Modular and Reciprocity Approaches to a Family of Diophantine Equations

PhD Thesis

Mostafa Ibrahim

A thesis submitted for the degree of Doctor of Philosophy

Mathematics Institute

University of Warwick

October 2009

Contents

List of Tables

Acknowledgements

I wish to express my gratitude to my supervisor, Samir Siksek, for his continuous support during this work.

I thank the Mathematics Institute and University of Warwick for providing excellent working conditions, and all my friends and colleagues for creating a pleasant atmosphere and for the scientific as well as not-so-scientific discussions.

Also, I would like to thank the Engineering and Physical Sciences Research Council (EPSRC) of the United Kingdom and the European Commission for financial support.

Finally, I would like to thank my family and all who have enriched my life during the studies and research.

Declaration of Authorship

I declare that this thesis is entirely my own work, except where otherwise stated, and that none of it has appeared before in print. I confirm that this thesis has not been submitted for a degree at another university.

Abstract

In this thesis we study the Diophantine equation

$$x^p - Dy^{2p} = z^2, \qquad \gcd(x, z) = 1, \quad p \text{ prime}.$$

We combine two approaches:

- The modular approach using in Wiles's proof of Fermat's Last Theorem.
- Elementary quadratic reciprocity.

We show how using this combination of approaches and computer calculations we can get congruence conditions for the exponent p.

Chapter 1

Introduction

Wiles' proof of Fermat's Last Theorem puts to rest one of the most famous unsolved problems in Mathematics, a question that has been a wellspring for much of modern algebraic number theory.

Inspired by the work of Wiles [43] there has been great deal of research focusing on ternary Diophantine equations from the perspective of (modular) elliptic curves and modular forms (see e.g. [3], [4], [5], [6], [18], [19], [26], [27], [31], [30], [29], [37]). These have, for the most part been concerned with equations of the shape $Ax^p + By^q = Cz^r$ for p, q and r positive integers with $1/p + 1/q + 1/r < 1$. We refer to the triple (p, q, r) as the signature of the corresponding equation.

This thesis is concerned with the following family of Diophantine equations,

$$x^p - D \cdot y^{2p} = z^2, \qquad (x, z) = 1, \quad p \text{ is a prime} \geq 7. \tag{1.1}$$

This equation is attacked using a combination of the above mentioned modular approach, and the law of quadratic reciprocity. To apply the modular approach to this Diophantine equation, one would have to construct a Frey curve or curves associated with this equation. The recent works of W. Ivorra and A. Kraus, [27], and M. Bennett and C. Skinner, [3], show that we can construct two Frey elliptic curves corresponding to hypothetical solutions of this Diophantine equation. Ribet's Level–Lowering Theorem then yields a finite set of newforms (rational and irrational), and these give strong congruence conditions on x^p, y^{2p}, z. Then we combine these conditions that come from the modular approach together with other restrictions that come from the Law of Quadratic Reciprocity. This would lead us to certain conditions and congruences for the prime exponent p of any putative solution of the Diophantine equation. The newforms one encounters depend on which of the integers x^p, Dy^{2p}, and z^2 is even, and so the congruences one obtains for the exponent p also depend on which of these is even.

As an example of the results we obtain, we state the following theorem proved in Chapter 5.

Theorem 1.1. *Let x, y, z satisfy the equation $x^p - Dy^{2p} = z^2$, with x even,* $\gcd(x, z) = 1$ *and p prime. If $p \geq 175$, then it must satisfy the following congruences*

D	$x \equiv 4, 6 \pmod 8$	$x \equiv 0, 2 \pmod 8$
7	*No Information*	*No Information*
15	$p \equiv 5 \pmod 6$	$p \equiv 1 \pmod 6$
23	$p \equiv 3, 7 \pmod{10}$	$p \equiv 1, 9 \pmod{10}$
31	*No Information*	*No Information*
39	$p \equiv 11, 13, 17 \pmod{18}$	$p \equiv 1, 5, 7 \pmod{18}$
47	$p \equiv 3, 13, 21 \pmod{22}$	$p \equiv 1, 9, 19 \pmod{22}$
55	*No Solution*	*No Solution*
63	$p \equiv 13, 19, 23, 29 \pmod{30}$	$p \equiv 1, 7, 11, 17 \pmod{30}$

The thesis is organised as follows. Chapter 2 is a brief history of similar Diophantine equations. In Chapter 3 we introduce the necessary technical tools from elliptic curves and modular forms and the modular approach to Diophantine equations. Chapter 4 recalls some recipes by Ivorra and Kraus for Frey curves and level-lowering for the Diophantine equation $ax^p + by^p = cz^2$. We apply these to our equation (1.1) with $1 \leq D \leq 100$ and show that if $p \geq 43$ then the irrational newforms at the levels predicted by Ivorra and Kraus are unrelated to the solutions.

In Chapter 5 we introduce the study equation (1.1) with x even. This case is easier than the general case. For many values of D in the above range, we show that we can reduce the number of newforms to 0 or 1. We also explain how to combine the modular approach with information given by quadratic reciprocity, to obtain the above theorem.

Chapter 6 tackles the general case of equation (1.1). There the discussion is much more technical; our main results are given at the end of that chapter.

The results obtained in this thesis for equation (1.1) are limited to a modest range for D because of computing problems. We hope to be able to run our programs on more powerful computers in the future to obtain more complete results. A much more exciting direction is to combine the modular approach with quadratic reciprocity over number fields as done in the paper of Chen and Siksek [11].

Chapter 2

Historical Background

2.1 The generalised Fermat equation $Ax^p + By^q = Cz^r$

This section will be devoted to generalisations of Fermat's equation

$$x^n + y^n = z^n.$$

In view of the proof of Wiles and Taylor, it is natural to wonder what would happen if the exponents in the three term equation are chosen differently, or if coefficients other than 1 are chosen.

Let $A, B, C \in \mathbb{Z}$ be non-zero and $p, q, r \in \mathbb{Z}_{\geq 2}$. Consider the Diophantine equation

$$Ax^p + By^q = Cz^r, \quad \gcd(x, y, z) = 1 \tag{2.1}$$

in the unknown integers x, y, z. As various authors have noted, if $c = a^p + b^p$ or $w = u + v$ then we have the equality

$$(ac)^p + (bc)^p = (c^{\frac{p+1}{2}})^2$$

or

$$(u^{11}v^7w^3)^2 + (u^7v^5w^2)^3 = (u^3v^2w^1)^7$$

thus providing us with infinitely many trivial solutions for

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

and

$$x^2 + y^3 = z^7$$

respectively. From an arithmetic point of view, these solutions are not very interesting. The restriction that the unknowns are coprime is imposed to avoid these trivialities.

Let us define the characteristic of the equation (2.1) to be

$$\chi(p, q, r) = p^{-1} + q^{-1} + r^{-1} - 1.$$

The study of equation (2.1) depends on whether $\chi(p, q, r)$ is > 0 (the spherical case), is zero (the Euclidean case) or is < 0 (the hyperbolic case) (see [6]).

- For $\chi < 0$, Henri Darmon and the Andrew Granville [20] showed that there are only finitely many integer solutions.

- If $\chi = 0$, then a simple calculation shows that the only possible sets for $\{p, q, r\}$ are $\{3, 3, 3\}$, $\{2, 4, 4\}$, $\{2, 3, 6\}$. In this case the solution of the equation comes down to the determination of rational points on twists of genus 1 curves over $\mathbb{Q}$ with j invariant 0 or 1728.

- If $\chi > 0$ then the only possible sets for $\{p, q, r\}$ are $\{2, 2, k\}$ with $k \geq 2$ or $\{2, 3, m\}$ with $m = 3, 4, 5$. In the latter case the solutions are given by a finite set of polynomial parameterisations of the equation. For a full account see [5] and [6].

2.1.1 The special case $x^p + y^q = z^r$

A special case of interest is when $A = B = C = 1$. In many such cases the solution set has been found (for details see [6], [31]). In [31], Kraus elegantly surveys results on coprime integer solutions of the equation

$$x^p + y^q = z^r. \tag{2.2}$$

Below we list the exponent triples (p, q, r) of solved equations together with the non-trivial solutions ($xyz \neq 0$).

We exclude the generic solution $1^k + 2^3 = 3^2$ from the list. If no solutions are mentioned, then it is proven that no other solutions exist. The notation

$\{p, q, r\}$ implies that all permutations of the order triple (p, q, r) are taken into account. This is important in the case of two even exponents.

- Let $\chi > 0$. In the spherical cases the solution set is infinite. The case $\{2, 3, 3\}$ was solved by Mordell, $\{2, 3, 4\}$ by Zagier and $\{2, 3, 5\}$ by J. Edwards [23]. In the case $\{2, 2, k\}$, we must consider the two equations $x^2 - y^2 = z^r$ and $x^2 + y^2 = z^r$ which are easy exercises in number theory (see [13]).

- For $\chi = 0$, it is well-known that the only non-trivial solutions arise from the equality $1^6 + 2^3 = 3^2$.

- Let $\chi < 0$. The first case $\{n, n, n\}$ is of course Wiles' proof of Fermat's Last Theorem. Table 2.1 lists the cases with variable n that are solved using the modular approach, with possibly a few exceptions which are resolved using other methods. Presumably the solutions listed above are the only solutions in the hyperbolic case. As one of the exponents equals 2 for all the known solutions, this led Henri Darmon and Andrew Granville [20] to conjecture that there is no solution for the Diophantine equation $x^p + y^q = z^r$ in $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$, $xyz \neq 0$ and $p, q, r \in \mathbb{Z}_{\geq 3}$.

The conjecture of Darmon and Granville can expressed as follows:

Conjecture 2.1.1. *(Generalised Fermat Conjecture) If* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$*, then the generalised Fermat equation* $x^p + y^q = z^r$ *has no solutions in coprime*

non-zero integers x, y, z, except the following ten solutions:

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9,$$

$$2^7 + 17^3 = 71^2, \qquad 3^5 + 11^4 = 122^2, \qquad 17^7 + 76271^3 = 21063928^2,$$

$$1414^3 + 2213459^2 = 65^7, \qquad 9262^3 + 15312283^2 = 113^7,$$

$$43^8 + 96222^3 = 30042907^2, \qquad 33^8 + 1549034^2 = 15613^3.$$

2.2 The Diophantine equation $x^2 = y^p + 2^k z^p$

In [14], J. H. E. Cohn proved the following theorem.

Theorem 2.1. *(Cohn) Let k be odd. Then the Diophantine equation*

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

has only the following solutions in positive integers x, y and $n \geq 3$:

k	x	y	n
$6\alpha + 1$	$5 \cdot 2^{3\alpha}$	$3 \cdot 2^{2\alpha}$	3
$4\alpha + 5$	$7 \cdot 2^{2\alpha}$	$3 \cdot 2^{\alpha}$	4
$10\alpha + 5$	$11 \cdot 2^{5\alpha+3}$	$3 \cdot 2^{2\alpha+1}$	5

with $\alpha \geq 0$.

In the same paper, Cohn conjectured that for k even (the remaining case), the only solutions are

$$(x, y) = (2^{k/2}, 2^{k+1})$$

and

$$(x, y) = (11 \cdot 2^{(k/2)-1}, 5 \cdot 2^{(k-2)/3}),$$

with the latter solution existing only when $(k, n) = (6M + 2, 3)$.

The case with k even has proven to be more troublesome. Then in [2], S. A. Arif and F. S. A. Muriefah use arguments based on arithmetic in the Gaussian integers to prove partial results in the direction of the conjecture. In particular, the conjecture is proved for all values of k in the case that $n = 3$, 7, or n has at least one prime divisor not of the form $8k + 7$. In the case that n is properly divisible by 3 to an even power and n is odd, it is shown that all solutions of the equation have x even. It is also shown that the equation has no solutions in the case that n is even. In [1], Arif and Muriefah continue their study of the Ramanujan-Nagell type equation $x^2 + 2^k = y^n$. They use the recent result of Y. F. Bilu, G. Hanrot and P. M. Voutier, [7], on primitive divisors in Lucas sequences, to prove Cohn's above conjecture for even k.

Among the many applications of these results is the generalised Ramanujan-Nagell equation $x^2 - 2^k = y^n$. This has been the object of much study, sometimes by transcendence methods, in which very large bounds for n have been proved.

Inspired by the success of modular form techniques in resolving the Fermat problem, H. Darmon and L. Merel, [18], examine the Diophantine equation

$$x^n + y^n = z^2.$$

An integer solution (x, y, z) is called trivial if $xyz = 0$ or 1. They proved that the equation $x^n + y^n = z^2$ has no positive integer pairwise coprime solutions for $n \geq 4$. In [37] Siksek adapted the method of Darmon and Merel in [18] to give results about the more general equation

$$x^2 = y^p + 2^k z^p \tag{2.3}$$

where k is a positive integer, and p is a prime.

Studying this equation (2.3) unifies the study of two well-known exponential Diophantine equations appearing in the literature:

$$x^2 + 2^k = y^n \quad \text{and} \quad x^2 - 2^k = y^n$$

(See [2], [10], [14], [15], [25]). We shall call an integral solution x, y, z of equation (2.3) primitive if x, y, z are pairwise coprime, and non-trivial if $xyz \neq 0$. The main result of [37] is the following theorem.

Theorem 2.2. *(Siksek) Suppose $k \geq 2$ and that $p \geq 7$ is prime. Then the only nontrivial primitive solution of equation $x^2 = y^p + 2^k z^p$ are $k = 3$, $x = \pm 3$, $y = z = 1$ and p arbitrary.*

The approach of [37] to prove Theorem 2.2 is to associate to each putative solution of equation (2.3) a Frey curve and apply Ribet's level-lowering theorem. This will be sufficient to eliminate all the cases of the theorem except for $k = 3$. For $k = 3$, Siksek in [37] adapted the method of Darmon and Merel to finish the proof. As a consequence of this result, Siksek solved completely the Diophantine equation $x^2+2^{2m} = y^n$ for $n \geq 3$: it has precisely two families of solutions given by $x = 2^m$ for all m, and by $n = 3$, $x = 11 \cdot 2^{3M}$ if $m = 3M + 1$. This particular result has been obtained independently by other methods (see [1], [32]).

Independently and at the same time, W. Ivorra proved in [26] strong results using similar methods. Ivorra considers the two equations

$$x^p + 2^\beta y^p = z^2,$$

$$x^p + 2^\beta y^p = 2z^2,$$

where $p \geq 7$, and without loss of generality $0 \leq \beta \leq p - 1$. The set of (nontrivial) positive integer solutions to the first equation is denoted by $S_0(\beta, p)$, while $S_1(\beta, p)$ denotes the set of nontrivial solutions to the second equation. The first theorem of [26] is concerned with the first of these two sets, and states the following.

Theorem 2.3. *(Ivorra) Let $S_0(\beta, p)$ be the set of (nontrivial) positive integer solutions to the equation $x^p + 2^\beta y^p = z^2$ then*

(a) if β is different from 1, 3, $p-3$, $p-1$, then $S_0(\beta, p)$ is empty;

(b) $S_0(3, p) = (1, 1, 3)$;

(c) $S_0(p-3, p) = (2, 1, 3 \cdot 2^{(p-3)/2})$;

(d) if $(a, b, c) \in S_0(1, p)$, then ab is odd;

(e) if $(a, b, c) \in S_0(p-1, p)$, then $a \equiv 2 \pmod 4$.

The other result of Ivorra is concerned with $S_1(\beta, p)$, and has a much simpler statement.

Theorem 2.4. *(Ivorra) Let $S_1(\beta, p)$ be the set of (nontrivial) positive integer solutions to the equation $x^p + 2^\beta y^p = 2z^2$. If $\beta > 0$, then $S_1(\beta, p)$ is empty, while $S_1(0, p) = (1, 1, 1)$.*

Also, as a consequence of other results of [26], Ivorra shows that the only solutions to $x^2 - 2^m = y^n$, in integers (x, y, m, n), with $(x, y) = 1$, $|y| > 1$, $m \geq 2$ and $n \geq 3$ are $(13, -7, 9, 3), (71, 17, 7, 3)$. It is important to note that this equation remains unresolved in the case $m = 1$. In other words, the equation $x^2 - 2 = y^n$ has not been solved yet.

2.3 The Diophantine equation $Ax^n + By^n = Cz^2$

M. A. Bennett and C. Skinner, [3], and W. Ivorra and A. Kraus, [27], have independently proved very similar results and developed techniques for solv-

ing ternary Diophantine equations of the shape $Ax^n + By^n = Cz^2$, based upon the theory of the modular approach to Diophantine equations. The basic technique was previously developed by mathematicians like Hellegouarch [28], Frey [22], Mazur, Serre [36], and Ribet in the 1970's and 1980's, and was exploited by Wiles, [43], in his epoch-making proof of Fermat's last theorem. After Wiles' breakthrough, [43], the relation between modular elliptic curves and ternary Diophantine equations was taken up and systematised by a number of mathematicians (see, for example [24], [31]). The papers [3], [27], are valuable contributions to the literature on this subject, giving a complete solution to the ternary equation $Ax^n + By^n = Cz^2$ for certain choices of the parameters A, B and C, and concluding with an appealing application of these results to certain classical polynomial-exponential equations such as the equation $x^2 + D = 2^n$ of Ramanujan-Nagell type. The two papers provide a simple procedure which, given A, B , C and n, enables us to decide whether techniques based on the theory of modular forms suffice to ensure that corresponding ternary equations lack nontrivial solutions in integers x , y, z and prime $n \geq 5$.

2.3.1 The Results of Ivorra and Kraus

The main result of the recipes of the paper [27] is that, under some technical restrictions on (l, k) and for $m \geq 1$, for n larger than an explicit bound

depending on l, k and m, the equation

$$Ax^n + By^n = Cz^2$$

has no solution for

$$(A, B, C) \in \{(2^k, l^m, 1), \qquad (2^k \cdot l^m, 1, 1), \qquad (1, l^m, 2)\}.$$

In the case $(A, B, C) = (4, 1, 3)$ it is proved that for $n \geq 7$ the equation

$$4x^n + y^n = 3z^2$$

has only the trivial solutions. Also for the case $(A, B, C) = (64, 1, 7)$ it is proved that for $n \geq 11$ the equation

$$64x^n + y^n = 7z^2$$

has only the trivial solutions.

From careful examination of elliptic curves with conductor $2^\alpha p$ possessing at least one rational 2-torsion point, Ivorra and Kraus proved the following theorem for $(A, B, C) = (1, p^m, 1)$.

Theorem 2.5. *(Ivorra and Kraus) For $m \in \mathbb{N}$ and $p \equiv 3, 5 \pmod 8$ prime, distinct from 3 or $k^2 + 1$ with $k \in \mathbb{N}$, the following Diophantine equation*

$$x^n + p^m y^n = z^2$$

is insoluble in coprime integers (x, y, z), provided n is a suitably large prime, relative to p.

Special Cases. This means that for suitably large prime n, relatively prime to p, the Diophantine equation

$$x^n + p^m y^n = z^2$$

has no solution for p in the set

$$\{11, 13, 19, 29, 43, 53, 59, 61, 67\}. \tag{2.4}$$

For this particular special list of small values for the prime p, Bennett and Skinner proved that the Diophantine equation

$$x^n + 2^\alpha p^m y^n = z^2$$

still has no solution for $\alpha \geq 3$ and occasionally for $\alpha = 2$ (see next section for details). As an application, W. Ivorra and A. Kraus showed how these results yield information on the rational points of the curves $y^2 = x^p + d$.

2.3.2 The Results of Bennett and Skinner

The main results of the paper [3] from the viewpoint of Diophantine equations, are as follows.

Theorem 2.6. *(Bennett and Skinner) If $n \geq 4$ is an integer and*

$$C \in \{1, 2, 3, 5, 6, 10, 11, 13, 17\}$$

then the equation

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

has no solutions in nonzero pairwise coprime integers (x, y, z) with, say, $x > y$, unless $(n, C) = (4, 17)$ or

$$(n, C, x, y, z) \in \{(5, 2, 3, -1, \pm 11), \qquad (5, 11, 3, 2, \pm 5), \qquad (4, 2, 1, -1, \pm 1)\}.$$

If $C = 1$ this is a result of Darmon and Merel [18]. The methods of Bennett and Skinner are unable to resolve the case $C = 7$ (see [3]).

Theorem 2.7. *(Bennett and Skinner) Suppose that $n \geq 7$ is prime. If*

$$(C, \alpha_0) \in \{(1, 2), (3, 2), (5, 6), (7, 4), (11, 2), (13, 2), (15, 6), (17, 6)\}$$

then the equation

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

has no solutions in nonzero pairwise coprime integers (x, y, z) *with* $xy \neq \pm 1$ *and integers* $\alpha \geq \alpha_0$*, unless, possibly,* $n \leq C$ *or* $(C, \alpha, n) = (11, 3, 13)$*.*

Theorem 2.8. *(Bennett and Skinner) Suppose that* $n \geq 11$ *is prime,* A, B *are coprime integers,* α, β *are nonnegative integers with* $\beta \geq 1$*. If*

$$AB \in \{2^\alpha 11^\beta, 2^\alpha 13^\beta, 2^\alpha 19^\beta, 2^\alpha 29^\beta, 2^\alpha 43^\beta, 2^\alpha 53^\beta, 2^\alpha 59^\beta, 2^\alpha 61^\beta, 2^\alpha 67^\beta\}$$

for $\alpha = 0$ *or* $\alpha \geq 3$*, or if*

$$AB \in \{2 \cdot 19^\beta, 4 \cdot 11^\beta, 4 \cdot 19^\beta, 4^\alpha 43^\beta, 4 \cdot 59^\beta, 4 \cdot 61^\beta, 4 \cdot 67^\beta\}$$

then the equation

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

has no solution in nonzero pairwise coprime integers (x, y, z)*, unless, possibly,* $n | AB$ *or we have* AB, n *and* α *as in the following table.*

AB	n	α	AB	n	α
$2^\alpha 19^\beta$	11	1	$2^\alpha 61^\beta$	13	$0, 3$
$2^\alpha 43^\beta$	11	$0, 3, \geq 7$	$2^\alpha 61^\beta$	31	≥ 7
$2^\alpha 53^\beta$	11	$2, 4, 5$	$2^\alpha 67^\beta$	11	$0, 3, 6$
$2^\alpha 53^\beta$	17	$0, 3$	$2^\alpha 67^\beta$	13	$0, 3$
$2^\alpha 59^\beta$	11	≥ 7	$2^\alpha 67^\beta$	17	$0, 3, \geq 7$
$2^\alpha 59^\beta$	29	6			

Theorem 2.9. *(Bennett and Skinner) Suppose that $n \geq 11$ is prime and α is a nonnegative integer. If $\beta \in \{5^\alpha, 11^\alpha, 13^\alpha\}$, then the equation*

$$x^n + By^n = 2z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z), unless, possibly, $n|B$.

Theorem 2.10. *(Bennett and Skinner) Suppose that $n \geq 11$ is prime, A, B are coprime integers α, β, γ, δ are nonnegative integers with $\alpha \geq 6$ and $AB = 2^\alpha p^\beta q^\gamma$, where*

$$(p, q) \in \{(3, 31)\ (\beta \geq 1), \quad (5, 11)\ (\alpha \geq 7), \quad (5, 19), \quad (5, 23)\ (\beta \geq 1),$$
$$(7, 19)\ (\gamma \geq 1), \quad (11, 13), \quad (11, 23)\ (\beta \geq 1), \quad (11, 29), \quad (11, 31)\ (\beta \geq 1),$$
$$(13, 31)\ (\beta \geq 1), \quad (19, 23)\ (\beta \geq 1), \quad (19, 29), \quad (29, 31)\ (\beta \geq 1)\}.$$

Then the equation

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

has no solution in nonzero pairwise coprime integers (x, y, z), unless, possibly, $n|AB$ or we have AB, n and α as in the following table.

AB	n	α	AB	n	α
$2^\alpha 5^\beta 23^\gamma$	11	≥ 7	$2^\alpha 11^\beta 29^\gamma$	13	≥ 7
$2^\alpha 7^\beta 19^\gamma$	11	≥ 7	$2^\alpha 19^\beta 23^\gamma$	11	≥ 7
$2^\alpha 11^\beta 23^\gamma$	11	≥ 6	$2^\alpha 19^\beta 29^\gamma$	11	≥ 7

In Theorem 2.5 Ivorra and Kraus proved that the Diophantine equation

$$x^n + p^m y^n = z^2$$

has no solution for certain class of primes $p \equiv 3,\ 5 \pmod 8$. For primes $p \equiv 7 \pmod 8$, Bennett and Skinner proved that this Diophantine equation still has no solution for the special choices of $p \in \{23, 31, 47, 71\}$ if we require z to be an even integer and n is not divisible by p. Here is the theorem.

Theorem 2.11. *(Bennett and Skinner) Suppose that $n \geq 11$ is prime and that m is a nonnegative integer. Then the following Diophantine equation*

$$x^n + p^m y^n = z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z) with $xy \equiv 1 \pmod 2$, and $p \in \{23, 31, 47, 71\}$ and unless, possibly, $p \neq n$.

2.4 Chen and Siksek

Recently, Chen and Siksek wrote a paper which proves that the equation

$$x^3 + y^3 = z^p, \qquad \gcd(x, y) = 1, \quad xyz \neq 0,$$

has no solutions for $p \equiv 51,\ 103,\ 105 \pmod{106}$ using a combination of the modular approach and quadratic reciprocity. Our approach is similar but has

to be much more complicated as we deal with a wider range of equations. In a more recent version of the paper, Chen and Siksek [11] also use quadratic reciprocity over number fields along with the modular approach to prove the following theorem.

Theorem 2.12. (Chen and Siksek) *Let $n \geq 3$. Suppose n is divisible by some positive integer d satisfying* **any** *of the following congruences,*

(I) $d \equiv 2, 3 \pmod 5$,

(II) $d \equiv 17, 61 \pmod{78}$,

(III) $d \equiv 51, 103, 105 \pmod{106}$,

(IV) $d \equiv 43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277, 295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529, 583, 589, 601, 619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835, 853, 907, 913, 925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123, 1129, 1141, 1159, 1177, 1231, 1237, 1249, 1267, 1285 \pmod{1296}$.

Then the equation $x^3 + y^3 = z^n$ does not have any primitive solutions with $xyz \neq 0$.

It follows from the above that the equation does not have primitive non-trivial solutions for a set of prime exponents n having Dirichlet density ≈ 0.628.

2.5 Conclusion and Aims

In short, the work of Darmon and Merel, Siksek, Ivorra and Kraus, Bennett and Skinner and others showed that the Diophantine equation

$$x^p - Dy^p = z^2$$

has no nontrivial solution for

$$D \in \{1, 4, 8, 11, 13, 16, 19, 29, 32, 38, 43, 44, 53, 59, 61, 64, 67, 76, 83, 88\}$$

and $p \geq 7$. Moreover, there is no nontrivial solution for

$$D \in \{23, 31, 47, 71\}$$

if z is even.

The aim of this thesis is to study the Diophantine equation (1.1) via the modular approach and quadratic reciprocity. This gives congruence conditions for the prime exponent p. For example, we will prove the following result if x is an even integer.

Theorem 2.13. *For sufficiently large prime p, and for x even, if the equation* (1.1) *has solutions, then the exponent p must satisfy the following congruences.*

D	$x \equiv 4, 6 \pmod 8$	$x \equiv 0, 2 \pmod 8$
15	$p \equiv 5 \pmod 6$	$p \equiv 1 \pmod 6$
23	$p \equiv 3, 7 \pmod{10}$	$p \equiv 1, 9 \pmod{10}$
39	$p \equiv 11, 13, 17 \pmod{18}$	$p \equiv 1, 5, 7 \pmod{18}$
47	$p \equiv 3, 13, 21 \pmod{22}$	$p \equiv 1, 9, 19 \pmod{22}$
55	*No Solution*	*No Solution*
63	$p \equiv 13, 19, 23, 29 \pmod{30}$	$p \equiv 1, 7, 11, 17 \pmod{30}$

We will find and study such list of restrictions and congruences for the exponents p for each case depending on which one of the integers x, y, z, D is even. We will do this case by case. We will try to study this family of Diophantine equation in general and in particular cases for $1 \leq D \leq 100$.

Table 2.1: List of exponent triples (p, q, r) of solved cases of the equation $x^p + y^q = z^r$ (for references see [13, Chapter 14] and [34]).

$\{n, n, n\}$	$n \geq 4$	Wiles and Taylor
$\{n, n, 2\}$	n prime ≥ 7	Darmon and Merel
$\{n, n, 2\}$	$n = 5, 6, 9$	Poonen
$\{n, n, 3\}$	n prime ≥ 7	Darmon and Merel
$\{n, n, 3\}$	$n = 4$	Lucas
$\{n, n, 3\}$	$n = 5$	Poonen
$\{3, 3, n\}$	$17 \leq n \leq 10000$	Kraus
$\{3, 3, n\}$	$n = 4, 5$	Bruin
$(2, n, 4)$		Darmon
$(4, n, 4)$		Darmon
$(2, 4, n)$	n prime ≥ 211	Ellenberg
$(2, 4, n)$	$n = 7$	Ghioca
$\{2n, 2n, 5\}$	$n \geq 7$ and $n = 2$	Bennett
$\{2n, 2n, 5\}$	$n = 3$	Bruin
$\{2n, 2n, 5\}$	$n = 5$	from Fermat's last theorem
$(2, 2n, 3)$	$7 < n < 1000$ and $n \neq 31$, n prime	Chen
$\{2, 4, 6\}$		Bruin
$\{2, 4, 5\}$	$2^5 + 7^2 = 3^4$	Bruin
$\{2, 4, 5\}$	$3^5 + 11^4 = 122^2$	Bruin
$\{2, 3, 9\}$	$13^2 + 7^3 = 2^9$	Bruin
$\{2, 3, 8\}$	$1^8 + 2^3 = 3^2$	Bruin
$\{2, 3, 8\}$	$43^8 + 96222^3 = 30042907^2$	Bruin
$\{2, 3, 8\}$	$33^8 + 1549034^2 = 15613^3$	Beukers and Zagier
$\{2, 3, 7\}$	$1^7 + 2^3 = 3^2$	Poonen, Schaefer, Stoll
$\{2, 3, 7\}$	$2^7 + 17^3 = 71^2$	Poonen, Schaefer, Stoll
$\{2, 3, 7\}$	$17^7 + 76271^3 = 21063928^2$	Poonen, Schaefer, Stoll
$\{2, 3, 7\}$	$9262^3 + 15312283^2 = 113^7$	Poonen, Schaefer, Stoll

Chapter 3

Technical Background

In this chapter we summarise the facts we need about elliptic curves, modular forms and the modular approach to Diophantine equations.

Here and elsewhere in the thesis, we use the computer package `MAGMA` [8] for our computations.

3.1 Notation, Terminology and Formulae Concerning Elliptic Curves

We collect here standard notation, terminology and formulae concerning elliptic curves which we will use throughout this thesis. Here we follow Cremona's book [17, Chapter 3] and Silverman's book [39, Chapter 3]. An

elliptic curve E defined over a field K has an equation or model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

with coefficients $a_i \in K$ and is non-singular. We call such an equation a Weierstrass equation for E. The set of K-rational points on E is denoted by $E(K)$ and given by

$$E(K) := \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity. It turns out that $E(K)$ forms an abelian group with $\mathcal{O}$ being the identity, as explained in any book on elliptic curves.

From these coefficients we derive the auxiliary quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_3^2a_2 - a_4^2, \end{aligned}$$

the discriminant of E

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

the invariants

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \end{aligned}$$

and the j-invariant $j = \frac{c_4^3}{\Delta}$. These are related by the identities

$$4b_8 = b_2b_6 - b_4^2 \qquad \text{and} \qquad 1728\Delta = c_4^3 - c_6^2.$$

The discriminant Δ must be non-zero for the curve defined by equation (3.1) to be nonsingular and hence an elliptic curve. If E has a Weierstrass equation in the simplified form $y^2 = x^3 + Ax + B$ then

$$\Delta = -16(4A^3 + 27B^2), \qquad j = -\frac{1728(4A)^3}{\Delta}.$$

If two Weierstrass equations

$$\begin{aligned} E &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E' &: y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'. \end{aligned}$$

are related by the change of variables $(x, y) \mapsto (x', y')$ of the form:

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t \tag{3.2}$$

with $u, r, s, t \in K$ and $u \neq 0$, then we say they are isomorphic. It turns out that the map

$$E(K) \to E'(K), \qquad (x, y) \mapsto (x', y'), \quad \mathcal{O} \mapsto \mathcal{O}'$$

is an isomorphism of abelian groups. We think of the two Weierstrass equations as two models for the same elliptic curve. The effect of this change of coordinates on the coefficients a_i is given by

$$\begin{aligned} a_1 + 2s &= ua_1' \\ a_2 - sa_1 + 3r - s^2 &= u^2 a_2' \\ a_3 + ra_1 + 2t &= u^3 a_3' \\ a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st &= u^4 a_4' \\ a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 &= u^6 a_6' \end{aligned}$$

so that

$$c_4 = u^4 c_4', \qquad c_6 = u^6 c_6', \qquad \Delta = u^{12}\Delta' \qquad \text{and} \qquad j = j'.$$

Let K be a field, and let $\overline{K}$ be a fixed algebraic closure of K. Two elliptic curves E and E' are isomorphic over $\overline{K}$ if and only if they have the same j invariant, i.e. $j(E) = j(E')$. The j-invariant is invariant under isomorphism;

elliptic curves with the same j are called twists: they are isomorphic over an algebraic extension, but not necessarily over K.

3.1.1 Minimal Models

Let E now be an elliptic curve over $\mathbb{Q}$. If $K = \mathbb{Q}$, we say that the model (3.1) is integral or defined over $\mathbb{Z}$ if all the a_i are in $\mathbb{Z}$. We denote the change of coordinates in (3.2) by $T(r, s, t, u)$. By applying $T(0, 0, 0, u)$ for suitable u we can always transform to an integral model; all the invariants are then integral, except (possibly) for j. Among such integral models, those for which the positive integer $|\Delta|$ is minimal are called global minimal models for E. The minimal discriminant $\Delta_{\min}$ is the discriminant of a global minimal Weierstrass equation for $E/\mathbb{Q}$. Every elliptic curve E defined over $\mathbb{Q}$ has a minimal model which is not unique, but $\Delta_{\min}$ is unique. Global minimial Weierstrass equations are good for studying the reductions of $E \pmod p$. Isomorphisms between minimal models must have $u = \pm 1$ and $r, s, t \in \mathbb{Z}$. There is an explicit algorithm due to Tate for computing the minimal model, given for example in [17, Section 3.2] and [40, Section IV.9].

To any elliptic curve E is associated an invariant called the conductor N_E. The conductor is a divisor of the (minimal) discriminant but is rather more difficult to describe precisely. The set of primes dividing the minimal discriminant coincides with the set of primes dividing the conductor (which are the primes such that the reduced curve is singular). The conductor N_E

of $E/\mathbb{Q}$ is equal

$$N_E = \prod_{p \text{ prime}} p^{\gamma_p(E)},$$

where

$$\gamma_p(E) = \begin{cases} 0 & \text{if } p \nmid \Delta \text{ } \textit{(p is a prime of good reduction)} \\ 1 & \text{if } p \mid \Delta \text{ and } p \nmid c_4 \text{ } \textit{(p is a prime of multiplicative reduction)}, \\ 2 + \delta_p & \text{if } p \mid \Delta,\ p \mid c_4 \text{ } \textit{(p is a prime of additive reduction)}. \end{cases}$$

Here $\delta_p \geq 0$ and $\delta_p = 0$ if $p \geq 5$. For $p = 2$, 3, δ_p is complicated and can be determined by Tate's algorithm. The conductor N_E of the curve E may be viewed as a convenient encoding of the places where E has bad reduction. It also encodes the nature of that reduction. If N_E is squarefree, then the elliptic curve E is said to be *semistable*.

3.2 Torsion

The torsion of a group G is the set

$$G_{\text{tors}} = \{g \in G : g^n = e \text{ for some } n \in \mathbb{N}\}.$$

A group is said to be torsion-free if $G_{\text{tors}} = \{e\}$, where e is the identity element. If G is abelian then G_{tors} is a subgroup *(the torsion subgroup)* of G. For any finite group G, $G_{\text{tors}} = G$.

The following theorem, proved independently by E. Lutz and T. Nagell, gives a very efficient method to compute the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$.

Theorem 3.1. (Nagell, Lutz) *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation:*

$$y^2 = x^3 + Ax + B, \qquad A,\ B \in \mathbb{Z}.$$

Then for all non-zero torsion points P, the coordinates of P are in $\mathbb{Z}$, i.e.

$$x(P),\ y(P) \in \mathbb{Z}.$$

If P is of order greater than 2 , then

$$y(P)^2 \mid (4A^3 + 27B^2).$$

If P is of order 2 then

$$y(P) = 0 \qquad \textit{and} \qquad x(P)^3 + Ax(P) + B = 0.$$

3.3 Isogenies

Here we follow [39, Chapter] and [12, Chapter 7]. Let E and E' be two elliptic curves over $\mathbb{Q}$ with identity elements $\mathcal{O}$, $\mathcal{O}'$ respectively, and let ϕ be a morphism of algebraic curves from E to E' (i.e. ϕ is defined by rational

functions). We say that ϕ is an *isogeny* if $\phi(\mathcal{O}) = \mathcal{O}'$. It turns out that an isogeny $\phi : E \to E'$ is a group homomorphism with respect to the group laws on E and E'. In other words, $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$. A non-constant isogeny is one such that there exists $P \in E$ such that $\phi(P) \neq \mathcal{O}'$. We say that E and E' are isogenous if there exists a nonconstant isogeny from E to E'. An isogeny of the curve with itself is called an endomorphism.

Let $\phi : E \to E'$ be a non-constant isogeny from the elliptic curve $E/\mathbb{Q}$ to the elliptic curve $E'/\mathbb{Q}$. We define the degree of isogeny ϕ to be $\deg(\phi) = \#\operatorname{Ker}(\phi)$ where

$$\operatorname{Ker}(\phi) = \{P \in E(\overline{\mathbb{Q}}) : \phi(P) = \mathcal{O}'\}$$

An *m-isogeny* is simply an isogeny of degree m.

If $\phi : E \to E'$ is an m-isogeny, then there is a *dual isogeny* $\hat{\phi} : E' \to E$, which is also of degree m and satisfies $\phi \circ \hat{\phi} = [m]_{E'}$ and $\hat{\phi} \circ \phi = [m]_E$; here $[m]_E$ and $[m]_{E'}$ denote multiplication by m on E and E' respectively. This makes isogenies into an equivalence relation.

3.3.1 Absence of Isogenies

We shall need to know that for certain Frey elliptic curves that there are no isogenies of large prime degree. The following two theorems appearing in [13, Chapter 15] are very useful.

Theorem 3.2. *(Mazur) Suppose $E/\mathbb{Q}$ is an elliptic curve of conductor N and that at least one of the following conditions holds.*

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

Then E *does not have any* p*-isogenies.*

Theorem 3.3. *(Diamond and Kramer) Suppose that* $E/\mathbb{Q}$ *is an elliptic curve with conductor* N*. If* $\mathrm{ord}_2(N) = 3,\ 5,\ 7$ *then* E *does not have any* p*-isogeny for* p *an odd prime.*

3.4 Elliptic curves over $\mathbb{F}_p$

We also need Hasse's estimate for the number of points on an elliptic curve of the field $\mathbb{F}_p$; for a proof see [39, Chapter V]

Theorem 3.4. (Hasse) *If* E *is an elliptic curve over the field* $\mathbb{F}_p$*, where* p *is a prime. Then the number of points* $\#E(\mathbb{F}_p)$ *satisfies*

$$|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}.$$

We define the *trace* $a_p(E)$ by

$$a_p(E) := p + 1 - \#E(\mathbb{F}_p).$$

By Theorem 3.4, $|a_p(E)| < 2\sqrt{p}$.

3.5 Modular Forms

This section briefly introduces modular forms; we follow Milne's book [33, Chapter 5]. We denote the imaginary part of a complex number z by $\Im(z)$. The complex *upper half plane* is given by

$$H = \{z \in \mathbb{C} : \Im(z) > 0\}.$$

The extended upper half plane is given by

$$H^* = H \cup \mathbb{Q} \cup \{i\infty\}.$$

The modular group $\mathrm{SL}_2(\mathbb{Z})$ is given by

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{Z} \right\}.$$

The modular group acts on H^* via fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & c \end{pmatrix} z = \frac{az + b}{cz + d}.$$

The matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

are both elements of $\mathrm{SL}_2(\mathbb{Z})$; the matrix S induces the function $z \mapsto -1/z$ on H, and T induces the function $z \mapsto z+1$. The modular group $\mathrm{SL}_2(\mathbb{Z})$ is generated by S and T.

If N is a positive integer, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

It is easy to see that $\Gamma_0(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

3.5.1 Modular Forms of level N and Weight k

Let k and N be positive integers. A modular form of weight k for $\Gamma_0(N)$ is a function $f : H \to \mathbb{C}$ such that

1. for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and $z \in H$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

2. f is holomorphic on H,

3. f is holomorphic on the cusps $\mathbb{Q} \cup \{i\infty\}$.

We shall explain this last condition. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, then $f(z+1) = f(z)$ for every z. Thus the modular forms are periodic with period 1, and

therefore have a Fourier series. This means that there are numbers c_n such that for all $z \in H$, we have

$$f(z) = \sum_{n=m}^{\infty} c_n q^n \qquad (q = e^{2\pi iz}),$$

for some integer $m \in \mathbb{Z}$; this series is called the *q-expansion* of f. The coefficients c_n are the Fourier coefficients of f. The order of f at $i\infty$ is defined to be m. Thus we want $m \geq 0$ to say that f is holomorphic at $i\infty$. If $r \neq \infty$ is any other cusp then choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(i\infty) = r$ and we say f is holomorphic at r if $f \circ \gamma$ is holomorphic at $i\infty$.

A modular form is called a *cusp form* if it is zero at all the cusps. This means for the cusp at infinity that

$$f(z) = \sum_{n\geq 1} c_n q^n \qquad (q = e^{2\pi iz}).$$

We shall only be concerned with modular forms of weight 2. The cusp forms of weight 2 for $\Gamma_0(N)$ form a finite dimensional vector space denoted by $S_2(N)$. The space $S_2(N)$ has a natural inner product (called the Peterson inner product), so that it is possible to consider orthogonality in $S_2(N)$.

Let $N \geq 1$. If K divides N then $\Gamma_0(N) \subseteq \Gamma_0(K)$ and so $S_2(K) \subseteq S_2(N)$. We define the *old subspace* $S_2^{\mathrm{old}}(N)$ of $S_2(N)$ to be the subspace generated by $S_2(K)$ for all $K \mid N$, $K < N$. We define the *new subspace* $S_2^{\mathrm{new}}(N)$ to be the subspace of $S_2(N)$ orthogonal to $S_2^{\mathrm{old}}(N)$.

Hecke defined for each $n \geq 1$ coprime to N, a linear operator T_n on $S_2(N)$. For $(nm, N) = 1$, the Hecke operators T_n and T_m commute: $T_n \circ T_m = T_m \circ T_n$. A cusp form which is an eigenfunction for all Hecke operators T_n is called an eigenform.

3.5.2 Newforms

Definition. *By a* newform of level N *we mean a cusp form of weight* 2 *for* $\Gamma_0(N)$*, belonging to the new space, normalised so that* $c_1 = 1$ *in the Fourier expansion at infinity, and is a simultaneous eigenfunction for all the Hecke operators.*

Thus a newform has a q-expansion

$$f = q + \sum_{n \geq 2} c_n q^n. \tag{3.3}$$

The following facts (see [13, page 496]) about newforms are crucial to us and will be used throughout the thesis:

1. If we fix N, then there are only finitely many newforms of level N.

2. If f is a newform with coefficients c_n as in (3.3) and $K = \mathbb{Q}(c_2, c_3, \ldots)$ then K is a totally real finite extension of $\mathbb{Q}$, in other words is a totally real number field.

3. The coefficients c_n are algebraic integers, in other words they belong to the ring of integers $\mathcal{O}_K$ of the number field K. If $\mathcal{O}_K = \mathbb{Z}$, then we call f a *rational newform*. Otherwise, we call f an *irrational newform*.

4. If ℓ is a prime then

$$|c_\ell^\sigma| \leq 2\sqrt{\ell} \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}. \tag{3.4}$$

We shall only be concerned about newforms up to Galois conjugacy. The number of newforms (up to Galois conjugacy) at a particular level depends in a very erratic way on the level N. For a given level N, the number of newforms (up to conjugacy or not) is finite. Below, we quote a standard formula for the number of newforms of level N.

Theorem 3.5. *([13, Proposition 15.1.1]) We define five arithmetic functions $A_i(N)$ for $1 \leq i \leq 5$ by asking that they be multiplicative, and that their values on prime powers p^k be given as follows:*

1. $A_1(p) = -1$, $A_1(p^k) = 0$ *for* $k \geq 2$.

2. $A_2(p) = p - 1$, $A_2(p^2) = p^2 - p - 1$, $A_2(p^k) = (p-1)(p^{k-1} - p^{k-3})$ *for* $k \geq 3$.

3. $A_3(p) = \left(\frac{-4}{p}\right) - 1$, $A_3(p^2) = -\left(\frac{-4}{p}\right)$, $A_3(p^k) = 0$ *when* $k \geq 3$ *and* $p \neq 2$. *While* $A_3(2) = A_3(4) = -1$, $A_3(8) = 1$, *and* $A_3(2^k) = 0$ *for* $k \geq 4$.

4. $A_4(p) = \left(\frac{-3}{p}\right) - 1$, $A_4(p^2) = -\left(\frac{-3}{p}\right)$, $A_4(p^k) = 0$ *when* $k \geq 3$ *and* $p \neq 3$. *While* $A_4(3) = A_4(9) = -1$, $A_4(27) = 1$, *and* $A_4(3^k) = 0$ *for* $k \geq 4$.

5. $A_5(p^2) = p-2$, $A_5(p^{2k}) = p^{k-2}(p-1)^2$, *for* $k \geq 2$. *While* $A_5(p^{2k-1}) = 0$ *for* $k \geq 1$.

The number of newforms of level N *(counting conjugate ones as distinct) is equal to*

$$A_1(N) + \frac{A_2(N)}{12} - \frac{A_3(N)}{4} - \frac{A_4(N)}{3} - \frac{A_5(N)}{2}.$$

According to [13, page 496], the number of newforms up to conjugacy does not have any known closed form. From this theorem, it is possible to deduce [13, page 497] the following well-known corollary.

Corollary 3.5.1. *There are no newforms at levels*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

Moreover, for all other levels there are newforms.

The computation of newforms at a particular level can be done using the modular symbols algorithm [17], [41]. This has been implemented by William Stein in `MAGMA`, and is used throughout the thesis for newform computations.

Example 3.5.1. The formula shows that the number of newforms of level 11 is equal to $A_1(11) + \frac{A_2(11)}{12} - \frac{A_3(11)}{4} - \frac{A_4(11)}{3} - \frac{A_5(11)}{2} = 1$. So, we have only

one newform at level 11 which is the following rational newform:

$$g = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots .$$

Example 3.5.2. The newforms at level 77 are

$$\begin{aligned}
f_1 &= q - 3q^3 - 2q^4 - q^5 - q^7 + 6q^9 - q^{11} + \cdots , \\
f_2 &= q + q^2 + 2q^3 - q^4 - 2q^5 + 2q^6 - q^7 - 3q^8 + q^9 + \cdots , \\
f_3 &= q + q^3 - 2q^4 + 3q^5 + q^7 - 2q^9 - q^{11} + \cdots , \\
f_4 &= q + \sqrt{5}q^2 + (-\sqrt{5}+1)q^3 + 3q^4 - 2q^5 + (\sqrt{5}-5)q^6 + \cdots \\
f_5 &= q - \sqrt{5}q^2 + (\sqrt{5}+1)q^3 + 3q^4 - 2q^5 + (-\sqrt{5}-5)q^6 + \cdots .
\end{aligned}$$

Here the first three are rational newforms and have coefficients in $\mathbb{Z}$. The last two are conjugate irrational newforms with coefficients in $\mathbb{Z}[(1+\sqrt{5})/2]$. As stated above, we will only need to worry about newforms up to Galois conjugacy.

3.6 Correspondence between rational newforms and elliptic curves

In this section, and for the rest of this chapter we follow Cohen's book [13, Chapter 15], although the examples are our own. Recall that a newform f is rational when the field K associated with f is equal to $\mathbb{Q}$; in other

words if all the Fourier coefficients of f are in $\mathbb{Z}$. Rational newforms will be particularly important for us. We recall the modularity theorem for elliptic curves, proved by Wiles and successors.

Theorem 3.6. (The Modularity Theorem for Elliptic Curves) *Associated to any rational newform f of level N is an elliptic curve E_f defined over $\mathbb{Q}$ and of conductor equal to N so that for all primes $\ell \nmid N$*

$$c_\ell = a_\ell(E_f)$$

where c_ℓ is the ℓ-th coefficient in the q-expansion of f and

$$a_\ell(E_f) = \ell + 1 - \#E_f(\mathbb{F}_\ell).$$

Moreover, for any given positive integer N, the association

$$f \longmapsto E_f$$

is a bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.

Remarks. The association $f \longmapsto E_f$ is due to Shimura. The fact that this association is surjective was previously known as the Modularity Conjecture, and first proved for squarefree N (the semi-stable case) by Wiles [43], [42]. The proof was completed in a series of papers by Diamond [21], Conrad, Diamond and Taylor [16], and finally Breuil, Conrad, Diamond and Taylor

[9]. The above theorem, is needed, as we will see in this thesis, to go back and forth with ease between rational newforms and elliptic curves.

Example 3.6.1. In example 3.5.2 we looked at the newforms at level 77. Let us return to these and examine them with a view towards the Modularity Theorem (Theorem 3.6). We see from the Modularity Theorem that up to isogeny there exists exactly three elliptic curves of conductor 77 defined over $\mathbb{Q}$. Using `MAGMA` we find that f_1,f_2,f_3 correspond respectively to the curves denoted by $77A1$, $77C1$, and $77B1$ in the tables of Cremona [17]. Therefore

$$f_1 \longmapsto E_1, \quad f_2 \longmapsto E_2, \quad f_3 \longmapsto E_3,$$

where E_1, E_2 and E_3 are the elliptic curves

$$E_1 : y^2 + y = x^3 + 2x,$$
$$E_2 : y^2 + xy = x^3 + x^2 + 4x + 11,$$
$$E_3 : y^2 + y = x^3 + x^2 - 49x + 600.$$

3.7 Ribet's Level-Lowering Theorem

We continue to follow the presentation in Cohen's book [13, Chapter 15].

3.7.1 'Definition of Arises From'

Definition. *Let E be an elliptic curve over the rationals of conductor N, and suppose that f is a newform (of weight 2 as always) and level N' with q-expansion as in (3.3), and coefficients c_i generating the number field $K/\mathbb{Q}$. We shall say that the curve E arises modulo p from the newform f, and write*

$$E \sim_p f,$$

if there is some prime ideal $\mathfrak{P} \mid p$ of K such that for all but finitely many primes ℓ, we have

$$a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}},$$

where c_ℓ is the ℓ-th Fourier coefficient of f and $a_\ell(E) = \ell + 1 - |E(\mathbb{F}_\ell)|$.

In fact we can be a little more precise.

Proposition 3.7.1. *Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of K such that for all primes ℓ*

(i) if $\ell \nmid pNN'$ then $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}}$, and

(ii) if $\ell \nmid pN'$ and $\ell \,||\, N$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{P}}$.

Notation. If f is a rational newform, then we know that f corresponds to some elliptic curve F say (this is E_f in the notation of Theorem 3.6). If E arises modulo p from f then we shall also say that E arises modulo p from F (and write $E \sim_p F$).

There is essential refinement of Proposition 3.7.1 due to Kraus and Oesterlé, which gives the final form of the notion $\sim_p$ that we will use continuously in the thesis.

Proposition 3.7.2. *(Kraus and Oesterlé) Suppose that E, F are elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that E arises modulo p from F. Then for all primes ℓ we have*

(i) if $\ell \nmid NN'$ then

$$a_\ell(E) \equiv a_\ell(F) \pmod{p},$$

and

(ii) if $\ell \nmid N'$ and $\ell \,||\, N$ then

$$\ell + 1 \equiv \pm a_\ell(F) \pmod{p}.$$

Remarks:

- Proposition 3.7.2 gives a very important strengthening namely the assumption that $\ell \neq p$ in Proposition 3.7.1 is now removed. This is important because later on p will be an unknown prime exponent for some equation that we would like to solve, and it would be awkward to have conditions depending on p.

- The condition $\ell \nmid NN'$ is equivalent to saying that the two elliptic curves E and F have good reduction at ℓ.

- The condition $\ell \nmid N'$ and $\ell \,||\, N$ means that E has multiplicative reduction at ℓ, whilst F has good reduction at ℓ.

3.7.2 Ribet's Level-Lowering Theorem

Definition. *Let E be an elliptic curve over $\mathbb{Q}$. Let $\Delta = \Delta_{\min}$ be the discriminant for a minimal model of E, and N be the conductor of E. Suppose p is a prime, and let*

$$N_p := N \Big/ \prod_{\substack{q||N, \\ p \,|\, \mathrm{ord}_q(\Delta)}} q; \tag{3.5}$$

in other words, N_p is equal to N divided by the product of all prime numbers q such that $v_q(N) = 1$ and $p \mid v_q(\Delta_{\min})$.

We emphasise that the Δ appearing in the definition of N_p must be the minimal discriminant.

Theorem 3.7. *(***Ribet's Level-Lowering Theorem***) Suppose E is an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ is prime number. Suppose further that there does not exist a p-isogeny (i.e of degree p) defined over $\mathbb{Q}$ from E to some other elliptic curve. Let N_p be defined as above. Then there exists a newform f of level N_p such that*

$$E \sim_p f.$$

Example 3.7.1. The following example is given in [13, page 500] but we give it in more detail. Consider the elliptic curve

$$E \ : \quad y^2 = x^3 - x^2 - 77x + 330$$

with Cremona reference 132B1. The minimal discriminant and conductor are respectively

$$\Delta_{\min} = 2^4 \times 3^{10} \times 11, \qquad N = 2^2 \times 3 \times 11.$$

From the table in Cremona's book [17] we find that the only isogeny that the curve E has is a 2-isogeny. Hence we may apply Ribet's Theorem with $p = 5$. From the above recipe (3.5) for the level we find that

$$N_p = \frac{2^2 \times 3 \times 11}{3} = 44.$$

However, there is only one newform at level 44 which is

$$f = q + q^3 - 3q^5 + 2q^7 - 2q^9 - q^{11} + \cdots,$$

which corresponds to the elliptic curve

$$F \ : \quad y^2 = x^3 + x^2 + 3x - 1$$

with conductor 44 and with Cremona reference $44A1$. Thus $E \sim_5 F$.

Then, by Proposition 3.7.2, for all primes ℓ we have

(i) if $\ell \notin \{2, 3, 11\}$ then

$$a_\ell(E) \equiv a_\ell(F) \pmod 5,$$

and

(ii) if $\ell = 3$ then

$$\ell + 1 \equiv \pm a_\ell(F) \pmod 5.$$

We record here the traces for E and F for primes $2 \leq l \leq 37$ which are consistent with what is expected from Proposition 3.7.2.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37
$a_\ell(E)$	0	-1	2	2	-1	6	-4	-2	-8	0	0	-6
$a_\ell(F)$	0	1	-3	2	-1	-4	6	8	-3	0	5	-1

Example 3.7.2. The following example is given as an exercise in [38]. We give it in detail as the idea used to identify the correct newform in Ribet's Theorem will be used throughout the thesis. Let

$$E \ : \quad y^2 + xy = x^3 - x^2 - 47808x + 4476064.$$

The minimal discriminant of E is

$$\Delta_{\min} = -1615648817503008 = 2^5 \times 3^{18} \times 19^4,$$

and its conductor is

$$N = 342 = 2 \times 3^2 \times 19.$$

We would like to apply Ribet's Theorem with $p = 5$. So we need to show that E has no 5-isogenies. Using `MAGMA` we computed the 5-th division polynomial of E and showed that it is irreducible. Therefore, E has no 5-isogenies. Now, we can apply Ribet's Theorem to E with $p = 5$. Clearly

$$N_5 = \frac{2 \times 3^2 \times 19}{2} = 171$$

Therefore $E \sim_5 f$ where f is a newform of level $N_5 = 171$.

We need to compute all the newforms at level 171. By using `MAGMA`, there are 4 rational newforms and 1 irrational newform at level 171:

$$f_1 = q - q^2 - q^4 + 2q^5 + 3q^8 - 2q^{10} + 6q^{13} + \cdots,$$

$$f_2 = q + 2q^2 + 2q^4 - q^5 + 3q^7 - 2q^{10} + 3q^{11} + \cdots,$$

$$f_3 = q + 2q^2 + 2q^4 + 3q^5 - 5q^7 + 6q^{10} - q^{11} + \cdots,$$

$$f_4 = q - 2q^4 - 3q^5 - q^7 - 3q^{11} + \cdots,$$

$$f_5 = q + aq^2 + (a^2 - 2)q^4 + 1/2(-a^3 + 5a)q^5 + (-a^2 + 5)q^7$$
$$+(a^3 - 4a)q^8 + (-2a^2 + 6)q^{10} + 1/2(a^3 - 9a)q^{11} + \cdots.$$

where a is a root of $x^4 - 9x^2 + 12$. Now let

$$f \in \{f_1, f_2, f_3, f_4, f_5\}.$$

If

$$E \sim_5 f$$

then, by Proposition 3.7.2, any prime $\ell \notin \{2, 3, 5, 19\}$ must satisfy

$$\mathrm{Norm}_{K/\mathbb{Q}}(a_\ell(E) - a_\ell(f)) \equiv 0 \pmod 5,$$

where K is the field of coefficients of f. Note that

- $a_{11}(E) - a_{11}(f_1) = 4 \not\equiv 0 \pmod 5$,
- $a_7(E) - a_7(f_2) = -3 \not\equiv 0 \pmod 5$,
- $a_7(E) - a_7(f_4) = 1 \not\equiv 0 \pmod 5$,
- $\mathrm{Norm}(a_7(E) - a_7(f_5)) = 64 \not\equiv 0 \pmod 5$.

Thus $E \not\sim_5 f_i$ for $i = 1, 2, 4, 5$. This finally means that

$$E \sim_5 f_3.$$

Again, we record here the traces for E and f_3 for the primes

$$\{5, 7, 11, 13, 17, 23, 29, 31, 37\}$$

which is consistent with what is expected from Proposition 3.7.2.

ℓ	5	7	11	13	17	23	29	31	37
$a_\ell(E)$	-2	0	4	2	6	4	2	4	10
$a_\ell(f_3)$	3	-5	-1	2	1	4	2	-6	0

3.8 Fermat's Last Theorem

In this section we use the above to give the proof of Fermat's Last Theorem, following Cohen's book [13, Chapter 15]. The main reason for doing this is to explain why our equation (1.1) is more difficult and cannot be done by exactly the same method.

Theorem 3.8. (Wiles) *Suppose $p \geq 5$ is prime. The equation*

$$x^p + y^p + z^p = 0 \tag{3.6}$$

has no solutions in non-zero integers.

Proof. Suppose x, y, z are non-zero integers satisfying (3.6). We can assume that x, y, z are pairwise coprime, and by interchanging them and changing the signs if necessary, that

$$2 \mid y, \qquad x \equiv -1 \pmod 4.$$

Associate to this equation the Frey elliptic curve,

$$E \ : \quad Y^2 = X(X - x^p)(X + y^p), \tag{3.7}$$

with associated invariants

$$c_4 = 16(z^{2p} - x^p y^p), \qquad \Delta = 2^4 (xyz)^{2p}.$$

We need to determine the conductor N of E. If p is an odd prime dividing Δ, then by the coprimality condition on x, y, z we have $p \nmid c_4$. So E is already minimal and has multiplicative reduction at p (see page 31). It turns out that E is not a minimal model. Using the change of coordinates $T(0, 4, 0, 2)$ we get the model,

$$E' \; : \quad Y^2 + XY = X^3 + \frac{1}{4}(-1 - x^p - y^p)X^2 - \frac{x^p y^p}{16} X.$$

Notice that this model is integral because of the congruence conditions above. Using the formulas in Section 3.1, the new invariants are

$$c_4' = (z^{2p} - x^p y^p), \qquad \Delta = \frac{(xyz)^{2p}}{2^8}.$$

In particular, $2 \nmid c_4'$, so this model is minimal at 2 and has multiplicative reduction. By Section 3.1.1 we know that the conductor N of E is

$$N = 2 \prod_{\substack{\ell | xyz,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell.$$

Now $E(\mathbb{Q})[2] = 4$ and the conductor N is squarefree. So by Mazur's Theorem (Theorem 3.2), E does not have p-isogenies. By Ribet's Theorem 3.7, $E \sim_p f$

where f is a newform at level

$$N_p := N \Big/ \prod_{\substack{q||N, \\ p \,|\, \mathrm{ord}_q(\Delta')}} q = 2.$$

By Corollary 3.5.1, there are no newforms with level 2. This contradiction proves the theorem. □

For our equation (1.1) there are Frey curves that give us small levels N_p. These are special cases of Frey curves by Ivorra and Kraus given in the next section. However, the level N_p will very rarely belong to the list in (1.1) and so we will not be able to deduce a contradiction.

3.9 Bounding the Exponent

The last result we need from the modular approach is the following result for bounding p if $E \sim_p f$. This is given in [13, Proposition 15.4.1] and [38].

Proposition 3.9.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and suppose that t divides the order of the torsion subgroup of $E(\mathbb{Q})$. Suppose that f is a newform of level N'. Let ℓ be a prime such that $\ell \nmid N'$ and $\ell^2 \nmid N$. Let*

$$S_\ell = \left\{ a \in \mathbb{Z} \ : \quad -2\sqrt{\ell} \le a \le 2\sqrt{\ell}, \quad a \equiv \ell + 1 \pmod{t} \right\}.$$

Let c_ℓ be the ℓ-th coefficient of f and define

$$B'_\ell(f) = \mathrm{Norm}_{K/\mathbb{Q}}((\ell+1)^2 - c_l^2) \prod_{a \in S_\ell} \mathrm{Norm}_{K/\mathbb{Q}}(a - c_\ell)$$

where $K = \mathbb{Q}(c_1, c_2, \dots)$ is the field generated by the coefficients of f. Let

$$B_\ell(f) = \begin{cases} \ell \cdot B'_\ell(f) & \text{if } f \text{ is irrational,} \\ B'_\ell(f) & \text{if } f \text{ is rational.} \end{cases}$$

If $E \sim_p f$ then $p \mid B_\ell(f)$.

It is easy to prove this proposition from Propositions 3.7.1, 3.7.2, Hasse's Theorem 3.4, and the fact the if ℓ is a prime of good reduction for E then $\ell + 1 - a_\ell(E) = \#E(\mathbb{F}_l) \equiv 0 \pmod{t}$.

Chapter 4

Modular Approach to the Diophantine Equations $x^p - Dy^{2p} = z^2$

4.1 Introduction

For the rest of the thesis we study the family of Diophantine equations

$$x^p - Dy^{2p} = z^2, \qquad (x, z) = 1, \quad y \neq 0, \quad p \text{ is a prime} \geq 7, \qquad (4.1)$$

where

$$1 \leq D \leq 100.$$

Our study combines the modular approach with the Law of Quadratic Reciprocity.

To apply the modular approach to this Diophantine equation, we need to construct a Frey curve or curves associated to our Diophantine equation. A recent paper of W. Ivorra and A. Kraus [27] gives recipes for Frey elliptic curves for the Diophantine equation

$$ax^p + by^p = cz^2. \tag{4.2}$$

We note that our family (4.1) is a special case of (4.2). We apply the modular approach and study the newforms (rational and irrational) that arise from the solutions. From this we derive certain conditions on the solutions. Then we combine these restrictions that come from the modular approach with other restrictions that come from quadratic reciprocity. This would lead us to certain conditions and congruences for the prime p.

4.2 The two Frey curves of Ivorra and Kraus

For the Diophantine equation (4.2) with the following restrictions:

$$\begin{cases} p \text{ prime } \geq 7,\ abcxyz \neq 0, \\ b \text{ is odd, } c \text{ is square-free, } \gcd(ax, by) = 1 \\ \text{if } cz \text{ is odd, then without loss of generality choose } z \text{ so that } cz \equiv -1 \pmod 4 \end{cases}$$

Ivorra and Kraus [27] construct two Frey curves E_1, E_2. The first Frey curve given by Ivorra and Kraus for equation (4.2) is

$$E_1 : Y^2 = X^3 + (2cz)X^2 + (acx^p)X,$$

with minimal discriminant

$$\Delta_{E_1} = \begin{cases} 2^6(a^2bc^3)(x^2y)^p & \text{if } E_1 \text{ has additive reduction at 2,} \\ 2^{-6}(a^2bc^3)(x^2y)^p & \text{otherwise,} \end{cases}$$

and conductor

$$N_{E_1} = \alpha_1 \cdot \prod_{\substack{\ell \mid abxy,\ \ell \neq 2 \\ \ell \text{ is prime}}} \ell \cdot \prod_{\substack{\ell \mid c,\ \ell \neq 2 \\ \ell \text{ is prime}}} \ell^2,$$

where α_1 is a power of 2 given below. The second Frey curve given by Ivorra and Kraus for equation (4.2) is

$$E_2 : Y^2 = X^3 + (2cz)X^2 + (bcy^p)X.$$

with minimal discriminant

$$\Delta_{E_2} = \begin{cases} 2^6(ab^2c^3)(xy^2)^p & \text{if } E_2 \text{ has additive reduction at 2,} \\ 2^{-6}(ab^2c^3)(xy^2)^p & \text{otherwise,} \end{cases}$$

and conductor

$$N_{E_2} = \alpha_2 \cdot \prod_{\substack{\ell \mid abxy,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell \cdot \prod_{\substack{\ell \mid c,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell^2,$$

where α_2 is a power of 2 also given below. Define

$$N_1 = \alpha_1 \cdot \prod_{\substack{\ell \mid ab,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell \cdot \prod_{\substack{\ell \mid c,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell^2$$

where

$$\alpha_1 := \begin{cases} 2^8 & 2 \mid c \\ 2^7 & 2 \| a, 2 \nmid x \\ 2^6 & 4 \mid a \\ 2^6 & 2 \mid x \\ 2^6 & acx \equiv 1 \pmod 4, 2 \mid z, 2 \nmid c \\ 2^5 & acx \equiv 3 \pmod 4, 2 \mid z, 2 \nmid c \\ 2 & 2 \mid y \end{cases}$$

and

$$N_2 := \alpha_2 \cdot \prod_{\substack{\ell \mid ab,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell \cdot \prod_{\substack{\ell \mid c,\, \ell \neq 2 \\ \ell \text{ is prime}}} \ell^2$$

where

$$\alpha_2 := \begin{cases} 2^8 & 2 \mid c \\ 2^6 & 2 \mid y \\ 2^6 & acx \equiv 3 \pmod 4, 2 \mid z, 2 \nmid c \\ 2^5 & acx \equiv 1 \pmod 4, 2 \mid z, 2 \nmid c \\ 2 & 2 \mid x \\ \alpha_2' & 2 \nmid x, 2 \mid a \end{cases}$$

and

$$\alpha_2' := \begin{cases} 2^7 & \mathrm{ord}_2(a) = 1 \\ 2^4 & \mathrm{ord}_2(a) = 2, acx \equiv 4 \pmod{16} \\ 2^2 & \mathrm{ord}_2(a) = 2, acx \equiv 12 \pmod{16} \\ 2^5 & \mathrm{ord}_2(a) = 3 \\ 2^3 & \mathrm{ord}_2(a) = 4, 5 \\ 1 & \mathrm{ord}_2(a) = 6 \\ 2 & \mathrm{ord}_2(a) \geq 7. \end{cases}$$

Ivorra and Kraus [27] proved the following theorem.

Theorem 4.1. *(Ivorra and Kraus) For the Frey curves E_1 and E_2 there are newforms f and g with levels N_1 and N_2 respectively such that*

$$E_1 \sim_p f, \quad E_2 \sim_p g.$$

This theorem actually follows from Ribet's Level-Lowering Theorem 3.7. The hard work is in computing the conductors of E_1 and E_2.

4.3 Eliminating the irrational newforms for $1 \leq D \leq 100$

In this section, we study all the possible irrational newforms that arise from the solutions of the Diophantine equation (4.1) for $1 \leq D \leq 100$. We prove the following theorem.

Theorem 4.2. *Let x, y, z, p satisfy the equation and conditions* (4.1). *Let $1 \leq D \leq 100$ and $p \geq 43$. Let E_1 and E_2 be the Frey curves constructed above applied to this special case. Then the newforms f and g in Theorem 4.1 are both rational.*

Proof. As $a = c = 1$, and $b = -D$, we get

$$E_1 : Y^2 = X^3 + (2z)X^2 + (x^p)X \tag{4.3}$$

$$E_2 : Y^2 = X^3 + (2z)X^2 + (-Dy^{2p})X \tag{4.4}$$

It is clear that the conductors of the Frey curves E_1, E_2 are not divisible by ℓ^2 for any odd prime ℓ. This means that we can choose ℓ in the Proposition 3.9.1 to be any odd prime that does not divide D.

Also, each of the Frey curves E_1 and E_2 has the rational point $(0,0)$ of order 2. Therefore $2 \mid \#E_1(\mathbb{Q})_{\text{tors}}$ and $2 \mid \#E_2(\mathbb{Q})_{\text{tors}}$. This means that we can choose $t = 2$ in Proposition 3.9.1.

Now, suppose that f is an irrational newform of level N_1 or N_2 with coefficients generating a number field K. It is clear that each of the levels N_1 and N_2 has the form $u \cdot 2^\alpha$ where

$$\alpha \in \{0, 1, 2, 3, 4, 5, 6, 7\}$$

and

$$u := \prod_{\substack{\ell \mid D, \\ \ell \text{ odd prime}}} \ell.$$

As $1 \leq D \leq 100$, it would be sufficient to eliminate all of the irrational newforms at the levels in Table 4.1. Let ℓ be an odd prime such that $\ell \nmid D$. Let

$$S_\ell = \left\{ a \in \mathbb{Z} \ : \quad -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell}, \quad a \equiv 0 \pmod 2 \right\}.$$

Let c_ℓ be the ℓ-th coefficient of f and define

$$B'_\ell(f) = \text{Norm}_{K/\mathbb{Q}}((\ell+1)^2 - c_\ell^2) \prod_{a \in S_\ell} \text{Norm}_{K/\mathbb{Q}}(a - c_\ell).$$

By Proposition 3.9.1, the prime p must divide the number

$$\ell \cdot B'_\ell(f)$$

for any odd prime ℓ not dividing D. For each D, consider any collection of primes

$$\{\ell_1, \ell_2, \ell_3, \ldots, \ell_k\} \subset \{a \in \mathbb{Z} \ : \ \ 1 \leq a \leq 100, \, a \text{ is prime}, \, a \nmid D \ \}.$$

Then the prime exponent p must divide the number

$$\gcd\left(\ell_1 \cdot B'_{\ell_1}(f), \ell_2 \cdot B'_{\ell_2}(f), \ell_3 \cdot B'_{\ell_3}(f), \ldots, \ell_k \cdot B'_{\ell_k}(f)\right)$$

Running a `MAGMA` program and choosing a suitable collection of primes $\{\ell_1, \ldots, \ell_k\}$, we can show that p satisfies the conditions of Tables 4.2–4.6. This implies that $p \leq 41$ and so completes the proof. □

Remark. As one of the integers x^p, $D \cdot y^{2p}$, and z^2 in our original equation (4.1) must be even and as the levels of the newforms that arise from the solutions depend on which one of the three is even, this leads us to a subdivision of cases according to which one of the integers $x, D \cdot y, z$ is even. The case x even is easier and we deal with it in the next chapter. The remaining cases are more technical and we deal with them in Chapter 6.

Table 4.1: The list of levels corresponding to $D \in \{1..100\}$

1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20,
21, 22, 23, 24, 26, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 39,
40, 41, 42, 43,44, 46, 47, 48, 51, 52,53, 55,56, 57, 58, 59,
60, 61,62, 64, 65, 66, 67, 68, 69, 70, 71, 73, 74, 76, 77, 78, 79,
80, 82, 83, 84, 85, 86, 87, 88, 89, 91, 92, 93, 94, 95, 96, 97,
102, 104, 106, 110, 112, 114, 116, 118, 120, 122, 124, 128,
130, 132, 134, 136, 138, 140, 142, 146, 148, 152, 154, 156, 158,
160, 164, 166, 168, 170, 172, 174, 176, 178, 182, 184, 186, 188,
190, 192, 194, 204, 208, 212, 220, 224, 228, 232, 236,
240, 244, 248, 260, 264, 268, 272, 276, 280, 284, 292, 296,
304, 308, 312, 316, 320, 328, 332, 336, 340, 344, 348,
352, 356, 364, 368, 372, 376, 380, 384, 388, 408, 416, 424,
440, 448,456, 464, 472, 480, 488, 496, 520, 528, 536, 544,
552, 560, 568, 584, 592, 608, 616, 624, 632, 640, 656, 664,
672, 680, 688, 696, 704, 712, 728, 736, 744, 752, 760, 776,
816, 832, 848, 880, 896, 912, 928, 944, 960, 976, 992,
1040, 1056, 1072, 1088, 1104, 1120, 1136, 1168, 1184, 1216,
1232, 1248, 1264, 1312, 1328, 1344, 1360, 1376, 1392, 1408,
1424, 1456, 1472, 1488, 1504, 1520, 1552, 1632, 1664, 1696,
1760, 1824, 1856, 1888, 1920, 1952, 1984, 2080, 2112, 2144, 2176,
2208, 2240, 2272, 2336, 2368, 2432, 2464, 2496, 2528, 2624, 2656,
2688, 2720, 2752, 2784, 2848, 2912, 2944, 2976, 3008, 3040,
3104, 3264, 3392, 3520, 3648, 3712, 3776, 3904, 3968, 4160, 4224,
4288,4416, 4480, 4544, 4672, 4736, 4928, 4992, 5056, 5248,
5312, 5440, 5504, 5568, 5696,5824, 5952, 6016, 6080, 6208

Table 4.2: The possible prime exponents p for equation (4.1) that correspond to irrational newforms at levels N

N	p	N	p	N	p
1	$\{\}$	2	$\{\}$	3	$\{\}$
4	$\{\}$	5	$\{\}$	6	$\{\}$
7	$\{\}$	8	$\{\}$	10	$\{\}$
11	$\{\}$	12	$\{\}$	13	$\{\}$
14	$\{\}$	15	$\{\}$	16	$\{\}$
17	$\{\}$	19	$\{\}$	20	$\{\}$
21	$\{\}$	22	$\{\}$	23	$\{5, 11\}$
24	$\{\}$	26	$\{\}$	28	$\{\}$
29	$\{7\}$	30	$\{\}$	31	$\{5\}$
32	$\{\}$	33	$\{\}$	34	$\{\}$
35	$\{2\}$	37	$\{\}$	38	$\{\}$
39	$\{2, 7\}$	40	$\{\}$	41	$\{2, 5\}$
42	$\{\}$	43	$\{7\}$	44	$\{\}$
46	$\{\}$	47	$\{3, 7, 23\}$	48	$\{\}$
51	$\{2\}$	52	$\{\}$	53	$\{5, 13\}$
55	$\{2\}$	56	$\{\}$	57	$\{\}$
58	$\{\}$	59	$\{7, 29\}$	60	$\{\}$
61	$\{5\}$	62	$\{2, 3\}$	64	$\{\}$
65	$\{2, 3, 7\}$	66	$\{\}$	67	$\{5, 11\}$
68	$\{2, 3\}$	69	$\{2, 5, 11\}$	70	$\{\}$
71	$\{3, 5, 7\}$	73	$\{3, 5\}$	74	$\{3, 5, 11, 19\}$
76	$\{\}$	77,	$\{2, 5\}$	78	$\{\}$
79	$\{13\}$	80	$\{\}$	82	$\{2, 7\}$
83	$\{5, 41\}$	84	$\{\}$	85	$\{2, 3, 7, 11\}$
86	$\{2, 5, 7, 11\}$	87	$\{2, 5, 7, 11\}$	88	$\{2\}$
89	$\{5, 7, 11\}$	91	$\{2, 7\}$	92	$\{\}$

Table 4.3: The possible prime exponents p for equation (4.1) that correspond to irrational newforms at levels N

N	p	N	p	N	p
93	$\{2,5,7,11\}$	94	$\{2\}$	95	$\{2,3,5\}$
96	$\{\}$	97	$\{2,13\}$	102	$\{\}$
104	$\{2\}$	106	$\{\}$	110	$\{2,3\}$
112	$\{\}$	114	$\{\}$	116	$\{\}$
118	$\{\}$	120	$\{\}$	122	$\{3,31\}$
124	$\{\}$	128	$\{\}$	130	$\{\}$
132	$\{\}$	134	$\{3,5,17\}$	136	$\{2,5\}$
138	$\{2,5,11\}$	140	$\{\}$	142	$\{\}$
146	$\{2,3,5,7,37\}$	148	$\{2\}$	152	$\{2\}$
154	$\{2,5\}$	156	$\{\}$	158	$\{2,3,5\}$
160	$\{2\}$	164	$\{2,3\}$	166	$\{5,7\}$
168	$\{\}$	170	$\{2\}$	172	$\{7\}$
174	$\{\}$	176	$\{2\}$	178	$\{2,5,7\}$
182	$\{\}$	184	$\{2\}$	186	$\{2\}$
188	$\{3,5,11\}$	190	$\{2\}$	192	$\{\}$
194	$\{3,7,19\}$	204	$\{\}$	208	$\{2\}$
212	$\{3,7,11\}$	220	$\{\}$	224	$\{2,5\}$
228	$\{2,3\}$	232	$\{2,5,7\}$	236	$\{3\}$
240	$\{\}$	244	$\{2,3\}$	248	$\{2,3\}$
260	$\{2,3\}$	264	$\{\}$	268	$\{3,5,7\}$
272	$\{2,3,5\}$	276	$\{2,3,5,7\}$	280	$\{2,3\}$
284	$\{3,7,17\}$	292	$\{2,5,11\}$	296	$\{2,5,7\}$
304	$\{2\}$	308	$\{2,3,5\}$	312	$\{\}$
316	$\{3,17\}$	320	$\{2\}$	328	$\{2,3,5,11\}$
332	$\{3,7,13,29\}$	336	$\{\}$	340	$\{2,3,7\}$
344	$\{2,3,5,7\}$	348	$\{\}$	352	$\{2\}$

Table 4.4: The possible prime exponents p for equation (4.1) that correspond to irrational newforms at levels N

N	p	N	p	N	p
356	$\{2,3,11\}$	364	$\{3,5,11\}$	368	$\{2,5,11\}$
372	$\{2,13\}$	376	$\{2,5,11\}$	380	$\{2,3,7\}$
384	$\{\}$	388	$\{2,3,7,13\}$	408	$\{2,3,7\}$
416	$\{2,5\}$	424	$\{2,5,7,11\}$	440	$\{2\}$
448	$\{2,5\}$	456	$\{2,5,13\}$	464	$\{2,5,7\}$
472	$\{2,5,7\}$	480	$\{\}$	488	$\{2,5,7\}$
496	$\{2,3,5\}$	520	$\{2,3,5,7\}$	528	$\{\}$
536	$\{2,3,5,7\}$	544	$\{2,3,5,7\}$	552	$\{2,3,11\}$
560	$\{2,3\}$	568	$\{2,5,7\}$	584	$\{2,5,7,11,19\}$
592	$\{2,3,5,7,11,19\}$	608	$\{2\}$	616	$\{2,7\}$
624	$\{2,7\}$	632	$\{2,5,7,13\}$	640	$\{2,5\}$
656	$\{2,3,5,7,11\}$	664	$\{2,5\}$	672	$\{2,3\}$
680	$\{2,3,5,7,11\}$	688	$\{2,3,5,7,11\}$	696	$\{2,5,23\}$
704	$\{2\}$	712	$\{2,5,7\}$	728	$\{2,3,5,7,11\}$
736	$\{2,3,7\}$	744	$\{2,5,11\}$	752	$\{2,3,5,7,11,23\}$
760	$\{2,3,5,7,11\}$	776	$\{2,3,5,7,17\}$	816	$\{2,3,7\}$
832	$\{2,5\}$	848	$\{2,3,5,7,11,13\}$	880	$\{2,3\}$
896	$\{2,3,11\}$	912	$\{2,3,5,13\}$	928	$\{2,5,7\}$
944	$\{2,3,5,7,29\}$	960	$\{\}$	976	$\{2,3,5,7,31\}$
992	$\{2,3,5,7\}$	1040	$\{2,3,5,7\}$	1056	$\{2,5,7,11\}$
1072	$\{2,3,5,7,11,17\}$	1088	$\{2,3,5,7\}$	1104	$\{2,3,5,7,11\}$
1120	$\{2\}$	1136	$\{2,3,5,7,17\}$	1168	$\{2,3,5,7,11,19,37\}$
1184	$\{2,3,5,7,11\}$	1216	$\{2\}$	1232	$\{2,3,5,7\}$
1248	$\{2,5,11\}$	1264	$\{2,3,5,7,13,17\}$	1312	$\{2,3,5,7,13\}$

Table 4.5: The possible prime exponents p for equation (4.1) that correspond to irrational newforms at levels N

N	p	N	p	N	p
1328	$\{2,3,5,7,13,29,41\}$	1344	$\{2,3\}$	1360	$\{2,3,5,7,11\}$
1376	$\{2,3,5,7,11\}$	1392	$\{2,5,7,11,23\}$	1408	$\{2,3,5,7\}$
1424	$\{2,3,5,7,11\}$	1456	$\{2,3,5,7,11\}$	1472	$\{2,3,5,7,11\}$
1488	$\{2,5,7,11,13\}$	1504	$\{2,3,5,7\}$	1520	$\{2,3,5,7,11\}$
1552	$\{2,3,5,7,13,17,19\}$	1632	$\{2,3,7,11\}$	1664	$\{2,7\}$
1696	$\{2,5,7,17\}$	1760	$\{2,3,5,7\}$	1824	$\{2,3,7,13\}$
1856	$\{2,5,7\}$	1888	$\{2,5,7\}$	1920	$\{2\}$
1952	$\{2,3,5,7,13\}$	1984	$\{2,3,5,7\}$	2080	$\{2,3,5,7,13\}$
2112	$\{2,5,7,11\}$	2144	$\{2,3,5,11,17\}$	2176	$\{2,5\}$
2208	$\{2,3,5,7,11\}$	2240	$\{2,3\}$	2272	$\{2,3,5,7\}$
2336	$\{2,3,5,7,13,17\}$	2368	$\{2,3,5,7,11,19\}$	2432	$\{2,3,5,7,11\}$
2464	$\{2,3,17\}$	2496	$\{2,5,7,11\}$	2528	$\{2,5,11\}$
2624	$\{2,3,5,7,11,13\}$	2656	$\{2,3,5,7\}$	2688	$\{2,5,7,11\}$
2720	$\{2,3,5,7,11,17\}$	2752	$\{2,3,5,7,11\}$	2784	$\{2,3,5,7\}$
2848	$\{2,3,5,7\}$	2912	$\{2,3,5,7,13\}$	2944	$\{2,5,7,13\}$
2976	$\{2,3,5,7,11\}$	3008	$\{2,3,5,7,11,23\}$	3040	$\{2,3,5,7\}$
3104	$\{2,3,5,7,29\}$	3264	$\{2,3,7,11\}$	3392	$\{2,3,5,7,11,13,17\}$
3520	$\{2,3,5,7\}$	3648	$\{2,3,5,7,13\}$	3712	$\{2,3,5,7,13\}$
3776	$\{2,3,5,7,29\}$	3904	$\{2,3,5,7,13,31\}$	3968	$\{2,5,7,13\}$
4160	$\{2,3,5,7,13\}$	4224	$\{2,5,7,13\}$	4288	$\{2,3,5,7,11,17\}$

Table 4.6: The possible prime exponents p for equation (4.1) that correspond to irrational newforms at levels N

N	p	N	p	N	p
4416	$\{2,3,5,7,11\}$	4480	$\{2,3,5,7,11,13\}$	4544	$\{2,3,5,7,17\}$
4672	$\{2,3,5,7,11,13,$ $17,19,37\}$	4736	$\{2,3,5,7,11,13\}$	4928	$\{2,3,5,7,17\}$
4992	$\{2,3,5,7,11\}$	5056	$\{2,3,5,7,11,13,17\}$	5248	$\{2,3,5,7,11\}$
5312	$\{2,3,5,7,13,29,41\}$	5440	$\{2,3,5,7,11,17\}$	5504	$\{2,3,5,7,11,19\}$
5568	$\{2,3,5,7,11,23\}$	5696	$\{2,3,5,7,11\}$	5824	$\{2,3,5,7,11,13\}$
5952	$\{2,3,5,7,11,13\}$	6016	$\{2,3,5,7,11,13\}$	6080	$\{2,3,5,7,11\}$
6208	$\{2,3,5,7,13,\}$ $17,19,29\}$				

Chapter 5

The Diophantine Equation $x^p - Dy^{2p} = z^2$ for x Even

In this chapter we focus on equation (4.1) with x even. In other words we study the Diophantine equation

$$x^p - Dy^{2p} = z^2,\ (x, z) = 1,\ x \text{ even and } p \geq 7 \text{ is prime.} \tag{5.1}$$

As

$$x^p \equiv 0 \pmod 8, \qquad y^{2p} \equiv z^2 \equiv 1 \pmod 8,$$

we get

$$D \equiv 7 \pmod 8.$$

We use the second Frey curve constructed by Ivorra and Kraus given in Section 4.2:

$$E_2^D : Y^2 = X^3 + (2z)X^2 + (-Dy^{2p})X.$$

The conductor of this Frey elliptic curve is

$$N = 2 \prod_{\substack{\ell | Dxy \\ \ell \text{ odd prime}}} \ell.$$

Let

$$N_D := 2 \prod_{\substack{\ell | D \\ \ell \text{ odd prime}}} \ell.$$

Now, by Theorem 4.1, there is a newform f at level N_D such that

$$E_2^D \sim_p f.$$

5.1 Eliminating Irrational Newforms

The newforms at level N_D may be rational newforms or irrational newforms. We know by Theorem 4.2 that for $1 \leq D \leq 100$ and $p \geq 43$, the solutions do not give rise to irrational newforms. In fact we do even better in this special case and eliminate the condition $p \geq 43$ for some values of D.

Lemma 5.1.1. *Let D be an integer belonging to the list*

$$7, 15, 23, 31, 39, 47, 55, 63.$$

Then equation (5.1) *does not have any solutions that give rise to irrational newforms via the Frey curve* E_2^D.

Proof. Running a `MAGMA` program, we obtain the following table for the irrational newforms at the levels N_D.

D	f	
7	None	
15	None	
23	None	
31	$q - q^2 + aq^3 + q^4 + (-2a+2)q^5 + \cdots,$	$a^2 - 2a - 2 = 0$
39	None	
47	$q - q^2 + aq^3 + q^4 + 1/2(-a+4)q^5 + \cdots,$	$a^2 - 8 = 0$
55	$q - q^2 + aq^3 + q^4 + q^5 + \cdots,$	$a^2 + a - 8 = 0$
63	None	

From this table we see that we need only consider $D \in \{31, 47, 55\}$. Suppose f is an irrational newform. By Proposition 3.9.1, if $E_2^D \sim_p f$ then $p \mid B_l(f)$ for any prime ℓ that satisfies the conditions

$$\ell \nmid N_D \quad \text{and} \quad \ell^2 \nmid N.$$

The prime $\ell = 3$ satisfies these conditions for $D \in \{31, 47, 55\}$, and $\ell = 5$ satisfies the conditions for $D \in \{31, 47\}$. As the Frey curve E_2^D has the

rational non-trivial 2-torsion point $(0,0)$, then

$$2 \mid \#E_2^D(\mathbb{Q})_{\text{tors}}.$$

Therefore we can choose $t = 2$ in Proposition 3.9.1. In the notation of that proposition,

$$S_3 := \{-2, 0, 2\}, \quad S_5 := \{-4, -2, 0, 2, 4\}.$$

Now, for $D = 31$, we have

$$B_3(f) = 2^5 \times 3^3 \times 11, \qquad \text{and} \qquad B_5(f) = 2^{18} \times 3^3 \times 5.$$

As p must divide both $B_3(f)$, $B_5(f)$, then $p = 3$ which contradicts our assumption that $p \geq 7$. Thus no solution gives rise to an irrational newform in this case.

For $D = 47$, we have $B_3(f) = 2^{13} \times 3$, which again gives a contradiction.

For $D = 55$, we have $B_3(f) = 2^9 \times 3^3$, which again gives contradiction. This completes the proof. □

5.1.1 Reducing the number of the rational Newforms

Now we need to consider only the rational newforms for D in the list

$$\{7, 15, 23, 31, 39, 47, 55, 63\}.$$

We prove the following lemma.

Lemma 5.1.2. *Let D belong to $\{7, 15, 23, 31, 39, 47, 55, 63\}$. Suppose (x, y, z) is a solution to (5.1) satisfying $p \geq 175$ that gives rise to newform f at level N_D. Then for any prime $\ell \leq 150$, $(\ell, D) = 1$,*

- *we have $\ell \nmid xy$,*
- *the traces satisfy the equality*

$$a_\ell(E_2^D) = a_\ell(f). \tag{5.2}$$

Proof. By Proposition 3.7.2, for any odd prime ℓ we have:

(i) if $\ell \nmid Dxy$ then $a_\ell(E_2^D) \equiv a_\ell(f) \pmod{p}$, and

(ii) if $\ell \nmid D$ and $\ell \mid xy$ then $\ell + 1 \equiv \pm a_\ell(f) \pmod{p}$.

Let ℓ be any odd prime, $\ell \nmid D$, $\ell \mid xy$. As

$$\ell + 1 \pm a_\ell(f) \neq 0,$$

the second congruence entails that

$$p \leq \ell + 1 + |a_\ell(f)|.$$

With Hasse's inequality 3.4, one has

$$|a_\ell(f)| \leq 2\sqrt{\ell}.$$

Therefore the second congruence gives the following bound for the prime p:

$$p \leq \ell + 1 + 2\sqrt{\ell}.$$

Therefore if we choose p sufficiently large (i.e. $p \geq 175$), and the primes ℓ (that we are interested in) satisfy the inequality $3 \leq \ell \leq 150$, we see that the second congruence must be impossible. Hence p must satisfy the first congruence relation:

$$a_\ell(E_2^D) \equiv a_\ell(f) \pmod{p}.$$

If

$$a_\ell(E_2^D) \neq a_\ell(f)$$

then we get

$$p \leq |a_\ell(E_2^D) - a_\ell(f)| \leq |a_\ell(E_2^D)| + |a_\ell(f)|.$$

Again, using the Hasse inequality, we get:

$$p \leq 4\sqrt{\ell}.$$

However this cannot happen for the primes ℓ less than 150 and for primes p greater than 175. This completes the proof. □

Remark. As we will see, the equality (5.2) has at least two advantages over the congruence $a_\ell(E_2^D) \equiv a_\ell(f) \pmod{p}$. On the one hand it helps reduce the number of rational newforms to be considered to at most one. On the

other hand it gives stronger information about the solutions x, y, z, p if they exist.

Suppose (x, y, z) is a solution to (5.1) satisfying $p \geq 175$ that gives rise to rational newform f at level N_D. Let ℓ satisfy

$$\ell \text{ is an odd prime}, \quad \ell \leq 150, \quad \ell \nmid D. \tag{5.3}$$

We define the set $\Omega_\ell(D)$ as:

$$\Omega_\ell(D) := \{(a, b, c) \mid 0 \leq a, b, c \leq \ell - 1,\ ab \neq 0,\ a - Db^2 \equiv c^2 \pmod{\ell}\}.$$

For any $(u, v, w) \in \Omega_\ell(D)$, we let $E_2^D(u, v, w)$ be the elliptic curve over the finite field $\mathbb{F}_\ell$ given by

$$E_2^D(u, v, w): \quad Y^2 = X^3 + (2w)X^2 + (-Dv^2)X.$$

Now, define

$$\Gamma(f, \ell) := \{(a, b, c) \quad | \quad (a, b, c) \in \Omega_\ell(D), \quad a_\ell(E_2^D(a, b, c)) = a_\ell(f)\}.$$

Theorem 5.1. *Let x, y, z satisfy the equation and conditions* (5.1)*, where D belongs to $\{7, 15, 23, 31, 39, 47, 55, 63\}$. Suppose $p \geq 175$. Suppose that the solution (x, y, z) gives rise to a rational newform f at level N_D. Then for*

any prime ℓ satisfying (5.3)*, we have*

$$(x^p,\ y^p,\ z) \equiv (a, b, c) \pmod{l}$$

for some $(a, b, c) \in \Gamma(f, \ell)$*, and subsequently* $\Gamma(f, \ell)$ *is a nonempty set.*

Proof. Suppose (x, y, z) is a solution to (5.1) satisfying $p \geq 175$ that gives rise to a rational newform f at level N_D. Let ℓ satisfy (5.3). By Lemma 5.1.2, $\ell \nmid xy$. Hence there exists $(\alpha_\ell, \beta_\ell, \gamma_\ell) \in \Omega_\ell(D)$ such that

$$x^p \equiv \alpha_\ell \pmod{\ell}, \quad y^p \equiv \beta_\ell \pmod{\ell}, \quad z^2 \equiv \gamma_\ell^2 \pmod{\ell}.$$

Define the elliptic curve

$$E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell): \quad Y^2 = X^3 + (2\gamma_\ell)X^2 + (-D\beta_\ell^2)X.$$

over the finite field $\mathbb{F}_\ell$. We know that modulo ℓ, E_2^D and $E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell)$ are isomorphic. Hence $a_\ell(E_2^D) = a_\ell(E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell))$. Therefore, by Lemma 5.1.2, we get $a_\ell(f) = a_\ell(E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell))$. Hence $(\alpha_\ell, \beta_\ell, \gamma_\ell) \in \Gamma(f, \ell)$. This completes the proof. □

Theorem 5.1 is very useful in eliminating rational newforms that do not correspond to any solution of the Diophantine equation (5.1). For example, we conclude that no solution to the Diophantine equation (5.1) gives rise to a rational newform f at level N_D if there exists an odd prime ℓ satisfying (5.3)

such that $a_\ell(f) \neq a_\ell(E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell))$ for every $(\alpha_\ell, \beta_\ell, \gamma_\ell) \in \Omega_\ell(D)$. Alternatively, a rational newform f at level N_D does not arise from any solution to the Diophantine equation (5.1) if there exists an odd prime ℓ satisfying (5.3), such that $\Gamma(f, \ell)$ is the empty set.

Now let $\Lambda(D)$ be the set of rational newforms f at level N_D such that $\Gamma(f, \ell) \neq \emptyset$ for all ℓ satisfying (5.3). Using a `MAGMA` program we computed $\Lambda(D)$ for each $D \in \{7, 15, 23, 31, 39, 47, 55, 63\}$. We found that $\Lambda(D) = \emptyset$ for $D = 55$, and that it has exactly one element for the other values of D. We obtain the following lemma.

Lemma 5.1.3. *For $D = 55$ there are no x, y, z satisfying equation and conditions (5.1) with $p \geq 175$. Let D belong to $\{7, 15, 23, 31, 39, 47, 63\}$. Suppose (x, y, z) is a solution to (5.1) satisfying $p \geq 175$, giving rise to newform f at level N_D. Let E_D be the elliptic curve associated to the rational newform f if exists. Then E_D is given by the following table:*

D	$\#\Lambda(D)$	E_D
7	*1*	$y^2 + xy + y = x^3 + 4x - 6$
15	*1*	$y^2 + xy + y = x^3 + x + 2$
23	*1*	$y^2 + xy = x^3 - x^2 - 10x - 12$
31	*1*	$y^2 + xy + y = x^3 - x^2 - x + 1$
39	*1*	$y^2 + xy = x^3 + x^2 - 19x + 685$
47	*1*	$y^2 + xy + y = x^3 - x^2 - 1$
55	*0*	*None*
63	*1*	$y^2 + xy + y = x^3 + x^2 - 4x + 5$

5.2 Properties of the Jacobi symbol $\left(\frac{x-y^2}{D_\star}\right)$

We now apply quadratic reciprocity to the study of equation (5.1).

For $D \in \{7, 15, 23, 31, 39, 47, 63\}$, we will find certain conditions for the prime exponent p. We need to define the following number:

$$D_\star := \prod_{\substack{\ell \text{ odd prime,} \\ \ell | (D-1), \\ val_\ell(D-1) \text{ odd,}}} \ell.$$

Lemma 5.2.1. *Let x, y, z satisfy the equation and conditions* (5.1)*. If $(D-1, z) = 1$, then $D_\star$ satisfies*

$$\left(\frac{x-y^2}{D_\star}\right) = \begin{cases} +1 & x \equiv 0, 2 \pmod 8, \\ -1 & x \equiv 4, 6 \pmod 8. \end{cases}$$

Proof. Since $(x - y^2) \mid (x^p - y^{2p})$ we have

$$z^2 \equiv -(D-1)y^{2p} \pmod{x - y^2}.$$

As $(D-1, z) = 1$ and $(z, y) = 1$, then

$$(x - y^2, z) = 1.$$

Thus

$$\left(\frac{z^2}{x-y^2}\right) = \left(\frac{y^{2p}}{x-y^2}\right) = 1,$$

then

$$\left(\frac{-(D-1)}{x-y^2}\right) = 1$$

Hence

$$\left(\frac{-1}{x-y^2}\right)\left(\frac{2}{x-y^2}\right)^{\beta}\left(\frac{D_\star}{x-y^2}\right) = 1,$$

where

$$\beta := val_2(D-1).$$

As observed at the beginning of the chapter, $D \equiv 7 \pmod 8$. Therefore $\beta = 1$. Now we can write

$$D - 1 = 2\lambda^2 D_\star$$

for some odd number $\lambda \in \mathbb{N}$. As

$$\lambda^2 \equiv 1 \pmod 8$$

then

$$6 \equiv 2D_\star \pmod 8.$$

Hence

$$D_\star \equiv 3 \pmod 4.$$

Using the Law of Quadratic Reciprocity, we get

$$\left(\frac{D_\star}{x-y^2}\right) = \left(\frac{x-y^2}{D_\star}\right)\left(\frac{-1}{x-y^2}\right).$$

Combining this with the fact that

$$\left(\frac{2}{x-y^2}\right) = \begin{cases} +1 & x \equiv 0, 2 \pmod 8 \\ -1 & x \equiv 4, 6 \pmod 8 \end{cases}$$

this finishes the proof. □

Lemma 5.2.2. *Let x, y, z satisfy the equation and conditions* (5.1)*. For all D in $\{7, 15, 23, 31, 39, 47, 63\}$, and for any prime p greater than* 175*, we have*

$$(D-1, z) = 1$$

Proof. We need to show that no prime dividing $D-1$ also divides z. We will do this by contradiction, so suppose ℓ divides both z and $D-1$. As z is odd, ℓ is an odd prime. By Lemma 5.1.2, we know that $a_\ell(E_2^D) = a_\ell(f)$. Since there is only one surviving newform given by the table in Lemma 5.1.3, we know $a_\ell(f)$ for any given prime ℓ. We do not know $a_\ell(E_2^D)$ since E_2^D depends on z and y^{2p}, but letting

$$E_u : \qquad Y^2 = X^3 - u^2 X,$$

we know that modulo ℓ, E_2^D and E_u are isomorphic, where $u = y^p$. Now we used a `MAGMA` program to run through the values of u modulo ℓ and found that the equality $a_\ell(E_u) = a_\ell(f)$ is never satisfied for odd prime $\ell \mid (D-1)$. This gives a contradiction. □

Combining Lemmas 5.2.2 and 5.2.1, we get the following result.

Theorem 5.2. *Let x, y, z satisfy the equation and conditions* (5.1)*. For all D in $\{7, 15, 23, 31, 39, 47, 63\}$, and for $p \geq 175$, we have*

$$\left(\frac{x - y^2}{D_\star}\right) = \begin{cases} +1 & x \equiv 0, 2 \pmod 8 \\ -1 & x \equiv 4, 6 \pmod 8 \end{cases}.$$

5.3 Combining the modular approach with quadratic reciprocity

Now, we are going to combine the information coming from Theorems 5.1 (the modular approach) and 5.2 (quadratic reciprocity) to give conditions on the prime exponent p. Clearly, Theorem 5.2 gives information about $x - y^2$ modulo D_*. Theorem 5.1 gives information about $(x)^p - (y^2)^p$ modulo ℓ for any prime ℓ satisfying (5.3).

As we know, by Lemma 5.1.3, for each $D \in \{7, 15, 23, 31, 39, 47, 63\}$, we have at most one rational newform f that can arise from solutions of the equation (5.1). For this particular f, we can compute $\Gamma(f, \ell)$ for any

prime ℓ as discussed before. By Theorem 5.1, we know that $(x^p \pmod{\ell}, y^p \pmod{\ell}, z \pmod{\ell}) \in \Gamma(f, \ell)$ for each ℓ satisfying (5.3).

For any q (not necessarily prime) We define

$$\Gamma_q(f, \ell) := \{(a, b, c) \in \mathbb{F}_\ell^3 \mid (a^q, b^q, c) \in \Gamma(f, \ell)\}.$$

In particular, if (x, y, z) is a solution to equation (5.1), and ℓ satisfies (5.3) then $(x, y, z) \equiv (a, b, c) \pmod{\ell}$ for some $(a, b, c) \in \Gamma_p(f, \ell)$. Clearly $\Gamma_q(f, \ell) = \Gamma_{q'}(f, \ell)$ if $(\ell - 1) \mid (q - q')$, so we can calculate $\Gamma_p(f, \ell)$ from the value of p modulo $\ell - 1$ without knowing p exactly. We also define

$$\Gamma_q(f, D_*) := \{(a, b, c) \in (\mathbb{Z}/D_*\mathbb{Z})^3 \mid (a, b, c) \in \Gamma_q(f, \ell) \text{ for all primes } \ell \mid D_*\}.$$

Clearly $\Gamma_q(f, D_*) = \Gamma_{q'}(f, D_*)$ if $q \equiv q' \pmod{e(D)}$ where

$$e(D) := \operatorname{lcm}\{\ell - 1 \mid \ell \text{ is prime}, \quad \ell \mid D_*\}.$$

Moreover, It is clear that all the prime factors of D_* satisfy (5.3). Let

$$\overline{e(D)} := \{q \mid 0 \leq q \leq e(D) - 1, \ (q, e(D)) = 1\}.$$

We know that if $p \geq 175$ then

- $p \equiv q \pmod{e(D)}$ for some $q \in \overline{e(D)}$, and

- any (x, y, z) satisfying equation and condition (5.1) satisfies $(x, y, z) \equiv (a, b, c) \pmod{D}_*$ for some $(a, b, c) \in \Gamma_q(f, D_*)$.

For any q we can compute $\Gamma_q(f, D_*)$ from the $\Gamma_q(f, \ell)$ using the Chinese Remainder Theorem.

Now consider the sets,

$$A_q(f, D_\star) := \left\{ (a, b, c) \in \Gamma_q(f, D_\star) \quad | \quad \left(\frac{a - b^2}{D_\star}\right) = 1 \right\},$$
$$B_q(f, D_\star) := \left\{ (a, b, c) \in \Gamma_q(f, D_\star) \quad | \quad \left(\frac{a - b^2}{D_\star}\right) = -1 \right\}.$$

From the above discussion and Theorem 5.2 we obtain

Lemma 5.3.1. *Let $D \in \{7, 15, 23, 31, 39, 47, 63\}$ and $q \in \overline{e(D)}$.*

- *Suppose $A_q(f, D_\star) = \emptyset$. Then for all prime $p \geq 175$ satisfying $p \equiv q \pmod{e(D)}$, the equation (5.1) does not have solutions with $x \equiv 0, 2 \pmod 8$.*

- *Suppose $B_q(f, D_\star) = \emptyset$. Then for all prime $p \geq 175$ satisfying $p \equiv q \pmod{e(D)}$, the equation (5.1) does not have solutions with $x \equiv 4, 6 \pmod 8$.*

We wrote a `MAGMA` program to calculate the sets $A_q(f, D_*)$ and $B_q(f, D_*)$ and obtained the following theorem.

Theorem 5.3. *Let x, y, z satisfy the equation and conditions (5.1). For $p \geq 175$, the prime p must satisfy the following congruences*

D	$x \equiv 4, 6 \pmod 8$	$x \equiv 0, 2 \pmod 8$
7	*No Information*	*No Information*
15	$p \equiv 5 \pmod 6$	$p \equiv 1 \pmod 6$
23	$p \equiv 3, 7 \pmod{10}$	$p \equiv 1, 9 \pmod{10}$
31	*No Information*	*No Information*
39	$p \equiv 11, 13, 17 \pmod{18}$	$p \equiv 1, 5, 7 \pmod{18}$
47	$p \equiv 3, 13, 21 \pmod{22}$	$p \equiv 1, 9, 19 \pmod{22}$
55	*No Solution*	*No Solution*
63	$p \equiv 13, 19, 23, 29 \pmod{30}$	$p \equiv 1, 7, 11, 17 \pmod{30}$

Remarks.

- For x even, we proved that

$$(D - 1, z) = 1.$$

This implies that the factor $x - y^2$ of $x^p - y^{2p}$ has no nontrivial common factor with the integer z. However, this is not the case if x is odd. Therefore, for the other case (Dyz even) we need to consider the second factor $\frac{x^p - y^{2p}}{x - y^2}$ of $x^p - y^{2p}$. As we will see in the next chapter, for p sufficiently large, we can prove that

$$\left(\frac{x^p - y^{2p}}{x - y^2}, z(D - 1) \right) = 1,$$

Then we can find similar congruences and conditions for the prime exponent p using the modular approach and the properties of the quadratic reciprocity of the other factor

$$\frac{x^p - y^{2p}}{x - y^2}.$$

- It is also beneficial to consider the integer

$$\frac{x^p + y^{2p}}{x + y^2}.$$

As we will see, in the next chapter, and for p sufficiently large, we will prove that

$$\left(\frac{x^p + y^{2p}}{x + y^2}, z(D+1)\right) = 1,$$

This gives other congruences and conditions for the prime exponent p.

Chapter 6

The Diophantine Equation $x^p - Dy^{2p} = z^2$: The General Case

We continue to study equation (4.1) but drop the condition that x is even. We will need to use both Frey curves given by Ivorra and Kraus.

6.1 Generalisation of Lemma 5.1.2

We generalise Lemma 5.1.2 and prove the following theorem.

Theorem 6.1. *Let (x, y, z) satisfy equation and conditions* (4.1) *with $p \geq 175$. Let E_1 and E_2 be the Frey curves* (4.3) *and* (4.4)*. Let f and g be the*

rational newforms at N_1, N_2 in Theorem 4.1, such that $E_1 \sim_p f$ and $E_2 \sim_p g$. Then for all ℓ satisfying (5.3)*,*

- $\ell \nmid xy$*,*
- *and*

$$a_\ell(E_1) = a_\ell(f), \qquad a_\ell(E_2) = a_\ell(g).$$

Proof. The proof is exactly the same as for Lemma 5.1.2. □

We should notice that Theorem 6.1 is true regardless of which of x, y, z, or D is even. From now on, we consider the Diophantine equation (4.1), for $p \geq 175$.

6.2 Evaluating $\frac{x^p \pm y^{2p}}{x \pm y^2}$ modulo $D_\star$, $D^\star$

As we have seen, for x even integer, and for all $D \in \{7, 15, 23, 31, 39, 47, 63\}$, there are no nontrivial common factors for the integers $x - y^2$ and $D - 1$. However this might not be true for the other cases where $2 \mid Dyz$. For $2 \mid Dyz$, the data that comes from the modular approach does not tell us that $x \pm y^2$ is relatively prime to $D \pm 1$ for the integers $1 \leq D \leq 100$. To apply the properties of the quadratic reciprocity and the modular approach, in this case, it is better to consider the second factor $\frac{x^p - y^{2p}}{x - y^2}$ of $x^p - y^{2p}$. This is because, as we will see, it is always true that $\left(\frac{x^p - y^{2p}}{x - y^2}, D_\star\right) = 1$ for sufficiently large p. This fact would help us evaluate $\left(\frac{\psi_\star}{D_\star}\right)$, where $\psi_\star :=$

$\frac{x^p-y^{2p}}{x-y^2}$. In this chapter, we show how to evaluate the possible values for $\frac{x^p-y^{2p}}{x-y^2} \pmod{D_\star}$. We will see that same result is true for factor $\frac{x^p+y^{2p}}{x+y^2}$ of $x^p + y^{2p}$. Eventually, for the family of Diophantine equations (4.1), we will show how this information can provide a useful means for finding conditions on $p \pmod{n}$, and $p \pmod{m}$ for certain numbers n and m.

Lemma 6.2.1. *For the family of Diophantine equations* (4.1)*, and for* $p \geq D+2$*, we have*

$$\left(\frac{x^p - y^{2p}}{x - y^2}, z(D-1)\right) = 1,$$

and

$$\left(\frac{x^p + y^{2p}}{x + y^2}, z(D+1)\right) = 1.$$

Proof. Let ℓ be any prime factor dividing $\left(\frac{x^p-y^{2p}}{x-y^2}, D-1\right)$. First, suppose $\ell \mid x - y^2$ then

$$\ell \mid \left(\frac{x^p - y^{2p}}{x - y^2}, x - y^2\right) \mid p.$$

This implies that $\ell = p$, which gives a contradiction as $\ell \leq D - 1 < p$.

Secondly, suppose $\ell \nmid x - y^2$. As $x^p \equiv (y^2)^p \pmod{\ell}$, we get $p \mid \ell - 1$ which again gives a contradiction. Thus $\left(\frac{x^p-y^{2p}}{x-y^2}, D-1\right) = 1$. Similarly we can prove $\left(\frac{x^p+y^{2p}}{x+y^2}, D+1\right) = 1$.

It is clear that $\left(\frac{x^p-y^{2p}}{x-y^2}, y\right) = \left(\frac{x^p+y^{2p}}{x+y^2}, y\right) = 1$. As

$$-z^2 \equiv (D-1) \cdot y^{2p} \mod \left(\frac{x^p - y^{2p}}{x - y^2}\right),$$

and

$$-z^2 \equiv (D+1) \cdot y^{2p} \mod \left(\frac{x^p + y^{2p}}{x + y^2} \right),$$

we have $\left(\frac{x^p - y^{2p}}{x - y^2}, z \right) = 1 = \left(\frac{x^p + y^{2p}}{x + y^2}, z \right)$. This finishes the proof. □

For computational purposes, we need to be able calculate $\frac{x^p \pm y^{2p}}{x \pm y^2}$ modulo primes ℓ where ℓ is an odd prime factor for $D \pm 1$. Actually, we need the following desirable lemma.

Lemma 6.2.2. *For any primes p, and ℓ, and for any integer θ and for any natural number T divisible by $\ell \cdot (\ell - 1)$, we have:*

$$\frac{\theta^p - 1}{\theta - 1} \equiv \frac{\theta^\tau - 1}{\theta - 1} \pmod{\ell}$$

where τ is the remainder of dividing p by T

Proof. By the Euclidean Division Algorithm, we can write p as:

$$p = a \cdot T + \tau, \quad 0 \leq \tau \leq T - 1$$

for some integer $a \geq 0$. Then $p = q \cdot \ell(\ell - 1) + \tau$, for some integer $q \geq 0$. First, suppose $\ell \nmid \theta - 1$. As $\theta^{\ell-1} \equiv 1 \pmod{\ell}$, then $\frac{\theta^{\ell-1}-1}{\theta-1} \equiv 0 \pmod{\ell}$. But

$$\frac{\theta^p - 1}{\theta - 1} = \left(\frac{(\theta^{\ell-1})^{q\ell} - 1}{\theta - 1} \right) \cdot \theta^\tau + \frac{\theta^\tau - 1}{\theta - 1},$$

and

$$\frac{(\theta^{\ell-1})^{q\ell} - 1}{\theta - 1} \equiv 0 \mod \left(\frac{\theta^{\ell-1} - 1}{\theta - 1} \right),$$

we get

$$\frac{\theta^p - 1}{\theta - 1} \equiv \frac{\theta^\tau - 1}{\theta - 1} \pmod{\ell}.$$

Secondly, suppose $\ell \mid \theta - 1$. Then

$$\frac{\theta^\ell - 1}{\theta - 1} = \theta^{\ell-1} + \theta^{\ell-2} + \cdots + \theta + 1 \equiv \underbrace{1 + 1 + \cdots + 1}_{\ell \text{ terms}} \equiv \ell \equiv 0 \pmod{\ell}.$$

As

$$\frac{\theta^p - 1}{\theta - 1} = \left(\frac{(\theta^\ell)^{q(\ell-1)} - 1}{\theta - 1}\right) \cdot \theta^\tau + \frac{\theta^\tau - 1}{\theta - 1},$$

and

$$\frac{(\theta^\ell)^{q(\ell-1)} - 1}{\theta - 1} \equiv 0 \mod \left(\frac{\theta^\ell - 1}{\theta - 1}\right),$$

we get

$$\frac{\theta^p - 1}{\theta - 1} \equiv \frac{\theta^\tau - 1}{\theta - 1} \pmod{\ell}.$$

□

6.3 Properties of the integers $\psi_\star$, $D_\star$, $L_\star$

For the solutions of the Diophantine equations (4.1), we define the integers $\psi_\star$ and $D_\star$ as follows

$$\psi_\star := \frac{x^p - y^{2p}}{x - y^2}, \qquad D_\star := \prod_{\substack{\ell \text{ odd prime,} \\ \ell \mid (D-1), \\ val_\ell(D-1) \text{ odd}}} \ell.$$

We define

$$L_\star = \begin{cases} a_\star & \text{if } xy \text{ even,} \\ \operatorname{lcm}\{a_\star, 8\} & \text{if } xy \text{ odd,} \end{cases}$$

where

$$a_\star := \operatorname{lcm}\{\ell(\ell-1) : \ell \text{ is a positive odd prime factor of } D_\star\}.$$

We will show in the next few sections how to find conditions for p modulo $L_\star$. We first combine the previous lemmas to prove the following theorem.

Theorem 6.2. *Let (x, y, z) satisfy the equation and conditions (4.1), with $p \geq 175$ and $1 \leq D \leq 100$. Let τ be the remainder on dividing p by $L_\star$. Then*

$$\tau \in \{w \ : \ 0 \leq w \leq L_\star - 1, \quad (w, L_\star) = 1\}. \tag{6.1}$$

Moreover, for any odd prime $\ell \mid D_\star$, we have

$$\psi_\star \equiv (y^2)^{(\tau-1)} \left(\frac{\mu^\tau - 1}{\mu - 1}\right) \pmod{\ell}, \tag{6.2}$$

where

$$\mu :\equiv x \cdot (y^2)^{-1} \pmod{\ell},$$

Also the integers $\psi_\star$ and $D_\star$ satisfy

$$\left(\frac{\psi_\star}{D_\star}\right) = (-1)^{\frac{(\psi_\star-1)}{2} + \frac{(\psi_\star^2-1)}{8} \cdot \lambda + \frac{(\psi_\star-1)}{2} \cdot \frac{(D_\star-1)}{2}}$$

where $\lambda := val_2(D-1)$.

Proof. Suppose $\ell \mid D_\star$. As $D_\star \mid (D-1)$, we see that $\ell \nmid D$. Moreover, as $1 \leq D \leq 100$, we see that ℓ satisfies (5.3). By Theorem 6.1, $\ell \nmid xy$. Thus μ is well-defined.

The integer τ was defined as the remainder of p divided by $L_\star$. Since $p \geq 175$ and any prime divisor of $L_\star$ is $\leq D \leq 100$, we see that $p \nmid D_\star$. This proves (6.1).

Consider

$$\psi_\star = \left(\frac{x^p - y^{2p}}{x - y^2}\right) = y^{2(p-1)} \left(\frac{(x/y^2)^p - 1}{(x/y^2) - 1}\right) \equiv y^{2(p-1)} \left(\frac{\mu^p - 1}{\mu - 1}\right) \pmod{\ell}.$$

Now $p-1 \equiv \tau-1 \pmod{\ell-1}$, so $(y^2)^{p-1} \equiv (y^2)^{\tau-1} \pmod{\ell}$. By Lemma 6.2.2, with $T = L_\star$, we have

$$\frac{\mu^p - 1}{\mu - 1} \equiv \frac{\mu^\tau - 1}{\mu - 1} \pmod{\ell}.$$

This proves (6.2).

As

$$\psi_\star \equiv x^{p-1} + x^{p-2}(y^2) + x^{p-3}(y^2)^2 + \cdots + x^2(y^2)^{p-3} + x(y^2)^{p-2} + (y^2)^{p-1} \pmod{2},$$

then $\psi_\star$ is odd positive integer if x or y is even. If both of x and y are odd, then

$$\psi_\star \equiv \underbrace{1+1+\cdots+1}_{p \text{ terms}} \pmod 2,$$

which means that $\psi_\star \equiv p \pmod 2$. As p is odd number, this again show that $\psi_\star$ is always odd positive integer.

By Lemma 6.2.1, and as $z^2 \equiv -(D-1)y^{2p} \pmod{\psi_\star}$, we have

$$((D-1)yz, \psi_\star) = 1.$$

Hence

$$\left(\frac{-(D-1)}{\psi_\star}\right) = \left(\frac{-(D-1)y^{2p}}{\psi_\star}\right) = \left(\frac{z^2}{\psi_\star}\right) = 1.$$

Now, write

$$D-1 = 2^\lambda m^2 D_\star, \qquad \lambda := val_2(D-1), \quad m \text{ odd and positive.}$$

Clearly, $(mD_\star, \psi_\star) = 1$. Therefore we get

$$\left(\frac{-1}{\psi_\star}\right)\left(\frac{D_\star}{\psi_\star}\right)\left(\frac{2}{\psi_\star}\right)^\lambda \left(\frac{m}{\psi_\star}\right)^2 = 1.$$

Then

$$\left(\frac{-1}{\psi_\star}\right)\left(\frac{D_\star}{\psi_\star}\right)\left(\frac{2}{\psi_\star}\right)^\lambda = 1. \tag{6.3}$$

Using the Law of Quadratic Reciprocity,

$$\left(\frac{D_\star}{\psi_\star}\right) = \left(\frac{\psi_\star}{D_\star}\right)(-1)^{(\frac{\psi_\star-1}{2})(\frac{D_\star-1}{2})}.$$

With the properties of the Jacobi symbol, we know the following relations

$$\left(\frac{2}{\psi_\star}\right) = (-1)^{(\frac{\psi_\star^2-1}{8})}, \quad \left(\frac{-1}{\psi_\star}\right) = (-1)^{(\frac{\psi_\star-1}{2})}.$$

Combining this with equation (6.3) completes the proof of the theorem. □

6.4 Properties for the integers $\psi^\star$, $D^\star$, $L^\star$

For the Diophantine equations (4.1), we can do the same with the factor $\frac{x^p+y^{2p}}{x+y^2}$ of $x^p + y^{2p}$. For this reason, we also define the integers $\psi^\star$, $D^\star$ and $L^\star$ as follows.

$$\psi^\star := \frac{x^p + y^{2p}}{x + y^2}, \qquad D^\star := \prod_{\substack{\ell \text{ odd prime},\\ \ell|(D+1),\\ val_\ell(D+1) \text{ odd}}} \ell.$$

Similarly, we define

$$L^\star = \begin{cases} a^\star & \text{if } xy \text{ even}, \\ \text{lcm}\{a^\star, 8\} & \text{if } xy \text{ odd}, \end{cases}$$

where

$$a^\star := \mathrm{lcm}\{\ell(\ell-1) \ : \ \ell \text{ is a positive odd prime factor of } D^\star\}.$$

The integers $\psi^\star$, $D^\star$, $L^\star$, enjoy similar properties to those we have discussed for $\psi_\star$, $D_\star$, $L_\star$. Actually, we can similarly prove the following theorem.

Theorem 6.3. *Let (x, y, z) satisfy the equation and conditions (4.1), with $p \geq 175$ and $1 \leq D \leq 100$. Let τ be the remainder on dividing p by $L^\star$. Then*

$$\tau \in \{w \ : \ 0 \leq w \leq L^\star - 1, \quad (w, L^\star) = 1\}. \tag{6.4}$$

Moreover, for any odd prime $\ell \mid D^\star$, we have

$$\psi^\star \equiv (-y^2)^{(\tau-1)} \left(\frac{\nu^\tau - 1}{\nu - 1}\right) \pmod{\ell}, \tag{6.5}$$

where

$$\nu :\equiv x \cdot (-y^2)^{-1} \pmod{\ell},$$

Also the integers $\psi^\star$ and $D^\star$ satisfy

$$\left(\frac{\psi^\star}{D^\star}\right) = (-1)^{\frac{(\psi^\star-1)}{2} + \frac{(\psi^{\star 2}-1)}{8} \cdot \kappa + \frac{(\psi^\star-1)}{2} \cdot \frac{(D^\star-1)}{2}}$$

where $\kappa := val_2(D+1)$.

Remarks.

- Theorems 6.2 and 6.3, combined with the modular approach, give useful means to find conditions on p modulo $L_\star$ and $L^\star$ respectively.

- Clearly, $D_\star \mid L_\star$, and $D^\star \mid L^\star$, and each of the integers $D_\star$, $D^\star$, $\psi_\star$, and $\psi^\star$ is an odd integer.

- If $D_\star = 1$, we define $L_\star = 1$. Also, if $D^\star = 1$, we define $L^\star = 1$. Therefore, we would not get useful information about $p \pmod{L_\star}$ or $p \pmod{L^\star}$ if $D_\star = 1$ or $D^\star = 1$ respectively. If $D_\star = 1$, we should consider $L^\star$, and vice versa we should consider $L_\star$ if $D^\star = 1$. For example, for $D = 31$, we have $D_\star = 15$, and $L_\star = 60$. Then we can find conditions on $p \pmod{60}$. However, $L^\star = 1$, so we do not obtain any congruence conditions on p by considering it. Also, for $D = 37$, we have $D^\star = 19$, and $L^\star = 342$. Then we can find conditions on $p \pmod{342}$. However $L_\star = 1$. It can happen that $L_\star = L^\star = 1$, for example when $D = 99$. As mentioned before, for $D = 1$, the Diophantine equations (4.1) has no solution, and therefore we do not need to define $D_\star$ in this case.

6.5 $\psi_\star \pmod 8$, $\psi^\star \pmod 8$

Theorems 6.2 and Theorem 6.3 provide certain information about the solutions of (4.1). To evaluate $\left(\frac{\psi_\star}{D_\star}\right)$ and $\left(\frac{\psi^\star}{D^\star}\right)$, we need to compute

$$\frac{(\psi_\star - 1)}{2} + \frac{(\psi_\star^2 - 1)}{8} \cdot \lambda + \frac{(\psi_\star - 1)}{2} \cdot \frac{(D_\star - 1)}{2} \pmod 2,$$
$$\frac{(\psi^\star - 1)}{2} + \frac{(\psi^{\star 2} - 1)}{8} \cdot \kappa + \frac{(\psi^\star - 1)}{2} \cdot \frac{(D^\star - 1)}{2} \pmod 2.$$

Therefore, for given D, we need to compute $\psi_\star \pmod 8$, and $\psi^\star \pmod 8$ respectively. This depends on whether xy is even or odd. If xy odd then the values $\psi_\star \pmod 8$, and $\psi^\star \pmod 8$ would depend on $p \pmod 8$ and also on which one of z and D is even. By definition, we know that

$$\psi_\star = x^{p-1} + x^{p-2}(y^2) + x^{p-3}(y^2)^2 + \cdots + x^2(y^2)^{p-3} + x(y^2)^{p-2} + (y^2)^{p-1},$$
$$\psi^\star = x^{p-1} + x^{p-2}(-y^2) + x^{p-3}(-y^2)^2 + \cdots + x^2(-y^2)^{p-3} + x(-y^2)^{p-2} + (-y^2)^{p-1}.$$

Clearly, the values of $\psi_\star \pmod 8$, and $\psi^\star \pmod 8$ depend on whether x, y, z or D even (and also depend on $p \pmod 8$ if xy is odd)). We consider each case separately and give tables for $\psi_\star \pmod 8$, and $\psi^\star \pmod 8$.

- x Even. In this case, y odd, $y^2 \equiv 1 \pmod 8$, and $\psi_\star \equiv x^2 + x + 1 \pmod 8$, $\psi^\star \equiv x^2 - x + 1 \pmod 8$. Then we have the following table

- y Even. In this case, $x \equiv 1 \pmod 8$, and $\psi_\star \equiv 1 + y^2 \pmod 8$, $\psi^\star \equiv 1 - y^2 \pmod 8$. Then we have the following table

Table 6.1: x Even

$x \pmod 8$	0	2	4	6
$\psi_\star \pmod 8$	1	7	5	3
$\psi^\star \pmod 8$	1	3	5	7

Table 6.2: y Even

$y \pmod 4$	0	2
$\psi_\star \pmod 8$	1	5
$\psi^\star \pmod 8$	1	5

- x, y both odd. In this case, $x - D \equiv z^2 \pmod 8$, $y^2 \equiv 1 \pmod 8$, $x^k \equiv 1 \pmod 8$ for k even, $x^k \equiv x \pmod 8$ for k odd, and

$$\psi_\star \equiv \underbrace{(1+x)+(1+x)+\cdots+(1+x)}_{(p-1)/2 \text{ terms}}+1 \pmod 8.$$

  Then $\psi_\star \equiv (\frac{p-1}{2})(1+D+z^2)+1 \pmod 8$. Similarly, $\psi^\star \equiv (\frac{p-1}{2})(1-D-z^2)+1 \pmod 8$. Therefore, we should consider the following three subcases:

- For $z \equiv 0 \pmod 4$ and D odd,

$$\psi_\star \equiv \left(\frac{1+D}{2}\right)(p-1)+1 \pmod 8, \qquad \psi^\star \equiv \left(\frac{1-D}{2}\right)(p-1)+1 \pmod 8.$$

Table 6.3: $z \equiv 0 \pmod 4$

$p \pmod 8$	1	3	5	7
$\psi_\star \pmod 8$	1	$2+D$	$3+2D$	$4+3D$
$\psi^\star \pmod 8$	1	$2-D$	$3-2D$	$4-3D$

- For $z \equiv 2 \pmod 4$, D odd,

$$\psi_\star \equiv \left(\frac{5+D}{2}\right)(p-1)+1 \pmod 8, \qquad \psi^\star \equiv \left(\frac{-3-D}{2}\right)(p-1)+1 \pmod 8.$$

Table 6.4: $z \equiv 2 \pmod 4$

$p \pmod 8$	1	3	5	7
$\psi_\star \pmod 8$	1	$6+D$	$3+2D$	$3D$
$\psi^\star \pmod 8$	1	$6-D$	$3-2D$	$-3D$

- For D even, z odd, then

$$\psi_\star \equiv \left(\frac{2+D}{2}\right)(p-1)+1 \pmod 8, \qquad \psi^\star \equiv \left(\frac{-D}{2}\right)(p-1)+1 \pmod 8.$$

Table 6.5: D even

$p \pmod 8$	1	3	5	7
$\psi_\star \pmod 8$	1	$3+D$	$5+2D$	$7+3D$
$\psi^\star \pmod 8$	1	$1-D$	$1-2D$	$1-3D$

6.6 Conditions on $p \pmod{L_\star}$ and $p \pmod{L^\star}$

Let (x, y, z) satisfy the equation and conditions (4.1) where $p \geq 175$ and $1 \leq D \leq 100$. In this section we explain in detail our computations to obtain congruence conditions for p modulo $L_\star$ and $L^\star$. We need first to fix some notation. Recall that for the Frey curves E_1 and E_2 there are rational newforms f and g with levels N_1 and N_2 respectively such that $E_1 \sim_p f$ and $E_2 \sim_p g$.

It is clear that no solutions exist for the Diophantine equations (4.1) (with the above conditions on p and D) if there are no rational newforms either at level N_1 or level N_2. It is possible that there are rational newforms at these levels that do not correspond to any solution of the Diophantine equations (4.1). We will eliminate some such rational newforms with the help of Theorem 6.4.

Let

$$\Omega_\ell(D) := \{(a,b,c) \mid 0 \leq a,b,c \leq \ell-1,\ ab \neq 0,\ a - D.b^2 \equiv c^2 \pmod{\ell}\}.$$

By Theorem 6.1, $\ell \nmid xy$ for any odd prime ℓ satisfying (5.3). Thus $(x^p, y^p, z) \equiv (a,b,c)$ for some $(a,b,c) \in \Omega_\ell(D)$.

For ℓ satisfying (5.3) and $(u,v,w) \in \Omega_\ell(D)$, we define the elliptic curves $E_1^D(u,v,w)$ and $E_2^D(u,v,w)$ over the finite field $\mathbb{F}_\ell$ by

$$E_1^D(u,v,w)\ :\ Y^2 = X^3 + (2w)X^2 + (u)X,$$
$$E_2^D(u,v,w)\ :\ Y^2 = X^3 + (2w)X^2 + (-Dv^2)X.$$

For $\delta \in \{1,2\}$, h_δ a newform at level N_δ, and ℓ satisfying conditions (5.3), we define

$$\Gamma(h_\delta, \ell) := \{(a,b,c) \quad | \quad (a,b,c) \in \Omega_\ell(D), \quad a_\ell(h_\delta) = a_\ell(E_\delta^D(a,b,c))\}.$$

Remark. We will show that there are rational newforms f at level N_1 and g at level N_2 such that for any ℓ satisfying (5.3), there exists $(a, b, c) \in \Gamma(f, \ell) \cap \Gamma(g, \ell)$ such that $(x^p, y^p, z) \equiv (a, b, c) \pmod{\ell}$.

For $\delta \in \{1, 2\}$, we define $\Lambda_\delta(D)$ to be the set of rational newforms h_δ at level N_δ such that $\Gamma(h_\delta, \ell) \neq \emptyset$ for all ℓ satisfying (5.3).

Theorem 6.4. *Let x, y, z, p satisfy the equation and conditions* (4.1)*, with $p \geq 175$ and $1 \leq D \leq 100$. Then for each $\delta \in \{1, 2\}$ there exist at least one rational newform $h_\delta \in \Lambda_\delta(D)$, such that for any prime ℓ satisfying* (5.3)*, there exists $(a, b, c) \in \Gamma(h_\delta, \ell)$ such that $(x^p, y^p, z) \equiv (a, b, c) \pmod{\ell}$.*

Proof. Suppose (x, y, z) is a solution to (4.1) satisfying $p \geq 175$ and $1 \leq D \leq 100$. Then, by Theorem 6.1, this gives rise to newforms h_δ at level N_δ for $\delta \in \{1, 2\}$. As $p \geq 43$, by Theorem 4.2, the newforms h_δ must be rational. Also, by Theorem 6.1, $a_\ell(E_\delta) = a_\ell(h_\delta)$, for each $\delta \in \{1, 2\}$, where E_1, and E_2 are the Frey curves

$$E_1 \ : \ Y^2 = X^3 + (2z)X^2 + (x^p)X,$$
$$E_2 \ : \ Y^2 = X^3 + (2z)X^2 + (-Dy^{2p})X.$$

By Theorem 6.1, for any prime satisfying (5.3), we have $xy \not\equiv 0 \pmod{\ell}$. Therefore, there exists $(\alpha_\ell, \beta_\ell, \gamma_\ell) \in \Omega_\ell(D)$ such that

$$x^p \equiv \alpha_\ell, \qquad y^p \equiv \beta_\ell, \qquad z \equiv \gamma_\ell \pmod{\ell}.$$

Now, consider the elliptic curves $E_1^D(\alpha_\ell, \beta_\ell, \gamma_\ell)$ and $E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell)$ over the finite field $\mathbb{F}_\ell$ given by

$$E_1^D(\alpha_\ell, \beta_\ell, \gamma_\ell) \ : \quad Y^2 = X^3 + (2\gamma_\ell)X^2 + (\alpha_\ell)X,$$
$$E_2^D(\alpha_\ell, \beta_\ell, \gamma_\ell) \ : \quad Y^2 = X^3 + (2\gamma_\ell)X^2 + (-D\beta_\ell^2)X.$$

We know that modulo ℓ, E_δ and $E_\delta^D(\alpha_\ell, \beta_\ell, \gamma_\ell)$ are isomorphic for $\delta \in \{1, 2\}$. Hence $a_\ell(E_\delta) = a_\ell(E_\delta^D(\alpha_\ell, \beta_\ell, \gamma_\ell))$. Therefore, by Theorem 6.1, we get $a_\ell(h_\delta) = a_\ell(E_\delta^D(\alpha_\ell, \beta_\ell, \gamma_\ell))$. Hence $(\alpha_\ell, \beta_\ell, \gamma_\ell) \in \Gamma(h_\delta, \ell)$ for $\delta \in \{1, 2\}$. Hence $\Gamma(h_\delta, \ell) \neq \emptyset$ for $\delta \in \{1, 2\}$. Then $h_\delta \in \Lambda_\delta(D)$ for $\delta \in \{1, 2\}$. This completes the proof. □

Theorem 6.4 will provide a useful check for our later computations. It is straightforward to calculate $\Lambda_\delta(D)$ using `MAGMA`. Now, for each newform h in $\Lambda_\delta(D)$, we want to compute the list of all possible triples for (x, y, z) modulo $D_\star$ and $D^\star$. For this reason, we need the following notation.

- For $\delta \in \{1, 2\}$, $h_\delta \in \Lambda_\delta(D)$, and primes ℓ satisfying (5.3), define

$$\Gamma_q(h_\delta, \ell) := \{(a, b, c) \in \mathbb{F}_l^3 \quad | \quad (a^q, b^q, c) \in \Gamma(h_\delta, \ell)\}.$$

- For $\delta \in \{1, 2\}$, $h_\delta \in \Lambda_\delta(D)$, and $m \in \{D_\star, D^\star\}$, define

$$\Gamma_q(h_\delta, m) := \{(a, b, c) \in (\mathbb{Z}/m\mathbb{Z})^3 \mid$$
$$((a, b, c) \bmod \ell) \in \Gamma_q(h_\delta, \ell) \text{ for all prime } \ell \mid m\}.$$

- $\overline{L_\star}, \overline{L^\star}$:

$$\overline{L_\star} = \{t \mid 1 \leq t < L_\star,\ (t, L_\star) = 1\}$$

$$\overline{L^\star} = \{t \mid 1 \leq t < L^\star,\ (t, L^\star) = 1\}.$$

Corollary 6.6.1. *Let x, y, z, p satisfy the equation and conditions* (4.1) *with $p \geq 175$ and $1 \leq D \leq 100$. Then for each $\delta \in \{1, 2\}$ there exist at least one rational newform $h_\delta \in \Lambda_\delta(D)$, $e_\star \in \overline{L_\star}$ and $e^\star \in \overline{L^\star}$ such that $p \equiv e_\star \pmod{L_\star}$, and $p \equiv e^\star \pmod{L^\star}$ and*

$$((x, y, z) \mod D_\star) \in \Gamma_{e_\star}(h_\delta, D_\star), \quad ((x, y, z) \mod D^\star) \in \Gamma_{e^\star}(h_\delta, D^\star).$$

Proof. By Theorem 6.4 , $(x^p \pmod{\ell}, y^p \pmod{\ell}, z \pmod{\ell}) \in \Gamma(h_\delta, \ell)$, for each ℓ satisfying (5.3). Let $e_\star \in \overline{L_\star}$ such that $p \equiv e_\star \pmod{L_\star}$. As $(\ell - 1) \mid L_\star$, then $p \equiv e_\star \pmod{\ell - 1}$. Thus

$$(x^p, y^p, z) \equiv (x^{e_\star}, y^{e_\star}, z) \pmod{\ell}.$$

Then $(x^{e_\star} \pmod{\ell}, y^{e_\star} \pmod{\ell}, z \pmod{\ell}) \in \Gamma(h_\delta, \ell)$. This means that $(x \pmod{\ell}, y \pmod{\ell}, z \pmod{\ell}) \in \Gamma_{e_\star}(h_\delta, \ell)$ for every prime $\ell \mid D_\star$. Clearly, $val_\ell(D_\star) = 1$ for any prime $\ell \mid D_\star$. Therefore, $(x \pmod{D_\star}, y \pmod{D_\star}, z \pmod{D_\star}) \in \Gamma_{e_\star}(h_\delta, D_\star)$. Similarly, $(x \pmod{D^\star}, y \pmod{D^\star}, z \pmod{D^\star}) \in \Gamma_{e^\star}(h_\delta, D^\star)$. This completes the proof. □

The modular approach gives us the collection $\Gamma_q(h,m)$ of all possible triples for $(x \pmod m, y \pmod m, z \pmod m)$ where $m \in \{D_\star, D^\star\}$ and q is $p \pmod{L_\star}$ or $p \pmod{L^\star}$. The quadratic reciprocity approach, and Theorems 6.2 and 6.3 provide other useful restrictions for the triples $(x \mod m, y \mod m, z \mod m)$. For this reason we need to refine the set $\Gamma_q(h,m)$ and define the collection $\overline{\Gamma_q(h,m)} \subset \Gamma_q(h,m)$ as follows.

- $S_m^q(a,b,c)$: For $(a,b,c) \in \Gamma_q(h,\ell)$, $m \in \{D_\star, D^\star\}$ we define

$$S_m^q(a,b,c) := \begin{cases} (b^2)^{q-1} \sum_{j=0}^{q-1} (a \cdot (b^2)^{-1})^j \pmod m & if\ m = D_\star, \\ (-b^2)^{q-1} \sum_{j=0}^{q-1} (-a \cdot (b^2)^{-1})^j \pmod m & if\ m = D^\star. \end{cases}$$

- $\chi(D_\star), \chi(D^\star)$: For $m \in \{D_\star, D^\star\}$, define

$$\chi(m) := \begin{cases} (-1)^{\frac{(a-1)}{2} + \frac{(a^2-1)}{8} \cdot \lambda + \frac{(a-1)}{2} \cdot \frac{(D_\star - 1)}{2}} & if\ m = D_\star, \\ (-1)^{\frac{(b-1)}{2} + \frac{(b^2-1)}{8} \cdot \kappa + \frac{(b-1)}{2} \cdot \frac{(D^\star - 1)}{2}} & if\ m = D^\star. \end{cases}$$

  where

$$a := \psi_\star \pmod 8, \quad b := \psi^\star \pmod 8,$$

  and again $\lambda = val_2(D-1)$, and $\kappa = val_2(D+1)$.

- $\overline{\Gamma_q(h,m)}$: For $\delta \in \{1,2\}$, $h \in \overline{\Lambda_\delta(D)}$, $m \in \{D_\star, D^\star\}$, we define

$$\overline{\Gamma_q(h,m)} := \{(a,b,c) | (a,b,c) \in \Gamma_q(h,m),\ \left(\frac{S_m^q(a,b,c)}{m}\right) = \chi(m)\}.$$

Finally, by Theorems 6.2, 6.3, and 6.4 we get the following main result.

Theorem 6.5. *Let x, y, z, p satisfy the equation and conditions* (4.1) *with $p \geq 175$ and $1 \leq D \leq 100$. Let $\delta \in \{1, 2\}$, $h_\delta \in \Lambda_\delta(D)$, $e_\star \in \overline{L_\star}$ and $e^\star \in \overline{L^\star}$. If $\overline{\Gamma_{e_\star}(h, D_\star)} = \emptyset$, then $p \not\equiv e_\star \pmod{L_\star}$. Similarly, if $\overline{\Gamma_{e^\star}(h, D^\star)} = \emptyset$, then $p \not\equiv e^\star \pmod{L^\star}$.*

6.7 Computations of $\Lambda_\delta(D)$, $\overline{\Gamma_{e_\star}(h, D_\star)}$, $\overline{\Gamma_{e^\star}(h, D^\star)}$

With the help of the computer package `MAGMA`, and for the equation and conditions (4.1), $p \geq 175$, we explain in this section how to compute $\Lambda_\delta(D)$, $\overline{\Gamma_{e_\star}(h_\delta, D_\star)}$, and $\overline{\Gamma_{e^\star}(h_\delta, D^\star)}$. The main steps are as follows:

(i) Choose D in the set {1,2, ...,100}.

(ii) We associate the Frey curves E_1, E_2 to putative solutions of the equation and conditions (4.1).

(iii) We then compute the levels N_1 and N_2, and list the primes ℓ satisfying (5.3).

(iv) With the help of the computer package `MAGMA`, we compute the set of rational newforms at the levels N_1 and N_2.

(v) We compute $\Omega_\ell(D)$ for ℓ satisfying (5.3).

(vi) For ℓ satisfying (5.3), $(u, v, w) \in \Omega_\ell(D)$, consider the elliptic curves $E_1^D(u, v, w) : Y^2 = X^3 + (2w)X^2 + (u)X$, $E_2^D(u, v, w) : Y^2 = X^3 + (2w)X^2 + (-Dv^2)X$ over $\mathbb{F}_\ell$.

(vii) The computer package `MAGMA` can compute the traces $a_\ell(E_1^D(u, v, w))$ and $a_\ell(E_2^D(u, v, w))$ and also any particular coefficient for the newforms. Therefore, we can compute $\Gamma(h_\delta, \ell)$ for each rational newform h_δ at level N_δ. Therefore, for $\delta \in \{1, 2\}$, we can now determine all the rational newforms h at level N_δ that make $\Gamma(h, \ell) = \emptyset$. Remove such newforms we obtain $\Lambda_\delta(D)$ for $\delta \in \{1, 2\}$.

(viii) If $\Lambda_\delta(D) = \emptyset$ for some $\delta \in \{1, 2\}$, then, by Theorem 6.4, there is no solution for the equation and conditions (4.1), for $p \geq 175$.

(ix) If $\Lambda_\delta(D) \neq \emptyset$ for both $\delta = 1$, 2, then we can compute $\Gamma_q(h_\delta, \ell)$ for each $h_\delta \in \Lambda_\delta(D)$, and prime ℓ satisfying (5.3).

(x) Using the Chinese Remainder Theorem, we can compute $\Gamma_q(h_\delta, m)$ for $\delta \in \{1, 2\}$, $h_\delta \in \Lambda_\delta(D)$ and $m \in \{D_\star, D^\star\}$, and for any natural number q.

(xi) Compute $L_\star$, $L^\star$, $\overline{L_\star}$, $\overline{L^\star}$.

(xii) Compute the sum $S_m^q(a, b, c)$ for $(a, b, c) \in \Gamma_q(h, \ell)$, $m \in \{D_\star, D^\star\}$ and for $q \in \overline{L_\star}, \overline{L^\star}$.

(xiii) Compute $\lambda = val_2(D - 1)$, and $\kappa = val_2(D + 1)$, $a := \psi_\star \pmod 8$, and $b := \psi^\star \pmod 8$.

(xiv) Compute $\chi(D_\star)$, $\chi(D^\star)$.

(xv) Write a `MAGMA` program to compute $\overline{\Gamma_u(h, D_\star)}$, and $\overline{\Gamma_v(h, D^\star)}$ for each $h_\delta \in \overline{\Lambda_\delta(D)}$, $\delta \in \{1, 2\}$ and u, v are any given numbers. Running this `MAGMA` program over $u \in \overline{L_\star}$ and $v \in \overline{L^\star}$, we can know which values for e_1,e_2 that make $\overline{\Gamma_{e_1}(h, D_\star)} = \emptyset$, and $\overline{\Gamma_{e_2}(h, D^\star)} = \emptyset$. By Theorem 6.5, for those values of e_1, e_2 we obtain the conditions on $p \not\equiv e_1 \pmod{L_\star}$ and $p \not\equiv e_2 \pmod{L^\star}$ respectively.

Remark. For many values for $D \in \{1, 2, \ldots, 100\}$, we will see that the number of newforms in $\Lambda_\delta(D)$ equals one at most.

6.8 Results for y even and D odd

In this section we study the Diophantine equation

$$x^p - Dy^{2p} = z^2, \qquad (x, z) = 1, \quad p \geq 175, \quad y \text{ even}, \tag{6.6}$$

where

$$1 \leq D \leq 100 \qquad \text{and} \qquad D \text{ is odd}.$$

As an example, we will explain how we find necessary conditions on $p \pmod{L_\star}$ if there is solution for the equation(6.6). We take $\delta = 1$ as $N_1 < N_2$. Now, we associate the Frey curve

$$E_1 : Y^2 = X^3 + (2z)X^2 + (x^p)X.$$

The conductor of this elliptic curve is

$$N = 2 \prod_{\substack{\ell | Dxy \\ \ell \text{ odd prime}}} \ell.$$

Let

$$N_D := 2 \prod_{\substack{\ell | D \\ \ell \text{ odd prime}}} \ell.$$

Theorem 6.6. *Let x, y, z p satisfy the equation and conditions* (6.6)*, where D is odd and $1 \leq D \leq 100$. Suppose (x, y, z) gives rise to newform f belonging to $\Lambda_1(D)$. Let E_D be the elliptic curve associated to the rational newform f if it exists. Then $\#\Lambda_1(D)$ and E_D are as in Tables 6.6 and 6.7. Therefore, no solution exists for*

$$D \in \{1, 3, 5, 9, 11, 13, 17, 19, 25, 27, 29, 37, 41, 43, 49, 53, 55, 59, 61, 67, 73, 81, 83, 85, 89, 93, 95, 97\}.$$

Moreover, $\Lambda_1(D)$ contains only one rational newform f_D for each

$$D \in \{7, 15, 21, 23, 31, 33, 35, 39, 45, 47, 51, 57, 63, 65, 69, 71, 75, 77, 79, 87, 91, 99\}. \quad (6.7)$$

Now, we are going to investigate the possible conditions on $p \pmod{L_\star}$. By Theorem 6.6, for D satisfying (6.7), there is only one rational newform

f_D in $\Lambda_1(D)$. Consider the elliptic curve E_D that is associated to the rational newform f_D. We exclude the values $\{33, 51, 65, 99\}$ of D as $D_\star = 1$ in these cases. We need to evaluate

$$\chi(D_\star) := (-1)^{\frac{(a-1)}{2}+\frac{(a^2-1)}{8}\lambda+\frac{(a-1)}{2}\frac{(D_\star-1)}{2}},$$

where $\lambda := val_2(D-1)$. As y even, it is clear that

$$\psi_\star \equiv \begin{cases} 1 \pmod 8 & \text{if } y \equiv 0 \pmod 4, \\ 5 \pmod 8 & \text{if } y \equiv 2 \pmod 4. \end{cases}$$

As $a := \psi_\star \pmod 8$, then $a \equiv 1 \pmod 4$. Then

$$(-1)^{\frac{(a-1)}{2}+\frac{(a-1)}{2}\cdot\frac{(D_\star-1)}{2}} = 1.$$

Hence

$$\chi(D_\star) = \begin{cases} 1 & \text{if } y \equiv 0 \pmod 4, \\ (-1)^\lambda & \text{if } y \equiv 2 \pmod 4. \end{cases}$$

As the value of $\chi(D_\star)$ depends on $y \pmod 4$, we need to find the conditions on $p \pmod{L_\star}$ in each case. By computing $\overline{\Gamma_u(h, D_\star)}$ for each $u \in \overline{L_\star}$ and appropriate newforms h, we obtain the following theorem.

Theorem 6.7. *The prime p must satisfy the congruences in Tables 6.8–6.10.*

6.8.1 Two Examples for conditions on $p \pmod{L^\star}$

We can do the same work with $\psi^\star$ to find conditions upon $p \pmod{L^\star}$. In this case we need to exclude the values $\{7, 15, 63, 71, 99\}$ where $D^\star = 1$. Therefore, by Theorem 6.6 we should consider the numbers D in the set $\{21, 23, 33, 39, 45, 47, 51, 57, 65, 69, 75, 77, 79, 87, 91\}$. Running a `MAGMA` program using Theorem 6.3, we get the following result:

Theorem 6.8. *For $D \in \{21, 23\}$, the prime p must satisfy the congruences in Table 6.11.*

6.9 Results for z Even

In this section we study the special case

$$x^p - Dy^{2p} = z^2, \qquad (x, z) = 1, \quad p \text{ prime} \geq 175, \quad z \text{ even} \tag{6.8}$$

where $1 \leq D \leq 100$.

First, we associate to any solution the Frey curve

$$E_1 : Y^2 = X^3 + (2z)X^2 + (x^p)X.$$

The conductor of this elliptic curve is

$$N = 2^\alpha \prod_{\substack{\ell | Dxy \\ \ell \text{ odd prime}}} \ell,$$

where

$$\alpha = \begin{cases} 2^6 & D \equiv 1 \pmod 4 \\ 2^5 & D \equiv 3 \pmod 4 \end{cases}$$

Let

$$N_D := 2^\alpha \prod_{\substack{\ell \mid D \\ \ell \text{ odd prime}}} \ell.$$

Theorem 6.9. *Let x, y, z, p satisfy the equation and conditions* (6.8) *with*

$$D \in \{7, 11, 13, 15, 21, 23, 25, 27, 29, 31, 35, 39, 41, 43, 45, 47, 49, 53, 55,$$
$$57, 59, 61, 63, 67, 69, 71, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97\}.$$

Suppose (x, y, z) gives rise to rational newform f at level N_D and let E_D be the elliptic curve associated to the rational newform f. Then $\#\Lambda_1(D)$ and the set $\Lambda_1(D)$ satisfy Tables 6.12–6.16. Therefore, from these tables, we have no solutions for (6.8) *for all D in the list*

$$\{11, 13, 23, 29, 31, 41, 43, 47, 53, 59, 61, 67, 71, 79, 83, 89, 95\}.$$

6.9.1 Conditions on $p \pmod{L_\star}$

Now, we are going to investigate the possible conditions on $p \pmod{L_\star}$. For computational purposes, we need to evaluate $\chi(D_\star)$. Clearly, $\psi_\star \pmod 8$ can be computed using the following formulas.

- If $z \equiv 0 \pmod 4$ then

$$\psi_\star \pmod 8 \equiv \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8, \\ 2+D & \text{if } p \equiv 3 \pmod 8, \\ 3+2D & \text{if } p \equiv 5 \pmod 8, \\ 4+3D & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

- If $z \equiv 2 \pmod 4$ then

$$\psi_\star \pmod 8 \equiv \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8, \\ 6+D & \text{if } p \equiv 3 \pmod 8, \\ 3+2D & \text{if } p \equiv 5 \pmod 8, \\ 3D & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

As xy is odd, $L_\star = \operatorname{lcm}\{a_\star, 8\}$ where

$$a_\star := \operatorname{lcm}\{\ell(\ell-1) \ : \ \ell \text{ is a positive odd prime factor of } D_\star\}.$$

As the value of $\chi(D_\star)$ depends on $z \pmod 4$, we need to examine the conditions on $p \pmod{L_\star}$ for each case. Consider the set

$$\overline{L_\star} := \{t \mid t \in \{1, 2, \ldots, L_\star - 1\}, \ (t, L\star) = 1\}.$$

Now, for each D, running a `MAGMA` program over the values $e \in \overline{L_\star}$ and over the rational newforms $h \in \overline{\Lambda_1(D)}$, we obtain the following theorem that determines the values of e that makes $\overline{\Gamma_e(h, D_\star)} = \emptyset$. By Theorem 6.5, for those values of e we have $p \not\equiv e \pmod{L_\star}$.

Theorem 6.10. *The prime p must satisfy the congruences in Tables 6.17–6.20 (some of these depend on the newform that solution arises from).*

Table 6.6: Reducing the number of newforms f to one or zero for y even

D	$\#\Lambda_D$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
1	0	None
3	0	None
5	0	None
7	1	$y^2 + xy + y = x^3 + 4x - 6$
9	0	None
11	0	None
13	0	None
15	1	$y^2 + xy + y = x^3 + x + 2$
17	0	None
19	0	None
21	1	$y^2 + xy + y = x^3 + x^2 - 4x + 5$
23	1	$y^2 + xy = x^3 - x^2 - 10x - 12$
25	0	None
27	0	None
29	0	None
31	1	$y^2 + xy + y = x^3 - x^2 - x + 1$
33	1	$y^2 + xy + y = x^3 + x^2 - 2x - 1$
35	1	$y^2 + xy + y = x^3 - x^2 + 2x - 3$
37	0	None
39	1	$y^2 + xy = x^3 + x^2 - 19x + 685$
41	0	None
43	0	None
45	1	$y^2 + xy + y = x^3 + x + 2$
47	1	$y^2 + xy + y = x^3 - x^2 - 1$
49	0	None
51	1	$y^2 + xy = x^3 - 34x + 68$
53	0	None
55	0	None
57	1	$y^2 + xy + y = x^3 + x^2 - 352x - 2431$
59	0	None
61	0	None
63	1	$y^2 + xy + y = x^3 + x^2 - 4x + 5$

Table 6.7: Reducing the number of newforms f to one or zero for y even

D	$\#\Lambda_D$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
65	1	$y^2 + xy + y = x^3 - x^2 - 7x - 1$
67	0	None
69	1	$y^2 + xy + y = x^3 + x^2 + 3x + 3$
71	1	$y^2 + xy = x^3 - x^2 - x - 3$
73	0	None
75	1	$y^2 + xy + y = x^3 + x + 2$
77	1	$y^2 + xy + y = x^3 - x^2 - 4x - 89$
79	1	$y^2 + xy + y = x^3 + x^2 + x + 1$
81	0	None
83	0	None
85	0	None
87	1	$y^2 + xy + y = x^3 - 2$
89	0	None
91	1	$y^2 + xy + y = x^3 - x^2 + 866x + 6445$
93	0	None
95	0	None
97	0	None
99	1	$y^2 + xy + y = x^3 + x^2 - 2x - 1$

Table 6.8: Congruences for Theorem 6.7

D	$y \pmod 4$	$p \pmod{L_\star}$
7	0	$p \equiv \pm 1 \pmod 6$
	2	No solution
15	0	$p \not\equiv 5, 11, 17, 23, 29, 41 \pmod{42}$
	2	$p \not\equiv 1, 13, 19, 25, 31, 37 \pmod{42}$
21	0	$p \not\equiv 3, 7 \pmod{20}$
	2	$p \not\equiv 3, 7 \pmod{20}$
23	0	$p \not\equiv 3, 7, 13, 17, 23, 27, 37, 43, 47, 53, 57, 63, 67, 73, 83, 87, 93, 97, 103, 107 \pmod{110}$
	2	$p \not\equiv 1, 9, 19, 21, 29, 31, 39, 41, 49, 51, 59, 61, 69, 71, 79, 81, 89, 91, 101, 109 \pmod{110}$
31	0	$p \not\equiv 7, 29, 41, 43 \pmod{60}$
	2	$p \not\equiv 1, 23, 47, 49 \pmod{60}$
35	0	$p \not\equiv 3, 99, 131, 147, 163, 211, 227, 243 \pmod{272}$
	2	$p \not\equiv 1, 33, 49, 81, 145, 161, 225, 257 \pmod{272}$

Table 6.9: Congruences for Theorem 6.7

D	$y \pmod 4$	$p \pmod{L_\star}$
39	0	$p \not\equiv 11, 13, 17, 29, 31, 35, 47, 49, 53, 65, 67, 71, 83, 85, 89, 101, 103, 107, 119, 121, 125, 137, 139, 143, 155, 157, 161, 173, 175, 179, 191, 193, 197, 211, 215, 227, 229, 233, 245, 251, 263, 265, 269, 281, 283, 287, 299, 301, 305, 317, 319, 335, 337, 341 \pmod{342}$
	2	$p \not\equiv 1, 5, 7, 23, 25, 37, 41, 43, 55, 59, 61, 73, 77, 79, 91, 97, 109, 113, 115, 127, 131, 145, 149, 151, 163, 167, 169, 181, 185, 187, 199, 203, 205, 217, 221, 223, 235, 239, 241, 253, 257, 259, 271, 275, 277, 289, 293, 295, 307, 311, 313, 325, 329, 331 \pmod{342}$
45	0	$p \not\equiv 7, 17, 19, 29, 39, 57, 79, 87, 107, 109 \pmod{110}$
	2	$p \not\equiv 7, 17, 19, 29, 39, 57, 79, 87, 107, 109 \pmod{101}$
57	0	$p \not\equiv 5, 13, 17, 19, 31, 41 \pmod{42}$
	2	$p \not\equiv 1, 11, 23, 25, 29, 37 \pmod{42}$

Table 6.10: Congruences for Theorem 6.7

D	$y \pmod 4$	$p \pmod{L_\star}$
63	0	$p \not\equiv 13, 23, 29, 43, 53, 73, 79, 83, 89, 119, 139, 179, 199, 203,$ $209, 223, 229, 239, 259, 263, 269, 313, 323, 353, 383, 389,$ $409, 433, 449, 463, 499, 509, 523, 533, 539, 553, 569, 613,$ $619, 623, 643, 649, 673, 703, 709, 719, 739, 743, 773, 799,$ $809, 823, 829, 833, 859, 863, 883, 889, 923, 929 \pmod{930}$
	2	$p \not\equiv 1, 7, 41, 47, 67, 71, 97, 101, 107, 121, 131, 157, 187, 191,$ $211, 221, 227, 257, 281, 287, 307, 311, 317, 361, 377, 391,$ $397, 407, 421, 431, 481, 497, 521, 541, 467, 547, 577, 607,$ $617, 661, 667, 671, 691, 701, 707, 721, 727, 731, 751, 791,$ $811, 841, 847, 851, 857, 877, 887, 901, 907, 917 \pmod{930}$

Table 6.11: Congruences for Theorem 6.8

D	$y \pmod 4$	$p \pmod{L^\star}$
21	0	$p \equiv 1, 7, 9, 17, 19, 21, 27, 29, 31, 37, 39, 41, 47, 49, 51, 57, 59,$ $61, 6769, 71, 79, 81, 87, 89, 91, 97, 101, 107, 109 \pmod{110}$
	2	$p \equiv 3, 7, 9, 13, 17, 19, 23, 27, 29, 37, 39, 43, 47, 49, 53, 57, 59,$ $63, 67, 69, 73, 79, 83, 87, 89, 93, 97, 103, 107, 109 \pmod{110}$
23	0	$p \equiv 1 \pmod 6$
	2	$p \equiv 5 \pmod 6$

Table 6.12: Reducing the number of newforms f for z even

D	$\#\Lambda_1(D)$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
7	2	$y^2 = x^3 + x^2 + 2x$
		$y^2 = x^3 - x^2 + 2x$
11	0	NONE
13	0	NONE
15	8	$y^2 = x^3 - x^2 - 6x$
		$y^2 = x^3 - x^2 - 10x - 8$
		$y^2 = x^3 + x^2 - 6x$
		$y^2 = x^3 + x^2 - 226x - 1360$
		$y^2 = x^3 - x^2 - 226x + 1360$
		$y^2 = x^3 - x^2 - 30x + 72$
		$y^2 = x^3 + x^2 - 10x + 8$
		$y^2 = x^3 + x^2 - 30x - 72$
21	12	$y^2 = x^3 - x^2 + 63x - 63$
		$y^2 = x^3 - x^2 - 29x - 51$
		$y^2 = x^3 + x^2 - 257x + 3423$
		$y^2 = x^3 + x^2 - 29x + 387$
		$y^2 = x^3 - x^2 - 12x + 18$
		$y^2 = x^3 - x^2 - 29x - 387$
		$y^2 = x^3 - x^2 - 257x - 3423$
		$y^2 = x^3 - x^2 - 84x - 270$
		$y^2 = x^3 + x^2 - 84x + 270$
		$y^2 = x^3 + x^2 + 63x + 63$
		$y^2 = x^3 + x^2 - 12x - 18$
		$y^2 = x^3 + x^2 - 29x + 51$
23	0	NONE

Table 6.13: Reducing the number of newforms f to one or zero for z even

D	$\#\Lambda_1(D)$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
25	6	$y^2 = x^3 - 8x + 8$
		$y^2 = x^3 - x^2 - 5x + 5$
		$y^2 = x^3 - x^2 + 2$
		$y^2 = x^3 + x^2 - 2$
		$y^2 = x^3 - 8x - 8$
		$y^2 = x^3 + x^2 - 5x - 5$
27	2	$y^2 = x^3 + x^2 - 2x$
		$y^2 = x^3 - x^2 - 2x$
29	0	NONE
31	0	NONE
35	4	$y^2 = x^3 - 13x + 12$
		$y^2 = x^3 - 13x - 12$
		$y^2 = x^3 - 817x + 8976$
		$y^2 = x^3 - 817x - 8976$
39	2	$y^2 = x^3 + x^2 - 234x + 1296$
		$y^2 = x^3 - x^2 - 234x - 1296$
41	0	NONE
43	0	NONE

Table 6.14: Reducing the number of newforms f to one or zero for z even

D	$\#\Lambda_1(D)$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
45	16	$y^2 = x^3 - x^2 + 4x + 6$
		$y^2 = x^3 - x^2 - 61x + 205$
		$y^2 = x^3 - x^2 + 15x - 15$
		$y^2 = x^3 - x^2 - 900x - 10098$
		$y^2 = x^3 - x^2 + 95x + 1057$
		$y^2 = x^3 + x^2 + 4x - 6$
		$y^2 = x^3 + x^2 - x + 95$
		$y^2 = x^3 + x^2 - 900x + 10098$
		$y^2 = x^3 - x^2 - x - 95$
		$y^2 = x^3 - x^2 + 4x - 30$
		$y^2 = x^3 - x^2 - 20x + 42$
		$y^2 = x^3 + x^2 - 61x - 205$
		$y^2 = x^3 + x^2 + 4x + 30$
		$y^2 = x^3 + x^2 - 20x - 42$
		$y^2 = x^3 + x^2 + 95x - 1057$
		$y^2 = x^3 + x^2 + 15x + 15$
47	0	NONE
49	2	$y^2 = x^3 + 4x + 16$
		$y^2 = x^3 + 4x - 16$
53	0	NONE
55	2	$y^2 = x^3 - 37x + 84$
		$y^2 = x^3 - 37x - 84$

Table 6.15: Reducing the number of newforms f to one or zero for z even

D	$\#\Lambda_1(D)$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
57	8	$y^2 = x^3 - x^2 - 97x - 287$
		$y^2 = x^3 - x^2 - 52x + 70$
		$y^2 = x^3 - x^2 - 689x - 6735$
		$y^2 = x^3 + x^2 - 52x - 70$
		$y^2 = x^3 + x^2 - 22529x - 1176993$
		$y^2 = x^3 - x^2 - 22529x + 1176993$
		$y^2 = x^3 + x^2 - 97x + 287$
		$y^2 = x^3 + x^2 - 689x + 6735$
59	0	NONE
61	0	NONE
63	4	$y^2 = x^3 - x^2 - 22x + 40$
		$y^2 = x^3 - x^2 - 14x + 24$
		$y^2 = x^3 + x^2 - 14x - 24$
		$y^2 = x^3 + x^2 - 22x - 40$
67	0	NONE
69	6	$y^2 = x^3 - x^2 - 17x + 273$
		$y^2 = x^3 + x^2 + 191x + 1055$
		$y^2 = x^3 + x^2 - 829x - 9469$
		$y^2 = x^3 - x^2 - 829x + 9469$
		$y^2 = x^3 - x^2 + 191x - 1055$
		$y^2 = x^3 + x^2 - 17x - 273$
71	0	NONE

Table 6.16: Reducing the number of newforms f to one or zero for z even

D	$\#\Lambda_1(D)$	The elliptic curves E_D associated to the rational newforms in $\Lambda_1(D)$
75	8	$y^2 = x^3 - x^2 - 6x$
		$y^2 = x^3 - x^2 - 10x - 8$
		$y^2 = x^3 + x^2 - 6x$
		$y^2 = x^3 + x^2 - 226x - 1360$
		$y^2 = x^3 - x^2 - 226x + 1360$
		$y^2 = x^3 - x^2 - 30x + 72$
		$y^2 = x^3 + x^2 - 10x + 8$
		$y^2 = x^3 + x^2 - 30x - 72$
77	4	$y^2 = x^3 - 236x - 45904$
		$y^2 = x^3 - 104x - 408$
		$y^2 = x^3 - 104x + 408$
		$y^2 = x^3 - 236x + 45904$
79	0	NONE
81	4	$y^2 = x^3 - x^2 - 4x - 2$
		$y^2 = x^3 + x^2 + 3x + 3$
		$y^2 = x^3 + x^2 - 4x + 2$
		$y^2 = x^3 - x^2 + 3x - 3o$
83	0	NONE
85	2	$y^2 = x^3 - 572x + 5264$
		$y^2 = x^3 - 572x - 5264$
87	2	$y^2 = x^3 - x^2 - 262x - 1520$
		$y^2 = x^3 + x^2 - 262x + 1520$
89	0	NONE
91	2	$y^2 = x^3 - 61x - 180$
		$y^2 = x^3 - 61x + 180$
93	2	$y^2 = x^3 - x^2 - 1117x - 14003$
		$y^2 = x^3 + x^2 - 1117x + 14003$
95	0	NONE

Table 6.17: Congruences for Theorem 6.10

D= 7	
$z \pmod 4$	$p \pmod{L_\star}$
0	No information
2	No solution
D=15	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 5, 13, 17, 19, 31, 41, 47, 55, 59, 61, 73, 83, 89, 97, 101, 103, 115, 125, 131, 139, 143, 145, 157, 167 \pmod{168}$
2	$p \not\equiv 1, 11, 23, 25, 29, 37, 43, 53, 65, 67, 71, 79, 85, 95, 107, 109, 113, 121, 127, 137, 149, 151, 155, 163 \pmod{168}$
D= 21	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 1, 9, 21, 29 \pmod{40}$
2	$p \not\equiv 1, 9, 21, 29 \pmod{40}$

Table 6.18: Congruences for Theorem 6.10

D= 25	
$y^2 = x^3 - 8x + 8$ $y^2 = x^3 - 8x - 8$	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 5, 11, 17, 23 \pmod{24}$
2	$p \not\equiv 1, 7, 13, 19 \pmod{24}$
$y^2 = x^3 - x^2 - 5x + 5$ $y^2 = x^3 + x^2 - 5x - 5$ $y^2 = x^3 + x^2 - 2$ $y^2 = x^3 - x^2 + 2$	
$z \pmod 4$	$p \pmod{L_\star}$
0	No information
2	No solution
D= 27	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 1, 7, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 97, 103, 109, 115, 121,$ $127, 133, 139, 145, 151, 157, 163, 175, 181, 187, 193, 199, 205, 211, 217,$ $223, 229, 235, 241, 253, 259, 265, 271, 277, 283, 289, 295, 301, 307 \pmod{312}$
2	No information

Table 6.19: Congruences for Theorem 6.10

D= 35	
$y^2 = x^3 - 13x + 12$ $y^2 = x^3 - 13x - 12$	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 1, 3, 19, 33, 35, 49, 65, 67, 81, 83, 97, 99, 113, 115, 129, 131, 145, 147, 161,$ $163, 177, 179, 193, 195, 209, 211, 225, 227, 241, 243, 257, 259 \pmod{272}$
2	No information
$y^2 = x^3 - 817x + 8976$ $y^2 = x^3 - 817x - 8976$	
$z \pmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 1, 33, 49, 81, 145, 161, 225, 257 \pmod{272}$
2	$p \not\equiv 3, 99, 131, 147, 163, 211, 227, 243 \pmod{272}$

Table 6.20: Congruences for Theorem 6.10

D= 39	
$z \bmod 4$	$p \pmod{L_\star}$
0	$p \not\equiv 11, 13, 17, 29, 31, 35, 47, 49, 53, 65, 67, 71, 83, 85, 89, 101, 103, 107, 119, 121, 125,$ $137, 139, 143, 155, 157, 161, 173, 175, 179, 191, 193, 197, 211, 215, 227, 229, 233, 245,$ $251, 263, 265, 269, 281, 283, 287, 299, 301, 305, 317, 319, 335, 337, 341, 353, 355, 359,$ $371, 373, 377, 389, 391, 395, 407, 409, 413, 425, 427, 431, 443, 445, 449, 461, 463, 467,$ $479, 481, 485, 497, 499, 503, 515, 517, 521, 533, 535, 539, 553, 557, 569, 571, 575, 587,$ $593, 605, 607, 611, 623, 625, 629, 641, 643, 647, 659, 661, 677, 679, 683, 695, 697, 701,$ $713, 715, 719, 731, 733, 737, 749, 751, 755, 767, 769, 773, 785, 787, 791, 803, 805, 809,$ $821, 823, 827, 839, 841, 845, 857, 859, 863, 875, 877, 881, 895, 899, 911, 913, 917, 929,$ $935, 947, 949, 953, 965, 967, 971, 983, 985, 989, 1001, 1003, 1019, 1021, 1025, 1037,$ $1039, 1043, 1055, 1057, 1061, 1073, 1075, 1079, 1091, 1093, 1097, 1109, 1111, 1115,$ $1127, 1129, 1133, 1145, 1147, 1151, 1163, 1165, 1169, 1181, 1183, 1187, 1199, 1201,$ $1205, 1217, 1219, 1223, 1237, 1241, 1253, 1255, 1259, 1271, 1277, 1289, 1291, 1295,$ $1307, 1309, 1313, 1325, 1327, 1331, 1343, 1345, 1361, 1363, 1367 \pmod{1368}$
2	$p \not\equiv 1, 5, 7, 23, 25, 37, 41, 43, 55, 59, 61, 73, 77, 79, 91, 97, 109, 113, 115, 127, 131, 145,$ $149, 151, 163, 167, 169, 181, 185, 187, 199, 203, 205, 217, 221, 223, 235, 239, 241, 253,$ $257, 259, 271, 275, 277, 289, 293, 295, 307, 311, 313, 325, 329, 331, 343, 347, 349, 365,$ $367, 379, 383, 385, 397, 401, 403, 415, 419, 421, 433, 439, 451, 455, 457, 469, 473, 487,$ $491, 493, 505, 509, 511, 523, 527, 529, 541, 545, 547, 559, 563, 565, 577, 581, 583, 595,$ $599, 601, 613, 617, 619, 631, 635, 637, 649, 653, 655, 667, 671, 673, 685, 689, 691, 707,$ $709, 721, 725, 727, 739, 743, 745, 757, 761, 763, 775, 781, 793, 797, 799, 811, 815, 829,$ $833, 835, 847, 851, 853, 865, 869, 871, 883, 887, 889, 901, 905, 907, 919, 923, 925, 937,$ $941, 943, 955, 959, 961, 973, 977, 979, 991, 995, 997, 1009, 1013, 1015, 1027, 1031, 1033,$ $1049, 1051, 1063, 1067, 1069, 1081, 1085, 1087, 1099, 1103, 1105, 1117, 1123, 1135,$ $1139, 1141, 1153, 1157, 1171, 1175, 1177, 1189, 1193, 1195, 1207, 1211, 1213, 1225,$ $1229, 1231, 1243, 1247, 1249, 1261, 1265, 1267, 1279, 1283, 1285, 1297, 1301, 1303,$ $1315, 1319, 1321, 1333, 1337, 1339, 1351, 1355, 1357 \pmod{1368}$

Bibliography

[1] A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 2^k = y^n$. *II.* Arab J. Math. and Sci. 7 (2001), no. 2, 67–71.

[2] A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 2^k = y^n$, Internat. J. Math. and Math. Sci. **20** no. 2, (1997), 299–304.

[3] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[4] M. A. Bennett, *Recipes for ternary Diophantine equations of signature* (p, p, k), Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55

[5] F. Beukers, *The Diophantine equations* $Ax^p + By^q = Cz^r$, Duke Math. J. **91** (1998), 61–88.

[6] F. Beukers, *The generalized Fermat equation* Preprint, Lectures held at Institut Henri Poincare, September 2004.

[7] Yu. Bilu , G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers* (English summary) J. Reine Angew. Math. 539 (2001) , 75–122.

[8] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[9] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14 No.4** (2001), 843–939.

[10] Y. Bugeaud, *On the Diophantine equation* $x^2 - 2^m = \pm y^n$, Proc. Amer. Math. Soc. **125** (1997), 3203–3208.

[11] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, Journal of Algebra **322** (2009), 638–656.

[12] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, **239**. Springer, New York, 2007.

[13] H. Cohen, *Number Theory. Vol. II. Analytic and Modern Tools* . Graduate Texts in Mathematics, **240**, Springer, New York, 2007.

[14] J.H.E. Cohn, *The Diophantine equation* $x^2 + 2^k = y^n$, Arch. Math. **59** (1992), 341–344.

[15] J.H.E. Cohn, *The Diophantine equation* $x^2 + 2^k = y^n$, II. Internat. J. Math. and Math. Sci. **22** no. 3, (1999), 459–462.

[16] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[17] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[18] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[19] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem* Duke Math. J. **102** (2000), 413–449.

[20] H. Darmon, and A. Granville, *On the equations* $x^p + y^q = z^r$ *and* $z^m = f(x, y)$, Bulletin London Math. Society No 129, **27** part 6, November 1995, 513–544.

[21] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), no. 1, 137–166.

[22] G. Frey, *Links between stable elliptic curves and certain Diophantine equations* Ann. Univ. Sarav. Ser. Math. (1) **1**, (1986).

[23] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$ J. Reine Angew. Math. **571** (2004), 213–236.

[24] E. Halberstadt and A. Kraus, J. Reine Angew. Math. **548** (2002), 167–234.

[25] Y. Guo, M. LE, *A note on the exponential Diophantine equation* $x^2 - 2^m = y^n$, Proc. Amer. Math. Soc. **123** (1995), 3627–3629.

[26] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$, Acta Arith. **108** (2003), 327–338.

[27] W. Ivorra and A. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canadian Journal of Mathematics **58** (2006), no. 1, 115–153.

[28] Y. Hellegouarch, *Sur l'équation diophantienne* $x_1^{p^h} + x_2^{p^h} = cx_3^{p^h}$, C. R. Acad. Sci. Paris Ser. A. B **274** (1972), A1385–A1387.

[29] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.

[30] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.

[31] A. Kraus, *On the Equation* $x^p + y^q = z^r$*: A Survey*, The Ramanujan Journal **3** (1999), 315–333.

[32] M. H. Le, Arch. Math. (Basel) **78** (2002), no. 1, 26–35.

[33] J. S. Milne, *Elliptic Curves*, Kea Books, 2006.

[34] B. Poonen, E. Schaefer and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158.

[35] K. Ribet, *On the equation* $a^p + 2b^p + c^p = 0$, Acta Arith. **LXXIX.1** (1997), 7–15.

[36] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[37] S. Siksek, *On the Diophantine equation* $x^2 = y^p + 2^k z^p$, Journal de Théorie des Nombres de Bordeaux **15** (2003), 839–846.

[38] S. Siksek, *The modular approach to Diophantine equations*, lecture notes available from
`http://www.math.leidenuniv.nl/ evertse/siksek-modular.pdf`

[39] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, GTM 106, 1985.

[40] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 151, 1994.

[41] W. A. Stein, *Modular Forms: A Computational Approach*, American Mathematical Society, Graduate Studies in Mathematics 79, 2007.

[42] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[43] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.