Theory of Elliptic Curves

Keshav Aggarwal

A dissertation submitted for the partial fulfilment of
BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
April 2013

Certificate of Examination

This is to certify that the dissertation titled "Theory of Elliptic Curves" submitted by Mr. Keshav Aggarwal (Reg. No. MS08030) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Amit Kulshrestha Dr. Alok Maharana Prof. Kapil H. Paranjape
(Supervisor)

Dated: April 26th 2013

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Prof. Kapil H. Paranjape at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Acknowledgment

I thank Prof. Kapil H. Paranjape for his guidance and for giving me enough freedom so that I could explore the subject according to my interest. I'd also like to thank KVPY and IISER Mohali for their support.

Finally, I am grateful to my friends and family for giving me all the non-technical support and of course sheer luck because of which I got the opportunity to learn mathematics.

Keshav Aggarwal
MS08030
IISER Mohali

Notation

E_K	Elliptic curve defined over a field K
$E_K(L)$	Elliptic curve defined over a field K with points in extension field L
$\mathcal{O}$	Additive identity of Elliptic curve
$v_p()$	p-adic valuation
$\#S$	Cardinality of a set S
$\left(\frac{n}{m}\right)$	Legendre symbol
$\mathbb{N}x$	Norm of an element or an ideal x
$\mathcal{R}s$	Real part of a complex number s
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{C}$	Field of Complex numbers
$\mathbb{R}$	Field of Real numbers
$\mathbb{Q}$	Field of Rational numbers
$\mathcal{O}_K$	Ring of integers of a field K
$\mathbb{P}^2$	Projective plane of dimension 2

Abstract

This exposition is the result of an year's study of the theory of elliptic curves. It has two parts. The first part of the report explains the group structure on points on elliptic curves and discusses two major results: Nagell-Lutz theorem and Mordell's Theorem. It turns out that over $\mathbb{Q}$, the group of points of an elliptic curve is a finitely generated Abelian group. A question of interest therefore is what the possible torsion and rank can be. A folklore conjecture asserts that there exist elliptic curves of arbitrary rank. The second part of this report explains a method due to Penney and Pomerance (1974) of creating elliptic curves of positive ranks. The report then discusses L-functions of elliptic curves and we explicitly compute L-function of certain elliptic curves. It is conjectured that the L-function and the group structure of an elliptic curve are intimately related. We end the report with a brief discussion of Birch and Swinnerton-Dyer conjecture.

Contents

Chapter 1

Introduction

This exposition is on the theory of elliptic curves.

A non singular cubic curve f in two variables over a field K having a point with coordinates in K is called an elliptic curve over K. The collection $E_K(L)$ of solutions of E_K with coordinates in an extension L of K can be given a group structure. When $L = \mathbb{C}$, the group of points $E_{\mathbb{Q}}(\mathbb{C})$ is isomorphic to a real two torus. It turns out that $E_{\mathbb{Q}}(\mathbb{Q})$ is a finitely generated Abelian group (Mordell's Theorem). The first part of this report will discuss this group structure and some results about rational points on elliptic curves like Nagell-Lutz theorem, computing the torsion part and Mordell's theorem.

The second part is devoted to a method to generate elliptic curves of positive rank and to study L-function of elliptic curves. The torsion part of the Abelian group of elliptic curve is well studied and a theorem of Mazur limits what the torsion part can be. However, less is known about the possible ranks of elliptic curves. A folklore conjecture is that there exist elliptic curves over $\mathbb{Q}$ with prescribed torsion (within Mazur's limits) and rank. A question of interest is therefore to find a method to generate elliptic curves of large ranks. Currently, an elliptic curve of rank at least 28 is known. We execute the algorithm due to Penney and Pomerance given in [PP74] to find examples of some elliptic curves of rank 6 and 7.

The group structure is expected to be intimately related to the L-function of the elliptic curve. The Birch and Swinnerton-Dyer (BSD) conjecture asserts that the rank of an elliptic curve equals the order of vanishing of its L-function at $s = 0$. In Chapter 6, we shall define the L-function of an elliptic curve. We will also consider

the congruent number problem and its relation to the elliptic curve $y^2 = x^3 - n^2x$. We shall compute the L-function of this curve explicitly. In a final chapter, we will discuss the Birch and Swinnerton-Dyer conjecture.

Part I

Basic Definitions and Structure of Elliptic Curves

Chapter 2

Group law on Elliptic Curves

The sources of this chapter are primarily [R V91] and [Ahl79]

Let $f(z)$ be a meromorphic function on $\mathbb{C}$ and let M be its set of periods. We first show that M is a discrete subgroup of the additive group $\mathbb{C}$. A doubly periodic meromorphic function will be called an elliptic function. We will then show that the sum of its residues in a fundamental domain is 0, so that the an elliptic function cannot have a single simple pole. This indicates the definition of the Weierstrass $\wp$ function which has only one pole of order 2. We will show that $\wp$ and $\wp'$ satisfy a cubic equation and end with a proof that doubly periodic functions are isomorphic to complex tori.

Definition 2.0.1. *ω is called a period of a function f if $f(z+\omega) = f(z)$ for all z in the domain.*

Let f be a meromorphic function on $\mathbb{C}$ and M be its set of periods. Then M is an additive subgroup of $\mathbb{C}$ because 0 is trivially a period; if ω_1 and ω_2 and periods, then so are $-\omega_1$ and $\omega_1 + \omega_2$. M is also a discrete subset of $\mathbb{C}$ as it is the set of zeros of the meromorphic function $f - f(0)$, which is discrete.

2.1 Doubly Periodic functions

Theorem 2.1.1. *A discrete subgroup of the additive group $\mathbb{C}$ is either $\{0\}$, is generated by a single complex number or is generated by two complex numbers which are linearly independent over $\mathbb{R}$.*

Proof: Let M have some nonzero point and let ω be such that $|\omega|$ is minimum. This can be chosen as M is discrete. Then $n\omega$ belong to M. If these cover all points in M, then it is a subgroup of dimension 1. Otherwise, let ω' be a point which is not an integral multiple of ω and its absolute value is the least among all such points. We claim that ω'/ω is not real. If it were, then there is an integer n such that $n < |\omega'/\omega| < n+1$. Thus, $0 < |n\omega' - \omega| < |\omega'|$ which is a contradiction. There cannot be a third point in $\mathbb{C}$ independent of ω and ω' as dimension of $\mathbb{C}$ as a vector space over $\mathbb{R}$ is 2. Thus M must be generated by ω and ω'.

Definition 2.1.2 (Fundamental Domain)**.** *All the values of f are covered in the rectangle with vertices $0, \omega, \omega'$ and $(\omega + \omega')$ or any of its translates. Such a domain is called a fundamental domain.*

Definition 2.1.3 (Lattice)**.** *A discrete subgroup of $\mathbb{C}$ that spans it as a real vector space is called a lattice.*

Lemma 2.1.4. *An elliptic function with no poles is a constant.*

Proof: If the elliptic function has no poles, then it is a holomorphic doubly periodic function. So its limits are achieved in the a fundamental domain. By Liouville's theorem, f is a constant.

Theorem 2.1.5. *Sum of residues of an elliptic function $f(z)$ is zero.*

Proof: Let P_a be the fundamental domain translated by a and let ∂P_a be its boundary. Traversing the boundary in positive sense, the sum of its residues is

$$\frac{1}{2\pi i}\int_{\partial P_a} f(z)dz$$

The integrals over the opposite sides of the parallelogram cancel each other due to periodicity. So the integral vanishes.

Corollary 2.1.6. *There does not exist an elliptic function with a single simple pole.*

Proof: The residue at a simple pole is nonzero.

Corollary 2.1.7. *A non constant elliptic function has equal number of poles and zeros counting multiplicities.*

Proof: Consider the meromorphic function f'/f. This is also an elliptic function with poles which are all simple and are exactly the zeros and poles of f. The residues of f'/f are the multiplicities counted negative for poles and positive for zeros.

2.2 Weierstrass $\wp$-function

We saw that a doubly periodic function has a period lattice. Conversely, given a lattice Γ, we can find a meromorphic function with period lattice Γ.

Definition 2.2.1. *Given a lattice Γ, we define the Weierstrass $\wp$-function related to Γ as*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Gamma;\omega\neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

We claim that this function is a doubly periodic function with period lattice Γ and its only poles are double poles at the points in Γ. We prove this in a series of lemmas.

Lemma 2.2.2. *The series defining the Weierstrass $\wp$-function converges absolutely on $\mathbb{C} - \Gamma$ and uniformly on every compact set.*

Proof: For a given z, leaving out the finitely many lattice points for which $|\omega| \leq 2|z|$, we have

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2(z-\omega)^2} \right| \leq \frac{10|z|}{|\omega|^3}$$

Thus we'll have absolute convergence and uniform convergence on every compact set provided

$$\sum_{\omega\neq 0} \frac{1}{|\omega^3|} < \infty$$

As ω'/ω is not real, there exists $c > 0$ such that $|n_1\omega + n_2\omega'| \geq c(|n_1| + |n_2|)$ for all integer pairs (n_1, n_2). There are $4n$ pairs for which $|n_1| + |n_2| = n$. This gives

$$\sum_{\omega\neq 0} \frac{1}{|\omega^3|} \leq \frac{4}{c^3} \sum_{n\geq 1} \frac{1}{n^2} < \infty$$

We have thus shown that the Weierstrass $\wp$-function is well defined. We next show that Γ is its period lattice.

Lemma 2.2.3. *The Weierstrass $\wp$-function has period lattice Γ.*

Proof: Differentiate the series of $\wp(z)$ term-wise to get

$$\wp'(z) = -\frac{2}{z^3} - \sum_{\omega\neq 0} \frac{2}{(z-\omega)^3} = -2\sum_{\omega} \frac{1}{(z-\omega)^3}$$

This series is obviously doubly periodic. To see absolute convergence on $\mathbb{C} - \Gamma$,

$$\sum_{\omega} \frac{1}{|z-\omega|^3} = \sum_{\omega} \frac{1}{|\omega|^3 |z/\omega - 1|^3} \leq \sum_{\omega} \frac{C}{|\omega|^3} < \infty$$

where the inequality follows as $|z/\omega - 1|$ is bounded away from 0. So $\wp(z+\omega) - \wp(z)$ and $\wp(z+\omega') - \wp(z)$ do not depend on z. From the series expansion we see that $\wp(z)$ is an even function. Choosing $z = -\omega/2$ and $z = -\omega'/2$, we get that these two quantities are zero. Thus $\wp(z)$ has periods ω and ω' and period lattice Γ.

Notice that the Laurent expansion of $\wp(z)$ at the origin gives the constant term 0.

Differential equation of $\wp$-function

We now give a method to expand $\wp(z)$ into Laurent series. Because $\wp(z)$ has zero residues at its poles, it is the derivative of a single valued function. The anti-derivative of $\wp(z)$ is traditionally denoted by $-\zeta(z)$, where we have the expression

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \neq 0} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right)$$

Convergence follows because leaving out $1/z$, the series can be obtained by integrating the series of $\wp-$function along any path from 0 to z that avoids poles. Moreover, the function is well defined since the residues of $\wp(z)$ are 0. The series of $\zeta(z)$ can be easily expanded. We have

$$\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} = -\frac{z^2}{\omega^3} - \frac{z^3}{\omega^4} - ...$$

Summing this, we obtain

$$\zeta(z) = \frac{1}{z} - \sum_{k \geq 2} G_k z^{2k-1}$$

where

$$G_k = \sum_{\omega \neq 0} \frac{1}{\omega^{2k}}$$

As $\wp(z) = -\zeta'(z)$, we get

$$\wp(z) = \frac{1}{z^2} + \sum_{k \geq 2} (2k-1) G_k z^{2k-2}$$

This helps us to write expansions of the following

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + ... \tag{2.1}$$

$$4\wp(z)^3 = \frac{4}{z^6} - \frac{36G_2}{z^2} + 60G_3 + ... \tag{2.2}$$

$$60G_2\wp(z) = \frac{60G_2}{z^2} + 0 + ... \tag{2.3}$$

which give

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_2\wp(z) = -140G_3 + ...$$

The left hand side is a doubly periodic function and the right side represents a function which is holomorphic in a neighborhood of 0. On the other hand the left-hand side can have poles only at 0 in the the fundamental domain. Thus the left hand side has no poles in the fundamental domain and so is a doubly periodic holomorphic function on $\mathbb{C}$. By Lemma 2.1.4, it is constant. Setting $g_2 = 60G_2$ and $g_3 = 140G_3$, we get the differential equation of the $\wp-$function

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

2.3 Group law on Cubics

Given a lattice Γ in $\mathbb{C}$, let $X = \mathbb{C}/\Gamma$. Then X is a compact Abelian group under quotient topology. It is in fact isomorphic to $S^1 \times S^1$, where S^1 is the circle group. This gives that X has exactly three points of order 2. We prove the addition law on nonsingular cubics. For this, we require some lemmas.

Lemma 2.3.1. *$\wp(z)$ takes every value exactly twice in the fundamental domain counting multiplicities.*

Proof: $\wp(z)$ has a pole exactly at 0 which is a double pole. So by Corollary 2.1.7, it has exactly two zeros counting multiplicities. Given $u \in \mathbb{C}$, the same holds $\wp(z) - u$. So $\wp(z) - u$ has exactly two zeros in the fundamental domain. That is, $\wp(z)$ takes each value $u \in \mathbb{C}$ exactly twice in the fundamental domain counting multiplicities.

As $\wp'(z)$ is odd with periods ω and ω'; $\omega/2, \omega'/2$ and $(\omega + \omega')/2$ are zeros of $\wp'(z)$. Also $\wp(z)$ and $\wp'(z)$ satisfy the cubic $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. It is not a priori clear if these three are the only zeros of $\wp'$. We claim that the three zeros of $\wp'(z)$

are distinct and these are the only zeros. We get this as a corollary of the following lemma.

Lemma 2.3.2. *Let $x_1, x_2 \in X$. Then $\wp(x_1) = \wp(x_2)$ iff $x_1 = \pm x_2$.*

Proof: $\wp(z)$ is even and takes each value exactly twice, which will occur at x and $-x$. We need to show that if $x \neq -x$, then $\wp(z) - \wp(x)$ has simple zero at $z = x$ and if $x = -x$, then $\wp(z) - \wp(x)$ has a double zero. This follows because $\wp(z) - \wp(x)$ takes each value exactly twice (due to 2.1.7). We have thus shown that $\wp'(x) = 0$ precisely when x is of order 2.

Corollary 2.3.3. *The value of $\wp$ at three points of order 2 are distinct.*

Proof: If $\wp$ took the same value at two points of order 2, then it would take that particular value at least four times.

This gives that the three points of order 2 are exactly the three zeros of $\wp'$. This cubic can thus be factorized as

$$\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

where $e_1 = \wp(\omega/2), e_2 = \wp(\omega'/2), e_3 = \wp((\omega + \omega')/2)$

Corollary 2.3.4. *Let Γ be the lattice of period of $\wp$. Then $\wp(z)$ gives a two-to-one map from $\mathbb{C}/\Gamma$ to the Riemann sphere $\mathbb{C} \cup \{\infty\}$ except for the four points of order 2: e_1, e_2, e_3, ∞ which have single pre-image in $\mathbb{C}/\Gamma$.*

Remark 2.3.5. *Every smooth cubic can be brought into the Weierstrass form (as we have defined) over a field of characteristic not equal $2, 3$. Also, for each Weierstrass form, we can find a corresponding lattice. This certainly needs a proof but we do not state it here. A proof can be found in [R V91] or [Sil86]*

With this background, we give the addition law on cubics. Let $X = \mathbb{C}/\Gamma$.

Theorem 2.3.6. *The map $\phi : u \mapsto (\wp(u), \wp'(u), 1)$ of $X - \{0\}$ into $\mathbb{P}^2$ extends to an isomorphism of X onto C.*

Proof: From the definition of $\wp(u)$ and the fact that its only pole is at 0, it is clear that ϕ is holomorphic in $X - \{0\}$. To see the behaviour at $u = 0$, we write

$$\wp(u) = \frac{h_1(u)}{u^2} \qquad \wp'(u) = \frac{h_2(u)}{u^3}$$

near $u = 0$, with h_i holomorphic and non-zero at 0. So ϕ can be extended to X by defining $\phi(u) = (uh_1(u), h_2(u), u^3)$. This map is holomorphic at $u = 0$ and sends 0 to (0,1,0). Moreover, ϕ is one-one on $X - \{0\}$ because $\wp'$ is odd and vanishes exactly at points of order two (corollary 2.3.3) and $\wp(u_1) = \wp(u_2)$ if and only if $u_1 = \pm u_2$. So ϕ is a one-one holomorphic map of Riemann surfaces. Hence it is an isomorphism.

Next we state explicitly the group law on cubics. For this we need a proposition.

Proposition 2.3.7. *Let u, v, w be three not necessarily distinct points of X. Then $u + v + w = 0$ if and only if $\phi(u), \phi(v), \phi(w)$ are collinear in $\mathbb{P}^2$.*

The proof of this proposition are some case by case calculations that we skip here. A proof can be found in [R V91]. Using this proposition, we get the addition law on cubics.

Theorem 2.3.8. *Let $u, v \in X - \{0\}$, $u \neq \pm v$. Let $\phi(u) = (x_1, y_1, 1)$ and $\phi(v) = (x_2, y_2, 1)$. Then $\phi(u + v) = (x, y, 1)$ where*

$$x = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \tag{2.4}$$

$$y = -\left(\frac{y_2 - y_1}{x_2 - x_1}x + \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}\right) \tag{2.5}$$

Proof: Let $y = ax + b$ be the line through $\phi(u)$ and $\phi(v)$ Then it meets the curve $y^2 = 4x^3 - g_2 x - g_3$ in the three points $\phi(u), \phi(v)$ and $\phi(-u - v)$ So x_1, x_2 and x are three roots of the equation

$$(ax + b)^2 = 4x^3 - g_2 x - g_3$$

. The sum of the roots is therefore

$$x_1 + x_2 + x = \frac{a^2}{4}$$

Since

$$a = \frac{y_2 - y_1}{x_2 - x_1}$$

2.4 is established. As

$$b = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$$

and $y = -ax - b$, 2.5 is established and the theorem is proved.

Corollary 2.3.9. *On the curve* $C : y^2 = x^3 + ax + b$*, if* $P \in C$ *is not of order* 2*, then the* x*-coordinate of* $2P$ *is*

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}$$

Chapter 3

Torsion Points

The sources of this chapter are primarily [ST92] and [Sil86].

Our next goal is to give two results on rational points on elliptic curves. After defining the group law, one can ask whether a point is of finite order. Nagell-Lutz theorem gives a criterion for determining if the given rational point is non-torsion.

3.1 Nagell-Lutz theorem

Theorem 3.1.1 (Nagell-Lutz Theorem)**.** *Let $E_{\mathbb{Q}}$ be an elliptic curve in its Weierstrass form $y^2 = f(x) = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. All nonzero torsion points $P = (x_0, y_0)$ satisfy*

1. *Coordinates of P are in $\mathbb{Z}$.*
2. *Either $y_0 = 0$, in which case P is of order 2 or $y_0^2 | D$ where D is the discriminant of $f(x)$.*

We note that the converse does not hold. An example is the cubic $y^2 = x^3 + x + 9$ and the point $P = (0, 3)$. Computation shows that $2P = (1/36, -649/216)$ which is a non-torsion point due to the above theorem.

Details of the proof can be found in [ST92].

The idea of the proof is that given a torsion point (x, y), no prime p divides the denominator of either x or y. We indicate the proof in several steps. We skip the proofs of the lemmas as they are based on straightforward calculations.

Definition 3.1.2. *Let v_p denote the p-adic norm on $\mathbb{Q}$. We define $R_p = \{q \in \mathbb{Q} | v_p(q) \geq 0\}$ where p is a prime. R_p is a closed neighborhood of 0 in p-adic topology on $\mathbb{Q}$.*

Definition 3.1.3. $C(p^\nu) = \{(x,y) \in E_{\mathbb{Q}} | v_p(x) \leq -2\nu, v_p(y) \leq -3\nu \text{ where } \nu \in \mathbb{Z}\}$

Lemma 3.1.4. *Let $(x,y) \in E_{\mathbb{Q}}$. Then $3v_p(x) = 2v_p(y)$.*

Proof: Write $x = m/np^\mu$ and $y = u/wp^\sigma$ where $p \nmid mnuw$. Substitute this expression for x and y in the equation and compare the p-adic valuation.

Lemma 3.1.5. *$C(p^\nu)$ is a subgroup of $E_{\mathbb{Q}}$ for all $\nu > 0$.*

Proof: First note that due to the definition of $C(p^\nu)$, we have

$$E_{\mathbb{Q}} \supseteq C(p) \supseteq C(p^2) \supseteq C(p^3) \supseteq ...$$

Map $\mathbb{R}^2 - \{(0,0)\} \to \mathbb{R}^2$ via the transformation $t = x/y$ and $s = 1/y$. Then lines on (x,y) plane are mapped to lines on the (t,s) plane. We can check that $(x,y) \in C(p^\nu)$ iff $t \in p^\nu R_p$ and $s \in p^{3\nu} R_p$. We need to show that if $P_1, P_2 \in C(p^\nu)$, then $P_1 + P_2 \in C(p^\nu)$ and $-P_1 \in C(p^\nu)$. This can be done by using the addition formula and calculating the p-adic norm of the result. .

Lemma 3.1.6. *The map φ given by*

$$\varphi : C(p^\nu) \to \frac{p^\nu R}{p^{3\nu} R} \tag{3.1}$$

$$(x,y) \mapsto \frac{x}{y} \tag{3.2}$$

is a homomorphism of groups with kernel $C(p^{3\nu})$.

Proof: Calculations of lemma 3.1.5 will reflect that $t(P_1 + P_2) \equiv t(P_1) + t(P_2)$ mod $p^{3\nu} R_p$. We will thus get the homomorphism

$$\varphi : C(p^\nu) \to p^\nu R_p / p^{3\nu} R_p$$
$$P \mapsto t(P) + p^{3\nu} R_p$$

It is easy to see now that $\ker(\varphi) = C(p^{3\nu})$.

Proof of the theorem: It suffices to show that for every prime p, $C(p)$ contains no points of finite order other than $\mathcal{O}$. On the contrary, let order of p be $m > 1$ and let $P \in C(p)$. Then there exists $\nu > 0$ such that $P \in C(p^\nu)$ but $P \notin C(p^{\nu+1})$.
Case 1: $p \nmid m$
$t(mP) = mt(P) \mod p^{3\nu}R_p$. And as $mP = \mathcal{O}$, we get $t(mP) = 0$. But since $p \nmid m$, m is a unit in R_p. Therefore

$$0 \equiv t(P) \mod p^{3\nu}R_p$$

which implies $P \in C(p^{3\nu})$ contradicting that $P \notin C(p^{\nu+1})$

Case 2: $p|m$
Let $m = pn$ and $P' = nP$. Then the order of P' is p. Further, since $P \in C(p)$, so $P' \in C(p)$. Again, there exists $\nu > 0$ such that $P' \in C(p^\nu)$ but $P' \notin C(p^{\nu+1})$. And

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \mod p^{3\nu}R_p \tag{3.3}$$

$$\Rightarrow t(P') \equiv 0 \mod p^{3\nu}R_p \tag{3.4}$$

As $3\nu - 1 \geq \nu + 1$, we arrive at a contradiction. This completes the proof of the theorem.

3.2 Applications

We will prove in the next chapter that the group of rational points on an elliptic curve is a finitely generated Abelian group. This theorem gives a very efficient way to compute the torsion subgroup. We will demonstrate this using some examples. We will also construct several families of curves with rank at least 1.

Computing the torsion part

The torsion part can be efficiently computed using the Nagell-Lutz theorem. We demonstrate this in some examples.

Example 3.2.1. *$C_1 : y^2 = x^3 + x$. The discriminant $D = -4$. So for a torsion point (x, y), we have $y = 0, \pm 1, \pm 2$. The point $(0, 0)$ is clearly only such solution. So the torsion part is $\mathbb{Z}/2\mathbb{Z}$. The Mordell group has rank 0. This can be seen by substituting $x = p/q$ and using that $a^4 + b^4 = c^2$ has solutions only on $abc = 0$ (as proved by*

Fermat).

Example 3.2.2. *$C_2 : y^2 = x^3 + 1$. The discriminant $D = -27$. So for a torsion point (x, y), we have $y = 0, \pm 1, \pm 3$. This gives the points $(-1, 0), (0, \pm 1), (2, \pm 3)$. For $P = (2, 3)$, we compute that $2P = (0, 1); 3P = (-1, 0); 4P = (0, -1); 5P = (2, -3); 6P = \mathcal{O}$. So the torsion part of the Mordell group is $\mathbb{Z}/6\mathbb{Z}$.*

Example 3.2.3. *$C_3 : y^2 = x^3 + x + 9$. The discriminant $D = -2391$ which is square-free. So for a torsion point (x, y), we must have $y = 0, \pm 1$. Hence there is no torsion part. It can be shown that the rank of its Mordell group is at least 2. $(0, 3)$ and $(8, 23)$ are independent.*

Families of curves of positive rank

$\mathcal{F}_1 = \{y^2 = x^3 + x + n^2 : n \in \mathbb{Z}\}$. Then the point $P = (0, n)$ lies on it and $x(2P) = 1/4n^2$. It follows that P is a non-torsion point.

Chapter 4

Mordell's theorem

The sources of this chapter are primarily [ST92] and [R V91].

Mordell's theorem asserts that $E_{\mathbb{Q}}$ is a finitely generated Abelian group. Although its proof can be found in many texts, we mention the main parts of the proof and sketch an outline because it is a central result.

We prove the theorem when the curve is of the form $y^2 = x^3 + ax^2 + bx$. The point $(0, 0)$ has order 2. We denote it by T.

4.1 Doubling map

Here we use Γ and $E_{\mathbb{Q}}$ interchangeably. We intend to prove that $|\Gamma/2\Gamma|$ is finite. This is also called weak Mordell's theorem. For this, we construct the homomorphism which sends P to $2P$.

Definition 4.1.1. *Given the curve $C : y^2 = x^3+ax^2+bx$, define $\bar{C} : y^2 = x^3+\bar{a}x^2+\bar{b}x$ where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$.*

Remark 4.1.2. *Note that $C \simeq \bar{\bar{C}}$ by replacing y by $8y$ and x by $4x$.*

Remark 4.1.3. *To prove that a map $\phi : E_{\mathbb{Q}} \to E_{\mathbb{Q}}$ is a homomorphism, it suffices to show that if $P_1 + P_2 + P_3 = O$, then $\phi(P_1) + \phi(P_2) + \phi(P_3) = \bar{O}$. This is because*

$$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$$

Proposition 4.1.4. *The map α defined as*

$$\begin{aligned}\alpha(\mathcal{O}) &= 1 \mod \mathbb{Q}^{*2}\\ \alpha(0,0) &= b \mod \mathbb{Q}^{*2}\\ \alpha(x,y) &= x \mod \mathbb{Q}^{*2} \text{ if } x \neq 0\end{aligned}$$

is a homomorphism. Moreover

$$Image(\alpha) \subseteq \{\pm p_1^{\epsilon_1}...p_t^{\epsilon_2} | \epsilon_i = 0 \text{ or } 1,\ p_i \text{ is a prime dividing } b\}$$

Proof: We start by showing that α takes inverses to inverses. For $P = \mathcal{O}, T$ it is clear. And for $P = (x,y)$, $\alpha(-P) = \alpha(x,-y) = x \equiv 1/x = \alpha(x,y)^{-1} = \alpha(P)^{-1}$ mod $\mathbb{Q}^{*2}$. Thus by Remark, it suffices to prove that $P_1 + P_2 + P_3 = O$ implies $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1$ mod $\mathbb{Q}^{*2}$. This can be proved in cases.

1. If one or both of P_i are O, then $\alpha(P_1 + O) = \alpha(P_1) = \alpha(P_1)\alpha(O)(\text{mod}\mathbb{Q}^{*2})$.

2. If both the P_i are T, then $\alpha(T+T) = \alpha(O) = 1 \equiv b^2 = \alpha(T)\alpha(T)(\text{mod}\mathbb{Q}^{*2})$

3. If $P_1 \neq O, T$ and $P_2 = T$ and say $P_1 = (x,y)$, then $\alpha(P_1{+}T) = \alpha(b/x, -by/x^2) = b/x \equiv xb = \alpha(P_1)\alpha(T)(\mod \mathbb{Q}^{*2})$.

4. Finally, if none of the $P_i s$ are $\mathcal{O}, T$, then let $y = \lambda x + \nu$ passes through $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3)$ of the cubic $y^2 = x^3 + ax^2 + bx + c$, We see that

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

$$\Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

Here $c = 0$ and $x_1x_2x_3 = \nu^2 - c = \nu^2 \in \mathbb{Q}^{*2}$. So if none of the P_i are T or O, we are done. If one of the P_i are O, say P_3, then

$$\begin{aligned}P_1 + P_2 + O &= O\\ \Rightarrow P_1 &= -P_2\end{aligned}$$

So that

$$\alpha(P_1)\alpha(P_2)\alpha(O) = \alpha(-P_2)\alpha(P_2) = \alpha(P_2)^{-1}\alpha(P_2) = 1(\text{mod}\mathbb{Q}^{*2})$$

If one of the P_i are T, say P_3, then

$$\begin{aligned} P_1 + P_2 + T &= O \\ \Rightarrow P_2 &= T - P_1 \end{aligned}$$

So that

$$\begin{aligned} \alpha(P_1)\alpha(P_2)\alpha(T) &= \alpha(P_1)\alpha(T - P_1)\alpha(T) \\ &= \alpha(P_1)\alpha(T)\alpha(-P_1)\alpha(T) \\ &= b^2 \equiv 1 \mod \mathbb{Q}^{*2} \end{aligned}$$

This shows that α is a homomorphism. Next to show where the image lies, by Lemma 3.1.4, we see that a general rational point on $E_{\mathbb{Q}}$ is of the form $\left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, where gcd$(m, e)$=gcd$(n, e)$=1. Substituting in the equation

$$n^2 = m^3 + am^2e^2 = be^4$$

Note that $\gcd(m, m^2 + ame^2 + be^4) = \gcd(m, b)$. As $n^2 = m(m^2 + ame^2 + be^4)$ is a square, we have

$$m = \pm(\text{integer})^2 p_1^{\epsilon_1} ... p_t^{\epsilon_t} \qquad \text{where } \epsilon_i = 0, 1 \text{ and } p_i | b$$

Thus, $\alpha(P) = x = m/e^2 \equiv p_1^{\epsilon_1} ... p_t^{\epsilon_t} (\text{mod} \mathbb{Q}^{*2})$ for $(x \neq 0)$. For $P = T, \alpha(T) = b \equiv p_1^{\epsilon_1} ... p_t^{\epsilon_t} (\text{mod} \mathbb{Q}^{*2})$. Thus the image of α is contained in the required group.

Proposition 4.1.5. *The map ϕ defined by*

$$\phi : C \to \bar{C} \tag{4.1}$$

$$(x, y) \mapsto (\bar{x}, \bar{y}) \qquad \text{if } x \neq 0 \tag{4.2}$$

$$\mathcal{O}, T \mapsto \bar{\mathcal{O}} \tag{4.3}$$

where $\bar{x} = y^2/x^2$ and $\bar{y} = y(x^2 - b)/x^2$ is a homomorphism with kernel $\{\mathcal{O}, T\}$.

Remark 4.1.6. *ϕ takes inverses to inverses. For $P = \mathcal{O}, T$, it is trivial. For $P \neq \mathcal{O}, T$*

$$\phi(-P) = \phi(x, -y) = \left(\left(\frac{-y}{x} \right)^2, \frac{-y(x^2 - b)}{x^2} \right) = -\phi(x, y) = -\phi(P)$$

Proof of Proposition 4.1.5: It is easy to see that ϕ is well defined and that its kernel is $\mathcal{O}, T$. To show that it is a homomorphism, we note that any morphism of curves that takes $\mathcal{O}$ to $\mathcal{O}$ is a homomorphism (see [Sil86]).

Construction of Doubling map

Let $\gamma : \bar{\bar{C}} \to C$ be the isomorphism given by $\gamma(x, y) = (x/4, y/8)$. Let $\psi = \gamma \circ \phi$. Then ψ is a well defined homomorphism. Calculations show that $\phi \circ \psi(P) = 2P$ and $\psi \circ \phi(\bar{P}) = 2\bar{P}$. This is the doubling map. We'll use these homomorphisms to prove that $\Gamma/2\Gamma$ is finite.

4.2 Weak Mordell theorem

Weak Mordell theorem asserts that $\Gamma/2\Gamma$ is finite. Before going ahead, we prove a lemma that we'll require.

Lemma 4.2.1. *Let A and B be two Abelian groups and $\phi : A \to B$ and $\psi : B \to A$ be homomorphisms such that $(A : \psi(B))$ and $(B : \phi(A))$ are finite and $\psi \circ \phi(a) = 2a$ $\forall a \in A$; $\phi \circ \psi(b) = 2b$ $\forall b \in B$ Then*

$$(A : 2A) \leq (A : \psi(B))(B : \phi(A))$$

Proof: Let $|A : \psi(B)| = n$, $|B : \phi(A)| = m$ and $\{a_1, ..., a_n\}$, $\{b_1, ..., b_n\}$ be respective set of coset representatives. Then for given $a \in A$, there exists a_i such that $a - a_i \in \psi(B)$. Let $a - a_i = \psi(b)$ for some $b \in B$. Similarly, there exists b_j such that $b - b_j \in \phi(A)$. Let $b - b_j = \phi(a')$. Thus, $a = a_i + \psi(b) = a_i + \psi(b_j + \phi(a')) = a_i + \psi(b_j) + \psi \circ \phi(a') = a_i + \psi(b_j) + 2a'$. Thus the set

$$\{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$$

covers the set of coset representatives of $(A : 2A)$. So we're done.

Lemma 4.2.2. $\ker(\alpha) = \psi(\bar{\Gamma})$

Proof: Follows from definitions.

Corollary 4.2.3. *With the notations of Proposition 4.1.4,* $|\Gamma/\psi(\bar{\Gamma})| \leq 2^{t+1}$

Proof of Weak Mordell theorem: Due to symmetry of the roles of Γ and $\bar{\Gamma}$, we have that $|\Gamma/\psi(\bar{\Gamma})|$ and $|\bar{\Gamma}/\phi(\Gamma)|$ are finite. Thus due to Lemma 4.2,1, $\Gamma/2\Gamma$ is finite.

4.3 Heights

We can define a subadditive function from the group of points $E_{\mathbb{Q}}$ to $\mathbb{R}$ called the Height function. In a sense, it measures the complexity of a rational point.

Definition 4.3.1. *Let $x = m/n$ be a rational number in its lowest form. We define Height of x as*

$$H(x) = H(m/n) = max\{|m|, |n|\}$$

For a rational point $P = (x, y) \in E_{\mathbb{Q}}$ and $x = m/n$, we define $H(P) = H(x)$. We further define $h(x) = \log H(x)$ and $h(P) = \log H(P)$.

We note three important properties of the height function.

Proposition 4.3.2. *There are finitely many points on $C : y^2 = f(x) = x^3+ax^2+bx+c$ having height bounded by a number.*

Proof: Given $k > 0$, there are finitely many rational numbers x with $h(x) < k$. For each x, there are only two choices of y. So there are finitely many points P with $h(P) < k$.

Proposition 4.3.3. *Given a point $P_0 \in C$, there exists a constant $k_0(P_0, a, b, c)$ such that for all $P \in C$,*

$$h(P + P_0) < 2h(P) + k_0$$

Proof: For $P_0 = \mathcal{O}$, take $k_0 = 0$. So we can take $P_0 \neq \mathcal{O}$. Let $P_0 = (x_0, y_0)$ and $P = (x, y)$. For $P = \mathcal{O}, \pm P_0$, we can find some k_0. So let $P \neq \mathcal{O}, \pm P_0$. By addition formula, if $P + P_0 = (\xi, \eta)$, we have

$$\xi = \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2}$$

Expanding this, we get

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

where $A, ..., G$ depend on P_0 and $C(\mathbb{Q})$. Substituting $x = m/e^2, y = n/e^3$ (due to Lemma 3.1.4), we get

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

$H(\xi) = max(|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|)$. Noting that $|m| < H(P)$, $|e| < H(P)^{1/2}$ and $|n| < KH(P)^{3/2}$ for some constant K depending on a, b, c,

we get

$$H(P+P_0) = H(\xi) \leq \max\{|AK|+|B|+|C|+|D|, |E|+|F|+|G|\}H(P)^2$$

Taking logarithms

$$h(P+P_0) \leq 2h(P) + \kappa_0$$

Proposition 4.3.4. *There is a constant $k(a,b,c) > 0$ such that for all $P \in C$,*

$$h(2P) > 4h(P) - k$$

Proof: For these finitely many points of order 2, we can choose a k such that $h(2P) \geq 4h(P) - k$. For the rest, let $P = (x,y)$ and $2P = (\xi, \eta)$. By duplication formula, we get

$$\xi + 2x = \lambda^2 - a \qquad \text{where } \lambda = f'(x)/2y$$

which gives

$$\xi = \frac{x^4 + ...}{4x^3 + ...} \tag{4.4}$$

To prove the proposition, we prove a general result.

Lemma 4.3.5. *Let $\phi(x)$and $\psi(x)$ be polynomials over $\mathbb{Z}$ with no common roots. Let d be max(deg(ϕ),deg(ψ)). Then*

1. *There exists $R \geq 1$ depending on ϕ, ψ so that $\forall m/n \in \mathbb{Q}$*

$$gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \text{ divides } R$$

2. *There exist constants κ_1, κ_2 depending only on ϕ, ψ so that $\forall m/n \in \mathbb{Q}$ which are not the roots of ψ,*

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2$$

Proof:

1. For notation, let deg(ϕ)=d and deg(ψ)=$e \leq d$. As gcd($\phi(x), \psi(x)$)=1, there

exist $F(x), G(x)$ over $\mathbb{Q}$ such that

$$F(x)\phi(x) + G(x)\psi(x) = 1$$

Let A be a large enough integer so that $AF(x), AG(x) \in \mathbb{Z}[x]$ and let $D = \max(deg(F), deg(G))$. Put $X = m/n$. Then

$$n^D AF\left(\frac{m}{n}\right) n^d \phi\left(\frac{m}{n}\right) + n^D AG\left(\frac{m}{n}\right) n^d \psi\left(\frac{m}{n}\right)$$

Let $\gamma = \gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$. Then $\gamma | An^{D+d}$. let

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + ... + a_dn^d$$
$$n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + ... + b_en^d$$

Since $\gamma | n^d\phi(m/n)$, it divides

$$An^{D+d-1}.n^d\phi\left(\frac{m}{n}\right) = Aa_0m^dn^{D+d-1} + ... + Aa_dn^{D+2d-1}$$

Thus, $\gamma | Aa_0m^dn^{D+d-1}$. So $\gamma | \gcd(An^{D+d}, Aa_0m^dn^{D+d-1})$. But $\gcd(m, n) = 1$. So, $\gamma | Aa_0n^{D+d-1}$. This gives that $\gamma | Aa_0n^{D+d-2}.\phi\left(\frac{m}{n}\right)$ and by repeating the arguments, we get that $\gamma | Aa_0n^{D+d-2}$. Continuing, we get $\gamma | Aa_0^{D+d} = R$.

2. We first prove the upper bound.

$$\begin{aligned} H\left(\frac{\phi(m/n)}{\psi(m/n)}\right) = & \max\{|a_0m^d + a_1m^{d-1}n + ... + a_dn^d|, \\ & |b_0m^en^{d-e} + ... + b_en^d|\} \\ |a_0m^d + a_1m^{d-1}n + ... + a_dn^d| \leq & \max(|a_i|).H(m/n)^d \\ |b_0m^en^{d-e} + ... + b_en^d| \leq & \max(|a_i|).H(m/n)^d \end{aligned}$$

Thus,

$$h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh(m/n) + \kappa_2$$

To prove the lower bound, exclude the finite set of points which are roots of $\phi(x)$. As $h(r) = h(1/r)$, we can assume the $\deg(\phi)$=d and $\deg(\psi)$= $e \leq d$. For ease of notation, let

$$\frac{\phi(m/n)}{\psi(m/n)} = \xi$$

Due to the last part we get that there exists $R \geq 1$ such that

$$\begin{aligned} H(\xi) &\geq \frac{1}{R} \max\left(|n^d\phi(m/n)|, |n^d\psi(m/n)|\right) \\ &\geq \frac{1}{2R}(|n^d\phi(m/n)| + |n^d\psi(m/n)|) \end{aligned}$$

We have to compare $h(\psi)$ with $dh(m/n)$. So consider

$$\begin{aligned} \frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2R}\frac{|n^d\phi(m/n)| + |n^d\psi(m/n)|}{\max(|m|^d, |n|^d)} \\ &= \frac{1}{2R}\frac{|\phi(m/n)| + |\psi(m/n)|}{\max(1, |m/n|^d)} \end{aligned}$$

So we look at

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max(1, |t|^d)}$$

As $t \to \infty$, $p(t) \to |a_0|$ or $|a_0 + b_0|$. So outside some closed interval, $p(t)$ is bounded away from 0. Inside a closed bounded interval, $p(t)$ never vanishes as $\phi(t)$ and $\psi(t)$ have no common zeros. So $p(t) \geq C_1 > 0\ \forall t \in \mathbb{R}$. Thus

$$H(\xi) \geq \frac{C_1}{2R} H(m/n)^d$$

Taking logarithms, we get

$$h(\xi) \geq dh(m/n) - \kappa_1 \qquad \text{where } \kappa_1 = \log(2R/C_1)$$

This completes the proof of the lemma.

Putting the expression for ξ as ratio given in (4.4) and noting that $d = 4$, we get the proposition.

4.4 Mordell's Theorem

Theorem 4.4.1. Γ *is finitely generated.*

Proof: Weak Mordell theorem asserts that $[\Gamma : 2\Gamma]$ is finite. Say $[\Gamma : 2\Gamma] = n$ and $\{Q_1, ..., Q_n\}$ be coset representatives of $\Gamma/2\Gamma$. Then for each $P \in \Gamma$, there is an i such

that $P - Q_i \in 2\Gamma$. Then

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \text{ for some } P_1 \in \Gamma \\ P_1 - Q_{i_2} &= 2P_2 \text{ for some } P_2 \in \Gamma \\ &\cdot \\ &\cdot \\ &\cdot \\ P_{m-1} - Q_{i_m} &= 2P_m \text{ for some } P_m \in \Gamma \end{aligned}$$

So we obtain

$$P = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m$$

Due to the relations satisfied by height,

$$h(P - Q_i) \leq 2h(P) + \kappa_i \forall P \in \Gamma$$

Letting κ' be the largest of $\kappa_1, ..., \kappa_n$, we have

$$h(P - Q_i) \leq 2h(P) + \kappa' \forall P \in \Gamma \text{ and } 1 \leq i \leq n$$

Also, there exists κ such that $h(2P) \geq 4h(P) - \kappa$. Thus

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa \qquad \forall j$$

This gives

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\kappa' + \kappa)\right) \end{aligned}$$

So if $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

Thus if P_i are such that $h(P_i) \geq \kappa' + \kappa$ for $i = 1, 2, ...$ then due to the above relation, there will be an m for which $h(P_m) \leq \kappa' + \kappa$. So any P can be written as

$$P = a_1 Q_1 + ... + a_n Q_n + 2^m R$$

for $a_i \in \mathbb{Z}$ and $R \in \Gamma$ satisfying $h(R) \leq \kappa + \kappa'$. As the number of such R is finite, we prove that Γ is finitely generated.

Because of the theorem, we know that $E_{\mathbb{Q}}$ is isomorphic to a finite product

$$\mathbb{Z} \oplus ... \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{\nu 1}} \oplus ... \oplus \mathbb{Z}_{p_s^{\nu s}}$$

The rank (of the non-torsion part) of the group is called the rank of elliptic curve. The next part gives a method to generate elliptic curves of positive ranks over $\mathbb{Q}$.

Part II

L-function and Rank of Elliptic Curves

Chapter 5

Finding curves of positive rank

The source of this chapter is primarily [PP74].

5.1 Method of Penney and Pomerance

Penney and Pomerance in their paper [PP74] use the homomorphism $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ to generate curves of large ranks. They consider the curves of the form $y^2 = x^3 + ax^2 + bx$ where $a^2 - 4b$ is not a square. This ensures that

1. $a^2 - 4b \neq 0$ so that the curve is smooth, and
2. As the points of order 2 have y-coordinate 0 and $a^2 - 4b$ is not a square, the only point of order 2 is $(0, 0)$. Therefore $\Gamma \simeq \mathbb{Z}^r \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{p_2^{a_2}} \oplus ... \oplus \mathbb{Z}_{p_t^{a_t}}$ for $p_2, ..., p_t$ odd primes.

So $\Gamma/2\Gamma \simeq (\mathbb{Z}/2\mathbb{Z})^{r+1}$ where r is the rank of the curve. From proposition 4.1.4 it follows that $2\Gamma \subset \ker(\alpha)$. As Γ is Abelian and

$$\frac{\Gamma}{\ker(\alpha)} \simeq \frac{\Gamma/2\Gamma}{\ker(\alpha)/2\Gamma}$$

we get $|\Gamma/2\Gamma| \geq |\Gamma/\ker(\alpha)|$. Summing up $|\text{Image}(\alpha)| = |\Gamma/\ker(\alpha)| \leq |\Gamma/2\Gamma| = |\mathbb{Z}_2^{r+1}| = 2^{r+1}$. From proposition 4.1.4, $\text{Image}(\alpha) \simeq \mathbb{Z}_2^s$ for some s. By finding $\text{Image}(\alpha)$ and s, we get a lower bound on the rank r.

We had seen earlier that Image(α) $\subseteq \{\pm p_1^{\epsilon_1}...p_t^{\epsilon_2} | \epsilon_i = 0 \text{ or } 1,\ p_i \text{ are primes dividing } b\}$. Penney and Pomerance use a stronger result in [PP74] which we do not prove here:

$$\text{image}(\alpha) = \{b\mathbb{Q}^{*2}\} \cup \{n\mathbb{Q}^{*2} : n \in \mathbb{Z}, n|b \text{ and } nu^4 + bv^4/n + au^2v^2 = w^2 \text{ has a solution in mutually coprime nonzero integers } u, v, w\} \quad (5.1)$$

For ease of calculations, they compute the subgroup A of Image(α) with $u = v = w = 1$. For ease of computations, they choose b square-free and search for a such that $|A|$ is large. We vary a upto $10b^{1/2}$. The authors have found some conditions on a that makes their algorithm faster. However, we do not employ those methods here and rely on better computing power. We present a program written in Python to execute their method.

Algorithm

1. Input a square-free integer $b = p_1p_2...p_n$. Its set of divisors is $C(b) = \{\pm p_1^{\epsilon_1}...p_n^{\epsilon_n}$ such that $p_i|b, \epsilon_i = 0, 1\}$. We index the divisors by variable j. Note that $|C(b)| = 2^{n+1}$

2. For a given a, if a divisor $d \in C(b)$ satisfies the condition $d + b/d + a$ =nonzero square, append it in a set $\mathcal{A}$. This set is represented by 'list1' in our program.

3. If $|\mathcal{A}| \leq 4$, discard the calculations and choose the next a. If $|\mathcal{A}| > 4$, generate the subgroup $\mathbf{A}$ of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ by the set $\mathcal{A}$. $\mathbf{A}$ is represented by 'list2' in our program.

4. Find $|\mathbf{A}| = 2^s$ (for some s). If the rank of the curve is r, then $r \geq s - 1$.

Program in Python

```
prime = [3,5,7,11,13,17,19,23]
b=1
for i in range(len(prime)):
  b=b*prime[i]
#b=-b

limita= 10*(b**0.5)
limitj= 2**(len(prime)+1)
```

```
a=0

def dectobin(n):     #Function to convert decimal to binary
  c=n
  dummylist=[]
  while c>0:
    dummylist.append(c%2)
    c=int(c/2)
  while len(dummylist)<len(prime)+1:
    dummylist.append(0)
  return dummylist

def add(lista,listb):  #Function to find index of product of two divisors
  dummylist=[]
  for i in range(len(lista)):
    dummylist.append((lista[i]+listb[i])%2)
  return dummylist

def bintodiv(l):     #Function to convert binary to decimal
  dummyvar=1
  for i in range(len(l)-1):
    dummyvar = dummyvar*(prime[i]**l[i])
  if l[-1]==1:
    dummyvar=-dummyvar
  return dummyvar

def divtobin(n):     #Function to find binary index of a divisor
  c=n
  dummylist=[]
  if c<0:
    c=-c
  for i in range(len(prime)):
    if c%prime[i]==0:
      dummylist.append(1)
    else:
```

```
      dummylist.append(0)
  if n>0:
    dummylist.append(0)
  else:
    dummylist.append(1)
  return dummylist

def log(n):      #Function to calculate log base 2
  val=0
  while n>1:
    val=val+1
    n=n/2
  return val

blist=divtobin(b)
rank=0

for a in range(limita):      #Step 1
  if b*b - 4*a>0:
    list1=[blist]
    list2=[]
    list3=[]
    divlist=[]

    for j in range(limitj):
      binlist=dectobin(j)
      divisor=1
      for i in range(len(prime)):             #Step 2
        divisor=divisor*(prime[i]**binlist[i])
      sign=binlist[-1]
      divisor=((-1)**sign)*divisor
      dummydiv= divisor + b/divisor + a
      if dummydiv>0:
        if(dummydiv==(int((dummydiv)**0.5))**2):
          list1.append(binlist)
```

```
if len(list1)>4:                          #Step 3
  for i1 in range(len(list1)):
    for i2 in range(len(list1)-i1):
      list2.append(add(list1[i1],list1[i1+i2]))
  for i in range(len(list2)):
    divlist.append(bintodiv(list2[i]))
  divlist=list(set(divlist))
  list2=[]
  for i in range(len(divlist)):
    list2.append(divtobin(divlist[i]))

  for i1 in range(len(list2)):
    for i2 in range(len(list2)-i1):
      list3.append(add(list2[i1],list2[i1+i2]))
      for i in range(len(list3)):
        divlist.append(bintodiv(list3[i]))
    divlist=list(set(divlist))
    list3=[]
    for i in range(len(divlist)):
      list3.append(divtobin(divlist[i]))

  for i in range(len(list3)):
  divlist.append(bintodiv(list3[i]))
  divlist=list(set(divlist))

rank=log(len(divlist))-1                   #Step 4

if len(divlist)>4:
  print "a=", a, "rank>=", rank
```

The divisors of b are given in the list 'prime'. This program reproduces the results of their papers [PP74] and [PP75]. We can modify this list to vary b. This program executes the algorithm for b= $3*5*7*11*13*17*19*23$ and reproduces the result that for a= 53213, the curve $y^2 = x^3 + ax^2 + bx$ has rank at least 6. We further found

that for given b, the least such positive $a = 47717$. We found the following examples.

b	a	rank$\geq$
$5 \times 13 \times 19 \times 23$	753	4
$5 \times 13 \times 19 \times 29 \times 37 \times 43$	34418	6
$3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23$	53213	6
$3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23$	47717	6
$-3 \times 7 \times 11 \times 17 \times 23 \times 31 \times 43 \times 47$	592154	7
$3 \times 5 \times 7 \times 11 \times 17 \times 23 \times 31 \times 43 \times 47$	1073	4
	12473	5
	124977	5
	349257	6
	349313	6
	562217	6
	647561	7

Chapter 6

L-series of elliptic curves

The sources of this chapter are primarily [Mil06] and [Kob84].

So far, we have considered elliptic curves over rationals. In this chapter, we shall consider elliptic curves over finite fields. We will count the number of points on the elliptic curve defined over a finite field and find a bound on the trace of the elliptic curve. For the special case of elliptic curve related to congruent number problem, we will explicitly calculate the trace and find the L-series of that elliptic curve.

6.1 Congruent number problem

Statement of the problem: Find all rational numbers q which represent area of a right triangle with sides of rational length.

We note that given a rational number q, we can find $s \in \mathbb{Q}$ such that s^2q is a square-free integer n. Moreover, if q is the area of the right triangle with sides x, y, z, then n is the area of the right triangle with sides sx, sy, sz. So we can restate our problem as

Statement of the problem: Find all square-free integers n which are area of a right triangle with sides of rational length. Such n are called congruent numbers.

We give two characterizations of the congruent number problem.

Lemma 6.1.1. *n is a congruent number if and only if there exists a rational number x such that $x - n, x, x + n$ are squares of rational numbers.*

Proof: Let n be area of the right triangle with legs X, Y and hypotenuse Z. Then $\frac{1}{2}XY = n$ and $X^2 + Y^2 = Z^2$. This gives us $(X \pm Y)^2 = Z^2 \pm 4n$. So $x = (Z/2)^2$ is the required rational number. Conversely, given x such that $x - n = a^2, x = b^2$ and $x+n = c^2$ for some $a, b, c \in \mathbb{Q}$, the right triangle with sides $X = c-a, Y = c+a, Z = 2b$ has area n.

Lemma 6.1.2. *n is a congruent number iff there is a rational point (x, y) on the curve $Y^2 = X^3 - n^2X$ such that x is a square of a nonzero rational number with even denominator.*

Proof: Let $\sqrt{x} = u \in \mathbb{Q}^+$ and $v = y/u$. Then $v^2 + n^2 = x^2$. Let t be the denominator of u. By assumption, t is even. As n is an integer, denominators of v and x are the same and so equals t^2. Thus t^2v, t^2n, t^2x is a primitive Pythagorean triplet with t^2n even. So there exist a, b such that $t^2n = 2ab, t^2v = a^2 - b^2, t^2x = a^2 + b^2$. So the right triangle with sides $2a/t, 2b/t, 2u$ has area n. Conversely, let n be a congruent number. Then by last lemma, we get rational number x with even denominator.

Definition 6.1.3. *$E_n : y^2 = f(x) = x^3 - n^2x$. By abuse of notation, $E_n : y^2z = x^3 - n^2xz^2$ in projective coordinates.*

Proposition 6.1.4. *$P \in E_n$ is a non-torsion point if and only if the x-coordinate of $2P$ is a square with even denominator.*

Proof: If part follows from Nagell-Lutz theorem. We need to prove the converse. From Corollary 2.3.9, if $P = (x, y) \in E_n$, then

$$x(2P) = \left(\frac{x^2 - n^2}{2y}\right)^2 \tag{6.1}$$

So $x(2P)$ is a square. Let X, Y, Z be the sides of a right triangle with area n. From constructions given in 6.1.1 and 6.1.2, there exists $Q \in E_n$ with $x(Q) = (Z/2)^2$. First, we show that Q is double of a point. Let

$$u = X/Z \qquad v = Y/Z$$

Then $u^2 + v^2 = 1$. So there exists $t \in \mathbb{Q}$ such that

$$u = \frac{1 - t^2}{1 + t^2} \qquad v = \frac{2t}{1 + t^2}$$

Then

$$uv = \frac{XY}{Z^2} = \frac{2n}{Z^2}$$
$$\frac{n}{Z^2} = \frac{(1-t^2)t}{(1+t^2)^2} \tag{6.2}$$

Let

$$x_0 = -nt \qquad y_0 = n^2(1+t^2)/Z$$

. By using 6.2, one can check that $P = (x_0, y_0) \in E_n$. 6.1 gives $Q = 2P$. This shows that each point Q which comes from a primitive triplet X, Y, Z with area n is double of a point. Tracing back the steps, we see that given a point which can be halved, there exists a primitive triplet X, Y, Z with area n. The numerator of Z is odd and so $(Z/2)$ has even denominator. This completes the proof.

Lemma 6.1.5. *Let $q = p^f$ and $p \nmid 2n$ (so that p is a prime of good reduction). Let $q \equiv 3 \mod 4$. Then there are $q+1$ points on E_n with coordinates in $\mathbb{F}_q$.*

Proof: By abuse of notation, we denote the image of an integer n after reduction mod p by n. There are four points of order four: $\{\mathcal{O}, (0,0), (\pm n, 0)\}$. For all other points $(x, f(x))$, $x \in \mathbb{F}_q - \{0, \pm n\}$. Arrange the elements of $x \in \mathbb{F}_q - \{0, \pm n\}$ in $(q-3)/2$ pairs as $\{x, -x\}$. As $f(x)$ is an odd function and -1 is not a square in $\mathbb{F}_q$, exactly one of $f(x)$ or $f(-x)$ is a square in $\mathbb{F}_q$. So each pair gives exactly two points $(x, \pm\sqrt{f(x)})$ or $(-x, \pm\sqrt{f(-x)})$. So we get $q-3$ points. That makes a total of $q+1$ points.

We use the idea of reduction mod p to find the torsion part of E_n. When $p \nmid 2n$, reduction mod p is a homomorphism from $E_n(\mathbb{Q})_{tors}$ to $E_n(\mathbb{F}_p)$. If this homomorphism is injective, $\#E_n(\mathbb{Q})_{tors} | \#E_n(\mathbb{F}_p)$. No number greater than 4 can divide all $\#E_n(\mathbb{F}_p)$ because there are infinitely many p of the form $p \equiv 3 \mod 4$. We just need to find for which p this homomorphism is injective. The image of a point P on $E(\mathbb{Q})_{tors}$ under this homomorphism will be denoted by $\bar{P}$.

Lemma 6.1.6. *Let $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$, then $\bar{P_1} = \bar{P_2}$ exactly when p divides $(y_1z_2 - z_1y_2), (x_2z_1 - x_1z_2)$ and $(x_1y_2 - x_2y_1)$.*

Proof: Let p divide the three expressions. We argue in cases

1. $p|x_1$: Then p divides x_2z_1 and x_2y_1. As $gcd(x_1, y_1, z_1) = 1$, so $p|x_2$. Let $p \nmid y_1$. Then $\bar{P_2} = (0 : \bar{y_1}\bar{y_2} : \bar{y_1}\bar{z_2}) = (0 : \bar{y_1}\bar{y_2} : \bar{y_2}\bar{z_1}) = (0 : \bar{y_1} : \bar{z_1}) = \bar{P_1}$. Similarly we handle the case $p \nmid z_1$.

2. $p \nmid x_1$: Then $\bar{P_2} = (\bar{x_1}\bar{x_2} : \bar{x_1}\bar{y_2} : \bar{x_1}\bar{z_2}) = (\bar{x_1}\bar{x_2} : \bar{x_2}\bar{y_1} : \bar{x_2}\bar{z_1}) = (\bar{x_1} : \bar{y_1} : \bar{z_1}) = \bar{P_1}$

Conversely, let $\bar{P_1} = \bar{P_2}$. We prove in three similar cases. First, let $\bar{x_1} \neq 0$. Then $\bar{x_2} \neq 0$. Therefore, $(\bar{x_1}\bar{x_2} : \bar{x_1}\bar{y_2} : \bar{x_1}\bar{z_2}) = (\bar{x_2}\bar{x_1} : \bar{x_2}\bar{y_1} : \bar{x_2}\bar{z_1})$. Since the first coordinate is same, the other two have to be equal as well. That is, $p|(x_2z_1 - x_1z_2)$ and $p|(x_1y_2 - x_2y_1)$. To show that $p|(y_1z_2 - z_1y_2)$, if $p|y_1, z_1$, we're done. Otherwise it follows from considering the cases by replacing x_1, x_2 by y_1, y_2 and z_1, z_2.

Proposition 6.1.7. $\#E_n(\mathbb{Q})_{tors} = 4$

Proof by contradiction: Suppose E_n contains a point of finite order greater than 2. Then it contains an element of odd order or there are 8 or more points of order dividing 4. In either case, we have a subgroup of $E_n(\mathbb{Q})_{tors}$ of order 8 or odd. Let it be $\{P_1, ..., P_m\}$ and $P_i = (x_i : y_i : z_i)$. Let n_{ij} be the gcd of $(y_iz_j - z_iy_j), (x_jz_i - x_iz_j)$ and $(x_iy_j - x_jy_i)$. Then by the previous lemma, $\bar{P_i} = \bar{P_j}$ iff $p|n_{ij}$. So if p is a prime of good reduction greater than all the n_{ij}, then reduction mod p is an injection. Thus for all but finitely many p, $m|\#E_n(\mathbb{F}_p)$. So for all large enough primes congruent to 3 mod 4, we have $p \equiv -1 \mod m$. But for both $m = 8$ or odd, this contradicts Dirichlet's theorem on primes in arithmetic progression. This completes the proof.

We also get a criterion for checking if a number is a congruent number.

Proposition 6.1.8. *n is a congruent number iff $E_n(\mathbb{Q})$ has positive rank.*

Proof: Let n be congruent. Then by Lemma 6.1.2, we have a rational point $(x, y) \in E_n$ such that x is a square. As the only points of order 2 are $(0, 0)$, $(\pm n, 0)$, there must be another point of order greater than 2. By Proposition 6.1.7, this has to be non torsion. Conversely, let P be of infinite order. Due to 6.1.4 the x coordinate of $2P$ is a square with even denominator. By Lemma 6.1.2, n is a congruent number.

6.2 Curves over Finite fields

Let K=$\mathbb{F}_p$ and L be an extension field. The problem is to find $\#E_K(L)$. We consider $p \neq 2, 3$ so that the curve can be reduced to the form $y^2 = x^3 + ax + b$. A prime p is called a prime of good reduction if the curve reduced mod p remains non-singular. Otherwise it is called a prime of bad reduction. Further, we'll work with the projective closure of this curve: $Y^2Z = X^3 + aXZ^2 + bZ^3$.

Let χ be a quadratic character of $\mathbb{F}_q$ for $q = p^r$. That is, $\chi(a) = 1$ if a is a square in $\mathbb{F}_q^\times$ and -1 otherwise. It is extended to $\mathbb{F}_q$ by assigning $\chi(0) = 0$. Let N_q be the number of points on $E_{\mathbb{F}_q}$. There is a point $(0:1:0)$ at infinity and all others are in the affine $x - y$ plane. We have

$$N_q = 1 + \sum_{x \in \mathbb{F}_q} (\chi(x^3 + ax + b) + 1) \tag{6.3}$$

$$= q + 1 - 2a_q \tag{6.4}$$

Here $-2a_q = \sum \chi(x^3 + ax + b)$. Heuristically, there is no reason to expect that $(x^3 + ax + b)$ is more likely to be a square than not. So $-2a_q$ is a sum of q terms randomly distributed between $+1$ and -1. The expected sum will therefore be of the order of $\sqrt{q}$. A general result that we do not prove here is the Riemann hypothesis for elliptic curves. It states

$$|a_q| < \sqrt{q} \tag{6.5}$$

In the next section, we will prove this result for E_n.

6.2.1 Zeta functions

Distribution of prime numbers in $\mathbb{Z}$ can be studied by studying the Dirichlet series

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ is a prime}} \frac{1}{(1 - p^{-s})}$$

The infinite sum converges for $s \in \mathbb{C}$ with $\mathcal{R}(s) > 1$. The product formula can be shown to hold in this domain. Moreover, this function can be extended to whole of $\mathbb{C}$ by a meromorphic function with single simple pole at $s = 1$. This idea can be generalized to varieties over number fields and finite fields. For a number field K, we define the $\zeta-$function of K as

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathbb{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{(1 - \mathbb{N}(\mathfrak{p})^{-s})}$$

where the sum is over all ideals $\mathfrak{a}$ of $\mathcal{O}_K$, the product runs over all the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and $\mathbb{N}$ is the norm of an ideal from K to $\mathbb{Q}$. These converge for $s \in \mathbb{C}$ with

$\mathcal{R}(s) > 1$. We can similarly define zeta function of a curve $C : f(x, y) = 0$ over $\mathbb{F}_p$ as

$$\zeta(C, s) = \prod_{\mathfrak{p}} \frac{1}{(1 - \mathbb{N}(\mathfrak{p})^{-s})}$$

where $\mathfrak{p}$ varies over prime ideals of $\mathbb{F}_p(x, y) = \mathbb{F}_p(X, Y)/(f(X, Y))$. We have $\mathbb{N}(\mathfrak{p}) = p^{\deg \mathfrak{p}}$. Defining

$$Z(C, T) = \prod_{\mathfrak{p}} \frac{1}{(1 - T^{deg\mathfrak{p}})} \tag{6.6}$$

we have $\zeta(C, s) = Z(C, p^{-s})$. For formal power series, we can define logarithms and exponents.

Definition 6.2.1.

$$\exp(T) = 1 + T + T^2/2! + ... + T^n/n! + ...$$
$$-\log(1 - T) = T + T^2/2 + ... + T^n/n + ...$$

One can check that these are inverses of each other in the ring of formal power series.

Take logarithms and expand $Z(C, T)$ as formal power series to get

$$\log Z(C, T) = -\sum_{\mathfrak{p}} \log(1 - T^{\deg \mathfrak{p}}) \tag{6.7}$$

Taking derivative of equation 6.7, we get the formal series

$$\frac{Z'(C, T)}{Z(C, T)} = \sum_{\mathfrak{p}} \sum_{n \geq 0} (\deg \mathfrak{p}) T^{(n+1) \deg \mathfrak{p}} \tag{6.8}$$

The coefficient of T^{m-1} is $\sum \deg \mathfrak{p}$ where the sum runs over monic irreducible $\mathfrak{p}$ with $\deg \mathfrak{p} | m$. As $\deg \mathfrak{p} = [\mathbb{F}_p[x, y]/\mathfrak{p} : \mathbb{F}_p]$, the condition $\deg \mathfrak{p} | m$ means that there exists a monomorphism $\mathbb{F}_p[C]/\mathfrak{p} \hookrightarrow \mathbb{F}_{p^m}$. As $\mathbb{F}_p[C]/\mathfrak{p}$ is separable over $\mathbb{F}_p$, there are exactly $\deg \mathfrak{p}$ homomorphisms. Conversely, every homomorphism $F_p[x, y] \to \mathbb{F}_{p^m}$ factors through $\mathbb{F}_p[x, y]/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ with $\deg \mathfrak{p} | m$. So the coefficient of T^{m-1} in 6.8 is the number of $\mathbb{F}_p-$algebra homomorphisms $\mathbb{F}_p[x, y] \to \mathbb{F}_{p^m}$. The image a, b of x, y determines the above homomorphisms and conversely, such a homomorphism factors through $\mathbb{F}_p[X, Y]/(f(X, Y))$ if and only if $f(a, b) = 0$. We thus have a one-one

correspondence

$$\{\mathbb{F}_p \text{ algebra homomorphisms } \mathbb{F}_p[C] \to \mathbb{F}_{p^m}\} \longleftrightarrow C(\mathbb{F}_{p^m})$$

This gives us the formal power series

$$\log Z(C,T) = \sum_{m\geq 1} N_m \frac{T^m}{m}$$

where $N_m = \#C(\mathbb{F}_{p^m})$. Taking exponents,

$$Z(C,T) = \exp\left(\sum_{m\geq 1} N_m \frac{T^m}{m}\right)$$

We state a lemma that will be used later.

Lemma 6.2.2. *If there exist $\alpha_1, ..., \alpha_s, \beta_1, ..., \beta_t$ such that for all $m \geq 1$, $N_m = \beta_1^m + ... + \beta_t^m - \alpha_1^m - ... - \alpha_s^m$. Then*

$$Z(T) = \frac{(1-\alpha_1 T)...(1-\alpha_s T)}{(1-\beta_1 T)...(1-\beta_t T)}$$

Proof:

$$\begin{aligned}
Z(T) &= \exp\left(\sum_{m\geq 1}(\beta_1^m + ... + \beta_t^m - \alpha_1^m - ... - \alpha_s^m)\frac{T^m}{m}\right) \\
\log Z(T) &= \sum_{m\geq 1}(\beta_1^m + ... + \beta_t^m - \alpha_1^m - ... - \alpha_s^m)\frac{T^m}{m} \\
&= \sum_{m\geq 1}\beta_1^m\frac{T^m}{m} + ... + \sum_{m\geq 1}\beta_t^m\frac{T^m}{m} - \sum_{m\geq 1}\alpha_1^m\frac{T^m}{m} - ... - \sum_{m\geq 1}\alpha_s^m\frac{T^m}{m} \\
&= -\log(1-\beta_1 T) - ... - \log(1-\beta_t T) + \log(1-\alpha_1 T) + ... + \log(1-\alpha_s T) \\
&= \log\left(\frac{(1-\alpha_1 T)...(1-\alpha_s T)}{(1-\beta_1 T)...(1-\beta_t T)}\right) \\
Z(T) &= \frac{(1-\alpha_1 T)...(1-\alpha_s T)}{(1-\beta_1 T)...(1-\beta_t T)}
\end{aligned}$$

6.3 Zeta function of E_n

It turns out that (see [Sil86]) the zeta function of an elliptic curve has the form

$$Z(E/\mathbb{F}_q, T) = \frac{1 - 2a_E T + qT^2}{(1-T)(1-qT)}$$

We shall show this for E_n. To calculate $\#E_n(\mathbb{F}_q)$ we first convert it into diagonal form.

Lemma 6.3.1. *There is a one-one correspondence between the points of* $E_n - \{(0,0), \mathcal{O}\}$ *and* $E'_n : u^2 = v^4 + 4n^2$.

Proof: Let $(u,v) \in E'_n$. Then we can check that $(x,y) = (\frac{1}{2}(u+v)^2, \frac{1}{2}v(u+v^2)) \in E_n$. Conversely, if $(x,y) \in E_n$ with $x \neq 0$ then the point $(u,v) = (2x - \frac{y^2}{x^2}, \frac{y}{x}) \in E'_n$.

Corollary 6.3.2. *Let* $p \nmid 2n$ *(that is,* p *is a prime of good reduction),* $q = p^r$, $N = \#E_n(\mathbb{F}_q)$ *and* $N' = \#E'_n(\mathbb{F}_q)$. *Then due to lemma 6.1.6* $N = N' + 2$.

Definition 6.3.3 (Characters on finite fields)**.** .

1. *An additive character of finite field* $\mathbb{F}_q$ *is a homomorphism* $\psi : \mathbb{F}_q \to \mathbb{C}^*$ *such that* $\psi(x+y) = \psi(x)\psi(y)$ *for* $x, y \in \mathbb{F}_q$. *In what follows, we will define* $\psi(x) = \xi^{tr(x)}$ *where* $tr(x)$ *is the trace of* x *from* $\mathbb{F}_q$ *to* $\mathbb{F}_p$ *and* ξ *is a primitive* q^{th} *root of unity.*

2. *A multiplicative character of finite field* $\mathbb{F}_q$ *is a homomorphism* $\psi : \mathbb{F}_q^* \to \mathbb{C}^*$ *such that* $\chi(x+y) = \chi(x)\chi(y)$ *for* $x, y \in \mathbb{F}_q^*$. *We extend* χ *to* $\mathbb{F}_q$ *by defining* $\chi(0) = 0$.

3. *For a multiplicative character* χ, $\bar{\chi}(x)$ *is defined as the complex conjugate of* $\chi(x)$. χ_0 *denotes the trivial multiplicative character which takes nonzero elements of* $\mathbb{F}_q$ *to 1.*

Definition 6.3.4 (Gauss sum and Jacobi sum)**.** .

1. *Given a multiplicative character* χ, *we define Gauss sum as*

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x)$$

2. *Given two multiplicative characters* χ_1, χ_2, *we define Jacobi sum as*

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x)$$

We next prove some properties of Gauss and Jacobi sums that will be used later.

Lemma 6.3.5. *Let χ, χ_1, χ_2 be nontrivial characters. Then*

1. $g(\chi_0) = -1; J(\chi_0, \chi_0) = q - 2; J(\chi_0, \chi) = -1; J(\chi, \bar{\chi}) = -\chi(-1); J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$
2. $g(\chi)g(\bar{\chi}) = \chi(-1)q; |g(\chi)| = \sqrt{q}$
3. $J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ *if* $\chi_2 \neq \bar{\chi}_1$

Proof:

1.

$$
\begin{aligned}
g(\chi_0) &= \sum_{x\in\mathbb{F}_q} \chi_0(x)\psi(x) = \sum_{x\neq 0} \psi(x) = -1 \\
J(\chi_0, \chi_0) &= \sum_{x\in\mathbb{F}_q} \chi_0(x)\chi_0(1-x) = \sum_{x\neq 0,1} 1 = q - 2 \\
J(\chi_1, \chi_2) &= \sum_{x\in\mathbb{F}_q} \chi_1(x)\chi_2(1-x) = \sum_{y\in\mathbb{F}_q} \chi_1(1-y)\chi_2(y) = J(\chi_2, \chi_1) \\
J(\chi_0, \chi) &= J(\chi, \chi_0) = \sum_{x\in\mathbb{F}_q} \chi(x)\chi_0(1-x) = \sum_{x\neq 1} \chi(x) = -\chi(1) = -1 \\
J(\chi, \bar{\chi}) &= J(\bar{\chi}, \chi) = \sum_{x\neq 0} \bar{\chi}(x)\chi(1-x) = \sum_{x\neq 0} \chi(x^{-1}-1) = \sum_{y\neq -1} \chi(y) = -\chi(-1)
\end{aligned}
$$

2.

$$
\begin{aligned}
g(\chi)g(\bar{\chi}) &= \left(\sum_{x\in\mathbb{F}_q} \chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q} \bar{\chi}(y)\psi(y)\right) = \sum_{x,y\neq 0} \chi(xy^{-1})\psi(x+y) \\
&= \sum_{y,t\neq 0} \chi(t)\psi(ty+y) = \sum_{t\neq 0,-1} \chi(t) \sum_{y\neq 0} \psi(y(t+1)) + \chi(-1)(q-1) \\
&= -\sum_{t\neq 0,-1} \chi(t) + (q-1)\chi(-1) = \chi(0) + \chi(-1) + (q-1)\chi(-1) \\
&= q\chi(-1)
\end{aligned}
$$

$$
\begin{aligned}
|g(\chi)|^2 = g(\chi)\overline{g(\chi)} &= \left(\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x)\right)\overline{\left(\sum_{y\in\mathbb{F}_q}\chi(y)\psi(y)\right)} \\
&= \left(\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\overline{\chi}(y)\overline{\psi}(y)\right) \\
&= \left(\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\overline{\chi}(y)\psi(-y)\right) \\
&= \left(\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\overline{\chi}(-y)\psi(y)\right) \\
&= \bar{\chi}(-1)\left(\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\overline{\chi}(y)\psi(y)\right) \\
&= \bar{\chi}(-1)g(\chi)g(\bar{\chi}) \\
&= \bar{\chi}(-1)q\chi(-1) = q \\
|g(\chi)| &= \sqrt{q}
\end{aligned}
$$

3.

$$
\begin{aligned}
J(\chi_1,\chi_2)g(\chi_1\chi_2) &= \left(\sum_{x\in\mathbb{F}_q}\chi_1(x)\chi_2(1-x)\right)\left(\sum_{y\in\mathbb{F}_q}\chi_1\chi_2(y)\psi(y)\right) \\
&= \sum_{x,y\in\mathbb{F}_q}\chi_1(xy)\chi_2(y(1-x))\psi(y) \\
&= \sum_{x\neq 0,1;y\neq 0}\chi_1(xy)\chi_2(y(1-x))\psi(y)
\end{aligned}
$$

Change variables as $t = xy$, $s = y - xy$

$$
J(\chi_1,\chi_2)g(\chi_1\chi_2) = \sum_{t,s\neq 0}\chi_1(t)\chi_2(s)\psi(s+t) = \sum_{t,s\in\mathbb{F}_q}\chi_1(t)\chi_2(s)\psi(s+t) = g(\chi_1)g(\chi_2)
$$

As $\chi_2 \neq \bar{\chi}_1, g(\chi_1\chi_2) \neq 0$ and we can invert it.

This completes the proof of the lemma.

We now compute N'. Observe that the number of solutions to the equation $x^m = a$ is given by

Lemma 6.3.6.

$$\#\{x^m = a\} = \sum_{\chi^m = \chi_0} \chi(a) \tag{6.9}$$

Proof: Let G be a finite Abelian group and $\hat{G}$ denote the group of characters. Then one can show that $G \simeq \hat{G}$ and we have the two orthogonality relations

$$\sum_{g \in G} \chi(g) = 0 \qquad \text{for } \chi \neq \chi_0$$

$$\sum_{\chi \in \hat{G}} \chi(g) = 0 \qquad \text{for } g \neq 1_G$$

For our purpose, let $G = \mathbb{F}_q^*$ and $S = \{\chi | \chi^m = \chi_0\}$. Note that S is a subgroup of $\hat{G}$. The restriction of a character of G to S gives a character of S. Consider the equation 6.9. If $LHS = 0$, then χ are independent characters of S and so $RHS = 0$ due to the orthogonality relation. So let there exist $x \in \mathbb{F}_q^*$ such that $x^m = a$. We have two cases:

1. $m \nmid (q-1)$: The homomorphism which sends $x \to x^m$ is an automorphism of $\mathbb{F}_q^*$. So $LHS = 1$. As $\#\hat{G} = q - 1$, $RHS = 1$.

2. $m | (q-1)$: $\sum_{\chi^m = \chi_0} \chi(a) = \sum_{\chi^m = \chi_0} \chi(x^m) = \sum_{\chi^m = \chi_0} \chi^m(x) = \sum_{\chi^m = \chi_0} \chi_0(x) = \#\{\chi | \chi^m = \chi_0\} = \#\{\zeta | \zeta^m = 1\} = \#\{\zeta x | (\zeta x)^m = a\} = \#\{y | y^m = a\}$

This proves the lemma.

Due to Lemma 6.1.5, we have $N = q + 1$ if $q \equiv 3 \mod 4$. So let $q \equiv 1 \mod 4$. We prove the following lemma and go on to calculate N' and N in the following proposition.

Lemma 6.3.7. *If* $q \equiv 1 \mod 4$, $\chi_4(-4) = 1$

Proof: Let $(q-1)/4 = m$. As $\mathbb{F}_q^*$ is a cyclic group, we can explicitly write $\chi_4(x) = \exp(2\pi i n m x/(q-1))$ where $gcd(q-1, n) = 1$. If $q \equiv 1 \mod 8$, then m is even and we get $\chi_4(4) = \exp(8\pi i n m/(q-1)) = 1$ and $\chi_4(-1) = \exp(-2\pi i n m/(q-1)) = 1$. Otherwise, if $q \equiv 5 \mod 8$, then m is odd and we get $\chi_4(4) = \exp(8\pi i n m/(q-1)) = -1$ and $\chi_4(-1) = \exp(-2\pi i n m/(q-1)) = -1$. In both cases, $\chi_4(-4) = 1$.

Proposition 6.3.8. *For $q \equiv 1 \mod 4$, $N = \#E_n(\mathbb{F}_q) = q+1-\alpha-\bar{\alpha}$ for an algebraic integer α in $\mathbb{Q}[i]$.*

Proof: We can express

$$N' = \#\{u \in F_q | u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} + \#\{u, v \in \mathbb{F}_q^* | u^2 = v^4 + 4n^2\}$$

The first term is 2 as $p \nmid 2n$. To evaluate the second term, let χ_4 be a character of exact order 4. Then by 6.3.6, the second term is

$$\sum_{j=1}^{4} \chi_4^j(-4n^2) = 2 + 2\chi_4(-4n^2)$$

To calculate the third term, let $\chi_2 = \chi_4^2$. Then χ_2 has exact order 2. Again by 6.3.6, we can write it as

$$\sum_{a,b \in \mathbb{F}_q^*; a=b+4n^2} \#\{u^2 = a\}\#\{v^4 = b\} = \sum_{a \in \mathbb{F}_q^*; a-4n^2 \neq 0} \sum_{j=1,2,3,4; k=1,2} \chi_2^k(a)\chi_4^j(a-4n^2)$$

Since $\chi_4(0) = 0$, we can drop the condition $a - 4n^2 \neq 0$ in the sum. Make a change of variable as $x = a/4n^2$ and rewrite the summation as

$$\sum_{j=1,2,3,4; k=1,2} \chi_4^j(-4n^2) \sum_{a \in \mathbb{F}_q^*} \chi_2^k(a)\chi_4^j(1-x) = \sum_{j=1,2,3,4; k=1,2} \chi_4^j(-4n^2) J(\chi_2^k, \chi_4^j)$$

Adding these three quantities and using the properties of Jacobi sums stated in 6.3.5, we get

$$N' = q - 1 + \chi_4(-4n^2)(J(\chi_2, \chi_4) + J(\chi_2, \bar{\chi}_4))$$

As $\chi_4(-4) = 1$, we have $\chi_4(-4n^2) = \chi_2(n)$. Setting $\alpha = -\chi_2(n)J(\chi_2, \chi_4)$, we get

$$N = q + 1 - \alpha - \bar{\alpha}$$

As α is a polynomial in χ_4, it is an algebraic integer in $\mathbb{Q}[i]$. This completes the proof.

We can write $\alpha = a + bi$ for $a, b \in Z$. By 6.3.5, we have

$$\alpha = \frac{-\chi_2(n)g(\chi_2)g(\chi_4)}{g(\bar{\chi}_4)}$$

Again by 6.3.5, we get $|\alpha|^2 = a^2 + b^2 = q$. This gives the result 6.5 for E_n. We can easily mention explicitly what α is in the cases $q = p \equiv 1 \mod 4$ and $q = p^2$ for $p \equiv 3 \mod 4$. In the case $q = p \equiv 1 \mod 4$, there are eight choices of α given by $\pm a \pm bi$ and $\pm b \pm ai$. In the case $q = p^2$ for $p \equiv 3 \mod 4$, $a^2 + b^2 = p^2$ there are four possibilities of α given by $\pm p, \pm pi$. The following lemma helps us determine them.

Lemma 6.3.9. *Let $q \equiv 1 \mod 4$. Then $1 + J(\chi_2, \chi_4)$ is divisible by $2 + 2i$ in $\mathbb{Z}[i]$.*

Proof: Noting that $\chi_2 = \chi_4^2$ and using Lemma 6.3.5, we get $J(\chi_2, \chi_4) = \chi_4(-1)J(\chi_4, \chi_4)$. We can write

$$J(\chi_4, \chi_4) = \sum \chi_4(x)\chi_4(1-x) = \chi_4^2\left(\frac{p+1}{2}\right) + 2 \sum^{*} \chi_4(x)\chi_4(1-x)$$

where $\sum^*$ is the sum over $(q-3)/2$ elements, one of each $x, 1-x$ without the pair $\frac{p+1}{2}, \frac{p+1}{2}$. Each $\chi_4(x)$ is a power of i and so is congruent to $1 \mod 1+i$. Thus $2\chi_4(x)\chi_4(1-x) \equiv 2 \mod 2+2i$. This gives

$$J(\chi_4, \chi_4) \equiv q - 3 + \chi_4^2\left(\frac{p+1}{2}\right) \mod 2+2i$$

. Since $(2+2i)(1-i) = 4$ and $q \equiv 1 \mod 4$, we get

$$q - 3 + \chi_4^2\left(\frac{p+1}{2}\right) \equiv 2 + \chi_4(4) \mod 2+2i$$

We thus get

$$1 + J(\chi_2, \chi_4) \equiv 1 + \chi_4(-1)J(\chi_4, \chi_4) \equiv 1 + 2\chi_4(-1) + \chi_4(-4) \mod 2+2i$$

Since $\chi_4(-4) = 1$ (due to 6.3.7) and $1 + \chi_4(-1) = 0$ or 2, the result follows.

We are one step from proving the main result of this section. We assert without proof the following theorem.

Theorem 6.3.10 (Hasse-Davenport relation)**.** *Let $\mathbb{N}_r$ be the norm of $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ and χ be a multiplicative character of $\mathbb{F}_q$. Then,*

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r$$

We now prove the main result of this section

Theorem 6.3.11. *Let E_n be defined over F_p with $p \nmid 2n$. Then*

$$Z(E_n/\mathbb{F}_p, T) = \frac{1 - 2aT + pT^2}{(1-T)(1-pT)} = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)} \tag{6.10}$$

where $\alpha = i\sqrt{p}$ if $p \equiv 3 \mod 4$; $\alpha \in \mathbb{Z}[i]$ with norm p and $\alpha \equiv \left(\frac{n}{p}\right) \mod (2+2i)$ if $p \equiv 1 \mod 4$.

Proof: We introduce a few notations. Let $\mathbb{N}_r$ denote the norm from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. Then $\chi_{l,r} = \chi_l \circ \mathbb{N}_r$ is a character of $\mathbb{F}_{q^r}$ if χ_l is a character of $\mathbb{F}_q$.

Using the proof of 6.3.8, we can write

$$\#E_n(\mathbb{F}_{q^r}) = q^r + 1 - \alpha_{n,q^r} - \bar{\alpha}_{n,q^r}$$

where

$$\alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\bar{\chi}_{4,r})} \tag{6.11}$$

We'll need Hasse-Davenport relation

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r$$

Applying this to 6.11 and observing that $\chi_{2,r}(n) = \chi_2(n)^r$, we get the relation

$$\alpha_{n,q^r} = \alpha_{n,q}^r$$

The theorem now follows. For $q = p \equiv 1 \mod 4$, $\chi_2(n) = \left(\frac{n}{p}\right)$. Then $\alpha = \alpha_{n,p} \in \mathbb{Z}[i]$ with norm p and $\alpha \equiv \left(\frac{n}{p}\right) \mod (2+2i)$. We thus get

$$N_r = p^r + 1 - \alpha^r - \bar{\alpha}^r$$

Using lemma 6.2.2 we get the result when $p \equiv 1 \mod 4$. For the case $p \equiv 3 \mod 4$ and $q = p^2$, $\chi_2(n) = 1$ since all elements of $\mathbb{F}_p$ are squares in $\mathbb{F}_{p^2}$. Then by previous lemma, $\alpha_{n,q}$ is a Gaussian integer of norm q and is congruent to $1 \mod (2+2i)$. Out of $p, ip, -p, -ip$ only $-p$ satisfies the congruence condition. So $\alpha_{n,q} = -p$. Thus for even r,

$$N_r = p^r + 1 - (-p)^{r/2} - (-p)^{r/2}$$

And for r odd, $N_r = p^r + 1$. Thus for any r, we have

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r$$

Again by lemma 6.2.2, we get the result. This completes the proof.

The primes in the ring $\mathbb{Z}[i]$ are either

1. $P = (1+i)$, which occurs in the splitting of $2 = (1+i)^2$
2. $P = (p)$ for $p \equiv 3 \mod 4$, p a prime in $\mathbb{Z}$
3. P such that $(p) = P\bar{P}$ for $p \equiv 1 \mod 4$, p a prime in $\mathbb{Z}$. p is said to split in this case.

For a prime P dividing (p), degree of P denoted by $\deg P$ is defined to be the degree of the extension $\mathbb{Z}[i]/P$ over $\mathbb{F}_p$. It is 1 if p splits and 2 otherwise. We can thus rephrase the above theorem.

Theorem 6.3.12.

$$(1-T)(1-pT)Z(E_n/\mathbb{F}_p, T) = \prod_{P|(p)} (1 - (\alpha_p T)^{\deg P})$$

where $\alpha_p = i\sqrt{p}$ if $P = (p)$ and $\alpha_p = a + bi$ if p splits. Here $a + bi$ is the unique generator of P such that $\alpha_p \equiv \left(\frac{n}{p}\right) \mod (2+2i)$. If $P|2n$, we take $\alpha_p = 0$.

6.4 L-series of E_n

In this section, we will define the L-series of an elliptic function, compute explicitly the L-series of E_n and find its functional equation. We will also define the root number. We will see that conjecturally, n must be a congruent number if $n \equiv 5, 6, 7 \mod 8$, but there is no obvious reason to believe it.

6.4.1 The prototype

Definition 6.4.1. *L-Series related to (an extended) multiplicative Dirichlet character χ of $\mathbb{F}_p$ is defined as the series*

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_{l \equiv \text{ prime in } \mathbb{Z}} \left(1 - \frac{\chi(l)}{l^s}\right)^{-1}$$

This converges absolutely for $\mathcal{R}(s) > 1$.

For the trivial character $\chi = \chi_0$, it is related to the Riemann zeta function as

$$L(s, \chi_0) = \left(1 - \frac{1}{p^s}\right) \zeta(s)$$

We will define L-series related to an elliptic curve and indicate the similarities with above definition.

6.4.2 L-series of E_n

Definition 6.4.2. *L-series of an elliptic curve $E_{\mathbb{Q}}$ is defined as*

$$L(E, s) = \frac{\zeta(s)\zeta(1-s)}{\prod_p Z(E/\mathbb{F}_p, p^{-s})} = \prod_{p \equiv \text{ good reduction}} \frac{1}{1 - 2a_p p^{-s} + p^{1-2s}}$$

where a_p occurs as in 6.4.

In the case of E_n, we have the formula for $Z(E_n/\mathbb{F}_p, p^{-s})$, which gives

$$L(E_n, s) = \frac{\zeta(s)\zeta(1-s)}{\prod_p Z(E_n/\mathbb{F}_p, p^{-s})} \tag{6.12}$$

$$= \prod_{p \nmid 2n} \frac{1}{1 - 2a_p p^{-s} + p^{1-2s}} \tag{6.13}$$

$$= \prod_{P \nmid 2n} \frac{1}{1 - \alpha_P^{\deg P} (\mathbb{N}P)^{-s}} \tag{6.14}$$

This product formula holds formally. In the following lemma, we find its domain of convergence.

Lemma 6.4.3. *The product formula for $L(E_n, s)$ converges for $s \in \mathbb{C}$ with $\mathcal{R}s > 3/2$.*

Proof: The product converges for s where $\sum_P |\alpha_P|^{\deg P} (\mathbb{N}P)^{-\mathcal{R}s}$ converges. By 6.3.8, $|\alpha_P|^{\deg P} = \mathbb{N}P^{1/2}$. As $(p) = P$ or $(p) = P\bar{P}$, $\mathbb{N}P \geq p$. So $\mathbb{N}P^{1/2-s} \leq p^{1/2-s}$ for $s \geq 1/2$. As each (p) has at most two factors, the sum is bounded by $2\sum_p p^{1/2-s}$, which converges for $\mathcal{R}s > 3/2$.

The aim of rest of this chapter will be to explicitly find the expression of $L(E_n, s)$.

Definition 6.4.4. *We define three maps that will be used to compute the L-series.*

1. *For $x \in \mathbb{Z}[i]$ prime to 2, define $\chi_1'(x)$ as*

$$\chi_1'(x) = i^j \text{ with } j \in \{0,1,2,3\} \text{ such that } i^j x \equiv 1 \mod (2+2i)$$

2. *For $x \in \mathbb{Z}[i]$, define $\chi_n'(x)$ as*

$$\chi_n'(x) = \begin{cases} \chi_1'(x)\left(\frac{n}{\mathbb{N}x}\right) & \text{for } x \text{ prime to } 2n \\ 0 & \text{otherwise} \end{cases}$$

3. *For $x \in \mathbb{Z}[i]$, define $\tilde{\chi}_n(x) = x\chi_n'(x)$*

Proposition 6.4.5. *$\tilde{\chi}_n$ is a multiplicative map $\mathbb{Z}[i] \to \mathbb{Z}[i]$ such that for any prime ideal P and any generator x of P, $\tilde{\chi}_n(x) = \alpha_P^{\deg P}$.*

Proof: Let x generate a prime ideal $P = (x)$. If $x|2n$, then $\left(\frac{n}{\mathbb{N}x}\right) = 0 = \alpha_P$. Otherwise, if $x \nmid 2n$,

1. If $P = (p)$ with $p \equiv 3 \mod 4$, then $\left(\frac{n}{\mathbb{N}x}\right) = \left(\frac{n}{p^2}\right) = \left(\frac{n}{p}\right)^2 = 1$. So $\tilde{\chi}_n(x) = x\chi_1'(x) = xi^j \equiv 1 \mod (2+2i)$. Therefore, $\tilde{\chi}_n(x) = -p = \alpha_P^2$.

2. If $(p) = P\bar{P}$ with $p \equiv 1 \mod 4$ and $P = (x)$, then x has norm p. $\tilde{\chi}_n(x) = xi^j\left(\frac{n}{p}\right) \equiv \left(\frac{n}{p}\right) \mod (2+2i)$. Due to 6.3.12 $\tilde{\chi}_n(x) = \alpha_P$.

Corollary 6.4.6. *It makes sense to define $\tilde{\chi}_n(P) = \tilde{\chi}_n(x)$ for a prime ideal $P = (x)$.*

If we assume x prime to 2 in $\mathbb{Z}[i]$, then we note that χ_1' is a character of $\mathbb{Z}[i]/(2+2i)^*$ which takes x to a root of unity in the class $1/x$.

Remark 6.4.7. *Due to the above proposition, we can write*

$$L(E_n, s) = \prod_{P \nmid 2n} \left(1 - \frac{\tilde{\chi}_n(P)}{(\mathbb{N}P)^s}\right)^{-1} \tag{6.15}$$

$\mathbb{Z}[i]$ is a Dedekind domain. So ideals factor uniquely as product of prime ideals. Also $\tilde{\chi}_n$ and $\mathbb{N}$ are multiplicative (follows from definitions). Thus we can expand 6.15 into formal series

$$L(E_n, s) = \sum_I \tilde{\chi}_n(I)(\mathbb{N}I)^{-s} \tag{6.16}$$

The sum runs over nonzero ideals I of $\mathbb{Z}[i]$. The series 6.16 is called a Hecke L-series and $\tilde{\chi}_n$ is called a Hecke character. This shows the similarity between $L(E_n, s)$ and

$L(\chi, s)$ in 6.4.1. We can formally expand 6.14 into the series

$$L(E_n, s) = \sum_{m \geq 1} b_{m,n} m^{-s} \tag{6.17}$$

Comparing the two expansions of $L(E_n, s)$ given above, we find

$$\begin{aligned} b_{m,n} &= \sum_{I \text{ with } \mathbb{N}I = m} \tilde{\chi}_n(I) && (6.18)\\ &= \left(\frac{n}{m}\right) \sum_{I \text{ with } \mathbb{N}I = m} \tilde{\chi}_1(I) && (6.19)\\ &= \left(\frac{n}{m}\right) b_{m,1} && (6.20) \end{aligned}$$

Every nonzero ideal $I \in \mathbb{Z}[i]$ is principal. We can thus write the above sum as

$$b_{m,n} = \frac{1}{4} \sum_{a+bi : a^2+b^2 = m} \tilde{\chi}_n(a+bi)$$

Where the factor of $1/4$ appears because of recounting. We can therefore write

$$L(E_n, s) = \frac{1}{4} \sum_{x \in \mathbb{Z}_{[i]}} \tilde{\chi}_n(x) (\mathbb{N}x)^{-s}$$

Equations 6.17 and 6.20 give us a way to explicitly calculate $L(E_n, s)$. Here $\mathcal{R}s > 3/2$. First, to calculate $b_{m,1}$, we need to consider the elliptic curve $E_1 : y^2 = x^3 - x$. If $p \equiv 3 \mod 4$, then $a_p = 0$. If $p \equiv 1 \mod 4$, then we can calculate a_p in two ways:

1. $a = a_p$ is the unique a that satisfies $a^2 + b^2 = p$ for which $a + bi \equiv 1 \mod (2+2i)$, or

2. Count the number N_p of $\mathbb{F}_p$ points on E_1 and find $a_p = p + 1 - N_p$.

This gives us coefficients in the product formula and we can write $L(E_1, s)$

$$\begin{aligned} L(E_1, s) &= \frac{1}{1 + 3.9^{-s}} \cdot \frac{1}{1 + 2.5^{-s} + 5.25^{-s}} \cdot \frac{1}{1 + 7.49^{-s}} \cdot \frac{1}{1 + 11.121^{-s}} \ldots && (6.21)\\ &= 1 - 2.5^{-s} - 3.9^{-s} + 6.13^{-s} + 2.17^{-s} + \ldots && (6.22) \end{aligned}$$

Thus we get the first few $b_{m,1}$. Using the expression 6.20, we can expand $L(E_n, s)$ as

$$L(E_n, s) = 1 - 2\left(\frac{n}{5}\right)5^{-s} - 3\left(\frac{n}{9}\right)9^{-s} + 6\left(\frac{n}{13}\right)13^{-s} + 2\left(\frac{n}{17}\right)17^{-s} + ... \qquad (6.23)$$

We have thus found explicit expression for the series $L(E_n, s)$. One should note that it makes sense only for $\mathcal{R}s > 3/2$. However, $L(E_n, s)$ can be extended analytically to the whole complex plane. We state without proof a proposition that is used in proving this fact.

Proposition 6.4.8. *χ'_n is a primitive multiplicative character of $\mathbb{Z}[i]/((2+2i)n)$ for odd n and of $\mathbb{Z}[i]/(2n)$ for even n.*

We end this chapter by stating (without proof) that $L(E_n, s)$ can be extended analytically.

Theorem 6.4.9. *$L(E_n, s)$ as defined by 6.14 extends analytically to an entire function on whole $\mathbb{C}$-plane. Let*

$$N = \begin{cases} 32n^2, & n \text{ odd} \\ 16n^2, & n \text{ even} \end{cases}$$

and

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(E_n, s)$$

Then $L(E_n, s)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2 - s)$$

where the sign is called the root number. It equals $+1$ if $n \equiv 1, 2, 3 \mod 8$ and -1 if $n \equiv 5, 6, 7 \mod 8$. N is called the conductor of E_n.

Chapter 7

BSD conjecture

The sources of this chapter are primarily [R V91] and [Kob84].

Birch and Swinnerton-Dyer conjectured that

Conjecture 1 (BSD conjecture)**.** *Let $E_{\mathbb{Q}}$ be an elliptic curve with rank r. Then there is a positive constant C_E depending only on E such that*

$$f(X) = \prod_{p \leq X} \frac{N_p}{p} \sim C_E (\log X)^r$$

This conjecture can be reformulated as

Conjecture 2. *Order of vanishing of $L(E, s)$ at $s = 1$ equals the rank of E.*

One must observe that $L(E, s)$ was shown to converge for $\mathcal{R}s > 3/2$. For $E = E_n$, we asserted that $L(E, s)$ can be extended analytically to the entire complex plane. A theorem of Coates and Wiles proves that for any elliptic curve E, $L(E, s)$ can be extended analytically beyond $s = 3/2$.

We give the motivation for the conjecture by some heuristic arguments. We write the partial product for the L-series and find its value at $s = 1$.

$$L_X(E, 1) = \prod_{p \leq X} \frac{1}{1 - 2a_p p^{-s} + p^{1-2s}}|_{s=1} = \prod_{p \leq X} \frac{p}{p + 1 - 2a_p} = \prod_{p \leq X} \frac{p}{N_p}$$

where N_p is the number of points on E modulo p. Riemann hypothesis (theorem) for elliptic curves states that $|N_p - p - 1| \leq 2\sqrt{p}$. So roughly $N_p = p \pm 2\sqrt{p}$. If there are infinitely many points on $E_{\mathbb{Q}}$, one could expect N_p to take values significantly greater

than p for all large primes p. Thus $N_p \sim p + f(p)$ where $f(p) > 0$. We would thus obtain

$$L_X(E,1) \sim \prod_{p \leq X} \frac{p}{p+f(p)} \sim \prod_{p \leq X} \frac{1}{1+f(p)/p} \sim 0$$

Thus, if E has positive rank, the L-function vanishes at $s = 0$.

As an aside of this conjecture, we state the following proposition.

Proposition 7.0.10. *If $n \equiv 5, 6, 7 \mod 8$ and the BSD conjecture holds for E_n, then n is a congruent number.*

Proof: The functional equation in Theorem 6.4.9 states that $\Lambda(s) = -\Lambda(2-s)$. Substituting $s = 1$, we get $\Lambda(1) = -\Lambda(1)$. Thus $\Lambda(1) = 0$. So if BSD conjecture holds for E_n, n is a congruent number.

Bibliography

[Ahl79] Lars V. Ahlfors, *An introduction to the theory of analytic functions of one complex variable*, McGraw-Hill Inc., 1979.

[Kob84] Neil Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1984.

[Mil06] J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006.

[PP74] David E. Penney and Carl Pomerance, *A search for curves with large ranks*, Mathematics of Computation **28** (1974), no. 127, 851–853.

[PP75] ———, *Three elliptic curves with rank at least seven*, Mathematics of Computation **29** (1975), no. 131, 965–967.

[R V91] R V Gurjar, Kirti Joshi, N. Mohan Kumar, Kapil H. Paranjape, A. Ramanathan, T. N. Shorey, R. R. Simha, V. Srinivas, *Elliptic curves*, National Board for Higher Mathematics, Bombay, 1991.

[Sil86] Joseph H Silverman, *Arithmetic of elliptic curves*, second ed., Springer, 1986.

[ST92] Joseph H Silverman and John Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, 1992.