equiv 1 \pmod 2 \\ 1 & \text{if } m \equiv 0 \pmod 2 \end{cases} \pmod 8 \\ &\equiv \begin{cases} 6 & \text{if } m \equiv 1 \pmod 2 \\ 2 & \text{if } m \equiv 0 \pmod 2 \end{cases} \pmod 8 \end{aligned}$$

which is a contradiction since neither are squares modulo 8. If $\ell = 1$, we have

$$d^2 = p^{2k} + 2 \cdot 5^m \equiv 1 + 2 \equiv 3 \pmod 8$$

which is a contradiction since 3 is not a square modulo 8. If $\ell = 2$, we have

$$d^2 = p^{2k} + 4 \cdot 5^m \equiv 1 + 4 \equiv 5 \pmod 8$$

which is a contradiction since 5 is not a square modulo 8. So hence we can assume that $\ell \geq 3$. Factoring gives

$$(d + p^k)(d - p^k) = 2^\ell 5^m.$$

Since $\gcd(d + p^k, d - p^k) = \gcd(d - p^k, 2d) = 2$, we have that

$$\begin{cases} d - p^k = 2 \\ d + p^k = 2^{\ell-1} 5^m \end{cases} \qquad \begin{cases} d \pm p^k = 2 \cdot 5^m \\ d \mp p^k = 2^{\ell-1} \end{cases}$$

where in the first case, we do not have the $d + p^k = 2$ case because this least to $k = 0$ and $d = 1$ which does not yield a solution.

Now in the first case, eliminating for d yields $2^{\ell-2} 5^m = p^k + 1$. Using the modularity method of Theorem 1.6.2 (where we think of $2^{\ell-2} 5^m = Cz^2$), we can see that $k \leq 3$.

The cases when $k = 0$ or 3 were solved already and so $k = 1$ or $k = 2$.

If $k = 2$, then $\ell = 3$ since otherwise modulo 8 considerations give a contradiction ($\ell = 4$ gives 3 is a square modulo 8 while $\ell \geq 5$ shows that -1 is a square modulo 8; both are contradictions). Now, rewriting the equation gives $-1 = p^2 - 2 \cdot 5^m$ which has no solutions when $m > 2$ by [Coh96]. When $m = 1$ or 2, we see that the only possible solutions come when $(d, \ell, m, n, p) = (11, 3, 1, 4, 3)$ or $(d, \ell, m, n, p) = (51, 3, 2, 4, 7)$. If $k = 1$, we get $p = 2^{\ell-2}5^m - 1$.

In the second case, we eliminate for d yielding $5^m \mp p^k = 2^{\ell-2}$. We break this into subcases.

Case 5a: $\ell \geq 6$. By the previous cases, we know that k is a power of 2 since no other primes divide n. Hence, considerations modulo 8 yield

$$p^k = \mp(2^{\ell-2} - 5^m) \equiv \pm 5^m \pmod 8.$$

Giving a contradiction unless m is even and the equation is $5^m - p^k = 2^{\ell-2}$. In this case, we factor the left hand side and see that

$$(5^{m/2} - p^{k/2})(5^{m/2} + p^{k/2}) = 2^{\ell-2}.$$

As $\gcd(5^{m/2} - p^{k/2}, 5^{m/2} + p^{k/2}) = \gcd(5^{m/2} - p^{k/2}, 2 \cdot 5^{m/2}) = 2$, we must have that

$$\begin{cases} 5^{m/2} + p^{k/2} = 2^{\ell-3} \\ 5^{m/2} - p^{k/2} = 2. \end{cases}$$

Eliminating $p^{k/2}$ in the above yields $5^{m/2} - 2^{\ell-4} = 1$ and Mihăilescu's Theorem (Theorem 3.3.8) says that the only solutions are when $m = 2$ and $\ell = 6$ giving $(d, \ell, m, n, p) = (41, 6, 2, 4, 3)$.

Case 5b: $\ell \leq 5$. In the case of $5^m + p^k = 2^{\ell-2}$, a quick inspection gives us that the only solution is when $\ell = 5$ with $m = k = 1$ and $p = 3$. This gives the solution $(d, \ell, m, n, p) = (13, 5, 1, 2, 3)$. In the case of $5^m - p^k = 2^{\ell-2}$, if $\ell = 3$, then Theorem 1.6.1 shows that only 2 and 3 can divide 5. We have already considered the case when $3 \mid k$ and so we suppose that k is even. Then modulo 5 considerations give us that $-p^k \equiv 2 \pmod 5$ which is a contradiction since -2 is not a quadratic residue modulo 5. If $\ell = 5$ then Theorem 1.6.7 tells us that only $2, 3$ or 5 may divide k. Since we have considered the case when $3, 5 \mid k$, we may suppose that k is even and the same argument as above gives a contradiction.

If $\ell = 4$ and k is even, the solutions to $x^2 + C = y^n$ with $C = 2, 4$, or 8 are given by [Coh03, Section 5] to be $(x, y, n, C) = (5, 3, 3, 2), (2, 2, 3, 4)$ and $(11, 5, 3, 4)$ (this offers an alternative proof to the above). For our purposes, we require that y is a power of 5 and so only the last solution is admissible in our setting.

Now, suppose k is odd. Thus looking modulo 4 tells us that $p \equiv 1 \pmod 4$. If m is even, then factoring $5^m - p^k = 4$ gives $(5^{m/2} - 2)(5^{m/2} + 2) = p^{n/2}$ and so $5^{m/2} - 2 = 1$ which is a contradiction. Hence m is odd.

2. **Case 1: $m = 0$ or $n = 0$.** If $m = 0$, then a check with Theorem 3.3.5 shows that $p = 7$ and $(d, \ell, m) = (13, 9, 3)$, $n = 0$ which contradicts [Coh03], or that $n = 1$ and ℓ is bounded by a constant depending on p.

   If $n = 0$ and $m > 0$, then Theorem 3.3.2 shows that $(\ell, n) \in \{(0, 1), (1, 1), (1, 2)\}$. We assume that $n, m > 0$ from now on.

   Case 2: $2 \mid n$. If $\ell = 0$ or $\ell = 1$, then there is little to say. If $\ell \geq 2$, then modulo 4, we see that
   $$1 + 1 \equiv d^2 + p^n \equiv 2^\ell 5^m \equiv 0 \pmod 4$$
   and this is a contradiction.

   Case 3: $3 \mid n$. Our equation becomes $d^2 = (-p^{n/3})^3 + 2^\ell 5^m$. So we use Theorem 3.1.4 to see that we get two solutions given by
   $$(d, \ell, m, p) \in \{(47, 8, 3, 31), (17, 9, 0, 7)\}.$$

   Case 4: $5 \mid n$. Checking with Theorem 3.2.11, we see that this case gives no solutions.

   Case 5: $P_{\min}(n) \geq 7$. In this case, using Theorem 1.6.4, we see that $\ell \leq 5$.

3. **Case 1: $n \geq 3$.** This is a result of [LT08, Theorem 1.1] if either $\ell > 0$ or $m > 0$ and gives solutions as stated in the following table.

α	β	x	y	n
1	4	9	11	3
3	2	23	9	3
5	2	261	41	3
7	6	383	129	3
9	2	17771	681	3
4	1	1	3	4
6	1	79	9	4
1	3	401	11	5
3	2	23	3	6
6	1	79	3	8

Table 3.20: Integer solutions to $x^2 + 2^\alpha 5^\beta = y^n$ with $x, y \geq 1$, $\gcd(x, y) = 1$ and $n \geq 3$ with $\alpha, \beta > 0$.

If $\ell = 0$ then Theorem 1 of [PR11] tells us that the equation has no solutions. If $m = 0$, then papers by [Coh92],[AAM01] and/or [Sik03] give the solutions to $x^2 + 2^k = y^n$ as

$$\begin{aligned}(x, y, k, n) \in \{&(5 \cdot 2^{3\alpha}, 3 \cdot 2^{2\alpha}, 6\alpha + 1, 3), (7 \cdot 2^{2\alpha}, 3 \cdot 2^{\alpha}, 4\alpha + 5, 4),\\ &(11 \cdot 2^{5\alpha+3}, 3 \cdot 2^{\alpha+1}, 10\alpha + 5, 5), (2^{\alpha}, 2^{2\alpha+1}, 6\alpha + 1, n),\\ &(11 \cdot 2^{3\alpha}, 5 \cdot 2^{2\alpha}, 6\alpha + 2, 3)\}\end{aligned}$$

holding for all $\alpha \geq 0$. In our setting, namely that y a prime power, we have no solutions.

Case 2: $n = 2$

If $\ell = 0$, then we factor to get $(d - p)(d + p) = -5^m$. Breaking into cases gives

$$\begin{cases} d - p = -1 \\ d + p = 5^m \end{cases} \qquad \begin{cases} d - p = -5^m \\ d + p = 1 \end{cases}$$

where the second case is inadmissible. For the first case, subtracting gives $p = \frac{5^m+1}{2}$ and this is a stated solution.

If $\ell = 1$, then modulo 4 considerations gives us that

$$0 \equiv 1 - 1 \equiv d^2 - p^2 \equiv -2^\ell 5^m \equiv 2 \pmod 4$$

a contradiction. If $\ell = 2$, then modulo 8 considerations give us that $d^2 \equiv -3 \pmod 8$ another contradiction. So we assume that $\ell \geq 3$. Here we have

$$-2^\ell 5^m = d^2 - p^2 = (d-p)(d+p).$$

Since $\gcd(d-p, d+p) = \gcd(d-p, 2d) = 2$, we have that we are in one of the following three cases

$$\begin{cases} d-p = -2 \cdot 5^m \\ d+p = 2^{\ell-1} \end{cases} \qquad \begin{cases} d-p = -2^{\ell-1} \\ d+p = 2 \cdot 5^m \end{cases} \qquad \begin{cases} d-p = -2 \cdot 5^m \\ d+p = 2^{\ell-1} \cdot 5^m. \end{cases}$$

In the first and second pairs of equations above, eliminating d via subtraction yields

$$p = 5^m + 2^{\ell-2}.$$

In the third pair of equations, Again subtracting to eliminate d yields

$$p = 2^{\ell-2} \cdot 5^m + 1$$

and all these cases are as stated in the lemma.

Case 3: $n = 0$. We get an immediate contradiction since $d^2 + 2^\ell 5^m = 1$ has no solutions.

■

Theorem 3.4.4. *Let $p \neq 2, 5$ be a prime number with $\ell, m, n \geq 0$ and $d \geq 1$.*

1. *Solutions to $d^2 - 2^\ell = 5^m p^n$ are given by*
   - *(a) $n = m = 0$ and $\ell = 3$.*
   - *(b) $n = 1$, $m = 0$ and $\ell < 435 + 10 \log_2 p$.*
   - *(c) $n = 1$, $m > 0$ and $p = 5^m \pm 2^{\ell/2+1}$ and $d = 5^m \pm 2^{\ell/2}$ and ℓ is even.*
   - *(d) $n = 2$ and $(d, \ell, m, p) = (123, 2, 3, 11)$.*
   - *(e) $n = 2$, $m = 0$ and $(d, \ell, p) = (p+2, \ell, 2^{\ell-2} - 1)$.*
   - *(f) $n = 3$ and $(d, \ell, m, p) \in \{(71, 7, 0, 17), (26, 0, 2, 3, 3)\}$.*
   - *(g) $P_{\min}(n) \geq 7$ and $p^n = 5^m \pm 4$ with $\ell = 2$ and $p \equiv 1 \pmod 4$.*
2. *Solutions to $d^2 + 5^m p^n = 2^\ell$ are given by*
   - *(a) $n = m = 0$ and $d = \ell = 1$.*

(b) $n = 1$, $m = 0$ *and* $\ell < 435 + 10 \log_2 p$.

(c) $n = 1$ *and* $p = 2^{\ell/2+1} - 5^m$.

(d) $n = 3$ *and* $(d, \ell, m, p) \in \{(13, 9, 0, 7), (11, 8, 1, 3, 3)\}$.

3. *Solutions to* $d^2 + 2^\ell = 5^m p^n$ *are given by*

(a) $n = 0$ *and* $(d, \ell, m, p) \in \{(3, 4, 2, 5), (11, 2, 3, 5)\}$.

(b) $n = 1$, $m = 0$ *and* $\ell < \log_2 p$.

(c) $n = 1$ *and* $p = \frac{d^2+2^\ell}{5^m}$.

(d) n *even,* $3, 5 \nmid n$ *and* $\ell = 0$ *with* $p^n = \frac{d^2+1}{5^m}$ *and* m *odd.*

(e) $2 \parallel n$, *either* $n = 2$ *or* $P_{\min}(n/2) \geq 7$, $\ell = 2$ *with* $p^n = \frac{d^2+4}{5^m}$ *and* m *odd.*

(f) $n = 2$ *and*

a) $m = 0$ *and* $(d, \ell, p) \in \{(1, 1, 3), (p - 2, \ell, 2^{\ell-2} + 1)\}$ *and in the second case we have that* $\ell \geq 5$.

b) $p = \frac{2^{\ell-2}+1}{5^{m/2}}$ *with* ℓ, m *even.*

(g) $n = 3$ *and* $(d, \ell, m, p) \in \{(5, 1, 0, 3), (83, 12, 1, 13), (503, 8, 1, 37), (349, 10, 2, 17)\}$.

(h) $n = 4$, $m = 0$ *and* $(d, \ell, p) \in \{(7, 5, 3)\}$.

(i) $P_{\min}(n) \geq 7$ *and* $\ell = 0, 2$ *or* 4.

Proof. In all cases, when $m > 0$, we know that

$$d^2 \pm 2^\ell \equiv \pm 5^m p^n \equiv 0 \pmod 5$$

and so $d^2 \equiv \mp 2^\ell \pmod 5$. If ℓ is odd, we get a contradiction since ∓ 2 is a non-quadratic residue. Hence in all three parts to this theorem, we know that ℓ is even.

1. **Case 1:** $m = 0$ **or** $n = 0$**.** In this setting if either $m = 0$ or $n = 0$, then Theorem 3.3.4 gives the results as stated. For the case when both $m = n = 0$, we have that $(d - 1)(d + 1) = 2^\ell$ and thus $d - 1 = 2$ and $d + 1 = 2^{\ell-1}$. Hence $d = 3$ and $\ell = 3$.

   Case 2: $3 \mid n$**.** If $m \equiv 0 \pmod 3$ then $(x, y) = (5^{m/3} p^{n/3}, d)$ is a solution to $y^2 = x^3 + 2^\ell$. If $m \equiv 1 \pmod 3$ then $(x, y) = (5^{(m+2)/3} p^{n/3}, 5d)$ is a solution to $y^2 = x^3 + 2^\ell 5^2$. If $m \equiv 2 \pmod 3$ then $(x, y) = (5^{(m+4)/3} p^{n/3}, 25d)$ is a solution to $y^2 = x^3 + 2^\ell 5^4$.

   A check in Theorem 3.1.4 shows us that the only solutions to the above comes from the first case with $(d, \ell, m, n, p) = (71, 7, 0, 3, 17)$ and from the third case with the solution given by $(d, \ell, m, n, p) = (26, 0, 2, 3, 3)$.

Case 3: $5 \mid n$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

Case 4: Remaining cases. The sign of 2^ℓ on the left hand side of the equation is negative and we will assume that our equation takes the shape $d^2 - 2^\ell = 5^m p^n$. We can factor the equation to get

$$(d - 2^{\ell/2})(d + 2^{\ell/2}) = 5^m p^n$$

As the elements on the left are coprime, we can break into factors giving

$$\begin{cases} d \mp 2^{\ell/2} = 5^m \\ d \pm 2^{\ell/2} = p^n. \end{cases}$$

Eliminating d gives $5^m \pm 2^{\ell/2+1} = p^n$. We break into cases.

Case 4a: $n > 0$ **is even** In this case, modulo 5 considerations show again that $\ell/2+1$ must be even since ± 2 are both non-quadratic residues modulo 5.

Case 4a (i): $p^n = 5^m + 2^{\ell/2+1}$**.** Let $k = \ell/2 + 1$. As k is even, factoring again gives $(p^{n/2} - 2^{k/2})(p^{n/2} + 2^{k/2}) = 5^m$ and so we get

$$\begin{cases} p^{n/2} \mp 2^{k/2} = -1 \\ p^{n/2} \pm 2^{k/2} = 5^m. \end{cases}$$

Eliminating p gives $\pm 2^{k/2+1} = 5^m + 1$. As $k > 0$ we know that $k/2 + 1 > 1$ and modulo 4 considerations give a contradiction.

Case 4a (ii): $p^n = 5^m - 2^{\ell/2+1}$**.** In this case, either $\ell = 0$ (impossible since $\ell/2 + 1$ is even), $\ell = 2$ or $\ell \geq 4$. In the case when $\ell \geq 4$, modulo 8 considerations give us that $p^n \equiv 5^m \pmod 8$ and as n is even, this implies that m is even as well. We factor the equation as $(p^{n/2} - 5^{m/2})(p^{n/2} + 5^{m/2}) = -2^{\ell/2+1}$. This gives

$$\begin{cases} p^{n/2} - 5^{m/2} = -2 \\ p^{n/2} + 5^{m/2} = 2^{\ell/2} \end{cases} \qquad \begin{cases} p^{n/2} - 5^{m/2} = -2^{\ell/2} \\ p^{n/2} + 5^{m/2} = 2. \end{cases}$$

Eliminating $p^{n/2}$ in both cases gives $5^{m/2} = 1 + 2^{\ell/2-1}$ and Mihăilescu's Theorem (Theorem 3.3.8) implies that there are no solutions. This leaves $\ell = 2$ and $p^n = 5^m - 4$. Now solutions to $x^2 + 4 = y^n$ are given in [Coh03] to be $x = 2, 11$ of which we only consider $x = 11$ which gives us $11^2 + 4 = 5^3$ and this is as stated in the theorem.

Case 4b: $P_{\max}(n) \geq 7$ **and** $\ell/2+1 \neq 2,3$**.** In this case, we immediately see via Theorem 1.6.1 that we have no solutions.

Case 4c: $P_{\max}(n) \geq 7$ **and** $\ell/2+1=3$**.** This gives $p^n = 5^m \pm 8$ and by Theorem 1.6.7, we get a contradiction.

Case 4d: $P_{\max}(n) \geq 7$ **and** $\ell/2+1=2$**.** This gives $p^n = 5^m \pm 4$.

2. **Case 1:** $\ell \leq 2$**.** This case has only solutions when $\ell = 1 = d$ and $n = m = 0$. Throughout we suppose that $\ell \geq 4$ (recalling that ℓ is even).

Case 2: $m = 0$ **or** $n = 0$**.** In this setting if either $m = 0$ or $n = 0$, then Theorem 8.4 in [BS04] gives the results as stated when the other variable is at least 1. When $n = 0$ and $m = 1$, then [Coh03] gives us no solutions. When $n = 1$ and $m = 0$ then the solutions are as stated.

Case 3: $3 \mid n$**.** If $m \equiv 0 \pmod 3$ then $(x, y) = (-5^{m/3}p^{n/3}, d)$ is a solution to $y^2 = x^3 + 2^\ell$. If $m \equiv 1 \pmod 3$ then $(x, y) = (-5^{(m+2)/3}p^{n/3}, 5d)$ is a solution to $y^2 = x^3 + 2^\ell 5^2$. If $m \equiv 2 \pmod 3$ then $(x, y) = (-5^{(m+4)/3}p^{n/3}, 25d)$ is a solution to $y^2 = x^3 + 2^\ell 5^4$.

A check in Theorem 3.1.4 shows us that the only solution to the above comes from the first case with $(d, \ell, m, n, p) = (13, 9, 0, 3, 7)$ and the third case with $(d, \ell, m, n, p) = (11, 8, 1, 3, 3)$.

Case 4: n **is even.** In $d^2 - 2^\ell = -5^m p^n$, we know that

$$d^2 \equiv d^2 - 2^\ell \equiv -5^m p^n \equiv -5^m \pmod 8$$

and this is a contradiction.

Case 5: Remaining cases. As ℓ is even, factoring gives

$$(d - 2^{\ell/2})(d + 2^{\ell/2}) = -5^m p^n$$

and breaking into cases gives

$$\begin{cases} d - 2^{\ell/2} = -5^m \\ d + 2^{\ell/2} = p^n \end{cases} \qquad \begin{cases} d - 2^{\ell/2} = -p^n \\ d + 2^{\ell/2} = 5^m. \end{cases}$$

Eliminating d in either case gives $2^{\ell/2+1} = 5^m + p^n$. When $\ell = 4$ we get a solution with $n = 1$ and $p = 3$. From here out, we assume that $\ell \geq 6$ so that $\ell/2 + 1 \geq 4$ and that n is odd and $P_{\min}(n) \geq 5$. Thus, we may apply Theorem 1.6.1 and see that the equation $2^{\ell/2+1} = 5^m + p^n$ has no solutions. This leaves only the case when $n = 1$ and $p = 2^{\ell/2+1} - 5^m$.

3. **Case 1:** $m = 0$ **or** $n = 0$**.** In this setting if either $m = 0$ or $n = 0$, then Theorem 3.3.3 gives the results as stated.

   Case 2: $3 \mid n$**.** If $m \equiv 0 \pmod 3$ then $(x, y) = (5^{m/3}p^{n/3}, d)$ is a solution to $y^2 = x^3 - 2^\ell$. Theorem 3.1.8 tells us that the only solution is with $(x, y) = (3, 5)$ and so $(d, \ell, m, n, p) = (5, 1, 0, 3, 3)$. If $m \equiv 1 \pmod 3$ then $(x, y) = (5^{(m+2)/3}p^{n/3}, 5d)$ is a solution to $y^2 = x^3 - 2^\ell 5^2$. Theorem 3.1.8 tells us that the only solutions are with

$$(x, y, \ell) \in \{(5 \cdot 13, 5 \cdot 83, 12), (5 \cdot 37, 5 \cdot 503, 8)\}$$

   and so

$$(d, \ell, m, n, p) \in \{(83, 12, 1, 3, 13), (503, 8, 1, 3, 37)\}.$$

   If $m \equiv 2 \pmod 3$ then $(x, y) = (5^{(m+4)/3}p^{n/3}, 25d)$ is a solution to $y^2 = x^3 - 2^\ell 5^4$. Theorem 3.1.8 tells us that the only solution is with $(x, y) = (25 \cdot 17, 25 \cdot 349)$ and so $(d, \ell, m, n, p) = (349, 10, 2, 3, 17)$.

   Case 3: $5 \mid n$. Checking with Theorem 3.2.11, we see that this case gives no solutions.

   Case 4: $P_{\min}(n) \geq 7$**,** $\ell \geq 6$**.** Use Theorem 1.6.5 on the original equation to reach a contradiction. Hence $\ell = 0, 2, 4$.

   Case 5: n **even and** $\ell \geq 3$**.** In the first case, modulo 8 arguments give that

$$d^2 \equiv d^2 + 2^\ell \equiv 5^m p^n \equiv 5^m \pmod 8$$

   and so m is even since 5 is not a square modulo 8. Factoring gives

$$\begin{cases} d - 5^{m/2}p^{n/2} = -2 \\ d + 5^{m/2}p^{n/2} = 2^{\ell-1} \end{cases} \quad \begin{cases} d - 5^{m/2}p^{n/2} = -2^{\ell-1} \\ d + 5^{m/2}p^{n/2} = 2. \end{cases}$$

   Eliminating d gives $5^{m/2}p^{n/2} = 2^{\ell-2} + 1$. If $\ell = 4$, we do not get any solutions since

both m and n are positive. So suppose that $\ell \geq 6$ (recall that ℓ is even). Now the other cases show that only powers of 2 divide n in this case. If $n = 2$ then we get the solution $p = \frac{2^{\ell-2}+1}{5^{m/2}}$. If $4 \mid n$, then another modulo 8 argument with the equation $5^{m/2}p^{n/2} = 2^{\ell-2} + 1$ shows that $m/2$ is even again. Thus, we can factor again to see that

$$\begin{cases} 5^{m/4}p^{n/4} - 1 = 2 \\ 5^{m/4}p^{n/4} + 1 = 2^{\ell-3} \end{cases}$$

and the first line gives a contradiction.

Case 6: n **is even and** $\ell = 2$**.** Then $d^2 + 4 = 5^m p^n$ so modulo 8 considerations gives that m is odd. Now if in fact $4 \mid n$, rearranging gives $5^m(p^{n/4})^4 - d^2 = 4$. By absorbing powers of 5 that are multiples of 4, we can examine the solutions to $5x^4 - d^2 = 4$ and $125x^4 - d^2 = 4$ to make a claim about solutions in this case. By [Lju67], we see that in both of these cases (the smallest solution to $5x^2 - d^2 = 4$ is given by $(x, d) = (1, 1)$ and the smallest solution to $125x^2 - d^2 = 4$ is given by $(x, d) = (1, 11)$) the only solutions are given by $n = 0$ which was already considered in case 1. Hence we have that $2 \parallel n$.

Case 7: n **is even** $4 \mid d$**.** This case can only occur if $\ell = 0$ and so in this case we get that $1 \equiv d^2 + 1 \equiv 5^m p^n \equiv 5^m \pmod 8$ and so again we see that m is even. Factoring here gives

$$\begin{cases} d - 5^{m/2}p^{n/2} = -1 \\ d + 5^{m/2}p^{n/2} = 1 \end{cases}$$

and this is a contradiction.

Case 9: n **is even** $2 \parallel d$**.** This case can only occur if $\ell = 0$ giving $1 = 5^m p^n - d^2$. Now, if m is even, as in case 7 we reach a contradiction. Thus m is odd.

■

Theorem 3.4.5. *Let $p \neq 2, 5$ be a prime number with $\ell, n \geq 0$ and $d \geq 1$.*

1. *Solutions to $5d^2 - 2^\ell p^n = -1$ are given by*
   - *(a) $n = 1$, $\ell = 0$ and $p = 5d^2 + 1$.*
   - *(b) $n = 1$, $\ell = 1$ and $p = \frac{5d^2+1}{2}$.*
   - *(c) $n = 2$ and $\ell = 0$.*

(d) $P_{\min}(n) \geq 7$ *and* $\ell = 1$ *and* $p \equiv 3 \pmod 4$.

2. Solutions to $5d^2 - 2^\ell p^n = 1$ *are given by*

(a) $n = 0$ *and* $\ell = 2$ *with* $d = 1$.

(b) $n = 1$ *and* $\ell = 0, 2$.

(c) $\ell = 2$ *with* $2 \parallel n$ *and either* $n = 2$ *or* $P_{\min}(n/2) \geq 7$, *or* $2 \nmid n$ *and* $P_{\min}(n) \geq 7$.

Proof. We will start by considering both cases simultaneously then breaking down this theorem into parts. Throughout, suppose that we have a solution to $5d^2 - 2^\ell p^n = \pm 1$.

Case 1: $\ell \geq 3$**.** In this case, modulo 8 considerations gives $d^2 \equiv \pm 5 \pmod 8$ which is a contradiction.

Case 2: $\ell = 0$**.** We use Theorem 1.6.2 to see that $n = 0, 1, 2, 3$. For $n = 3$, notice that solutions to this equation are associated to solutions of $(5d)^2 = (5p)^3 \pm 5^3$ which the theorems from Section 3.1 show is impossible. For $n = 1$, we get that $p = 5d^2 \pm 1$ which are as stated in the theorem. When $n = 0$, we have no solutions.

1. **Case 3:** $\ell = 2$. In this case, modulo 8 considerations gives $5d^2 \equiv 4p^n - 1 \equiv 3 \pmod 8$. Isolating gives $d^2 \equiv -1 \pmod 8$ which is a contradiction.

   Case 4: $\ell = 1$**.** Here we have $5d^2 = 2p^n - 1$. We have two cases

   Case 4a: $2 \mid n$. Here, considerations modulo 5 give us that $p^n \equiv 3 \pmod 5$ which is a contradiction. Hence n is odd.

   Case 4b: n **is odd** Here we can break it up into subcases. First notice that if $2p^n \equiv 2 \pmod 8$ then $5d^2 \equiv 2p^n - 1 \equiv 1 \pmod 8$ and this is a contradiction since 5 is not a square modulo 8. So we have that $2p^n \equiv 6 \pmod 8$ which means that $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$. This translates to $p \equiv 3 \pmod 4$.

   Case 4bi: $3 \mid n$ Transform the equation to $(50d)^2 = (10p)^3 - 2^2 \cdot 5^3$ and then use Section 3.1 to see that there are no solutions.

2. We proceed in cases.

   Case 3: $\ell = 1$**.** Modulo 4 considerations gives $d^2 \equiv 2p^n + 1 \equiv 3 \pmod 4$ a contradiction since 3 is not a square modulo 4.

Case 4: $\ell = 0$ **and** n **even**. This gives the equation $5d^2 = p^n + 1$. Note that d is even. Modulo 4 considerations shows that $0 \equiv p^n + 1 \equiv 2 \pmod 4$ a contradiction.

Case 5: $\ell = 0$ **or** $\ell = 2$ **and** $3 \mid n$**.** In these cases, multiplying through by suitable powers of 2 and 5 gives $D^2 - X^n = 2^{k_1}5^{k_2}$ where k_1 and k_2 are integers. Section 3.1 shows that 3 does not divide n in these cases.

Case 6: $\ell = 2$ **and** $4 \mid n$**.** In this case, using [Lju54], we see that the equation $5x^2 - 4y^4 = 1$ only has the solution $(x, y) = (1, 1)$. Thus $n = 0$ in this case and we have $d = 1$.

Case 7: $5 \mid n$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

■

Theorem 3.4.6. *Let $p \neq 2, 5$ be a prime number with $\ell, n \geq 0$ and $d \geq 1$.*

1. *Solutions to $5d^2 - 2^\ell = p^n$ are given by*
   (a) *$n = 0$ and $(d, \ell) = (1, 2)$.*
   (b) *$n = 1$ and $p = 5d^2 - 2^\ell$.*
   (c) *$2 \parallel n$, either $n = 2$ or $P_{\min}(n/2) \geq 7$, and $\ell = 2$.*
   (d) *$n = 3$ and $(d, \ell, p) = (21, 3, 13)$.*
   (e) *$n = 5$ and $(d, \ell, p) = (7, 1, 3)$.*
   (f) *$P_{\min}(n) \geq 7$ and $1 \leq \ell \leq 5$.*
2. *Solutions to $5d^2 + p^n = 2^\ell$ are given by*
   (a) *$n = 1$.*
   (b) *$n = 3$ and $(d, \ell, p) = (1, 5, 3)$.*
   (c) *$n = 5$ and $(d, \ell, p) = (19, 11, 3)$.*
3. *Solutions to $5d^2 + 2^\ell = p^n$ are given by*
   (a) *$n = 1$ so $p = 5d^2 + 2^\ell$.*
   (b) *$2 \parallel n$, $n = 2$ or $P_{\min}(n/2) \geq 7$, and $\ell = 0, 2$.*
   (c) *$P_{\min}(n) \geq 7$ and $1 \leq \ell \leq 5$.*

Proof. First, let's consider the above cases simultaneously. Suppose n is even. If $\ell \geq 3$, then local considerations at 8 reveal that

$$p^n \equiv \pm 5d^2 \equiv \pm 5 \pmod 8$$

which is a contradiction. If instead $\ell = 1$, then locally at 5 reveals that

$$\pm 2 \equiv 5d^2 \pm 2 \equiv \pm p^n \equiv \pm 1 \pmod 5$$

which is a contradiction. Hence when n is even, $\ell = 0$ or $\ell = 2$ in each case. Now we look individually at each equation.

1. **Case 1:** $\ell = 0$**.** This implies that d is even. Considerations modulo 8 show that

$$p^n = 5d^2 - 1 \equiv \begin{cases} 3 & \text{if } 2 \parallel d \\ -1 & \text{if } 4 \mid d \end{cases} \pmod 8$$

and this is a contradiction if n is even. Hence n is odd. By Theorem 1.6.2, there are no solutions when $n \geq 4$. Hence $n = 1$ or $n = 3$. For $n = 3$, the equation is $5d^2 - 1 = p^3$ has no solutions via theorem 2 of [Coh91]. Thus, we are left with the case when $n = 1$ and the equation is $p = 5d^2 - 1$ which has many solutions.

Case 3: $3 \mid n$. Rearrange the original equation to give $(25d)^2 = (5p^{n/3})^3 + 2^\ell 5^3$. We can solve this using Theorem 3.1.4 to see that the only solution comes when $(d, \ell, n, p) = (21, 3, 3, 13)$.

Case 4: $5 \mid n$. Checking with Theorem 3.2.11, we see that the only solution is given by $(d, \ell, n, p) = (7, 1, 53)$.

Case 5: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$. We can use Theorem 1.6.4 to reach a contradiction.

Case 6: $4 \mid n$ **and** $\ell = 2$. For this, we use [LY07] to see that the equation $5d^2 - (p^{n/4})^4 = 4$ only has a solution when $n = 0$ and $d = 1$. Thus if n is even then $2 \parallel n$.

2. **Case 1:** n **is even** By above we know that $\ell = 0$ or $\ell = 2$ both of which quickly do not yield a solution.

Case 2: $\ell \leq 5$**.** As $d > 0$, it is clear that the only solutions occur when

$$(d, \ell, n, p) \in \{(1, 3, 1, 3), (1, 4, 1, 11), (1, 5, 3, 3)\}.$$

Hence we may suppose that $\ell \geq 6$. In fact, using the preliminary remark, we know that n even gives no solutions.

Case 3: $3 \mid n$ **and** $\ell \geq 6$. Rearrange the original equation to give $(25d)^2 = (-5p^{n/3})^3 + 2^\ell 5^3$. We can solve this using Theorem 3.1.4 to see that the only solution comes when $(d, \ell, n, p) = (1, 5, 3, 3)$.

Case 4: $5 \mid n$ **and** $\ell \geq 6$. Checking with Theorem 3.2.11, we see that the only solution is given by $(d, \ell, n, p) = (19, 11, 5, 3)$.

Case 5: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$. This follows from Theorem 1.6.4 that the associated equation has no solutions.

3. **Case 1:** $3 \mid n$ **and** $\ell \geq 6$**.** Rearrange the original equation to give $(25d)^2 = (5p^{n/3})^3 - 2^\ell 5^3$. We can solve this using Theorem 3.1.8 to see that there are no solutions.

   Case 2: $5 \mid n$ **and** $\ell \geq 6$**.** Checking with Theorem 3.2.11, we see that this case gives no solutions.

   Case 3: $P_{\min}(n) \geq 7$ **and** $\ell \geq 6$**.** We can use Theorem 1.6.4 to reach a contradiction.

   Case 4: $4 \mid n$ **and** $\ell = 0, 2$**.** In this case, we rewrite the given equation as

   $$(p^{n/4})^4 - 5d^2 = 2^\ell$$

   When $\ell = 0$, results due to Cohn and Ljunggren (see [Coh07a], [Lju42], [Coh97]) show that the only solution to $x^4 - 5y^2 = 1$ is given by $(x, y) = (3, 4)$. When $\ell = 2$, so the equation is $x^4 - 5d^2 = 4$, Ljunggren showed that there are no solutions to this equation (see [Lju67]). For a survey of these results, see [HPPT13]. Thus, we see that if n is even, then $2 \parallel n$.

■

To complete this section, I will summarize the results above into a table. We will be particularly interested in the cases when $n \geq 1$, $m \geq 0$ and $\ell = 2$ or $\ell \geq 4$. We organize the above by prime p. We will also include all sporadic cases for each prime and when we state relevant theorems later in this thesis, we will check these primes by hand if necessary.

p^N	ℓ	m	n	N	ϵ
3,7					
$2^{\ell-2} \pm 1$	≥ 5	0	1	1	1
$\frac{2^{\ell-2}+1}{5^m}$	≥ 2 even	≥ 1	1	1	1
$2^{\ell-2}5^m \pm 1$	≥ 4	≥ 1	1	1	1
$\frac{5^m-1}{4}$	4 even	≥ 1 odd	1 or $P_{\min}(n) \geq 7$	n	1

Table 3.21: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $d^2 + 2^\ell 5^m p^n = \epsilon$.

Note: The above with $\epsilon = -1$ has no solutions when $\ell \geq 2$.

p^N	ℓ	m	n	N	δ	ϵ
3,11						
$2^{\ell-2} \pm 1$	≥ 5	0	1	1	-1	1
$\frac{d^2-5^m}{4}$	2	≥ 1 odd	1	1	-1	1
$2^{\ell-2} \pm 5^{m/2}$	≥ 4	≥ 2 even	1	1	-1	1
$\frac{5^m-1}{4}$	2	≥ 1 odd	2	1	-1	1
$\left(\frac{5^m-1}{4}\right)^2$	2	≥ 1 odd	$2 \parallel n$ and either $n = 2$ or $P_{\min}(n/2) \geq 7$	n	-1	1
$\frac{d^2-5^m}{4}$	2	≥ 1 odd	$P_{\min}(n) \geq 7$	n	-1	1
$2^{\ell-2} \pm 5^{m/2}$	4, 5	≥ 2 even	$P_{\min}(n) \geq 7$	n	-1	1
$\frac{5^m-d^2}{4}$	2	≥ 1 odd	1	1	1	1
$5^{m/2} - 2^{\ell-2}$	≥ 4	≥ 2 even	1	1	1	1
$\frac{5^{m/2}-1}{4}$	4	≥ 2 even	1	1	1	1
$\frac{5^m-d^2}{4}$	2	≥ 1 odd	≥ 2 even	n	1	1
$\frac{5^m-d^2}{4}$	2	≥ 1 odd	$P_{\min}(n) \geq 7$	n	1	1
$\frac{5^m-d^2}{2^\ell}$	4, 5	≥ 1 even	$P_{\min}(n) \geq 7$	n	1	1

Table 3.22: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $d^2 + \delta 2^\ell p^n = \epsilon 5^m$.

Note: The above with $\delta = \epsilon = -1$ has no solutions when $\ell \geq 2$.

p^N	ℓ	m	n	N	δ	ϵ
3,7,11,17,31,41						
$d^2 - 2^\ell \cdot 5^m$	ℓ	m	1	1	-1	1
$2^{\ell-2} - 5^m$	≥ 4	m	2	1	-1	1
$5^m - 2^{\ell-2}$	≥ 4	m	2	1	-1	1
$2^{\ell-2} \cdot 5^m - 1$	≥ 4	m	2	1	-1	1
$d^2 - 2^\ell \cdot 5^m$	$2, 4, 5$	m	$P_{\min}(n) \geq 7$	n	-1	1
$(5^m - 4)^2$	4	≥ 1 odd	$n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$	n	-1	1
$2^\ell \cdot 5^m - d^2$	ℓ	m	1	1	-1	-1
$2^\ell \cdot 5^m - d^2$	$2, 4, 5$	m	$P_{\min}(n) \geq 7$	n	-1	-1
$d^2 + 2^\ell \cdot 5^m$	ℓ	m	1	1	1	1
$5^m + 2^{\ell-2}$	≥ 3	m	2	1	1	1
$2^\ell \cdot 5^m + 1$	≥ 3	m	2	1	1	1

Table 3.23: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $d^2 + \delta 2^\ell 5^m = \epsilon p^n$.

p^N	ℓ	m	n	N	δ	ϵ
3,11,13,17,37						
$d^2 - 2^\ell$	ℓ	0	1	1	-1	1
$5^{m/2} \pm 2^{\ell/2+1}$	≥ 2 even	≥ 1	1	1	-1	1
$2^{\ell-2} - 1$	≥ 4 even	0	2	1	-1	1
$5^m \pm 4$	2	≥ 1	$P_{\min}(n) \geq 7$	n	-1	1
$2^\ell - d^2$	≥ 4	0	1	1	-1	-1
$2^{\ell/2+1} - 5^m$	≥ 2 even	m	1	1	-1	-1
$\frac{d^2+2^\ell}{5^m}$	ℓ	m	1	1	1	1
$\frac{d^2+4}{5^m}$	2	m odd	$n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$	n	1	1
$\frac{d^2+2^\ell}{5^m}$	$2, 4$	m	$P_{\min}(n) \geq 7$	n	1	1
$\frac{2^{\ell-2}+1}{5^{m/2}}$	even	$m \geq 0$ even	2	1	1	1

Table 3.24: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $d^2 + \delta 2^\ell = \epsilon 5^m p^n$.

p^N	ℓ	n	N	ϵ
$\frac{5d^2-1}{4}$	2	One of $n=1$, $n=2$ or $2 \parallel n$ with $P_{\min}(n/2) \geq 7$	n	1

Table 3.25: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $5d^2 - 2^\ell p^n = \epsilon$.

Note: The above with $\epsilon = -1$ has no solutions when $\ell \geq 2$.

p^N	ℓ	n	N	δ	ϵ
3					
$5d^2 - 2^\ell$	ℓ	1	1	-1	1
$5d^2 - 4$	2	$n=2$, or $2 \parallel n$ with $P_{\min}(n/2) \geq 7$	n	-1	1
$5d^2 - 2^\ell$	$2, 4, 5$	$P_{\min}(n) \geq 7$	n	-1	1
$2^\ell - 5d^2$	ℓ	1	1	-1	-1
$5d^2 + 2^\ell$	ℓ	1	1	1	1
$5d^2 + 4$	2	$n=2$, or $2 \parallel n$ with $P_{\min}(n/2) \geq 7$	n	1	1
$5d^2 + 2^\ell$	$2, 4, 5$	$P_{\min}(n) \geq 7$	n	1	1

Table 3.26: Summary of solutions with $n \geq 1$, $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ for the equation $5d^2 - \delta 2^\ell = \epsilon p^n$.

Chapter 4

Elliptic Curves With Rational Two Torsion and Conductor $18p$, $36p$ or $72p$ Organized by Primes

In this section we recall, simplify and summarize the results from [Mul06]. The majority of the work was done in the aforementioned thesis however the theorems there were presented differently and were not organized by the form of the prime p. In the following theorems, if a case shows up degenerately, for example if some exponent is 0, then many cases of curves might give the same elliptic curves. I have made an attempt to not duplicate any elliptic curves represented below.

Additionally in the following theorems, much like what happened in the tables at the end of Section 3.4, we see that sometimes the n substituted into the elliptic curves is not the same as the n in the prime decomposition. For an example, in the theorem for curves of conductor of $18p$, we see a case where $p = 2^a 3^b + 1$ which suggests that the exponent of n is 1 and so we are to plug 1 in the tables obtained from [Mul06]. However this is not necessarily the case. Somewhat annoyingly, some cases will have, for example, $n = 2$ in the Diophantine equation and after factoring yield a prime of the form $p = 2^a 3^b + 1$ which has $n = 1$. Despite this potential confusion, I have left the notation the same. This only becomes a problem when $n = 2$. If you are simply reading the theorem and do not care about deriving it, then this is not a problem and this note can be ignored without harm.

Theorem 4.0.7. *Let p be a prime distinct from 2 and 3. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $18p$ provided that p satisfies at least one of the following where $d > 0$, $\ell_1 \geq 5$, $\ell_2 \geq 7$ and $m \geq 0$ are integers:*

1. $p = 2^{\ell_1} 3^m + 1$.
2. $p = 2^{\ell_1} 3^m - 1$.

3. $p = 3^m + 2^{\ell_1}$.

4. $p = 3^m - 2^{\ell_1}$.

5. $p = 2^{\ell_1} - 3^m$.

6. $p = d^2 + 2^{\ell_2}3^m$.

7. $p = d^2 - 2^{\ell_2}3^m$.

8. $p = 2^{\ell_2}3^m - d^2$.

9. $p = \frac{d^2+2^{\ell_2}}{3^m}$.

10. $p = 3d^2 + 2^{\ell_2}$.

11. $p = 3d^2 - 2^{\ell_2}$.

12. $p = 2^{\ell_2} - 3d^2$.

13. $p \in \{5, 7, 11, 17, 19, 23, 73\}$.

Theorem 4.0.8. *Let p be a prime distinct from 2 and 3. Then up to the finitely many primes in*

$$p \in \{5, 7, 11, 17, 19, 23, 73\}$$

the following gives a complete list of the families of elliptic curves with nontrivial rational two torsion of conductor $18p$ associated with the primes in the previous theorem:

(1) The prime p has the form $p = 2^{\ell-2} \cdot 3^m + 1$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$-3\psi(2^\ell 3^m p + 1)$	$2^{\ell-2}3^{m+2}p$	$2^{2\ell}3^{2m+6}p^2$
A2	$2 \cdot 3\psi(2^\ell 3^m p + 1)$	3^2	$2^{\ell+6}3^{m+6}p$

	a_2	a_4	Δ
D1	$-3\psi(p^2 - 2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
D2	$2 \cdot 3\psi(p^2 - 2^\ell 3^m)$	3^2p^2	$-2^{\ell+6}3^{m+6}p^4$

(2) The prime p has the form $p = 2^{\ell-2} \cdot 3^m - 1$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
A1	$-3\psi(2^\ell 3^m p+1)$	$2^{\ell-2}3^{m+2}p$	$2^{2\ell}3^{2m+6}p^2$
A2	$2\cdot 3\psi(2^\ell 3^m p+1)$	3^2	$2^{\ell+6}3^{m+6}p$

-

	a_2	a_4	Δ
B1	$-3\psi(2^\ell 3^m+p^2)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
B2	$2\cdot 3\psi(2^\ell 3^m+p^2)$	3^2p^2	$2^{\ell+6}3^{m+6}p^4$

(3) The prime p has the form $p=3^m+2^{\ell-2}$ with $\ell\geq 7$ and $m\geq 0$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
D1	$-3\psi(p^2-2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
D2	$2\cdot 3\psi(p^2-2^\ell 3^m)$	3^2p^2	$-2^{\ell+6}3^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p=3^{(2m)/2}+2^{\ell-2}$ given by*

	a_2	a_4	Δ
E1	$-3\psi(2^\ell p+3^{2m})$	$2^{\ell-2}3^2p$	$2^{2\ell}3^{2m+6}p^2$
E2	$2\cdot 3\psi(2^\ell p+3^{2m})$	3^{2m+2}	$2^{\ell+6}3^{4m+6}p$

- *Rewriting $\ell-2$ as $\hat{\ell}/2+1$, we get solutions with $p=3^m+2^{\hat{\ell}/2+1}$ given by*

	a_2	a_4	Δ
H1	$-3\psi(2^{\hat{\ell}}+3^m p)$	$2^{\hat{\ell}-2}3^2$	$2^{2\hat{\ell}}3^{m+6}p$
H2	$2\cdot 3\psi(2^{\hat{\ell}}+3^m p)$	$3^{m+2}p$	$2^{\hat{\ell}+6}3^{2m+6}p^2$

(4) The prime p has the form $p=3^m-2^{\ell-2}$ with $\ell\geq 7$ and $m\geq 0$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
B1	$-3\psi(2^\ell 3^m+p)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
B2	$2\cdot 3\psi(2^\ell 3^m+p)$	3^2p^2	$2^{\ell+6}3^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p=3^{(2m)/2}-2^{\ell-2}$ given by*

	a_2	a_4	Δ
G1	$\epsilon\cdot 3\psi(3^{2m}-2^\ell p)$	$-2^{\ell-2}3^2p$	$2^{2\ell}3^{2m+6}p^2$
G2	$-\epsilon\cdot 2\cdot 3\psi(3^{2m}-2^\ell p)$	3^{2m+2}	$-2^{\ell+6}3^{4m+6}p$

- *Rewriting $\ell - 2$ as $\hat{\ell}/2 + 1$, we get solutions with $p = 3^m - 2^{\hat{\ell}/2+1}$ given by*

	a_2	a_4	Δ
H1	$-3\psi(2^{\hat{\ell}} + 3^m p)$	$2^{\hat{\ell}-2}3^2$	$2^{2\hat{\ell}}3^{m+6}p$
H2	$2 \cdot 3\psi(2^{\hat{\ell}} + 3^m p)$	$3^{m+2}p$	$2^{\hat{\ell}+6}3^{2m+6}p^2$

(5) The prime p has the form $p = 2^{\ell-2} - 3^m$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
B1	$-3\psi(2^\ell 3^m + p)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
B2	$2 \cdot 3\psi(2^\ell 3^m + p)$	3^2p^2	$2^{\ell+6}3^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p = 2^{\ell-2} - 3^{(2m)/2}$ given by*

	a_2	a_4	Δ
E1	$-3\psi(2^\ell p + 3^{2m})$	$2^{\ell-2}3^2p$	$2^{2\ell}3^{2m+6}p^2$
E2	$2 \cdot 3\psi(2^\ell p + 3^{2m})$	3^{2m+2}	$2^{\ell+6}3^{4m+6}p$

- *Rewriting $\ell - 2$ as $\hat{\ell}/2 + 1$, we get solutions with $p = 2^{\hat{\ell}/2+1} - 3^m$ given by*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3\psi(2^{\hat{\ell}} - 3^m p)$	$2^{\hat{\ell}-2}3^2$	$-2^{2\hat{\ell}}3^{m+6}p$
I2	$-\epsilon \cdot 2 \cdot 3\psi(2^{\hat{\ell}} - 3^m p)$	$-3^{m+2}p$	$2^{\hat{\ell}+6}3^{2m+6}p^2$

(6) The prime p has the form $p = d^2 + 2^\ell 3^m$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
D1	$-3\psi(p - 2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p$
D2	$2 \cdot 3\psi(p - 2^\ell 3^m)$	3^2p	$-2^{\ell+6}3^{m+6}p^2$

(7) The prime p has the form $p = d^2 - 2^\ell 3^m$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
B1	$-3\psi(2^\ell 3^m + p)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p$
B2	$2 \cdot 3\psi(2^\ell 3^m + p)$	3^2p	$2^{\ell+6}3^{m+6}p^2$

(8) The prime p has the form $p = 2^\ell 3^m - d^2$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
C1	$-3\psi(2^\ell 3^m - p)$	$2^{\ell-2}3^{m+2}$	$-2^{2\ell}3^{2m+6}p$
C2	$2 \cdot 3\psi(2^\ell 3^m - p)$	$-3^2 p$	$2^{\ell+6}3^{m+6}p^2$

(9) The prime p has the form $p = \frac{d^2+2^L}{3^m}$ with $L \geq 5$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

- *If $L = \ell/2 + 1$ then we get a curve as given by*

	a_2	a_4	Δ
H1	$-3\psi(2^\ell + 3^m p)$	$2^{\ell-2}3^2$	$2^{2\ell}3^{m+6}p$
H2	$2 \cdot 3\psi(2^\ell + 3^m p)$	$3^{m+2}p$	$2^{\ell+6}3^{2m+6}p^2$

- *In the case where $d = 1$, we get a solution with $L = \ell - 2$ as given by*

	a_2	a_4	Δ
A1	$-3\psi(2^\ell 3^m p + 1)$	$2^{\ell-2}3^{m+2}p$	$2^{2\ell}3^{2m+6}p^2$
A2	$2 \cdot 3\psi(2^\ell 3^m p + 1)$	3^2	$2^{\ell+6}3^{m+6}p$

- *In the case where $d = 1$, we get a solution with $L = \ell - 2$ and $p = 2^\ell 3^{(2m)/2} - d^2$ as given by*

	a_2	a_4	Δ
J1	$-3\psi(3^{2m}p - 2^\ell)$	$-2^{\ell-2}3^2$	$2^{2\ell}3^{2m+6}p$
J2	$2 \cdot 3\psi(3^{2m}p - 2^\ell)$	$3^{2m+2}p$	$-2^{\ell+6}3^{4m+6}p^2$

(10) The prime p has the form $p = 3d^2 + 2^\ell$ with $\ell \geq 7$, $m \geq 0$, $d \in \mathbb{Z}$ and $s \in \{0, 1\}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{s+1}\psi(\frac{p-2^\ell}{3})$	$-2^{\ell-2}3^{2s+1}$	$2^{2\ell}3^{6s+3}p$
O2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{p-2^\ell}{3})$	$3^{2s+1}p$	$-2^{\ell+6}3^{6s+3}p^2$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

(11) The prime p has the form $p = 3d^2 - 2^\ell$ with $\ell \geq 7$, $m \geq 0$, $d \in \mathbb{Z}$ and $s \in \{0, 1\}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
M1	$\epsilon \cdot 3^{s+1}\psi(\frac{2^\ell+p}{3})$	$2^{\ell-2}3^{2s+1}$	$2^{2\ell}3^{6s+3}p$
M2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{2^\ell+p}{3})$	$3^{2s+1}p$	$2^{\ell+6}3^{6s+3}p^2$

where $\epsilon \in \{\pm 1\}$ *is the residue of* 3^{s+1} *modulo* 4.

(12) The prime p *has the form* $p = 2^\ell - 3d^2$ *with* $\ell \geq 7$, $m \geq 0$, $d \in \mathbb{Z}$ *and* $s \in \{0, 1\}$ *and corresponds to the following elliptic curves*

-

	a_2	a_4	Δ
N1	$\epsilon \cdot 3^{s+1}\psi(\frac{2^\ell-p}{3})$	$2^{\ell-2}3^{2s+1}$	$-2^{2\ell}3^{6s+3}p$
N2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{2^\ell-p}{3})$	$-3^{2s+1}p$	$2^{\ell+6}3^{6s+3}p^2$

where $\epsilon \in \{\pm 1\}$ *is the residue of* 3^{s+1} *modulo* 4.

Proof. To show this, we proceed in cases. We use the families in [Mul06, p.58-60] and simplify them according to [Mul06, p.153-175]. In what follows, $\delta, \epsilon \in \{\pm 1\}$ not both negative. Also $a, b \in \mathbb{Z}$ are positive integers.

Case 1: $t^2 = 2^a 3^b p^n + 1$. This is case 1 in [Mul06, p.58-60]. We can use Lemma 4.7 in [Mul06, p.153] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n	Extra Information
$2^{a-2} \cdot 3^b \pm 1$	≥ 3	≥ 0	$2p \mp 1$	1	none
$2^{a-2} \pm 1$	≥ 5	0	$2p \mp 1$	1	none
$\frac{2^{a-2}+1}{3^b}$	≥ 5	≥ 1	$2^{a-1}+1$	1	$3^b \mid a-2$
17	7	2	577	2	none

As this case only has solutions when $n = 1$ or $p = 17$, we can verify that these two situations are covered by the finitely many primes listed above and by families (1), (2) and (9).

Case 2: $t^2 = p^n + \delta 2^a 3^b$. This case is a combination of cases 2 and 9 in [Mul06, p.58-60]. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n	δ
$t^2 - 2^a \cdot 3^b$	≥ 2	≥ 0	t	1	1
$2^{a-2} \cdot 3^b - 1$	≥ 3	≥ 0	$p+2$	2	1
$3^b - 2^{a-2}$	≥ 3	≥ 0	$2^{a-1}+p$	2	1
$2^{a-2} - 3^b$	≥ 5	≥ 0	$2^{a-1}-p$	2	1
17	7	0	71	3	1
73	15	2	827	3	1
7	7	4	113	4	1
5	9	1	131	6	1
$t^2 + 2^a \cdot 3^b$	≥ 1	≥ 0	t	1	-1
$2^{a-2} \cdot 3^b + 1$	≥ 3	≥ 0	$p-2$	2	-1
$3^b + 2^{a-2}$	≥ 3	≥ 0	$p - 2 \cdot 3^b$	2	-1
17	7	2	287	4	-1

As this case only has solutions when $n = 1$, $n = 2$ or $p = 5, 7, 17$ or 73, we can verify that these three situations are covered by the finitely many primes listed above and by families (1), (2), (3), (4), (5), (6) and (7).

Case 3: $t^2 = 2^a 3^b - p^n$. This case is case 3 in [Mul06, p.58-60]. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n
$2^a \cdot 3^b - t^2$	≥ 1	≥ 0	t	1
7	9	0	13	3
23	12	1	11	3

As this case only has solutions when $n = 1$ or $p = 7$ or 23, we can verify that these two situations are covered by the finitely many primes listed above and by family (8).

Case 4: $t^2 = 3^b + \delta 2^a p^n$. This case is a combination of cases 4 and 8 in [Mul06, p.58-60]. We can use Lemma 4.8 in [Mul06, p.156-157] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n	δ
$2^{a-2} \pm 3^{b/2}$	≥ 3	≥ 0 (even)	$2p \mp 3^{b/2}$	1	1
5	9	2	253	3	1
$3^{b/2} - 2^{a-2}$	≥ 3	≥ 0 (even)	$\pm(2p - 3^{b/2})$	1	-1
7	7	8	17	2	-1

As this case only has solutions when $n = 1$ or $p = 5$ or 7, we can verify that these two situations are covered by the finitely many primes listed above and by families (3), (4) and (5).

Case 5: $t^2 = 2^a + \delta 3^b p^n$. This case is a combination of cases 5 and 6 in [Mul06, p.58-60]. We can use Lemma 4.10 in [Mul06, p.171] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n	δ
$t^2 - 2^a$	≥ 1 (odd)	0	t	1	1
$\frac{2^{a/2+1}+1}{3^b}$	≥ 1 (even)	≥ 1	$2^{a/2}+1$	1	1
$3^b \pm 2^{a/2+1}$	≥ 1 (even)	≥ 1	$p \pm 2^{a/2}$	1	1
7	8	4	65	2	1
$2^{a-2} - 1$	≥ 5	0	$p+2$	2	1
17	7	0	71	3	1
$2^a - t^2$	≥ 5 (odd)	0	t	1	-1
$2^{a/2+1} - 3^b$	≥ 4 (even)	≥ 1	$\pm(2^{a/2} - p)$	1	-1
7	10	2	31	1	-1
5	12	1	61	3	-1
7	9	0	13	3	-1

Firstly, all the cases above when $n = 1$ and $b = 0$ have been covered by cases 2 and 3 so for this case we can assume that $b \geq 1$ when $n = 1$. Under this additional restriction, we only have solutions when $n = 1$, $n = 2$ or $p = 5, 7$ or 17. We can verify that these three situations are covered by the finitely many primes listed above and by families (1), (6) and (7).

Case 6: $t^2 = 3^b p^n - 2^a$. This is case 7 in [Mul06, p.58-60]. We can use Lemma 4.10 in [Mul06, p.171] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	b	t	n
$\frac{t^2+2^a}{3^b}$	≥ 2	≥ 0	t	1
$\frac{2^{a-2}+1}{3^{b/2}}$	≥ 3 (odd)	≥ 0 (even)	$3^{b/2}p - 2$	2
11	9	1	59	3
17	15	2	107	3
19	7	1	143	3

As a note for later, notice that in the second case above, setting $a = 7$ gives $b = 2$ and $p = 11$ as a solution which is already accounted for and so in the second case, we can assume

that $a-1 \geq 7$. This case only has solutions when $n=1$, $n=2$ or $p=11,17$ or 19, and thus we can verify that these three situations are covered by the finitely many primes listed above and by family (9).

Case 7: $3t^2 = \epsilon 2^a + \delta p$. This case is a combination of cases 10 to 12 in [Mul06, p.58-60]. We can use Lemma 4.11 in [Mul06, p.174-175] to see that the solutions with $a \geq 7$ and $b \geq 0$ are

p	a	t	n	δ	ϵ
$3t^2-2^a$	≥ 0	t	1	1	1
11	8	23	3	1	1
2^a-3t^2	≥ 0	t	1	-1	1
5	7	1	3	-1	1
$3t^2+2^a$	≥ 0	t	1	1	-1

This case only has solutions when $n=1$ or $p=5$ or 11, and thus we can verify that these three situations are covered by the finitely many primes listed above and by families (10),(11) and (12).

■

Theorem 4.0.9. *Let p be a prime distinct from 2 and 3. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $36p$ provided that p satisfies at least one of the following where $d>0$, $n_1=1$ or $P_{\min}(n_1) \geq 7$, $n_2 \in \{1,2\}$ and $m_1, m_2 \geq 0$ are integers with m_1 odd and m_2 even:*

1. $p = d^2 + 4 \cdot 3^{m_2}$.
2. $p^{n_1} = d^2 - 4 \cdot 3^{m_1}$.
3. $p^{n_1} = 4 \cdot 3^{m_1} - d^2$.
4. $p = \frac{d^2+3^{m_1}}{4}$ *and* $p \equiv -1 \pmod 4$.
5. $p^{n_2} = \frac{3d^2+1}{4}$ *and* $p \equiv 1 \pmod 4$.
6. $p = 3d^2 - 4$.
7. $p \in \{5, 13\}$.

Theorem 4.0.10. *Let p be a prime distinct from 2 and 3. Then up to the finitely many primes in*

$$p \in \{5, 13\}$$

the following gives a complete list of the families of elliptic curves with nontrivial rational two torsion of conductor $36p$ *associated with the primes in the previous theorem:*

(1) The prime p *has the form* $p = d^2 + 4 \cdot 3^m$ *with* $m \geq 0$ *even,* $d \in \mathbb{Z}$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
C1	$-3\psi(p - 4 \cdot 3^m)$	-3^{m+2}	$2^4 3^{2m+6} p$
C2	$2 \cdot 3\psi(p - 4 \cdot 3^m)$	$3^2 p$	$-2^8 3^{m+6} p^2$

(2) The prime p *has the form* $p^n = d^2 - 4 \cdot 3^m$ *with* $m \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$, $d \in \mathbb{Z}$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
A1	$-3\psi(4 \cdot 3^m + p^n)$	3^{m+2}	$2^4 3^{2m+6} p^n$
A2	$2 \cdot 3\psi(4 \cdot 3^m + p^n)$	$3^2 p^n$	$2^8 3^{m+6} p^{2n}$

(3) The prime p *has the form* $p^n = 4 \cdot 3^m - d^2$ *with* $m \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$, $d \in \mathbb{Z}$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
B1	$-3\psi(4 \cdot 3^m - p^n)$	3^{m+2}	$-2^4 3^{2m+6} p^n$
B2	$2 \cdot 3\psi(4 \cdot 3^m - p^n)$	$-3^2 p^n$	$2^8 3^{m+6} p^{2n}$

(4) The prime p *has the form* $p = \frac{d^2+3^m}{4}$ *with* $m \geq 1$ *odd,* $p \equiv -1 \pmod 4$ *and* $d \in \mathbb{Z}$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
E1	$-3\psi(4p - 3^m)$	$3^2 p$	$-2^4 3^{m+6} p^2$
E2	$2 \cdot 3\psi(4p - 3^m)$	-3^{m+2}	$2^8 3^{2m+6} p$

(5) The prime p *has the form* $p^n = \frac{3d^2+1}{4}$ *with* d *an integer,* $n \in \{1, 2\}$, $s \in \{0, 1\}$, $p \equiv 1 \pmod 4$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{s+1}\psi(\frac{4p^n-1}{3})$	$3^{2s+1} p^n$	$-2^4 3^{6s+3} p^{2n}$
I2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{4p^n-1}{3})$	-3^{2s+1}	$2^8 3^{6s+3} p^n$

where $\epsilon \in \{\pm 1\}$ *is the residue of* 3^{s+1} *modulo* 4.

(6) The prime p has the form $p = 3d^2 - 4$ with d an integer, $s \in \{0, 1\}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{s+1}\psi(\frac{4+p}{3})$	3^{2s+1}	$2^4 3^{6s+3} p$
J2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{4+p}{3})$	$3^{2s+1}p$	$2^8 3^{6s+3} p^2$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

Proof. To show this, we proceed in cases. We use the families in [Mul06, p.61-62] and simplify them according to [Mul06, p.153-175].

Case 1: $t^2 = p^n - 4 \cdot 3^b$. This is case 4 in [Mul06, p.61-62]. Here b even is given. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $b \geq 0$ are

p	b	t	n
$t^2 + 4 \cdot 3^b$	≥ 0	t	1
5	0	11	3
13	5	35	3
$\sqrt[n]{t^2 + 4 \cdot 3^b}$	≥ 1	t	$P_{\min}(n) \geq 7$

According to [Luc02], we know that in the last case $n < 5$ and and thus this case gives solutions only when $n = 1$ or $p = 5$ or 13. We can verify that these two situations are covered by the finitely many primes listed above and by (1).

Case 2: $t^2 = 4 \cdot 3^b + \delta p^n$ **for** $\delta \in \{\pm 1\}$. This case is a combination of cases 1 and 2 in [Mul06, p.61-62]. Here b odd is given. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $b \geq 0$ are

p	b	t	n	δ
$t^2 - 4 \cdot 3^b$	≥ 0	t	1	1
13	1	47	3	1
$\sqrt[n]{t^2 - 4 \cdot 3^b}$	≥ 1	t	$P_{\min}(n) \geq 7$	1
$4 \cdot 3^b - t^2$	≥ 0	t	1	-1
$\sqrt[n]{4 \cdot 3^b - t^2}$	≥ 1	t	$P_{\min}(n) \geq 7$	-1

As this case only has solutions when $n = 1$, $P_{\min}(n) \geq 7$ or $p = 13$, we can verify that these two situations are covered by the finitely many primes listed above by (2) and by (3).

Case 3: $t^2 = 4p^n - 3^b$. This is case 3 in [Mul06, p.61-62]. Here $p^n \equiv -1 \pmod 4$ is given and so the case n even is impossible. We can use Lemma 4.8 in [Mul06, p.156-157] to see that the solutions with $b \geq 0$ and n odd are

p	b	t	n	Extra Information
$\frac{t^2+3^b}{4}$	≥ 1 (odd)	t	1	$p \equiv 1 \pmod 3$
$\sqrt[n]{\frac{t^2+3^b}{4}}$	≥ 1 (odd)	t	$P_{\min}(n) \geq 7$	$p \equiv 1 \pmod 3$

As shown in [AAA02], the second case cannot occur for $n \geq 7$. As this case only has solutions when $n = 1$, we can verify that this situation is covered by family (4).

Case 4: $3t^2 = 4p^n - 1$. This is case 5 in [Mul06, p.61-62]. Here $p^n \equiv 1 \pmod 4$ is given. By [Coh07a, p.353] Corollary 6.3.15, we have when $n = 2$ that

$$p = \epsilon(\sigma^2 + \tau^2 + \sigma\tau) \qquad 1 = \delta(\sigma^2 + \tau^2 + 4\sigma\tau)$$

with σ and τ of opposite parity and $\delta, \epsilon \in \{\pm 1\}$. We assume without loss of generality that σ is the even term. In the second equation above, notice that if $\delta = -1$, then modulo 4 considerations give us a contradiction. Hence $\delta = 1$. Next assume towards a contradiction that $2 \parallel \sigma$. Then modulo 8, we have that $1 \equiv 4+1+0 \equiv 5 \pmod 8$ and that is a contradiction. Hence $4 \mid \sigma$. Further, in the equation above involving p, we have that $\sigma^2 + \tau^2 + \sigma\tau > 0$ for any integers σ and τ and so $\epsilon > 0$. Combining this with $4 \mid \sigma$ shows us that

$$p = \sigma^2 + \tau^2 + \sigma\tau \equiv 0 + 1 + 0 \equiv 1 \pmod 4.$$

Thus $p \equiv 1 \pmod 4$ when $n = 2$ and $p \equiv 1 \pmod 4$ when $n = 1$ by necessity of this case. We can use Lemma 4.11 in [Mul06, p.175] to see that the solutions are

p	b	t	n
$\frac{3t^2+1}{4}$	≥ 0	t	1
$\sqrt{\frac{3t^2+1}{4}}$	≥ 1	t	2

As this case only has solutions when $n = 1$ or 2, we can verify that these two situations are covered by family (5).

Case 5: $3t^2 = p^n + 4$. This is case 6 in [Mul06, p.61-62]. We can use Lemma 4.11 in [Mul06, p.174-175] to see that the only solutions are with $p = 3t^2 - 4$. This situation is covered by family (6).

■

Theorem 4.0.11. *Let p be a prime distinct from 2 and 3. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $72p$ provided that p satisfies at least one of the following where $d > 0$, $\ell_1 \in \{2,3\}$, $\ell_2 \in \{4,5\}$, $\ell_3 \in \{2,4,5\}$, $n_1 = 1$ or $P_{\min}(n_1) \geq 7$, $n_2 \in \{1,2\}$ and $m, m_1 \geq 0$ are integers with m_1 odd:*

1. $p = 2^{\ell_1}3^m + 1$.
2. $p = 2^{\ell_1}3^m - 1$.
3. $p = 3^m + 2^{\ell_1}$.
4. $p = 3^m - 2^{\ell_1}$.
5. $p = d^2 + 2^{\ell_3}3^m$.
6. $p^{n_1} = d^2 - 2^{\ell_2}3^m$.
7. $p^{n_1} = 2^{\ell_2}3^m - d^2$.
8. $p = \frac{3^{m_1}+1}{4}$.
9. $p = \frac{3^{m_1}+d^2}{4}$ *with* $p \equiv 1 \pmod 4$.
10. $p^{n_2} = \frac{3d^2+1}{4}$.
11. [1] $p^{n_1} = \frac{d^2+32}{3^m}$.
12. $p = 3d^2 + 2^{\ell_3}$.
13. $p = 3d^2 - 2^{\ell_2}$.
14. $p \in \{5, 7, 11, 13, 17, 23, 29, 31, 37, 47, 67, 73, 107, 109, 193, 1153\}$.

Theorem 4.0.12. *Let p be a prime distinct from 2 and 3. Then up to the finitely many primes in*

$$p \in \{5, 7, 11, 13, 17, 23, 29, 31, 37, 47, 67, 73, 107, 109, 193, 1153\}$$

the following gives a complete list of the families of elliptic curves with nontrivial rational two torsion of conductor $72p$ associated with the primes in the previous theorem:

(1) The prime p has the form $p = 2^{\ell-2} \cdot 3^m + 1$ with $\ell \in \{4,5\}$, $m \geq 0$ and corresponds to the following elliptic curves

[1] In [BLM11, p.7], this case was erroneously claimed to be for odd m only. In fact cases such as $m = 2$ and $d = 11$ do give valid elliptic curves.

	a_2	a_4	Δ
A1	$-3\psi(2^\ell 3^m p+1)$	$2^{\ell-2}3^{m+2}p$	$2^{2\ell}3^{2m+6}p^2$
A2	$2\cdot 3\psi(2^\ell 3^m p+1)$	3^2	$2^{\ell+6}3^{m+6}p$

	a_2	a_4	Δ
G1	$-3\psi(p^2-2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
G2	$2\cdot 3\psi(p^2-2^\ell 3^m)$	3^2p^2	$-2^{\ell+6}3^{m+6}p^4$

- *In the additional case when $\ell-2=2$, we get solutions given by $p=2^\ell 3^{(2m)/2}+1$ and the curve is given by*

	a_2	a_4	Δ
B1	$3\psi(4\cdot 3^m+p)$	3^{2m+2}	$2^4 3^{4m+6}p$
B2	$-2\cdot 3\psi(4\cdot 3^m+p)$	3^2p	$2^8 3^{2m+6}p^2$

(2) The prime p has the form $p=2^{\ell-2}\cdot 3^m-1$ with $\ell\in\{4,5\}$, $m\geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$-3\psi(2^\ell 3^m p+1)$	$2^{\ell-2}3^{m+2}p$	$2^{2\ell}3^{2m+6}p^2$
A2	$2\cdot 3\psi(2^\ell 3^m p+1)$	3^2	$2^{\ell+6}3^{m+6}p$

	a_2	a_4	Δ
E1	$-3\psi(2^\ell 3^m+p^2)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
E2	$2\cdot 3\psi(2^\ell 3^m+p^2)$	3^2p^2	$2^{\ell+6}3^{m+6}p^4$

- *In the additional case when $\ell-2=2$, we get solutions given by $p=4\cdot 3^{(2m)/2}-1$ with m odd and the curve is given by*

	a_2	a_4	Δ
C1	$3\psi(4\cdot 3^m-p^n)$	3^{2m+2}	$-2^4 3^{4m+6}p$
C2	$-2\cdot 3\psi(4\cdot 3^m-p^n)$	-3^2p	$2^8 3^{2m+6}p^2$

(3) The prime p has the form $p=3^m+2^{\ell-2}$ with $\ell\in\{4,5\}$, $m\geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
G1	$-3\psi(p^2-2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
G2	$2\cdot 3\psi(p^2-2^\ell 3^m)$	3^2p^2	$-2^{\ell+6}3^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p=3^{(2m)/2}+2^{\ell-2}$ given by*

	a_2	a_4	Δ
K1	$-3\psi(2^\ell p + 3^m)$	$2^{\ell-2}3^2 p$	$2^{2\ell}3^{2m+6}p^2$
K2	$2\cdot 3\psi(2^\ell p + 3^m)$	3^{2m+2}	$2^{\ell+6}3^{4m+6}p$

- *Rewriting $\ell - 2$ as $\hat{\ell}/2+1$, we get solutions with $p = 3^m + 2^{\hat{\ell}/2+1}$ given by*

	a_2	a_4	Δ
O1	$-3\psi(2^{\hat{\ell}} + 3^m p)$	$2^{\hat{\ell}-2}3^2$	$2^{2\hat{\ell}}3^{m+6}p$
O2	$2\cdot 3\psi(2^{\hat{\ell}} + 3^m p)$	$3^{m+2}p$	$2^{\hat{\ell}+6}3^{2m+6}p^2$

(4) The prime p has the form $p = 3^m - 2^{\ell-2}$ with $\ell \in \{4,5\}$, $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
E1	$-3\psi(2^\ell 3^m + p^2)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^2$
E2	$2\cdot 3\psi(2^\ell 3^m + p^2)$	$3^2 p^2$	$2^{\ell+6}3^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p = 3^{(2m)/2} + 2^{\ell-2}$ given by*

	a_2	a_4	Δ
M1	$-3\psi(3^m - 2^\ell p^n)$	$-2^{\ell-2}3^2 p$	$2^{2\ell}3^{2m+6}p^2$
M2	$2\cdot 3\psi(3^m - 2^\ell p^n)$	3^{2m+2}	$-2^{\ell+6}3^{4m+6}p$

- *Rewriting $\ell - 2$ as $\hat{\ell}/2+1$, we get solutions with $p = 3^m + 2^{\hat{\ell}/2+1}$ given by*

	a_2	a_4	Δ
O1	$-3\psi(2^{\hat{\ell}} + 3^m p)$	$2^{\hat{\ell}-2}3^2$	$2^{2\hat{\ell}}3^{m+6}p$
O2	$2\cdot 3\psi(2^{\hat{\ell}} + 3^m p)$	$3^{m+2}p$	$2^{\hat{\ell}+6}3^{2m+6}p^2$

(5) The prime p has the form $p = d^2 + 2^\ell 3^m$ with $\ell \in \{2,4,5\}$, $m \geq 0$, $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

- *In the case when $\ell = 2$, we have*

	a_2	a_4	Δ
D1	$3\psi(p - 4\cdot 3^m)$	-3^{m+2}	$2^4 3^{2m+6}p$
D2	$-2\cdot 3\psi(p - 4\cdot 3^m)$	$3^2 p$	$-2^8 3^{m+6}p^2$

- *In the case when $\ell \neq 2$, we have*

	a_2	a_4	Δ
G1	$-3\psi(p-2^\ell 3^m)$	$-2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p$
G2	$2\cdot 3\psi(p-2^\ell 3^m)$	$3^2 p$	$-2^{\ell+6}3^{m+6}p^2$

(6) The prime p has the form $p^n = d^2 - 2^\ell 3^m$ with $\ell \in \{4,5\}$, $m \geq 0$, $n = 1$ or $P_{\min}(n) \geq 7$, $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
E1	$-3\psi(2^\ell 3^m + p^n)$	$2^{\ell-2}3^{m+2}$	$2^{2\ell}3^{2m+6}p^n$
E2	$2\cdot 3\psi(2^\ell 3^m + p^n)$	$3^2 p^n$	$2^{\ell+6}3^{m+6}p^{2n}$

(7) The prime p has the form $p^n = 2^\ell 3^m - d^2$ with $\ell \in \{4,5\}$, $m \geq 0$, $n = 1$ or $P_{\min}(n) \geq 7$, $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
F1	$-3\psi(2^\ell 3^m - p^n)$	$2^{\ell-2}3^{m+2}$	$-2^{2\ell}3^{2m+6}p^n$
F2	$2\cdot 3\psi(2^\ell 3^m - p^n)$	$-3^2 p^n$	$2^{\ell+6}3^{m+6}p^{2n}$

(8) The prime p has the form $p = \frac{3^m+1}{4}$ with $m \geq 1$ odd and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$-3\psi(2^4 3^m p + 1)$	$2^2 3^{m+2}p$	$2^8 3^{2m+6}p^2$
A2	$2\cdot 3\psi(2^4 3^m p + 1)$	3^2	$2^{10}3^{m+6}p$

- *If $p \equiv 1 \pmod 4$ then also*

	a_2	a_4	Δ
I1	$3\psi(4p^2 - 3^m)$	$3^2 p^2$	$-2^4 3^{m+6}p^4$
I2	$-2\cdot 3\psi(4p^2 - 3^m)$	-3^{m+2}	$2^8 3^{2m+6}p^2$

- *In addition, replacing m above with $2m$, then we get solutions with $p = \frac{3^{(2m)/2}+1}{4}$ given by*

	a_2	a_4	Δ
K1	$-3\psi(2^4 p + 3^{2m})$	$2^2 3^2 p$	$2^8 3^{2m+6}p^2$
K2	$2\cdot 3\psi(2^4 p + 3^{2m})$	3^{2m+2}	$2^{10}3^{4m+6}p$

(9) The prime p has the form $p = \frac{d^2+3^m}{4}$ with $m \geq 1$ odd, $p \equiv 1 \pmod 4$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
I1	$3\psi(4p-3^m)$	3^2p	$-2^43^{m+6}p^2$
I2	$-2\cdot 3\psi(4p-3^m)$	-3^{m+2}	$2^83^{2m+6}p$

(10) The prime p has the form $p^n=\frac{3d^2+1}{4}$ with d an integer, $n\in\{1,2\}$, $s\in\{0,1\}$, and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
S1	$-\epsilon\cdot 3^{s+1}\psi(\frac{4p^n-1}{3})$	$3^{2s+1}p^n$	$-2^43^{6s+3}p^{2n}$
S2	$\epsilon\cdot 2\cdot 3^{s+1}\psi(\frac{4p^n-1}{3})$	-3^{2s+1}	$2^83^{6s+3}p^n$

where $\epsilon\in\{\pm1\}$ is the residue of 3^{s+1} modulo 4.

(11) The prime p has the form $p^n=\frac{d^2+32}{3^m}$ with $m\geq 0$, $n=1$ or $P_{\min}(n)\geq 7$, $d\in\mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
Q1	$-3\psi(3^mp^n-2^5)$	-2^33^2	$2^{10}3^{m+6}p^n$
Q2	$2\cdot 3\psi(3^mp^n-2^5)$	$3^{m+2}p^n$	$-2^{11}3^{2m+6}p^{2n}$

(12) The prime p has the form $p=3d^2-2^\ell$ with $\ell\in\{4,5\}$, $s\in\{0,1\}$, $d\in\mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
X1	$\epsilon\cdot 3^{s+1}\psi(\frac{2^\ell+p}{3})$	$2^{\ell-2}3^{2s+1}$	$2^{2\ell}3^{6s+3}p$
X2	$-\epsilon\cdot 2\cdot 3^{s+1}\psi(\frac{2^\ell+p}{3})$	$3^{2s+1}p$	$2^{\ell+6}3^{6s+3}p^2$

where $\epsilon\in\{\pm1\}$ is the residue of 3^{s+1} modulo 4.

(13) The prime p has the form $p=3d^2+2^\ell$ with $\ell\in\{2,4,5\}$, $s\in\{0,1\}$, $d\in\mathbb{Z}$ and corresponds to the following elliptic curves

- *$\ell=2$ and*

	a_2	a_4	Δ
W1	$-\epsilon\cdot 3^{s+1}\psi(\frac{p-4}{3})$	-3^{2s+1}	$2^43^{6s+3}p$
W2	$\epsilon\cdot 2\cdot 3^{s+1}\psi(\frac{p-4}{3})$	$3^{2s+1}p$	$-2^83^{6s+3}p^2$

where $\epsilon\in\{\pm1\}$ is the residue of 3^{s+1} modulo 4.

- *$\ell\in\{4,5\}$ and*

	a_2	a_4	Δ
Z1	$\epsilon \cdot 3^{s+1}\psi(\frac{p-2^\ell}{3})$	$-2^{\ell-2}3^{2s+1}$	$2^{2\ell}3^{6s+3}p$
Z2	$-\epsilon \cdot 2 \cdot 3^{s+1}\psi(\frac{p-2^\ell}{3})$	$3^{2s+1}p$	$-2^{\ell+6}3^{6s+3}p^2$

where $\epsilon \in \{\pm 1\}$ *is the residue of* 3^{s+1} *modulo* 4.

Proof. To show this, we proceed in cases. We use the families in [Mul06, p.58-60] and simplify them according to [Mul06, p.153-175]. In what follows, $\delta, \epsilon \in \{\pm 1\}$ not both negative.

Case 1: $t^2 = 2^a 3^b p^n + 1$. This is case 1 in [Mul06, p.62-67]. We can use Lemma 4.7 in [Mul06, p.153] to see that the solutions with $a \in \{4, 5\}$ and $b \geq 0$ are

p	a	b	t	n	Extra Information
$\frac{3^b+1}{4}$	4	≥ 0 odd	$8p-1$	1	none
$2^{a-2} \cdot 3^b \pm 1$	≥ 3	≥ 0	$2p \mp 1$	1	none
$2^{a-2} \pm 1$	≥ 5	0	$2p \mp 1$	1	none
$\frac{2^{a-2}+1}{3^b}$	≥ 5	≥ 1	$2^{a-1}+1$	1	$3^b \vert a-2$
5	4	0	9	1	none
5	5	1	49	2	none

Since we only care about cases when $a = 4$ or 5, in the fourth case above, since $3^b | a-2$ and $a = 5$, the only case that this applies is $a = 5$ and $b = 1$. Here $\frac{2^{a-2}+1}{3^b} = 3$ is impossible since $p > 3$. Further, cases two and three in the table above can be merged together. As this case only has solutions when $n = 1$ or $p = 5$, we can verify that these situations are covered by the finitely many primes listed above and families (1), (2) and (8).

Case 2: $t^2 = 4 \cdot 3^b + \delta p^n$. This is a combination of cases 2 and 4 in [Mul06, p.62-67]. Here b is given to be even. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $b \geq 0$ are

p	b	t	n	δ
$t^2 - 4 \cdot 3^b$	≥ 0	t	1	1
13	0	47	3	1
$\sqrt[n]{t^2 - 4 \cdot 3^b}$	≥ 1	t	$P_{\min}(n) \geq 7$	1
$4 \cdot 3^b - t^2$	≥ 0	t	1	-1
$\sqrt[n]{4 \cdot 3^b - t^2}$	≥ 0	t	$P_{\min}(n) \geq 7$	-1

In the cases above when $p \neq 13$, notice that we have

$$p^n = t^2 - 4 \cdot 3^b = (t - 2 \cdot 3^{b/2})(t + 2 \cdot 3^{b/2}) \quad \text{or} \quad p^n = 4 \cdot 3^b - t^2 = (2 \cdot 3^{b/2} - t)(2 \cdot 3^{b/2} + t)$$

As the two factors are coprime, we have that $t - 2 \cdot 3^{b/2} = 1$ or $2 \cdot 3^{b/2} - t = 1$. Plugging this into the original equation gives

$$p^n = t^2 - 4 \cdot 3^b = (2 \cdot 3^{b/2} + 1)^2 - 4 \cdot 3^b = 4 \cdot 3^{b/2} + 1$$

which according to [Luc02] cannot occur when $n \geq 5$ and so we can assume that $n = 1$ in this case or

$$p^n = 4 \cdot 3^b - t^2 = 4 \cdot 3^b - (2 \cdot 3^{b/2} - 1)^2 = 4 \cdot 3^{b/2} - 1.$$

Now, if $b/2$ is even, we can repeat the above procedure to get

$$p^n = (2 \cdot 3^{b/4} - 1)(2 \cdot 3^{b/4} + 1)$$

and thus $2 \cdot 3^{b/4} - 1 = 1$ so $b = 0$ which gives $p = 3$, a contradiction. Hence in the second case we must have that $b/2$ is odd. If $b/2 < 5$, then we see that

$$4 \cdot 3^{b/2} + 1 \in \{13, 37, 109, 325\}$$

(of which only 325 is not prime) or in the case with $b/2$ odd

$$4 \cdot 3^{b/2} - 1 \in \{11, 107\}$$

and all of these cases are in the list of finitely many primes. Next, suppose that $b/2 \geq 5$. In either case above, via [BVY04], we have that solutions of the form

$$p^n + 4 \cdot 3^{b/2}(-1)^n = (\pm 1)^3$$

correspond to newforms at level 6 which cannot occur. A summary of this result can be found in [Coh07b, p.526-527]. Hence, this case only has solutions when $n = 1$ or p is in the finitely many primes above. We can verify that these situations are covered by the finitely many primes listed above and families (1) and (2).

Case 3: $t^2 = p^n - 4 \cdot 3^b$. This is case 13 in [Mul06, p.62-67]. Here b is given to be odd. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $b \geq 0$ are

p	b	t	n
$t^2 + 4 \cdot 3^b$	≥ 0	t	1
5	0	11	3
13	5	35	3
$\sqrt[n]{t^2 + 4 \cdot 3^b}$	≥ 0	t	$P_{\min}(n) \geq 7$

According to [Luc02], we know that in the final case $n < 5$ and so this case only has solutions when $n = 1$ or $p = 5$ or 13. We can verify that these situations are covered by the finitely many primes listed above and family (5).

Case 4: $t^2 = \epsilon p^n + \delta 2^a 3^b$. This is a combination of cases 3,5, and 14 in [Mul06, p.62-67]. We can use Lemma 4.9 in [Mul06, p.165] to see that the solutions with $a \in \{4.5\}$ and $b \geq 0$ are

p	a	b	t	n	δ	ϵ
$t^2 - 2^a \cdot 3^b$	≥ 2	≥ 0	t	1	1	1
$2^{a-2} \cdot 3^b - 1$	≥ 3	≥ 0	$2^{a-1} + p$	2	1	1
$3^b - 2^{a-2}$	≥ 3	≥ 0	$2^{a-1} - p$	2	1	1
$2^{a-2} - 3^b$	≥ 5	≥ 1	$p + 2$	2	1	1
$\sqrt[n]{t^2 - 2^a \cdot 3^b}$	≤ 5	≥ 0	t	$P_{\min}(n) \geq 7$	1	1
$t^2 + 2^a \cdot 3^b$	≥ 1	≥ 0	t	1	-1	1
$2^{a-2} \cdot 3^b + 1$	≥ 3	≥ 0	$2^{a-1} + p$	2	-1	1
$3^b + 2^{a-2}$	≥ 3	≥ 0	$2^{a-1} - p$	2	-1	1
73	4	7	595	3	-1	1
193	4	4	2681	3	-1	1
1153	5	5	39151	3	-1	1
5	5	1	23	4	-1	1
$\sqrt[n]{t^2 + 2^a \cdot 3^b}$	≤ 5	≥ 0	t	$P_{\min}(n) \geq 7$	-1	1
$2^a \cdot 3^b - t^2$	≥ 1	≥ 0	t	1	1	-1
73	5	11	2359	3	1	-1
$\sqrt[n]{2^a \cdot 3^b - t^2}$	≤ 5	≥ 0	t	$P_{\min}(n) \geq 7$	1	-1

As before, we can use [Luc02], we know that $n < 5$ when $p^n = t^2 + 2^a 3^b$. Also, the case where $p = 2^{a-2} - 3^b$ when $a = 4$ or 5 only gives the case $p = 3, 5$, or 7 and so this can be simplified. Summarizing, this case only has solutions when $n = 1$, $n = 2$, $P_{\min}(n) \geq 7$ or $p = 5, 7, 73, 193$, or 1153, we can verify that these situations are covered by the finitely many primes listed above and families (1), (2), (3), (4), (5), (6), and (7).

Case 5: $t^2 = 3^b + \delta 2^a p^n$. This is a combination of cases 6 and 12 in [Mul06, p.62-67]. We can use Lemma 4.8 in [Mul06, p.156-157] to see that the solutions with $a \in \{4, 5\}$ and $b \geq 0$ are

p	a	b	t	n	δ
$\frac{3^{b/2}+1}{4}$	4	$b/2$ odd	$3^{b/2}+2$	1	1
$2^{a-2} \pm 3^{b/2}$	≥ 3	≥ 0 even	$2p \mp 3^{b/2}$	1	1
$3^{b/2} - 2^{a-2}$	≥ 3	≥ 0 even	$\pm(2p - 3^{b/2})$	1	-1

In the second case above, we only need the positive case as the negative case gives solutions $p = 5$ and $p = 7$, both of which are in the first family. As this case only has solutions when $n = 1$ or $p = 5$ or 7 under the simplification above, we can verify that these situations are covered by the finitely many primes listed above and families (3), (4) and (8).

Case 6: $t^2 = 4p^n - 3^b$. This is case 7 in [Mul06, p.62-67]. We can use Lemma 4.8 in [Mul06, p.156-157] to see that the solutions with $b \geq 0$ are

p	b	t	n	Extra Information
$\frac{t^2+3^b}{4}$	≥ 0 odd	t	1	$p \equiv 1 \pmod 3$
$\frac{3^b+1}{4}$	≥ 0 odd	$2p-1$	2	none
$\sqrt[n]{\frac{3^b+1}{4}}$	≥ 0 odd	t	$P_{\min}(n) \geq 7$	$p \equiv 1 \pmod 3$

As shown in [AAA02], the third case cannot occur for $n \geq 7$. All of the situations above are covered in the family (8) and (9).

Case 7: $t^2 = 2^a + \delta 3^b p^n$. This is a combination of cases 9 and 10 in [Mul06, p.62-67]. We can use Lemma 4.10 in [Mul06, p.171-172] to see that the solutions with $a \in \{2, 4, 5\}$ and $b \geq 1$ (possible to assume since we covered $b = 0$ in case 4) are

p	a	b	t	n	δ
$3^b \pm 4$	2	≥ 1	$p \mp 2$	1	1
$3^b \pm 2^3$	4	≥ 1	$p \mp 4$	1	1
$2^3 - 3^b$	4	≥ 1	$\pm(4 - p)$	1	-1

The last case above only has positive solutions for $b = 0$ or $b = 1$ giving $p = 7$ or $p = 5$. As this case only has solutions when $n = 1$ and $a = 2, 4$ or $p = 5$, or 7, we can verify that these situations are covered by the finitely many primes listed above and families (3) and (4).

Case 8: $t^2 = 3^b p^n - 2^a$. This is case 11 in [Mul06, p.62-67]. Now, we can assume that $b \geq 1$ since when $b = 0$, we can refer back to case 4. Notice that since $b \geq 1$, we know that

$a = 4$ cannot happen by local considerations of the equation at 3. We can use Lemma 4.10 in [Mul06, p.156-157] to see that the solutions with $a \in \{4, 5\}$ and $b \geq 1$ are

p	a	b	t	n
$\frac{t^2+2^a}{3^b}$	5	≥ 1	t	1
$\frac{2^{a-2}+1}{3^{b/2}}$	5	≥ 1 (even)	$3^{b/2}p - 2$	2
67	5	3	8549	3
$\sqrt[n]{\frac{t^2+2^a}{3^b}}$	5	≥ 1	t	$P_{\min}(n) \geq 7$

As this case only has solutions when $n = 1$, $P_{\min}(n) \geq 7$ or $p = 17$, we can verify that these situations are covered by the finitely many primes listed above and family (11).

Case 9: $3t^2 = 2^a + \delta p^n$. This is a combination of cases 15 and 16 in [Mul06, p.62-67]. We can use Lemma 4.10 in [Mul06, p.174-175] to see that the solutions with $a \in \{4, 5\}$ are of the form $p = \delta(3t^2 - 2^a)$. When $\delta = -1$ then since we are only considering cases with $a \in \{4, 5\}$, we only get the primes $p = 13, 29$. This situation is covered by family (13).

Case 10: $3t^2 = p^n - 2^a$. This is a combination of cases 18 and 19 in [Mul06, p.62-67]. We can use Lemma 4.10 in [Mul06, p.174-175] to see that the solutions with $a \in \{2, 4, 5\}$ are of the form $p = 3t^2 + 2^a$. This situation is covered by family (12).

Case 11: $3t^2 = 4p^n - 1$. This is case 17 in [Mul06, p.62-67]. We can use Lemma 4.10 in [Mul06, p.174-175] to see that the solutions to this equation are of the form $p^n = 3t^2 - 1$ with $n = 1$ or 2. This situation is covered by family (10).

■

Chapter 5

Elliptic Curves With Rational Two Torsion and Conductor $50p$, $200p$ or $400p$ Organized by Primes

In this section, we continue our classification of elliptic curves with rational two torsion and given conductor. Before beginning this section, I would like to remind the reader of the notes of Chapter 4. These same notes apply here. In this section I suppress the formal proof as well. These are done the same way as in the previous chapter except all of this work is contained in this thesis.

Theorem 5.0.13. *Let p be a prime distinct from 2 and 5. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $50p$ provided that p satisfies at least one of the following where $d > 0$, $\ell_1 \geq 5$, $\ell_2 \geq 7$ and $m \geq 0$ are integers:*

1. $p \in \{3, 7, 11, 13, 17, 31, 37, 41\}$
2. $p = 2^{\ell_1}5^m + 1$.
3. $p = 2^{\ell_1}5^m - 1$.
4. $p = \frac{2^{\ell_1}+1}{5^m}$.
5. $p = 2^{\ell_1} - 5^m$.
6. $p = 5^m - 2^{\ell_1}$.
7. $p = 2^{\ell_2} + 5^m$.
8. $p = d^2 - 2^{\ell_2}5^m$.
9. $p = 2^{\ell_2}5^m - d^2$.

10. $p = d^2 + 2^{\ell_2}5^m$.

11. $p = 5d^2 - 2^{\ell_2}$.

12. $p = 2^{\ell_2} - 5d^2$.

13. $p = 5d^2 + 2^{\ell_2}$.

Theorem 5.0.14. *Let p be a prime distinct from 2 and 5. Then up to the finitely many primes in*

$$p \in \{3, 7, 11, 13, 17, 31, 37, 41\}$$

the following gives a complete list of the elliptic curves with nontrivial rational two torsion of conductor $50p$ associated with the primes in the previous theorem:

(1) The prime p has the form $p = 2^{\ell-2} \cdot 5^m + 1$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$-2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
D1	$5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
D2	$-2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

(2) The prime p has the form $p = 2^{\ell-2} \cdot 5^m - 1$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$-2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
B1	$5\psi(2^\ell 5^m + p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
B2	$-2 \cdot 5\psi(2^\ell 5^m + p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

(3) The prime p has the form $p = \frac{2^{\ell-2}+1}{5^m}$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$-2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

- *In addition, replacing m above with $2m$, then we get solutions via $p = \frac{2^{\ell-2}+1}{5^{(2m)/2}}$ given by,*

	a_2	a_4	Δ
J1	$5\psi(5^{2m}p^2 - 2^\ell)$	$-2^{\ell-2}5^2$	$2^{2\ell}5^{2m+6}p^2$
J2	$-2\cdot 5\psi(5^{2m}p^2 - 2^\ell)$	$5^{2m+2}p^2$	$-2^{\ell+6}5^{4m+6}p^4$

(4) The prime p has the form $p = 2^{\ell-2} - 5^m$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
B1	$5\psi(2^\ell 5^m + p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
B2	$-2\cdot 5\psi(2^\ell 5^m + p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions via $p = 2^{\ell-2} - 5^{(2m)/2}$ given by,*

	a_2	a_4	Δ
E1	$5\psi(2^\ell p + 5^{2m})$	$2^{\ell-2}5^2p$	$2^{2\ell}5^{2m+6}p^2$
E2	$-2\cdot 5\psi(2^\ell p + 5^{2m})$	5^{2m+2}	$2^{\ell+6}5^{4m+6}p$

- *In the additional case that $\ell-2$ can be written as $\hat{\ell}/2+1$ with $\hat{\ell}$ even, we get solutions with $p = 2^{\ell/2+1} - 5^m$ given by*

	a_2	a_4	Δ
I1	$5\psi(2^{\hat{\ell}} - 5^m p)$	$2^{\hat{\ell}-2}5^2$	$-2^{2\hat{\ell}}5^{m+6}p$
I2	$-2\cdot 5\psi(2^{\hat{\ell}} - 5^m p)$	$-5^{m+2}p$	$2^{\hat{\ell}+6}5^{2m+6}p^2$

for this new ℓ

(5) The prime p has the form $p = 5^m - 2^{\ell-2}$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
B1	$5\psi(2^\ell 5^m + p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
B2	$-2\cdot 5\psi(2^\ell 5^m + p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p = 5^{(2m)/2} - 2^{\ell-2}$ given by*

	a_2	a_4	Δ
G1	$5\psi(5^{2m} - 2^\ell p)$	$-2^{\ell-2}5^2p$	$2^{2\ell}5^{2m+6}p^2$
G2	$-2\cdot 5\psi(5^{2m} - 2^\ell p)$	5^{2m+2}	$-2^{\ell+6}5^{4m+6}p$

- *In the additional case that $\ell-2$ can be written as $\hat{\ell}/2+1$ with $\hat{\ell}$ even, we get solutions with $p = 5^m - 2^{\hat{\ell}/2+1}$ given by*

	a_2	a_4	Δ
H1	$5\psi(2^{\hat{\ell}} + 5^m p)$	$2^{\hat{\ell}-2}5^2$	$2^{2\hat{\ell}}5^{m+6}p$
H2	$-2 \cdot 5\psi(2^{\hat{\ell}} + 5^m p)$	$5^{m+2}p$	$2^{\hat{\ell}+6}5^{2m+6}p^2$

(6) The prime p has the form $p = 2^{\ell-2} + 5^m$ with $\ell \geq 7$ and $m \geq 0$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
D1	$5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
D2	$-2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

- *In addition, replacing m above with $2m$, then we get solutions with $p = 2^{\ell-2}+5^{(2m)/2}$ given by*

	a_2	a_4	Δ
E1	$5\psi(2^\ell p + 5^{2m})$	$2^{\ell-2}5^2p$	$2^{2\ell}5^{2m+6}p^2$
E2	$-2 \cdot 5\psi(2^\ell p + 5^{2m})$	5^{2m+2}	$2^{\ell+6}5^{4m+6}p$

- *In the additional case that $\ell-2$ can be written as $\hat{\ell}/2+1$ with $\hat{\ell}$ even, we get solutions with $p = 2^{\hat{\ell}/2+1} + 5^m$ given by*

	a_2	a_4	Δ
H1	$5\psi(2^{\hat{\ell}} + 5^m p)$	$2^{\hat{\ell}-2}5^2$	$2^{2\hat{\ell}}5^{m+6}p$
H2	$-2 \cdot 5\psi(2^{\hat{\ell}} + 5^m p)$	$5^{m+2}p$	$2^{\hat{\ell}+6}5^{2m+6}p^2$

(7) The prime p has the form $p = d^2 - 2^\ell 5^m$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
B1	$5\psi(2^\ell 5^m + p)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p$
B2	$-2 \cdot 5\psi(2^\ell 5^m + p)$	5^2p	$2^{\ell+6}5^{m+6}p^2$

(8) The prime p has the form $p = 2^\ell 5^m - d^2$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
C1	$5\psi(2^\ell 5^m - p)$	$2^{\ell-2}5^{m+2}$	$-2^{2\ell}5^{2m+6}p$
C2	$-2 \cdot 5\psi(2^\ell 5^m - p)$	-5^2p	$2^{\ell+6}5^{m+6}p^2$

(9) The prime p has the form $p = d^2 + 2^\ell 5^m$ with $\ell \geq 7$, $m \geq 0$ and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
D1	$5\psi(p-2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p$
D2	$-2\cdot 5\psi(p-2^\ell 5^m)$	$5^2 p$	$-2^{\ell+6}5^{m+6}p^2$

(10) The prime p has the form $p=5d^2-2^\ell$ with $\ell\geq 7$, $m\geq 0$, $d\in\mathbb{Z}$ and $s\in\{0,1\}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
M1	$5^{s+1}\psi(\frac{2^\ell+p}{5})$	$2^{\ell-2}5^{2s+1}$	$2^{2\ell}5^{6s+3}p$
M2	$-2\cdot 5^{s+1}\psi(\frac{2^\ell+p}{5})$	$5^{2s+1}p$	$2^{\ell+6}5^{6s+3}p^2$

(11) The prime p has the form $p=2^\ell-5d^2$ with $\ell\geq 7$, $m\geq 0$, $d\in\mathbb{Z}$ and $s\in\{0,1\}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
N1	$5^{s+1}\psi(\frac{2^\ell-p}{5})$	$2^{\ell-2}5^{2s+1}$	$-2^{2\ell}5^{6s+3}p$
N2	$-2\cdot 5^{s+1}\psi(\frac{2^\ell-p}{5})$	$-5^{2s+1}p$	$2^{\ell+6}5^{6s+3}p^2$

(12) The prime p has the form $p=5d^2+2^\ell$ with $\ell\geq 7$, $m\geq 0$, $d\in\mathbb{Z}$ and $s\in\{0,1\}$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
O1	$5^{s+1}\psi(\frac{p-2^\ell}{5})$	$-2^{\ell-2}5^{2s+1}$	$2^{2\ell}5^{6s+3}p$
O2	$-2\cdot 5^{s+1}\psi(\frac{p-2^\ell}{5})$	$5^{2s+1}p$	$-2^{\ell+6}5^{6s+3}p^2$

Theorem 5.0.15. *Let p be a prime distinct from 2 and 5. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $200p$ provided that p satisfies at least one of the following where $d>0$, $\ell_1\in\{2,4,5\}$, $\ell_2\in\{4,5\}$, $\ell_3\in\{3,4,5\}$ and $m\geq 0$ are integers:*

1. $p\in\{3,7,11,13,17,23,31,37,41\}$.
2. $p=2^{\ell_2-2}\cdot 5^m+1$ *with* $m\geq 1$.
3. $p=2^{\ell_2-2}\cdot 5^m-1$ *with* $m\geq 1$.
4. $p^n=\frac{5^m-1}{4}$ *with* $m\geq 1$ *odd and* $n=1$ *or* $P_{\min}(n)\geq 7$.
5. $p^n=\left(\frac{5^m-1}{4}\right)^2$ *with* $n=2$ *or* $2\parallel n$ *and* $P_{\min}(n/2)\geq 7$.
6. $p^n=\frac{d^2-5^m}{4}$ *with* m *odd and either* $n=1$ *or* $P_{\min}(n)\geq 7$.
7. $p^n=\frac{5^m-d^2}{4}$ *with* m *odd and either* $n=1$ *or* $P_{\min}(n)\geq 7$ *or* n *even.*
8. $p^n=\frac{5^m-d^2}{2^{\ell_2}}$ *with* m *even and* $P_{\min}(n)\geq 7$.

9. $p^n = 2^{\ell_2-2} + 5^m$ *with* $m \geq 1$ *and either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

10. $p^n = 5^m - 2^{\ell_2-2}$ *with* $m \geq 1$ *and either* $n = 1$ *or both* $\ell_2 = 4$ *and* $P_{\min}(n) \geq 7$.

11. $p^n = (5^m - 4)^2$ *with* $m \geq 1$ *and either* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

12. $p^n = d^2 - 2^{\ell_1}5^m$ *with* $n = 1$ *or* $P_{\min}(n) \geq 7$.

13. $p^n = 2^{\ell_1}5^m - d^2$ *with* $n = 1$ *or* $P_{\min}(n) \geq 7$.

14. $p = d^2 + 2^{\ell_1}5^m$.

15. $p^n = \frac{d^2+4}{5^m}$ *with* $m \geq 1$ *odd and either* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

16. $p^n = \frac{d^2+2^{\ell_1}}{5^m}$ *with* $m \geq 1$ *and either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

17. $p^n = \frac{5d^2-1}{4}$ *with* $p^n \equiv 1 \pmod 4$ *and* $n = 1$, $n = 2$, $P_{\min}(n) \geq 7$ *or both* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

18. $p^n = 5d^2 - 2^{\ell_1}$ *with either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

19. $p^n = 5d^2 - 4$ *with either* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

20. $p^n = 5d^2 + 2^{\ell_2}$ *with either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

21. $p^n = 5d^2 + 4$ *with either* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

Theorem 5.0.16. *Let* p *be a prime distinct from* 2 *and* 5. *Then up to the finitely many primes in*

$$p \in \{3, 7, 11, 13, 17, 23, 31, 37, 41\}$$

the following gives a complete list of the elliptic curves with nontrivial rational two torsion of conductor $200p$ *associated with the primes in the previous theorem:*

(1) The prime p *has the form* $p = 2^{\ell-2} \cdot 5^m + 1$ *with* $\ell \in \{4, 5\}$ *and* $m > 0$ *and corresponds to the following elliptic curves*

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$-2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
G1	$5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
G2	$-2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

(2) The prime p has the form $p = 2^{\ell-2} \cdot 5^m - 1$ with $\ell \in \{4, 5\}$ and $m > 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$-2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
E1	$5\psi(2^\ell 5^m + p^n)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
E2	$-2 \cdot 5\psi(2^\ell 5^m + p^n)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

(3) The prime p has the form $p^n = \frac{5^m-1}{4}$ with and $m \geq 1$ odd and corresponds to the following elliptic curves

- *Either $n = 1$ or $P_{\min}(n) \geq 7$ and the curve is given by*

	a_2	a_4	Δ
A1	$5\psi(2^\ell 5^m p^n + 1)$	$2^2 5^{m+2}p^n$	$2^8 5^{2m+6}p^{2n}$
A2	$-2 \cdot 5\psi(2^\ell 5^m p^n + 1)$	5^2	$2^{10}5^{m+6}p^n$

- *$n = 1$ and the curve is given by*

	a_2	a_4	Δ
H1	$-5\psi(4p^2 + 5^m)$	5^2p^2	$2^4 5^{m+6}p^4$
H2	$2 \cdot 5\psi(4p^2 + 5^m)$	5^{m+2}	$2^8 5^{2m+6}p^2$

- *We have $n = 1$ and in addition, replacing m above with $2m$, then we get solutions via $p = \frac{5^{(2m)/2}-1}{4}$ given by,*

	a_2	a_4	Δ
M1	$5\psi(5^{2m} - 2^4p^n)$	$-2^2 5^2 p$	$2^8 5^{2m+6}p^2$
M2	$-2 \cdot 5\psi(5^{2m} - 2^4p^n)$	5^{2m+2}	$-2^{10}5^{4m+6}p$

(4) The prime p has the form $p^n = \left(\frac{5^m-1}{4}\right)^2$ with and $m \geq 1$ odd, $n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
H1	$-5\psi(4p^n + 5^m)$	5^2p^n	$2^4 5^{m+6}p^{2n}$
H2	$2 \cdot 5\psi(4p^n + 5^m)$	5^{m+2}	$2^8 5^{2m+6}p^n$

(5) The prime p has the form $p^n = \frac{d^2-5^m}{4}$ with $m \geq 1$ odd and $d \in \mathbb{Z}$ and corresponds to the following elliptic curves

- *Either* $n = 1$ *or* $P_{\min}(n) \geq 7$ *and the curve is given by*

	a_2	a_4	Δ
H1	$-5\psi(4p^n + 5^m)$	$5^2 p^n$	$2^4 5^{m+6} p^{2n}$
H2	$2 \cdot 5\psi(4p^n + 5^m)$	5^{m+2}	$2^8 5^{2m+6} p^n$

(6) The prime p *has the form* $p^n = \frac{5^m - d^2}{4}$ *with* $m \geq 1$ *odd and* $d \in \mathbb{Z}$ *and corresponds to the following elliptic curves*

- *Either* $n = 1$, $P_{\min}(n) \geq 7$ *or* n *is even,* m *is odd and the curve is given by*

	a_2	a_4	Δ
J1	$-5\psi(5^m - 4p^n)$	$-5^2 p^n$	$2^4 5^{m+6} p^{2n}$
J2	$2 \cdot 5\psi(5^m - 4p^n)$	5^{m+2}	$-2^8 5^{2m+6} p^n$

(7) The prime p *has the form* $p^n = \frac{5^m - d^2}{2^\ell}$ *with* $\ell \in \{4, 5\}$, m *even,* $P_{\min}(n) \geq 7$ *and corresponds to the following elliptic curve*

-

	a_2	a_4	Δ
M1	$5\psi(5^m - 2^\ell p^n)$	$-2^{\ell-2} 5^2 p^n$	$2^{2\ell} 5^{m+6} p^{2n}$
M2	$-2 \cdot 5\psi(5^m - 2^\ell p^n)$	5^{m+2}	$-2^{\ell+6} 5^{2m+6} p^n$

(8) The prime p *has the form* $p^n = 2^{\ell-2} + 5^m$ *with and* $m \geq 1$ *and corresponds to the following elliptic curves*

- $n = 1$, $\ell \in \{4, 5\}$ *and*

	a_2	a_4	Δ
G1	$5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2} 5^{m+2}$	$2^{2\ell} 5^{2m+6} p^2$
G2	$-\epsilon \cdot 2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	$5^2 p^2$	$-2^{\ell+6} 5^{m+6} p^4$

- $n = 1$ *or* $P_{\min}(n) \geq 7$, $\ell \in \{4, 5\}$ *with* $p^n = 2^{\ell-2} + 5^{(2m)/2}$ *and*

	a_2	a_4	Δ
K1	$5\psi(2^\ell p^n + 5^m)$	$2^{\ell-2} 5^2 p^n$	$2^{2\ell} 5^{2m+6} p^{2n}$
K2	$-\epsilon \cdot 2 \cdot 5\psi(2^\ell p^n + 5^m)$	5^{2m+2}	$2^{\ell+6} 5^{4m+6} p^n$

- $\ell = 4$ *so* $\ell - 2 = 2$, $n = 1$ *or* $P_{\min}(n) \geq 7$ *and*

	a_2	a_4	Δ
N1	$-5\psi(4 + 5^m p^n)$	5^2	$2^4 5^{m+6} p^n$
N2	$2 \cdot 5\psi(4 + 5^m p^n)$	$5^{m+2} p^n$	$2^8 5^{2m+6} p^{2n}$

- $n = 1$, $\ell = 5$ *so* $\ell - 2 = 3 = 4/2 + 1$ *and*

	a_2	a_4	Δ
O1	$5\psi(16+5^m p)$	$2^2 5^2$	$2^8 5^{m+6} p$
O2	$-2\cdot 5\psi(16+5^m p)$	$5^{m+2} p$	$2^{10} 5^{2m+6} p^2$

(9) The prime p has the form $p^n = 5^m - 2^{\ell-2}$ with and $m \geq 1$ and corresponds to the following elliptic curves

- *$n = 1$ and $\ell \in \{4, 5\}$ and the elliptic curve is given by*

	a_2	a_4	Δ
M1	$5\psi(5^m - 2^\ell p)$	$-2^{\ell-2} 5^2 p$	$2^{2\ell} 5^{m+6} p^2$
M2	$-2\cdot 5\psi(5^m - 2^\ell p)$	5^{m+2}	$-2^{\ell+6} 5^{2m+6} p$

- *Either $n = 1$ or $P_{\min}(n) \geq 7$ and $\ell = 4$ so $\ell - 2 = 2 = 2/2 + 1$giving*

	a_2	a_4	Δ
N1	$-5\psi(4+5^m p^n)$	5^2	$2^4 5^{m+6} p^n$
N2	$2\cdot 5\psi(4+5^m p^n)$	$5^{m+2} p^n$	$2^8 5^{2m+6} p^{2n}$

- *$n = 1$ with $\ell \in \{4, 5\}$ and the elliptic curve is given by*

	a_2	a_4	Δ
E1	$5\psi(2^\ell 5^m + p)$	$2^{\ell-2} 5^{m+2}$	$2^{2\ell} 5^{2m+6} p$
E2	$-2\cdot 5\psi(2^\ell 5^m + p)$	$5^2 p$	$2^{\ell+6} 5^{m+6} p^2$

- *$n = 1$, $\ell = 5$ and so $\ell - 2 = 3 = 4/2 + 1$ and*

	a_2	a_4	Δ
O1	$5\psi(16+5^m p)$	$2^2 5^2$	$2^8 5^{m+6} p$
O2	$-2\cdot 5\psi(16+5^m p)$	$5^{m+2} p$	$2^{10} 5^{2m+6} p^2$

(10) The prime p has the form $p^n = (5^m - 4)^2$ with $m \geq 1$ odd and either $n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and corresponds to the following elliptic curve

	a_2	a_4	Δ
E1	$5\psi(2^4 5^m + p^n)$	$2^2 5^{m+2}$	$2^8 5^{2m+6} p^n$
E2	$-2\cdot 5\psi(2^4 5^m + p^n)$	$5^2 p^n$	$2^{10} 5^{m+6} p^{2n}$

(11) The prime p has the form $p^n = d^2 - 2^\ell \cdot 5^m$ with $m \geq 0$, $d \in \mathbb{Z}$, $\ell \in \{2, 4, 5\}$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

- *$\ell = 2$ and*

	a_2	a_4	Δ
B1	$-5\psi(4\cdot 5^m + p^n)$	5^{m+2}	$2^4 5^{2m+6} p^n$
B2	$2\cdot 5\psi(4\cdot 5^m + p^n)$	$5^2 p^n$	$2^8 5^{m+6} p^{2n}$

- $\ell \in \{4,5\}$ *and*

	a_2	a_4	Δ
E1	$5\psi(2^\ell 5^m + p^n)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^n$
E2	$-2\cdot 5\psi(2^\ell 5^m + p^n)$	$5^2 p^n$	$2^{\ell+6}5^{m+6}p^{2n}$

(12) The prime p has the form $p^n = 2^\ell \cdot 5^m - d^2$ with $m \geq 0$, $d \in \mathbb{Z}$, $\ell \in \{2,4,5\}$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

- $\ell = 2$ *and*

	a_2	a_4	Δ
C1	$-5\psi(4\cdot 5^m - p^n)$	5^{m+2}	$-2^4 5^{2m+6} p^n$
C2	$2\cdot 5\psi(4\cdot 5^m - p^n)$	$-5^2 p^n$	$2^8 5^{m+6} p^{2n}$

- $\ell \in \{4,5\}$ *and*

	a_2	a_4	Δ
F1	$5\psi(2^\ell 5^m - p^n)$	$2^{\ell-2}5^{m+2}$	$-2^{2\ell}5^{2m+6}p^n$
F2	$-2\cdot 5\psi(2^\ell 5^m - p^n)$	$-5^2 p^n$	$2^{\ell+6}5^{m+6}p^{2n}$

(13) The prime p has the form $p = d^2 + 2^\ell \cdot 5^m$ with $m \geq 0$, $d \in \mathbb{Z}$ and $\ell \in \{2,4,5\}$ and corresponds to the following elliptic curves

- $\ell = 2$ *and*

	a_2	a_4	Δ
D1	$-5\psi(p - 4\cdot 5^m)$	-5^{m+2}	$2^4 5^{2m+6} p$
D2	$2\cdot 5\psi(p - 4\cdot 5^m)$	$5^2 p$	$-2^8 5^{m+6} p^2$

- $\ell \in \{4,5\}$ *and*

	a_2	a_4	Δ
G1	$5\psi(p - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p$
G2	$-2\cdot 5\psi(p - 2^\ell 5^m)$	$5^2 p$	$-2^{\ell+6}5^{m+6}p^2$

(14) The prime p has the form $p^n = \frac{d^2+16}{5^m}$ with $m \geq 0$, $d \in \mathbb{Z}$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
Q1	$5\psi(5^m p^n - 16)$	$-2^2 5^2$	$2^8 5^{m+6} p^n$
Q2	$-2 \cdot 5\psi(5^m p^n - 16)$	$5^{m+2} p^n$	$-2^{10} 5^{2m+6} p^{2n}$

(15) The prime p has the form $p^n = \frac{5d^2-1}{4}$ with $p^n \equiv 1 \pmod 4$, $s \in \{0,1\}$, one of $n = 1$, $n = 2$, $P_{\min}(n) \geq 7$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
R1	$-5^{s+1}\psi(\frac{4p^n+1}{5})$	$5^{2s+1} p^n$	$2^4 5^{6s+3} p^{2n}$
R2	$2 \cdot 5^{s+1}\psi(\frac{4p^n+1}{5})$	5^{2s+1}	$2^8 5^{6s+3} p^n$

(16) The prime p has the form $p^n = 5d^2 - 2^\ell$ with $\ell \in \{2,4,5\}$, $s \in \{0,1\}$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

- $\ell = 2$ *and*

	a_2	a_4	Δ
V1	$-5^{s+1}\psi(\frac{4+p^n}{5})$	5^{2s+1}	$2^4 5^{6s+3} p^n$
V2	$2 \cdot 5^{s+1}\psi(\frac{4+p^n}{5})$	$5^{2s+1} p^n$	$2^8 5^{6s+3} p^{2n}$

- $\ell \in \{4,5\}$ *and*

	a_2	a_4	Δ
X1	$5^{s+1}\psi(\frac{2^\ell+p^n}{5})$	$2^{\ell-2} 5^{2s+1}$	$2^{2\ell} 5^{6s+3} p^n$
X2	$-2 \cdot 5^{s+1}\psi(\frac{2^\ell+p^n}{5})$	$5^{2s+1} p^n$	$2^{\ell+6} 5^{6s+3} p^{2n}$

(17) The prime p has the form $p^n = 5d^2 + 2^\ell$ with $\ell \in \{4,5\}$, $s \in \{0,1\}$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
Z1	$5^{s+1}\psi(\frac{p^n-2^\ell}{5})$	$-2^{\ell-2} 5^{2s+1}$	$2^{2\ell} 5^{6s+3} p^n$
Z2	$-2 \cdot 5^{s+1}\psi(\frac{p^n-2^\ell}{5})$	$5^{2s+1} p^n$	$-2^{\ell+6} 5^{6s+3} p^{2n}$

Theorem 5.0.17. *Let p be a prime distinct from 2 and 5. Then there exists an elliptic curve with nontrivial rational two torsion of conductor $400p$ provided that p satisfies at least one of the following where $d > 0$, $\ell_1 \geq 2$, $\ell_2 \geq 4$, $\ell_3 = \lambda$ with $\lambda = 2$ or $\lambda \geq 4$ and $m \geq 0$ are integers:*

1. $p \in \{3, 7, 11, 13, 17, 23, 31, 37, 41\}$.
2. $p = 2^{\ell_1} 5^m + 1$.

3. $p = 2^{\ell_1}5^m - 1$.

4. $p = \frac{2^{\ell_1}+1}{5^m}$.

5. $p^n = \frac{5^m-1}{4}$ *with* m *odd and* $n = 1$ *or* $P_{\min}(n) \geq 7$.

6. $p^n = \left(\frac{5^m-1}{4}\right)^2$ *with* $m \geq 1$ *and* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

7. $p^n = \frac{d^2-5^m}{4}$ *with* m *odd and either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

8. $p^n = \frac{5^m-d^2}{4}$ *with* m *odd and either* $n = 1$, $P_{\min}(n) \geq 7$ *or* n *even.*

9. $p^n = \frac{5^m-d^2}{2^{\ell_3}}$ *with* $\ell_3 \in \{4, 5\}$, m *even and either* $n = 1$ *or* $P_{\min}(n) \geq 7$.

10. $p^n = 2^{\ell_1} + 5^m$ *with* $n = 1$ *or* $P_{\min}(n) \geq 7$.

11. $p^n = 2^{\ell_1} - 5^m$ *with* $n = 1$ *or* $P_{\min}(n) \geq 7$.

12. $p = 5^m - 2^{\ell_2}$ *with* $n = 1$ *or both* $P_{\min}(n) \geq 7$ *and* $\ell_1 = 2$.

13. $p^n = (5^m - 4)^2$ *with* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

14. $p^n = d^2 - 2^{\ell_3}5^m$ *with either* $n = 1$ *or both* $P_{\min}(n) \geq 7$ *and* $\ell_3 \in \{2, 4, 5\}$.

15. $p^n = 2^{\ell_3}5^m - d^2$ *with either* $n = 1$ *or both* $P_{\min}(n) \geq 7$ *and* $\ell_3 \in \{2, 4, 5\}$.

16. $p = d^2 + 2^{\ell_3}5^m$.

17. $p^n = \frac{d^2+2^{\ell_3}}{5^m}$ *with* $m \geq 1$, $n = 1$ *or* $P_{\min}(n) \geq 7$.

18. $p^n = \frac{d^2+4}{5^m}$ *with* $m \geq 1$ *odd and either* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

19. $p^n = \frac{5d^2-1}{4}$ *with* $p^n \equiv 1 \pmod 4$ *and one of* $n = 1$, $n = 2$, $P_{\min}(n) \geq 7$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

20. $p^n = 5d^2 - 2^{\ell_3}$ *with* $n = 1$ *or both* $P_{\min}(n) \geq 7$ *and* $\ell_3 \in \{4, 5\}$.

21. $p^n = 5d^2 - 4$ *with* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

22. $p = 2^{\ell_3} - 5d^2$.

23. $p^n = 5d^2 + 2^{\ell_3}$ *with* $n = 1$ *or both* $P_{\min}(n) \geq 7$ *and* $\ell_3 \in \{4, 5\}$.

24. $p^n = 5d^2 + 4$ *with* $n = 2$ *or* $2 \parallel n$ *and* $P_{\min}(n/2) \geq 7$.

Theorem 5.0.18. *Let p be a prime distinct from 2 and 5. Then up to the finitely many primes in*

$$p \in \{3, 7, 11, 13, 17, 23, 31, 37, 41\}$$

the following gives a complete list of the elliptic curves with nontrivial rational two torsion of conductor $400p$ associated with the primes in the previous theorem:

(1) The prime p has the form $p = 2^{\ell-2} \cdot 5^m + 1$ with $\ell \geq 4$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$-5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
G1	$-5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
G2	$2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

(2) The prime p has the form $p = 2^{\ell-2} \cdot 5^m - 1$ with $\ell \geq 4$ and $m \geq 0$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
A1	$-5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

	a_2	a_4	Δ
E1	$-5\psi(2^\ell 5^m + p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
E2	$2 \cdot 5\psi(2^\ell 5^m + p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

(3) The prime p has the form $p = \frac{2^L+1}{5^m}$ with $L, m \geq 0$ and corresponds to the following elliptic curves

- *If $L = \ell - 2$ for $\ell \geq 4$ even, then*

	a_2	a_4	Δ
A1	$-5\psi(2^\ell 5^m p + 1)$	$2^{\ell-2}5^{m+2}p$	$2^{2\ell}5^{2m+6}p^2$
A2	$2 \cdot 5\psi(2^\ell 5^m p + 1)$	5^2	$2^{\ell+6}5^{m+6}p$

- *If $L = \ell/2$ for $\ell \geq 4$ even and $p = \frac{2^{\ell/2}+1}{5^{(2m)/2}}$ giving*

	a_2	a_4	Δ
R1	$-5\psi(5^{2m}p^n - 2^\ell)$	$-2^{\ell-2}5^2$	$2^{2\ell}5^{2m+6}p^2$
R2	$2 \cdot 5\psi(5^{2m}p^n - 2^\ell)$	$5^{2m+2}p^2$	$-2^{\ell+6}5^{4m+6}p^4$

(4) The prime p has the form $p^n = \frac{5^m-1}{4}$ with $m > 0$ odd and corresponds to the following elliptic curves

- *Either $n = 1$ or $P_{\min}(n) \geq 7$ and*

	a_2	a_4	Δ
A1	$-5\psi(2^\ell 5^m p^n + 1)$	$2^2 5^{m+2} p^n$	$2^8 5^{2m+6} p^{2n}$
A2	$2 \cdot 5\psi(2^\ell 5^m p^n + 1)$	5^2	$2^{10} 5^{m+6} p^n$

- *$n = 1$, $p \equiv 1 \pmod 4$ and*

	a_2	a_4	Δ
J1	$5\psi(5^m - 4p)$	$-5^2 p$	$2^4 5^{m+6} p^2$
J2	$-2 \cdot 5\psi(5^m - 4p)$	5^{m+2}	$-2^8 5^{2m+6} p$

- *$n = 1$ and we have a solution with $p = \frac{5^{(2m)/2}-1}{4}$ given by*

	a_2	a_4	Δ
M1	$-5\psi(5^{2m} - 16p)$	$-2^2 5^2 p$	$2^8 5^{2m+6} p^2$
M2	$2 \cdot 5\psi(5^{2m} - 16p)$	5^{2m+2}	$-2^{10} 5^{4m+6} p$

(5) The prime p has the form $p^n = \left(\frac{5^m-1}{4}\right)^2$ with $m \geq 1$ odd and either $n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and corresponds to the following curve

-

	a_2	a_4	Δ
J1	$5\psi(5^m - 4p^n)$	$-5^2 p^n$	$2^4 5^{m+6} p^{2n}$
J2	$-2 \cdot 5\psi(5^m - 4p^n)$	5^{m+2}	$-2^8 5^{2m+6} p^n$

(6) The prime p has the form $p^n = \frac{d^2-5^m}{4}$ with $m > 0$ odd, $n = 1$ or $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curves

-

	a_2	a_4	Δ
H1	$5\psi(4p^n + 5^m)$	$5^2 p^n$	$2^4 5^{m+6} p^{2n}$
H2	$-2 \cdot 5\psi(4p^n + 5^m)$	5^{m+2}	$2^8 5^{2m+6} p^n$

(7) The prime p has the form $p^n = \frac{5^m-d^2}{4}$ with $m \geq 0$ and either $n = 1$ or both m is odd and $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curve

-

	a_2	a_4	Δ
J1	$5\psi(5^m - 4p^n)$	$-5^2 p^n$	$2^4 5^{m+6} p^{2n}$
J2	$-2 \cdot 5\psi(5^m - 4p^n)$	5^{m+2}	$-2^8 5^{2m+6} p^n$

(8) The prime p has the form $p^n = \frac{5^m - d^2}{2^\ell}$ with $m \geq 0$, $\ell \in \{4, 5\}$ and $P_{\min}(n) \geq 7$ and corresponds to the following elliptic curve

	a_2	a_4	Δ
M1	$-5\psi(5^m - 2^\ell p^n)$	$-2^{\ell-2}5^2p^n$	$2^{2\ell}5^{2m+6}p^{2n}$
M2	$2 \cdot 5\psi(5^m - 2^\ell p^n)$	5^{2m+2}	$-2^{\ell+6}5^{4m+6}p^n$

(9) The prime p has the form $p^n = 2^L + 5^m$ with $L > 0$, $m \geq 0$ and corresponds to the following elliptic curves

- *If $L = \ell - 2$, $\ell \geq 4$ and in this case $p^n = 2^{\ell-2} + 5^{(2m)/2}$ with $n = 1$ or $P_{\min}(n) \geq 7$ and $\ell \in \{4, 5\}$, then we have*

	a_2	a_4	Δ
K1	$-5\psi(2^\ell p^n + 5^{2m})$	$2^{\ell-2}5^2p^n$	$2^{2\ell}5^{2m+6}p^{2n}$
K2	$2 \cdot 5\psi(2^\ell p^n + 5^{2m})$	5^{2m+2}	$2^{\ell+6}5^{4m+6}p^n$

- *If $L = \ell - 2$, $\ell \geq 4$, and $n = 1$, then*

	a_2	a_4	Δ
G1	$-5\psi(p^2 - 2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
G2	$2 \cdot 5\psi(p^2 - 2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

- *If $L = \ell/2 + 1$ for $\ell \geq 4$ even and $n = 1$, then*

	a_2	a_4	Δ
P1	$-5\psi(2^\ell + 5^m p)$	$2^{\ell-2}5^2$	$2^{2\ell}5^{m+6}p$
P2	$2 \cdot 5\psi(2^\ell + 5^m p)$	$5^{m+2}p$	$2^{\ell+6}5^{2m+6}p^2$

- *If $L = 2$ and $n = 1$ or $P_{\min}(n) \geq 7$, then we have*

	a_2	a_4	Δ
N1	$5\psi(4 + 5^m p^n)$	5^2	$2^4 5^{m+6}p^n$
N2	$-2 \cdot 5\psi(4 + 5^m p^n)$	$5^{m+2}p^n$	$2^8 5^{2m+6}p^{2n}$

(10) The prime p has the form $p^n = 2^L - 5^m$ with $L > 0$, $m \geq 0$ and corresponds to the following elliptic curves

- *If $n = 1$ and $L = \ell - 2 \geq 2$ hold we have*

	a_2	a_4	Δ
E1	$-5\psi(2^\ell 5^m + p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
E2	$2 \cdot 5\psi(2^\ell 5^m + p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

- *If $L=\ell-2$, $\ell\geq 4$ and in this case $p^n=2^{\ell-2}+5^{(2m)/2}$ with $n=1$ or $P_{\min}(n)\geq 7$ and $\ell\in\{4,5\}$, then we have*

	a_2	a_4	Δ
K1	$-5\psi(2^\ell p^n+5^{2m})$	$2^{\ell-2}5^2p^n$	$2^{2\ell}5^{2m+6}p^{2n}$
K2	$2\cdot 5\psi(2^\ell p^n+5^{2m})$	5^{2m+2}	$2^{\ell+6}5^{4m+6}p^n$

- *If $n=1$ and $L=\ell-2$ with $\ell\geq 4$, then we have*

	a_2	a_4	Δ
G1	$-5\psi(p^2-2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
G2	$2\cdot 5\psi(p^2-2^\ell 5^m)$	5^2p^2	$-2^{\ell+6}5^{m+6}p^4$

- *If $n=1$ and $L=\ell/2+1$ for $\ell\geq 4$ even we have*

	a_2	a_4	Δ
Q1	$-5\psi(2^\ell-5^mp)$	$2^{\ell-2}5^2$	$-2^{2\ell}5^{m+6}p$
Q2	$2\cdot 5\psi(2^\ell-5^mp)$	$-5^{m+2}p$	$2^{\ell+6}5^{2m+6}p^2$

(11) The prime p has the form $p^n=5^m-2^L$ with $L>0$, $m\geq 0$ and corresponds to the following elliptic curves

- *If $L=\ell-2$, $\ell\geq 4$ and in this case $p=5^{(2m)/2}-2^{\ell-2}$, then we have*

	a_2	a_4	Δ
M1	$-5\psi(5^{2m}-2^\ell p)$	$-2^{\ell-2}5^2p$	$2^{2\ell}5^{2m+6}p^2$
M2	$2\cdot 5\psi(5^{2m}-2^\ell p)$	5^{2m+2}	$-2^{\ell+6}5^{4m+6}p$

- *If $n=1$ and $L=\ell-2\geq 2$ hold we have*

	a_2	a_4	Δ
E1	$-5\psi(2^\ell 5^m+p^2)$	$2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p^2$
E2	$2\cdot 5\psi(2^\ell 5^m+p^2)$	5^2p^2	$2^{\ell+6}5^{m+6}p^4$

- *If $L=\ell/2+1$ for $\ell\geq 4$ even with $n=1$, we have*

	a_2	a_4	Δ
P1	$-5\psi(2^\ell+5^mp)$	$2^{\ell-2}5^2$	$2^{2\ell}5^{m+6}p$
P2	$2\cdot 5\psi(2^\ell+5^mp)$	$5^{m+2}p$	$2^{\ell+6}5^{2m+6}p^2$

- *If $L=2$ and $n=1$ or $P_{\min}(n)\geq 7$, then we have*

	a_2	a_4	Δ
N1	$5\psi(4+5^mp^n)$	5^2	$2^45^{m+6}p^n$
N2	$-2\cdot 5\psi(4+5^mp^n)$	$5^{m+2}p^n$	$2^85^{2m+6}p^{2n}$

(12) The prime p has the form $p^n = (5^m - 4)^2$ with $m \geq 0$ odd, $n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and corresponds to the following elliptic curve

	a_2	a_4	Δ
E1	$-5\psi(16 \cdot 5^m + p^n)$	$2^2 5^{m+2}$	$2^8 5^{2m+6} p^n$
E2	$2 \cdot 5\psi(16 \cdot 5^m + p^n)$	$5^2 p^n$	$2^{10} 5^{m+6} p^{2n}$

(13) The prime p has the form $p^n = d^2 - 2^\ell 5^m$ with $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ and corresponds to the following elliptic curves

- *Either $n = 1$ and $\ell \geq 4$ or $P_{\min}(n) \geq 7$ and $\ell \in \{4, 5\}$ and*

	a_2	a_4	Δ
E1	$-5\psi(2^\ell 5^m + p^n)$	$2^{\ell-2} 5^{m+2}$	$2^{2\ell} 5^{2m+6} p^n$
E2	$2 \cdot 5\psi(2^\ell 5^m + p^n)$	$5^2 p^n$	$2^{\ell+6} 5^{m+6} p^{2n}$

- *$\ell = 2$ and either $n = 1$ or $P_{\min}(n) \geq 7$ and the elliptic curve is given by*

	a_2	a_4	Δ
B1	$5\psi(4 \cdot 5^m + p^n)$	5^{m+2}	$2^4 5^{2m+6} p^n$
B2	$-2 \cdot 5\psi(4 \cdot 5^m + p^n)$	$5^2 p^n$	$2^8 5^{m+6} p^{2n}$

(14) The prime p has the form $p^n = 2^\ell 5^m - d^2$ with $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ and corresponds to the following elliptic curves

- *Either $n = 1$ or $P_{\min}(n) \geq 7$, $\ell = 2$ and $p \equiv 3 \pmod 8$*

	a_2	a_4	Δ
C1	$5\psi(4 \cdot 5^m - p^n)$	5^{m+2}	$-2^4 5^{2m+6} p^n$
C2	$-2 \cdot 5\psi(4 \cdot 5^m - p^n)$	$-5^2 p^n$	$2^8 5^{m+6} p^{2n}$

- *Either $n = 1$ with $\ell \geq 4$ or $P_{\min}(n) \geq 7$ with $\ell \in \{4, 5\}$, $p \equiv 7 \pmod 8$ and the elliptic curve is given by*

	a_2	a_4	Δ
F1	$-5\psi(2^\ell 5^m - p^n)$	$2^{\ell-2} 5^{m+2}$	$-2^{2\ell} 5^{2m+6} p^n$
F2	$2 \cdot 5\psi(2^\ell 5^m - p^n)$	$-5^2 p^n$	$2^{\ell+6} 5^{m+6} p^{2n}$

(15) The prime p has the form $p = d^2 + 2^\ell 5^m$ with $\ell = 2$ or $\ell \geq 4$ and $m \geq 0$ and corresponds to the following elliptic curves

- *Either $m = 0$ and $\ell = 2$ or $\ell \geq 4$ and*

	a_2	a_4	Δ
G1	$-5\psi(p-2^\ell 5^m)$	$-2^{\ell-2}5^{m+2}$	$2^{2\ell}5^{2m+6}p$
G2	$2\cdot 5\psi(p-2^\ell 5^m)$	$5^2 p$	$-2^{\ell+6}5^{m+6}p^2$

(16) The prime p has the form $p^n=\frac{d^2+2^\ell}{5^m}$ with $\ell=2$ or $\ell\geq 4$ and $m\geq 0$ and corresponds to the following elliptic curves

- *$\ell=2$ and either $n=1$, $n=2$, $P_{\min}(n)\geq 7$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$ and*

	a_2	a_4	Δ
O1	$5\psi(5^m p^n-4)$	-5^2	$2^4 5^{m+6}p^n$
O2	$-2\cdot 5\psi(5^m p^n-4)$	$5^{m+2}p^n$	$-2^{10}5^{2m+6}p^{2n}$

- *Either $n=1$ with $\ell\geq 4$ or $P_{\min}(n)\geq 7$ with $\ell=4$ and*

	a_2	a_4	Δ
R1	$-5\psi(5^m p^n-2^\ell)$	$-2^{\ell-2}5^2$	$2^{2\ell}5^{m+6}p^n$
R2	$2\cdot 5\psi(5^m p^n-2^\ell)$	$5^{m+2}p^n$	$-2^{\ell+6}5^{2m+6}p^{2n}$

(17) The prime p has the form $p^n=\frac{5d^2-1}{4}$ with $p^n\equiv 1 \pmod 4$ and either $n=1$, $n=2$, $P_{\min}(n)\geq 7$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$ and corresponds to the following elliptic curve

-

	a_2	a_4	Δ
S1	$5^{s+1}\psi(\frac{4p^n+1}{5})$	$5^{2s+1}p^n$	$2^4 5^{6s+3}p^{2n}$
S2	$-2\cdot 5^{s+1}\psi(\frac{4p^n+1}{5})$	5^{2s+1}	$2^8 5^{6s+3}p^n$

(18) The prime p has the form $p^n=5d^2-2^\ell$ with either $\ell=2$ or $\ell\geq 4$, $s\in\{0,1\}$ and corresponds to the following elliptic curves

- *We have $\ell=2$ with either $n=1$, $n=2$, $P_{\min}(n)\geq 7$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$ giving*

	a_2	a_4	Δ
W1	$5^{s+1}\psi(\frac{4+p^n}{5})$	5^{2s+1}	$2^4 5^{6s+3}p^n$
W2	$-2\cdot 5^{s+1}\psi(\frac{4+p^n}{5})$	$5^{2s+1}p^n$	$2^8 5^{6s+3}p^{2n}$

- *Either $n=1$ and $\ell\geq 4$ or both $\ell\in\{4,5\}$ and $P_{\min}(n)\geq 7$.*

	a_2	a_4	Δ
Y1	$-5^{s+1}\psi(\frac{2^\ell+p^n}{5})$	$2^{\ell-2}5^{2s+1}$	$2^{2\ell}5^{6s+3}p^n$
Y2	$2\cdot 5^{s+1}\psi(\frac{2^\ell+p^n}{5})$	$5^{2s+1}p^n$	$2^{\ell+6}5^{6s+3}p^{2n}$

(19) The prime p has the form $p = 2^\ell - 5d^2$ with $\ell \geq 4$, $s \in \{0,1\}$ and corresponds to the following elliptic curves

	a_2	a_4	Δ
Z1	$-5^{s+1}\psi(\frac{2^\ell - p^n}{5})$	$2^{\ell-2}5^{2s+1}$	$-2^{2\ell}5^{6s+3}p$
Z2	$2\cdot 5^{s+1}\psi(\frac{2^\ell - p^n}{5})$	$-5^{2s+1}p$	$2^{\ell+6}5^{6s+3}p^2$

(20) The prime p has the form $p^n = 5d^2 + 2^\ell$ with either $\ell = 2$ or $\ell \geq 4$, $s \in \{0,1\}$ and corresponds to the following elliptic curves

- *We have $\ell = 2$ with either $n = 1$, $n = 2$, $P_{\min}(n) \geq 7$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ giving*

	a_2	a_4	Δ
X1	$-5^{s+1}\psi(\frac{p^n - 4}{5})$	-5^{2s+1}	$2^4 5^{6s+3}p^n$
X2	$2\cdot 5^{s+1}\psi(\frac{p^n - 4}{5})$	$5^{2s+1}p^n$	$-2^8 5^{6s+3}p^{2n}$

- *Either $n = 1$ and $\ell \geq 4$ or both $P_{\min}(n) \geq 7$ and $\ell \in \{4,5\}$ giving*

	a_2	a_4	Δ
AA1	$-5^{s+1}\psi(\frac{p^n - 2^\ell}{5})$	$-2^{\ell-2}5^{2s+1}$	$2^{2\ell}5^{6s+3}p^n$
AA2	$2\cdot 5^{s+1}\psi(\frac{p^n - 2^\ell}{5})$	$5^{2s+1}p^n$	$-2^{\ell+6}5^{6s+3}p^{2n}$

Chapter 6

On the Diophantine Equation $x^5 + y^5 = p^\alpha z^n$

In this section, we discuss the results on the equation $x^5+y^5 = p^\alpha z^n$ with $n, p \geq 7$ primes, $\alpha \geq 1$ an integer and (x, y, z) a nontrivial solution. Throughout let S_5 be the set of primes $p' \geq 7$ such that there is an elliptic curve $E/\mathbb{Q}$ with conductor $N_E \in \{50p', 200p', 400p'\}$ and at least one nontrivial rational 2-torsion point. The set S_5 contains the primes between 7 and 41 with the first exception being 43. Denote by $C_5(p) = p^{13p}$.

Let $p = 3$ or $p \geq 7$ be a prime and suppose $n \geq C_5(p)$ is prime. Suppose that (a, b, c) is a proper nontrivial solution to $x^5 + y^5 = p^\alpha z^n$, that is,

$$a^5 + b^5 = p^\alpha c^n$$

with a, b, c pairwise coprime. Suppose further that $p \nmid c$, ac is even and that b is odd (possible since at least one of a or b is odd). Further, suppose that $b \equiv -1 \pmod 4$ if c is even and $b \equiv 1 \pmod 4$ if c is odd (to keep consistent with the $q = 3$ case). Following [BD10] via [Kra99][1], we consider the Frey-Hellegouarch curve

$$E_{5,a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x.$$

Setting $R := \mathrm{rad}_{10p}(c)$, we can observe through the use of Tate's Algorithm [Bil07, p.174] or

[1] We have changed the Frey-Hellegouarch curve slightly from this reference inserting a negative coefficient for x^2

more generally using [Mul06, p.13-16] that the conductor of the curve is

$$N(E_{5,a,b}) = \begin{cases} 50pR & \text{if } c \text{ is even, } b \equiv -1 \pmod 4 \\ 200pR & \text{if } c \text{ is odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4 \\ 400pR & \text{if } c \text{ is odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4 \end{cases}$$

where v_2 denotes the usual 2-adic valuation. The standard invariants are given by [Bil07, p.165]

$$\begin{aligned} c_4 &= 2^4 \cdot 5 \left(5(a^2+b^2)^2 - 3\frac{a^5+b^5}{a+b}\right) \\ c_6 &= 2^5 \cdot 5^2 (a^2+b^2) \left(2 \cdot 5(a^2+b^2)^2 - 3^2 \frac{a^5+b^5}{a+b}\right) \\ \Delta &= 2^4 \cdot 5^3 (a+b)^2 (a^5+b^5)^2 = 2^4 \cdot 5^3 (a+b)^2 p^{2\alpha} c^{2n} \\ j(E_{5,a,b}) := \frac{c_4^3}{\Delta} &= \frac{256\left(5(a^2+b^2)^2 - 3\frac{a^5+b^5}{a+b}\right)^3}{(a+b)^2 p^{2\alpha} c^{2n}}. \end{aligned}$$

Since $n \geq C_5(p) \geq 17$ and $j(E_{5,a,b}) \notin \mathbb{Z}[\frac{1}{2}]$, we may apply the result from Mazur (Theorem 1.4.7) to see that $E_{5,a,b}$ does not have any p-isogenies. Thus we can apply Ribet's Level Lowering Theorem. In the case where $n \mid \alpha$, we get a modular form at level $N_{E_{5,a,b}}/(Rp)$ (there is an extra power of n in the discriminant given by p) and when $n \nmid \alpha$, we get a modular form of level $N_{E_{5,a,b}}/R$.

For now, assume that $n \mid \alpha$. Then level lowering gives us a newform f at level 50, 200 or 400. All the newforms at these levels are rational and hence correspond to elliptic curves. For the newforms whose corresponding elliptic curves do not have rational two torsion (curves 50a1, 50b1, 200a1, 200e1, 400b1, 400c1, 400g1, 400h1), we can use Theorem 1.4.12 and see that the B_3 values for these curves are given by

$$\{45, -45, 105, -105, 45, -45, -105, 105\}$$

respectively. Thus so long as $p \geq 11$, we get a contradiction for these curves. For the other 7 curves at levels 200 and 400, we can use Theorem 1.4.4 to see that $n \mid p + 1 \pm a_p$ which combining with the Hasse bound gives $n \leq p + 1 + 2\sqrt{p}$ contradicting that $n \geq C_5(p)$.

Hence we assume from now on that $n \nmid \alpha$ so that we get a modular form of level $N_{E_{5,a,b}}/R$. Now, we can prove our theorem.

Theorem 6.0.19. *Suppose that $p \geq 7$ and that $p \notin S_5$. Let $\alpha \geq 1$ be an integer. Then the*

equation

$$x^5 + y^5 = p^\alpha z^n$$

has no solutions in coprime nonzero integers x, y, z and prime n satisfying $n \geq p^{13p}$

Proof. Let $g_0^+(N) = \dim_{\mathbb{C}}(\Gamma_0(N))$. Suppose that f is a corresponding normalized newform of conductor $\{50p, 200p, 400p\}$ to $E_{a,b}$ which corresponds to a solution of $x^5+y^5 = p^\alpha z^n$. Let K_f be the associated number field corresponding to the Fourier coefficients of the newform f. By lemme 1 of [Kra97], there exists a prime ℓ satisfying in all cases $\ell \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2^4 \cdot 5^2 \cdot p)] = 120 \cdot (p+1)$ with $a_\ell(f) \notin \mathbb{Z}$. Since f is normalized, the Fourier coefficients a_2, a_5 and a_p all live in $\{0, \pm 1\}$ and hence $\ell \notin \{2, 5, p\}$. Notice that $a_\ell(E_{a,b})$ is a rational integer satisfying the Hasse bound, namely $|a_\ell(E_{a,b})| \leq 2\sqrt{\ell}$ and that for any embedding $\sigma : K_f \to \mathbb{R}$, we have that $|\sigma(a_\ell(f))| \leq 2\sqrt{\ell}$. We can apply the the results from Kraus and Oesterlé from Theorem 1.4.4:

$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_\ell(f) - a_\ell(E_{a,b}))$$
$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_\ell(f) - (\ell + 1))$$

holding for each prime ℓ distinct from n and dividing R to obtain

$$n \leq (\ell + 1 + 2\sqrt{\ell})^{[K_f:\mathbb{Q}]} \leq (\sqrt{\ell} + 1)^{2g_0^+(N)}.$$

Next, we apply theorem 1 of [Mar05] and see that $2g_0^+(N) \leq \frac{19p}{2}$. Hence, we obtain

$$n \leq (\sqrt{120(p+1)} + 1)^{19p/2} < p^{13p}$$

holding for[2] $p \geq 43$. This is a contradiction.

Now, suppose that all the Fourier coefficients are integers. This means that our f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N \in \{50p, 200p, 400p\}$. Applying Pproposition 2 of Appendice II of [Kra97], we see that we must have one of the two following claims.

1. There exists a prime $\ell \leq 120(p+1)$ coprime to $10p$ with $a_\ell(f) \equiv 1 \pmod 2$.
2. We have $a_\ell(f) \equiv 0 \pmod 2$ for all primes ℓ coprime to $10p$.

In the first case, as before since

$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_\ell(f) - a_\ell(E_{a,b})) = a_\ell(f) - a_\ell(E_{a,b}) \leq \ell + 1 + 2\sqrt{\ell}$$

[2]The value p^{13p} can be improved at the sacrifice of the lower bound being increased. However note that the smallest prime not in S_5 is $p = 43$.

we have that

$$n \leq \ell + 1 + 2\sqrt{\ell} \leq 120(p+1) + 1 + 4\sqrt{30(p+1)} < p^{13p}$$

where the last inequality holds for all $p \geq 23$. This is a contradiction.

Now for a small lemma.

Lemma 6.0.20. *If $E/\mathbb{Q}$ is an elliptic curve with $a_\ell(E) \equiv 0 \pmod 2$ for all primes ℓ coprime to the conductor, then E has rational 2 torsion.*

Proof. Let $E : y^2 = p(x)$ for $p(x) \in \mathbb{Z}[x]$ a degree 3 monic polynomial. Since we know that $a_\ell(E) \equiv 0 \pmod 2$ for all primes ℓ coprime to the conductor, we have that the polynomial $p(x)$ must have a linear factor for all but finitely many primes. If $p(x)$ were irreducible, then the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ for the splitting field L must contain a 3 cycle. The Chebotarev Density Theorem states that there must exist infinitely many primes that also have the same cycle structure as elements of the Galois group. Thus, for infinitely many primes, the polynomial must be irreducible which is a contradiction. Hence $p(x)$ is reducible and since it has degree 3 it must contain a rational linear factor by the Rational Root Theorem. Thus E has a rational 2 torsion point. ■

Applying this in our situation, this gives us that E_f is an elliptic curve over $\mathbb{Q}$ with rational 2-torsion and conductor $50p, 200p$ or $400p$. Thus $p \in S_5$, contradicting our assumptions on p.

■

To finish this section off, I now show that the primes not in S_5 comprise most of the primes. That is to say,

Theorem 6.0.21. *We have*

$$\pi_{S_5} := \#\{p \leq x : p \in S_5\} \ll \sqrt{x}\log^2(x)\}$$

Proof. We proceed in a similar fashion to [BLM11]. First, suppose that $n > 3$ for the primes in the prime families in Theorems 5.0.13, 5.0.15, 5.0.17 that allow for $n > 3$. In this case, we can use [ST86, p.180] to see that the largest prime divisor of $Ap^n + By^m$ gets large as n tends to infinity (where $m > 1$ and $\gcd(p, y) = 1$). In our setting, the largest prime divisor is always at worst 5 and so n must be bounded by an absolute constant. Using [DG95, p,4 Theorem 2], we see that the number of solutions is finite for p, n, ℓ, m, d.

We have excluded the case when $n = 3$ by using elliptic curves. For $n = 2$, the cases in which $p^2 = (5^m - 4)^2$ or $p^2 = \left(\frac{5^m-1}{4}\right)^2$ reduce to the cases where $n = 1$. Otherwise, up to the constant term which is okay since it only changes the solutions by its prime factors, we

get Pell equations whose solutions grow exponentially and so there are only asymptotically $\log(x)$ of these solutions.

Thus from now on we suppose that $n = 1$. For most of the prime families in Theorems 5.0.13, 5.0.15, 5.0.17, the work done in [BLM11] was independent of the number 3. Thus, we reduce our list to the consideration of the prime families given by the following. Unless otherwise stated, m and ℓ are arbitrary non negative integers in the following list:

- $$p = \frac{2^\ell + 1}{5^m} \tag{6.1}$$
- $$p = \frac{5^m - 1}{4} \tag{6.2}$$
- m is odd and
$$p = \frac{|d^2 - 5^m|}{4} \tag{6.3}$$
- $$p = \frac{d^2 + 2^\ell}{5^m} \tag{6.4}$$
- $$p = \frac{5d^2 - 1}{4}. \tag{6.5}$$

Equations 6.1 and 6.2 are covered by 6.4 and 6.5 respectively leaving only the last 3 cases above. Throughout suppose that $p \leq x$ and that d is positive (allowing d negative doubles the total possible values of d). Beginning with the last case, notice that

$$\frac{5d^2 - 1}{4} \leq \frac{5d^2}{4} \leq x + 1.$$

Thus the total number possible values of d is $O(\sqrt{x})$, let alone primes.

For equation 6.3, write $m = 2m_0 + 1$. Factoring gives us that

$$|d - 5^{m_0}\sqrt{5}||d + 5^{m_0}\sqrt{5}| = 4p \leq 4x.$$

Hence as $d > 0$,

$$\left|\sqrt{5} - \frac{d}{5^{m_0}}\right| = \frac{4p}{5^{m_0}(d + \sqrt{5}5^{m_0})} \leq \frac{4x}{5^{2m_0}}.$$

Next, we use a theorem of Ridout [Rid57, p.125][3] which can be thought of as a p-adic analogue

[3] In the paper, we set $\mu = 1$, $\nu = 0$, $\kappa = 1 + \epsilon$, $Q_1 = 5$

to Roth's theorem, to see that there exists a constant depending only on ϵ such that

$$\left|\sqrt{5} - \frac{d}{5^{m_0}}\right| > \frac{C(\epsilon)}{5^{m_0(1+\epsilon)}}.$$

We set $\epsilon = 1/2$ and combine the previous two displayed equations to see

$$5^{m_0/2} \ll x.$$

Hence $m \ll \log(x)$. For each fixed value of m, notice that there are $O(\sqrt{x})$ values for d. Thus the number of primes up to x is $O(\sqrt{x}\log x)$.

For the last case, the case of $p = \frac{d^2+2^\ell}{5^m}$, we argue similarly to [BLM11] and the case $\frac{t^2+2^a}{3^b}$. To do this, we begin by noting that modulo 5 considerations give us that $d^2 \equiv -2^\ell$ and so ℓ must be even otherwise the right hand side is not a quadratic residue modulo 5.

Next, since $d^2 + 2^\ell \equiv 0 \pmod 5$ has two simple roots, we lift using Hensel's lemma to see that $d^2 + 2^\ell \equiv 0 \pmod{5^m}$ has only two solutions. Let d_1 and d_2 be the least positive such solutions. Then $d = d_j + 5^m M$ for some integer $M \geq 0$ and $j \in \{1, 2\}$. Then

$$\frac{d^2 + 2^\ell}{5^m} = \frac{d_j^2 + 2^\ell}{5^m} + 2d_j M + 5^m M^2 \leq x$$

Hence $5^m M^2 < x$ hence $M < 5^{-m/2}\sqrt{x}$. Thus, the number of positive integer values possible for d is

$$2\left(\frac{\sqrt{x}}{5^{m/2}} + 1\right)$$

where we double the above to account for d_1 and d_2.

Also notice that

$$2^\ell \leq d^2 + 2^\ell = 5^m p \leq 5^m x.$$

Hence $\ell \ll m + \log x$. Thus with the above it suffices to show that $m \ll \log x$ for then combined with the estimates for the number of admissible values for d gives us an upper bound for $O(\sqrt{x}\log x)$.

Assume towards a contradiction that $m > \kappa \log x$ where κ is some large positive constant. Recalling that ℓ is even and that $\mathbb{Z}[i]$ has class number 1, we have

$$5^m p = d^2 + 2^\ell = (d + 2^{\ell/2}i)(d - 2^{\ell/2}i).$$

Thus, we have

$$d + 2^{\ell/2} i = \alpha^m p_1$$
$$d - 2^{\ell/2} i = \overline{\alpha}^m \overline{p_1}$$

where α is one of $1 \pm 2i$ and $p_1 = u + vi$ is such that $u^2 + v^2 = p$. Eliminating for d yields

$$2^{\ell/2+1} i = \alpha^m p_1 - \overline{\alpha}^m \overline{p_1}.$$

Now the 2-adic valuation of the left hand side above is $\ell/2 + 1$ and the right hand side has 2-adic valuation of

$$v_2 \left(\alpha^m p_1 - \overline{\alpha}^m \overline{p_1} \right) = v_2 \left(\left(\frac{\alpha}{\overline{\alpha}} \right)^m \frac{p_1}{\overline{p_1}} - 1 \right)$$

valid since α and p_1 have odd norms. Using [BL96, Théorém 4] a 2-adic linear forms in logarithms estimate, we see that there exists a constant C such that

$$v_2 \left(\left(\frac{\alpha}{\overline{\alpha}} \right)^m \frac{p_1}{\overline{p_1}} - 1 \right) < C \log^2 \left(\frac{m}{\log x} \right) \log x.$$

Thus, we may conclude that

$$\ell < \ell + \frac{1}{2} < 2C \log^2 \left(\frac{m}{\log x} \right) \log x.$$

Assume towards a contradiction that $\ell > (\log \kappa)^{-1} m$. It follows that

$$\frac{\frac{m}{\log x}}{\log^2 \left(\frac{m}{\log x} \right)} < 2C \log \kappa.$$

and recalling that we assumed that $m > \kappa \log x$ and that $x / \log^2 x$ is an increasing function, we have

$$\kappa < 2C \log^3 \kappa.$$

which is a contradiction if κ is large enough. Hence, we have that $\ell \leq (\log \kappa)^{-1} m$. This gives us that

$$2^{\ell/2} \leq 2^{m/(2 \log \kappa)} \leq 5^{m/4} \tag{6.6}$$

following since $\frac{2 \log 2}{\log 5} < \log \kappa$ for sufficiently large κ. We now apply a generalization of the Schmidt Subspace Theorem due to Schlickewei [Sch77], [Sch91, p.177 Theorem 1D] to the equation

$$2^{\ell/2+1} i = \alpha^m p_1 - \overline{\alpha}^m \overline{p_1}.$$

Let $K = \mathbb{Q}[i]$ and take a set of valuations to be $\mathcal{S} = \{\alpha, \overline{\alpha}, \infty\}$. Let $\mathbf{x} = (x_1, x_2)$. For $j = 1, 2$

and $\nu \in \mathcal{S}$, take

$$L_{j,\nu}(\mathbf{x}) = \begin{cases} x_1 - x_2 & \text{if } (j,\nu) = (2,\infty) \\ x_j & \text{otherwise.} \end{cases}$$

Next, for $\mathbf{x} = (\alpha^m p_1, \overline{\alpha}^m \overline{p_1})$, we show that

$$A := \prod_{(j,\nu)\in\{1,2\}\times\mathcal{S}} |L_{j,\nu}(\mathbf{x})|_\nu \ll \frac{1}{(\max\{|x_1, |x_2|\})^{1/8}}. \tag{6.7}$$

First, compute that

$$\begin{aligned} \prod_{\nu\in\mathcal{S}} |L_{1,\nu}(\mathbf{x})|_\nu &= |\alpha^m p_1|_\alpha |\alpha^m p_1|_{\overline{\alpha}} |\alpha^m p_1| \\ &= \alpha^{-m}\overline{\alpha}^{-m}|\alpha^m p_1| = |p_1|. \end{aligned}$$

Further,

$$\prod_{\nu\in\mathcal{S}\setminus\{\infty\}} |L_{2,\nu}(\mathbf{x})|_\nu = |\overline{\alpha}^m \overline{p_1}|_\alpha |\overline{\alpha}^m \overline{p_1}|_{\overline{\alpha}} = |\alpha^{-m}| = 5^{-m/2}.$$

Lastly,

$$|L_{2,\infty}(\mathbf{x})| = |x_1 - x_2| = |\alpha^m p_1 - \overline{\alpha}^m \overline{p_1}| = 2^{\ell/2+1}.$$

Hence from equations 6.6, the product in equation 6.7 becomes

$$A \le \frac{|p_1| 2^{\ell/2+1}}{5^{m/2}} \le \frac{2\sqrt{x} 2^{\ell/2}}{5^{m/2}} \le \frac{2\sqrt{x}}{5^{m/4}} \le 5^{-m/8}.$$

where the last inequality holds since $m > \kappa \log x$ and so $x < e^{m/\kappa}$ giving $2\sqrt{x} < 2e^{m/(2\kappa)} \le 5^{m/8}$ provided κ is large enough. This also gives that $x \le 5^{m/2}$ and hence,

$$|\alpha^m p_1| = |\overline{\alpha}^m \overline{p_1}| \le 5^{m/2} x \le 5^m.$$

Combining the above shows that equation 6.7 holds. The Generalized Schmidt Subspace Theorem [Sch91, p.177 Theorem 1D] asserts that there exists finitely many pairs $(c_k, d_k) \in K^2\setminus\{(0,0)\}$ for $1 \le k \le s$ such that equation 6.6 satisfies $c_k x_1 = d_k x_2$. Without loss of generality, we may assume that c_k and d_k are coprime. For a fixed k, this implies that

$$c_k \alpha^m p_1 = c_k x_1 = d_k x_2 = d_k \overline{\alpha}^m \overline{p_1}$$

which shows that $\alpha^m \mid d_k \overline{\alpha}^m \overline{p_1}$. Since α and $\overline{\alpha}$ are coprime, we get that $\alpha^m \mid d_k \overline{p_1}$. Since

$|\overline{p_1}| \leq \sqrt{p} \leq \sqrt{x}$, choosing $\kappa \geq \max_{1\leq k\leq s} |d_k|$ shows that $\alpha^m \leq \kappa\sqrt{x}$. This will contradict that $m > \kappa \log x$. Hence $m < \kappa \log x$

■

Chapter 7

Strengthening Results on the Diophantine Equation $x^q + y^q = p^\alpha z^n$

In this section, we will discuss solutions to $x^q + y^q = p^\alpha z^n$ for primes not considered above or in [BLM11]. Let

$$\begin{aligned} \mathcal{S}_{3,p} &= \{18p, 36p, 72p\} \qquad & C_3(p) &= p^{2p} \\ \mathcal{S}_{5,p} &= \{50p, 200p, 400p\} \qquad & C_5(p) &= p^{13p} \end{aligned}$$

and let S_q be the set of primes $p \geq 5$ (or $p \geq 7$ if $q = 5$) for which there exists an elliptic curve E with conductor $N_E \in \mathcal{S}_{q,p}$ with at least one non-trivial rational two torsion point. The trick to strengthening the theorem above and the results from [BLM11] is to exploit more information contained in our Frey-Hellegouarch curve other than the fact that it has a non-trivial rational two torsion point. Recall that for the curves $x^q + y^q = p^\alpha z^n$ with $q \in \{3, 5\}$, we have the following associated Frey-Hellegouarch curves given by

$$E_{3,a,b} : y^2 = (x + b - a)(x^2 + (a - b)x + (a^2 + ab + b^2)) =: f_3(x).$$

$$\begin{aligned} E_{5,a,b} : y^2 &= x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x \\ &= x\left(x^2 - 5(a^2 + b^2)x + 5\left(\frac{a^5 + b^5}{a + b}\right)\right) =: f_5(x). \end{aligned}$$

where (a, b, c) is a solution to $x^q + y^q = p^\alpha z^n$. As notation, we denote by Δ_E the discriminant of the elliptic curve, $\Delta_{E,3}$ the elliptic curve of $E_{3,a,b}$ and $\Delta_{E,5}$ the elliptic curve of $E_{5,a,b}$ and similarly for $\Delta_{E,\min}$ to denote the minimal discriminant and N_E to denote the conductor for the elliptic curve E. We make the assumption that if one of a or b is even, we assume without loss of generality that a is even. This only occurs when c is odd. For the above, we have by

[BLM11] and [Bil07] that the invariants are

$$\Delta_{E,3,\min} = -2^4 3^3 p^{2\alpha} c^{2n},$$

$$N_{E,3} = \begin{cases} 18p \cdot \mathrm{rad}_{6p}(c) & \text{if } c \text{ is even, } b \equiv -1 \pmod 4 \\ 36p \cdot \mathrm{rad}_{6p}(c) & \text{if } c \text{ is odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4 \\ 72p \cdot \mathrm{rad}_{6p}(c) & \text{if } c \text{ is odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4, \end{cases}$$

$$\Delta_{E,5,\min} = 2^4 5^3 (a+b)^2 p^{2\alpha} c^{2n}$$

$$N_{E,5}, = \begin{cases} 50p \cdot \mathrm{rad}_{10p}(c) & \text{if } c \text{ is even, } b \equiv -1 \pmod 4 \\ 200p \cdot \mathrm{rad}_{10p}(c) & \text{if } c \text{ is odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4 \\ 400p \cdot \mathrm{rad}_{10p}(c) & \text{if } c \text{ is odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4. \end{cases}$$

For curves with a rational two torsion point say $y^2 = x^3 + a_2 x^2 + a_4 x$, let Δ_q denote the discriminant of the quadratic polynomial $x^2 + a_2 x + a_4$. In the above, let $\Delta_{Q,3}$ be the discriminant of $x^2 + (a-b)x + (a^2 + ab + b^2)$ and let $\Delta_{Q,5}$ be the discriminant of $\left(x^2 - 5(a^2+b^2)x + 5\left(\frac{a^5+b^5}{a+b}\right)\right)$.

Notice that $\Delta_{Q,3} = -3(a+b)^2$ and that $\Delta_{Q,5} = 5(a+b)^2$. Thus, $f_3(x)$ splits completely over $\mathbb{F}_{\ell'}$, where ℓ' is prime, whenever $\left(\frac{-3}{\ell'}\right) = 1$ and $f_5(x)$ splits completely over $\mathbb{F}_{\ell'}$ whenever $\left(\frac{5}{\ell'}\right) = 1$. The first case occurs whenever $\ell' \equiv 1 \pmod 6$ and the second occurs whenever $\ell' \equiv \pm 1 \pmod 5$. Modulo these primes ℓ', we see that our elliptic curve does not have full rational two torsion but modulo the primes ℓ' is pretending to have full rational two torsion. Mathematically, this means that while $\#E_{\mathrm{tor}}(\mathbb{Q}) \not\equiv 0 \pmod 4$ we do have that $\#E_{\mathrm{tor}}(\mathbb{F}_{\ell'}) \equiv 0 \pmod 4$ for E being one of $E_{3,a,b}$ or $E_{5,a,b}$ as appropriate. Via Ribet's Level Lowering Theorem as in Theorem 1.4.6 (see [BLM11] and [Bil07] for the details) we see that there is a modular form f of level N where

$$N = \begin{cases} 18p & \text{if } q = 3, c \text{ is even, } b \equiv -1 \pmod 4 \\ 36p & \text{if } q = 3, c \text{ is odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4 \\ 72p & \text{if } q = 3, c \text{ is odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4 \\ 50p & \text{if } q = 5, c \text{ is even, } b \equiv -1 \pmod 4 \\ 200p & \text{if } q = 5, c \text{ is odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4 \\ 400p & \text{if } q = 5, c \text{ is odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4 \end{cases}$$

such that $a_{\ell'}(f) \equiv a_{\ell'}(E) \pmod p$. Let's further assume that this f is a rational newform with nontrivial 2 torsion and $a_{\ell'}(f) \not\equiv \ell + 1 \pmod 4$. Then we have that $a_{\ell'}(E) \not\equiv a_{\ell'}(f) \pmod 4$. Since at some prime ℓ' as mentioned above we get that $a_{\ell'}(f) \neq a_{\ell'}(E)$, we see via appendice

II of [Kra97] that the prime where this difference occurs is small when compared to p^2. This tells us that for such prime p, the equation $x^q + y^q = p^\alpha z^n$ has no nontrivial coprime solutions in integers (x, y, z). After a few more definitions, we can summarize the above work in a theorem.

Definition 7.0.22. For ℓ' prime and $q \in \{3, 5\}$, let $R(\ell', q)$ be the condition $\left(\frac{\left(\frac{-1}{q}\right)q}{\ell'}\right) = 1$. This is equivalent to $\left(\frac{-3}{\ell'}\right) = 1$ and $\left(\frac{5}{\ell'}\right) = 1$ for $q = 3$ and $q = 5$ respectively.

Definition 7.0.23. Let $\mathcal{P}_{g,q}$ denote the set of primes p such that there are no elliptic curves E with conductor in the set $\mathcal{S}_{q.p}$ such that $4|\#E_{\mathrm{Tor}}(\mathbb{Q})$ but at least one curve E' with conductor in the same set such that $2|\#E'_{\mathrm{Tor}}(\mathbb{Q})$.

Primes in $\mathcal{P}_{g,3}$ less than 200 include

$$53, 79, 83, 103, 149, 151, 157, 163, 167, 173, 181, 199.$$

and primes in $\mathcal{P}_{g,5}$ less that 200 include

$$23, 47, 53, 71, 83, 97, 107, 137, 139, 149, 151, 173, 179, 181, 191, 193, 197.$$

See the appendix for a longer list.

Note: According to the definition, there needs to be only one curve with conductor in the set S_q. It could be, for example when $q = 3$, that you have a curve of conductor $18p$ with the required property and no curves with conductor $36p$ or $72p$ with $2 \mid E_{\mathrm{Tor}}(\mathbb{Q})$.

Definition 7.0.24. Let $\mathcal{P}_{b,q} \subseteq \mathcal{P}_{g,q}$ be the set of primes p such that $p \in \mathcal{P}_{g,q}$ and for every elliptic curves E with conductor in the set $\mathcal{S}_{q,p}$ such that $2|\#E_{\mathrm{Tor}}(\mathbb{Q})$, there exists a prime ℓ' satisfying both $R(\ell', q)$ and $a_{\ell'}(E) \not\equiv \ell' + 1 \pmod 4$. Equivalently, there exists a prime ℓ' satisfying both $R(\ell', q)$ and $\#E_{\mathrm{Tor}}(\mathbb{F}_{\ell'}) \not\equiv 0 \pmod 4$.

Primes in $\mathcal{P}_{b,3}$ less than 200 include[1]

$$53, 83, 149, 167, 173, 199.$$

Primes in $\mathcal{P}_{b,5}$ less that 200 include

$$23, 53, 71, 73, 83, 97, 107, 137, 151, 173, 181, 191, 193, 197.$$

Again for longer lists, see the appendix. We now have enough notation to state the main result of this section.

[1]Note that in [BLM11] paper, the prime 53 listed above was omitted for $\mathcal{P}_{b,3}$.

Theorem 7.0.25. *Suppose that $q \in \{3,5\}$. Suppose that either $p \in \mathcal{P}_{b,q} \subseteq \mathcal{S}_{q,p}$ or that $p \notin \mathcal{S}_{q,p}$. Then the equation*

$$x^q + y^q = p^\alpha z^n$$

has no solutions in nonzero, coprime integers x, y and z, integer $\alpha \geq 1$ and prime $n \geq C_q(p)$.

The theorem above tells us that if we can give conditions for primes belonging to $\mathcal{P}_{b,q}$, then we can show which primes satisfy the above theorem. First, we show which primes do not belong to $\mathcal{P}_{g,q}$.

Theorem 7.0.26. *Let p be a prime, $q \in \{3.5\}$ and let $E : y^2 = x^3 + a_2x^2 + a_4$ be an elliptic curve with integer coefficients and nontrivial two torsion and conductor in the set $\mathcal{S}_{q,p}$. Suppose further that Δ_E is a positive square. Then $p \notin \mathcal{P}_{g,q}$.*

Proof. Notice that the discriminant of $x^2+a_2x+a_4$ is $\Delta_Q = a_2^2-4a_4$. Further, the discriminant of E is

$$\Delta_E = 16a_4^2(a_2^2 - 4a_4) = (4a_4)^2\Delta_Q$$

Hence, if Δ_E is a square, then Δ_Q is also a square. Thus, the polynomial $x^2 + a_2x + a_4$ splits over $\mathbb{Z}$. This means that

$$y^2 = x^3 + a_2x^2 + a_4x = x(x - \alpha)(x - \beta)$$

for some $\alpha, \beta \in \mathbb{Z}$. Hence the curve has full rational two torsion and so $p \notin \mathcal{P}_{g,q}$ as required. ■

Now, we display the types of primes that are not in $\mathcal{P}_{g,3}$ and $\mathcal{P}_{g,5}$. To form these lists, we use Theorems 4.0.8, 4.0.10, 4.0.12, 5.0.14, 5.0.16 and 5.0.18 to figure out which cases have the possibility of having an elliptic curve with square conductor. If there are any present, then these primes are not members of $\mathcal{P}_{g,q}$ and thus are included below. In all of the tables below, $m \geq 0$ and $d \in \mathbb{Z}$ unless stated otherwise. The third column throughout we will abbreviate using the letters TC to mean "Theorem Case", the entry in the list in the associated theorem.

p^n	Conductor	TC	Extra Information
$2^{\ell-2}\cdot 3^m+1$	$18p$	1	$n=1$, $\ell\geq 7$
$2^{\ell-2}\cdot 3^m-1$	$18p$	2	$n=1$, $\ell\geq 7$
$3^m+2^{\ell-2}$	$18p$	3	$n=1$, $\ell\geq 7$
$3^m-2^{\ell-2}$	$18p$	4	$n=1$, $\ell\geq 7$
$2^{\ell-2}-3^m$	$18p$	5	$n=1$, $\ell\geq 7$
$d^2-2^\ell 3^m$	$18p$	7	$n=1$, $\ell\geq 7$ even, m even
$2^\ell 3^m-d^2$	$18p$	8	$n=1$, $\ell\geq 7$ even, m even
$\frac{d^2+2^L}{3^m}$	$18p$	9	$n=1$, $L\geq 5$
$2^{\ell-2}\cdot 3^m+1$	$72p$	1	$n=1$, $\ell\in\{4,5\}$
$2^{\ell-2}\cdot 3^m-1$	$72p$	2	$n=1$, $\ell\in\{4,5\}$
$3^m+2^{\ell-2}$	$72p$	3	$n=1$, $\ell\in\{4,5\}$
$3^m-2^{\ell-2}$	$72p$	4	$n=1$, $\ell\in\{4,5\}$
$d^2-2^\ell 3^m$	$72p$	6	$n=1$ or $P_{\min}(n)\geq 7$, $\ell=4$, m even
$2^\ell 3^m-d^2$	$72p$	7	$n=1$ or $P_{\min}(n)\geq 7$, $\ell=4$, m even
$\frac{3^m+1}{4}$	$72p$	8	$n=1$

Table 7.1: Primes not in $\mathcal{P}_{g,3}$.

p^n	Conductor	TC	Extra Information
$2^{\ell-2}\cdot 5^m+1$	$50p$	1	$n=1$, $\ell\geq 7$
$2^{\ell-2}\cdot 5^m-1$	$50p$	2	$n=1$, $\ell\geq 7$
$\frac{2^{\ell-2}+1}{5^m}$	$50p$	3	$n=1$, $\ell\geq 7$
$2^{\ell-2}-5^m$	$50p$	4	$n=1$, $\ell\geq 7$
$5^m-2^{\ell-2}$	$50p$	5	$n=1$, $\ell\geq 7$
$2^{\ell-2}+5^m$	$50p$	6	$n=1$, $\ell\geq 7$
$d^2-2^\ell 5^m$	$50p$	7	$n=1$, $\ell\geq 7$, ℓ, m even
$2^\ell 5^m-d^2$	$50p$	8	$n=1$, $\ell\geq 7$, ℓ, m even
$2^{\ell-2}\cdot 5^m+1$	$200p$	1	$n=1$, $\ell\in\{4,5\}$
$2^{\ell-2}\cdot 5^m-1$	$200p$	2	$n=1$, $\ell\in\{4,5\}$
$\frac{5^m-1}{4}$	$200p$	3	$n=1$ or $P_{\min}(n)\geq 7$
$\left(\frac{5^m-1}{4}\right)^2$	$200p$	4	$n=2$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$, m odd
$\frac{5^m-d^2}{2^\ell}$	$200p$	7	$P_{\min}(n)\geq 7$, $\ell\in\{2,4,5\}$, m even
$2^{\ell-2}+5^m$	$200p$	8	$n=1$ or $P_{\min}(n)\geq 7$, $\ell\in\{4,5\}$
$5^m-2^{\ell-2}$	$200p$	9	$n=1$ and $\ell\in\{4,5\}$ or $P_{\min}(n)\geq 7$ when $\ell=4$
$(5^m-4)^2$	$200p$	10	$n=2$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$, m odd
$d^2-2^\ell 5^m$	$200p$	11	$n=1$ or $P_{\min}(n)\geq 7$, $\ell\in\{2,4\}$, m even
$2^\ell 5^m-d^2$	$200p$	12	$n=1$ or $P_{\min}(n)\geq 7$, $\ell\in\{2,4\}$, m even
$2^{\ell-2}\cdot 5^m+1$	$400p$	1	$n=1$, $\ell\geq 4$
$2^{\ell-2}\cdot 5^m-1$	$400p$	2	$n=1$, $\ell\geq 4$
$\frac{2^L+1}{5^m}$	$400p$	3	$n=1$, $L\geq 2$
$\frac{5^m-1}{4}$	$400p$	4	$n=1$ or $P_{\min}(n)\geq 7$, m odd
$\frac{5^m-d^2}{4}$	$400p$	7	$n=1$ and m even
$\frac{5^m-d^2}{4}$	$400p$	8	$P_{\min}(n)\geq 7$, $\ell\in\{4,5\}$
2^L+5^m	$400p$	9	$P_{\min}(n)\geq 7$ and $(L+2)\in\{4,5\}$, $n=1$ and $L\geq 2$
2^L-5^m	$400p$	10	$P_{\min}(n)\geq 7$ and $(L+2)\in\{4,5\}$, $n=1$ and $L\geq 2$
5^m-2^L	$400p$	11	$P_{\min}(n)\geq 7$ and $L=2$, $n=1$ and $L\geq 2$
$(5^m-4)^2$	$400p$	12	$n=2$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$, m odd
$d^2-2^\ell 5^m$	$400p$	13	Either $n=1$ and $\ell\geq 4$ even or both $P_{\min}(n)\geq 7$ and $\ell\in\{2,4\}$, m even
$2^\ell 5^m-d^2$	$400p$	14	Either $n=1$ and $\ell\geq 4$ even or both $P_{\min}(n)\geq 7$ and $\ell\in\{2,4\}$, m even
$\frac{d^2+4}{5^m}$	$400p$	16	$n=2$ or $2\parallel n$ and $P_{\min}(n/2)\geq 7$, m even

Table 7.2: Primes not in $\mathcal{P}_{g,5}$.

At first, the goal to classify primes in $\mathcal{P}_{g,q}$ but not in $\mathcal{P}_{b,q}$ is much easier. In fact, we have

the following.

Theorem 7.0.27. *Let $q \in \{3,5\}$. Let $p \in \mathcal{P}_{g,q}$ and let $E/\mathbb{Q}$ be an elliptic curve with conductor in $\mathcal{S}_{q,p}$ with rational two torsion. Suppose further that the discriminant of the elliptic curve is of the form*

$$\Delta_E = \begin{cases} (-3)m^2 & \text{if } q = 3 \\ 5m^2 & \text{if } q = 5 \end{cases}$$

for some integer m. Then $p \notin \mathcal{P}_{b,q}$.

Proof. By shifting the rational two torsion point to $(0,0)$, the curve E can be seen to be isomorphic to a curve of the form

$$y^2 = x^3 + a_2x^2 + a_4x = x(x^2 + a_2x + a_4)$$

so without loss of generality, suppose E is of this form. According to [Sil09, p.42], we have that

$$\Delta_E = 16a_4^2(a_2^2 - 4a_4) = (4a_4)^2\Delta_Q$$

where Δ_Q is the discriminant of the quadratic polynomial $x^2 + a_2x + a_4$. By assumption $\Delta_E = \Delta_{Q,q}$ and so in fact, we have that

$$\Delta_Q = \frac{\Delta_E}{(4a_4)^2} = \begin{cases} (-3)n^2 & \text{if } q = 3 \\ 5n^2 & \text{if } q = 5 \end{cases}$$

where $(4a_4n)^2 = m^2$. Let $\Delta_{Q,q,n}$ represent the right most side of the above equality.

Assume towards a contradiction that $p \in \mathcal{P}_{b,q}$. Then there exists a prime[2] $\ell' \neq p$ satisfying $R(\ell', q)$ such that $4 \nmid \#E_{\text{Tor}}(\mathbb{F}_{\ell'})$. However, in this case, we know that $\Delta_Q = \Delta_{Q,q,n}$. But for such ℓ', we have that the Legendre symbol evaluates to $\left(\frac{\Delta_{Q,q,n}}{\ell'}\right) = 1$ by definition of $R(\ell', q)$. Thus, Δ_Q is a square in $\mathbb{F}_{\ell'}$. Hence, the polynomial $x^2 + a_2x + a_4$ splits and thus

$$y^2 = x^3 + a_2x^2 + a_4x = x(x^2 + a_2x + a_4) = x(x - \alpha)(x - \beta)$$

where $\alpha, \beta \in \mathbb{F}_{\ell'}$. Hence, we have that the curve has full rational two torsion over $\mathbb{F}_{\ell'}$ and so we have that $4 | \#E_{\text{Tor}}(\mathbb{F}_{\ell'})$ which is a contradiction. Thus $p \notin \mathcal{P}_{b,q}$ as was required. ∎

Now, we can list the families with discriminant of the form $-3m^2$. Hence a prime p that lives in these families and belongs to $\mathcal{P}_{g,q}$ does not belong to $\mathcal{P}_{b,q}$. I summarize these families in the following table. As before, $m \geq 0$ and $d \in \mathbb{Z}$ unless otherwise indicated.

[2] we need to avoid the conductor for reduction purposes so ensure that $\ell' \neq p$.

p^n	Conductor	TC	Extra Information
$d^2 + 2^\ell 3^m$	$18p$	6	$n = 1$, $\ell \geq 7$ even, m odd
$3d^2 + 2^\ell$	$18p$	10	$n = 1$, $\ell \geq 7$ even
$\frac{d^2+3^m}{4}$	$36p$	4	$n = 1$, $p \equiv -1 \pmod 4$, m odd
$\frac{3d^2+1}{4}$	$36p$	5	$n \in \{1, 2\}$, $p \equiv 1 \pmod 4$
$d^2 + 2^\ell 3^m$	$72p$	5	$n = 1$, $\ell \in \{2, 4\}$, m odd
$\frac{3^m+d^2}{4}$	$72p$	9	$n = 1$, $p \equiv 1 \pmod 4$, m odd
$\frac{3d^2+1}{4}$	$72p$	10	$n \in \{1, 2\}$
$3d^2 + 2^\ell$	$72p$	13	$n = 1$, $\ell \in \{2, 4\}$

Table 7.3: Primes not in $\mathcal{P}_{b,3}$ but in $\mathcal{P}_{g,3}$.

p^n	Conductor	TC	Extra Information
$d^2 - 2^\ell 5^m$	$50p$	7	$n = 1$, $\ell \geq 7$ even, m odd
$2^\ell 5^m - d^2$	$50p$	8	$n = 1$, $\ell \geq 7$ even, m odd
$5d^2 - 2^\ell$	$50p$	10	$n = 1$, $\ell \geq 7$ even
$2^\ell - 5d^2$	$50p$	11	$n = 1$, $\ell \geq 7$ even
$\frac{d^2-5^m}{4}$	$200p$	5	$n = 1$ or $P_{\min}(n) \geq 7$, m odd
$\frac{5^m-d^2}{4}$	$200p$	6	$n = 1$ or $P_{\min}(n) \geq 7$, m odd
$\frac{5^m-d^2}{2^\ell}$	$200p$	7	$P_{\min}(n) \geq 7$, $\ell \in \{2, 4, 5\}$ m odd
$d^2 - 2^\ell 5^m$	$200p$	11	$n = 1$ or $P_{\min}(n) \geq 7$, $\ell \in \{2, 4\}$, m odd
$2^\ell 5^m - d^2$	$200p$	12	$n = 1$ or $P_{\min}(n) \geq 7$, $\ell \in \{2, 4\}$, m odd
$\frac{5d^2-1}{4}$	$200p$	15	$n = 1$ or $n = 2$ or $P_{\min}(n) \geq 7$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$, $p^n \equiv 1 \pmod 4$
$5d^2 - 2^\ell$	$200p$	16	$n = 1$ or $P_{\min}(n) \geq 7$ and $\ell \in \{2, 4\}$
$\left(\frac{5^m-1}{4}\right)^2$	$400p$	5	$n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$, m odd
$\frac{d^2-5^m}{4}$	$400p$	6	$n = 1$ or $P_{\min}(n) \geq 7$, m odd
$\frac{5^m-d^2}{4}$	$400p$	7	$n = 1$ or $P_{\min}(n) \geq 7$, m odd
$d^2 - 2^\ell 5^m$	$400p$	13	Either $n = 1$ and $\ell \geq 4$ even or $P_{\min}(n) \geq 7$ and $\ell \in \{2, 4\}$, m odd
$2^\ell 5^m - d^2$	$400p$	14	Either $n = 1$ and $\ell \geq 2$ even or $P_{\min}(n) \geq 7$ and $\ell \in \{2, 4\}$, m odd
$\frac{d^2+4}{5^m}$	$400p$	16	$n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$, m odd
$\frac{5d^2-1}{4}$	$400p$	17	$n = 1$ or $n = 2$ or $P_{\min}(n) \geq 7$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$, $p^n \equiv 1 \pmod 4$
$5d^2 - 2^\ell$	$400p$	18	One of $n = 1$ and $\ell \geq 2$ even, $P_{\min}(n) \geq 7$ and $\ell \in \{2, 4\}$, $n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$ and $\ell = 2$
$2^\ell - 5d^2$	$400p$	19	$n = 1$, $\ell \geq 4$ even
$5d^2 + 4$	$400p$	20	$n = 2$ or $2 \parallel n$ and $P_{\min}(n/2) \geq 7$

Table 7.4: Primes not in $\mathcal{P}_{b,5}$ but in $\mathcal{P}_{g,5}$.

This leaves the following primes. Below we let $m \geq 0$, $d > 0$ be integers and $s \in \{0, 1\}$ unless otherwise specified.

p^n	Conductor	TC	Extra Information	a_4	Legendre for a_4	Δ	Legendre for Δ
$d^2+2^\ell 3^m$	$18p$	6	$n=1, \ell \geq 7$, either ℓ odd or both ℓ, m even	$-2^{\ell-2}3^{m+2}$	$\left(\frac{-2\cdot 3}{\ell'}\right)$ or $\left(\frac{-2}{\ell'}\right)$ or $\left(\frac{-1}{\ell'}\right)$	$2^{2\ell}3^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$d^2-2^\ell 3^m$	$18p$	7	$n=1, \ell \geq 7$, either ℓ odd or m odd	$2^{\ell-2}3^{m+2}$	$\left(\frac{2\cdot 3}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$ or $\left(\frac{3}{\ell'}\right)$	$2^{2\ell}3^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$2^\ell 3^m-d^2$	$18p$	8	$n=1, \ell \geq 7$, either ℓ odd or m odd	$2^{\ell-2}3^{m+2}$	$\left(\frac{2\cdot 3}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$ or $\left(\frac{3}{\ell'}\right)$	$-2^{2\ell}3^{2m+6}p$	$\left(\frac{-p}{\ell'}\right)$
$3d^2+2^\ell$	$18p$	10	$n=1, \ell \geq 7$ odd	$-2^{\ell-2}3^{2s+1}$	$\left(\frac{-2\cdot 3}{\ell'}\right)$	$2^{2\ell}3^{6s+3}p$	$\left(\frac{3p}{\ell'}\right)$
$3d^2-2^\ell$	$18p$	11	$n=1, \ell \geq 7$	$2^{\ell-2}3^{2s+1}$	$\left(\frac{3}{\ell'}\right)$ or $\left(\frac{2\cdot 3}{\ell'}\right)$	$2^{2\ell}3^{6s+3}p$	$\left(\frac{3p}{\ell'}\right)$
$2^\ell-3d^2$	$18p$	12	$n=1, \ell \geq 7$	$2^{\ell-2}3^{2s+1}$	$\left(\frac{3}{\ell'}\right)$ or $\left(\frac{2\cdot 3}{\ell'}\right)$	$-2^{2\ell}3^{6s+3}p$	$\left(\frac{-3p}{\ell'}\right)$
$d^2+4\cdot 3^m$	$36p$	1	$n=1, m$ even	-3^{m+2}	$\left(\frac{-1}{\ell'}\right)$	$2^4 3^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$d^2-4\cdot 3^m$	$36p$	2	$n=1$ or $P_{\min}(n)\geq 7, m$ odd	-3^{m+2}	$\left(\frac{3}{\ell'}\right)$	$2^4 3^{2m+6}p^n$	$\left(\frac{p}{\ell'}\right)$
$4\cdot 3^m-d^2$	$36p$	3	$n=1$ or $P_{\min}(n)\geq 7, m$ odd	-3^{m+2}	$\left(\frac{3}{\ell'}\right)$	$-2^4 3^{2m+6}p^n$	$\left(\frac{-p}{\ell'}\right)$
$3d^2-4$	$36p$	6	$n=1$	3^{2s+1}	$\left(\frac{3}{\ell'}\right)$	$2^4 3^{6s+3}p$	$\left(\frac{3p}{\ell'}\right)$
$d^2+2^\ell 3^m$	$72p$	5	$n=1$, either both $\ell \in \{2,4\}$ and m even or just $\ell=5$	$-2^{\ell-2}3^{m+2}$	$\left(\frac{-1}{\ell'}\right)$ or $\left(\frac{-2}{\ell'}\right)$ or $\left(\frac{-2\cdot 3}{\ell'}\right)$	$2^{2\ell}3^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$d^2-2^\ell 3^m$	$72p$	6	$n=1$ or $P_{\min}(n)\geq 7$, either both $\ell=4$ and m even or just $\ell=5$	$2^{\ell-2}3^{m+2}$	$\left(\frac{2}{\ell'}\right)$ or $\left(\frac{2\cdot 3}{\ell'}\right)$ or $\left(\frac{3}{\ell'}\right)$	$2^{2\ell}3^{2m+6}p^n$	$\left(\frac{p}{\ell'}\right)$
$2^\ell 3^m-d^2$	$72p$	7	$n=1$ or $P_{\min}(n)\geq 7$, either both $\ell=4$ and m even or just $\ell=5$	$2^{\ell-2}3^{m+2}$	$\left(\frac{2}{\ell'}\right)$ or $\left(\frac{2\cdot 3}{\ell'}\right)$ or $\left(\frac{3}{\ell'}\right)$	$-2^{2\ell}3^{2m+6}p^n$	$\left(\frac{-p}{\ell'}\right)$
$\frac{d^2+32}{3^m}$	$72p$	11	$n=1$ or $P_{\min}(n)\geq 7$	$-2^3 3^{m+2}$	$\left(\frac{-2}{\ell'}\right)$	$2^{10}3^{m+6}p^n$	$\left(\frac{p}{\ell'}\right)$ or $\left(\frac{3p}{\ell'}\right)$
$3d^2-2^\ell$	$72p$	12	$n=1, \ell \in \{4,5\}$	$2^{\ell-2}3^{2s+1}$	$\left(\frac{2\cdot 3}{\ell'}\right)$ or $\left(\frac{3}{\ell'}\right)$	$2^{2\ell}3^{6s+3}p$	$\left(\frac{3p}{\ell'}\right)$
$3d^2+32$	$72p$	13	$n=1$	$-2^3 3^{2s+1}$	$\left(\frac{-2\cdot 3}{\ell'}\right)$	$2^{10}3^{6s+3}p$	$\left(\frac{3p}{\ell'}\right)$

Table 7.5: Remaining primes for $q=3$.

p^n	Conductor	TC	Extra Information	a_4	Legendre for a_4	Δ	Legendre for Δ
$d^2-2^\ell 5^m$	$50p$	7	$n=1, \ell \geq 7$ odd	$2^{\ell-2}5^{m+2}$	$\left(\frac{2\cdot 5}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$2^\ell 5^m-d^2$	$50p$	8	$n=1, \ell \geq 7$ odd	$2^{\ell-2}5^{m+2}$	$\left(\frac{2\cdot 5}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$	$-2^{2\ell}5^{2m+6}p$	$\left(\frac{-p}{\ell'}\right)$
$d^2+2^\ell 5^m$	$50p$	9	$n=1, \ell \geq 7$	$-2^{\ell-2}5^{m+2}$	$\left(\frac{-2\cdot 5}{\ell'}\right)$ or $\left(\frac{-2}{\ell'}\right)$ or $\left(\frac{-5}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$5d^2-2^\ell$	$50p$	10	$n=1, \ell \geq 7$ odd	$2^{\ell-2}5^{2s+1}$	$\left(\frac{2\cdot 5}{\ell'}\right)$	$2^{2\ell}5^{6s+3}p$	$\left(\frac{5p}{\ell'}\right)$
$2^\ell-5d^2$	$50p$	11	$n=1, \ell \geq 7$ odd	$2^{\ell-2}5^{2s+1}$	$\left(\frac{2\cdot 5}{\ell'}\right)$	$-2^{2\ell}5^{6s+3}p$	$\left(\frac{-5p}{\ell'}\right)$
$5d^2+2^\ell$	$50p$	12	$n=1, \ell \geq 7$	$-2^{\ell-2}5^{2s+1}$	$\left(\frac{-2\cdot 5}{\ell'}\right)$ or $\left(\frac{-5}{\ell'}\right)$	$2^{2\ell}5^{6s+3}p$	$\left(\frac{5p}{\ell'}\right)$
$d^2-32\cdot 5^m$	$200p$	11	$n=1$ or $P_{\min}(n)\geq 7$	$2^3 5^{m+2}$	$\left(\frac{2}{\ell'}\right)$ or $\left(\frac{2\cdot 5}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p^n$	$\left(\frac{p}{\ell'}\right)$
$32\cdot 5^m-d^2$	$200p$	12	$n=1$ or $P_{\min}(n)\geq 7$	$2^3 5^{m+2}$	$\left(\frac{2}{\ell'}\right)$ or $\left(\frac{2\cdot 5}{\ell'}\right)$	$-2^{2\ell}5^{2m+6}p^n$	$\left(\frac{-p}{\ell'}\right)$
$d^2+2^\ell 5^m$	$200p$	13	$n=1$, $\ell \in \{2,4,5\}$	$-2^{\ell-2}5^{m+2}$	$\left(\frac{-5}{\ell'}\right)$ or $\left(\frac{-2\cdot 5}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$\frac{d^2+16}{5^m}$	$200p$	14	$n=1$ or $P_{\min}(n)\geq 7$	$-2^2 3^{m+2}$	$\left(\frac{-1}{\ell'}\right)$	$2^8 5^{m+6}p^n$	$\left(\frac{p}{\ell'}\right)$ or $\left(\frac{5p}{\ell'}\right)$
$5d^2-32$	$200p$	16	$n=1$ or $P_{\min}(n)\geq 7$	$2^3 5^{2s+1}$	$\left(\frac{2\cdot 5}{\ell'}\right)$	$2^{10}5^{6s+3}p^n$	$\left(\frac{5p}{\ell'}\right)$
$5d^2+2^\ell$	$200p$	17	$n=1$ or $P_{\min}(n)\geq 7$	$-2^{\ell-2}5^{2s+1}$	$\left(\frac{-2\cdot 5}{\ell'}\right)$ or $\left(\frac{-5}{\ell'}\right)$	$2^{2\ell}5^{6s+3}p$	$\left(\frac{5p}{\ell'}\right)$
$d^2-2^\ell 5^m$	$400p$	13	$n=1$ and $\ell \geq 5$ odd or both $P_{\min}(n)\geq 7$ and $\ell=5$	$2^{\ell-2}5^{m+2}$	$\left(\frac{2\cdot 5}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p^n$	$\left(\frac{p}{\ell'}\right)$
$2^\ell 5^m-d^2$	$400p$	14	$n=1$ and $\ell \geq 5$ odd or both $P_{\min}(n)\geq 7$ and $\ell=5$	$2^{\ell-2}5^{m+2}$	$\left(\frac{2\cdot 5}{\ell'}\right)$ or $\left(\frac{2}{\ell'}\right)$	$-2^{2\ell}5^{2m+6}p$	$\left(\frac{-p}{\ell'}\right)$
$d^2+2^\ell 5^m$	$400p$	15	$n=1$, either both $m=0$ and $\ell=2$ or $\ell \geq 4$	$-2^{\ell-2}5^{m+2}$	$\left(\frac{-2\cdot 5}{\ell'}\right)$ or $\left(\frac{-2}{\ell'}\right)$ or $\left(\frac{-5}{\ell'}\right)$ or $\left(\frac{-1}{\ell'}\right)$	$2^{2\ell}5^{2m+6}p$	$\left(\frac{p}{\ell'}\right)$
$\frac{d^2+2^\ell}{5^m}$	$400p$	16	$n=1$ or $P_{\min}(n)\geq 7$ and $\ell \in \{2,4\}$, or $n=1$ and $\ell \geq 5$	$-2^{\ell-2}5^2$	$\left(\frac{2\cdot 5}{\ell'}\right)$ or $\left(\frac{-1}{\ell'}\right)$	$2^{2\ell}5^{m+6}p^n$	$\left(\frac{5p}{\ell'}\right)$ or $\left(\frac{p}{\ell'}\right)$
$5d^2-2^\ell$	$400p$	18	$n=1$ and $\ell \geq 5$ odd, or $P_{\min}(n)\geq 7$ and $\ell=5$	$2^{\ell-2}5^{2s+1}$	$\left(\frac{2\cdot 5}{\ell'}\right)$	$2^{2\ell}5^{6s+3}p^n$	$\left(\frac{5p}{\ell'}\right)$
$2^\ell-5d^2$	$400p$	19	$n=1, \ell \geq 5$ odd	$2^{\ell-2}5^{2s+1}$	$\left(\frac{2\cdot 5}{\ell'}\right)$	$-2^{2\ell}5^{6s+3}p$	$\left(\frac{-5p}{\ell'}\right)$
$5d^2+2^\ell$	$400p$	20	$n=1$ or $P_{\min}(n)\geq 7$ and $\ell \in \{2,4,5\}$, or $n=1$ and $\ell \geq 6$	$-2^{\ell-2}5^{2s+1}$	$\left(\frac{-2\cdot 5}{\ell'}\right)$ or $\left(\frac{-5}{\ell'}\right)$	$2^{2\ell}5^{6s+3}p$	$\left(\frac{5p}{\ell'}\right)$

Table 7.6: Remaining primes for $q=5$.

In fact, the data suggest that the converse is also true, that is, primes that are not in tables 7.3 and 7.1 (thus, ones that are in 7.5) are in $\mathcal{P}_{b,3}$ and similarly, primes that are not in tables 7.4 and 7.2 (thus, ones that are in 7.6) are in $\mathcal{P}_{b,5}$. One has to be a bit careful though with the argument as the following example illustrates.

Example 7.0.28. Suppose $q = 3$ and consider the curves in the isogeny class 25902a. As $25902 = (18)(1439)$ and $1439 = 2^{15} - (177)^2$, we have that this curve belongs to Theorem 4.0.8 case 8 with $t = 177$, $a = 15$ and $b = 0$. Thus, we have that our curve is isogenous to say

$$y^2 = x^3 - 3(177)x^2 + 2^{13}3^2x$$

with discriminant $\Delta = -2^{30}3^6(1439)$. This discriminant is not of the form $(-3)m^2$ and so there should be a prime ℓ' so that $4 \nmid \#E_{\text{Tor}}(\mathbb{Q})$. Notice that $\ell = 7$ is a prime such that $\left(\frac{-1439}{7}\right) = -1$ and so the polynomial does not split in $\mathbb{F}_7$. However, the above elliptic curve over $\mathbb{F}_7$ has torsion subgroup of order 4. What has happened here is that over $\mathbb{F}_7$ even though we do not get splitting, we have that the torsion subgroup has gone from a group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ to a group isomorphic to $\mathbb{Z}/4\mathbb{Z}$. As it turns out, the smallest prime that shows that $1439 \in \mathcal{P}_b$ is actually $\ell = 139$ where the torsion subgroup of the curve over $\mathbb{F}_{139}$ is isomorphic to $\mathbb{Z}/162\mathbb{Z}$.

Lemma 7.0.29. *Let $q \in \{3, 5\}$. Let $a \in \{2, 3\}$, $m = 2^a q$ and $b \in (\mathbb{Z}/m\mathbb{Z})^\times$. For every prime $p \geq 3$ distinct from q and $\delta, \epsilon \in \{\pm 1\}$, there exists a prime ℓ' such that $\left(\frac{\delta p}{\ell'}\right) = \epsilon$ and $\ell' \equiv b \pmod{m}$.*

Proof. Notice that

$$\epsilon = \left(\frac{\delta p}{\ell'}\right) = (\delta)^{\frac{\ell'-1}{2}}\left(\frac{p}{\ell'}\right) = (\delta)^{\frac{\ell'-1}{2}}(-1)^{\frac{p-1}{2}\frac{\ell'-1}{2}}\left(\frac{\ell'}{p}\right).$$

By multiplying both sides by $(\delta)^{\frac{\ell'-1}{2}}(-1)^{\frac{p-1}{2}\frac{\ell'-1}{2}}$, we see that we are then reduced to finding an ℓ' so that

$$\left(\frac{\ell'}{p}\right) = \epsilon(\delta)^{\frac{\ell'-1}{2}}(-1)^{\frac{p-1}{2}\frac{\ell'-1}{2}}$$

If $\ell' \equiv 1 \pmod 4$ is consistent with $\ell' \equiv b \pmod m$, then notice that the right hand side is just ϵ. Alternatively, if $\ell' \equiv 3 \pmod 4$, then the right hand side becomes $\pm\epsilon\delta$ where the $\pm$ sign is determined by $p \equiv \pm 1 \pmod 4$. In either case, we need to find a value of ℓ' such that $\left(\frac{\ell'}{p}\right) = \pm 1$. If we want $\left(\frac{\ell'}{p}\right) = -1$, choose an integer d such that $\left(\frac{d}{p}\right) = -1$. Such an d must exist since the Legendre symbol is a nontrivial real character when $p \geq 3$. If we want $\left(\frac{\ell'}{p}\right) = 1$, then we can choose $d = 1$ and notice that $\left(\frac{d}{p}\right) = 1$. Now via the Chinese Remainder Theorem, find a simultaneous solution, say ℓ_0 such that

$$\ell_0 \equiv d \not\equiv 0 \pmod p \qquad \text{and} \qquad \ell_0 \equiv b \not\equiv 0 \pmod m.$$

The Chinese Remainder Theorem also gives that all solutions are given by $\ell' \equiv \ell_0 \pmod{pm}$. As $\gcd(\ell_0, pm) = 1$, by Dirichlet's Theorem for Primes in an Arithmetic Progression, we have that there exists a prime ℓ' such that $\ell' \equiv \ell_0 \pmod{pm}$. This completes the proof. ■

Now we prove the main theorem.

Theorem 7.0.30. *Let $q \in \{3, 5\}$ and let $p \in \mathcal{P}_{g,q}$. Then $p \in \mathcal{P}_{b,q}$ if and only if every elliptic curve with conductor in $\mathcal{S}_{q,p}$ with non-trivial rational two torsion has discriminant not of the form $\Delta_{Q,q,m} := \left(\frac{-1}{q}\right)qm^2$ for all integers m.*

Proof. The reverse direction was Theorem 7.0.27 so it suffices to show the forward direction. Notice that there are only two cases where $p \notin \mathcal{P}_{b,q}$.

1. The polynomial $x^3 + a_2x^2 + a_4x$ associated to our elliptic curve splits modulo every prime $\ell' \equiv 1 \pmod 6$.

2. For every prime $\ell' \equiv 1 \pmod 6$, there exists a point P on our elliptic curve such that $P \neq (0, 0)$ but $2P = (0, 0)$.

Hence, we need to show that for each curve avoiding discriminants of the form $\left(\frac{-1}{q}\right)qm^2$, we can find a prime ℓ satisfying $R(\ell', q)$ where the curve does not split and that there is no point P as specified above. To show this, notice that the duplication formula [ST92, p. 31] for curves of the form $E : y^2 = x^3 + a_2x^2 + a_4x$ says that if $P = (x, y)$ is a point on E, then

$$x(2P) = \frac{x^4 - 2a_4x^2 + a_4^2}{4y^2} = \frac{(x^2 - a_4)^2}{4y^2}.$$

According to the duplication formula, the second condition above can occur for a prime ℓ' only if $(x^2 - a_4)^2 \equiv 0 \pmod{\ell'}$ and so we must have that a_4 is a quadratic residue modulo ℓ' for every prime $\ell' \equiv 1 \pmod 6$ if our theorem is to be false. Thus, for every curve in our families from Theorems 4.0.8, 4.0.10, 4.0.12, 5.0.14, 5.0.16 and 5.0.18, we must show that we can find a prime ℓ' so that

1. $\left(\frac{\Delta}{\ell'}\right) = -1$

2. $\left(\frac{a_4}{\ell'}\right) = -1$

3. $\left(\frac{\left(\frac{-1}{q}\right)qm^2}{\ell'}\right) = \left(\frac{\left(\frac{-1}{q}\right)q}{\ell'}\right) = 1$ or equivalently $R(\ell', q)$ holds.

All that's left to do is show that this is possible for each curve in the list with the exception of the two forbidden families we have already discarded. We look at Tables 7.5 and 7.6. In those tables, the a_4 and Δ values correspond to the first curve in each case. Choosing other curves in the family will flip the roles of Δ and a_4 so we reduce our argument to just looking at the table given.

Notice that in the tables, the Legendre symbol for Δ never contains a 2. Thus the value $\left(\frac{\Delta}{\ell'}\right)$ is always of the form $\left(\frac{\pm pq}{\ell'}\right)$ or $\left(\frac{\pm p}{\ell'}\right)$. Since $R(\ell', q)$ holds, we can multiply the case of $\left(\frac{\pm pq}{\ell'}\right) = -1$ by the condition $\left(\frac{\left(\frac{-1}{q}\right)q}{\ell'}\right) = 1$ on both sides to see that the condition $\left(\frac{\Delta}{\ell'}\right) = -1$ is always of the form $\left(\frac{\pm p}{\ell'}\right) = -1$.

As for a_4, using the tables, we see that $\left(\frac{a_4}{\ell'}\right)$, up to multiplication by $\left(\frac{\left(\frac{-1}{q}\right)q}{\ell'}\right) = 1$ is one of the following cases:

1. $\left(\frac{-1}{\ell'}\right)$
2. $\left(\frac{\pm 2}{\ell'}\right)$

Next, recall that $R(\ell', 3)$ is the condition that $\ell' \equiv 1 \pmod 6$ which splits into the conditions that $\ell' \equiv 1 \pmod 2$ and $\ell' \equiv 1 \pmod 3$. The first condition tells us that ℓ' is odd and this is consistent with the first three cases above. Recall also that $\left(\frac{-1}{\ell'}\right)$ and $\left(\frac{\pm 2}{\ell'}\right)$ each impose conditions on the prime ℓ' modulo 8. Thus, combining these gives us that either $\ell' \equiv k \pmod 8$ and one of $\ell' \equiv 1 \pmod 3$ or $\ell' \equiv \pm 1 \pmod 5$. The Chinese Remainder Theorem puts us in the situation as needed in Lemma 7.0.29 which gives us an admissible prime ℓ'. This completes the proof.

■

This gives the following theorem

Theorem 7.0.31. *Let $q \in \{3, 5\}$ and suppose that p is a prime such that $p \notin S_q$ or that $p \in \mathcal{P}_{b,q} \subseteq S_q$. Then the equation $x^q + y^q = p^\alpha z^n$ has no nontrivial coprime integer solutions (x, y, z) where $\alpha \geq 1$ and $n \geq C_q(p)$ a prime. Furthermore, if the prime p avoids the lists in Tables 7.1 and 7.3 (hence residing in Table 7.5) when $q = 3$ or in Tables 7.2 and 7.4 (hence residing in Table 7.6) when $q = 5$, then we have that $p \notin S_q$ or that $p \in \mathcal{P}_{b,q} \subseteq S_q$.*

Some final comments. To what end can this technique be extended? Can we try to solve the Diophantine equation $x^7 + y^7 = p^\alpha z^n$? Suppose that $a^7 + b^7 = p^\alpha c^n$ is a given solution. In this case, the only known Frey curve is given by

$$\begin{aligned} y^2 = x^3 - (a-b)^2x^2 + (-2a^4 + ba^3 - 5b^2a^2 + b^3a - 2b^4)x \\ + a^6 - 6ba^5 + 8b^2a^4 - 13b^3a^3 + 8b^4a^2 - 6^5a + b^6 \end{aligned}$$

with discriminant

$$\Delta = 2^4 7^2 \left(\frac{a^7 + b^7}{a + b}\right)^2.$$

This curve does not have rational two torsion, which was a crucial ingredient for this technique to work. A natural place to perhaps use this technique would be over $\mathbb{Q}$-curves, that is, elliptic

curves over some number field that are isogenous to its Galois conjugates. An example of this curve is the one associated to a solution (a, b, c) to the Diophantine equation $x^2 + y^4 = z^n$ given by

$$y^2 = x^3 + 2(1 + i)bx^2 + i(b^2 + ia)x.$$

There is a possibility that the techniques above could all extend over to the equation $x^2+y^4 = p^\alpha z^n$ though I have not attempted to adapt the above to elliptic curves over $\mathbb{Q}(i)$. Here with units being ± 1 and $\pm i$, the techniques used in [Mul06] have a chance of carrying over. There is also potential for this technique to work with Hilbert modularity forms extending the recent work of [Fre10] though much of the work would need to be substantially revised to work over arbitrary totally real fields instead of over $\mathbb{Q}$. Work in this direction is still relatively new and there is much hope that modifications of the above will lead to fruitful mathematical research in the upcoming years.

Bibliography

[AAA02] S. A. Arif and A. S. Al-Ali. On the Diophantine equation $x^2 + p^{2k+1} = 4y^n$. *Int. J. Math. Math. Sci.*, 31(11):695–699, 2002.

[AAM01] S. A. Arif and F. S. Abu Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. II. *Arab J. Math. Sci.*, 7(2):67–71, 2001.

[Ahl66] L. V. Ahlfors. *Complex analysis: An introduction of the theory of analytic functions of one complex variable*. Second edition. McGraw-Hill Book Co., New York, 1966.

[Akh09] S. Akhtari. The Diophantine equation $aX^4 - bY^2 = 1$. *J. Reine Angew. Math.*, 630:33–57, 2009.

[AMLST09] F. S. Abu Muriefah, F. Luca, S. Siksek, and S. Tengely. On the Diophantine equation $x^2 + C = 2y^n$. *Int. J. Number Theory*, 5(6):1117–1128, 2009.

[Bak67] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[Bak68] A. Baker. Linear forms in the logarithms of algebraic numbers. IV. *Mathematika*, 15:204–216, 1968.

[Bal60] W. W. R. Ball. *A short account of the history of mathematics*. Dover Publications Inc., New York, 1960.

[BC06] W. Bosma and J. Cannon, editors. *Discovering mathematics with Magma*, volume 19 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006. Reducing the abstract to the concrete.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BCDY14] M. A. Bennett, I. Chen, S. R. Dahmen, and S. Yazdani. On the equation $a^3 + b^{3n} = c^2$. *Acta Arith.*, 163(4):327–343, 2014.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD10] N. Billerey and L. V. Dieulefait. Solving Fermat-type equations $x^5 + y^5 = dz^p$. *Math. Comp.*, 79(269):535–544, 2010.

[Bil07] N. Billerey. Équations de Fermat de type $(5, 5, p)$. *Bull. Austral. Math. Soc.*, 76(2):161–194, 2007.

[BK94] A. Brumer and K. Kramer. The conductor of an abelian variety. *Compositio Math.*, 92(2):227–248, 1994.

[BL96] Y. Bugeaud and M. Laurent. Minoration effective de la distance p-adique entre puissances de nombres algébriques. *J. Number Theory*, 61(2):311–342, 1996.

[BLM11] M. A. Bennett, F. Luca, and J. Mulholland. Twisted extensions of the cubic case of Fermat's last theorem. *Ann. Sci. Math. Québec*, 35(1):1–15, 2011.

[BMS+08] Y. Bugeaud, M. Mignotte, S. Siksek, Michael Stoll, and Szabolcs Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

[Bru00] Nils Bruin. On powers as sums of two cubes. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 169–184. Springer, Berlin, 2000.

[Bru02] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[Bru03] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[BS04] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[BS08] N. Bruin and M. Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[BS09] N. Bruin and M. Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[BS10] N. Bruin and M. Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[BVY04] M. A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[Cha41] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[Coh91] J. H. E. Cohn. The Diophantine equations $x^3 = Ny^2 \pm 1$. *Quart. J. Math. Oxford Ser. (2)*, 42(165):27–30, 1991.

[Coh92] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[Coh96] J. H. E. Cohn. Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20, 1996.

[Coh97] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[Coh03] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. II. *Acta Arith.*, 109(2):205–206, 2003.

[Coh07a] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Coh07b] H. Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Col85] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Cre] J. Cremona. Elliptic curve data. http://homepages.warwick.ac.uk/~masgaj/ftp/data/, visited 2015-01-26.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[CS09] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322(3):638–656, 2009.

[Dah08] S. R. Dahmen. *Classical and modular methods applied to Diophantine equations*. 2008. Utrecht University, Ph.D. thesis.

[Dav95] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[Del74] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Del80] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[Dén52] P. Dénes. Über die Diophantische Gleichung $x^l + y^l = cz^l$. *Acta Math.*, 88:241–251, 1952.

[Dev90] K. Devlin. *Mathematics: the new Golden Age*. Penguin Books, New York, 1990.

[DF04] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[DG95] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DK95] Fred Diamond and Kenneth Kramer. Modularity of a family of elliptic curves. *Math. Res. Lett.*, 2(3):299–304, 1995.

[DM97] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[DR11] V. Dragović and M. Radnović. *Poncelet porisms and beyond*. Frontiers in Mathematics. Birkhäuser/Springer Basel AG, Basel, 2011. Integrable billiards, hyperelliptic Jacobians and pencils of quadrics.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[dW89] B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[Ell04] J. S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.

[Euc02] Euclid. *Euclid's Elements*. Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, The Thomas L. Heath translation, Edited by Dana Densmore.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Fre86] G. Frey. Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1(1):iv+40, 1986.

[Fre09] G. Frey. The way to the proof of Fermat's last theorem. *Ann. Fac. Sci. Toulouse Math. (6)*, 18(Fascicule Special):5–23, 2009.

[Fre10] N. R. B. Freitas. *Some Generalized Fermat-Type Equations via Q-curves and Modularity*. 2010. Thesis (Ph.D.)–Universitat de Barcelona (Spain).

[GLT08] E. Goins, F. Luca, and A. Togbé. On the Diophantine equation $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 430–442. Springer, Berlin, 2008.

[GR11] H. R. Gallegos-Ruiz. S-integral points on hyperelliptic curves. *Int. J. Number Theory*, 7(3):803–824, 2011.

[Ham11] K. D. Hambrook. *Implementaiton of a Thue-Mahler Equation Solver*. 2011. Thesis (M.Sc.)–The University of British Columbia (Canada).

[Hel75] Y. Hellegouarch. Points d'ordre $2p^h$ sur les courbes elliptiques. *Acta Arith.*, 26(3):253–263, 1974/75.

[HK98] E. Halberstadt and A. Kraus. Sur les modules de torsion des courbes elliptiques. *Math. Ann.*, 310(1):47–54, 1998.

[HPPT13] B. He, I. Pink, Á. Pintér, and A. Togbé. On the Diophantine inequality $|X^2 - cXY^2 + Y^4| \leq c + 2$. *Glas. Mat. Ser. III*, 48(68)(2):291–299, 2013.

[HS00] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Itō87] K. Itō, editor. *Encyclopedic dictionary of mathematics. Vol. I–IV*. MIT Press, Cambridge, MA, second edition, 1987. Translated from the Japanese.

[Ivo04] W. Ivorra. *Equations diophantiennes ternaires de type (p,p,2) et courbes elliptiques*. 2004. Thesis (Ph.D.)– Universite Pierre et Marie Curie.

[Ken82] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[Kna92] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[KO92] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[Kra97] A. Kraus. Majorations effectives pour l'équation de Fermat généralisée. *Canad. J. Math.*, 49(6):1139–1161, 1997.

[Kra98] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[Kra99] A. Kraus. On the equation $x^p + y^q = z^r$: a survey. *Ramanujan J.*, 3(3):315–333, 1999.

[KW09a] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lju42] W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70, 1942.

[Lju54] W. Ljunggren. Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$). In *Tolfte Skandinaviska Matematikerkongressen, Lund, 1953*, pages 188–194. Lunds Universitets Matematiska Inst., Lund, 1954.

[Lju67] W. Ljunggren. On the diophantine equation $Ax^4 - By^2 = C$ ($C = 1, 4$). *Math. Scand.*, 21:149–158 (1969), 1967.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[LS93] M. Lockhart, P. Rosen and J. H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.

[LT08] F. Luca and A. Togbé. On the Diophantine equation $x^2 + 2^a \cdot 5^b = y^n$. *Int. J. Number Theory*, 4(6):973–979, 2008.

[LTT09] F. Luca, S. Tengely, and A. Togbé. On the Diophantine equation $x^2 + C = 4y^n$. *Ann. Sci. Math. Québec*, 33(2):171–184, 2009.

[Luc02] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[LY07] J. Luo and P. Yuan. Square-classes in Lehmer sequences having odd parameters and their applications. *Acta Arith.*, 127(1):49–62, 2007.

[Mar05] G. Martin. Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. *J. Number Theory*, 112(2):298–331, 2005.

[Mat00] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64(6):125–180, 2000.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mih04] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[Mil06] J. S. Milne. *Elliptic curves*. BookSurge Publishers, Charleston, SC, 2006.

[Mom84] F. Momose. Rational points on the modular curves $X_{\text{split}}(p)$. *Compositio Math.*, 52(1):115–137, 1984.

[MP12] W. McCallum and B. Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[Mul06] J. T. Mulholland. *Elliptic curves with rational 2-torsion and related ternary Diophantine equations*. ProQuest LLC, Ann Arbor, MI, 2006. Thesis (Ph.D.)–The University of British Columbia (Canada).

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[NZM91] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.

[Ogg67] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[Pap93] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2):119–152, 1993.

[PR11] I. Pink and Z. Rábai. On the Diophantine equation $x^2 + 5^k 17^l = y^n$. *Commun. Math.*, 19(1):1–9, 2011.

[PS97] B. Poonen and E. F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Rib94] K. A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[Rid57] D. Ridout. Rational approximations to algebraic numbers. *Mathematika*, 4:125–131, 1957.

[RU96] G. Rémond and F. Urfels. Approximation diophantienne de logarithmes elliptiques p-adiques. *J. Number Theory*, 57(1):133–169, 1996.

[Rud76] W. Rudin. *Principles of mathematical analysis*. McGraw-Hill Book Co., New York, third edition, 1976. International Series in Pure and Applied Mathematics.

[S+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.4.1)*. The Sage Development Team, 2014. http://www.sagemath.org, visited 2015-01-26.

[Sai88] T. Saito. Conductor, discriminant, and the Noether formula of arithmetic surfaces. *Duke Math. J.*, 57(1):151–173, 1988.

[Sch77] H. Schlickewei. The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt theorem. *Arch. Math. (Basel)*, 29(3):267–270, 1977.

[Sch91] W. M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1991.

[Sch98] N. Schappacher. "Wer war Diophant?". *Math. Semesterber.*, 45(2):141–156, 1998.

[Ser87] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Sik03] S. Siksek. On the Diophantine equation $x^2 = y^p + 2^k z^p$. *J. Théor. Nombres Bordeaux*, 15(3):839–846, 2003.

[Sik13] S. Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil07] J. H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST86] T. N. Shorey and R. Tijdeman. *Exponential Diophantine equations*, volume 87 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.

[ST92] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Ste] W. Stein. The l-functions and modular forms database. http://www.lmfdb.org/, visited 2015-01-26.

[Sto98] M. Stoll. On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians. *J. Reine Angew. Math.*, 501:171–189, 1998.

[Sto99] M. Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.

[Sto02a] M. Stoll. On the arithmetic of the curves $y^2 = x^l + A$. II. *J. Number Theory*, 93(2):183–206, 2002.

[Sto02b] M. Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.

[SvL13] M. Stoll and R. van Luijk. Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$. *Acta Arith.*, 159(2):133–148, 2013.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[TdW92] N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Math.*, 84(3):223–288, 1992.

[TdW93] N. Tzanakis and B. M. M. de Weger. Corrections to: "How to explicitly solve a Thue-Mahler equation" [Compositio Math. **84** (1992), no. 3, 223–288; MR1189890 (93k:11025)]. *Compositio Math.*, 89(2):241–242, 1993.

[Tor] G. Tornaria. Computational number theory - tables and computations. http://www.ma.utexas.edu/users/tornaria/cnt/, visited 2015-01-26.

[TW95] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Was08] L. C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[YZ10] P. Z. Yuan and Z. F. Zhang. The Diophantine equation $aX^4 - bY^2 = 1$. *Acta Math. Sinica (Chin. Ser.)*, 53(3):443–454, 2010.

Appendix A

Final Collection of Tables

Below is a list of the elements of $\mathcal{P}_{g,3}$ less than 1800.

53	233	367	463	617	751	887	1019	1181	1303	1451	1559	1669
79	241	373	467	619	757	907	1031	1187	1307	1453	1567	1693
83	263	379	479	631	787	911	1049	1193	1321	1459	1571	1697
103	271	389	487	641	809	919	1063	1201	1327	1481	1579	1699
149	277	397	491	643	811	929	1069	1213	1361	1483	1583	1721
151	281	401	523	659	823	937	1087	1217	1367	1487	1597	1723
157	293	409	541	661	827	941	1091	1223	1373	1489	1601	1741
163	311	419	563	673	829	947	1093	1229	1381	1499	1607	1747
167	313	421	569	691	839	953	1097	1237	1409	1511	1609	1759
173	331	433	571	709	853	967	1103	1249	1423	1523	1619	1777
181	347	443	587	719	859	977	1117	1259	1427	1531	1621	1783
199	349	449	599	727	877	983	1123	1283	1429	1543	1627	1787
223	353	457	607	739	881	991	1129	1291	1433	1549	1657	1789
227	359	461	613	743	883	1009	1171	1297	1439	1553	1667	

Table A.1: Primes p of $\mathcal{P}_{g,3}$ with $p \leq 1800$

Below is a list of the elements of $\mathcal{P}_{b,3}$ less than 1800.

53	263	419	569	727	839	953	1181	1283	1429	1511	1619	1787
83	281	443	571	739	859	977	1187	1291	1433	1523	1627	
149	293	449	587	743	881	983	1193	1307	1439	1549	1667	
167	311	461	599	751	887	1019	1201	1361	1451	1553	1697	
173	347	467	617	809	907	1031	1213	1367	1453	1559	1721	
199	353	479	641	811	911	1049	1217	1373	1459	1571	1741	
223	359	487	643	823	929	1091	1223	1409	1481	1583	1747	
227	389	491	659	827	941	1097	1229	1423	1487	1601	1759	
233	401	563	719	829	947	1103	1259	1427	1499	1607	1777	

Table A.2: Primes p of $\mathcal{P}_{b,3}$ with $p \leq 1800$

Below is a list of the elements of $\mathcal{P}_{g,5}$ less than 320.

23	71	97	139	173	191	197	223	233	241	271	293	313
47	73	107	149	179	193	211	229	239	269	277	311	317
53	83	137	151	181								

Table A.3: Primes p of $\mathcal{P}_{g,5}$ with $p \leq 320$

Below is a list of the elements of $\mathcal{P}_{b,5}$ less than 320.

23	71	83	107	151	181	193	211	241	277	311	313	317
53	73	97	137	173	191	197	223	271	293			

Table A.4: Primes p of $\mathcal{P}_{b,5}$ with $p \leq 320$