Master's Thesis

Ranks of Elliptic Curves

Jae Hun Park

Department of Mathematical Sciences

Graduate School of UNIST

2019

Ranks of Elliptic Curves

Jae Hun Park

Department of Mathematical Sciences

Graduate School of UNIST

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Ranks of Elliptic Curves

A dissertation
submitted to the Graduate School of UNIST
in partial fulfillment of the
requirements for the degree of
Master of Science

Jae-Hun Park

06/10/2019

Approved by

조재현인

____

Advisor
Peter Jae-Hyun Cho

ULSAN NATIONAL INSTITUTE OF
SCIENCE AND TECHNOLOGY

Ranks of Elliptic Curves

Jae-Hun Park

This certifies that the dissertation of Jae-Hun Park is approved.

06/10/2019

signature

____

Advisor: Peter Jae-Hyun Cho

signature

____

Hae-Sang Sun : Thesis Committee Member #1

signature

____

Chol Park : Thesis Committee Member #2

Abstract

This thesis is a thorough review of the Ph.D thesis titled "The Zeros of Elliptic Curve L-functions" [Spi15] by Simon Spicer. His thesis is devoted to compute the ranks of elliptic curves. Firstly, we provide basic knowledge and facts about elliptic curves and in Section 8, we explain his algorithm. The below is his algorithm to compute the rank of elliptic curves.

Let E be an elliptic curve with the global minimal Weierstrass equation $E : y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$ with the conductor N_E.

The algorithm goes like :

1. Compute the real period Ω_E of E.

2. Set $k = \lceil 26 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 0.25 \log N_E)) - \log_2 \Omega_E \rceil$.

3. Evaluate $L_E(1)$ to k bits precision.

4. If k-bit binary digits are not zero, then the rank is 0.

5. Otherwise, $L_E(1) \equiv 0$ and now evaluate $L'_E(1)$. That is, $m \mapsto m + 1$.

6. This procedure stops if $L_E^{(m)}(1)$ is not zero to k bits precision, and then output the analytic rank of elliptic curve $r_E = m$.

For elliptic curves with large conductors, we give an upper bound and a lower bound on the rank.

$$\frac{1}{2} \log N_E - 4.426 - \beta_E < r_E < 0.5 + 0.32 \log N_E.$$

In the last section, we collected a list of minor mistakes and typos in his thesis.

Contents

List of Figures

I Introduction

1.1 Basic Definitions and Backgrounds

An elliptic curve is a smooth curve of genus one and represented by the Weierstrass equation. Explicitly,

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

And the reduced curve $\tilde{E}/\mathbb{F}_p$ modulo p is given by

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$$

where $\tilde{a_i}$ is a_i modulo prime p.

The discriminant of an elliptic curve, D_E, is defined by some values associated to E, can be computed by coefficients of the curve.

$$b_2 = {a_1}^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

$$D_E := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

A prime p is called a good prime if a curve $\tilde{E}/\mathbb{F}_p$ is non-singular. In the case, E is said to have good reduction at p. If $\tilde{E}/\mathbb{F}_p$ is singular, then E is said to have a bad reduction at p.

Example I.1. $E : y^2 = x^3 + 35x + 5$ have good reduction at $p = 7$ since $y^2 = x^3 + 5$ is non-singular, and E has bad reduction at $p = 5$ since $y^2 = x^3$ is singular. In this case, E has additive reduction at 5 since the tangent space at the singular point of $y^2 = x^3$, is one dimensional. In other words, the singular point of E $(0, 0)$ is a cusp.

Example I.2. $E : y^2 = x^3 - x^2 + 35$ have bad reduction at $p = 5$ and 7, but they are slightly not the same type of bad reduction. At first, both primes are multiplicative bad reduction since the tangent space of the singular points is two dimensional(called a node).

However, when $p = 5$, the tangent space of E at the singular point is defined over $\mathbb{F}_p$. Because $y^2 + x^2 - x^3 = (y + 2x)(y - 2x) - x^3 = 0$ is the Taylor expansion at $(0, 0)$. When $p = 7$, the tangent space at $(0, 0)$ is defined over a quadratic extension of $\mathbb{F}_p$. Precisely, $y^2 + x^2 - x^3 = (y + \sqrt{i}x)(y - \sqrt{i}x) - x^3 = 0$. The former is called split multiplicative reduction, and the latter is called non-split one.

The conductor of an elliptic curve N_E, is defined by

$$N_E = \prod_{primes} p^{f_p(E)},\ f_p(E) = \begin{cases} 0 & \text{if } E \text{ has a good reduction at } p \\ 1 & \text{if } E \text{ has a multiplicative reduction at } p \\ 2 & \text{if } E \text{ has an additive reduction at } p \end{cases}$$

L-function attached to E is represented by the following Euler product.

$$L(E,s) = \prod_{bad \ primes} \frac{1}{1-a_p p^{-s}} \times \prod_{good \ primes} \frac{1}{1-a_p p^{-s} + p^{1-2s}}$$

where a_p is $1, -1$ and 0 if E has a split, non-split, and an additive bad reduction at p respectively.

The completed L-function is made by L-function

$$\Lambda_E(s) = (N_E)^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$$

For elliptic curve L-functions, the point $s = 1$ is called the critical point, and the line $\Re(s) = 1$ is called the critical line.

The analytic rank of E, denoted by $r_{an}(E)$, is defined by the first non-zero coefficient of the Taylor series of $L(E,s)$ at $s = 1$. That is, if $L(E, 1+s) = a_0 + a_1 s + a_2 s^2 + \cdots$, then the first non-zero a_n(vanishing order of the series) is said to be the analytic rank of E.

By the Mordell-Weil theorem, the group of rational points on E is $E(\mathbb{Q}) \cong E_{tor}(\mathbb{Q}) \times \mathbb{Z}^r$ and the algebraic rank of an elliptic curve is $r_{al}(E) = r$, which is the exponent of non-torsion part. $r_{al}(E)$ is finite since E($\mathbb{Q}$) is finitely generated as above.

II The Conjectures

Conjecture II.1 (Birch, Swinnerton-Dyer, BSD). *According to the BSD conjecture, the analytic rank and the algebraic rank are exactly same. Moreover, the value of the first non-zero coefficient of the L-series at the central point is computed by*

$$C_E = \frac{\Omega_E \times Reg_E \times \#Sha(E) \times \prod_p c_p}{(\#E_{tor}(\mathbb{Q}))^2}$$

where Ω_E is the real period of E, Reg_E is the regulator of E, $\#Sha(E)$ is the order of the Shafarevich-Tate group to $E/\mathbb{Q}$, $\prod_p c_p$ is the product of the Tamagawa numbers of E, and $\#E_{tor}(\mathbb{Q})$ is the number of torsion points on E.

Conjecture II.2 (Generalized Riemann Hypothesis, GRH). *Let $L(E, s)$ be the L-series of the elliptic curve $E/\mathbb{Q}$, then its non-trivial zero always lie on the critical line $Re(s) = 1$.*

Conjecture II.3 (Masser-Oesterlé conjecture ver.1, ABC). *Let a, b, c be the relatively prime satisfying $a + b = c$. And the radical of abc is defined by $rad(abc) = \prod_{p|abc} p$. Then for any $\epsilon > 0$, there exist a constant K_ϵ such that $c < K_\epsilon \cdot rad(abc)^{1+\epsilon}$.*

Note that the radical is square-free integer. Equivalently,

Conjecture II.4 (Masser-Oesterlé conjecture ver.2, ABC). *There are only finitely many triples (a, b, c) satisfying the same condition above, such that $c > rad(abc)^{1+\epsilon}$*

III The Gamma Function

3.1 The Gamma function

The Gamma function is well-known function as a continuous extension of the factorial function on natural numbers. As an extension, if n is a positive integer, it needs to be the factorial function. More various information can be seen at [Vio16].

Definition III.1 (Gamma function)**.** *For $s \in \mathbb{C}$, $\Re(s) > 0$,*

$$\Gamma(s) := \int_0^\infty e^{-t} t^{s-1} dt$$

Note that $\Gamma(s+1) = s\Gamma(s)$ by integration by parts. But one can wonder that indeed the extension is unique. We have the answer, under some conditions.

Theorem III.2 (Bohr-Mollerup)**.** *Let $\Gamma(x)$ be the Gamma function. This is the only function on $x > 0$ satisfying*

1. $\Gamma(1) = 1$.
2. $\Gamma(x+1) = x\Gamma(x)$ *for* $x > 0$.
3. $\log \Gamma(x)$ *is convex.*

Lemma III.3. $0 < e^{-t} - (1 - t/N)^N < t^2 e^{-t}/N$ *for* $0 < t < N$.

Proof.

$$1 + \frac{t}{N} < 1 + \frac{t}{N} + \frac{t^2}{2!N^2} + \cdots < 1 + \frac{t}{N} + \frac{t^2}{N^2} + \cdots \text{ gives } 1 + \frac{t}{N} < e^{\frac{t}{N}} < \left(1 - \frac{t}{N}\right)^{-1}$$

It means that $(1 + t/N) < e^t$ and $(1 - t/N) < e^{-t}$. And

$$0 < e^{-t} - \left(1 - \frac{t}{N}\right)^N = e^{-t}\left(1 - e^t\left(1 - \frac{t}{N}\right)^N\right) < e^{-t}\left(1 - \left(1 - \frac{t^2}{N^2}\right)^N\right)$$

Note that $1 - Nx < (1-x)^N$ for $0 < x \leq 1/N$, it gives $1 - t^2/N < (1 - t^2/N^2)^N$ □

And through the next theorem, we can obtain the limit form of the Gamma function so that simple poles of the Gamma function lies on the non-positive integers.

Theorem III.4 (Euler)**.** *For any* $s \in \mathbb{C} \setminus \{0, -1, \cdots\}$,

$$\Gamma(s) = \lim_{n\to\infty} \frac{n^s n!}{s(s+1)\cdots(s+n)}$$

Proof. For $\Re(s) > 0$, $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$. And note that

$$\lim_{n\to\infty} \int_0^n \left(1 - \frac{t}{n}\right)^n t^{s-1}dt = \Gamma(s) - \lim_{n\to\infty} \int_0^n \left(e^t - \left(1 - \frac{t}{n}\right)^n\right) t^{s-1}dt$$

Using the Lemma III.3, as $n \to \infty$,

$$\left|\int_0^n \left(e^{-t} - \left(1 - \frac{t}{n}\right)^n\right) t^{s-1}dt\right| \leq \int_0^n \frac{t^2}{n} e^{-t}t^{\Re(s)-1}dt \leq \frac{1}{n}\int_0^\infty e^{-t}t^{\Re(s)+1}dt \to 0.$$

So $\lim_{n\to\infty} \int_0^n \left(1 - \frac{t}{n}\right)^n t^{s-1}dt = \Gamma(s)$.

Now through the change of variable, let $\frac{t}{n} = \tau$ and repeating integration by parts, we can get

$$\int_0^n \left(1 - \frac{t}{n}\right)^n t^{s-1}dt = n^s \int_0^1 (1-\tau)^n \tau^{s-1}d\tau = \frac{n^s n!}{s(s+1)\cdots(s+n)}$$

If $\Re(s) \leq 0$, for $k \in \mathbb{N}$ such that $-(k+1) < \Re(s) \leq -k, s \neq k$, the remaining thing is

$$\begin{aligned}\Gamma(s) &= \frac{1}{s\cdots(s+k)}\Gamma(s+k+1) = \frac{1}{s\cdots(s+k)} \lim_{n\to\infty} \frac{n^{s+k+1}n!}{(s+k+1)\cdots(s+k+1+n)} \\ &= \lim_{n\to\infty} \frac{n^s n!}{(s+1)(s+2)\cdots(s+n)} \cdot \frac{n^{k+1}}{(s+n+1)\cdots(s+n+k+1)}\end{aligned}$$

and the second factor will be 1 by the limit. □

Through this theorem, one can prove the Bohr-Mollerup theorem also. The first and the second condition will be directly obtained by the resulting formula, and the third condition - convexity of $\log(\Gamma(s))$ can be obtained by the definition of convexity and some calculations.

Using the theorem III.4, we can make the recursive relation of the Gamma function wider to the whole real line. The simple poles of the Gamma function also can be found by the recursive relation. For example, $\Gamma(s+1) = s\Gamma(s)$ implies that 0 is a simple pole of $\Gamma(s)$.

Note that, for a complex function $f(s)$, at a simple pole c, the residue of f is given by $\text{Res}(f, c) = \lim_{s\to c}(s-c)f(s)$. If $s = -n$,

$$\text{Res}(\Gamma, -n) = \lim_{s\to -n}(s-(-n))\Gamma(s) = \lim_{s\to -n}\frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n-1)} = \frac{(-1)^n}{n!}$$

3.2 A relation to the Riemann zeta function

For $\Re(s) > 1$, the Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

By the change of variable, $n \mapsto nt$ for $\Gamma(s)$,

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt \Rightarrow \Gamma(s) = \int_0^\infty n^s e^{-nt}t^{s-1}dt$$

Then

$$\sum_{n=1}^{N}\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty \sum_{n=1}^{N} e^{-nt}t^{s-1}dt = \frac{1}{\Gamma(s)}\left\{\int_0^\infty \frac{e^{-t}t^{s-1}}{1-e^{-t}} - \int_0^\infty \frac{e^{-t}e^{-Nt}}{1-e^{-t}}t^{s-1}dt\right\}$$

Now let N go to ∞,

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty \frac{t^{s-1}}{e^t-1}dt$$

In case of the incomplete Gamma function,

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \frac{1}{\Gamma(s,x)}\int_x^\infty \frac{t^{s-1}}{e^t-1}dt$$

And there is another famous functional relation between the zeta function and the Gamma function.

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\sin(\frac{\pi s}{2})\zeta(1-s)$$

To obtain this relation, note that the zeta function is analytic for $s \neq 1$ and $\Gamma(1-s)$ has simple poles at positive integers. Then the last two factors of the right hand side should have simple zeros at $s = 2, 3, 4, \cdots$. Since the sine factor has zeros when s is even, the zeta factor obviously has zeros when s is odd. That means the zeta function have zeros for a negative even numbers. These zeros are called the trivial zeros.

3.3 The Digamma function

In chapter to come about nontrivial zeros and their summations, the logarithmic derivative of some functions have an important role to play with summation of nontrivial zeros. And the Digamma function is one of them, as the logarithmic derivative of the Gamma function.

Definition III.5 (Digamma function)**.** *The Digamma function $\psi(s)$ is the logarithmic derivative of the Gamma function.*

$$\psi(s) := \frac{d}{ds}\log\Gamma(s) = \frac{\Gamma'(s)}{\Gamma(s)}$$

Obviously many properties of the Digamma function inherits the properties of the Gamma function. For example, $\Gamma(s+1) = s\Gamma(s)$ and $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$ give the followings.

$$\psi(s+1) = \psi(s) + \frac{1}{s},\ \psi(1-s) = \psi(s) + \pi\cot(\pi s)$$

And using the Weierstrass factorization of the Gamma function, we can obtain the series form of the Digamma function. More precisely, take the logarithmic derivative to the Gamma function

$$\Gamma(s) = s^{-1}\cdot e^{-\gamma s}\cdot\prod_{n=1}^{\infty}\left(1+\frac{s}{n}\right)^{-1}\cdot e^{s/n}$$

then

$$\psi(s) = -\gamma - \frac{1}{s} + \sum_{n=1}^{\infty}\left(\frac{1}{n} - \frac{1}{n+s}\right)$$

Since $\psi(s+1) = \psi(s) + 1/s$, more brief form is shown.

$$\psi(s+1) = -\gamma + \sum_{n=1}^{\infty}\frac{s}{n(n+s)}$$

This series converges absolutely for any $s \in \mathbb{C}$ except for the negative integer. If x is an integer, by using the fact that

$$\psi(1+x) = -\gamma + \sum_{n=1}^{\infty}\left(\frac{1}{n} - \frac{1}{n+x}\right) = -\gamma + \sum_{n=1}^{x}\frac{1}{n} = -\gamma + H_x$$

where H_x is the harmonic series. Note that $H_x - \gamma < \log x$, then we obtain a bound for the Digamma function on the non-negative real line.

$$\psi(1+x) < \log(1+x)$$

IV L-function attached to an Elliptic curves

4.1 L-function

Let's recall the Euler product of $L_E(s)$.

$$L_E(s) = \prod_{bad\ primes} \frac{1}{1 - a_p p^{-s}} \times \prod_{good\ primes} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

The coefficient a_p is $1, -1$ and 0 if E has split, non-split, and additive bad reduction at p respectively. For good primes, we have the bound for a_p obtained by Hasse.

Theorem IV.1 (Hasse)**.** *For all elliptic curves over $\mathbb{Q}$ and for all p,*

$$|a_p| \leq 2\sqrt{p}$$

If we normalize a_p, that is, observe the distribution of $a_p/2\sqrt{p}$, it is the semicircular distribution.

Theorem IV.2 (Taylor)**.** *For $E/\mathbb{Q}$, the distribution of $a_p/2\sqrt{p}$ is semicircular.*

So by the Hasse's theorem, the Dirichlet series for $L_E(s)$ converge absolutely for $\Re(s) > 3/2$. By the Taylor's theorem, the Dirichlet series for $L_E(s)$ converge conditionally for $\Re(s) > 1/2$.

And for the completed L-function $\Lambda_E(s)$, it obeys the functional relation

$$\Lambda_E(s) = \omega_E \Lambda_E(2 - s)$$

where $\omega_E \in \{-1, 1\}$.

To get the coefficients of $\Lambda_E(s)$, we need the following formula

Theorem IV.3.

$$\Lambda_E(1) = \begin{cases} \frac{\sqrt{N_E}}{\pi} \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\frac{2\pi n}{\sqrt{N_E}}} & \textit{if } \omega_E = 1 \\ 0 & \textit{if } \omega_E = -1 \end{cases}$$

Proof. Before we start the proof, we need to define the auxiliary function $\lambda_E(s)$ by

$$\lambda_E(s) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \sum_{n=1}^{\infty} a_n n^{-s} \Gamma\left(s, \frac{2\pi n}{\sqrt{N_E}}\right) \tag{1}$$

where a_n is given by the Dirichlet series for $L_E(s)$. And from [Kna92], page 270, the formula $\Lambda_E(s) = \lambda_E(s) + \omega_E \lambda_E(2 - s)$. And the incomplete Gamma function is

$$\Gamma(s, x) = \int_x^{\infty} t^{s-1} e^{-t} dt$$

Since the sum in the equation (1) converges absolutely for any s, the summation in $\lambda_E(s)$ can be switched to any order. Then

$$\lambda_E(1 + s) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^{1+s} \int_{2\pi n/\sqrt{N_E}}^{\infty} t^s e^{-t} \sum_{n=1}^{\infty} a_n n^{-1-s} dt$$

Take $t \mapsto 2\pi nt$ and $dt \mapsto 2\pi ndt$,

$$\lambda_E(1+s) = {N_E}^{(1+s)/2} \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt$$

Note that $\Lambda_E(1+s) = \lambda_E(1+s) + \omega_E \lambda_E(1-s)$, if $\omega_E = 1$,

$$\begin{aligned}\Lambda_E(1+s) &= \left({N_E}^{(1+s)/2} + \omega_E {N_E}^{(1-s)/2}\right) \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt \\ &= \left({N_E}^{(1+s)/2} + {N_E}^{(1-s)/2}\right) \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt\end{aligned}$$

And if $\omega_E = -1$,

$$\Lambda_E(1+s) = \left({N_E}^{(1+s)/2} - {N_E}^{(1-s)/2}\right) \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt$$

Substituting $s = 0$, we obtain the desired result. □

Theorem IV.4. *If m has the same parity as E,*

$$\Lambda_E^{(m)}(1) = 2 \sum_{n=1}^{\infty} a_n \int_1^{\infty} e^{-\frac{2\pi n}{\sqrt{N_E}} t} (\log t)^m dt$$

Otherwise, $\Lambda_E^{(m)}(1) = 0$.

Proof. Also get started with

$$\lambda_E(1+s) = {N_E}^{(1+s)/2} \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt$$

The derivative of $\lambda_E(1+s)$ is

$$\lambda'_E(1+s) = \left({N_E}^{(1+s)/2}\right)' \int_{1/\sqrt{N_E}}^{\infty} t^s e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt + {N_E}^{(1+s)/2} \int_{1/\sqrt{N_E}}^{\infty} (t^s)' e^{-2\pi nt} \sum_{n=1}^{\infty} a_n dt$$

Use the binomial expansion for derivatives, we can generalize

$$\lambda_E^{(m)}(1+s) = \sum_{n=1}^{\infty} a_n \int_{1/\sqrt{N_E}}^{\infty} e^{-2\pi nt} \left(\sum_{i=0}^{m} \binom{m}{i} f^{(m-i)}(s) g^{(i)}(s) \right) dt$$

where $f(s) = {N_E}^{(1+s)/2}$, $g(s) = t^s$. And note that

$$f^{(m-i)}(s) = \left(\frac{1}{2}\right)^{m-i} {N_E}^{(1+s)/2} (\log N_E)^{m-i}, \; g^{(i)}(s) = t^s (\log t)^i$$

Now consider $\Lambda'_E(1+s) = \lambda'_E(1+s) + \omega_E \lambda'_E(1-s)(-1)^m$, if ω_E and m have the same parity, $\omega_E(-1)^m = 1$. And if they have the opposite parity, then $\omega_E(-1)^m = -1$. So for the same parity,

$$\begin{aligned}\Lambda_E^{(m)}(1) = \lambda_E^{(m)}(1) + \lambda_E^{(m)}(1) &= \sum_{n=1}^{\infty} a_n \int_{1/\sqrt{N_E}}^{\infty} e^{-2\pi nt} \left(\sum_{i=0}^{m} \binom{m}{i} f^{(m-i)}(0) g^{(i)}(0) \right) dt \\ &= \sum_{n=1}^{\infty} a_n \int_{1/\sqrt{N_E}}^{\infty} e^{-2\pi nt} \sqrt{N_E} \left(\sum_{i=0}^{m} \binom{m}{i} (\log \sqrt{N_E})^{m-i} (\log t)^i \right) dt\end{aligned}$$

The inner binomial summation is nothing but $(\log \sqrt{N_E} + \log t)^m$. For the final trimming, take $t \mapsto t/\sqrt{N_E}$ and $dt \mapsto dt/\sqrt{N_E}$

$$\Lambda_E^{(m)}(1) = 2\sum_{n=1}^{\infty} a_n \int_1^{\infty} e^{\frac{-2\pi n}{\sqrt{N_E}}t} (\log t)^m dt$$

And for the opposite parity,

$$\Lambda_E^{(m)}(1) = \lambda_E^{(m)}(1) - \lambda_E^{(m)}(1) = 0$$

Proof is done. □

Like the Digamma function, the logarithmic derivative of the completed L-function will be useful later.

Theorem IV.5. *The logarithmic derivative of the L-function is given by*

$$\frac{\Lambda_E'}{\Lambda_E}(s) = \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \psi(s) + \frac{L_E'}{L_E}(s)$$

where $\psi(s)$ is the Digamma function.

Proof. It is directly deduced from the definition of the completed L-function. □

If we are not on the critical strip, we can roughly estimate the L-series and its logarithmic derivative.

Theorem IV.6. *For any $s \in \mathbb{C}$ with $\Re(s) := \sigma > 3/2$, we have*

1.

$$\frac{\zeta(2\sigma-1)^2}{\zeta(\sigma-1/2)^2} < |L_E(s)| < \zeta\left(\sigma - \frac{1}{2}\right)^2$$

2.

$$2\frac{\zeta'}{\zeta}\left(\sigma - \frac{1}{2}\right) < \left|\frac{L_E'}{L_E}(s)\right| < -2\frac{\zeta'}{\zeta}\left(\sigma - \frac{1}{2}\right)$$

where $\zeta(s)$ is the Riemann zeta function.

V The Real Period Ω_E of an Elliptic curve E

5.1 Elliptic curve and Torus

An elliptic curve over the complex numbers $\mathbb{C}$, is actually isomorphic to some lattice quotient of a complex number group. And the real period of an elliptic curve shows us how those shapes that torus(that is, $\mathbb{C}/\Lambda$). More precisely, the non-singular elliptic curve over the real numbers have two topologically distinct shapes. One is connected, and the other is separated. The real period is an index to determine these two distinct shapes of curve on the real plane.

Definition V.1. *For ω_1, $\omega_2 \in \mathbb{C}$ such that linearly independent over $\mathbb{R}$, i.e., $r_1\omega_1 + r_2\omega_2 = 0$ only when $r_1 = r_2 = 0$,*

1. *Lattice : $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n\omega_1 + m\omega_2 | n, m \in \mathbb{Z}\}$*

2. *Fundamental parallelogram : $F = \{a\omega_1 + b\omega_2 | 0 \leq a, b < 1\}$*

3. *Doubly periodic function : Meromorphic function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ s.t. $f(s+\omega) = f(s)$ for all $s \in \mathbb{C}$, $\omega \in L$. That ω's are called a period.*

4. *Note that since f is meromorphic, $f(s) = a_r(s-\omega)^r + a_{r+1}(s-\omega)^{r+1} + \cdots$ with all $a_r \neq 0$.*

5. *The order of f at ω : $r = ord_\omega f \in \mathbb{Z}$*

6. *The divisor of f : div(f) $= \sum_{\omega \in F}(ord_\omega f)[\omega]$*

Note that, if meromorphic f is bounded, then it is a constant.

5.2 Weierstrass $\wp$ - function

Lemma V.2. *If $k > 2$, then $\sum_{\omega \in L, \omega \neq 0} \frac{1}{|\omega|^k}$ converges.*

Theorem V.3. *Given a lattice L, define the Weierstrass $\wp$-function*

$$\wp(s) = \wp(s; L) = \frac{1}{s^2} + \sum_{\omega \in F,\ \omega \neq 0} \left(\frac{1}{(s-\omega)^2} - \frac{1}{\omega^2} \right)$$

Then

1. *The summation part converges absolutely and uniformly on compact sets not intersecting L*

2. *$\wp(s)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $\omega \in L$.*

3. *$\wp(-s) = \wp(s)$ for all $s \in \mathbb{C}$*

4. *$\wp(s+\omega) = \wp(s)$ for all $\omega \in L$*

5. *{ doubly periodic function for L } $= \mathbb{C}(\wp, \wp')$*

Proof. Having V.2, then the remaining thing is to prove that the summation part is dominated by the cubic reciprocal terms. Note that

$$\left|\frac{1}{(s-\omega)^2}-\frac{1}{\omega^2}\right| = \left|\frac{s(2\omega-s)}{(s-\omega)^2\omega^2}\right| \leq \frac{|s|(2|\omega|+|s|)}{|\omega|^2(|\omega|-|s|)^2}.$$

For a compact set containing s, if $|\omega| \geq 2|s|$ for all s, we have

$$|s-\omega| \geq \frac{|\omega|}{2}, |2\omega - s| \leq \frac{5|\omega|}{2}$$

It's easy to check by drawing some area on $\mathbb{C}$. So we have

$$\left|\frac{1}{(s-\omega)^2}-\frac{1}{\omega^2}\right| \leq \frac{|s|(2|\omega|+|s|)}{|\omega|^2(|\omega|-|s|)^2} \leq \frac{|s||\omega|(5/2)}{|\omega|^2(|\omega|^2/4)} = \frac{10|s|}{|\omega|^3}$$

So the summation part is dominated by converging term.

The remaining proofs can be seen at [Was03].

□

Theorem V.4 (Doubly periodic)**.** *Let f be a doubly periodic function for L and F be a fundamental parallelogram for L. Then,*

1. *If f has no poles, then f is a constant.*
2. *If f is not identically equal to 0, then $deg(div(f)) = \sum_{\omega\in F} ord_\omega f = 0$.*
3. *If f is not identically equal to 0, then $\sum_{\omega\in F} \omega \cdot ord_\omega f \in L$.*
4. *If f is not constant, then $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is surjective.*
5. *If n = the sum of the orders of the poles of f in F and $s_0 \in \mathbb{C}$, then $f(s) = s_0$ has n solutions.*

Definition For $k \geq 3$, the Eisenstein series is given by

$$G_k(L) = \sum_{\omega\in L, \omega\neq 0} \omega^{-k}$$

Note that this sum converges(lemma V.2) and $G_{2k+1} = 0$. And under the condition $|s/\omega| < 1$, some manipulation gives

$$\frac{1}{(s-\omega)^2}-\frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-(s/\omega))^2}-1\right) = \frac{1}{\omega^2}\cdot\frac{s/\omega}{(1-s/\omega)^2} = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{s}{\omega}\right)^n$$

So the Weierstrass $\wp$-function can be expressed by the Eisenstein series.

$$\wp(s) = \frac{1}{s^2} + \sum_{\omega\neq 0}\sum_{n=1}^{\infty}(n+1)\frac{s^n}{\omega^{n+2}} = \frac{1}{s^2} + \sum_{k=1}^{\infty}(2k+1)\frac{s^{2k}}{\omega^{2k+2}} = \frac{1}{s^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(L)s^{2k}$$

Using this, we can compute

$$\wp(s) = \frac{1}{s^2} + 3G_4s^2 + 5G_6s^4 + \cdots, \wp'(s) = \frac{-2}{s^3} + 6G_4s + 20G_6s^3 + \cdots$$

So $\wp'(s)$ has a triple pole at 0, and through further computation, we can delete all reciprocal terms as followings

$$f(s) = \wp'(s)^2 - 4\wp(s)^3 + 60G_4\wp(s) + 140G_6 = c_1 s + c_2 s^2 + \cdots \in \mathbb{C}(\wp, \wp')$$

Now f is doubly periodic and has no constant term, no negative powers. So f has no poles, then f is constant with $f(0) = 0$.

Then the equality is now familiar relation.

$$\wp'(s)^2 = 4\wp(s)^3 - 60G_4\wp(s) - 140G_6$$

And fortunately, the curve is non-singular. i.e., The discriminant of that cubic polynomial is nonzero.

Theorem V.5. *Let $60G_4 = g_2$ and $140G_6 = g_3$. Then $\Delta = g_2^3 - 27g_3^2 \neq 0$.*

Now we can obtain the isomorphism between $\mathbb{C}/L$ and $E(\mathbb{C})$.

Theorem V.6. *Let L be a lattice and E be an elliptic curve $y^2 = 4x^3 - g_2 x - g_3$. Then the map $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ defined by $\Phi(s) = (\wp(s), \wp'(s)), \Phi(0) = \{\infty\}$ is an isomorphism of groups.*

Proof. First, we want to show that for a point of an elliptic curve $\Phi(s_i) = P_i = (x_i, y_i)$, the given Φ is a group homomorphism. I'll give some part of a proof. The remaining things can be found at [Was03].

Assume that P_1, P_2 are finite points and $\overline{P_1P_2}$ intersects E in a finite point. The other cases are easy to check. Now namely $s_1, s_2, s_3 \in \mathbb{C}$ and $\Phi(s_i) = P_i = (x_i, y_i)$ such that $\overline{P_1P_2} \cap E = P_3$.

For an elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$, the group law formula gives

$$x_3 = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1 = \frac{1}{4}\left(\frac{\wp'(s_2) - \wp'(s_1)}{\wp(s_2) - \wp(s_1)}\right)^2 - \wp(s_2) - \wp(s_1)$$

So we can consider the intersecting line $\overline{P_1P_2} : y = ax + b$.

For $h(s) = \wp'(s) - a\wp(s) + b$, $h(s)$ has triple poles at 0. So $h(s) = 0$ at $\{s_1, s_2, s_3\} = \overline{P_1P_2} \cap E = P_3$

Therefore,

$$\operatorname{div}(h) = \sum_{\omega \in F} (\operatorname{ord}_\omega h)[\omega] = [s_1] + [s_2] + [s_3] - 3[0]$$

Since h is not identically 0, by theorem V.4 (3),

$$\sum_{\omega \in F} \omega \cdot \operatorname{ord}_\omega h = s_1 + s_2 + s_3 \in L$$

Then, $s_1 + s_2 \equiv -s_3 \pmod{L}$, so $\wp(s_1 + s_2) = \wp(-s_3) = \wp(s_3) = x_3$.

If $s_1 = s_2$, then use the duplication formula. □

In fact, two homothetic lattices have the same j-invariants. Homothety classes of lattices are in one-to-one correspondence with $\mathbb{C}$-isomorphism classes of elliptic curves.

$$\Big(\text{Lattice } \Lambda_1 \cong \Lambda_2\Big) \iff \Big(\text{Elliptic curves } \mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2\Big).$$

The lattice Λ have a basis (ω_1, ω_2) properly(that is, $\omega_1 \in \mathbb{R}$), and the real part of ω_2 is either 0 or $\omega_1/2$ corresponding to the case that the discriminant $D_E > 0$ or that of $D_E < 0$ respectively. A overall proof can be seen in Chapter 9 of [Was03].

5.3 The Real period

In this sense, we can define the real period of a rational elliptic curve.

Definition V.7 (The real period)**.** *The real period of E is given by*

$$\Omega_E = \begin{cases} 2\omega_1 & \textit{if } D_E > 0 \\ \omega_1 & \textit{if } D_E < 0 \end{cases}$$

Let define the Ramanujan Delta function $\Delta(s)$ on the upper half plane

$$\Delta(s) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \text{ where } q = e^{2\pi i s}$$

If we set $s = \frac{\omega_2}{\omega_1}$ with $\Im(s) > 0$, then we obtain a relation between the discriminant D_E and the lattice basis of $E/\mathbb{C}$ [Sil13].

$$D_E = \left(\frac{2\pi}{\omega_1}\right)^{12}\Delta(s) \tag{2}$$

Theorem V.8. *For $E/\mathbb{Q}$, $\Omega_E < 8.829\cdots|D_E|^{-\frac{1}{12}}$.*

Proof. Using (2) and $s = \frac{\omega_2}{\omega_1}$, we get

$$\omega_1 = 2\pi\left(\frac{1}{D_E}\Delta\left(\frac{\omega_2}{\omega_1}\right)\right)^{\frac{1}{12}} \tag{3}$$

Now we have that if $D_E > 0$ then $\Re(s) = 0$, and if $D_E < 0$ then $\Re(s) = 1/2$. That is, if $D_E > 0$ then $\omega_2/\omega_1 = it$, and if $D_E < 0$ then $\omega_2/\omega_1 = 1/2 + it$. Therefore,

$$\begin{aligned} D_E > 0 &\implies q = e^{2\pi i(it)} = e^{-2\pi i t} \in (0,1) \\ D_E < 0 &\implies q = e^{2\pi i(1/2+it)} = e^{\pi i}\cdot e^{-2\pi i t} \in (-1,0) \end{aligned}$$

Since $\Delta(s)$ is a holomorphic cusp form, as a function of q, $\Delta(q)$ is continuous on $(-1,1)$, and zero at $q = -1, 0$ and 1. So its maximum absolute value will be located on $(-1,0)$ or $(0,1)$. By [IJT14] [WY14], $\Delta(q)$ has only one critical point on each $(-1,0)$ and $(0,1)$, moreover the values are $q = 0.03728\cdots$ and $q = -0.43929\cdots$. Then, $\Delta(q)^{1/12}$ is $0.7026\cdots$ and $1.4052\cdots$ respectively. Since $\Omega_E \leq 2\omega_1$, by (3),

$$\Omega_E \leq 2\pi\cdot 1.4052\cdots|D_E|^{-1/12} = 8.829\cdots|D_E|^{-1/12}$$

□

And since the conductor divides the discriminant of an elliptic curve,

Corollary V.9. *For $E/\mathbb{Q}$, $\Omega_E < 8.829\cdots|N_E|^{-\frac{1}{12}}$.*

We'll use this theorem to make a bound for the Taylor coefficient, which is key object in the rank algorithm.

VI A Summation over Nontrivial zeros of zeta

Let's recall the Riemann hypothesis again.

Conjecture VI.1 (GRH)**.** *Let $L(E,s)$ be the L-series of the elliptic curve $E/\mathbb{Q}$, then the nontrivial zeros always lie on the critical line $\Re(s) = 1$.*

Now we can denote nontrivial zeros as $1 + it$ under GRH assumption. For a moment, let's think about the Riemann zeta function. We want to see how the nontrivial zeros are distributed along the line $\Re(s) = 1/2$. First, the number of nontrivial zeros with $t \in (0, T]$, $N(T)$ is given by

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi e} + O(\log T)$$

Second, the gaps between two consecutive nontrivial zeros along the line $\Re(s) = 1/2$ is bounded by

$$t_{n+1} - t_n \ll \frac{1}{\log\log\log t_n}$$

for nontrivial zeros $\rho_n = 1/2 + t_n$.

It might be helpful adding the zeros in specific way and analyzing its behavior for obtaining some information on the distribution of the zeros. Analogously, the twin prime conjecture is the idea of gaps, and the Erdös conjecture on arithmetic progressions is the idea of summations. Extremely simple cases are reciprocal sum of the natural numbers and the squares. The former diverges and the latter converges. It tells us that the square numbers are distributed more sparsely than the natural numbers. More deep discussion can be seen in several topics with Szemerédi's theorem.

The first way to add them is a simple reciprocal sum of nontrivial zeros $\rho = 1/2 + it$ along the line $\Re(s) = 1/2$ and $\Im(s) > 0$. Lower half plane is not our business since conjugate of zeros are also zeros of the zeta function.

Theorem VI.2. *Let ρ be nontrivial zeros of the Riemann zeta function.*

$$\sum_{\rho}\frac{1}{\rho} = -\log(2\sqrt{\pi}) + 1 + \frac{\gamma}{2}$$

where γ is the Euler constant.

Proof of this theorem can be found at [Edw74]. According to this result, intuitively, the imaginary parts of nontrivial zeros are distributed sparsely than natural numbers.

And under RH, some plain computation can show that

$$\sum_{\rho} \frac{1}{\rho} = \sum_{t=\Im(\rho)} \frac{4}{1+4t^2}$$

$$\sum_{\rho} \frac{1}{\rho^2} = -\sum_{t=\Im(\rho)} \frac{8(4t^2-1)}{(4t^2+1)^2}$$

$$\sum_{\rho} \frac{1}{\rho^3} = -\sum_{t=\Im(\rho)} \frac{16(12t^2-1)}{(4t^2+1)^3}$$

By theorem 5.2., the reciprocal sum of nontrivial zeros converges, so the summation of any power of the reciprocals will also converge. Naturally we extend this idea to nontrivial zeros of the L-series for an elliptic curve.

Under the same philosophy of the Hadamard product, we can obtain representation of the completed L-function as a product over its zeros, and the logarithmic derivative of the completed L-function as a sum over its zeros. Let the leading coefficient of Λ_E at the central point be C'_E.

$$\Lambda_E(1+s) = C'_E \cdot s^{r_E} \cdot \prod_{\rho>0} \left(1 + \frac{s^2}{\rho^2}\right) \tag{4}$$

the product term is made by the product of nontrivial zero terms, which have commonly conjugates of it. And obviously r_E is the analytic rank, which is the vanishing order of Λ_E at $s = 0$. And the logarithmic derivative of Λ_E is given by

$$\frac{\Lambda'_E}{\Lambda_E}(1+s) = \frac{r_E}{s} + 2\sum_{\rho>0} \frac{s}{s^2+\rho^2} = \sum_{\rho\neq 0} \frac{s}{s^2+\rho^2} \tag{5}$$

which can be directly computed from the above product form.

Using these forms, unconditional bound for the analytic rank is obtained.

Theorem VI.3. *Let r_E be the analytic rank of an elliptic curve E and N_E be its conductor. Then*

$$r_E < 1.6 + \frac{1}{2}\log N_E$$

this result does not depend on the GRH.

Proof. First, under the GRH, using the equation 5, we know that

$$r_E < r_E + 2\sum_{\rho>0} \frac{1}{1+\rho^2} = \frac{\Lambda'_E}{\Lambda_E}(2) \tag{6}$$

And we are with theorem IV.5,

$$\frac{\Lambda'_E}{\Lambda_E}(2) = \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \psi(2) + \frac{L'_E}{L_E}(2)$$

From the Harmonic series form of the Digamma function, $\psi(2) = 1 - \gamma$. And by the inequality (2) from the theorem IV.6, we have the case of $\sigma = 2$. So

$$\frac{L'_E}{L_E}(2) < -2\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)$$

Then the final trimming gives

$$r_E < \frac{\Lambda'_E}{\Lambda_E}(2) < \frac{1}{2}\log N_E - \log(2\pi) + 1 - \gamma - 2\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right)$$

so the remaining thing is just evaluating them. And note that the inequality 6 still hold if we are not under the GRH. □

And if we use the GRH with the sinc function, which is given by

$$sinc^2(x) = \left(\frac{\sin(\pi x)}{\pi x}\right)^2$$

then we can bound the analytic rank more tightly so that the following corollary is obtained. See the proof in [Spi15] page 67-71.

Corollary VI.4. *(GRH)*

$$r_E < 0.5 + 0.32\log N_E$$

Now let me introduce one important quantity called the bite of an elliptic curve. This definition is directly from [MS13].

Definition VI.5 (The bite)**.** *For L-series $L_E(s)$, the bite is given by*

$$\beta(E) = \sum_{\gamma}\frac{1}{\gamma^2}$$

where γ is nonzero imaginary part of nontrivial zeros of $L_E(s)$.

This quantity is deeply related to the completed L-function and the rank of an elliptic curve. From the equality (4), we know that

$$\Lambda_E(1+s) = C'_E \cdot (s^{r_E} + \beta_E s^{r_E+2} + p(s))$$

where $p(s)$ is polynomial with higher order than $r_E + 4$ and C'_E is the leading coefficient at the central point. Then we get

$$\frac{\Lambda_E^{(r_E+2)}(1)}{(r_E+2)!} = \beta_E \cdot C'_E$$

or

$$\frac{1}{(r_E+1)(r_E+2)}\frac{\Lambda_E^{(r_E+2)}(1)}{\Lambda_E^{(r_E)}(1)} = \beta_E$$

And the bite can be one way to represent the exact value of the analytic rank. Despite of its simple form, it is not easy to compute the logarithmic derivative of L-function, and the bite is also tough to know if there are many low-lying zeros.

Theorem VI.6. *For the analytic rank r_E of an elliptic curve and the bite β_E,*

$$r_E = \left\lfloor \frac{1}{\sqrt{\beta_E}} \cdot \frac{\Lambda_E'}{\Lambda_E} \left(1 + \frac{1}{\sqrt{\beta_E}}\right) \right\rfloor$$

Proof. From the equation 5, multiplying s on both sides,

$$s \cdot \frac{\Lambda_E'}{\Lambda_E}(1+s) = r_E + 2\sum_{\rho>0} \frac{s^2}{s^2+\rho^2}$$

Then we have

$$s \cdot \frac{\Lambda_E'}{\Lambda_E}(1+s) = r_E + \sum_{\rho\neq 0} \frac{1}{1+(\rho/s)^2} < r_E + \sum_{\rho\neq 0} \frac{1}{(\rho/s)^2} = r_E + \beta_E \cdot s^2$$

so if we substitute $s = \sqrt{1/\beta_E}$, then we have one bound

$$r_E < \frac{1}{\sqrt{\beta_E}} \cdot \frac{\Lambda_E'}{\Lambda_E} \left(1 + \frac{1}{\sqrt{\beta_E}}\right) < r_E + 1.$$

□

VII The Regulator Reg_E of an Elliptic curve E

The mordell theorem tells us that the elliptic curve over $\mathbb{Q}$ is isomorphic to the product of the torsion points part and the free part. So we can consider a generators of $E(\mathbb{Q})/E_{tor}(\mathbb{Q})$, namely $P_1, P_2, \cdots, P_r$ where r is rank of an elliptic curve. Before we define the regulator, let's consider a height function on the elliptic curve over rational numbers.

Definition VII.1 (The naive logarithmic height)**.** *Let h be a function from $E/\mathbb{Q}$ to $\mathbb{R}$ such that $h(O) = 0$. For nonzero point P on E, let $x(P) = \frac{p}{q}$ denotes the reduced fraction of the first coordinate of P under assumption that $q > 0$. Then the naive height of P is given by*

$$h(P) = max\{\log|p|, \log|q|\}$$

We can easily prove that this function is nearly a quadratic form on E, that is, $h([n]P) \sim n^2 h(P)$ for all integer n. Without loss of generality, we can consider n coprime to q (if not, then reduce once more). Then the left-hand side is simply computed by the Double-and-Add numerical method, and the right-hand side is more straightforward. To compute the Double-and-Add method, we need about $\log_2 n$ doubling and some adding procedure. And the remaining thing is only a brief case classification (for example, whether $h(P) = \log|p|$ or not).

Through this, the naive height can be exactly a quadratic form.

Definition VII.2 (The Néron-Tate height)**.** *Let h be the naive logarithmic height as above. Then define $\hat{h} : E/\mathbb{Q} \to \mathbb{R}$ as following*

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h([2^n]P)}{(2^n)^2}$$

Theorem VII.3 (Néron-Tate)**.** *Let $\hat{h}$ be the Néron-Tate height function as above. Then for all points P, $Q \in E(\mathbb{Q})$, we have the followings*

1. *$\hat{h}(P+Q) + \hat{h}(P-Q) = 2(\hat{h}(P) + \hat{h}(Q))$. This equality is nothing but the parallelogram law for $\hat{h}$.*

2. *$\hat{h}$ is even and quadratic. That is, $\hat{h}([n]P) = n^2\hat{h}(P)$.*

3. *The pairing $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ as following is bilinear.*
$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$$

4. *$\hat{h}(P) = 0$ iff P is a torsion point.*

Proof. Proof is easy when we have (1) already. For (2), even-ness is obtained by substituting P into O. Then $\hat{h}(O+Q)+\hat{h}(O-Q) = 2(\hat{h}(O)+\hat{h}(Q))$ and this implies $\hat{h}(-Q) = \hat{h}(Q)$. And note that $\hat{h}([n]P) = n^2\hat{h}(P)$ hold for $n = 0$ and $n = 1$. Let assume that $\hat{h}$ is quadratic form for k and $k-1$. Then from (1), we have $\hat{h}([k+1]P)+\hat{h}([k-1]P) = 2(\hat{h}([k]P)+\hat{h}(P))$ by substituting P and Q to $[k]P$ and P respectively. Then $\hat{h}([k+1]P) = (-(k-1)^2+2k^2+2)\hat{h}(P) = (k+1)^2\hat{h}(P)$. Also (4) is obtained simultaneously by (2). To prove (3), we only need $\langle P_1+P_2, Q\rangle = \langle P_1, Q\rangle+\langle P_2, Q\rangle$ without loss of generality. There is a four-equations argument in Linear Algebra. In (1), use $P_1 + P_2$ and Q instead of P and Q. And use P_1 and $P_2 - Q$, use $P_1 + Q$ and P_2, use P_2 and Q instead of P and Q respectively. Then the four equations are given by

$$\hat{h}(P_1 + P_2 + Q) + \hat{h}(P_1 + P_2 - Q) = 2\hat{h}(P_1 + P_2) + 2\hat{h}(Q)$$

$$\hat{h}(P_1 + P_2 - Q) + \hat{h}(P_1 - P_2 + Q) = 2\hat{h}(P_1) + 2\hat{h}(P_2 - Q)$$

$$\hat{h}(P_1 + P_2 + Q) + \hat{h}(P_1 - P_2 + Q) = 2\hat{h}(P_1 + Q) + 2\hat{h}(P_2)$$

$$2\hat{h}(P_2 + Q) + 2\hat{h}(P_2 - Q) = 4\hat{h}(P_2) + 4\hat{h}(Q)$$

(The first)$-$(The second)+(The third)$-$(The fourth) gives $2\hat{h}(P_1 + P_2 + Q) - 2\hat{h}(P_2 + Q) = 2\hat{h}(P_1 + P_2) + 2\hat{h}(Q) - 2\hat{h}(P_1) + 2\hat{h}(P_1 + Q) + 2\hat{h}(P_2) - 2\hat{h}(P_2) - 4\hat{h}(Q)$. Divide both sides into 4 and after brief rearranging,

$$LHS = \frac{1}{2}\left(\hat{h}(P_1 + P_2 + Q) - \hat{h}(P_1 + P_2) - \hat{h}(Q)\right)$$

$$RHS = \frac{1}{2}\left(\hat{h}(P_1 + Q) - \hat{h}(P_1) - \hat{h}(Q)\right) + \frac{1}{2}\left(\hat{h}(P_2 + Q) - \hat{h}(P_2) - \hat{h}(Q)\right)$$

the obtained equality is what we desired. □

By using this height function, the regulator can be defined. Through the pairing made by the Néron-Tate height function, the quotient of the Mordell-Weil group $E(\mathbb{Q})/E_{tor}(\mathbb{Q})$ is embedded to $\mathbb{R}^r$ where r is the algebraic rank of an elliptic curve.

Definition VII.4 (The regulator). *Let $\{P_1, P_2, \cdots, P_r\}$ be a generator set of the quotient $E(\mathbb{Q})/E_{tor}(\mathbb{Q})$. Then the regulator of an elliptic curve Reg_E is given by*

$$Reg_E = \det\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}$$

where $\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}$ is the square matrix made by $\langle P_i, P_j\rangle$ for (i, j)-component.

Since we got started with a basis of the quotient of the Mordell-Weil group, the value of the regulator does not depend on the choice of generators. Because any linear combination of row vectors can be negligible when we compute the determinant. So this is well-defined, THE regulator makes sense.

If we consider a rank 1 curve, then the regulator is just the determinant of a singleton matrix. And $\mathrm{Reg}_E = \langle P, P \rangle = \hat{h}(P)$. Since P is a generator and $\hat{h}$ is a quadratic form, the regulator is the smallest positive height of the curve. If generators P_i jump with big steps (or tiny steps) while generating the free part, the regulator will be large (or small). That is, the regulator regulates a regularity size of the free part.

Conjecture VII.5 (Lang's height conjecture)**.** *There exists a positive constant K such that $\hat{h}(P) \geq K \log |D_E|$ for any non-torsion point P of an elliptic curve.*

This conjecture is from [LLL+97]. By Elkies [Elk06], assuming the ABC, K is bounded below by 3.9479×10^{-5}. Since the conductor always divides the discriminant,

Corollary VII.6. *There exists a positive constant K such that $\hat{h}(P) \geq K$ for any non-torsion point P of an elliptic curve.*

Theorem VII.7. *Under BSD and ABC,*

$$Reg_E \geq 4.36 \cdot 10^{-6} \cdot (N_E)^{-3.86} \cdot \frac{1}{\Gamma(1.8 + 0.25 \log N_E)}$$

Furthermore, under GRH,

$$Reg_E \geq 2.11 \cdot 10^{-2} \cdot (N_E)^{-2.47} \cdot \frac{1}{\Gamma(1.25 + 0.16 \log N_E)}$$

Proof. For a conductor less than 350000, the Cremona table gives us numerical proof. So let assume that $N_E \geq 350000$. By Elkies' bound for conjecture 5.5,

$$\hat{h} \geq 3.9479 \cdot 10^{-5} \cdot \log |D_E| \geq 3.9479 \cdot 10^{-5} \cdot \log(350000) = 5.0397 \cdot 10^{-4}$$

Then the minimum height is given by $h = 5.0397 \cdot 10^{-4}$ Consider the quotient image of $E(\mathbb{Q})$ under the map $\hat{h}$ where r is the rank of E. By Minkowski's inequality about r-dimensional lattice covolume V_L,

$$V_L \geq \left(\frac{\sqrt{\pi}}{2} h\right)^r \cdot \frac{1}{\Gamma(1 + 0.5r)}$$

where h is the non-zero vector in L with the minimum length. Now we obtain

$$\mathrm{Reg}_E \geq \left(\frac{\sqrt{\pi}}{2} h\right)^r \cdot \frac{1}{\Gamma(1 + 0.5r)}$$

Note that the regulator is defined as the covolume of the lattice under Néron-Tate pairing map.

We know that there are two bounds from the theorem VI.3 and corollary VI.4,

$$r < 0.5 \log N_E + 1.6, \; r < 0.32 \log N_E + 0.5$$

Additionally under the GRH, the latter one is given. So trim the regulator inequality by using two bounds and $h = 5.0397 \cdot 10^{-4}$, then it yields

$$\mathrm{Reg}_E \geq \left(\frac{\sqrt{\pi}}{2} \cdot h\right)^{a \log N_E + b} \cdot \frac{1}{\Gamma(1 + 0.5(a \log N_E + b))}$$

Note that the base of the first factor is less than 1 obviously, and the Gamma function is increasing since $N_E > 350000$, so the inequality still hold for upper bound of rank. Now direct substitution gives the results as stated. □

As the conductor grows up, bounds of the regulator decrease since negative power of the conductor and the gamma value of $\log N_E$ is in denominator, so it is nearly obeys a factorial scale. The one sad thing is rank bound stated. According to recent works, average value of rank is nearly between 0 and 1. Especially Goldfeld, Katz-Sarnak guessed 1/2 for the average value. Under the BSD and GRH, Heath-Brown [HB$^+$04] improved that value to be 2. Bhargava and Shankar [BS15a] [BS15b] [BS13] cut this upper bound down to 0.885 unconditionally.

VIII The Algorithm and Bounds

8.1 The analytic algorithm

Now we have all ingredients to make the algorithm, and we basically assume the BSD conjecture, so we actually obtain the analytic rank but it is the rank of an elliptic curve. For the basic setting, we have global minimal Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with the conductor N_E. The following is Spicer's analytic rank algorithm.

Algorithm 1 Analytic Rank Algorithm.

```
1: Compute the real period $\Omega_E$ of $E$.
2: Set $k = \lceil 26 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 0.25 \log N_E)) - \log_2 \Omega_E \rceil$.
3: Evaluate $L_E(1)$ to $k$ bits precision.
4: If all $k$-bit digits are non-zero, then the rank is 0.
5: Otherwise, $L_E(1) \equiv 0$ and now evaluate $L'_E(1)$. That is, $m \mapsto m + 1$.
6: This procedure stops if $L_E^{(m)}(1)$ is not zero to $k$ bits precision, and then output the analytic
   rank of elliptic curve $r_E = m$.
```

In this algorithm, we have one important step. It is the step (5). Why would we conclude that $L_E(1)$ is identically 0? Spicer offers the right route in [Spi15].

Theorem VIII.1 (Spicer)**.** *Let k be the given value*

$$k = \lceil 26 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 0.25 \log N_E)) - \log_2 \Omega_E \rceil$$

For $m \geq 0$, if $L_E^{(m)}(1)$ is zero to k bits precision, then $L_E^{(m)}(1)$ is identically 0.

Proof. Note that the Taylor series of $L_E(1 + s)$ at $s = 0$ is given by

$$L_E(1 + s) = L_E(1) + L'_E(1)s + L''_E(1)\frac{s^2}{2!} + \cdots$$

As considering the rank of E,

$$L_E(1 + s) = C_E \cdot L_E^{(r_E)}(1)\frac{s^{r_E}}{(r_E)!} + D_E \cdot L_E^{(r_E+1)}(1)\frac{s^{r_E+1}}{(r_E + 1)!} + \cdots$$

And by the BSD conjecture, we can compute that leading coefficient C_E

$$C_E = \frac{\Omega_E \times \mathrm{Reg}_E \times \#Sha(E) \times \prod_p c_p}{(\#E_{tor}(\mathbb{Q}))^2}$$

we have the following trivial bounds

$$\#Sha(E) \geq 1, \ \prod_p c_p \geq 1, \ \#E_{tor}(\mathbb{Q}) \leq 16$$

Taking log with base 2 both sides and use the theorem VII.7,

$$\log_2 C_E \geq -25.81 - 3.86 \log_2 N_E - \log_2(\Gamma(1.8 + 0.25 \log N_E)) + \log_2 \Omega_E > -k$$

. □

8.2 Some bounds of the rank

Theoritically, the analytic algorithm in [Spi15] can run for all elliptic curves. But for an elliptic curve with the large conductor, the speed of algorithm is much slower. In that situation, instead of the algorithm which gives us the exact value of the rank, we can bound the rank of an elliptic curve in the shorter runtime. Let $\Re(s) > 0$ and $s = \sigma + i\tau$, then the equation (5) says that

$$\begin{aligned}\Re\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right) = \Re\left(\sum_{\rho\neq 0}\frac{s}{s^2+\rho^2}\right) &= \frac{1}{2}\sum_{\rho\neq 0}\Re\left(\frac{1}{\sigma+i\tau}+\frac{1}{\sigma-i\tau}\right)\\ &= \frac{1}{2}\sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+(\rho-\tau)^2}+\frac{\sigma}{\sigma^2+(\rho+\tau)^2}\right)\end{aligned}$$

In the last summation, the first inner term and the second inner term are symmetric as a result, since the first inner term for $\rho < 0$ is the same as the second inner term for $\rho > 0$ and vice versa. Therefore

$$\Re\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right) = \sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+(\rho-\tau)^2}\right)$$

Using this, we can approximate the growth tendency of the real part of the logarithmic derivative.

Lemma VIII.2. *Let $s = \sigma + i\tau$ and ρ be a nontrivial zeros of L-function.*

$$\left|\sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+(\rho-\tau)^2}\right) - \left\{\log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \Re(\psi(1+\sigma+i\tau))\right\}\right| < -2\frac{\zeta'}{\zeta}\left(\frac{1}{2}+\sigma\right)$$

where N_E is the conductor, $\psi(s)$ is the Digamma function.

Proof.

$$\begin{aligned}\sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+(\rho-\tau)^2}\right) &= \Re\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right)\\ &= \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \Re(\psi(1+\sigma+i\tau)) + \Re\left(\frac{L_E'}{L_E}(1+s)\right)\end{aligned}$$

Properly transpose the logarithm and the Digamma function, and use the inequality (2) of theorem IV.6. □

Theorem VIII.3. *(GRH) Let $\sigma > 1/2$, and r_E be the analytic rank of an elliptic curve, then*

$$\sigma\cdot\beta_E + \frac{r_E}{\sigma} > \frac{1}{2}\log N_E + \psi(1+\sigma) - \log(2\pi) + 2\frac{\zeta'}{\zeta}\left(\frac{1}{2}+\sigma\right)$$

where β_E is the bite, $\psi(s)$ is the Digamma function and N_E is the conductor of an elliptic curve E.

Proof. By the lemma VIII.2, taking $\tau = 0$,

$$\log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \Re(\psi(1+\sigma)) + 2\frac{\zeta'}{\zeta}\left(\frac{1}{2}+\sigma\right) < \sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+\rho^2}\right)$$

And

$$\begin{aligned}\sum_{\rho\neq 0}\left(\frac{\sigma}{\sigma^2+\rho^2}\right) &= \frac{1}{\sigma}\sum_{\rho\neq 0}\frac{1}{1+(\rho/\sigma)^2}\\ &< \frac{1}{\sigma}\left(r_E+\sum_{\rho\neq 0}\frac{1}{(\rho/\sigma)^2}\right) = \frac{r_E}{\sigma}+\sigma\cdot\beta_E\end{aligned}$$

□

Using this theorem, finally we get some bounds of the bite, the rank, and the leading coefficient. With these inequalities, we can approximate the growth rate of those quantities with the logarithm scale of the conductor of E.

Corollary VIII.4. *Let C'_E be the leading coefficient of the Taylor series of the completed L-function, then*

1. $(1+\beta_E)\cdot C'_E < 0.173\cdot N_E$
2. $\beta_E+\log C'_E > \log N_E - 5.229$
3. $\beta_E + r_E > \frac{1}{2}\log N_E - 4.426$

where β_E is the bite, N_E is the conductor of E, and r_E is the analytic rank of E.

Proof. Noting that the equality 4 and the definition of $\Lambda_E(s)$, we have

$$C'_E\cdot\prod_{\rho\neq 0}\left(1+\frac{1}{\rho^2}\right) = \Lambda_E(2) = \frac{N_E}{(2\pi)^2}\cdot L_E(2)$$

And using (1) of theorem IV.6, we can bound $L_E(2)$

$$C'_E\cdot(1+\beta_E) < C'_E\cdot\prod_{\rho\neq 0}\left(1+\frac{1}{\rho^2}\right) = \Lambda_E(2) = \frac{N_E}{(2\pi)^2}\cdot L_E(2) < \frac{N_E}{(2\pi)^2}\cdot\zeta\left(\frac{3}{2}\right)^2$$

This gives the first inequality. In other way,

$$C'_E\cdot e^{\beta_E} > C'_E\cdot\prod_{\rho\neq 0}\left(1+\frac{1}{\rho^2}\right) = \Lambda_E(2) = \frac{N_E}{(2\pi)^2}\cdot L_E(2) > \frac{N_E}{(2\pi)^2}\cdot\frac{\zeta(3)^2}{\zeta(3/2)^2}$$

so this gives the second inequality. The third inequality is just the case of $\sigma = 1$ for the theorem VIII.3. □

IX The List of Corrections

Actually Simon Spicer take some insignificant mistakes in his thesis [Spi15]. As I have reviewed his thesis, I corrected his computations. In [Spi15],

1. If m has the same parity as E, the derivative of the completed L-function at the central point is
$$\Lambda_E^{(m)}(1) = 2\sum_{n=1}^{\infty} a_n \int_1^{\infty} e^{-\frac{2\pi n}{\sqrt{N_E}}t} \left(\log \frac{t}{\sqrt{N_E}}\right)^m dt.$$

2. In the Spicer's algorithm, the original k value is given by
$$k = \lceil 34 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 0.25 \log N_E)) - \log_2 \Omega_E \rceil.$$

The Corrections

1. If m has the same parity as E, the derivative of the completed L-function at the central point is
$$\Lambda_E^{(m)}(1) = 2\sum_{n=1}^{\infty} a_n \int_1^{\infty} e^{-\frac{2\pi n}{\sqrt{N_E}}t} (\log t)^m dt$$
The inner logarithm is fixed.

2. In the Spicer's algorithm, the original k value is given by
$$k = \lceil 26 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 0.25 \log N_E)) - \log_2 \Omega_E \rceil$$
the k value becomes smaller, so the algorithm becomes better since the less bit-precision checking is needed.

References

[BS13] Manjul Bhargava and Arul Shankar, *The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1*, arXiv preprint arXiv:1312.7859 (2013).

[BS15a] ———, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics (2015), 191–242.

[BS15b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Annals of Mathematics (2015), 587–621.

[Edw74] Harold M Edwards, *Riemann's zeta function*, vol. 58, Academic press, 1974.

[Elk06] Noam D Elkies, *Points of low height on elliptic curves an d surfaces i: Elliptic surfaces over $\mathbb{P}^1$ with small d*, International Algorithmic Number Theory Symposium, Springer, 2006, pp. 287–301.

[HB$^+$04] DR Heath-Brown et al., *The average analytic rank of elliptic curves*, Duke Mathematical Journal **122** (2004), no. 3, 591–623.

[IJT14] Özlem Imamoḡlu, Jonas Jermann, and Árpád Tóth, *Estimates on the zeros of E_2*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, vol. 84, Springer, 2014, pp. 123–138.

[Kna92] Anthony W Knapp, *Elliptic curves*, vol. 40, Princeton University Press, 1992.

[LLL$^+$97] Serge Lang, Serge Lang, Serge Lang, France Mathematician, Serge Lang, and France Mathématicien, *Survey of diophantine geometry*, vol. 309, Springer Berlin, 1997.

[MS13] Barry Mazur and William Stein, *How explicit is the explicit formula?*, preprint, available at http://www. math. harvard. edu/˜ mazur/papers/How. Explicit. pdf Last Updated March (2013).

[Sil13] Joseph H Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 2013.

[Spi15] Simon Vernon Bok Spicer, *The zeros of elliptic curve l-functions: analytic algorithms with explicit time complexity*, Ph.D. thesis, 2015.

[Vio16] Carlo Viola, *An introduction to special functions*, Unitext, vol. 102, Springer, [Cham], 2016, La Matematica per il 3+2. MR 3586206

[Was03] Lawrence C Washington, *Elliptic curves: number theory and cryptography*, Chapman and Hall/CRC, 2003.

[WY14] Rachael Wood and Matthew P Young, *Zeros of the weight two eisenstein series*, Journal of Number Theory **143** (2014), 320–333.

Acknowledgements

I sincerely thanks to my advisor Peter Jae-Hyun Cho, who has provided many mathematical teachings, philosophies, and personal mentorships to make this paper exist. I also thanks to the other members of my dissertation reading committee, Hae-Sang Sun and Chol Park.

And my family - parents, and two younger brothers(and two pretty cats) always give me an endless supports, trust and love. They are the anchor of all of me. My high school teacher Jae-Yong Baek, he taught me how math is beautiful. He really made me love my own math.