On Arithmetic Progressions and Perfect Powers

Samuel Luke Edis

Submitted for the degree of Doctor of Philosophy.

School of Mathematics and Statistics

August 2019

Supervisor: Frazer Jarvis

University of Sheffield

Firstly, I want to thank my parents, without their support over the past 27 years I would not be where I am, and I certainly would not have been able to study for a Ph.D. Next I would like to thank my brother Ben, without his sense of humour I'm not sure I could have kept my sanity during this process.

In the mathematical community I would first like to thank Frazer Jarvis. Without Frazer none of the ideas in this thesis would have been possible, additionally it would be in an almost unreadable state. Further I would like to thank Samir Siksek, as he suggested I look at the problem of Erdős-Selfridge curves. Throughout my thesis, Siksek's papers have been a great inspiration. Additionally I would like to thank Michael Bennett, for pointing out an error in one of my papers and suggesting a method to fix it.

Of my friends, all of whom have been important, James Kilbane has been the most important. Without James I would still be writing in LyX and indenting all of my paragraphs. Finally, I would like to thank Chen Wang, for being able to distract me from Maths, when it was all getting a bit too much.

Abstract

In this thesis we will consider the problems that occur at the intersection of arithmetic progressions and perfect powers. In particular we will study the Erdős-Selfridge curves, $By^\ell = x(x+d)\dots(x+(k-1)d)$, and sums of powers of arithmetic progressions, in particular $y^\ell = (x-d)^3+x^3+(x+d)^3$.

We shall study these curves using aspects of algebraic and analytic number theory. To all the equations studied we shall show that a putative solution gives rise to solutions of (potentially many) Fermat equations. In the case of Erdős-Selfridge curves we will use the modular method to understand the prime divisors of d for large ℓ. Then we shall attach Dirichlet characters to such solutions, which allows us to use analytic methods regarding bounds on the value of sums of characters. These bounds will allow us to show that there can't be too many simultaneous solutions to the Fermat equations we described. This leads to a contradiction for large k, as the number of Fermat equations generated will grow faster than the possible number of simultaneous solutions.

We study the arithmetic progression curves by attaching Fermat equations of signature $(\ell, \ell, 2)$. We then use the classical modular method to attach Frey-Hellegouarch curves and level lowered modular forms. It is possible to show that the Frey-Hellegouarch curves that associate to modular forms in a non-trivial cuspidal newspace are all quadratic twists of each other. It is then possible to compute if there are modular forms of the right level that could associate to such a twist of an elliptic curve.

Contents

List of Tables

Chapter 1

Introduction

§ 1.1 Introduction to the Thesis

Number theory is one of the oldest areas of mathematical research, with core ideas in number theory dating back over two millennia to the time of the Greek mathematicians. The original aim was to find integral solutions to given equations, including examples such as Pell's equations.

1.1.1. *For M a positive non-square integer, do there exist integers x and y such that*

$$x^2 - My^2 = 1?$$

In fact this equation is known to have been studied, in the $M = 2$ case, as far back as 400BC in India and Greece [27]. They were interested in the solutions because of the connection between solutions and rational approximations to $\sqrt{2}$. The first general method for solving this equation for any M was found in the 12th century by Bhāskara II. Since then the questions asked, and the methods developed, in number theory have grown increasingly complex.

Number theory is now split into at least two distinct but overlapping branches, that of algebraic number theory and analytic number theory, each with their own methods and sets of problems. A more modern view on number theory is that it aims to understand the properties of numbers more generally. While integral solutions to equations might have been the starting point for algebraic number theory, it now encapsulates a much greater area of study with algebraic solutions of points on algebraic varieties just being one of many areas. Similarly, analytic number theory mostly arose as a way to study

distributions of primes using analytic methods, but has developed into a very large body of work. In this thesis we will be using a combination of both areas to understand points on curves.

We start the thesis with a chapter on analytic number theory. This will cover only three topics, that of primes, arithmetic progressions and Dirichlet characters. In the section concerning primes we will mostly be interested in what is known about primes in given intervals, more specifically the generalizations of Bertrand's Postulate.

Postulate 1.1.2. *For $n > 1$ there exists a prime in the interval $[n, 2n)$.*

Additionally, we will also briefly touch upon the Prime Number Theorem and some bounds for series involving functions of primes. This will be required in sections regarding the Erdős-Selfridge curves, as we will need to understand the distribution of primes arising in the arithmetic progressions. Next we shall discuss arithmetic progressions in general, from an analytic standpoint. We will be interested in the Chebyshev function. This function is useful as it allows us to study the distribution of primes in a given congruence class in intervals. Roth's theorem will also be stated here, as it will be needed in Chapter 5 (for a sieving argument in Theorem 5.4.1). Finally we will talk about Dirichlet characters, define them in the usual manner and give the method of attaching an L-function, as is classically given in the literature. We will then state some theorems about sums of characters, in particular an estimate for the sum of characters multiplied with the Von Mangoldt function, and additionally a bound of the sum of the product of characters. These theorems will be crucial in Chapter 5, as they will allow us to bound the number of potential solutions to a given Erdős-Selfridge curve.

In Chapter 3 we will give a very brief introduction to the theory of elliptic curves, modular forms and Galois representations. This chapter will be aimed purely at the developments of algebraic number theory in its applications to Fermat equations. We shall discuss Fermat equations separately a little later in the introduction, as they are so important in this thesis. We will start by defining a Frey-Hellegouarch curve and then turn our attention to what is known regarding modular forms attached to such curves. This includes modularity, Ribet's Level Lowering Theorem and bounds on the modulus of level lowered forms coming from Kraus's Theorem. We additionally will look at the method of studying Fermat equations of signature $(\ell, \ell, 2)$ as developed by Bennett and Skinner [8], and Ivorra and Kraus [26]. We will need these in Chapter 6 as these are exactly the Fermat equations that we will attach to the equations we study in that chapter.

It is quite often the case in number theory that easy to understand problems have fiendishly difficult solutions that are non-obvious and require traversing through what look to be unrelated abstract areas. However by utilising the relations between these different areas, which are of great importance to number theory, it is possible to transform the question from an obvious to state, difficult to answer question, to one which is normally harder to state but easier to answer. We will see some examples of this further in this introduction.

§ 1.2 Congruent Numbers

We begin by asking the following question.

1.2.1. *Does there exist a method that will calculate in finite time if a given positive integer n is the area of a right angled triangle with rational side lengths?*

This question was first discussed by the Greek mathematicians, however they were only interested in its relation to special cases of n. It was the Arab scholars of the tenth century that started systematically studying this problem. Almost no progress was made on the problem, apart from giving examples of some n for which it is known to be congruent. The next main breakthrough came from Fermat, who showed using a descent method that 1 is not a congruent number. This is equivalent to the fact that there are no nontrivial integer solutions to $X^4 + Y^4 = Z^2$. In the 16th century, Euler [28, pg. 2] showed that $n = 7$ is a congruent number.

This motivates the following definition,

Definition 1.2.2. A non-zero rational number n is called *congruent* if it is the area of a right angled triangle with rational side lengths.

After the work of Euler there was very little progress on the congruent number problem, until in 1983 Tunnell proved the following theorem [58].

Theorem 1.2.3. *If n is a square-free and odd (respectively, even) positive integer and n is the area of a right triangle with rational sides, then*

$$2|\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 32z^2\}| = |\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 8z^2\}|$$

respectively,

$$2|\{x, y, z \in \mathbb{Z} \mid \tfrac{n}{2} = 2x^2 + y^2 + 32z^2\}| = |\{x, y, z \in \mathbb{Z} \mid \tfrac{n}{2} = 2x^2 + y^2 + 8z^2\}|.$$

If the weak Birch-Swinnerton-Dyer conjecture is true for the elliptic curves

$$E_n : y^2 = x^3 - n^2 x,$$

then conversely, these equalities imply that n is a congruent number.

This is a great example of where modern number theory can be used to solve ancient problems. The maths that Tunnell used was new at the time and could not have been replicated using more classical techniques. We will give a brief explanation of Tunnell's method. For each n it is possible to attach an elliptic curve

$$E_n : y^2 = x^3 - n^2 x.$$

This curve has the property that n is a congruent number if and only if E_n has infinitely many rational points on it. Using a theorem of Coates and Wiles on elliptic curves with complex multiplication [13], it is possible to see that if n is congruent, then the critical value of the L-function attached to E_n is zero. Now applying modularity of ellitpic curves with complex multiplication, it is possible to change the problem from that of elliptic curves to one of modular forms. Using work of Shimura on half integral modular forms and the Shimura lift [50], [51], Tunnell showed that the L-function of E_n could be calculated from the coefficients of a ternary theta form. In fact, the difference of the two terms in the equalities given in Theorem 1.2.3 are the coefficients of the theta forms, hence up to scaling are the critical L values. The above theorem now follows.

During the production of this thesis the author considered the problem of congruent numbers over real quadratic number fields with trivial narrow class number. In [17] a congruence field is defined, and it is shown that there is a finite time method to determine congruent numbers in a congruence field (assuming the Birch-Swinnerton-Dyer conjecture for that field). It is worth noting that it is not shown that a non-congruence field does not have a finite time method to determine congruent numbers, e.g. $\mathbb{Q}$ is not a congruence field. Additionally it is shown that there is a finite time method for determining if a real quadratic number fields with trivial narrow class number is a congruence field, in particular $\mathbb{Q}(\sqrt{2})$ is a congruence field, and if so how to determine the method. This work follows Tunnell's closely and replicates his arguments as closely as possible. However, as this work requires a detailed explanation of Hilbert modular forms and quaternionic modular forms, it has not been included here as it is too different from the rest of the work presented.

§ 1.3 Fermat Equations

Fermat's Last Theorem is another problem that is easy to state but difficult to answer. In the 17th century Fermat wrote that he had a proof of the following fact:

Theorem 1.3.1. *For a, b and c positive integers and $n \geq 3$ there are no solutions to*

$$a^n + b^n = c^n.$$

This is clearly a very easy to understand problem, however the solution took several hundred years. In fact many famous mathematicians, and amateurs, have attempted solutions to this problem over the years, and in doing so have created new areas of maths. For example, Kummer's development of the ideal class group grew from his proof of Fermat's last theorem for odd regular primes.

The statement in its entirety is now known to be correct, and was contributed to by a lot of mathematicians, but most importantly Andrew Wiles in [59], for showing the modularity of rational semi-stable elliptic curves. Wiles's Theorem has now been extended to all elliptic curves over many papers by many mathematicians, this is now known as the Modularity Theorem.

Theorem 1.3.2. *If E is a rational elliptic curve, then there is a cuspidal newform with the same Galois representation.*

The outline of the solution to Fermat's Last Theorem goes as follows; assume that there is a co-prime triple of integers (a, b, c) such that $a^n + b^n = c^n$ for $n > 2$. Then we consider the elliptic curve

$$E : y^2 = x(x - a^n)(x + b^n).$$

This elliptic curve has discriminant $\Delta = 16(abc)^{2n}$. However, once modularity of E was shown in [59], then by using Ribet's Level Lowering Theorem it would follow that there is a newform of level 2 and weight 2, which was known not to exist. So, it follows that a proof of modularity demonstrated the non-existence of a solution to Fermat's equation. It is this argument that motivated Wiles to pursue a proof of modularity.

Since then, many more equations in a similar style have been studied and called Fermat equations. It is standard in the literature to call an equation of the form

$$AX^p + BY^q + CZ^r = 0,$$

a *Fermat equation of signature* (p, q, r).

The literature on these equations is now both deep and wide, and it is impossible to explain all the methods that people have used to treat such equations in a constantly evolving field. However, almost all attempts at solving these equations using the modular method will start by attaching a Frey-Hellegouarch curve. That is to say, to the equation

$$u + v + w = 0 \text{ and } uvw \neq 0,$$

for u, v and w coprime we consider the elliptic curve

$$E : y^2 = x(x - u)(x + v).$$

Currently equations of the signature $(\ell, \ell, 2)$ and $(\ell, \ell, 3)$ are quite well understood for coefficients divisible only by small primes. For example in [55], Siksek studies the equation

$$x^2 = y^\ell + 2^k z^\ell, \tag{1.1}$$

where the following theorem is proven:

Theorem 1.3.3. *Suppose $k \geq 2$ and $\ell \geq 7$ is a prime. Then the only non-trivial primitive solutions of equation* (1.1) *are $k = 3$, $x = \pm 3$, $y = z = 1$ and ℓ arbitrary.*

As the theory around Fermat equations has developed, they too have become almost a method in themselves. It is increasingly common to try to find a way to attach Fermat equations to a Diophantine equation, with the hope that the theory surrounding those Fermat equations will be easier to study than the original equation. For example this is seen in [11], where the authors use the work regarding Fermat equations of signature $(\ell, \ell, 2)$ in their proofs of the following two theorems.

Theorem 1.3.4. *Let F_n be the n-th term in the Fibonacci sequence. The only perfect powers in the sequence are $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_6 = 8$ and $F_{12} = 144$.*

Theorem 1.3.5. *Let L_n be the n-th term in the Lucas sequence. The only perfect powers in the sequence are $L_1 = 1$ and $L_3 = 4$.*

This idea of passing from the original equation to a Fermat equation attached to the original equation has also been developed in the literature regarding Erdős-Selfridge curves, which form the main topic of this thesis.

§ 1.4 Erdős-Selfridge Curves

Perfect powers and arithmetic progressions are two main areas of study in number theory. For example, the Fermat equations we just discussed are part of the study on perfect powers. While it is clear that problems concerning perfect powers can be very difficult to answer, problems concerning arithmetic progressions can be just as hard. However it is not impossible to derive results about problems concerning both of them.

In 1975 Erdős and Selfridge [20] showed that the product of two or more consecutive positive integers cannot be a perfect power. Algebraically this is the following theorem:

Theorem 1.4.1. *For x, y, k and ℓ positive integers with k and $\ell \geq 2$, then there is no solution to the equation*

$$\prod_{i=0}^{i=k-1} (x+i) = y^{\ell}. \tag{1.2}$$

This was proved using ideas in combinatorics and graph theory, which we shall not see in this thesis.

The question of rational solutions to this problem is a lot harder however. For any fixed pair of integers (k, ℓ) such that $\ell + k > 6$ with k and $\ell > 2$, then it follows that the equation given by (1.2) is a super-elliptic curve. Hence by Faltings's theorem there are only finitely many rational points on the curve. However, showing that there are only finitely many points on the family of curves for all pairs of (k, ℓ) with $k + \ell > 6$ is an even harder problem.

These curves admit the obvious rational solutions with $y = 0$, and there are known families of rational solutions for some small values of k.

$$(x, y, k, \ell) = \left(\frac{a^2}{b^2 - a^2}, \frac{ab}{b^2 - a^2}, 2, 2 \right), \quad a \neq \pm b \tag{1.3}$$

and

$$(x, y, k, \ell) = \left(\frac{1-2j}{2}, \frac{\pm 1}{2^j} \prod_{i=1}^{j} (2i-1), 2j, 2 \right), \tag{1.4}$$

for a, b and j integers with j positive. There are two more known rational solutions,

$$\left(\frac{-4}{3}, \frac{2}{3}, 3, 3 \right) \text{ and } \left(\frac{-2}{3}, \frac{-2}{3}, 3, 3 \right). \tag{1.5}$$

Sander [47] proposed that these are the only rational solutions in the following conjecture, with corrections made in [2].

Conjecture 1.4.2. *If $k \geq 2$ and $\ell \geq 2$ are integers, then the only rational points on the curve given by* (1.2) *are the solutions given in 1.3, 1.4, 1.5 or by $y = 0$.*

This conjecture is known to be true for small values of k, in particular for $k \leq 34$. The conjecture for $k \leq 4$ was proven by Sander in [47] and the case of $k = 5$ was dealt with in [34]. In [2] Bennett, Bruin, Győry and Hajdu extended this result to $k \leq 11$, and Győry, Hajdu and Pintér [24] then further extended it to $k \leq 34$.

The first case of a result in this conjecture for a general k, is that of bounding the size of the exponent ℓ, for a prime ℓ.

Theorem 1.4.3. *Let $k \geq 2$ be a positive integer. Then the equation*

$$x(x+1)\dots(x+k-1) = y^{\ell} \tag{1.6}$$

has at most finitely many solutions in rational numbers x and y and integers $\ell \geq 2$, with $(k, \ell) \neq (2, 2)$ and $y \neq 0$. If additionally ℓ is prime, then all solutions satisfy $\log(\ell) < 3^k$.

This result was proven by Bennett and Siksek in 2015 [7]. The main idea in this paper is to create Fermat equations by creating identities out of combinations of the factors on the left hand side. The size of the prime factors in the coefficients of these Fermat equations can be controlled and even shown to be bounded in terms of k. Using modularity it is then possible to bound the exponent ℓ as we can bound the level lowered conductor of the elliptic curve attached to our Fermat equation.

As well as the original Erdős-Selfridge curve, it is possible to write down many variants that are equally as interesting. It is these variants that will make up the bulk of this thesis.

In 2016 Das, Laishram and Saradha considered the following situation.

For $1 \leq i \leq k$ let

$$\Delta_i = (x+1)\dots(x+i-1)(x+i+1)\dots(x+k).$$

Let p be the smallest prime greater than or equal to $k/2$.

Theorem 1.4.4. *If there is a rational solution* (x, y) *to*

$$y^\ell = \Delta_i,$$

with $2 \leq i \leq k - p$ *or* $p < i < k$, $\ell > 2$ *a prime,* y *non zero then* $\log(\ell) \leq 3^k$.

Further, they study the above curves for small values of k. For values of k less than 26 it is possible to find more identities on products of two terms without losing control over the primes in the coefficients. In particular they show the following result.

Theorem 1.4.5. *If there is a rational solution* (x, y) *to*

$$y^\ell = \Delta_i,$$

$3 \leq k \leq 26$, $\ell > 2$ *a prime and* y *non zero, then it follows that* $\log(\ell) \leq 3^k$.

These are Theorem 1.1 and Corollary 1.5 in [14].

A further generalization of this problem is to consider the equation

$$\prod_{i \in [0,k-1] \setminus S} (x + i) = y^\ell, \tag{1.7}$$

for S a subset of $[0, k-1]$, x, y, k and ℓ integers and y non-zero.

We will prove the following results in Chapter 4.

Theorem 1.4.6. *For* $k \geq 27$ *and* S *a subset of* $[1, k]$ *that satisfies one of the following conditions*

(1) $S \subset [s, t] \subset [1, k]$ *and* $t - s < \frac{k}{18} - 1$*;*

(2) $|S| < \frac{3}{2} + 0.37\sqrt{\frac{k}{\log k}}$.

Then any non-trivial rational solution to equation (1.7) *satisfies* $\log(\ell) < 3^k$.

This is the first original work of the author, published in 2019 [18].

Corollary 1.4.7. *For* $k \geq 3$ *and* S *a set with a single element, then any rational solution to equation* (1.7) *satisfies* $\log(\ell) < 3^k$.

This removes the hypothesis on p in Theorem 1.4.4.

Another way to generalize equation (1.2) is to move from products of consecutive integers to products of arithmetic progressions. This is a much more difficult problem than the original, but Erdős allegedly conjectured the following:

Conjecture 1.4.8. *There is a constant k_0 such that*

$$\prod_{i=0}^{k-1}(n+id) = y^{\ell} \text{ with } \gcd(n,d) = 1, \tag{1.8}$$

has no solutions for n, d, k, y and ℓ positive integers with $\ell \geq 2$ and $k \geq k_0$.

While Erdős is believed to be the first person to state this conjecture, work on this equation started considerably before Erdős. One of the first results goes back to Euler, showing that there are no non-trivial solutions for $k = 4$ and $\ell = 2$.

There are two main categories of work in the literature on this problem; those that use elementary or combinatorial arguments, and the more modern approach using Frey-Hellegouarch curves to create Fermat equations.

Shorey, in particular, produced many results using elementary methods. For example in [52] he showed that if the greatest prime divisor of d is fixed and $\ell \geq 3$ then Conjecture 1.4.8 is true. Additionally in [53] he showed that if n is fixed and $\ell \geq 7$ then the conjecture still holds.

Using more modern methods of Galois representations and modular methods there have been slightly stronger results that do not require fixing variables other than k. For example in [2] it is shown that there are no non-trivial solutions for $6 \leq k \leq 11$ and further that there are at most finitely many non-trivial solutions for all $k \leq 82$.

The first result to work for a general k without limiting the possibilities of the other variables was given by Bennett and Siksek in Theorem 2 of [6] and is the following theorem:

Theorem 1.4.9. *There is an effectively computable absolute constant k_0 such that if $k \geq k_0$ is a positive integer, then any solution in integers to equation* (1.8) *with prime exponent ℓ satisfies either $y = 0$ or $d = 0$ or $\ell \leq \exp(10^k)$.*

This method starts by using the same ideas as in previous modern studies of the Erdős-Selfridge curves, that is, to attach many Fermat equations to a putative solution.

However, unlike in the $d = 1$ case this does not allow us to bound ℓ. It does, however, allow us to show that d must be divisible by all primes in a large interval.

Further, Bennett and Siksek showed how to attach Dirichlet characters to such a given Fermat equation. Then, using analytic methods it is possible to show that there is a bound on the number of characters with given properties, i.e. smooth conductor, or bound on the largest prime in the conductor. Finally, they show that if one sieves off all characters that are not those that they have previously studied, one will always be left with too many given their previous bounds on the number of possible characters.

In this thesis we will study these methods and develop them further. In particular we will take the hypothesis and the results of Bennett and Siksek regarding the number of possible characters and produce lower bounds. This then means that at the sieving stage of the argument, we have far fewer characters needed to reach a contradiction. This allows us to prove the following theorem:

Theorem 1.4.10. *For k sufficiently large and ℓ a prime, if there is a non-trivial integral solution to*

$$By^\ell = \prod_{i=0}^{k-1}(x + id) \tag{1.9}$$

such that

(1) $p \nmid B$ for all primes in $[k/2, k]$,

(2) fewer than $k/4$ primes greater than k divide B,

then it follows that $\ell < \exp(10^{\max(k,P(B))})$, where $P(B)$ is the largest prime dividing B.

In particular we will also be able to generalise some of our work in the case of $d = 1$ showing the following:

Theorem 1.4.11. *For k sufficiently large and ℓ a prime, if there is a non-trivial rational solution to*

$$By^\ell = \prod_{i=0}^{k-1}(x + i) \tag{1.10}$$

such that

(1) $p \nmid B$ for all primes in $[k/2, k]$,

(2) fewer than $k/4$ primes greater than k divide B,

then it follows that $\ell < \exp(10^{\max(k,P(B))})$*, where* $P(B)$ *is the largest prime dividing* B*.*

Further, with some conditions on d we can study these curves with coefficient and omitted terms.

Theorem 1.4.12. *For* k *sufficiently large and* ℓ *a prime, if there is a non-trivial integral solution to*

$$By^{\ell} = \prod_{\substack{i=0 \\ i \neq j}}^{k-1} (x+i) \tag{1.11}$$

such that

(1) $p \nmid B$ *for all primes in* $[k/3, k/2]$*;*

(2) fewer than $k/4 - 1$ *primes greater than* k *divide* B*;*

(3) $v_p(d) \equiv 0 \pmod{\ell}$ *for all primes* p *greater than* k*;*

then it follows that $\ell < \exp(10^{\max(k,P(B))})$*.*

§ 1.5 Sums of Powers of Arithmetic Progressions

An alternative way of looking at the relation between arithmetic progression and perfect powers would be to consider powers of arithmetic progressions. In particular the understanding of forms of sums of such expressions has been growing in recent years.

More precisely, let $a_i = n + id$ for n and d coprime integers and consider equations of the form

$$y^{\ell} = \sum_{i=1}^{m} a_i^k, \tag{1.12}$$

for m and k integers. Then it is relevant to ask if it possible to find a bound on k or ℓ or even d.

There are two distinct areas of study in the literature regarding equation (1.12). There are those that study when m is a general integer, or when m is fixed, in particular $m = 3$, with the latter being much better understood. We will first discuss some of what is known regarding the general case.

The study of such equations goes back all the way to Euler who noted the relation $6^3 = 5^3 + 4^3 + 3^3$. It should be noted that it is possible to construct a sequence of consecutive integers of any length, such that the sum of their cubes is a square. This follows from the well known identity that

$$\left(\frac{d(d+1)}{2}\right)^2 = \sum_{i=1}^{d} i^3. \tag{1.13}$$

It is even possible to create other parametric solutions that are less obvious. Pagliani [40] showed that

$$\left(\frac{v^5 + v^3 - 2v}{6}\right)^6 = \sum_{i=1}^{v^3} \left(\frac{v^4 - 3v^3 - 2v^2 - 2}{6} + i\right)^3, \tag{1.14}$$

where v is chosen to be either 2 or 4 modulo 6.

A more modern result in the study of powers of consecutive integers for a large number of terms can be found in [4] by Bennett, Patel and Siksek.

Theorem 1.5.1. *Let $2 \leq d \leq 50$ and ℓ be a prime. There are only finitely many integral solutions to the equation*

$$(x+1)^3 + (x+2)^3 + \ldots + (x+d)^3 = y^\ell \tag{1.15}$$

with $x \geq 1$, and given in Table 1 in [4].

We shall now focus on the case when $m = 3$. This problem was originally solved in cases where k, ℓ and d are all fixed. For example Cassels [12] showed that

$$(x-1)^3 + x^3 + (x+1)^3 = y^2, \tag{1.16}$$

for x and y integers has only finitely many solutions, in-particular $x = 0, 1, 2, 24$.

The more general form of this equation

$$(x-1)^k + x^k + (x+1)^k = y^n, \tag{1.17}$$

for x, y, k and n integers with k and n both greater than or equal to 2, was studied by Zhang in [61]. Zhang attached Fermat equations to a putative solution of equation (1.17) in the case that $k \in \{2, 3, 4\}$. Using modular methods and level

lowering techniques he managed to show that the only solutions are $(x, y, k, n) = (1, \pm 3, 3, 2), (2, \pm 6, 3, 2), (24, \pm 204, 3, 2), (\pm 4, \pm 6, 3, 3), (0, 0, 3, n)$.

In [5] Bennett, Patel and Siksek extended this result to the case of $k \in \{5, 6\}$. In particular they prove the following two theorems.

Theorem 1.5.2. *The only solutions to the equation*

$$(x-1)^5 + x^5 + (x+1)^5 = y^n, \tag{1.18}$$

for x and y integers and $n \geq 2$ a positive integer, satisfy $x = y = 0$.

Theorem 1.5.3. *There are no solutions to the equation*

$$(x-1)^6 + x^6 + (x+1)^6 = y^n, \tag{1.19}$$

for x and y integers and $n \geq 2$ a positive integer.

There has also been work in the cases of a more general arithmetic progression. For example in [29], Koutsianas studies the equation

$$(x-d)^2 + x^2 + (x+d)^2 = y^n \tag{1.20}$$

for $d = p^b$ for b a non-negative integer and p a prime less than 10^4. In particular he shows that there are only finitely many solutions in this case and determines all of them, given in Table 1 of [29].

Additionally, Koutsianas with Patel studied the same equation where d is any positive integer less than 5000. In [30] they showed that for n a prime exponent then there are only finitely many solutions and calculated all of them.

In Chapter 6 we shall consider a similar equation. In particular we will look at the solutions of the equation

$$y^\ell = (x-d)^3 + x^3 + (x+d)^3, \tag{1.21}$$

for x, y and d integers. We shall do this using the modular method. It is possible to attach Fermat equations to a putative solution of Equation (1.21). There will in fact be four Fermat equations that we attach depending upon the greatest common divisor of $3x$ and $x^2 + 2d^2$. We then use the modular method and level lowering to show that there are modular forms of small level for a given solution; in particular we will see that

if x is even then there are no solutions, as this would give rise to a level 6 newform. In the odd case, the level lowered form does not come from a trivial space of modular forms.

In 2017 Garcia and Patel studied the same equation, at the same time as this author. In [22] they prove the following theorem.

Theorem 1.5.4. *Let $p \geq 5$ be a prime. The only integer solutions to the equation*

$$(x-r)^3 + x^3 + (x+r)^3 = y^p \tag{1.22}$$

with x and r coprime and $0 < r \leq 10^6$, are the trivial ones satisfying $xy = 0$.

In particular in this paper they independently showed our result regarding the case that x is even; this is Lemma 5.1 in [22]. While they used the modular method in the even case, the rest of their work relied on bounds for sums of logarithms.

We will also be able to deal with the case where x is odd for all r, improving the work of Garcia and Patel. This is possible, as we note that all the Frey-Hellegouarch curves are twists of one particular elliptic curve. This means that when we study the space of level lowered modular forms, we do not have to look at all the newforms, but only those that could come from a twist of the given curve. We then use Magma to study this problem and show that no such modular form exists.

Chapter 2

Analytic Number Theory

To develop our understanding of the Erdős-Selfridge curves in later chapters, we will first have to state some well known theorems and functions used in analytic number theory.

In the first section we will deal with classical ideas about primes, although we will need the modern developments of these ideas as well. In particular we will be looking at the idea of primes in intervals and primes in arithmetic progressions. Both are questions that started in the 18th century, but even now we are seeing developments in the theory. This will be relevant in Chapter 4 as well as Section 5.1.

In the second section we will deal with characters, functions from abelian groups to the complex numbers, and in particular we will show how to attach an L-function and results about summing characters over short intervals. These are very important questions in analytic number theory. We will need these ideas when we are attaching characters to our Erdős-Selfridge curves in Section 5.2.

§ 2.1 Primes

2.1.1 Primes in Intervals

A well known problem in the area of analytic number theory is that of showing that primes exist in given intervals. The first result in this area was conjectured by Bertrand in 1845, stating that for $n \geq 1$ there is always a prime in the interval $[n, 2n]$, with the first proof being provided by Chebyshev in 1852. Since then there have been many proofs provided for this statement.

Theorem 2.1.1 (Bertrand's Postulate)**.** *For every $n > 1$ there is always at least one prime p such that $n < p < 2n$.*

A generalization of this problem is to consider intervals that are comparatively shorter. In particular there are effective bounds for sizes of intervals that are of order $O(n/\log^2(n))$ and bounds for distances that are of order $O(n^{21/40})$. This is very close to the absolute best that would be permitted under the Riemann hypothesis.

Theorem 2.1.2. *For every $n \geq 25$ there is always a prime between n and $(1 + \frac{1}{5})n$.*

Proof. This is due to Nagura [38]. □

We now present an easy corollary that we will need in Subsection 4.2.

Corollary 2.1.3. *For all $n \geq 22$, there exists a prime p such that $\frac{n}{3} \leq p \leq \frac{n}{2}$.*

Proof. From Theorem 2.1.2 we know that there is always a prime p such that

$$p \in \left(n, (1 + \tfrac{1}{5})n\right), \text{ for } n \geq 25.$$

Hence for $n \geq 75$ the result now follows. For $22 \leq n \leq 75$ we can explicitly calculate the primes in the given interval, hence the result follows. □

We will not need the following three theorems, however as they are the most advanced theorems in this area, we have included them to show the depth of this branch of maths.

Theorem 2.1.4. *For all $n \geq 468991632$ there is at least one prime in*

$$\left[n, \left(1 + \tfrac{1}{5000\log^2(n)}\right) n\right].$$

Proof. This result is due to Dusart [15]. □

The following is an incredibly strong theorem in this area; however, unlike all previous results it does not provide a lower bound on n from which we know the result holds.

Theorem 2.1.5. *For all sufficiently large n there is a prime in the interval*

$$\left[n, n + n^{21/40}\right].$$

Proof. This was shown by Baker, Harman and Pintz [1]. □

The following theorem is conditional on the Riemann hypothesis. Under that assumption it gives the best bound for the intervals that will contain primes. Compared to the above theorem we see just how close the current best result is to the theoretical best.

Theorem 2.1.6. *Assuming the Riemann hypothesis to be true then the interval*

$$\left[n - K\sqrt{n}\log n, n\right]$$

contains a prime, for K an effective large constant and n sufficiently large.

Proof. This is due to work of Wolke [60]. □

2.1.2 The Prime Number Theorem

Ever since the proof of the infinitude of primes, the question of determining the rate of growth of the number of primes has been of pressing importance in analytic number theory. The Prime Number Theorem gave the first answer to this question, showing that the rate of growth is of order $O(x/\log(x))$. The Prime Number Theorem is strongly related to the first Chebyshev function. The Chebyshev function makes it easier to study not only the distribution of primes but also primes in arithmetic progressions. We will outline all of these functions and theorems in the current section.

Definition 2.1.7. We define the *prime counting function* as

$$\pi(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} 1. \tag{2.1}$$

The Prime Number Theorem is the statement that

$$\pi(x) \sim \frac{x}{\log(x)},$$

proven independently by Hadamard and de la Vallée Poussin.

Definition 2.1.8. For x a real positive number we define the *Chebyshev function* $\theta(x)$ as

$$\theta(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} \log(p).$$

The Prime Number Theorem is also equivalent to the following statement [25, pg. 31];

$$\theta(x) \sim x. \tag{2.2}$$

The Chebyshev function plays a vital role in analytic number theory and is interesting in its own right. However, in this thesis we shall only scratch the surface of what is known, and limit ourselves to only what is useful to our aims. The following bound for $\theta(x)$ will be very important in later chapters.

Theorem 2.1.9. *For all $x > 0$*

$$\theta(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} \log(p) < 1.000081x. \tag{2.3}$$

Proof. Note in Schoenfeld [49, pg. 360]. □

A consequence of the Prime Number Theorem is that for all $\epsilon > 0$ there exists an N such that for all $x > N$ the following inequality holds

$$\frac{x}{\log(x)}(1-\epsilon) < \pi(x) < \frac{x}{\log(x)}(1+\epsilon).$$

However we can normally do a lot better than for a fixed ϵ as given by the following theorem.

Theorem 2.1.10. *If $x \geq 59$ then*

$$\frac{x}{\log(x)}\left(1 + \frac{1}{2\log(x)}\right) < \pi(x) < \frac{x}{\log(x)}\left(1 + \frac{3}{2\log(x)}\right).$$

Proof. This was proven by Rosser and Schoenfeld [45]. □

Just like in the previous section, the Riemann hypothesis determines the best possible bound on $\pi(x)$.

Definition 2.1.11. For $x \geq 0$ we define the following function to be the *logarithmic integral*

$$li(x) = \int_0^x \frac{dt}{\log(t)},$$

interpreted as a Cauchy principal value for $x > 1$.

Theorem 2.1.12. *Assuming the Riemann hypothesis is correct, then for* $x \geq 2657$

$$|\pi(x) - li(x)| < \frac{\sqrt{x}\log(x)}{8\pi}.$$

Proof. See [49]. □

Not only can we understand the rate of growth of the number of primes, but we can also accurately understand the rate of growth of the sum of functions of primes, including the functions

$$f(x) = \frac{1}{x} \text{ and } f(x) = \frac{\log(x)}{x}.$$

Theorem 2.1.13. *For* $x \geq 286$ *and* τ *an explicit constant the following inequality holds,*

$$\left| \sum_{p \leq x} \frac{1}{p} - \log\log x - \tau \right| < \frac{1}{2\log^2(x)}.$$

Proof. See [45]. □

Theorem 2.1.14. *For* $x \geq 319$ *and* E *an explicit constant,*

$$\left| \sum_{p \leq x} \frac{\log(p)}{p} - \log(x) - E \right| < \frac{1}{2\log(x)}.$$

Proof. Theorem 6 of [45]. □

§ 2.2 Arithmetic Progressions

Arithmetic progressions are sequences of integers of the form $a_n = a + nd$ for n either in a finite interval of the positive integers or the whole set of positive integers. They have been of much interest in analytic number theory for their deep connection with prime numbers. It is one of the aims of this thesis to highlight the connection between arithmetic progressions and perfect powers.

Another problem related to that of the Prime Number Theorem is whether there exists an infinite number of primes in every infinite arithmetic progression? This is trivially false if the starting value of the sequence and the common difference are not coprime. In the alternate case one would expect the answer to be yes, and for the number of primes to be equally distributed among the classes of $a \pmod d$ for d the common

difference and a coprime to d. In this case, Dirichlet answered in the affirmative that there are infinitely many primes, and de la Vallée Poussin proved that the primes are equally distributed among the congruence classes.

Theorem 2.2.1 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *If a and d are coprime integers, then the arithmetic progression $a_n = a + nd$ contains infinitely many primes.*

We might also want to know whether, given a d is it possible to know a bound on n such that we know $a_1, \dots a_n$ contains a prime. To understand this we are going to have to define some machinery first. We will define the arithmetic progression equivalent of the $\theta(x)$ function defined in the previous section.

Definition 2.2.2. For x a real variable, a and d coprime integers, we set

$$\theta(x; a, d) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{d}}} \log(p).$$

We call this the *first Chebyshev function associated to the arithmetic progression* $a \pmod{d}$.

A classical result in the literature from [43] is the following theorem.

Theorem 2.2.3. *If $d \leq 13$, $x \geq 10^{10}$, $\epsilon = 0.004560$ and a an integer coprime to d then*

$$(1 - \epsilon)\frac{x}{\varphi(d)} \leq \theta(x; a, d) \leq (1 + \epsilon)\frac{x}{\varphi(d)}$$

Remark 2.2.4. The paper [43] contains more results; for example, for greater values of x we may take a smaller ϵ.

We now state and prove the following simple corollary as it will be needed later in 5.2.

Corollary 2.2.5. *For $x \geq 10^{10}$ there exists a prime in the interval $(x, 1.06x]$ for each odd $\pmod 8$ class.*

Proof. It is clear that we just have to show that

$$\sum_{\substack{x < p \leq 1.06x \\ p \equiv a \pmod{8}}} \log(p) \neq 0.$$

It follows from Theorem 2.2.3 that

$$(1-\epsilon)\frac{1.06x}{\varphi(8)} - (1+\epsilon)\frac{x}{\varphi(8)} \leq \theta(1.06x;a,8) - \theta(x;a,8) = \sum_{\substack{x<p\leq 1.06x \\ p\equiv a \pmod 8}} \log(p). \tag{2.4}$$

Factorising the left hand side and checking that it is positive now gives the result. □

Very recently there has been a major generalization of the work above, due to Bennett, Martin, O'Bryant and Rechnitzer [3]. While the previous theorem about $\theta(x)$ will be more than sufficient for most of our work, we will require this more accurate formulation in Subsection 5.3.1.

Theorem 2.2.6. *Let $d \geq 3$ be an integer and let a be an integer that is coprime to d. Then there exist explicit constants $c_\theta(d)$ and $x_\theta(d)$ such that*

$$\left|\theta(x;a,d) - \frac{x}{\varphi(d)}\right| < c_\theta(d)\frac{x}{\log(x)} \text{ for all } x \geq x_\theta(d).$$

Moreover, $c_\theta(d)$ and $x_\theta(d)$ satisfy $c_\theta(d) \leq c_0(d)$ and $x_\theta(d) \leq x_0(d)$, where

$$c_0(d) = \begin{cases} \frac{1}{840}, & \text{if } 3 \leq d \leq 10^4, \\ \frac{1}{160}, & \text{if } d > 10^4, \end{cases} \tag{2.5}$$

and

$$x_0(d) = \begin{cases} 8\cdot 10^9, & \text{if } 3 \leq d \leq 10^5, \\ \exp(0.03\sqrt{d}\log^3(d)), & \text{if } d > 10^5. \end{cases} \tag{2.6}$$

Proof. This is Theorem 1.1 and 1.2 in [3]. □

The connection between primes and arithmetic progression is even deeper still. It is possible to create a finite arithmetic progression of any given length such that all terms in the progression are primes. This is the celebrated Green-Tao Theorem [23].

Theorem 2.2.7. *For every natural number k, there exist arithmetic progressions of primes with k terms.*

The following theorem, Roth's theorem, will be vital to our work in Section 5.4. This theorem answers the question of whether a subset of an interval can contain a 3-term arithmetic progression.

Theorem 2.2.8. *Let $0 < \delta < 1$. Then there exists a positive constant $K_0(\delta)$ such that if $k \geq K_0(\delta)$ and $J \subset \{0, 1, \ldots, k-1\}$ with $|J| \geq \delta k$, then there is at least one non-trivial 3-term arithmetic progression in J.*

Proof. See [46]. □

It is worthwhile noting that $K_0(\delta)$ can be explicitly described; for example

$$K_0(\delta) = \exp(\exp(132 \log(2) \cdot \delta^{-1})),$$

follows from [41], however we will not be using such an explicit version.

§ 2.3 Characters

Characters are an important aspect in all areas of number theory. They were first defined by Dirichlet to explain the ideas in the previous section, such as primes in arithmetic progression. As we were only giving a recollection of theorems we will need in the later sections and not their proofs we delayed defining them until now. In later sections we will use solutions of superelliptic curves to construct characters, then analyse their analytic properties. In this section we will define characters and the aspects of them that we will need later, such as L-functions.

2.3.1 Characters and L-functions

Here we will define characters and attach L-functions to them in the usual way, in line with [25]. Further we will explain the nature of the zeros of the L-functions.

Definition 2.3.1. Let G be a finite abelian group. A homomorphism $\chi : G \to \mathbb{C}^\star$ is called a *character*.

We call χ *real* if $\chi(g) \in \mathbb{R}$ for all $g \in G$.

Definition 2.3.2. For m an integer, let χ be a character on $(\mathbb{Z}/m\mathbb{Z})^\star$,

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}.$$

Extend this character to all integers by setting $\chi(n) = 0$ for n not coprime to m. We call this χ a *Dirichlet character of modulus m*.

Example 2.3.3. For p a prime number, then

$$\chi(n) = \left(\frac{n}{p}\right)$$

is a Dirichlet character mod p.

Definition 2.3.4. The Dirichlet character $\pmod m$ that corresponds to the trivial character

$$\chi_0(a) = 1, \text{ for all } a \text{ coprime to } m,$$

is called the *trivial character* of modulus m.

If χ is a Dirichlet character such that $\chi^2 = \chi_0$, we say it is a *quadratic character*.

Remark 2.3.5. We will sometimes use the phrase *principal character* interchangeably with trivial character.

Definition 2.3.6. For χ a character of modulus m, we define $m^\star$, the *conductor* of χ, to be the smallest divisor of m such that $\chi = \chi_0\chi^\star$, where χ_0 is the principal character to modulus m and $\chi^\star$ is a character of modulus $m^\star$. We call a character *primitive*, if its modulus is equal to its conductor. We also define the function $N(\chi)$, which is the conductor of the character χ.

Remark 2.3.7. In fact all quadratic characters of a given modulus m can be easily determined. If $m = p$ for an odd prime, there is exactly one such character and it is the one given in Example 2.3.3. For $m = 4$, we have exactly one primitive character defined by

$$\chi_4(n) = (-1)^{\frac{n-1}{2}} \text{ if } 2 \nmid n.$$

If $m = 8$, there are two primitive characters defined by

$$\chi_8(n) = (-1)^{\frac{(n-1)(n+1)}{8}} \text{ if } 2 \nmid n, \tag{2.7}$$

$$\chi_4(n)\chi_8(n) = (-1)^{\frac{(n-1)(n+5)}{8}} \text{ if } 2 \nmid n. \tag{2.8}$$

Other than those listed above, there are no quadratic primitive characters for m a prime power. Every real primitive character of conductor m is a product of the above types.

We can attach a *Dirichlet series* to a Dirichlet character. These are very important in analytic number theory and also for our results on the Erdős-Selfridge curves.

Definition 2.3.8. For χ a Dirichlet character, we define a *Dirichlet L-function* $L(s,\chi)$ by the following:

$$L(s,\chi) = \sum_{n\geq 1} \chi(n)n^{-s} = \prod_{p \text{ prime}} (1-\chi(p)p^{-s})^{-1}.$$

The series and the Euler product are absolutely convergent for $\Re(s) > 1$. Moreover they can be analytically continued to $\mathbb{C}$.

We now state the Prime Number Theorem for Dirichlet characters as it will be vital for understanding characters with small conductor. The following combines Theorems 5.26 and 5.28 of [25]:

Theorem 2.3.9. *There exists an effectively computable absolute constant $c^* > 0$ such that the following holds.*

(I) If χ is any primitive, quadratic character of conductor N, then $L(s,\chi)$ has at most a single real zero β_χ with

$$1 - \frac{c^*}{\log(N)} < \beta_\chi < 1. \tag{2.9}$$

If such a zero exists, the χ is necessarily real and β_χ is a simple zero. We call β_χ an exceptional zero and N an exceptional conductor.

(II) If χ_1 and χ_2 are distinct real, primitive quadratic characters of conductor N_1 and N_2 respectively, with associated L-functions $L(s,\chi_1)$ and $L(s,\chi_2)$ having real zeros β_{χ_1} and β_{χ_2}, respectively, then

$$\min\{\beta_{\chi_1}, \beta_{\chi_2}\} < 1 - \frac{3c^*}{\log(N_1 N_2)}. \tag{2.10}$$

The combination of (2.10) and (2.9) causes the conductors for exceptional characters to, in some sense, repel each other. This is often described as "Landau's repulsion principle".

Corollary 2.3.10. *If $N_1 < N_2$ are two exceptional conductors then $N_2 > N_1^2$.*

Remark 2.3.11. A proof of this can be found in section 7 of [6], which we have restated here.

Proof. Let β_{χ_1} and β_{χ_2} be the zeros of the characters with conductor N_1 and N_2 respectively. Then applying (2.10) and (2.9) we see that,

$$1 - \frac{c^*}{\log(N_1)} < min\{\beta_{\chi_1}, \beta_{\chi_2}\} < 1 - \frac{3c^*}{\log(N_1 N_2)}.$$

Simplifying this and collecting like terms gives the result. □

As in [6] we will define the function $P(N)$ to be the largest prime factor of N. We will then bound $P(N)$, where N is the conductor of a quadratic character, in terms of N.

Lemma 2.3.12. *Let N be the conductor of a quadratic character, and let $P(N)$ be the largest prime factor of N. Then $P(N) > 0.94\log(N)$.*

Proof. This is Lemma 7.3 in [6]. □

Definition 2.3.13. We denote by $\Lambda(n)$ the *Von Mangoldt function* as defined below,

$$\Lambda(n) = \begin{cases} \log(p), \text{ if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1; \\ 0, \text{ otherwise.} \end{cases} \tag{2.11}$$

Definition 2.3.14. We denote by $\psi(x)$ the second Chebyshev functions as defined below,

$$\psi(x) = \sum_{n \leq x} \Lambda(n). \tag{2.12}$$

The following theorem, from [15], is another form of the Prime Number Theorem.

Theorem 2.3.15. *For $x \geq 10^{10}$,*

$$|\psi(x) - x| \leq 0.001 \frac{x}{\log x}. \tag{2.13}$$

The following theorem, which is Theorem 5.27 of [25], is an explicit version of the Prime Number Theorem for Dirichlet characters.

Theorem 2.3.16. *Let χ be a non-trivial primitive Dirichlet character of conductor N. Then*

$$\sum_{m \leq X} \chi(m)\Lambda(m) = -\frac{X^{\beta_\chi}}{\beta_\chi} + O\left(X \exp\left(\frac{-c\log X}{\sqrt{\log X} + \log(N)}\right)\log^4(N)\right).$$

Moreover, $c > 0$ is an absolute effective constant, and the implied constant is absolute. Also β_χ denotes the exceptional zero if present, otherwise the term $-\frac{X^{\beta_\chi}}{\beta_\chi}$ is omitted.

It is important to point out that for N small enough, the error term is genuinely smaller than the length of summation. Only when $\log N \ll \log^\kappa X$ for $\kappa < 1$ can we apply this theorem. Further the existence of possible exceptional zeros complicates matters.

Definition 2.3.17. We denote by $\tau(n)$ the number of divisors function for a positive integer n.

We now deal with character sums over short intervals, in particular a theorem of Graham and Ringrose.

Theorem 2.3.18. *For $r \geq 3$, let $\chi_i \pmod{q_i}$ be characters for $1 \leq i < r$ and $\chi \pmod{q}$ be a primitive character of conductor $q > 1$, q square-free with $(q, q_1 \dots q_{r-1}) = 1$. Then for $N \geq N_0 = max\{q_1, \dots, q_{r-1}\}q^{1+2^{-r}}$ we have*

$$\left| \sum_{M < m \leq M+N} \chi_1\chi_2 \cdots \chi_{r-1}\chi(n) \right| \leq 4N \left(\frac{\tau(q)^{r^2}}{q} \right)^{2^{-r}}.$$

Proof. This is found in [25, pg. 333], except that because we are making the assumption that $r \geq 3$ we can modify line 15 of p.333 to get the result. □

Chapter 3

Elliptic Curves, Modular Forms and Galois Representations

In this chapter we will give a brief account of the algebraic number theory that will be required to achieve our results.

§ 3.1 Frey-Hellegouarch Curves and Modular Forms

In this section we are going to explain the idea of Frey-Hellegouarch curves, a type of elliptic curve that capture very well the arithmetic information of equations of the form $u+v+w=0$, modular forms, and how combined they can be used to understand solutions of these equations. In our later chapters we will reduce our problems to solving many simultaneous equations of the form

$$Ax^\ell + By^\ell + Cz^\ell = 0 \text{ or} \tag{3.1}$$

$$Ax^\ell + By^\ell + Cz^2 = 0, \tag{3.2}$$

so our understanding of the Frey-Hellegouarch curves attached to these equations will be vital.

We will do this using four powerful and important ideas in number theory these are modularity, level-lowering, Kraus's lemma and exponent bounding. The modularity theorem tells us that to an elliptic curve defined over the rationals there is a unique modular form that can be attached to it, such that their Galois representations agree. This was first proven in the semi-stable case by Wiles in his proof of Fermat's Last

Theorem [59]. It is now known entirely over the rationals by the work of Wiles, Breuil, Conrad, Diamond and Taylor [10], and even known in the real quadratic case thanks to Freitas, Le Hung and Siksek [16].

Level lowering of modular forms attached to elliptic curves was first done by Ribet [44]. The theorem shows that if a modular form comes from an elliptic curve, and under certain hypotheses on the elliptic curve and modular form, then it is possible to find another modular form of smaller level such that the modular forms agree (mod ℓ) for some prime ℓ. These two very powerful theorems combined are enough to prove Fermat's Last Theorem; this is the case that $A = B = C = 1$ in Equation (3.1), which we shall use as an example. This proof of Fermat's Last Theorem relies on the fact that when the modular forms attached to these Frey-Hellegouarch curves are level lowered they belong to a space having no non-trivial elements.

However for more general A, B and C we will not always get so lucky that the space we are interested in is non-trivial. In particular we will not always be able to show that there are no solutions, but instead show that ℓ is bounded.

Kraus's lemma allows us to show that provided that ℓ is sufficiently bigger than the conductor of the elliptic curve, then the level lowered modular form is also coming from an elliptic curve. We will need this in later chapters as it allows us to retain much of the arithmetic information of the original elliptic curve, which we will later use to construct characters.

We now start with the definition of a Frey-Hellegouarch curve.

Definition 3.1.1. Let u, v and w be integers such that $uvw \neq 0$ and $u + v + w = 0$, and define

$$E : y^2 = x(x - u)(x + v). \tag{3.3}$$

Then E is an elliptic curve with discriminant $\Delta = 16u^2v^2w^2$, which we shall call a *Frey-Hellegouarch curve*.

The terms defined below will be used liberally throughout this thesis.

Definition 3.1.2. For N an integer, $\mathrm{Rad}(N)$ is the product of all distinct primes dividing N. Also, we write $\mathrm{Rad}_2(N)$ for the product of all distinct odd primes dividing N.

We first define the following notation so that we may soon state Ribet's Level Lowering Theorem.

Let E be an elliptic curve defined over $\mathbb{Q}$, with minimal discriminant Δ and conductor M. For a rational prime $\ell \geq 3$, we denote by

$$\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to Aut(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$$

the representation describing the action of $G_{\mathbb{Q}} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-torsion subgroup $E[\ell]$.

Set

$$M_0 = M/\prod_{\substack{q||M,\ q \text{ prime} \\ \ell|\mathrm{ord}_q(\Delta)}} q, \tag{3.4}$$

where $\mathrm{ord}_q(x)$, as usual, is the largest power of the prime q that divides a non-zero integer x.

Remark 3.1.3. We note here that these Frey-Hellegouarch curves have full 2-torsion, so for $\ell \geq 7$ $E[\ell]$ is irreducible by [37].

The following theorem is a well known consequence of Ribet's Level Lowering Theorem [44]. In the original formulation, the hypothesis required that E is modular over $\mathbb{Q}$. However, this is now known for all elliptic curves over $\mathbb{Q}$ by Wiles, Breuil, Conrad, Diamond and Taylor [10], [59].

Theorem 3.1.4. *If $E[\ell]$ is irreducible then there is a cuspidal newform $f = \sum_{n\geq 1} c_n q^n$ of weight 2 and level M_0 such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$ where $\lambda \mid \ell$ is a prime of the totally real field $K = \mathbb{Q}(c_1, c_2, \ldots)$.*

Definition 3.1.5. For f a weight 2 cuspidal newform $f = \sum_{n\geq 1} c_n q^n$ we call $\mathbb{Q}_f = \mathbb{Q}(c_1, c_2, \ldots)$ the *field of coefficients of f*. Further, we shall say f is *rational* if $K = \mathbb{Q}$ and *irrational* if $K \neq \mathbb{Q}$.

We explain what we mean by $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$ in the following standard lemma which can be found stated in [6].

Lemma 3.1.6. *With notation as in Theorem 3.1.4, let p be a rational prime. Then*

(I) if $p \nmid \ell M M_0$ then $a_p(E) \equiv c_p \pmod{\lambda}$;

(II) if $p \nmid \ell M_0$ and $p \,||\, M$ then $p + 1 \equiv \pm c_p \pmod{\lambda}$.

In the case that f is rational we may actually do slightly better than the above lemma. If f is a rational newform, then we know that f corresponds to some elliptic curve, which we denote by F. If E arises $\pmod{\ell}$ from f then we shall also say that E arises modulo ℓ from F, written in the usual way as $E \sim_\ell F$.

Lemma 3.1.7. *Let E and F be elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that E arises modulo ℓ from F. Then for all primes p*

(I) if $p \nmid NN'$ then $a_p(E) \equiv a_p(F) \pmod{\ell}$;

(II) if $p \nmid N'$ and $p \,||\, N$ then $p + 1 \equiv \pm a_p(F) \pmod{\ell}$.

Proof. This strengthening is due to Kraus and Oesterlé [33]. □

We now want to highlight for the reader just how powerful these theorems are with the following example.

Example 3.1.8 (Fermat's Last Theorem)**.** Assume for contradiction that a, b and c are non-zero co-prime integers and $\ell \geq 7$ a prime such that

$$a^\ell + b^\ell + c^\ell = 0.$$

Without loss of generality we can reorder the integers such that $a \equiv -1 \pmod{4}$ and b is even. We attach the following Frey-Hellegouarch curve

$$E : y^2 = x(x - a^\ell)(x + b^\ell),$$

as explained in Definition 3.1.1.

It is a simple computation using Tate's algorithm to compute that the minimal discriminant is $2^{-8}(abc)^{2\ell}$ and conductor $2\,\mathrm{Rad}_2(abc)$. Using the notation as above we conclude that $M_0 = 2$. Remembering Remark 3.1.3, we see we are now in a position to apply Ribet's Level Lowering Theorem 3.1.4. However this would imply the existence of a non-trivial modular form of weight 2 and level 2, but this is known not to exist, contradicting our assumption.

This example highlights the combined strength of the modularity theorem and Ribet's Level Lowering Theorem in the application of determining if solutions exist to generalized Fermat equations.

However in more complicated examples it is not possible to completely eliminate all possible solutions. This can happen when the space $S_2(M_0)$ of cuspidal modular forms of weight 2 and level M_0, for the calculated M_0 is non-trivial. In this case there are possible remedies. In the following few pages we will see one of them. In some situations it is possible to bound an exponent in the equation, for example the ℓ in the Fermat equation. The bounding of exponents in generalized Fermat equations will be of great importance to us to prove our theorems.

The following is Lemma 2.2 in [6] and is crucial in Chapters 4 and 5.

Lemma 3.1.9. *With notation as above, suppose that $p \neq \ell$ is a prime with $p \parallel M$ and, $\ell \mid \mathrm{ord}_p(\Delta)$. Then*

$$\ell \leq (\sqrt{p}+1)^{\frac{M_0+1}{6}}.$$

We now state a theorem of Kraus that shows that if the residual characteristic ℓ is sufficiently large compared to the level of a modular form f, then f has rational eigenvalues, and hence corresponds to an elliptic curve over $\mathbb{Q}$.

For a positive integer n let

$$\mu(n) = n \prod_{\substack{q \mid n \\ q \text{ prime}}} \left(1+\frac{1}{q}\right) \text{ and } g_0^+(n) = \mathrm{Dim}(S_2^{new}(n)). \tag{3.5}$$

Define

$$F(n) = \left(\sqrt{\frac{\mu(n)}{6}}+1\right)^{2g_0^+(n)}, \; G(n) = \left(\sqrt{\frac{\mu(\mathrm{lcm}(n,4))}{6}}+1\right)^2$$

and set

$$H(n) = \max(F(n), G(n)).$$

Then the following is Théorème 4 of [31].

Theorem 3.1.10. *With notation as in Theorem 3.1.4, suppose that E has full 2-torsion and that $\ell > H(M_0)$. Then there exists an elliptic curve $F/\mathbb{Q}$ having full 2-torsion of conductor M_0, such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{F,\ell}$.*

It is clear that results in Chapter 2 will allow us to understand the μ function. Additionally, Theorem 2 of Martin [36] gives us the following bound for $g_0^+(M_0)$, which allows us to completely understand the H function.

Lemma 3.1.11. *For all positive integers n, we have $g_0^+(n) \leq \frac{n+1}{12}$.*

This lemma will be vital to bounding $H(M_0)$ in Chapters 4 and 5.

§ 3.2 Equations with Signature $(\ell, \ell, 2)$

In Chapter 6 we are going to transform solutions of our original equation into solutions of Fermat equations of signature $(\ell, \ell, 2)$. There it will be important that we understand all of the properties of these Fermat equations, so we have dedicated a section to discussing them. This all follows the work of Bennett and Skinner [8], and Ivorra and Kraus [26].

Consider the equation

$$Ax^\ell + By^\ell = Cz^2, \tag{3.6}$$

for $\ell \geq 7$ a prime and under the condition that

$$Ax, By \text{ and } Cz \text{ are non-zero and pairwise coprime.}$$

Further we shall assume that A and B are ℓ-th power free and C is square free. Without loss of generality we may suppose that we are in one of the following situations:

(I) $ABCxy \equiv 1 \pmod 2$ and $y \equiv BC \pmod 4$;

(II) $xy \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(B) = 1$ or $\mathrm{ord}_2(C) = 1$;

(III) $xy \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) = 2$ and $z \equiv By/4 \pmod 4$;

(IV) $xy \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) \in \{3, 4, 5\}$ and $z \equiv C \pmod 4$;

(V) $\mathrm{ord}_2(By^\ell) \geq 6$ and $z \equiv C \pmod 4$.

In cases (I) and (II) we consider the curve

$$E_1 : Y^2 = X^3 + 2CzX^2 + BCy^\ell X.$$

In cases (III) and (IV) we consider

$$E_2 : Y^2 = X^3 + CzX^2 + \frac{BCy^\ell}{4}X,$$

and in case (V) we consider

$$E_3 : Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^\ell}{64}X.$$

Theorem 3.2.1. *(Bennett and Skinner [2]) With assumptions and notation as above, we have:*

(a) The minimal discriminant of E_i is given by

$$\Delta_i = 2^{\delta_i} C^3 B^2 A (xy^2)^\ell,$$

where

$$\delta_1 = 6, \quad \delta_2 = 0, \quad \delta_3 = 12.$$

(b) The conductor of the curve E_i is given by

$$N = 2^\alpha C^2 \operatorname{Rad}(ABxy),$$

where

$$\alpha = \begin{cases} 5 \text{ if } i = 1, \text{ case } (I); \\ 6 \text{ if } i = 1, \text{ case } (II); \\ 1 \text{ if } i = 2, \text{ case } (III), \ \operatorname{ord}_2(B) = 2 \text{ and } y \equiv -BC/4 \pmod 4; \\ 2 \text{ if } i = 2, \text{ case } (III), \ \operatorname{ord}_2(B) = 2 \text{ and } y \equiv BC/4 \pmod 4; \\ 4 \text{ if } i = 2, \text{ case } (IV) \text{ and } \operatorname{ord}_2(B) = 3; \\ 2 \text{ if } i = 2, \text{ case } (IV) \text{ and } \operatorname{ord}_2(B) = 4 \text{ or } 5; \\ 1 \text{ if } i = 3, \text{ case } (V) \text{ and } \operatorname{ord}_2(By^7) = 6; \\ 0 \text{ if } i = 3, \text{ case } (V) \text{ and } \operatorname{ord}_2(By^7) \geq 7. \end{cases}$$

(c) Suppose that E_i does not have complex multiplication (this would follow if we assume that $xy \neq \pm 1$). Then $E_i \sim_\ell f$ for some newform f of level $N_\ell = 2^\beta C^2 \operatorname{Rad}(AB)$ where

$$\beta = \begin{cases} \alpha \text{ cases } (I) - (IV); \\ 0 \text{ case (V) and } \operatorname{ord}_2(B) \neq 0, 6; \\ 1 \text{ case (V) and } \operatorname{ord}_2(B) = 0; \\ -1 \text{ case (V) and } \operatorname{ord}_2(B) = 6. \end{cases}$$

(d) The curves E_i have non-trivial 2-torsion.

(e) Suppose $E = E_i$ is a curve associated to some solution (x, y, z) of Equation (3.6) satisfying the above conditions. Suppose that F is another curve defined over $\mathbb{Q}$ such that $E \sim_\ell F$. Then the denominator of the j-invariant $j(F)$ is not divisible by any odd prime $q \neq \ell$ dividing C.

The following is a theorem that we will need for bounding exponents in Chapter 6.

Theorem 3.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and suppose that $t \mid |E(\mathbb{Q})_{\text{tors}}|$ (N.B. t does not have to be prime). Suppose that f is a newform of level N'. Let p be a prime such that $p \nmid N'$ and $p^2 \nmid N$. Let*

$$S_p = \{a \in \mathbb{Z} \text{ such that } -2\sqrt{p} \leq a \leq 2\sqrt{p}, \quad a \equiv p+1 \pmod{t}\}.$$

Let c_p be the p-th coefficient of f and define

$$B'_p(f) = \text{Norm}_{\mathbb{Q}_f/\mathbb{Q}}\left((p+1)^2 - c_p^2\right) \prod_{a \in S_p} \text{Norm}_{\mathbb{Q}_f/\mathbb{Q}}(a - c_p)$$

and

$$B_p(f) = \begin{cases} p \cdot B'_p(f) \text{ if } f \text{ is irrational,} \\ B'_p(f) \text{ if } f \text{ is rational.} \end{cases}$$

If $E \sim_\ell f$ then $\ell \mid B_p(f)$.

Proof. As $p \nmid N'$ and $p^2 \nmid N$ it follows that p is either a prime of good reduction or of multiplicative reduction for E. If p is a prime of good reduction it follows that

$$p + 1 - a_p(E) = |E(\mathbb{F}_p)| \equiv 0 \pmod{t},$$

with the $\pmod{t}$ equality coming from the fact that $t \mid |E(\mathbb{Q})_{\text{tors}}|$. Hence it follows that $a_p(E) \in S_p$, once we account for the Hasse bound.

If f is irrational then we may apply Theorem 3.1.6. If $\ell = p$ then the result follows obviously from the definition of $B_p(f)$. If however $p \nmid \ell N'$ and $p \,||\, N$ then $p + 1 \equiv \pm c_p \pmod{\lambda}$ for λ being some prime lying over ℓ, hence ℓ divides the first term in $B'_p(f)$. The only remaining case is $p \nmid \ell N N'$, in which case it follows from Theorem 3.1.6 that $a_p(E) \equiv c_p \pmod{\lambda}$. Hence if we take the product of the norms over all elements in S_p, it has to be divisible by ℓ.

If f is rational then we apply the same argument but using Lemma 3.1.7, however we do not need to consider the case that $p \mid \ell$. $\square$

Chapter 4

The Consecutive Erdős-Selfridge Curves

In this chapter we will explain what superelliptic curves are, show that several open problems in number theory can be written in terms of them and provide two examples of families that will be studied. Both of these families will be made up of arithmetic progressions. The Erdős-Selfridge curves will be constructed by taking products of terms in an arithmetic progression and asking if these products can ever be a perfect ℓ-th power. We will also consider curves that are made by summing powers of consecutive terms in arithmetic progression and determining if these can be perfect ℓ-th powers.

In this chapter we will also completely study the simplest case of the Erdős-Selfridge curves, in particular when the terms in the arithmetic progression are consecutive numbers. Our main result will be to improve that of Bennett and Siksek in [7], by proving it is possible to bound the exponent ℓ in terms of the number of terms in the arithmetic progression, even when some terms in the product are missing.

We shall do this by attaching Fermat equations to our curve, showing that it is possible to find one with a sufficiently nice radical. It is then a matter of applying Ribet's Level Lowering Theorem 3.1.4 to bound ℓ in terms of the radical.

§ 4.1 Introduction

In this section we will be interested in bounds of the exponent of superelliptic curves.

Definition 4.1.1 (Superelliptic curves)**.** A *superelliptic curve* is an equation of the

following form

$$y^\ell = f(x) \tag{4.1}$$

for ℓ a fixed constant integer and f a polynomial of degree k with ℓ and k greater than 2.

Definition 4.1.2. For an equation of the form

$$By^\ell = f(x),$$

we call ℓ the *exponent* of the equation.

For a fixed pair of integers (k, ℓ) and f a separable polynomial, such an equation defines a rational curve with genus at least

$$\frac{(k-2)(\ell-1)}{2}.$$

It follows that for $k+\ell > 6$, such a curve has genus greater than 1. Hence by Faltings's theorem there are only finitely many rational solutions for a fixed f and ℓ.

Theorem 4.1.3 (Faltings)**.** *If C is a non-singular algebraic curve over $\mathbb{Q}$ with genus greater than 1, then C has only finitely many rational points.*

Proof. See [21]. □

While Faltings's theorem is very strong, when we restrict ourselves to just the integer points of superelliptic curves, we can get the following much stronger statement.

Theorem 4.1.4 (Schinzel and Tijdeman)**.** *If $f(x) \in \mathbb{Z}[x]$ is a polynomial with at least 2 distinct roots, then the integer solutions to $y^\ell = f(x)$ satisfy either $y \in \{0, \pm 1\}$ or $\ell \leqslant \ell_0$ for some effectively computable constant $\ell_0 = \ell_0(f)$.*

Proof. See [48]. □

Remark 4.1.5. When we considered applying Faltings's theorem to superelliptic curves, we had to fix both ℓ and f, however the above theorem allows us to be a lot more general. Consider a superelliptic curve of the form $y^\ell = f(x)$. First consider the case when $y \in \{0, \pm 1\}$; then it is clear there are only finitely many x that can satisfy our superelliptic curve. It is also clear for any $\ell \leqslant \ell_0$ by Faltings's theorem there are only finitely many rational (hence integral) solutions to $y^\ell = f(x)$, showing that for a fixed f there are only finitely many integer pairs (x, y) such that $y^\ell = f(x)$.

It now follows that one might ask if it is possible to generalize this work to rational points.

4.1.6 (A question on the exponent bound for rational points on superelliptic curves)**.** *Does there exist a large set $\mathcal{F}$ of polynomials inside $\mathbb{Z}[x]$ such that the rational solutions of $y^\ell = f(x)$ satisfy either $y \in \{0, \pm 1\}$ or $\ell \leqslant \ell_0$ for some effectively computable constant $\ell_0 = \ell_0(f)$?*

This is a very difficult problem, and one that will not be solved in this thesis, however it is worthwhile thinking about as we proceed.

The bulk of this thesis is going to consider three different curves: two variants of the Erdős-Selfridge curves and the arithmetic progression curves. We will now define them below.

Definition 4.1.7 (The family of AP curves)**.** An *AP curve for k and d* is an equation of the form

$$y^\ell = (x-d)^k + x^k + (x+d)^k, \tag{4.2}$$

for k and d fixed integers.

Definition 4.1.8 (The family of Erdős-Selfridge curves)**.** An *Erdős-Selfridge curve of k and d* is an equation of the form

$$y^\ell = x(x+d)\dots(x+(k-1)d), \tag{4.3}$$

for k and d fixed integers.

Definition 4.1.9 (The family of Erdős-Selfridge Curve with a missing set and coefficient)**.** Let k, d and B be fixed integers. Further, let S be a subset of $[0, k-1]$. Set

$$f(x) = \prod_{i \in [0,k-1] \setminus S} (x + id), \tag{4.4}$$

then we call equations of the following type over $\mathbb{Q}$:

$$By^\ell = f(x) \tag{4.5}$$

the family of *Erdős-Selfridge curves of k and d with missing set S and coefficient B*. We shall write $ES(\ell, k, d, B, S)$ for the equation

$$By^\ell = \prod_{i \in [0,k-1] \setminus S} (x + id), \tag{4.6}$$

and write $I = [0, k-1] \setminus S$.

Remark 4.1.10. While is it possible to study the Erdős-Selfridge curves for any positive integer ℓ, we shall always restrict to the case that ℓ is a prime. From here onwards, unless explicitly stated otherwise, we shall always assume ℓ to be a prime number.

§ 4.2 The Erdős-Selfridge Curves for $d = 1$

We start our work by first considering the easiest of these curves, the Erdős-Selfridge curve with $d = 1$. The main theorem in this section is Theorem 4.2.2, improving Theorem 1.4.3 of Bennett, Siksek [7] and Theorem 1.4.4 of Das, Laishram and Saradha [14]. The sketch of this theorem is as follows. Using the perfect power structure of each factor in the product of the Erdős-Selfridge curve it is possible to attach many generalised Fermat equations to this superelliptic curve. In particular it is possible to attach Fermat equations of the form

$$au^\ell + bv^\ell + cw^\ell = 0,$$

such that the largest prime dividing abc is bounded by k. Additionally, it is shown that a prime p in a certain interval will divide exactly one of u, v or w, but none of the coefficients of the Fermat equation. This allows us to use Ribet's Level Lowering Theorem 3.1.4, Kraus's Lemma 3.1.10 and Lemma 3.1.11 to bound ℓ.

Definition 4.2.1. A pair $(x, y) \in \mathbb{Q}^2$ that lies on the curve $ES(\ell, k, 1, 1, S)$ is *non trivial* if $xy \neq 0$.

We now state our first theorem regarding the $d = 1$ case of the Erdős-Selfridge curve with missing terms.

Theorem 4.2.2. *Suppose $k \geq 27$ and S is a subset of $[0, k-1]$ that satisfies one of the following conditions*

(1) $S \subset [s, t] \subset [0, k-1]$ and $t - s < \frac{k}{18} - 1$;

(2) $|S| < \frac{1}{2} + 0.37\sqrt{\frac{k}{\log k}}$.

Then any non-trivial rational solution to $ES(\ell, k, 1, 1, S)$ satisfies $\log(\ell) < 3^k$.

Corollary 4.2.3. *Suppose $k \geq 3$ and S is a set with a single element, then any rational solution to $ES(\ell, k, 1, 1, S)$ satisfies $\log(\ell) < 3^k$.*

Proof. If $k \geq 27$ this follows from Theorem 4.2.2 in case (2). If $k \leq 26$, then this is covered by [14]. □

Remark 4.2.4. The case of $k \leq 26$ is dealt with in [14]. This relies on being able to create more Fermat identities and get stricter properties, in these more specific cases. From these stronger properties it is possible to prove the result using only identities with a maximum of two term products.

Remark 4.2.5. This corollary is the author's generalisation [18] of Theorem 1.1 of [14]. Further, this corollary will be generalised in Chapter 5 to a version that allows for a y coefficient B; this is the content of Remark 5.6.3.

In this section we will prove Theorem 4.2.2 and Corollary 4.2.3 following the method presented in [7]. We start this section by proving a result about Erdős-Selfridge curves in general, as we will need it in the following chapters. We demonstrate how a rational point on an Erdős-Selfridge curve gives rise to an integral solution on a different Erdős-Selfridge curve.

Lemma 4.2.6. *Let (x, y) be a rational solution of $ES(\ell, k, d, 1, S)$ with exponent $\ell > k$. Then there exists a d' such that d'/d is an ℓ-th power and $ES(\ell, k, d', 1, S)$ has an integral solution.*

Proof. Write $x = m/a$ and $y = n/b$ for a, b, m and n integers, such that m, a are coprime and n, b are coprime.

Then we may rewrite our solution to $ES(\ell, k, d, 1, S)$ as the following:

$$\frac{n^\ell}{b^\ell} = \frac{1}{a^{k-|S|}} \prod_{i \in [0,k-1] \setminus S} (m + iad). \tag{4.7}$$

By our assumption about coprimeness it then follows that $a^{k-|S|} = b^\ell$. As $\ell > k$ and ℓ is prime, this implies that a is an ℓ-th power. We shall write $a = c^\ell$ for some integer c. We now further simplify our equation to:

$$n^\ell = \prod_{i \in [0,k-1] \setminus S} (m + ic^\ell d). \tag{4.8}$$

Hence we now have an integral solution (m, n) with exponent ℓ of $ES(\ell, k, c^\ell d, 1, S)$. □

Hence to show that there is a bound for the exponent of the Erdős-Selfridge curve for rational points, we need to show there is a bound for each d, that does not depend on

d. We will apply two different methods depending on whether $d = 1$ or d is another integer.

The Erdős-Selfridge Curves for $d = 1$

Assume we have a putative rational solution to $ES(\ell, k, 1, 1, S)$. Then applying Lemma 4.2.6, we know that we have an integral solution (m, n) to $ES(\ell, k, c^\ell, 1, S)$ for some integer c, where m and c must be coprime.

We now write each term in the product of the Erdős-Selfridge curve as

$$m + ic^\ell = a_i x_i^\ell, \tag{4.9}$$

for $i \in I$ such that x_i is an integer and a_i is an ℓ-th power free integer.

Lemma 4.2.7. *If p is a prime that divides a_i as given by Equation (4.9) for some i, then $p \leq k$.*

Proof. Let p be a prime that divides a_i. Then as p must appear to an ℓ-th power in the product, but does not in the a_i term, it follows that there is a $j \neq i$ such that p also divides a_j for some $j \in I$. It now follows that p divides their difference, $(i - j)c^\ell$. If p divides c, then it must also divide m, contradicting them being co-prime. Hence p divides $i - j$, and therefore p is bounded by k. It now follows that all prime factors of a_i are bounded above by k. □

This is a really important observation, as when we construct Fermat equations later on, it is the primes dividing the a_i's that will make up the radical we see in the conductor of the Frey-Hellegouarch curves.

Lemma 4.2.8. *Suppose (m, n) is an integral solution of $ES(\ell, k, c^\ell, 1, S)$ with*

$$|S| < \frac{1}{2} + 0.37\sqrt{\frac{k}{\log k}} \text{ and } k \geq 22.$$

Then there exists a prime $\frac{1}{3}k \leq p \leq \frac{1}{2}k$ such that p divides either c or n.

Proof. Assume that no prime p in the range $[k/3, k/2]$, which is known to exist by Corollary 2.1.3, divides c, otherwise the result follows obviously. Such a prime must divide at least two and at most three of the terms $m + ic^\ell$ for $i \in [0, k - 1]$. If p does

not divide n, then there are at least 2 values of i such that $i \in S$. We will label these as i_p and $i_p + p$. It is then clear that p is in the set of differences of the elements in S. If we label the elements in $S = \{i_1, \ldots, i_L\}$, then it is easily seen that

$$|\{i_\alpha - i_\beta : 1 \leq \alpha < \beta \leq L\}| \leq \sum_{m=1}^{L-1} m = \frac{|S|^2 - |S|}{2}. \tag{4.10}$$

It then follows that if

$$\frac{|S|^2 - |S|}{2} < \pi(k/2) - \pi(k/3), \tag{4.11}$$

then there must be such a prime p as specified by the lemma.

For $k < 181000$ we can explicitly calculate, using Code 7.1, the following bound

$$0.07\frac{k}{\log(k)} < \pi(k/2) - \pi(k/3). \tag{4.12}$$

For $k \geq 181000$ we use the following bounds in [15]:

$$\frac{x}{\log(x) - 1} < \pi(x) \text{ for } x \geq 5393, \tag{4.13}$$

and

$$\pi(x) < \frac{x}{\log(x) - 1.1} \text{ for } x \geq 60184. \tag{4.14}$$

It is then simple algebraic manipulation to see that for $k \geq 181000$

$$\frac{k}{\log(k)} \left(\frac{1/2}{1 - \frac{1+\log(2)}{\log(k)}} - \frac{1/3}{1 - \frac{1.1+\log(3)}{\log(k)}} \right) < \pi(k/2) - \pi(k/3). \tag{4.15}$$

Elementary calculus shows that each of the two functions in k inside of the brackets is a decreasing function for $k > 9000$, which in particular is less than our bound for k and tends to their numerator.

Putting $k = 181000$ into inequality (4.15) we see that,

$$0.17\frac{k}{\log(k)} < \pi(k/2) - \pi(k/3). \tag{4.16}$$

We can therefore always use the bound given by inequality (4.12). It is now clear that if

$$\frac{|S|^2 - |S|}{2} < 0.07\frac{k}{\log(k)}, \tag{4.17}$$

then inequality (4.11) follows obviously.

It follows from solving the above quadratic equation, that if

$$|S| < \frac{1}{2} + 0.37\sqrt{\frac{k}{\log k}},$$

inequality (4.11) is true, completing the lemma. □

We will now present a lemma that will be required later to show that we have enough equations.

Lemma 4.2.9. *For t a fixed integer, α an integer, and p a prime greater than 3, let*

$$A_\alpha = \left\{ t+\alpha, t+\frac{2(p+\alpha)}{3}, t+p+\alpha, t+2p-2\alpha \right\}.$$

If α and α' are distinct integers both in $(0, p/2)$ and congruent to $-p \pmod 3$, then $A_\alpha \cap A_{\alpha'} = \emptyset$.

Remark 4.2.10. The condition that $\alpha \equiv -p \pmod 3$ is so that all the elements in A_α are integers.

Proof. Assume that $A_\alpha \cap A_{\alpha'} \neq \emptyset$. Label the elements in the set A_α as a_i for $i = 1, \ldots, 4$. Do similarly for $A_{\alpha'}$, labelling these elements as a'_i. For $i = 1, 3, 4$ we can work $\pmod 3$ and see that

$$a_1 \equiv t - p \pmod 3, \quad a_3 \equiv t \pmod 3, \quad a_4 \equiv t + p \pmod 3.$$

As $p > 3$, it follows that if $a_i = a'_j$ for $i, j \neq 2$, then $i = j$. If $a_i = a'_j$ for $i, j \neq 2$, it follows that $\alpha = \alpha'$, giving a contradiction. Hence, after possibly swapping α and α', we can assume that either $a_1 = a'_2$, $a_3 = a'_2$ or $a_4 = a'_2$.

Case (1) : $a_1 = a'_2$.

It follows that $3\alpha = 2p + 2\alpha'$, hence $\alpha > 2p/3$, contradicting $\alpha \in (0, p/2)$.

Case (2) : $a_3 = a'_2$.

It follows that $p + 3\alpha = 2\alpha'$, hence $\alpha' > p/2$, contradicting $\alpha' \in (0, p/2)$.

Case (3) : $a_4 = a'_2$.

It follows that $2p = \alpha' + 3\alpha$, which would imply that $2p < p/2 + 3p/2$, giving a contradiction. □

We will now use this lemma to construct Fermat equations that come from the solution of $ES(\ell, k, c^\ell, 1, S)$ superelliptic curves.

Lemma 4.2.11. *For $k \geq 27$ and S a subset of $[0, k-1]$ that satisfies one of the following*

(1) $S \subset [s, t] \subset [1, k]$ and $t - s < \frac{k}{18} - 1$;

(2) $|S| < \frac{1}{2} + 0.37\sqrt{\frac{k}{\log k}}$,

suppose that $ES(\ell, k, 1, 1, S)$ has a non-trivial rational point (x, y). Then there exists a prime $\frac{1}{3}k \leq p \leq \frac{1}{2}k$ such that there are non-zero integers a, b, c, u, v, w satisfying

$$au^\ell + bv^\ell + cw^\ell = 0 \tag{4.18}$$

such that

(I) a, b, c are ℓ-th power free integers;

(II) all prime factors of abc are less than or equal to k;

(III) $p \nmid abc$;

(IV) p divides precisely one of u, v, w.

Proof. Under the hypotheses of the lemma, we can apply Lemma 4.2.6 to find an integral solution (m, n) of $ES(\ell, k, d^\ell, 1, S)$. There exists a prime p in the interval $[k/3, k/2]$ such that p divides either d or n.

In case (1), if p does not divide d then there are atleast two terms in the arithmetic progression that are divisible by p. They are atleast $k/3$ terms apart, which is bigger than $|S|$, hence atleast one of them appears in the product. Hence either at least one of the terms in (4.9) is divisible by p or p divides d. In case (2) it follows from Lemma 4.2.8.

It is clear that if p does not divide d, then p can divide at most 3 distinct factors of (4.8). We will deal with the cases of p dividing exactly 0, 1, 2 and 3 terms individually.

We first deal with the case that p divides d. Noting that in every case $|S| < k/2$, it follows that there is an i such that i and $i+1 \notin S$. Hence, by subtracting two identities given in equation (4.9) we see that

$$a_i x_i^\ell - a_{i+1} x_{i+1}^\ell + d^\ell = 0.$$

The lemma now follows.

We now deal with the case that p divides exactly one factor, which we take to be $n+id^\ell$. We consider the identity

$$(n + id^\ell) - (n + jd^\ell) = (i - j)d^\ell,$$

for j a positive integer less than k such that $|i - j| < p$. Because $|S| < p - 1$, it follows that there exists a $j \notin S$, hence $(n + jd^\ell)$ appears as a factor in (4.8). As p must divide $n + id^\ell$ to an ℓ-th power, applying (4.9), we then get an equation satisfying the lemma, i.e.

$$a_i x_i^\ell - a_j x_j^\ell - (i - j)d^\ell = 0.$$

We now consider the case that p divides exactly two factors, $n + id^\ell$ and $n + (i + p)d^\ell$. We consider a similar identity as before,

$$(n + id^\ell)(n + (i + p)d^\ell) - (n + (i + \alpha)d^\ell)(n + (i + p - \alpha)d^\ell) = \alpha(\alpha - p)d^{2\ell},$$

for α a positive integer less than p.

It is clear that for distinct α and $\alpha' \leq p/2$, then $\{i+\alpha, i+p-\alpha\} \cap \{i+\alpha', i+p-\alpha'\} = \emptyset$. Hence, as $|S| < p/2 - 1$ there exists α such that both $n + (i+\alpha)d^\ell$ and $n + (i+p-\alpha)d^\ell$ appear as factors in (4.8). Hence the result now follows from (4.9) and the same finishing argument as above.

We are left to deal with the case that p divides exactly three factors, $n+id^\ell$, $n+(i+p)d^\ell$ and $n + (i + 2p)d^\ell$.

We point out the following identity:

$$\begin{aligned} 3\alpha(\alpha - p)(n + (i + \tfrac{2(p+\alpha)}{3})d^\ell)d^{2l} &= (n + id^\ell)(n + (i + p)d^\ell)(n + (i + 2p)d^\ell) \\ &\quad - (n + (i + \alpha)d^\ell)(n + (i + p + \alpha)d^\ell)(n + (i + 2p - 2\alpha)d^\ell), \quad (4.19) \end{aligned}$$

defined for α a positive integer less than p with $\alpha \equiv -p \pmod 3$.

From Lemma 4.2.9 we know that for α and α' in the interval $(0, p/2)$, then

$$\{t+\alpha, t+\tfrac{2(p+\alpha)}{3}, t+p+\alpha, t+2p-2\alpha\} \cap \{t+\alpha', t+\tfrac{2(p+\alpha')}{3}, t+p+\alpha', t+2p-2\alpha'\} = \emptyset.$$

Hence it follows that there are more than $\frac{p}{6}-1$ distinct values of α with $\alpha \equiv -p \pmod 3$, such that the terms in (4.19) involving α don't coincide with the terms involving i. So we see from the size of S that we have more choices of α than terms deleted, hence at least one α will give us such an equation with all terms defined. □

We now state a lemma which follows from [7].

Remark 4.2.12. The following proof is not materially different from the one given by Bennett and Siksek in [7], but has been included here for completeness.

Lemma 4.2.13. *If a, b, c, u, v, w are non-zero integers satisfying*

$$au^\ell + bv^\ell + cw^\ell = 0, \tag{4.20}$$

$k \geq 27$ is a fixed integer and $\frac{1}{3}k \leq p \leq \frac{1}{2}k$ is a prime such that

(1) a, b, c are ℓ-th power free integers;

(2) all prime factors of abc are less than or equal to k;

(3) $p \nmid abc$;

(4) p divides precisely one of u, v, w;

(5) $\ell > k$ is prime.

Then

$$\log \ell \leq \frac{(N'+1)}{6} \log(\sqrt{p}+1),$$

where $N' = 2^4 \operatorname{Rad}_2(abc)$.

Proof. Without loss of generality we permute the three terms and change signs so that

$$au^\ell \equiv -1 \pmod 4 \text{ and } bv^\ell \equiv 0 \pmod 2.$$

We now attach the Frey-Hellegouarch curve

$$E : Y^2 = X(X - au^\ell)(X + bv^\ell).$$

Using Ribet's Level Lowering Theorem 3.1.4 it follows that there exists a level lowered modular form f of level N', with

$$N' \mid 2^5 \operatorname{Rad}_2(abc).$$

It follows from Properties (2) and (3) that

$$\operatorname{Rad}_2(abc) \mid \prod_{q \leq k, q \neq p} q,$$

taken over primes q.

As E has multiplicative reduction at p, but p does not divide abc, we may use Lemma 3.1.6 (2). It follows that $p + 1 \equiv \pm c_p \pmod{\lambda}$, for c_p the p-th coefficient of f and λ a prime lying over ℓ in $K = \mathbb{Q}_f$. It is now clear that ℓ divides $\operatorname{Norm}_{K/\mathbb{Q}}(p + 1 \pm c_p)$. Using the bound for $c_p < 2\sqrt{p}$ in all real embeddings it follows that

$$\ell < (p + 1 + 2\sqrt{p})^{[K:\mathbb{Q}]}.$$

It is an elementary fact that $[\mathbb{Q}_f : \mathbb{Q}]$ is less than or equal to the dimension of the space of cuspidal newforms containing f.

We now apply Lemma 3.1.11 to see that

$$[K : \mathbb{Q}] \leq \frac{N' + 1}{12}.$$

Taking logs of the expression bounding ℓ, the result now follows. □

Proof of Theorem 4.2.2. It follows immediately from Lemma 4.2.11 and Lemma 4.2.13 that

$$\log \ell \leq \tfrac{(N'+1)}{6} \log(\sqrt{p} + 1),$$

where

$$N' < 2^5 \prod_{q \leq k, q \neq p} q.$$

Using Theorem 2.1.9 we can now bound N',

$$N' < 2^5 \exp(1.000081k).$$

It now follows that

$$\log \ell \leq \frac{2^5}{3} \log(\sqrt{k-1}+1) \exp(1.000081k).$$

We can bound the non-exponential part of the above product by $\exp(\beta k)$ for some β. Using the standard fact that exponentials grow slower than logarithms, we can find the β that works for $k = 27$. In this case we can take $\beta = 0.084$. It now follows that

$$\log \ell \leq \exp((1.000081 + 0.084)k) < 3^k,$$

finishing the theorem. □

Chapter 5

Erdős-Selfridge Curves for General d

In this chapter we will consider the Erdős-Selfridge curves for a general d. The ideas in this chapter are generalizations of those given by Bennett and Siksek in [6]. The case of general d, while seeming very similar to that seen in the previous chapter, has to be handled entirely differently. This is because if we try copying the methods in the previous section exactly for a general d, we would no longer be able to guarantee a bound on the prime factors of the coefficients in the Fermat equations. In particular as we change the d, the prime factors that would appear change as well.

We generalize the work in [6] by considering curves where elements in the product are missing or there is a coefficient in front of the power. The broad outline of the method is to start by attaching many Fermat equations to our Erdős-Selfridge curves. Using standard techniques in the study of Fermat equations we attach Frey-Hellegouarch curves to these. These will allow us to show that either ℓ is bounded or d must have specific divisibility properties. Further we will show that it is possible to attach characters to these Frey-Hellegouarch curves. We will then classify the characters into one of four categories. It is then possible to show that there are bounds on the number of characters in three of these classifications. Finally we show that in all cases we violate one of these bounds on our conductors, contradicting the assumption of a solution.

There will be six sections in this chapter. In Section 5.1 we will show how to attach Frey-Hellegouarch curves to our Erdős-Selfridge curves. This is very similar to the previous chapter, however we will need slightly different identities, so that the d in our

curve does not appear in the coefficients of our Fermat equations. Further we shall show that provided that k is sufficiently large and ℓ sufficiently large depending on k, then there will be a level-lowered rational elliptic curve with full 2-torsion and a predetermined bounded conductor. This will follow from applications of Lemma 4.2.13 and Kraus's Theorem 3.1.10.

In Section 5.2 we develop the idea in [6], showing how to attach characters to the curves given in Section 5.1. These will be vital for further study, as they allow us to transform the problem from one of algebraic number theory into a more analytical analogue. In particular we will show that the absolute value of the inner product sum of a character and the Von-Mangoldt function can be bounded below linearly in k; this is Theorem 5.2.5. This will become very important in Section 5.4 when we are calculating properties of non-smooth characters.

In Section 5.3 we distinguish three subsets of the set of all characters, developed for an Erdős-Selfridge curve, these classes are non necessarily disjoint. The desired outcome of this section is to show that there can't be too many characters with prescribed properties on their conductors. The three classes will be labelled as the super smooth set, the smooth set and the non-smooth set. The super smooth set will be the set of characters whose conductors are bounded by $\log(k)^2$. In Lemma 5.3.2, it will be shown that they do not exist for k sufficiently large; while this is not useful in itself, it will be required when studying smooth characters. The smooth characters will be those with largest prime divisor of their conductor bounded by $\log(k)$. In the smooth characters subsection we measure the number of characters that we have by looking at the sum of the inverse of the largest prime in the conductor. We will show that for k sufficiently large, we can make this sum as small as we want to; in the proof of this we will have to apply the non-existence of super smooth characters from the previous subsection (this is Theorem 5.3.4). Finally we shall consider the non-smooth characters. These will be characters such that the largest prime dividing their conductor is bounded by a power of k and whose conductor is bounded by a power of k. We will show that the size of the set of such characters grows with k at a rate of order $\log(k)$. This is Theorem 5.3.6.

In Section 5.4 we prove Theorem 5.4.1. This theorem shows that for k sufficiently large and S a subset of primes with a bounded harmonic sum, then we can find a character with sufficiently nice properties, including bounded conductor, bounding the largest prime in the conductor and such that no primes that divide the conductor are in the set S. The proof of this follows from sieving off characters that violate the given properties and then showing combinatorially that there is a non-empty subset with size

that grows at least as fast as a multiple of k.

In Section 5.5 we create a subset of all characters that can be found using what we know from Section 5.4. We then apply the results from Section 5.3 regarding the number of "nice" characters that we can have. It is a straightforward argument to show that our produced subset violates one of the theorems in Section 5.3, allowing us to conclude by contradiction that k is bounded.

In Section 5.6 we explicitly consider different variations of Erdős-Selfridge curves allowing us to prove our main theorem.

§ 5.1 Attaching Frey-Hellegouarch Curves

In this section we will consider the integral solutions of $ES(\ell, k, d, B, S)$. More specifically we will attach Fermat equations to

$$By^\ell = \prod_{i\in[0,k-1]\setminus S} (x + id),$$

and study the properties of d as k and ℓ get large. Recall the earlier definition:

Definition 5.1.1. We say that a pair of integers (n, m) are a *non-trivial integral solution* to $ES(\ell, k, d, B, S)$ if $mn \neq 0$, $\gcd(n, d) = 1$ and

$$Bm^\ell = \prod_{i\in[0,k-1]\setminus S} (n + id). \tag{5.1}$$

Remark 5.1.2. For the rest of this chapter we will only be interested in non-trivial integral solutions, and will assume throughout that if not specifically mentioned we are referring to non-trivial integral solutions. Further recall our convention that $[0, k-1] \setminus S = I$.

Lemma 5.1.3. *Suppose there is a non-trivial integral solution (n, m) to $ES(\ell, k, d, B, S)$ with ℓ prime, then*

(I) for $0 \leq i < j \leq k-1$, $\gcd(n + id, n + jd) \mid (j - i)$;

(II) let $i \in I$ and $q \geq k$ be prime such that $q \nmid B$, then $\ell \mid \mathrm{ord}_q(n + id)$.

Thus we may write

$$n + id = a_i y_i^\ell \text{ for } i \in I, \tag{5.2}$$

where the a_i are positive integers divisible only by primes $< k$ or primes dividing B, whereas the y_i are divisible only by primes $\geq k$.

Proof. For part (I), let g be a the greatest common divisor of $n+id$ and $n+jd$, then it follows that g also divides $(i-j)d$. If $\gcd(g,d) = h > 1$, then h must also divide n, but this contradicts the assumption that the solution is non-trivial, hence g divides $i-j$.

For part (II), let q be such a prime. Then from part (I), it is clear that there is at most one i such that $\mathrm{ord}_q(n+id) \neq 0$ and as $q \nmid B$, it follows that $q \mid y$.

It now follows simply that the only prime factors that divide $n+id$ but not to an ℓ-th power must be either less than k or dividing B. □

5.1.1 Fermat Equations of Signature (ℓ, ℓ, ℓ)

In this subsection we will show that by picking triples of $(i,j,k) \in I^3$ we can construct Fermat equations of signature (ℓ,ℓ,ℓ). We will further show that there is a mod ℓ level lowered modular form attached to these Fermat equations. In particular the level of these modular forms can be bounded depending only on k and B, but not on d. These bounds will be vital in proving that the prime factors of d will have special properties. We will construct two different Fermat equations; the first is applicable in the case that $S = \emptyset$ and is the same as in [6]. In the case that $S \neq \emptyset$ we will use the same identity as in the previous chapter, however we will require some condition on d to make it applicable to our needs.

We will use the arithmetic information given to us by Equation (5.2), with the following identity.

Given any integers $0 \leq i_1 < i_2 < i_3 \leq k-1$, we have the following identity

$$(i_3 - i_2)(n+i_1 d) + (i_1 - i_3)(n+i_2 d) + (i_2 - i_1)(n+i_3 d) = 0, \tag{5.3}$$

which combined with (5.2) gives rise to a Fermat equation of signature (ℓ,ℓ,ℓ) as we will show below.

Let $\mathcal{A} = \{(i,j,2j-i) \text{ s.t. } i,j,2j-i \in I \text{ and } i<j\}$ denote the set of non-trivial 3-term arithmetic progressions in the set I. Associated to any such tuple $\mathbf{a} = (i,j,2j-i) \in \mathcal{A}$ is the identity

$$(n+id) - 2(n+jd) + (n+(2j-i)d) = 0.$$

From Lemma 5.1.3 and the above identity, we see that $(r, s, t) = (y_i, y_j, y_{2j-i})$ is a solution of the following generalized Fermat equation of signature (ℓ, ℓ, ℓ):

$$a_i r^\ell - 2a_j s^\ell + a_{2j-i} t^\ell = 0.$$

We may now attach a Frey-Hellegouarch curve as in Kraus [31]. If we take

$$g = \gcd(n + id, n + jd, n + (2j - i)d)$$

and

$$a_{\mathbf{a}} = \frac{n + id}{g}, \quad b_{\mathbf{a}} = \frac{-2(n + jd)}{g}, \quad c_{\mathbf{a}} = \frac{n + (2j - i)d}{g},$$

then we can associate the following Frey-Hellegouarch curve, $E_{\mathbf{a}}$, to $\mathbf{a}$ by

$$E_{\mathbf{a}} : Y^2 = X(X - a_{\mathbf{a}})(X + c_{\mathbf{a}}).$$

Remark 5.1.4. It is worthwhile pointing out here that by any mention of $\mathbf{a}$ we always mean a non-trivial 3 term arithmetic progression with its terms in I. It is important to note that this is different from [6], where the terms in the arithmetic progression are in the more general interval $[0, k - 1]$.

Lemma 5.1.5. *The model $E_{\mathbf{a}}$ is minimal and semistable at all odd primes. Its discriminant is*

$$\Delta_{\mathbf{a}} = 16(a_{\mathbf{a}} b_{\mathbf{a}} c_{\mathbf{a}})^2.$$

In particular for any prime $p \geq k$ and $p \nmid B$, we have $\ell | \operatorname{ord}_p(\Delta_{\mathbf{a}})$.

Proof. This follows from applying Tate's algorithm. We calculate the b invariants of $E_{\mathbf{a}}$:

$$b_2 = 4(c_{\mathbf{a}} - a_{\mathbf{a}}), \quad b_4 = -2a_{\mathbf{a}} c_{\mathbf{a}}, \quad b_6 = 0, \quad b_8 = -(a_{\mathbf{a}} c_{\mathbf{a}})^2.$$

From this we calculate the discriminant of $E_{\mathbf{a}}$ to be,

$$\Delta_{\mathbf{a}} = 16(a_{\mathbf{a}} b_{\mathbf{a}} c_{\mathbf{a}})^2.$$

Let p be an odd prime that divides $a_{\mathbf{a}} c_{\mathbf{a}}$. Then p divides the X and constant coefficient of $E_{\mathbf{a}}$. As $\gcd(a_{\mathbf{a}}, c_{\mathbf{a}}) \mid 2$, it follows $p \nmid b_2$. Hence we apply the first two steps of Tate's algorithm to show that p is semistable.

If $p \mid b_{\mathbf{a}}$, then we use the change of variable

$$X \to X + a_{\mathbf{a}}.$$

Repeating the above argument implies that $E_{\mathbf{a}}$ is semistable at all odd primes.

The final part of this lemma now follows from applying Lemma 5.1.3. □

Definition 5.1.6. For a positive integer M we will define $P(M)$ to be the largest prime dividing M.

Lemma 5.1.7. *Let $\ell \geq 7$. Then $\overline{\rho}_{E_{\mathbf{a}},\ell} \sim \overline{\rho}_{f,\ell}$ where f is a newform of weight 2 and level $M_{\mathbf{a}}$, with*

$$M_{\mathbf{a}} | 2^8 a_i a_j a_{2j-i}. \tag{5.4}$$

It then follows that

$$M_{\mathbf{a}} \leq 2^7 \cdot \exp(1.000081 \max(k, P(B))). \tag{5.5}$$

Proof. As $E_{\mathbf{a}}$ has full 2-torsion and $\ell \geq 7$, it follows $E_{\mathbf{a}}[\ell]$ is irreducible. We apply Theorem 3.1.4, giving a modular form f of weight 2 and level M_0 such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$, for

$$M_0 = M / \prod_{\substack{q || M,\ q \text{ prime} \\ \ell | \mathrm{ord}_q(\Delta)}} q.$$

Equation (5.4) follows immediately from the discriminant of $E_{\mathbf{a}}$.

We can explicitly bound M_0 by applying Lemma 5.1.5. It follows that

$$M_0 \mid 2^7 \prod_{\substack{q \leq \max(k, P(B)) \\ q \text{ prime}}} q.$$

We now apply Theorem 2.1.9 to bound this product, giving the result. □

We now state the three term identities we used in the previous chapter. We will not be able to apply these for all d, as we will not be able to bound the radical of the coefficients. However, if we write $d = d_1 d_2^{\ell}$ with d_1 being an ℓ-th power free integer, then it will become clear that if $P(d_1) < k$, then we can apply the usual methods. These equations will be useful when we deal with the case that S is non-empty.

We now construct a different Fermat equation of signature (ℓ, ℓ, ℓ) via the product of three terms. Let p be a prime in the domain $(k/3, k/2]$, and let γ be an integer in

$(0, p/2]$ such that $\gamma \equiv -p \pmod 3$. Then we have the following identity:

$$\begin{aligned}(n+id)(n+(i+p)d)(n+(i+2p)d)&\\ -(n+(i+\gamma)d)(n+(i+p+\gamma)d)(n+(i+2p-2\gamma)d)&\\ = 3\gamma(\gamma-p)\left(n+\left(i+\frac{2(p+\gamma)}{3}\right)d\right)d^2.&\quad (5.6)\end{aligned}$$

Remark 5.1.8. This identity is essentially the same as Identity (4.19) in Chapter 4, except it picks up a factor of d^2 on the right hand side.

Using Equation (5.2) this can be simplified to a solution of

$$a_i a_{i+p} a_{i+2p} x^\ell - a_{i+\gamma} a_{i+p+\gamma} a_{i+2p-2\gamma} y^\ell = 3\gamma(\gamma-p) d_1^2 a_{i+\frac{2(p+\gamma)}{3}} z^\ell,$$

where $(x, y, z) = (y_i y_{i+p} y_{i+2p}, y_{i+\gamma} y_{i+p+\gamma} y_{i+2p-2\gamma}, d_2^2 y_{i+\frac{2(p+\gamma)}{3}})$.
We may now attach a Frey-Hellegouarch curve as in Kraus [31] and above. If we take

$$g = \gcd(a_i a_{i+p} a_{i+2p} x^\ell, a_{i+\gamma} a_{i+p+\gamma} a_{i+2p-2\gamma} y^\ell, 3\gamma(\gamma-p) d_1^2 a_{i+\frac{2(p+\gamma)}{3}} z^\ell), \quad (5.7)$$

$$\zeta = (i, i+p, i+2p, i+\gamma, i+p+\gamma, i+2p-2\gamma), \quad (5.8)$$

$$a_\zeta = \frac{(n+id)(n+(i+p)d)(n+(i+2p)d)}{g}, \quad (5.9)$$

$$b_\zeta = \frac{(n+(i+\gamma)d)(n+(i+p+\gamma)d)(n+(i+2p-2\gamma)d)}{g} \text{ and} \quad (5.10)$$

$$c_\zeta = \frac{3\gamma(\gamma-p)(n+(i+\frac{2(p+\gamma)}{3})d)d^2}{g}, \quad (5.11)$$

then we can associate the following Frey-Hellegouarch curve, E_ζ, to ζ by

$$E_\zeta : Y^2 = X(X-a_\zeta)(X-c_\zeta).$$

Lemma 5.1.9. *The model E_ζ is minimal and semistable at all odd primes. Its discriminant is*

$$\Delta_\zeta = 16(a_\zeta b_\zeta c_\zeta)^2.$$

It follows that for any prime $p \geq k$ that doesn't divide $d_1 B$, we have $\ell | \operatorname{ord}_p(\Delta_\zeta)$.

Proof. This proof is the same as for Lemma 5.1.5, except primes dividing d_1 appear in

the coefficients of the attached Fermat equation. □

Lemma 5.1.10. *Let $\ell \geq 7$. Then $\overline{\rho}_{E_\zeta,\ell} \sim \overline{\rho}_{f,\ell}$ where f is a newform of weight 2 and level M_ζ, with*

$$M_\zeta | 2^8 a_i a_{i+p} a_{i+2p} a_{i+\gamma} a_{i+p+\gamma} a_{i+2p-2\gamma} 3\gamma(\gamma-p) a_{i+\frac{2(p+\gamma)}{3}} d_1. \tag{5.12}$$

Let q be the largest prime dividing $a_i a_{i+p} a_{i+2p} a_{i+\gamma} a_{i+p+\gamma} a_{i+2p-2\gamma} 3\gamma(\gamma-p) a_{i+\frac{2(p+\gamma)}{3}} d_1$. Then

$$M_\zeta \leq 2^7 \cdot \exp(1.000081q). \tag{5.13}$$

In particular, if the greatest prime factor of d_1 is less than k then we have the bound

$$M_\zeta \leq 2^7 \cdot \exp(1.000081 \max(k, P(B))).$$

Proof. This proof is the same as the one given for Lemma 5.1.7. □

Remark 5.1.11. As in the previous chapter we have $k/18 - 1$ choices for ζ, as implied by Lemma 4.2.9.

5.1.2 Fermat Equations of Signature $(\ell, \ell, 2)$.

Using the arithmetic information given by Equation (5.2) we will construct Fermat equations of signature $(\ell, \ell, 2)$. Let

$$\mathcal{I} = \{(j_1, i_1, i_2, j_2) \in I^4 \text{ s.t. no pair of terms are equal and } i_1 + i_2 = j_1 + j_2\}. \tag{5.14}$$

Then in Section 3.2 of [6] it is shown how to attach to each $\mathbf{i} \in \mathcal{I}$ a Frey-Hellegouarch elliptic curve $\mathcal{E}_\mathbf{i}$ in the following way.

For any fixed quadruple $\mathbf{i} \in \mathcal{I}$, we see that the following identity holds:

$$(n + j_1 d)(n + j_2 d) - (n + i_1 d)(n + i_2 d) = (j_1 j_2 - i_1 i_2) d^2.$$

It follows that $(r, s, t) = (y_{j_1} y_{j_2}, y_{i_1} y_{i_2}, d)$ is a solution to the following generalized Fermat equation with signature $(\ell, \ell, 2)$:

$$a_{j_1} a_{j_2} r^\ell - a_{i_1} a_{i_2} s^\ell = (j_1 j_2 - i_1 i_2) t^2.$$

In [8], Bennett and Skinner showed how to attach Frey-Hellegouarch elliptic curves to such equations over $\mathbb{Q}$. We set the following notation

$$C = (n + j_1 d)(n + j_2 d),\ D = (n + i_1 d)(n + i_2 d) \text{ and } \kappa = j_1 j_2 - i_1 i_2. \tag{5.15}$$

With this notation we have

$$C - D = \kappa d^2. \tag{5.16}$$

We now define the following elliptic curve:

$$\mathcal{E}_{\mathbf{i}} : Y^2 = X(X^2 + 2\kappa d X + \kappa C).$$

Lemma 5.1.12. *The model $\mathcal{E}_{\mathbf{i}}$ is minimal and semistable at all primes $p \geq k$ that also satisfy $p \nmid \kappa$. It has discriminant*

$$\Delta_{\mathbf{i}} = -64\kappa^3 C^2 D.$$

In particular, for any prime $p \geq k$ with $p \nmid \kappa B$, we have $\ell \mid \mathrm{ord}_p(\Delta_{\mathbf{i}})$.

Proof. The first statement is a short application of Tate's algorithm. We start by calculating the b invariants of the elliptic curve $\mathcal{E}_{\mathbf{i}}$:

$$b_2 = 8\kappa d, \quad b_4 = 2\kappa C, \quad b_6 = 0, \quad b_8 = -(\kappa C)^2.$$

It follows that the discriminant is

$$\Delta_{\mathbf{i}} = -64\kappa^3 C^2 D.$$

Let $p \geq k$ be a prime that does not divide κ, then if p does not divide C or D it follows that p is a prime of good reduction for $\mathcal{E}_{\mathbf{i}}$. We now deal with the two cases that $p \mid C$ or $p \mid D$.

We will re-write our elliptic curve in the standard notation

$$\mathcal{E}_{\mathbf{i}} : Y^2 = X^3 + \alpha_2 X^2 + \alpha_4 X,$$

with $\alpha_2 = 2\kappa d$ and $\alpha_4 = \kappa C$.

Case (1) : $p \mid C$**.** In this case $p \mid \alpha_4$, so we may apply step (2) of Tate's algorithm. As d and C are coprime, and $p \nmid 8\kappa$, it follows that $p \nmid b_2$. Hence, Tate's algorithm terminates on the second step, showing that p is a semistable prime.

Case (2) : $p \mid D$**.** We may assume that $p \nmid C$, as otherwise we could apply case (1). It follows that $p \nmid \alpha_4$, so we must change coordinates to apply Tate's algorithm. By using the change of coordinates

$$X \to X - \kappa d,$$

we find another model for $\mathcal{E}_{\mathbf{i}}$ given by:

$$\mathcal{E}_{\mathbf{i}} : Y^2 = X^3 - \kappa d X^2 + \kappa D X - \kappa^2 d D.$$

In this model $p \mid \alpha_4$, so we may apply step (2) of Tate's algorithm. In these coordinates $b_2 = -4\kappa d$. As D and d are coprime, it follows that $p \nmid b_2$, hence by Tate's algorithm, p is a prime of semistable reduction.

The final line of the lemma now follows from applying Lemma 5.1.3. □

Lemma 5.1.13. *Let $\ell \geq 11$. Then $\overline{\rho}_{\mathcal{E}_{\mathbf{i}},\ell} \sim \overline{\rho}_{f,\lambda}$ where f is a newform of weight 2 and level $M_{\mathbf{i}}$ satisfying*

$$M_{\mathbf{i}} \leq 2^7 \cdot 3^5 \cdot k^4 \cdot \exp(2.000162 \max(k, P(B))).$$

Proof. As $E_{\mathbf{i}}$ has a rational 2-torsion point and $\ell \geq 11$, it follows $E_{\mathbf{i}}[\ell]$ is irreducible. We apply Theorem 3.1.4, giving a modular form f of weight 2 and level M_0 such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$, for

$$M_0 = M / \prod_{\substack{q \| M,\ q \text{ prime} \\ \ell \mid \mathrm{ord}_q(\Delta)}} q.$$

We may now bound M_0 by applying Lemma 5.1.12. It follows that

$$M_0 \mid 2^7 \cdot 3^5 \cdot \kappa^2 \cdot \prod_{\substack{q \leq \max(k, P(B)) \\ q \text{ prime}}} q^2.$$

As $|\kappa| < k^2$, applying Theorem 2.1.9, the result now follows. □

5.1.3 Further properties of $E_{\mathbf{a}}$

We now use bound (5.5), Theorem 3.1.10 and Lemma 3.1.11, to find level lowered elliptic curves attached to our Frey-Hellegouarch curves.

Lemma 5.1.14. *Suppose that there exists a non-trivial solution of $ES(\ell, k, d, B, S)$. Let $\mathbf{a} \in \mathcal{A}$. Then for $k > 10^{10}$ and $\ell > \exp(10^{\max(k,P(B))})$ there is an elliptic curve $F_{\mathbf{a}}/\mathbb{Q}$ having full rational 2-torsion and conductor $M_{\mathbf{a}}$ such that $\overline{\rho}_{E_{\mathbf{a}},\ell} \sim \overline{\rho}_{F_{\mathbf{a}},\ell}$.*

Proof. By Theorem 3.1.10, it is sufficient to show that $\ell > H(M_{\mathbf{a}})$ for $M_{\mathbf{a}}$ the level of the modular form attached to $E_{\mathbf{a}}$ in Lemma 5.1.7. It is seen from Theorem 9 of [57] that

$$\prod_{\substack{q \leq k \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right) \leq \exp\left(0.27 + \frac{5}{\log(k)}\right) \log(k).$$

For $k > 10^{10}$ we see that

$$\prod_{\substack{q \leq k \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right) \leq 2 \log(k).$$

Combining this with Lemma 5.1.7 we now get that $\mu(M_{\mathbf{a}})$ and $\mu(\mathrm{lcm}(M_{\mathbf{a}}, 4))$ are bounded by

$$2^8 \log(\max(k, P(B))) \exp(1.000081 \max(k, P(B))),$$

which we shall denote as U.

Using Lemma 3.1.11 it then follows that to calculate an upper bound for $H(M_{\mathbf{a}})$ we only need to calculate $F(U)$ using the exponent $\frac{M_{\mathbf{a}}+1}{12}$ instead of g_0^+, for F as given in Lemma 3.1.10.

Taking logs it then follows that

$$\log(H(M_{\mathbf{a}})) \leq \frac{M_{\mathbf{a}} + 1}{6} \log\left(\sqrt{\frac{U}{6}} + 1\right).$$

Using $\log(1 + x) < x$ it then immediately follows that

$$\begin{aligned} \log(H(M_{\mathbf{a}})) &\leq \frac{M_{\mathbf{a}} + 1}{6} \sqrt{\frac{U}{6}} \\ &< 2^{21/2} \cdot 3^{-1/2} \exp(1.000081 \cdot 1.5 \max(k, P(B))) \sqrt{\log(\max(k, P(B)))} \end{aligned}$$

It now follows for $k > 10^{10}$ that $\ell > H(M_{\mathbf{a}})$, and applying Theorem 3.1.10, this completes the proof. □

5.1.4 Results regarding d

Here we show that under certain hypotheses all primes in a specified interval must divide d.

Lemma 5.1.15. *For $k > 10^{10}$, suppose that (n, m) is a non-trivial integral solution to $ES(\ell, k, d, B, \emptyset)$,*

$$Bm^{\ell} = \prod_{i=0}^{k-1}(n + id), \tag{5.17}$$

such that $p \nmid B$ for all primes in $[k/2, k]$.

Then for $\ell > \exp(10^{\max(k,P(B))})$ it follows that all primes $p \in (k/2, k]$ divide d.

Proof. Let p be such a prime and assume that $p \nmid d$. Then p must divide at least one of the terms $n + id$ and at most two of the terms. Suppose that p divides exactly one such term, $n + i_p d$ say. Let $\mathbf{a}$ be any $\mathbf{a} \in \mathcal{A}$ which contains the term i_p. It follows from the fact that $p \nmid B$ that

$$\ell \mid \mathrm{ord}_p(n + id).$$

Now let $E_{\mathbf{a}}$ be the elliptic curve attached to $\mathbf{a}$ by Lemma 5.1.5. It follows from Lemma 5.1.5 that $E_{\mathbf{a}}$ is semistable at p with multiplicative reduction, and that $\ell \mid \mathrm{ord}_p(\Delta_{\mathbf{a}})$.

We are now in a position to apply Lemma 4.2.13, from which it follows that

$$\ell \leq (\sqrt{p} + 1)^{\frac{M_{\mathbf{a}+1}}{6}}.$$

Now using Lemma 5.1.7 to bound

$$M_{\mathbf{a}} \leq 2^7 \exp(1.000081 \max(k, P(B))),$$

it follows simply that for k sufficiently large

$$\log \ell < 3^{\max(k,P(B))}.$$

Now suppose that p divides exactly 2 terms, $n + i_p d$ and $n + (i_p + p)d$. Choose an $\mathbf{i} \in \mathcal{I}$ that contains both i_p and $i_p + p$ as one of the pairs. Attach the elliptic curve $\mathcal{E}_{\mathbf{i}}$ as

given by Lemma 5.1.12. It is clear that $p \nmid \kappa$ and so it follows that $\mathcal{E}_{\mathbf{i}}$ has multiplicative reduction at p.

Similarly to above, but using Lemma 5.1.13 it follows that,

$$\log \ell < 10^{\max(k,P(B))},$$

completing the lemma. □

We have now shown that if the exponent ℓ is large enough then we have some control over the primes that divide d, in particular all primes in the range $(k/2, k]$ divide d. We have also seen that for ℓ sufficiently large we cannot only level lower each elliptic curve attached to an arithmetic progression in $\mathcal{A}$ to a modular form, but further to an elliptic curve with full 2-torsion. Both of these properties will be vital in the next section where we use them to attach characters to our arithmetic progression.

Lemma 5.1.16. *For k sufficiently large, suppose that (n, m) is a non-trivial integral solution to $ES(\ell, k, d, B, S)$, and that*

(1) B not divisible by any prime in the domain $(k/3, k/2]$;

(2) $S = \{j\}$ a singleton;

(3) $v_p(d) \equiv 0 \pmod{\ell}$ for all primes p greater than k.

Then for $\ell > \exp(10^{\max(k,P(B))})$ it follows that any prime $p \in [k/3, k/2]$ divides d.

Remark 5.1.17. It is clear from the work in Chapter 4 that this theorem also applies when dealing with the rational solutions of Erdős-Selfridge curves with $d = 1$.

Proof. Let p be a prime in the interval $(k/3, k/2]$ and assume that p does not divide d. From condition (2) it follows that there is an $i \in I$ such that $p \mid (n + id)$. If p divides exactly one term in the right hand side of

$$Bm^{\ell} = \prod_{i \neq j} (n + id),$$

it follows from condition (1) that

$$\ell \mid \operatorname{ord}_p(n + id).$$

Let $\mathbf{a}$ be any triple of indices in $\mathcal{A}$ containing i. It follows from Lemma 5.1.5 that $E_{\mathbf{a}}$ is semistable at p with multiplicative reduction, and that $\ell \mid \mathrm{ord}_p(\Delta_{\mathbf{a}})$. Applying Lemma 4.2.13, we see that

$$\ell \leq (\sqrt{p}+1)^{\frac{M_{\mathbf{a}}+1}{6}}.$$

Applying the bound for $M_{\mathbf{a}}$ given by Lemma 5.1.7 contradicts our assumption that $\ell > \exp(10^{\max(k,P(B))})$.

We now deal with the case that p divides exactly two terms. Assume that p divides $n+id$ and $n+(i+p)d$, then let $\mathbf{i} = (j_1, i, i+p, j_2)$ be any quadruple in $\mathcal{I}$. Then from Lemma 5.1.12 and Lemma 5.1.13 we see that this contradicts our bound on ℓ.

Now assume that p divides exactly 3 terms $n+id$, $n+(i+p)d$ and $n+(i+2p)d$. Let γ be an integer in $(0, p/2)$ such that $\gamma \equiv -p \pmod 3$ and $\zeta \in I^6$ as given by Equation (5.8). Using condition (3) we now construct E_ζ as given in Lemma 5.1.9. Now applying Lemma 5.1.10 and the same arguments as above we conclude

$$\ell \leq (\sqrt{p}+1)^{\frac{M_{\mathbf{a}}+1}{6}}.$$

However this contradicts our assumption that $\ell > \exp(10^{\max(k,P(B))})$. □

§ 5.2 Attaching Characters

To understand the Erdős-Selfridge curves we will prove the following statement about arithmetic progressions.

Theorem 5.2.1. *Let $S \subset [0, k-1]$ with $|S| < 0.25k$. Further, let d be an integer divisible by all primes p in the interval $(k/t', k/t]$ for fixed $t' > 1.06t$ and $t \geq 1$. Let B be a positive constant not divisible by any primes in the interval $(k/t', k/t]$. If k is larger than a constant that depends only on t and t' and there is a non-trivial solution to $ES(\ell, k, d, B, S)$, then*

$$\ell < \exp(10^k).$$

Remark 5.2.2. The value of 1.06 appearing in the theorem is so that bounds later are positive. In particular we will need to use this number in Theorem 5.2.5 and 5.3.2. It is in fact possible to pick an even better bound of $t' > 1.012t$.

Lemma 5.2.3. *Under the same conditions as Lemma 5.1.14, with the hypothesis of Theorem 5.2.1 and $k > 10^{10}$, let p be a prime in the interval $(k/t', k/t]$. If $p \nmid M_{\mathbf{a}}$ then*

p is a prime of good reduction for both $E_{\mathbf{a}}$ and $F_{\mathbf{a}}$, and we have $a_p(E_{\mathbf{a}}) = a_p(F_{\mathbf{a}})$. If, moreover, $p \equiv 3 \pmod 4$, then $a_p(F_{\mathbf{a}}) = 0$ and hence p is a prime of supersingular reduction for $F_{\mathbf{a}}$.

Remark 5.2.4. The following proof is not substantially different from that given for Lemma 5.2 in [6], with no real changes apart from the interval of primes considered, however it has been included here for clarity and ease of reading.

Proof. By the hypothesis of 5.2.1 it follows that every prime p in $(k/t', k/t]$ divides d. As n and d are coprime it follows that p doesn't divide any of the A_i. It hence follows by Lemma 5.1.5 that $E_{\mathbf{a}}$ has good reduction at p and it also follows that p is a prime of good reduction for $F_{\mathbf{a}}$ given by Lemma 5.1.14. Hence by Lemma 3.1.6 it follows that $a_p(E_{\mathbf{a}}) \equiv a_p(F_{\mathbf{a}}) \pmod \ell$. Applying the Hasse-Weil bounds we see that

$$|a_p(E_{\mathbf{a}}) - a_p(F_{\mathbf{a}})| \leq 4p \leq 4k.$$

It now follows that $a_p(E_{\mathbf{a}}) = a_p(F_{\mathbf{a}})$, as by the hypothesis of Lemma 5.1.14 ℓ is bigger than $4k$.

From our definition of the Frey-Hellegouarch curves $E_{\mathbf{a}}$ it is clear that $\pmod p$ the curve becomes

$$Y^2 = X(X - n/g)(X + n/g).$$

If $p \equiv 3 \pmod 4$ then it follows that $a_p(E_{\mathbf{a}}) = 0$ and hence also $a_p(F_{\mathbf{a}}) = 0$. □

From now on we shall take $F_{\mathbf{a}}$ to be the elliptic curve over $\mathbb{Q}$ associated to $\mathbf{a}$ by Lemma 5.1.14. For a positive integer N, we shall take $N^{\text{odd}} = N \cdot 2^{-\text{ord}_2(N)}$ for the odd part of N. Further we will take Λ to be the usual von Mangoldt function as given in Definition 2.3.13.

Theorem 5.2.5. *Let $k \geq t' \times 10^{10}$ and suppose that equation (**??**) holds. Let $\mathbf{a} \in \mathcal{A}$ and assume $\ell > \exp(10^k)$. Then there exists a quadratic character $\chi_{\mathbf{a}}$ that is primitive of conductor $N_{\mathbf{a}}$ such that*

$$\left| \sum_{k/t' < m \leq k/t} \chi_{\mathbf{a}}(m)\Lambda(m) \right| \geq \frac{(t' - t - \epsilon(t + t'))}{\varphi(8)tt'} k > \beta k, \tag{5.18}$$

for $\beta > 0$ and $\epsilon = 0.002811$. Moreover, we have that $N_{\mathbf{a}}^{\text{odd}} | M_{\mathbf{a}}$ and $N_{\mathbf{a}}^{\text{odd}} \neq 1$.

Further the character $\chi_{\mathbf{a}}$ is constant on the set of primes of some $\pmod 8$ *congruence class in the interval* $(k/t', k/t]$.

Remark 5.2.6. This theorem is identical to Proposition 6.1 in [6]. The only differences are cosmetic, being the change in the interval of summation, which leads to a change in bound. Additionally the final statement in the theorem is new; however it requires no changes to the original proof to achieve.

Definition 5.2.7. For every $\lambda \in \mathbb{Q} \setminus \{0, 1\}$, the elliptic curve

$$G_\lambda : Y^2 = X(X-1)(X-\lambda),$$

is called a *Legendre elliptic curve.*

Remark 5.2.8. It is important to note that λ is not unique and there are 6 possible choices for λ. In particular if λ is one of the invariants, define the following three values

$$\lambda_1 = \lambda,\ \lambda_2 = (1-\lambda) \text{ and } \lambda_3 = \frac{\lambda - 1}{\lambda}; \tag{5.19}$$

then all of the λ invariants can be given as one of $\{\lambda_1^{\pm 1}, \lambda_2^{\pm 1}, \lambda_3^{\pm 1}\}$, [54, pg. 50].

Remark 5.2.9. Further, as both G_λ and $F_{\mathbf{a}}$ have full 2-torsion, it follows that $F_{\mathbf{a}}$ is a quadratic twist of some G_λ.

Definition 5.2.10 (Subsets of $\mathcal{A}$)**.** Define the following set

$$\mathcal{G} = \{-t^2 : t \in \mathbb{Q}\} \cup \{2t^2 : t \in \mathbb{Q}\}.$$

We partition the set $\mathcal{A}$ into two disjoint subsets, $\mathcal{A}^{(I)}$ and $\mathcal{A}^{(II)}$.

$\mathcal{A}^{(I)}$ is the subset of $\mathbf{a} \in \mathcal{A}$ such that at least one of the λ-invariants of $F_{\mathbf{a}}$ lies outside $\mathcal{G}$.

$\mathcal{A}^{(II)}$ is the complement of $\mathcal{A}^{(I)}$, hence contains the $\mathbf{a} \in \mathcal{A}$ such that all λ-invariants of $F_{\mathbf{a}}$ lie inside $\mathcal{G}$.

Lemma 5.2.11. *Let $F/\mathbb{Q}$ be an elliptic curve of conductor M, semistable away from 2, having full rational 2-torsion. Let $\lambda \in \mathbb{Q}$ be any of the six λ-invariants of F. Then the following hold.*

(1) $\mathrm{ord}_p(\lambda) = \mathrm{ord}_p(1-\lambda) = 0$ *for all odd primes p of good reduction for F.*

(2) Let $\omega \in \{\pm 1, \pm 2\}$ and let χ be the unique primitive quadratic character of conductor N which satisfies

$$\chi(p) = \left(\frac{\omega\lambda}{p}\right)$$

for odd primes p with $\mathrm{ord}_p(\lambda) = 0$. Then $N^{\mathrm{odd}} \mid M$.

Proof. Lemma 6.2 in [6]. □

Lemma 5.2.12. *Let $p \equiv 3 \pmod 4$ be prime and suppose that $F/\mathbb{F}_p$ is an elliptic curve of the form*

$$F : Y^2 = X(X-1)(X-\eta^2)$$

for some $\eta \in \mathbb{F}_p \setminus \{0, 1, -1\}$. Then $F(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proof. Lemma 6.3 in [6]. □

Lemma 5.2.13. *Let $k \geq 10^{10}$ and suppose that $\ell > \exp(10^k)$ is a prime. Assume that there is a non-trivial solution to the curve given in Theorem 5.2.1. Let $\mathbf{a} \in \mathcal{A}$ and let λ be any of the λ-invariants of $F_{\mathbf{a}}$. If $p \equiv 3 \pmod 8$ is a prime in the interval $(k/t', k/t]$ then*

$$\left(\frac{\lambda}{p}\right) = -1$$

Proof. From Lemma 5.2.3 we know that p is a good prime of supersingular reduction. The proof now follows identically to Lemma 6.4 in [6]. □

Attaching the character for $\mathbf{a} \in \mathcal{A}^{(I)}$

For $\mathbf{a} \in \mathcal{A}^{(I)}$, let λ be any of the associated λ-invariants that isn't in $\mathcal{G}$. Assume for contradiction that λ is either t^2 or $-2t^2$ for $t \in \mathbb{Q}^\times$. Then it follows that

$$\left(\frac{\lambda}{p}\right) = 1$$

for all primes $p \equiv 3 \pmod 8$ in the interval $(k/t', k/t]$. Lemma 5.2.13 therefore implies that there are no primes in the interval $(k/t', k/t]$ that are congruent to 3 (mod 8). However applying Lemma 2.2.5, we see that as $k \geq t' \cdot 10^{10}$ we have reached a contradiction, so

$$\lambda \notin \{\pm t^2 : t \in \mathbb{Q}\} \cup \{\pm 2t^2 : t \in \mathbb{Q}\}.$$

Using Lemma 5.2.13 and Equation (2.4) it follows that

$$\sum_{\substack{k/t'<p\leq k/t \\ p\equiv 3 \pmod 8}} -\left(\frac{\lambda}{p}\right)\log(p) \geq \frac{(t'-t-\epsilon(t+t'))}{\varphi(8)tt'}k. \tag{5.20}$$

Let μ_i be the primitive quadratic Dirichlet characters which on odd primes $p \nmid \lambda$ satisfy

$$\mu_1(p) = \left(\frac{\lambda}{p}\right),\ \mu_2(p) = \left(\frac{-\lambda}{p}\right),\ \mu_3(p) = \left(\frac{2\lambda}{p}\right) \text{ and } \mu_4(p) = \left(\frac{-2\lambda}{p}\right).$$

As shown in [6],

$$\mu_1(p) - \mu_2(p) - \mu_3(p) + \mu_4(p) = \begin{cases} 4\left(\frac{\lambda}{p}\right) & \text{if } p \equiv 3 \pmod 8 \\ 0 \text{ otherwise.} \end{cases}$$

Rewrite inequality (5.20) as

$$\sum_{\substack{k/t'<p\leq k/t \\ p\equiv 3 \pmod 8}} (-\mu_1(p) + \mu_2(p) + \mu_3(p) - \mu_4(p))\log(p) \geq \frac{4(t'-t-\epsilon(t+t'))}{\varphi(8)tt'}k.$$

It follows that for some i, there is a μ_i such that

$$\left|\sum_{k/t'<p\leq k/t} \mu_i(p)\log(p)\right| \geq \frac{(t'-t-\epsilon(t+t'))}{\varphi(8)tt'}k.$$

We then take the character $\chi_{\mathbf{a}} = \mu_i$ as the character required for Theorem 5.2.5.

As each term

$$\left(\frac{1}{p}\right),\ \left(\frac{-1}{p}\right),\ \left(\frac{2}{p}\right) \text{ and } \left(\frac{-2}{p}\right),$$

is determined by the congruence class of $p \pmod 8$, it follows using Lemma 5.2.13 that $\chi_{\mathbf{a}}(p)$ is constant on the set of primes $p \equiv 3 \pmod 8$ in the interval $(k/t', k/t]$.

Attaching the character for $\mathbf{a} \in \mathcal{A}^{(II)}$

In this subsubsection we will show how to attach characters when $\mathbf{a} \in \mathcal{A}^{(II)}$ such that they satisfy Theorem 5.2.5. This is similar to the case $\mathbf{a} \in \mathcal{A}^{(I)}$, except with some additional complications. This too was first explained in [6] and is here to improve understanding in this document.

Let $\mathbf{a} \in \mathcal{A}^{(II)}$, then by definition every λ-invariant of $F_{\mathbf{a}}$ lies in $\mathcal{G}$. If $\lambda = -w^2$, then it follows simply that $\lambda_2 = 2v^2$ for some rational v. If $\lambda = 2w^2$ for some rational value w then it follows that one of λ_2 or λ_3 can be written as $2v^2$ for a rational v. Hence after possibly relabelling we see that

$$\lambda = 2w^2 \text{ and } 1 - \lambda = 2v^2. \tag{5.21}$$

Lemma 5.2.14. *Let $k \geq 10^{10}$ and suppose that $\ell > \exp(10^k)$ is prime. Assume that there is a non-trivial integral solution to the curve given in Theorem 5.2.1. Let $\mathbf{a} \in \mathcal{A}$ and λ be one of the λ-invariants of $F_{\mathbf{a}}$. Suppose further that λ satisfies* (5.21) *for positive rational numbers w and v. If $p \equiv 5 \pmod 8$ is prime with $k/t' < p \leq k/t$, then* $\mathrm{ord}_p(w) = \mathrm{ord}_p(v) = 0$ *and*

$$\left(\frac{wv}{p}\right) = 1.$$

Proof. This is Lemma 6.6 in [6]. □

We are now in a position to describe the character constructed. We take $\chi_{\mathbf{a}}$ to be a primitive quadratic character which for odd primes away from the support of wv is given by

$$\chi_{\mathbf{a}} = \left(\frac{\omega wv}{p}\right),$$

for some $\omega \in \{\pm 1, \pm 2\}$ that depends only on $\mathbf{a}$. This ω is chosen similar to in the previous subsection; it is the character that gives us the largest absolute value sum.

It is now clear that for primes $p \equiv 5 \pmod 8$ in $(k/t', k/t]$ that $\chi_{\mathbf{a}}(p)$ is constant.

The proof of Theorem 5.2.5 now follows similarly to the case of $\mathbf{a} \in \mathcal{A}^{(I)}$ except it involves slightly more details. See [6, pg. 15–16], but will not be repeated here, as we only wanted to highlight the construction of the characters and the final statement in Theorem 5.2.5.

§ 5.3 Classifying Characters

In this section we will study three subsets of all of the characters. These are in some sense separated by the smoothness of the conductor of the characters.

The first are what we will call super smooth characters, whose conductor is bounded by $\log(k)^2$. These characters would have much smaller conductor compared to the others that arise. In fact we will show that if one does exist then this bounds k. While we cannot show that one will always be created, allowing us to prove Theorem 5.2.1 immediately, we will use them in the next subsection to complete a proof by contradiction.

The second are characters such that the largest prime in the conductor is bounded by $\log(k)$. Here we show that if there are too many of them, then k must be bounded.

The third are characters with conductor and largest prime factor bounded by a power of k. Again we show that if there are too many, then k must also be bounded.

The purpose of this section is to show that the three subsets that we consider cannot be too large.

5.3.1 Super Smooth Characters

Definition 5.3.1. For χ a character as given by Theorem 5.2.5, we call it *super smooth* if $P(N(\chi)) < (\log\log k)^{\lambda'}$ for $\lambda' < 1$, with N as given by Definition 2.3.6.

Lemma 5.3.2. *Let χ be a super smooth character given by Theorem 5.2.5, then k is bounded in terms of t and t'.*

Proof. As χ is given by Theorem 5.2.5 it follows that there is an i such that for all primes p in the interval $(k/t', k/t]$ with $p \equiv i \pmod 8$, then

$$\chi(p) = \left(\frac{\mu}{p}\right)$$

is constant on such primes in the interval $(k/t', k/t]$.

Writing μ as a product of even and odd parts $\mu = \mu^{\text{even}}\mu^{\text{odd}}$ it follows simply from quadratic reciprocity and that quadratic residues of ± 1 and ± 2 are determined $\pmod 8$ that

$$\left(\frac{p}{\mu^{\text{odd}}}\right)$$

is constant. For all p in the interval congruent to $i \pmod 8$, write

$$\left(\frac{p}{\mu^{\text{odd}}}\right) = j.$$

Then it follows from Equation (2.4) and the above explanation of j that

$$\frac{k(t'-t-\epsilon(t+t'))}{\varphi(8)tt'} \leq \theta(k/t;i,8) - \theta(k/t';i,8) \tag{5.22}$$

$$= \sum_{\substack{a \pmod{8\mu^{\text{odd}}} \text{ s.t.} \\ a \equiv i \pmod 8, \\ \left(\frac{a}{\mu^{\text{odd}}}\right)=j}} \theta(k/t;a,8\mu^{\text{odd}}) - \theta(k/t';a,8\mu^{\text{odd}}). \tag{5.23}$$

Hence it follows that there exists an a such that

$$|\theta(k/t;a,8\mu^{\text{odd}}) - \theta(k/t';a,8\mu^{\text{odd}})| \geq \frac{2k(t'-t-\epsilon(t+t'))}{\varphi(8\mu^{\text{odd}})tt'}, \tag{5.24}$$

as there are $\varphi(\mu^{\text{odd}})/2$ many classes $\pmod{\mu^{\text{odd}}}$ for a given quadratic residue, and 4 $\pmod 8$ residues.

From Theorem 2.2.6 we see that

$$\theta(k/t;a,8\mu^{\text{odd}}) - \theta(k/t';a,8\mu^{\text{odd}}) \leq \frac{k(t'-t)}{tt'\varphi(8\mu^{\text{odd}})} + \frac{k}{840}\left(\frac{1}{t\log(k/t)} - \frac{1}{t'\log(k/t')}\right). \tag{5.25}$$

Combing Equations (5.24) and (5.25) and cancelling the k terms we see that

$$\frac{t'-t-2\epsilon(t+t')}{tt'\varphi(8\mu^{\text{odd}})} \leq \frac{1}{840}\left(\frac{1}{t\log(k/t)} - \frac{1}{t'\log(k/t')}\right).$$

From the bound on t and t' it follows that the numerator is positive. We now want to bound $\varphi(\mu^{\text{odd}})$. It follows from elementary considerations that $\varphi(\mu^{\text{odd}}) \leq \mu^{\text{odd}}$. As χ is primitive it follows that $\mu^{\text{odd}} = N^{odd}(\chi)$. Using the condition that χ is super smooth

and applying Theorem 2.1.9 it now follows that

$$N(\chi) \leq \exp(1.000081(\log\log k)^{\lambda}).$$

It now follows that $\varphi(\mu^{\text{odd}}) < (\log k)^{\lambda'}$, for $\lambda' < 1$.

It is clear that the left hand side tends to 0 more slowly than the right hand side. This contradicts the inequality, hence k is bounded in terms of t and t'. □

5.3.2 Smooth Characters

In this part we are going to show that there cannot be too many characters such that the largest prime in their conductor is bounded by $\log(k)^{1-\epsilon}$ for $\epsilon > 0$. We will not however count the number of characters with this property in the usual manner; instead, we will consider the sum of the reciprocal of the largest prime in the conductor of the characters. This might not immediately seem like the obvious thing to take, however it has its advantages, namely it is more amenable to the analytic methods that we developed earlier in Section 2.3. It also makes sense as we would expect characters with smaller conductors to be more likely to violate our bounds, in particular as seen in the previous subsection, so they should receive a greater weight in our sum.

Definition 5.3.3. For χ a character as given by Theorem 5.2.5, we call it *smooth* if $P(N(\chi)) < \log(k)^{\lambda'}$ for $\lambda' < 1$.

Theorem 5.3.4. *Fix $0 < c_1 < 1$ and $\epsilon_0 > 0$. Suppose that there is a subset $\mathcal{D}$ of $\mathcal{A}$ such that the following hold:*

(I) $P(N_{\mathbf{a}}) \neq P(N_{\mathbf{a}'})$ *for all* $\mathbf{a} \neq \mathbf{a}' \in \mathcal{D}$;

(II) $P(N_{\mathbf{a}}) < \log(k)^{1-c_1}$ *for all* $\mathbf{a} \in \mathcal{D}$;

(III)

$$\sum_{\mathbf{a}\in\mathcal{D}} \frac{1}{P(N_{\mathbf{a}})} \geq \epsilon_0.$$

Then there exists an effectively computable constant k_1, depending only on c_1 and ϵ_0, such that $k \leq k_1$.

Remark 5.3.5. The above theorem is a generalisation of Proposition 7.2 in [6]. Our proofs start in the same way, however whereas [6] uses a geometric sum and work of

Platt [39] to bound the sum of reciprocals of primes; we instead bound the size of $\mathcal{D}$ and using bounds for the harmonic sum of primes are able to achieve a lower bound. In [6] the bound on the harmonic sum is 0.166, here it is lowered to any non-negative number.

Proof. Suppose that there is some $\mathbf{a} \in \mathcal{D}$ such that the character $\chi_{\mathbf{a}}$ is non-exceptional (as defined in Theorem 2.3.9). Then it follows by Lemma 2.3.12 and condition (II) that $\log(N_{\mathbf{a}}) < 1.07(\log(k))^{1-c_1}$. We now apply Theorem 2.3.16 to see that

$$\sum_{k/t'<m\leq k/t} \chi_{\mathbf{a}}(m)\Lambda(m) = O((k/t)\exp(-c'(\log(k/t))^{c_1})(\log(k/t))^4),$$

for some effectively computable positive constant c', contradicting Theorem 5.2.5 for k large enough.

We therefore assume that $\chi_{\mathbf{a}}$ is exceptional for every $\mathbf{a}$ in $\mathcal{D}$. Hence, we obtain a sequence of exceptional conductors

$$N_1 < N_2 < \ldots < N_s,$$

where $s = |\mathcal{D}|$. From Corollary 2.3.10 we get that $N_j > N_1^{2^{j-1}}$. Taking logs of both sides when $j = s$, applying Lemma 2.3.12 and condition (II), we see that

$$1.07 \log k > 1.07 P(N_s) > \log N_s > 2^{s-1} \log N_1.$$

Hence it follows that $s < 2 \log\log k$.

Let p be the minimal prime in the set $\{P(N_{\mathbf{a}}) \text{ s.t. } \mathbf{a} \in \mathcal{D}\}$. Let p_j be the sequence of all prime numbers, $p_1 = 2$, $p_2 = 3$, and so on, and let i be such that $p_i = p$. Then it is clear that

$$\sum_{m=i}^{i+s} \frac{1}{p_m} \geq \sum_{\mathbf{a}\in\mathcal{D}} \frac{1}{P(N_{\mathbf{a}})} \geq \epsilon_0.$$

We can now bound this left hand side using Theorem 2.1.13.

It now follows that

$$\log\left(\frac{\log(p_{i+s})}{\log(p_i)}\right) > \epsilon_0 - \frac{2}{\log^2(p_i)}.$$

If

$$\frac{\epsilon_0}{2} > \epsilon_0 - \frac{2}{\log^2(p_i)},$$

then it follows that

$$p_i < \exp\left(\frac{2}{\sqrt{\epsilon_0}}\right).$$

Note that this bound is independent of k.

We now assume that

$$\epsilon_0 - \frac{1}{\log^2(p_i)} \geq \frac{\epsilon_0}{2},$$

hence it follows that $p_{i+s} \geq p_i^{\exp(\epsilon_0/2)}$.

It is now seen that $2\log\log k > s = \pi(p_{i+s}) - \pi(p_i) \geq \pi(p_i^{\exp(\epsilon_0/2)}) - \pi(p_i)$. Using Theorem 2.1.10, we have

$$\begin{aligned}\pi(p_i^{\exp(\epsilon_0/2)}) - \pi(p_i) > &\frac{p_i^{\exp(\epsilon_0/2)}}{\exp(\epsilon_0/2)\log(p_i)}\left(1 + \frac{1}{2\exp(\epsilon_0/2)\log(p_i)}\right)\\ &- \frac{p_i}{\log(p_i)}\left(1 + \frac{3}{2\log(p_i)}\right).\end{aligned}$$

It follows that if $p_i > (\log\log k)^\lambda$ where $\lambda > 1/\exp(\epsilon_0/2)$, then k is bounded. Hence we can assume that $p_i < (\log\log k)^\lambda$ where $\lambda < 1$. However by applying Lemma 5.3.2 we see that k is bounded. □

5.3.3 Non-Smooth Characters

In the last two sections we showed that if we have suitably many $\mathbf{a}$ with a very small $N_\mathbf{a}$ or $P(N_\mathbf{a})$, then k is effectively bounded. In this section we show that with more $\mathbf{a}$ we can loosen the condition on how smooth the conductor of $\chi_\mathbf{a}$ can be and still get a bound on k.

Theorem 5.3.6. *Suppose that $c_2 > 10$ is a constant and that there exists a subset $\mathcal{B} \subset \mathcal{A}$ such that*

(I) $|\mathcal{B}| > 2\beta^{-2}\log(k)$ (N.B. this is the same β as in Theorem 5.2.5);

(II) for every distinct pair $\mathbf{a}, \mathbf{a}' \in \mathcal{B}$ we have $\chi_\mathbf{a} \neq \chi_{\mathbf{a}'}$;

(III) for all $\mathbf{a} \in B$ we have $P(N_\mathbf{a}) \leq k^{47/99}$;

(IV) for all $\mathbf{a} \in B$ we have $N_\mathbf{a} < k^{c_2}$.

Then there is an effectively computable constant k_2, depending only upon c_2, such that $k \leq k_2$.

This theorem is a generalisation of Proposition 8.1 in [6]. We have increased the exponent in condition (III) from 7/16 to 47/99, at a cost of increasing the size of $|\mathcal{B}|$.

Theorem 5.3.7. *Let $c_2 > 0$ be a constant. Then there exist effectively computable positive constants k_3 and c_3, each depending only on c_2, such that the following holds. Let $k \geq k_3$ be an integer and suppose that χ_1 and χ_2 are distinct primitive quadratic characters modulo N_1 and N_2 respectively, where the N_i satisfy*

$$P(N_i) \leq k^{47/99},\ N_i \leq k^{c_2},\ N_1N_2 \neq p_1p_2p_3 \text{ for distinct primes } p_j.$$

Then

$$\left| \sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) \right| \leq k^{1-c_3}.$$

Remark 5.3.8. The proof of this theorem involves two cases, one where the conductor of the product of characters is small enough to be bounded by a trivial sum. The other is to apply Theorem 2.3.18 when the conductor has sufficiently many prime factors. While the condition on N_1N_2 may seem contrived, it is required as it is the situation that is not covered by these two cases. However it will not have any major effect on our proof of Theorem 5.3.6 as there is a simple way to avoid all such characters.

Proof. Let $\chi = \chi_1\chi_2$ and write M for the conductor of χ, which divides $\text{lcm}(N_1, N_2)$ and inparticular $M \leq \text{lcm}(N_1, N_2)$. We can thus rewrite $\chi = \eta\psi$ where η is primitive of conductor M_1 and ψ is principal of conductor M_2 with $M = M_1M_2$ and $\gcd(M_1, M_2) = 1$. As η is quadratic, we see that M_1^{odd} is square free. Clearly, $M_2 \mid \gcd(N_1, N_2)$, and so M_2^{odd} is also square free. The following two inequalities follow:

$$P(M) \leq k^{47/99} \text{ and } M \leq k^{2c_2}. \tag{5.26}$$

We split this problem up into three distinct cases as discussed in the above remark.

Case (1): There are exactly 2 primes dividing M.

M either equals $2^a p$ or $p \cdot q$ for p and q distinct odd primes. Using that $P(N_i) \leq k^{47/99}$

for $i = 1, 2$ and $a \leq 3$, then it follows that $M < P(N_1)P(N_2) < k^{98/99}$. Hence

$$\left| \sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) \right| \leq M < k^{98/99},$$

for k sufficiently large, because the sum of values of a character of given conductor can at most be that conductor.

Case (2): There are exactly 3 primes dividing M.

As M_1 and M_2 are coprime and the odd parts of M_1 and M_2 are squarefree, it follows M either equals $2^a pq$ or pqr for p, q and r distinct odd primes. If $M = 2^a pq$ then it follows that $M < 2^a P(N_1)P(N_2) < 2^a k^{98/99}$, and for k large enough that $M < k^{98.5/99}$, and so the theorem follows by the above argument. So, suppose that $M = pqr$. If $M_2 = 1$ then it is clear that $N_1 N_2 = pqr$ contradicting our assumptions. So we now assume that $M_2 \neq 1$, hence M_1 is at most a product of 2 primes, and it follows that $M_1 \leq k^{98/99}$.

$$\begin{aligned}
\sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) &= \sum_{k/t' < m \leq k/t} \eta(m)\psi(m) \\
&= \sum_{\substack{k/t' < m \leq k/t \\ \gcd(m, M_2) = 1}} \eta(m) \\
&= \sum_{k/t' < m \leq k/t} \eta(m) \sum_{d \mid \gcd(m, M_2)} \mu(d) \\
&= \sum_{d \mid M_2} \sum_{k/t' < nd \leq k/t} \eta(nd)\mu(d) \\
&= \sum_{d \mid M_2} \eta(d)\mu(d) \sum_{k/(t'd) < n \leq k/td} \eta(n).
\end{aligned}$$

As η is non-principal and has conductor $M_1 < k^{98/99}$, we have

$$\left| \sum_{k/(t'd) < m \leq k/(td)} \eta(m) \right| < M_1 < k^{98/99}.$$

Thus

$$\left| \sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) \right| \leq \tau(M_2) k^{98/99} \leq 8k^{98/99},$$

where τ denotes the usual number of divisor function.

Case (3): There are 4 or more primes dividing M.

We will deal with this case using a slight modification of the proof of Theorem 8.2 in [6]. We will split this case into two subcases, $M_1 \geq 8k^{47/198}$ or $M_1 < 8k^{47/198}$.

Case (3.1) $M_1 \geq 8k^{47/198}$.

It follows that $M_1^{\text{odd}} \geq k^{47/198}$. We factorise the characters η and ψ as

$$\eta = \pi_1 \dots \pi_s \text{ and } \psi = \pi_{s+1} \dots \pi_r,$$

where π_i is primitive of conductor q_i for $i \in [1, s]$ and principal of conductor q_i for $i \in [s+1, r]$. We choose the q_i (which are not necessarily primes) such that

(a) $q_1 \dots q_s = M_1$ and $q_{s+1} \dots q_r = M_2$;

(b) $q_1 \mid M_1^{\text{odd}}$ and so $\gcd(q_1, q_2 \dots q_r) = 1$;

(c) $k^{47/198} \leq q_i \leq k^{47/99}$ for $i \neq s, r$;

(d) $1 < q_r \leq k^{47/99}$ and

(e) $s \geq 1$, and if $s > 1$ then $1 \leq q_s \leq k^{47/99}$.

We will now explain why it is possible to choose q_i with these properties. Property (a) follows from the definition of the q_i. We first factorise η and ψ into a product of π_j' of conductor q_j', where each character is either of even or prime conductor. We then group the π_j' together to form the π_i. If q_j' satisfies condition (c), it follows from inequality (5.26) that all other $q_j' < k^{47/198}$. We group these π_j' together until they satisfy either property (c), or bundle the remaining factors together into π_r or π_s. Additionally we re-order the π_i such that q_1 is odd. As M_1^{odd} is squarefree and not 1, it follows that $\gcd(q_1, q_2 \dots q_r) = 1$.

From property (c) and inequality (5.26) it follows that

$$(k^{47/198})^{r-2} \leq M \leq k^{2c_2}.$$

So, we deduce

$$r - 2 \leq \frac{\log(M)}{\log(k^{47/198})} \leq 2c_2 \frac{\log(k)}{\log(k^{47/198})}.$$

Hence it follows that

$$r \leq 2 + 8.5c_2.$$

We now calculate N_0 as given in Theorem 2.3.18, using $r = 4$;

$$N_0 \leq k^{47/99} \cdot (k^{47/99})^{1+2^{-4}} = k^{47/48} < k/t - k/t'.$$

We now apply Theorem 2.3.18 with $q = q_1$. We appeal to the inequality

$$\tau(q) \leq q^{1/\log(\log(q))}, \tag{5.27}$$

given in [25, pg. 334]. As $q \geq k^{47/198}$ and r is bounded, it follows for k sufficiently large

$$\tau(q)^{r^2} < q^{1/2}.$$

Applying the inequality in Theorem 2.3.18 we see

$$\left| \sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) \right| \leq \frac{4k}{q^{(1/2)^{r+1}}}.$$

The result now follows from $r \leq 2 + 8.5c_2$ and $q \geq k^{47/198}$.

Case (3.2) $M_1 < 8k^{47/198}$**.**

As χ_1 and χ_2 are distinct it follows $\chi = \chi_1\chi_2$ is not principal, so

$$\left| \sum_{k/t' < m \leq k/t} \chi_1(m)\chi_2(m) \right| < M = M_1M_2.$$

If $M_2 < k^{24/33}$ then the result follows by multiplying M_1 and M_2 together. So, we shall assume $M_2 \geq k^{24/33}$.

$$\begin{aligned}\sum_{k/t'<m\leq k/t}\chi_1(m)\chi_2(m) &= \sum_{k/t'<m\leq k/t}\eta(m)\psi(m)\\ &= \sum_{\substack{k/t'<m\leq k/t\\ \gcd(m,M_2)=1}}\eta(m)\\ &= \sum_{k/t'<m\leq k/t}\eta(m)\sum_{d|\gcd(m,M_2)}\mu(d)\\ &= \sum_{d|M_2}\sum_{k/t'<nd\leq k/t}\eta(nd)\mu(d)\\ &= \sum_{d|M_2}\eta(d)\mu(d)\sum_{k/(t'd)<n\leq k/td}\eta(n).\end{aligned}$$

As η is non-principal and has conductor $M_1 < 8k^{47/198}$, we have

$$\left|\sum_{k/(t'd)<m\leq k/(td)}\eta(m)\right| < M_1 < 8k^{47/198}.$$

Thus

$$\left|\sum_{k/t'<m\leq k/t}\chi_1(m)\chi_2(m)\right| \leq \tau(M_2)\cdot 8k^{47/198} \leq M_2^{1/\log\log(M_2)}\cdot 8k^{47/198},$$

with the last inequality following from Inequality (5.27).

Because M_2 is bounded $k^{24/33} < M_2 < k^{c_2}$, the result now follows.

□

We now state a theorem of Bombieri, Proposition 1 in [9], attributed to Selberg.

Theorem 5.3.9. *If $\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_m$ are vectors in an inner product space then*

$$\sum_{i=1}^{m}|\mathbf{x}\cdot\mathbf{y}_i|^2 \leq ||\mathbf{x}||\cdot\max_{1\leq i\leq m}\left\{\sum_{j=1}^{m}|\mathbf{y}_i\cdot\mathbf{y}_j|\right\}.$$

Proof of Theorem 5.3.6. We write $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_{\geq 3}$, where $\mathcal{B}_i$ is the subset of $\mathcal{B}$ such that the conductors of $\chi_{\mathbf{a}}$ have exactly i prime factors, and $\mathcal{B}_{\geq i}$ is the subset of $\mathcal{B}$ such that the conductors of $\chi_{\mathbf{a}}$ have i or more prime factors. It is clear that one of $|\mathcal{B}_1 \cup \mathcal{B}_{\geq 3}|$

or $|\mathcal{B}_2 \cup \mathcal{B}_{\geq 3}|$ is greater than $\beta^{-2}\log(k)$; call such a set $\mathcal{C}$. It is now clear that the product of the conductors of any two characters in $\mathcal{C}$ is not a product of 3 distinct odd primes.

We now recreate the proof of Proposition 8.1 in [6], making minor change where necessary. From Theorem 5.2.5 to prove Theorem 5.3.6 it is enough to show that

$$\frac{1}{|\mathcal{C}|}\sum_{\mathbf{a}\in\mathcal{C}}\left|\sum_{k/t'<m\leq k/t}\chi_{\mathbf{a}}(m)\cdot\Lambda(m)\right|^2 \leq \beta^2 k^2. \tag{5.28}$$

Let $\mathbf{x} = (\Lambda(m))_{k/t'<m\leq k/t}$ and for each $\mathbf{a}\in\mathcal{C}$, write $\mathbf{y_a} = (\chi_{\mathbf{a}}(m))_{k/t'<m\leq k/t}$. Hence we can re-write inequality (5.28) as

$$\frac{1}{|\mathcal{C}|}\sum_{\mathbf{a}\in\mathcal{C}}|\mathbf{x}\cdot\mathbf{y_a}|^2 \leq \beta^2 k^2. \tag{5.29}$$

After applying Theorem 5.3.9, we have

$$\frac{1}{|\mathcal{C}|}\sum_{\mathbf{a}\in\mathcal{C}}|\mathbf{x}\cdot\mathbf{y_a}|^2 \leq ||\mathbf{x}||^2\cdot\max_{\mathbf{a}\in\mathcal{C}}\left\{\frac{1}{|\mathcal{C}|}\sum_{\mathbf{a'}\in\mathcal{C}}|\mathbf{y_a}\cdot\mathbf{y_{a'}}|\right\}. \tag{5.30}$$

We first calculate $||\mathbf{x}||^2$:

$$\begin{aligned}||\mathbf{x}||^2 &= \sum_{k/t'<m\leq k/t}\Lambda(m)^2\\ &\leq \log(k)(\psi(k/t)-\psi(k/t'))\\ &\leq (\frac{k}{t}-\frac{k}{t'})\log k + O(k),\end{aligned}$$

where the last line follows from the Prime Number Theorem 2.3.15.

We can now apply the proof of Proposition 8.1 in [6], replacing $\varpi = 0.1239^2$ by $\varpi = \beta^2$ to get the result.

For each $\mathbf{a}\in\mathcal{C}$, it follows that

$$|\mathbf{y_a}\cdot\mathbf{y_a}| \leq \frac{k}{t}-\frac{k}{t'} \leq k+1.$$

As $|\mathcal{C}| > (\beta^{-2})\log(k)$, it follows that

$$\frac{|\mathbf{y_a} \cdot \mathbf{y_a}|^2}{|\mathcal{C}|} \leq \frac{\beta^2(k+1)}{\log(k)}.$$

From Properties (II), (III) and (IV) it follows we may apply Theorem 5.3.7. This gives

$$|\mathbf{y_a} \cdot \mathbf{y_{a'}}| = \left| \sum_{k/t' < m \leq k/t} \chi_{\mathbf{a}} \cdot \chi_{\mathbf{a'}} \right| \leq k^{1-c_3}.$$

It now follows from inequality (5.30) that

$$\begin{aligned} \frac{1}{|\mathcal{C}|} \sum_{\mathbf{a} \in \mathcal{C}} |\mathbf{x} \cdot \mathbf{y_a}|^2 &\leq \left(\left(\frac{k}{t} - \frac{k}{t'} \right) \log k + O(k) \right) \cdot \left(\frac{\beta^2(k+1)}{\log(k)} + k^{1-c_3} \right) \\ &= \left(\frac{1}{t} - \frac{1}{t'} \right) \beta^2 k^2 (1 + o(1)), \end{aligned}$$

for k sufficiently large. □

§ 5.4 Sieving and Generating enough $\chi_{\mathbf{a}}$

We now know that if we have enough characters of the forms described in the previous section we can bound k. We now sieve through the set $\mathcal{A}$, so that we can generate enough $\chi_{\mathbf{a}}$ with conductors small and smooth enough so that we can apply either Theorem 5.3.6 or Theorem 5.3.4 to bound k. Explicitly this will be the proof of Theorem 5.4.1, which is a generalisation of Proposition 9.1 in [6].

We now define the following subsets of I, where I is as usual the set of integers that are not missing in the Erdős-Selfridge product. For p a prime we define

$$I_p = \{i \in I \text{ s.t. } p \mid (n + id)\}$$

and it is clear that

$$|I_p| \leq \frac{k}{p} + 1. \tag{5.31}$$

We now sieve through the set I removing such I_p for p large, leaving a small set that is still large enough to apply Theorem 2.2.8. The remaining $\mathbf{a}$ in our sieved $\mathcal{A}$ will then

all have small, smooth conductors, leaving us in a position to apply Theorem 5.3.6 or Theorem 5.3.4.

We define α to be $1 - |I|/k$, to ease notation.

Theorem 5.4.1. *Suppose that k is sufficiently large, $\epsilon_0 < 0.00001$, $c_1 > 0$ is a constant such that $\log(1/(1-c_1)) + \epsilon_0 < 0.001$, and $S \subset [1,k]$ is a set of primes such that*

$$\sum_{p \in S} \frac{1}{p} < \epsilon_0. \tag{5.32}$$

Then there exists an $\mathbf{a} \in \mathcal{A}$ satisfying the following:

(I) $p \nmid N_{\mathbf{a}}$ *for* $p \in S$;

(II) $N_{\mathbf{a}}$ *is not divisible by primes in the range* $((\log\ k)^{1-c_1}, A \log\ k]$ *with* $A > 3$ *a constant;*

(III) $P(N_{\mathbf{a}}) < k^{47/99}$;

(IV) $N_{\mathbf{a}} < k^{\frac{3}{2(0.2505-\alpha)}+1}$.

Proof. Let us define T to be the set of primes in the interval $(k^{47/99}, k]$, U to be the set of primes in the interval $((\log k)^{1-c_1}, A \log k]$ and set

$$J = I \setminus \bigcup_{p \in S \cup T \cup U} I_p.$$

We start by showing that the size of J grows linearly with k. Note that

$$\left| \bigcup_{p \in S \cup T \cup U} I_p \right| \leq \sum_{p \in S} |I_p| + \sum_{p \in T} |I_p| + \sum_{p \in U} |I_p|.$$

From Equation (5.32) and (5.31) we clearly have that

$$\sum_{p \in S} |I_p| \leq \epsilon_0 k + \pi(k).$$

From the definition of T we see that

$$\sum_{p \in T} |I_p| \leq k \sum_{k^{47/99} < p < k} \frac{1}{p} + \pi(k). \tag{5.33}$$

Applying the bound from Theorem 2.1.13, we have

$$\sum_{k^{47/99}<p<k} \frac{1}{p} < \log(99/47) + \frac{99^2}{47^2 \log^2(k)}.$$

From (5.33) and an application of the Prime Number Theorem, we now see that

$$\sum_{p \in T} |I_p| \leq \log(99/47)k + \frac{1.1k}{\log(k)},$$

for sufficiently large k.

Using the same method we see that

$$\begin{aligned}\sum_{p \in U} \frac{1}{p} &< \log(\log(A\log(k))) - \log(\log(\log^{1-c_1}(k))) \\ &\quad + \frac{1}{2}\left(\frac{1}{\log^2(A\log(k))} + \frac{1}{\log^2(\log^{1-c_1}(k))}\right) \\ &= \log\left(\frac{1}{1-c_1}\right) + \log\left(1 + \frac{\log(A)}{\log\log k}\right) \\ &\quad + \frac{1}{2}\left(\frac{1}{\log^2(A\log(k))} + \frac{1}{\log^2(\log^{1-c_1}(k))}\right)\end{aligned}$$

Using the well known bound $\log(1+x) < x$ for $x > 0$ the above inequality can be easily transformed into

$$\sum_{p \in U} \frac{1}{p} < \log\left(\frac{1}{1-c_1}\right) + \frac{1}{\log\log k}\left(\log(A) + \frac{1}{(1-c_1)^2}\right).$$

Hence,

$$\sum_{p \in U} |I_p| < k\log\left(\frac{1}{1-c_1}\right) + \frac{k}{\log\log k}\left(\log(A) + \frac{1}{(1-c_1)^2}\right) + A\log k.$$

From the definition of c_1 it follows that

$$1 < \frac{1}{1-c_1} < \exp(0.001)$$

and as $A > 3$ we can naively combine the two terms together to simplify

$$\sum_{p\in U}|I_p| < k\log\left(\frac{1}{1-c_1}\right) + \frac{2\log(A)k}{\log\log k} + A\log k.$$

Combining these three estimates, we see that

$$\left|\bigcup_{p\in S\cup T\cup U} I_p\right| \leq \left(\log\left(\frac{99}{47}\right) + \log\left(\frac{1}{1-c_1}\right) + \epsilon_0\right)k + \frac{Ck}{\log\log k} + D\log(d),$$

for some constants C and D depending only on A.

Now calculating the k coefficient we see that

$$\left|\bigcup_{p\in S\cup T\cup U} I_p\right| \leq 0.746k,$$

for k sufficiently large.

It now follows that $|J| > (0.254-\alpha)k$, so in particular J is non-empty.

We now apply the same argument as in [6], which is a classic argument of Erdős [19] by defining a set $J_1 \subset J$, obtained from J by deleting, for each $p \leq k$, an index i_p with the property that $\mathrm{ord}_p(A_{i_p})$ is maximal. It follows that

$$|J_1| > (0.254-\alpha)k - \pi(k) > (0.253-\alpha)k$$

for k sufficiently large and further that

$$\prod_{i\in J_1} A_i \mid k!.$$

The following uses the same methods as the proof of Proposition 9.1 in [6].

Noting that no prime $p \geq k^{47/99}$ divides $\prod\limits_{i\in J_1} A_i$, we use Stirling's formula [56]

$$\prod_{i\in J_1} A_i \leq \sqrt{2\pi k}\left(\frac{k}{e}\right)^{k-1} e^{1/12k} \prod_{k^{47/99}<p\leq k} p^{-\mathrm{ord}_p(k!)}. \tag{5.34}$$

Using Theorem 2.1.14, we see that for k sufficiently large

$$\log\left(\prod_{k^{47/99}<p\leq k} p^{\mathrm{ord}_p(k!)}\right) \geq \sum_{k^{47/99}<p\leq k}\left(\frac{k}{p}-1\right)\log(p) > \frac{52}{99}k\log(k) - 2k.$$

From elementary comparisons of both sides of inequality (5.34) it now follows that

$$\prod_{i\in J_1} A_i \leq k^{k/2}. \tag{5.35}$$

We now define $J_2 \subset J_1$ to be the set of indices $i \in J_1$ such that $A_i \leq k^{\frac{1}{2(0.2505-\alpha)}}$. We will shortly provide a bound for the size of J_2. Suppose that $x = |J_1 \setminus J_2|$. Then it follows that

$$\begin{aligned}\prod_{i\in J_1} A_i &= \prod_{i\in J_2} A_i \prod_{i\in J_1\setminus J_2} A_i \\ &> \prod_{i\in J_1\setminus J_2} A_i \\ &> k^{\frac{x}{2(0.2505-\alpha)}}.\end{aligned}$$

Comparing this with (5.35), it then follows immediately that $x < (0.2505-\alpha)k$, giving the result that $|J_2| \geq 0.0005k$.

We now apply Roth's Theorem 2.2.8 to find a non-trivial 3-term arithmetic progression $\mathbf{a}$ in J_2 for k sufficiently large.

By (5.4) it now follows that

$$N_{\mathbf{a}} \leq 2^8 A_i A_j A_{2j-i} \leq 2^8 (k^{\frac{1}{2(0.2505-\alpha)}})^3 < k^{\frac{3}{2(0.2505-\alpha)}+1}.$$

Hence the result now follows. □

§ 5.5 Proof of Theorem 5.2.1

Let $\mathcal{B} \subset \mathcal{A}$ be a non-empty subset satisfying

(I) $P(N_{\mathbf{a}}) \neq P(N_{\mathbf{a}'})$ whenever $\mathbf{a} \neq \mathbf{a}' \in \mathcal{B}$;

(II) $P(N_{\mathbf{a}}) \leq k^{47/99}$ for all $\mathbf{a} \in \mathcal{B}$;

(III) $N_{\mathbf{a}}$ is not divisible by primes in the range $[\log(k)^{1-c_1}, A\log(k)]$ for all $\mathbf{a} \in \mathcal{B}$;

(IV) $N_{\mathbf{a}} < k^{\frac{3}{2(0.2505-\alpha)}+1}$ for all $\mathbf{a} \in \mathcal{B}$.

We first explain why such a $\mathcal{B}$ should exist; this essentially follows from applying Theorem 5.4.1 when $S = \emptyset$. Then for $\ell \geq \exp(10^k)$ and k sufficiently large, we can apply Theorem 5.2.5 to attach to each $\mathbf{a} \in \mathcal{A}$ a character $\chi_{\mathbf{a}}$. We then pick ϵ_0 and c_1 such that $-\log(1-c_1) + \epsilon_0 < 0.00001$ and $A = 4/(\epsilon_0\beta^{-2})$ (N.B. this β is the same β as in Theorem 5.3.6). Now we can generate such a $\mathcal{B}$ by applying Theorem 5.4.1 with $S = \emptyset$.

Now let $\mathcal{B}$ be the maximal such subset of $\mathcal{A}$ satisfying (I)-(IV). If $|\mathcal{B}| > 2\beta^{-2}\log(k)$, then k is effectively bounded by Theorem 5.3.6. We may thus suppose that $|\mathcal{B}| \leq 2\beta^{-2}\log(k)$. Assume first that

$$\sum_{\mathbf{a}\in\mathcal{B}} \frac{1}{P(N_{\mathbf{a}})} < \epsilon_0.$$

If we take $S = \{P(N_{\mathbf{a}}) \text{ such that } \mathbf{a} \in \mathcal{B}\}$, then S satisfies (5.32). Theorem 5.4.1 thus yields another $\mathbf{a} \in \mathcal{A}$ satisfying (II), (III), (IV), and $N_{\mathbf{a}}$ is not divisible by any primes in S. Thus $\mathcal{B}' = \mathcal{B} \cup \{\mathbf{a}\}$ is a strictly larger subset with the same properties as $\mathcal{B}$. We may thus assume that

$$\sum_{\mathbf{a}\in\mathcal{B}} \frac{1}{P(N_{\mathbf{a}})} \geq \epsilon_0.$$

Let

$$\mathcal{C} = \{\mathbf{a} \in \mathcal{B} \text{ such that } P(N_{\mathbf{a}}) > A\log(k)\}$$

and

$$\mathcal{D} = \{\mathbf{a} \in \mathcal{B} \text{ such that } P(N_{\mathbf{a}}) < \log(k)^{1-c_1}\}.$$

Then it follows from condition (III) that $\mathcal{B}$ is the disjoint union of $\mathcal{C}$ and $\mathcal{D}$. It follows that

$$\sum_{\mathbf{a}\in\mathcal{C}} \frac{1}{P(N_{\mathbf{a}})} \leq \frac{|\mathcal{C}|}{A\log(k)} \leq \frac{|\mathcal{B}|}{A\log(k)} \leq \frac{2\beta^{-2}\log(k)}{A\log(k)},$$

hence it follows that

$$\sum_{\mathbf{a}\in\mathcal{D}} \frac{1}{P(N_{\mathbf{a}})} \geq \epsilon_0 - \frac{2\beta^{-2}}{A} > \epsilon_0/2.$$

We now apply Theorem 5.3.4 to deduce that k is bounded, completing the proof of Theorem 5.2.1. □

§ 5.6 Applications of Theorem 5.2.1

In this section we will study two families of equations and show that they lead to situations like that found in Theorem 5.2.1.

5.6.1 Erdős-Selfridge curves

Corollary 5.6.1. *For k sufficiently large, if there is a non-trivial integral solution to $ES(\ell, k, d, B, \emptyset)$ such that*

(1) $p \nmid B$ for all primes in $[k/2, k]$;

(2) fewer than $k/4$ primes greater than k divide B;

then it follows that $\ell < \exp(10^{\max(k, P(B))})$.

Proof. Assume that there is a putative solution for $\ell > \exp(10^{\max(k,P(B))})$. Then it follows from Lemma 5.1.15 that all primes $p \in [k/2, k]$ divide d.

Now for each prime q greater than k that divides B, let i_q denote the unique i such that $q|(n + id)$, further let $U = \{i_q \text{ such that } q|B \text{ and } q \text{ is a prime greater than } k\}$. Then we can divide these terms out, cancelling the prime factors of B greater than k, leaving a solution to the equation

$$B'y^\ell = \prod_{i \notin U} (n + id).$$

B' by construction is not divisible by any primes greater than k. Further, it is not divisible by any primes in the interval $[k/2, k]$. This follows as B was not divisible by any such primes, and neither are any of the deleted terms, because d is divisible by all such primes. Hence B' is divisible only by primes less than $k/2$.

By condition (2) it follows that there are over $0.75k$ of the terms left in the product, so we can now apply Theorem 5.2.1. □

Corollary 5.6.2. *For k sufficiently large, if there is a non-trivial integral solution to $ES(\ell, k, d, B, \{j\})$ such that*

(1) $p \nmid B$ for all primes in $[k/3, k/2]$;

(2) fewer than $k/4 - 1$ primes greater than k divide B;

(3) $v_p(d) \equiv 0 \pmod{\ell}$ *for all primes* p *greater than* k*;*

then it follows that $\ell < \exp(10^{\max(k,P(B))})$.

Proof. Assume that there is a putative solution for $\ell > \exp(10^{\max(k,P(B))})$, then it follows from Lemma 5.1.16 that all primes $p \in [k/3, k/2]$ divide d.

Now for each prime q greater than k that divides B, let i_q denote the unique i such that $q|(n+id)$, further let $U = \{i_q \text{ such that } q|B \text{ and } q \text{ is a prime greater than } k\}$. Then we can divide these terms out, cancelling the prime factors of B greater than k, leaving a solution to the equation

$$B'y^{\ell} = \prod_{i \notin U \cup \{j\}} (n+id),$$

with B' divisible only by primes less than k and not divisible by any primes in the interval $[k/3, k/2]$.

By condition (2) it follows that there are over $0.75k$ of the terms are left in the product, so we can now apply Theorem 5.2.1. □

Remark 5.6.3. It is clear that the above corollary is applicable in the case that all the primes of d are bounded by k. Furthermore it applies in the case of rational solutions for $d = 1$.

Chapter 6

Arithmetic Progression Curves

§ 6.1 Introduction

In this chapter we consider the AP curves, which are the equations of the form

$$y^\ell = (x-d)^k + x^k + (x+d)^k, \tag{6.1}$$

for k, d, x and y integers and ℓ a prime. We require that $x \neq 0$ otherwise we get the trivial solution $(0,0)$ for odd k. We also require that x and d are coprime, otherwise it is possible to generate artificial solutions via scaling. A general solution for all k and d is still currently unsolved, however there are results depending on k and d.

We are going to focus on the case where $k = 3$. This allows us to attach Fermat equations of signature $(\ell, \ell, 2)$ to a putative solution, that we may then study using the modular method.

Theorem 6.1.1. *For $\ell > 7$ a prime, the equation*

$$y^\ell = (x-d)^3 + x^3 + (x+d)^3, \tag{6.2}$$

has no solutions for x, y and d integers with x and d coprime.

§ 6.2 Preliminaries

In this section we attach a solution to one of 4 possible Fermat equations to a putative solution of Equation (6.2). These equations however have already been discussed in the

literature, so we will attach Frey-Hellegouarch curves to them in the traditional way.

Lemma 6.2.1. *An integer solution (x, y) to Equation (6.2), with $x \neq 0$, gives rise to an integer solution of a Fermat equation with coefficients derived from the divisors of x and d. These equations are given in Table 6.1.*

Excluding the case that $d = \pm 2$ and $\ell = 3$, these equations further satisfy $XY \neq \pm 1$.

Additionally in cases (2) and (4) it follows that if we write the given equation in the usual form of $AX^\ell + BY^\ell = CZ^2$, then $\mathrm{ord}_2(BY^7) > 7$.

Case	$x \pmod 2$	$xd \pmod 3$	Equation
1	1	0	$X^\ell + 3^{\ell-2}Y^\ell = 2Z^2$
2	0	0	$X^\ell + 2^{\ell-3}3^{\ell-2}Y^\ell = Z^2$
3	1	± 1	$3^{\ell-1}X^\ell + Y^\ell = 2Z^2$
4	0	± 1	$3^{\ell-1}X^\ell + 2^{\ell-3}Y^\ell = Z^2$

Table 6.1: Fermat equations attached to putative solutions of Equation (6.2).

Further, in cases (1) and (3) if we write the equations in the standard notation

$$AX^\ell + BY^\ell = CZ^2,$$

it follows that $BCY^\ell = -2\alpha^2$ for some odd integer α.

Proof. Expanding out the cubes and simplifying in Equation (6.2), we see that a putative solution (x, y) satisfies

$$3x(x^2 + 2d^2) = y^\ell. \tag{6.3}$$

We calculate the greatest common divisor of $3x$ and x^2+2d^2 to be a divisor of 6, simply because

$$3(x^2 + 2d^2) - x(3x) = 6d^2, \tag{6.4}$$

and we know that x and d are coprime.

We define $g = \gcd(3x, x^2 + 2d^2)$. It follows simply that 2 divides g if and only if 2 divides x. It also follows that 3 divides g if and only if $x^2 + 2d^2 \equiv 0 \pmod 3$. As x and d are coprime they both can't be divisible by 3, hence this is only possible if they are both not divisible by 3.

Case (1) : $g = 1$.

In the case that $3x$ and $x^2 + 2d^2$ are coprime then it is clear that

$$3x = y_1^\ell \text{ and } x^2 + 2d^2 = y_2^\ell,$$

for some integers y_1 and y_2. It then follows that

$$x = 3^{\ell-1} z^\ell,$$

for some odd integer z, and substituting this into $x^2 + 2d^2 = y_2^\ell$ we therefore see that

$$y_2^\ell - 3^{\ell-2}(3z^2)^\ell = 2d^2.$$

This gives a solution of the equation

$$X^\ell + 3^{\ell-2} Y^\ell = 2Z^2$$

and it is clear that $XY \neq \pm 1$. Writing this equation in the form

$$AX^\ell + BY^\ell = CZ^2,$$

it also follows that $BCY^\ell = -2 \cdot 3^{2(\ell-1)} z^{2\ell} = -2\alpha^2$, where $\alpha = 3^{\ell-1} z^\ell$.

Case (2) : $g = 2$**.**

In this case, 2 divides x and as d is coprime to x, we see

$$3x = 2^{\ell-1} y_1^\ell \text{ and } x^2 + 2d^2 = 2y_2^\ell,$$

for some integers y_1 and y_2. It is now clear after combining these two equations that

$$d^2 = y_2^\ell - 2^{\ell-3} 3^{\ell-2} (6z^2)^\ell,$$

for some integral z. Hence it follows we have a solution of

$$X^\ell + 2^{\ell-3} 3^{\ell-2} Y^\ell = Z^2$$

and it is clear that $XY \neq \pm 1$. Additionally it is seen that 2 divides Y, giving the final result for case (2).

Case (3) : $g = 3$**.**

In this case, it is clear that 3 does not divide x, hence

$$3x = 3y_1^\ell \text{ and } x^2 + 2d^2 = 3^{\ell-1}y_2^\ell,$$

for some integers y_1 and y_2. Substituting as above, we see that this gives rise to an equation of the form

$$2d^2 = 3^{\ell-1}y_2^\ell - y_1^{2\ell}.$$

We will now show that $y_1y_2 \neq \pm 1$. Assume the opposite for contradiction. It follows from the definition of y_2 that it would have to be positive.

So we have to consider the case

$$2d^2 = 3^{\ell-1} - 1.$$

Factorizing this as

$$2d^2 = (3^{(\ell-1)/2} - 1)(3^{(\ell-1)/2} + 1),$$

and noting that each factor is even, with the greatest common divisor between the two terms being 2 then it follows that either $3^{(\ell-1)/2} + 1$ or $3^{(\ell-1)/2} - 1$ is a perfect square. Considering $3^{(\ell-1)/2} - 1 \pmod 3$, it follows that the second case cannot occur. Hence we are left to consider if it is possible for $3^{(\ell-1)/2} + 1 = m^2$. Now factorizing this we see that $3^{(\ell-1)/2} = (m-1)(m+1)$.

It follows similarly to above that these factors must be coprime. We can now just try all possible cases. It then follows that $\ell = 3$ and $m = \pm 2$, but this contradicts $\ell \geq 7$.

Hence it follows we have a solution of

$$3^{\ell-1}X^\ell + Y^\ell = 2Z^2,$$

and provided that $d \neq \pm 2$ and $\ell \neq 3$, then $XY \neq \pm 1$. Again, it follows simply that $BCY^\ell = -2\alpha^2$, where $\alpha = y_1^\ell$, and as y_1 divides x it follows that α is odd.

Case (4) **:** $g = 6$**.**

In this case it is clear that 3 does not divide x but 2 does, hence

$$3x = 3 \cdot 2^{\ell-1}y_1^\ell \text{ and } x^2 + 2d^2 = 2 \cdot 3^{\ell-1}y_2^\ell,$$

for some y_1 and y_2. Substituting as above, we see that this gives rise to an equation of

the form

$$d^2 = 3^{\ell-1}y_2^\ell - 2^{\ell-3}(2y_1)^\ell,$$

for some y_1 and y_2.

Hence it follows we have a solution of

$$3^{\ell-1}X^\ell + 2^{\ell-3}Y^\ell = Z^2$$

and it is clear that $XY \neq \pm 1$. Here it is also clear that 2 divides Y, finishing the lemma. □

§ 6.3 Modularity

In this section we use the modular method. This means that we attach an elliptic curve to our putative solution, and by modularity this allows us to further attach a modular form to this solution. We can then use Ribet's Level Lowering Theorem, to lower the level of these forms $\pmod{\ell}$. This then allows us to compute all mod modular forms at this smaller level.

Theorem 6.3.1. *A putative solution (x, y, z) of the Fermat equations in Table 6.1 give rise to an elliptic curve E and a newform f of level N_ℓ, such that $E \sim_\ell f$ as described in the following table.*

Case	E	N_ℓ
1	$Y^2 = X^3 + 4zX^2 + 2 \cdot 3^{\ell-2}y^\ell X$	$2^8 \cdot 3$
2	$Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{2^{\ell-2} \cdot 3^{\ell-3}y^\ell}{64}X$	6
3	$Y^2 = X^3 + 4zX^2 + 2 \cdot 3^{\ell-1}y^\ell X$	$2^8 \cdot 3$
4	$Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{2^{\ell-3}y^\ell}{64}X$	6

Table 6.2: The attached Frey-Hellegouarch curves and level lowered conductors for each equation given in Table 6.1

Proof. We will consider the four cases as given by Lemma 6.2.1. It is then mostly just

an application of Theorem 3.2.1, as we shall show below. It is important to remember from Lemma 6.2.1 that $xy \neq \pm 1$.

Case (1) **:** $X^\ell + 3^{\ell-2}Y^\ell = 2Z^2$**.**

It follows from the Z coefficient being even that we are in case (II) of Theorem 3.2.1. So we attach the elliptic curve

$$E : Y^2 = X^3 + 4zX^2 + 2 \cdot 3^{\ell-2}y^\ell X.$$

It follows from parts (b) and (c) of Theorem 3.2.1 that that conductor of E is given by

$$N = 2^8 \operatorname{Rad}(3^{\ell-2}xy),$$

and there is a modular form f attached to E such that $E \sim_\ell f$ of level

$$N_\ell = 2^8 \operatorname{Rad}(AB) = 2^8 \cdot 3.$$

Case (2) **:** $X^\ell + 2^{\ell-3}3^{\ell-2}Y^\ell = Z^2$**.**

As above we apply Theorem 3.2.1; here by the final remark in Lemma 6.2.1 we are in case (V). Hence we attach the elliptic curve

$$E : Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{2^{\ell-3} \cdot 3^{\ell-2}y^\ell}{64}X.$$

We now apply part (c) of Theorem 3.2.1 to see that there is a modular form f such that $E \sim_\ell f$, and as E does not have complex multiplication, following from part (c) of Theorem 3.2.1 and that $xy \neq \pm 1$,, we have

$$N_\ell = \operatorname{Rad}(AB) = 6.$$

Case (3) **:** $X^\ell + 3^{\ell-1}Y^\ell = 2Z^2$**.**

As in case (1) it follows that we are in case (II) of Theorem 3.2.1. We attach the elliptic curve

$$E : Y^2 = X^3 + 4zX^2 + 2 \cdot 3^{\ell-1}y^\ell X.$$

It follows from parts (b) and (c) of Theorem 3.2.1 that there is a modular form f such

that $E \sim_\ell f$ for some newform f of level

$$N_\ell = 2^8 \operatorname{Rad}(AB) = 2^8 \cdot 3.$$

Case (4) **:** $3^{\ell-1}X^\ell + 2^{\ell-3}Y^\ell = Z^2$**.**

This follows similarly to case (2); as $\operatorname{ord}_2(BY^\ell) > 7$ we are in case (V) of Theorem 3.2.1. Hence we attach the elliptic curve

$$E : Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{2^{\ell-3}y^\ell}{64}X.$$

And as E does not have complex multiplication, following from part (c) of Theorem 3.2.1 and that $xy \neq \pm 1$, there is a modular form f such that $E \sim_\ell f$ with

$$N_\ell = \operatorname{Rad}(AB) = 6.$$

□

Theorem 6.3.2. *There are no integral solutions* (x, y) *to Equation* (6.1) *with* x *even and* $k = 3$*.*

Proof. To a given putative solution with x even, we may attach a Fermat equation of signature $(\ell, \ell, 2)$ as given by Lemma 6.2.1. This will correspond to either case (2) or (4) in Table 6.1. We may now apply Theorem 6.3.1 to derive a modular form f of weight 2 and level 6. However there are no level 6 newforms, contradicting the assumption of a solution. □

Remark 6.3.3. From the above theorem, it follows we only need to consider the remaining case of $i = 1$ or $i = 3$. We know from Theorem 6.2.1 that $BCY^\ell = -2\alpha^2$. This means that the elliptic curves in the previous theorem can be written as

$$E : Y^2 = X^3 + 4zX^2 - 2\alpha^2 X.$$

This implies that our curves E are all quadratic twists of some curve

$$F_m : Y^2 = X^3 + mX^2 - 2X,$$

for some m.

Remark 6.3.4. It is well known that if E is a quadratic twist of F, for E and F elliptic curves, $a_q(E)^2 = a_q(F)^2$ for q a prime of good reduction.

§ 6.4 Computation

In this section we use our Frey-Hellegouarch curves and Magma computation to complete Theorem 6.1.1.

Lemma 6.4.1. *For E an elliptic curve as in case* (1) *or* (3) *from Theorem 6.3.1, we have $E \nsim_\ell f$ for f newform at a level N_ℓ.*

Proof. Assume for contradiction that $E \sim_\ell f$, for some f and ℓ. For q a prime that doesn't divide 6, we define

$$B_q(\alpha) = \begin{cases} \text{Norm}(a_q(F_m)^2 - a_q(f)^2), \text{ if } q \nmid \Delta_m \\ \text{Norm}(a_q(F_m)^2 - (q+1)^2), \text{ if } q \mid \Delta_m \end{cases}$$

and

$$B_q = q \prod_{0 \leq \alpha \leq q-1} B_q(\alpha). \tag{6.5}$$

Using the remark above that our E is a quadratic twist of some F_m, so that $a_q(E)^2 = a_q(F_m)^2$ for some m, the fact that $\pmod q$ there are only q such curves, determined by $m \pmod q$ and applying Lemma 3.1.6, we see that ℓ divides $G(f) = \gcd(\{B_q \mid q \leq 100, q \nmid 6\})$.

We compute $G(f)$ for every f of level $2^8 \cdot 3$ using Code 7.2. The calculation shows that $\ell = 2, 3, 5$ or 7 are the only possible exponents. □

Proof of Theorem 6.1.1. We see from Lemma 6.4.1 that for x odd there are no solutions for $\ell > 7$, and from Theorem 6.3.2 that there are no even solutions for $\ell > 7$. The result now follows. □

Chapter 7

Code

Here are the Magma programs that have needed to be run during the writing of this thesis.

Listing 7.1: Magma Code: Prime Bound

```
N:=1;
for k:=22 to 181000 do
M:=(Log(k)/k)*(#PrimesUpTo(Floor(k/2))-#PrimesUpTo(Floor(k/3)));
if M lt N then
N:=M;
end if;
end for;
N;
```

Listing 7.2: Magma Code: Calculating G(f)

```
S:=CuspForms((2^8)*3);
Snew:=Newforms(S);
//Here we calculate the newforms in our space.
G:=1;
B:=[];
s:=[];
G:=[];
for j:=1 to #Snew do
f:=Newform(S,j);
```

```
//We now iterate through each modular form.
for i:=4 to 50 do
//We will now iterate through the first 50 primes,
// excluding the smallest few.
a:=1;
l:=NthPrime(i);

//We now compute Bl, note that the curve Ea
// has good reduction at l
// if and only if a^2+8 mod l isn't 0
Bl:=l;
for a:=1 to l do
Ea:=EllipticCurve([0,0,a,-2,0]);
//We now define each elliptic curve that needs to be considered
if a^2+8 mod l ne 0 then
Bla:=Floor(Norm(TraceOfFrobenius(Ea,l)^2-Coefficient(f,l)^2));
else
Bla:=Floor(Norm((l+1)^2-Coefficient(f,l)^2));
end if;

Bl:=Bl*Bla;

end for;
s:=Append(s,Bl);
//We now create a vector of all the Bl's we have calculated

end for;

G:=Append(G,Gcd(s));

end for;
G:=LeastCommonMultiple(G);
print(PrimeDivisors(G));
//We now compute the prime factors of G(f)
```

References

[1] R.C. Baker, G. Harman, J. Pitz , *The difference between consecutive primes, II,* Proceddings of the London Mathematical Society 83 (3), 532-562, 2001.

[2] M.A. Bennett, N.B. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression,* Proc. London Math. Soc 92, 273-306, 2006.

[3] M.A. Bennett, G. Martin, K. O'Bryant, A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions,* arXiv:1802.00085, 2018.

[4] M.A. Bennett, V. Patel, S. Siksek, *Perfect powers that are sums of consecutive cubes,* Mathematika 63, 230-249, 2016.

[5] M.A. Bennett, V. Patel, S. Siksek, *Superelliptic equations arising from sums of consecutive powers,* Acta Arithmetica 172 no 4, 377-393, 2016.

[6] M.A. Bennett, S. Siksek, *A conjecture of Erdős, supersingular primes and short character sums,* arXiv:1709.01022, 2017.

[7] M.A. Bennett, S. Siksek, *Rational points on Erdős-Selfridge superelliptic curves,* Compositio Mathematica 152 (11), 2249-2254, 2016.

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

[9] E. Bombieri, *A note on the large sieve,* Acta Arith. 18, 401-404, 1971.

[10] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises,* J. Amer. Math. Soc.14 No. 4 843-939, 2001.

[11] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and Modular Approaches to Exponential Diophantine Equations I. Fibonacci and Lucas Perfect Powers,* Annals of Mathematics 163, 969-1018, 2006.

[12] J.W.S. Cassels, *A Diophantine equation,* Glasgow Math. Journal 27, 1188, 1985.

[13] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer,* Inventiones Math. 39, 223-251, 1977.

[14] P. Das, S. Laishram, N. Saradha, *Variations of Erdős-Selfridge superelliptic curves and their rational points,* preprint, 2016.

[15] P. Dusart, *Explicit estimates of some functions over primes,* The Ramanujan Journal 45 (1), 227-251 2016.

[16] N. Freitas, B.V. Le Hung, S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular* Inventiones mathematicae. 201 (1), 159206, 2015.

[17] S.L. Edis, *On Congruent Numbers over Real Quadratic Fields,* pre-print, 2019.

[18] S.L. Edis, *On a variation of the Erdős-Selfridge superelliptic curve,* Bull. London Math. Soc. 51 (4), 633-638, 2019.

[19] P. Erdős, *On the product of consecutive integers III,* Indagationes Math. 17, 85-90, 1955.

[20] P. Erdős, J.L. Selfridge, *The product of consecutive integers is never a power,* Illinois J. Math. 19, 292-301, 1975.

[21] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen,* Invent. Math. 73, 349-366, 1983.

[22] A. Argáez-García, V. Patel, *On perfect powers that are sums of cubes of a three term arithmetic progression,* arxiv:1711.06407v1, 2017.

[23] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions,* Annals of Mathematics 167, 481-547, 2016.

[24] K. Győry, L. Hajdu, A. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression,* Compositio Math. 145, 845864, 2009.

[25] H. Iwaniec, E. Kowalski, *Analytic Number Theory,* American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, xii+615 pp, 2004.

[26] W. Ivorra, I. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canad. J. Math. 58, 115-153, 2006.

[27] W.R. Knorr, *Archimedes and the measurement of the circle: a new interpretation,* Archive for History of Exact Sciences 15 (2), 115-140, 1976.

[28] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms,* Spring Graduate Texts in Mathematics, 1984.

[29] A. Koutsianas, *On the solutions of the Diophantine equation* $(x-d)^2 + x^2 + (x+d)^2 = y^n$ *for* d *a prime power,* arXiv:1708.00928 [math.NT], 2019.

[30] A. Koutsianas, V. Patel *Perfect powers that are sums of squares in a three term arithmetic progression,* Intl J. Number Theory 14 (10), 2729-2735, 2018.

[31] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée,* Canad. J. Math. 49, no. 6, 1139-1161, 1997.

[32] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive,* Manuscripta Math. 69 (4), 129-162, 1978.

[33] A. Kraus, J. Oesterlé, *Sur une question de B. Mazur,* Math. Ann. 293, 259-275, 1992.

[34] M. Lakhal J.W. Sander, *Rational points on the superelliptic Erdős-Selfridge curve of fifth degree* Mathematika 50, 113124, 2003.

[35] J. Liouville, Jour. de Math.(2), 2, 227, 1857.

[36] G. Martin, *Dimensions of the spaces of cuspforms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$*,* J. Number Theory. 112, 298-331, 2005.

[37] B. Mazur, *Rational isogenies of prime degree,* Invent. Math. 44, 129162, 1978.

[38] J. Nagura, *On the interval containing at least one prime number,* Proc. Japan Acad Vol. 28 (4), 177-181, 1952.

[39] D.J. Platt, *Numerical computations concerning the GRH,* Math. Comp. 85, 3009-3027, 2016.

[40] C. Pagliani, *Solution du problème d'analyse indéterminée énoncé à la pag.* 212*,* du présent volume, Annales de Mathématiques pures et appliquées 20, 382-384, 1829-1830.

[41] M. Rahman, *Roth's theorem on* 3*-term arithmetic progressions,* available at http://math.mit.edu/∼mustazee/Roth.pdf

[42] S. Ramanujan, *A proof of Bertrand's postulate,* J. Indian Math. Soc. 11,181-182, 1919.

[43] O. Ramaré, R. Rumely, *Primes in arithmetic progressions,* Math. Comp. 65, no. 213, 397-425, 1996.

[44] K. Ribet, *On modular representations of Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms,* Invent. Math. 100, 431-476, 1990.

[45] J.B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers,* Illinois J. Math. 6, 64-94, 1962.

[46] K. Roth, *On certain sets of integers,* J. London Math Soc. 28, 104-109, 1953.

[47] J. W. Sander *Rational points on a class of superelliptic curves,* J. London Math. Soc 59, 422-434, 1999.

[48] A. Schinzel, R. Tijdeman *On the equation* $y^m = P(x)$*,* Acta Arithmetica XXXI, 199204, 1976.

[49] L. Schoenfeld *Sharper Bounds for the Chebyshev Functions* $\theta(x)$ *and* $\psi(x)$*,* Mathematics of Computation vol 30, no 134, 337-360, 1976.

[50] G. Shimura *On modular forms of half-integral weight,* Annals of Math 97, 1973.

[51] G. Shimura *Modular forms of half integral weight,* Springer-Verlag Lecture Notes in Math 320, 59-74, 1973.

[52] T.N. Shorey *Some exponential Diophantine equations, New Advances in Transcendence Theory,* Cambridge University Press 352-365, 1988.

[53] T.N. Shorey *Perfect powers in products of arithmetical progressions with fixed initial term,* Indage. Math. N.S. 7, 521-525, 1996.

[54] J.H. Silverman *The Arithmetic of Elliptic Curves,* (2nd ed.) Springer, Graduate Texts in Mathematics 106, 2009.

[55] S. Siksek *On the diophantine equation* $x^2 = y^p + 2^k z^p$*,* Journal de théorie des nombres de Bordeaux 15 (3), 839-846, 2003

[56] K. Stromberg *An Introduction to Classical Real Analysis,* Wadsworth International Mathematical Series, 1971.

[57] G. Tenenbaum, *Introduction to analytic and probabilistic number theory,* Cambridge studies in advanced mathematics 46, Cambridge University Press, Cambridge, 1995.

[58] J.B. Tunnell, *A classic Diophantine problem and modular forms of weight 3/2,* Inventiones Mathematicae Vol. 72 No. 2, 1983, 323-334.

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

[60] D. Wolke, *On the explicit formula of Riemannvon Mangoldt, ii,* J. London Math 28 (2), 406-416, 1983.

[61] Z. Zhang, *On the Diophantine equation* $(x-1)^k + x^k + (x+1)^k = y^n$, Publ. Math. Debrecen 85, 93-100, 2014.