On Zeros of the p-adic zeta-Function, and Generic Newton Polygons of Hecke Polynomials

Guowei Shan

May 8, 2019

Abstract

This paper introduces the p-adic ζ-function and Hecke polynomials with Newton Polygon, respectively. Motivated by finding zeros of p-adic ζ-function, we study so-called Δ-conjecture, using p-adic techniques. In the second section of the paper, we consider the generic Newton polygon of Hecke polynomials for fixed prime p and congruence subgroup Γ. We then give some conjectures on length of the zero slope and quadratic lower bounds of generic Newton polygons for different p and Γ.

Contents

1 The p-adic ζ-Function **1**
1.1 Introduction to p-adic ζ-Function . . . 1
1.2 Irregular pair and Δ-conjecture . . . 3

2 Hecke Polynomials **6**
2.1 Introduction to Hecke Polynomial . . . 6
2.2 Newton Polygons for congruence subgroup $\Gamma_0(3)$ . . . 7
2.3 Newton Polygons for other congruence subgroups . . . 10

3 Appendix **11**
3.1 Magma Code . . . 11
3.2 Sage Code . . . 11

1 The p-adic ζ-Function

1.1 Introduction to p-adic ζ-Function

The Riemann ζ-function is defined as a function of real numbers greater than 1 by :

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

One can easily show that this series converges for $s > 1$.

The p-adic ζ-function can be constructed by the p-adic interpolation of Riemann ζ-function. However, instead of exploring the interpolation step by step, we will first introduce some basic definitions and theorems, and then define the p-adic ζ-function directly.

Definition 1.1. *The k^{th} Bernoulli number B_k is defined as the coefficient of the term $t^k/k!$ in the Taylor series for*

$$\begin{aligned}\frac{t}{e^t-1} &= \frac{1}{1+t/2!+t^2/3!+t^3/4!+\cdots} \\ &= \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.\end{aligned}$$

Here are the first few Bernoulli numbers:

$$B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0, B_4 = -1/30, \ldots$$

All Bernoulli numbers are rational. In addition, we define $\widehat{B}(k) = B_k/k$. The following theorem [3, Chap. 2] provides us with some useful properties of Bernoulli numbers.

Theorem 1.2. *Let $k \in \mathbb{N}$ and p be a prime number.*

1. *If $k > 1$ is odd, then $\widehat{B}(k) = 0$.*
2. *If $p-1 \nmid k$, then $\widehat{B}(k)$ is a p-adic integer.*

Throughout this paper, we only consider odd prime numbers p and Bernoulli numbers with even index k.

Theorem 1.3 (Kummer's congruence)**.** *Let p be a prime, $k, k', N \in \mathbb{N}$. If $p-1 \nmid k$ and $k \equiv k' (mod\ p^N(p-1))$, then*

$$(1-p^{k-1})\widehat{B}(k) \equiv (1-p^{k'-1})\widehat{B}(k') (mod\ p^{N+1}).$$

Theorem 1.4 (E. Lehmer [1])**.** *Let p be a prime and k be a positive even integer. If $p-1 \nmid k-2$, then*

$$(2^k-1)\widehat{B}(k) \equiv \sum_{0<a<p/2} (p-2a)^{k-1} (mod\ p^2).$$

Now let's consider the function in two variables t and x:

$$\frac{te^{xt}}{e^t-1} = (\sum_{k=0}^{\infty} B_k \frac{t^k}{k!})(\sum_{k=0}^{\infty} \frac{(xt)^k}{k!}).$$

In this product, by collecting terms with t^k, we obtain a polynomial in x for each k. The k^{th} Bernoulli polynomial $B_k(x)$ is defined by the product of $k!$ and that polynomial, i.e.

$$\frac{te^{xt}}{e^t-1} = \sum_{k=0}^{\infty} B_k(x) \frac{t^k}{k!}.$$

In the following definitions, $\mathbb{Q}_p$ is the set of all p-adic numbers. In addition, $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ mean the set of p-adic integers and the set of p-adic units, which are the compact-open subsets of $\mathbb{Q}_p$. A p-adic interval $a + p^N\mathbb{Z}_p$ is defined by

$$a + p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x-a|_p \leqslant 1/p^N\}$$

for some $a \in \mathbb{Q}_p$ and $N \in \mathbb{Z}$. It is sometimes abbreviated as $a + (p^N)$, where $a \in \mathbb{Z}_p$. Without loss of generality, we can further assume that a is an integer between 0 and $p^N - 1$.

Definition 1.5. *Let X be a compact-open subset of $\mathbb{Q}_p$, such as $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$. A p-adic distribution μ on X is an additive map from the set of compact-opens in X to $\mathbb{Q}_p$. It means that if $U \subset X$ is the disjoint union of compact-open sets $U_1, U_2, \ldots, U_n$, then $\mu(U) = \mu(U_1) + \mu(U_2) + \cdots + \mu(U_n)$. And the p-adic distribution μ is a measure if its values on $U \subset X$ are bounded by some constant $B \in \mathbb{R}$, i.e., $|\mu(U)|_p \leqslant B$ for every compact-open $U \subset X$.*

Now we define a map $\mu_{B,k}$ on the intervals $a + (p^N)$ by

$$\mu_{B,k}(a + (p^N)) = p^{N(k-1)} B_k(\frac{a}{p^N}).$$

Since

$$\mu_{B,k}(a + (p^N)) = \sum_{b=0}^{p-1} \mu_{B,k}(a + bp^N + (p^{N+1})), \forall a + (p^N) \subset \mathbb{Z}_p,$$

$\mu_{B,k}$ extends uniquely [3, p.32] to a p-adic distribution on $\mathbb{Z}_p$, which is called the k^{th} Bernoulli distribution.

Although Bernoulli distributions are not measures, they can be turned into measures by "regularization". Let α be an integer not equal to 1 and not divisible by p, and $\mu_{B,k}$ be the k^{th} Bernoulli distribution. The regularized Bernoulli distribution on $\mathbb{Z}_p$ is defined by

$$\mu_{k,\alpha}(U) = \mu_{B,k}(U) - \alpha^{-k}\mu_{B,k}(\alpha U), \text{ for all compact-open } U \subset \mathbb{Z}_p.$$

One can verify that $\mu_{k,\alpha}$ is a measure on $\mathbb{Z}_p$.

Definition 1.6. *Let μ be a p-adic measure on X and let $f : X \to \mathbb{Q}_p$ be a continuous function. We define the Riemann sums*

$$S_{N,(x_{a,N})} = \sum_{\substack{0 \leqslant a < p^N; \\ a+(p^N) \subset X}} f(x_{a,N})\mu(a + (p^N)),$$

where the sum is taken over all a for which $0 \leqslant a < p^N$ and $a + (p^N) \subset X$, and $x_{a,N}$ is an arbitrary point in the interval $a + (p^N)$. And we define $\int_X f\mu$ to be the limit of $S_{N,(x_{a,N})}$, as $N \to \infty$.

With the definition of $\int_X f\mu$, we can define the p-adic ζ-function.

Definition 1.7. *Fix prime number p and $s_0 \in \{0, 1, 2, \ldots, p-2\}$. For $s \in \mathbb{Z}_p (s \neq 0$ if $s_0 = 0)$, the p-adic ζ-function $\zeta_{p,s_0}(s)$ is defined by*

$$\zeta_{p,s_0}(s) = \frac{1}{\alpha^{-(s_0+(p-1)s)} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1} \mu_{1,\alpha}.$$

It is worth noting that the p-adic ζ-function ζ_{p,s_0} is independent of the choice of α.

1.2 Irregular pair and Δ-conjecture

For fixed prime p and s_0 as above, does the p-adic ζ-function ζ_{p,s_0} have any zero? In other words, can we find some p-adic integer s, such that $\zeta_{p,s_0}(s) = 0$? B.C. Kellner studied this question and proved that $\zeta_{p,l}(s)$ has a unique zero [2, Theorem 4.6] when (p, l) is an irregular pair (defined below), assuming the so-called "Δ-Conjecture" holds.

Definition 1.8. *Let p be an odd prime and l be a positive integer. The pair (p, l) is an irregular pair if $p \mid \widehat{B}(l)$, where l is even and $2 \leqslant l \leqslant p-3$. The index of irregularity of p is defined by*

$$i(p) = \#\{(p, l) : p \mid \widehat{B}(l); l = 2, 4 \ldots p-3\}$$

The prime p is called an irregular prime if $i(p) \neq 0$

Here $p \mid \widehat{B}(l)$ means p divides the numerator of $\widehat{B}(l)$. Or if we think $\widehat{B}(l)$ as a p-adic integer, i.e. $\widehat{B}(l) = \sum_{n=0}^{\infty} a_n p^n$, then $p \mid \widehat{B}(l)$ implies a_0=0. Then we define Ψ^{irr} to be the set of all irregular pairs.

Definition 1.9. *For $(p,l) \in \Psi^{irr}$, define*

$$\Delta_{(p,l)} \equiv p^{-1}(\widehat{B}(l+p-1) - \widehat{B}(l)) \ (mod\ p),$$

where $0 \leqslant \Delta_{(p,l)} < p$. If $\Delta_{(p,l)} = 0$, then we say $\Delta_{(p,l)}$ is singular, otherwise nonsingular .

Conjecture 1.10 (Δ-Conjecture)**.** *$\Delta_{(p,l)}$ is nonsingular for all irregular pairs $(p,l) \in \Psi^{irr}$.*

Consider $(p,l) \in \Psi^{irr}$. By the definition of irregular pair, we already know $p \mid \widehat{B}(l)$. In order to have $\Delta_{(p,l)}$ well-defined, p should also divide $\widehat{B}(l+p-1))$, which is proved by the following lemma.

Lemma 1.11. *For every irregular pair $(p,l) \in \Psi^{irr}$, $p \mid \widehat{B}(l+p-1)$.*

Proof. By definition, l is an even integer between 2 and $p-3$. So $p-1 \nmid l$. Since $l \equiv l+p-1 \pmod{p-1}$, by Kummer Congruence, $(1-p^{l-1})\widehat{B}(l) \equiv (1-p^{l+p-2})\widehat{B}(l+p-1) \pmod p$. Since $l \geqslant 2$, $p^{l-1}\widehat{B}(l) \equiv p^{l+p-2}\widehat{B}(l+p-1) \equiv 0 \pmod p$. It implies that $\widehat{B}(l) \equiv \widehat{B}(l+p-1) \pmod p$. Since $(p,l) \in \Psi_1^{irr}$, $p \mid \widehat{B}(l)$. Therefore, $\widehat{B}(l+p-1) \equiv 0 \pmod p$. □

By the previous lemma, in order to prove Δ-conjecture holds, it suffices to show that $\widehat{B}(l+p-1) - \widehat{B}(l) \not\equiv 0 \pmod{p^2}$.

Lemma 1.12. *Let p be an odd prime and k be an even natural number. If $p-1 \nmid k$, then*

$$\sum_{0<a<p/2} a^k \equiv 0 (mod\ p).$$

Proof. Since p is odd, 2 and p are relatively prime. It suffices to show that $2 \sum_{0<a<p/2} a^k \equiv 0 (\text{mod } p)$. Since k is even,

$$\begin{aligned} 2 \sum_{0<a<p/2} a^k &\equiv \sum_{0<a<p/2} a^k + \sum_{0<a<p/2} (p-a)^k \\ &\equiv \sum_{0<a<p/2} a^k + \sum_{p/2<a<p} a^k \\ &\equiv \sum_{0<a<p} a^k (\text{mod } p) \end{aligned}$$

Since $\mathbb{F}_p^\times = \{1, 2, \dots p-1\}$ is a cyclic group, there exists a $l \in \mathbb{F}_p^\times$, such that $\langle l \rangle = \mathbb{F}_p^\times$. Since $p-1 \nmid k$, $l^k \not\equiv 1 \pmod p$. Assume $S = \sum_{0<a<p} a^k$, then

$$l^k S \equiv \sum_{0<a<p} (la)^k \equiv \sum_{0<b<p} b^k \equiv S \pmod p$$

It follows that $(l^k-1)S \equiv 0 \pmod p$. Since $l^k \not\equiv 1 \pmod p$, S must be congruent to 0 mod p. □

Theorem 1.13. *Δ-conjecture holds if for every irregular pair (p,l), $(2^l-1) \cdot \sum_{0<a<p/2} (-2a)^{l-1} m_a \not\equiv 0$ (mod p), where $(-2a)^{p-1} \equiv 1 + m_a \cdot p$ (mod p^2).*

Proof. Since $(2^l-1) \cdot \sum_{0<a<p/2} (-2a)^{l-1} m_a \not\equiv 0 \pmod p$, $2^l \not\equiv 1 (\text{mod } p)$. By Fermat's Little Theorem, $2^{l+p-1} \not\equiv 1 \pmod p$. It follows that $2^l, 2^{l+p-1} \not\equiv 1 \pmod{p^2}$. Let's consider $(\widehat{B}(l+p-1) - \widehat{B}(l))(2^{l+p-1}-1)(2^l-1) \pmod{p^2}$ and replace l by $2k$. Since $p-1 \nmid 2k-2$, by Theorem 1.4, we obtain:

$$
\begin{aligned}
(\widehat{B}(2k+p-1) - \widehat{B}(2k))(2^{2k+p-1}-1)(2^{2k}-1)& \\
&\equiv (2^{2k}-1) \sum_{0<a<p/2} (p-2a)^{2k+p-2} - (2^{2k+p-1}-1) \sum_{0<a<p/2} (p-2a)^{2k-1} \\
&\equiv A + B \pmod{p^2}
\end{aligned}
$$

where

$$
A := \left((2^{2k}-1) \sum_{0<a<p/2} (-2a)^{2k+p-2} \right) - \left((2^{2k}2^{p-1}-1) \sum_{0<a<p/2} (-2a)^{2k-1} \right).
$$

$$
B := \left((2^{2k}-1) \sum_{0<a<p/2} (2k+p-2)(-2a)^{2k+p-3}p \right) - \left((2^{2k}2^{p-1}-1) \sum_{0<a<p/2} (2k-1)(-2a)^{2k-2}p \right).
$$

If we divide B by p, then

$$
p^{-1}B \equiv (2^{2k}-1) \sum (2k+p-2)(-2a)^{2k+p-3} - (2^{2k}2^{p-1}-1) \sum (2k-1)(-2a)^{2k-2} \pmod{p}.
$$

Since $gcd(-2a, p) = gcd(2, p) = 1$, by Fermat's Little Theorem, we obtain:

$$
\begin{aligned}
p^{-1}B &\equiv (2^{2k}-1) \sum (2k+p-2)(-2a)^{2k-2} - (2^{2k}-1) \sum (2k-1)(-2a)^{2k-2} \\
&\equiv (2^{2k}-1) \sum (p-1)(-2a)^{2k-2} \\
&\equiv (2^{2k}-1)2^{2k-2}(-1) \sum a^{2k-2} \pmod{p}.
\end{aligned}
$$

By Lemma 1.12, B is congruent to 0 mod p^2.

Now let's consider A. Fermat's Little Theorem implies that $2^{p-1} \equiv 1 + l \cdot p \pmod{p^2}$ and $(-2a)^{p-1} \equiv 1 + m_a \cdot p \pmod{p^2}$, for some integers $0 \leqslant l, m_a \leqslant (p-1)$. If we replace 2^{p-1} by $1 + lp$ and $(-2a)^{p-1}$ by $1 + m_a p$ in A, we obtain:

$$
\begin{aligned}
A &\equiv (2^{2k}-1) \sum (1+m_a p)(-2a)^{2k-1} - (2^{2k}(1+lp)-1) \sum (-2a)^{2k-1} \\
&\equiv (2^{2k}-1) \sum m_a p(-2a)^{2k-1} - 2^{2k} lp \sum (-2a)^{2k-1} \pmod{p^2}
\end{aligned}
$$

If we divide A by p, then

$$
p^{-1}A \equiv (2^{2k}-1) \sum m_a (-2a)^{2k-1} - 2^{2k} l \sum (-2a)^{2k-1} \pmod{p}.
$$

Since $(p, 2k)$ is an irregular prime, by definition, $p|\widehat{B}(2k)$. Thus $(2^{2k}-1)\widehat{B}(2k) \equiv 0 \pmod{p}$. By Theorem 1.4,

$$
(2^{2k}-1)\widehat{B}(2k) \equiv \sum_{0<a<p/2} (p-2a)^{2k-1} \pmod{p^2}.
$$

The congruence relation also holds for modulo p. Hence,

$$
(2^{2k}-1)\widehat{B}(2k) \equiv \sum_{0<a<p/2} (p-2a)^{2k-1} \equiv \sum_{0<a<p/2} (-2a)^{2k-1} \equiv 0 \pmod{p}
$$

It implies that $p^{-1}A \equiv (2^{2k}-1) \sum m_a (-2a)^{2k-1} \pmod{p}$. Since $(2^{2k}-1) \sum m_a (-2a)^{2k-1} \not\equiv 0 \pmod{p}$, by assumption, $A \not\equiv 0 \pmod{p^2}$. Since $2^{2k}, 2^{2k+p-1} \not\equiv 1 \pmod{p^2}$, we obtain $\widehat{B}(2k+p-1) - \widehat{B}(2k) \not\equiv 0 \pmod{p^2}$. Therefore, Δ-conjecture holds.

□

2 Hecke Polynomials

2.1 Introduction to Hecke Polynomial

Definition 2.1. *The special linear group of degree 2 over integers*

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

is called the full modular group.

For any positive integer N, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | a \equiv d \equiv 1, b \equiv c \equiv 0 (\text{mod } N) \right\}.$$

$\Gamma(N)$ is a normal subgroup of $SL_2(\mathbb{Z})$ and is called the principal congruence subgroup of level N. A subgroup of $SL_2(\mathbb{Z})$ is called a congruence subgroup of level N if it contains $\Gamma(N)$. Here are two important congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \equiv 0 \ (\text{mod } N) \right\};$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) | a \equiv 1 \ (\text{mod } N) \right\}.$$

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $H = \{z \in \mathbb{C} | Im(z) > 0\}$. Let $f(z)$ be a function on $\bar{H} = H \cup \mathbb{Q} \cup \{\infty\}$ with values in $\mathbb{C} \cup \{\infty\}$, and let $k \in \mathbb{Z}$. We define $f|[\gamma]_k$ as a function whose value at $z \in \bar{H}$ is $(cz+d)^{-k} f((az+b)/(cz+d))$, i.e.

$$f(z)|[\gamma]_k = (cz+d)^{-k} f((az+b)/(cz+d)), for\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Definition 2.2. *Let $f(z)$ be a meromorphic function on H, and Γ be a congruence subgroup of level N. Let $k \in \mathbb{Z}$.*

1. *$f(z)$ is a modular function of weight k for Γ if*

$$f|[\gamma]_k = f, \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

   and if for any $\gamma_0 \in SL_2(\mathbb{Z})$,

$$f(z)|[\gamma_0]_k \text{ has the form } \sum_{-\infty}^{\infty} a_n q^n \text{ with } q = e^{2\pi i z} \text{ and } a_n = 0 \text{ for } n << 0.$$

2. *If a modular function $f(z)$ is holomorphic on H, and if for all $\gamma_0 \in SL_2(\mathbb{Z})$, $a_n = 0$ for all $n < 0$, then $f(z)$ is a modular form of weight k for Γ.*
3. *If $f(z)$ is a modular form with $a_0 = 0$, then $f(z)$ is a cusp-form.*

The set of all modular forms of weight k for Γ and the set of all cusp-forms of weight k for Γ are denoted by $M_k(\Gamma)$ and $S_k(\Gamma)$ respectively. Both $M_k(\Gamma)$ and $S_k(\Gamma)$ are vector spaces.

Although the general definition of Hecke operator is complicated, we can obtain the following equivalent definition [4] of the p^{th}-Hecke operator T_p for prime number p.

Definition 2.3. *Let p be a prime number and $S_k(\Gamma)$ be the set of cusp forms of weight k, for some congruence subgroup Γ of level N. Let $f(z) = \sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi i z}$, $f \in S_k(\Gamma)$. If we define $U_p(f) = \sum_{n=1}^{\infty} a_{pn} q^n$ and $V_p(f) = \sum_{n=1}^{\infty} a_n q^{pn}$, then the p^{th}-Hecke operator*

$$T_p = \begin{cases} U_p & \text{if } p|N \\ U_p + p^{k-1}V_p & \text{if } p \nmid N \end{cases}.$$

T_p is an operator on $S_k(\Gamma)$. Then we can define the Hecke polynomial as

$$H_k(x) = \begin{cases} det(I - T_p x | S_k(\Gamma)) & \text{if } p \mid N \\ det(I - T_p x + p^{k-1}x^2 I | S_k(\Gamma)) & \text{if } p \nmid N \end{cases},$$

where I is the identity matrix whose size is the same as T_p.

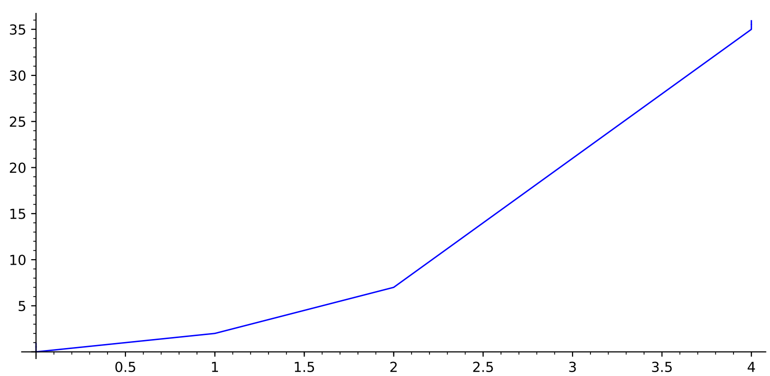
For example, suppose $T_p = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a Hecke operator T_p and $p \nmid N$. By definition, we obtain:

$$\begin{aligned} H_k &= det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} p^{k-1}x^2 & 0 \\ 0 & p^{k-1}x^2 \end{pmatrix}\right) \\ &= det\begin{pmatrix} 1 - ax + p^{k-1}x^2 & -bx \\ -cx & 1 - dx + p^{k-1}x^2 \end{pmatrix} \end{aligned}$$

We can write $H_k = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4$ by expanding the polynomial in powers of x. Given any Hecke polynomial H_k with prime p, we can define what the newton polygon of H_k is.

Definition 2.4 (Newton Polygon). *Let $H_k = \sum_{i=0}^{n} c_i x^i$ be a Hecke polynomial. The Newton polygon of H_k is defined to be the lower convex hull of the set of points $P_{p,k} = \{(i, ord_p(c_i)) : 0 \leqslant i \leqslant n\}$.*

Example:



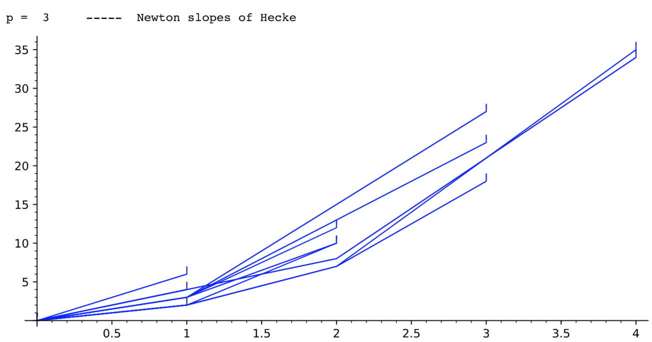
(a) Newton polygon: $p = 3, \Gamma' = \Gamma_1(3), k = 30$

2.2 Newton Polygons for congruence subgroup $\Gamma_0(3)$

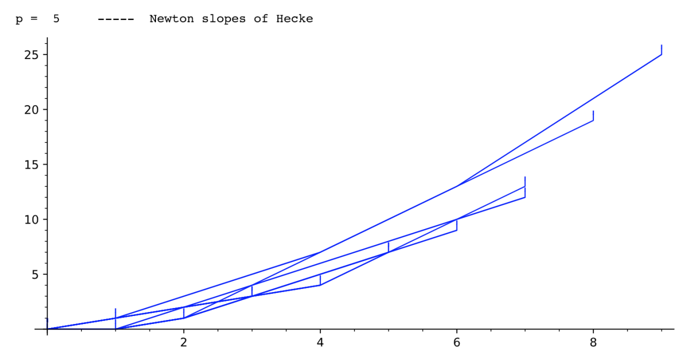
In this section, we fix the congruence subgroup to be $\Gamma_0(3)$ and study the Hecke operators and their corresponding Newton Polygons as prime p varies.

Firstly, let's define the generic Newton polygon for prime p to be the lower convex hull of the set of points $P_p = \bigcup_{k=1}^{\infty} P_{p,k}$. Figure 2 shows the graphs of the Newton Polygons for $p = 3, 5, 7$ and 11 respectively, as k varies between 3 and 30. From the graphs, we notice that for $p = 3$, all the vertices lie above the x-axis except the origin, i.e. the length of zero slope is 0, and the length of zero slope increases as p increases.

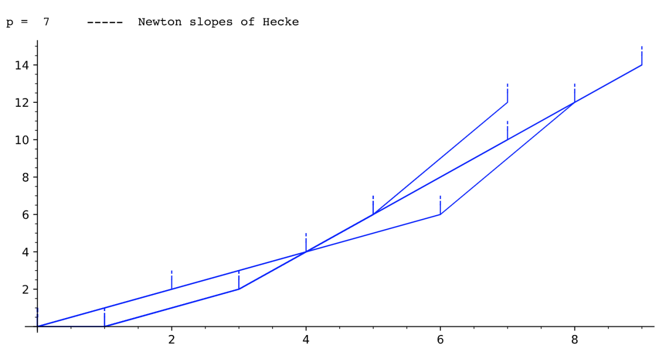
Based on the observation above, can we determine the length of zero slope of the generic Newton polygon under fixed prime p? In other words, can we find the vertex $(i_0, ord_p(c_{i_0}))$ of the generic Newton polygon, such that $ord_p(c_{i_0}) = 0$ and $ord_p(c_j) > 0$ for all $j > i_0$? So far, we are unable to prove a specific vertex works for all k, but the following conjecture can be obtained from the results calculated by Magma (codes in Appendix).



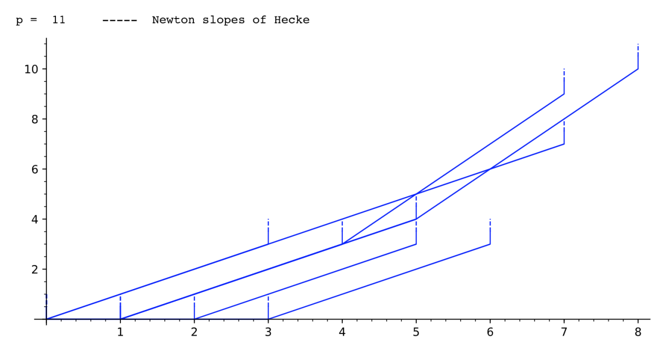
(a) $p = 3$



(b) $p = 5$



(c) $p = 7$



(d) $p = 11$

Figure 2: The Newton Polygons for $p = 3, 5, 7, 11$; $3 \leqslant k \leqslant 30$

Conjecture 2.5. *For congruence subgroup $\Gamma_0(3)$ and prime number $p \geqslant 3$, $(\lfloor \frac{p-2}{3} \rfloor, 0)$ is the length of the zero slope.*

Let's focus on the case $p = 3$. Our conjecture claims that $(0, 0)$ is the only zero point and $ord_3(c_i) > 0$ for all $i \geqslant 1$. It is easy to show that $(0, 0)$ is a vertex of the Newton Polygon. By definition, the Hecke polynomial $H_k(x) = det(I - T_p x)$, where T_p is the p^{th}-Hecke operator. If we expand H_k in powers of x, then the constant term of H_k only comes of the identity matrix I. It follows that the constant terms of H_k must be 1, which is not divisible by 3. Thus, $(0, ord_3(c_0)) = (0, 0)$ for all weight k.

Now let's write $H_k = \sum_{i=0}^{n} c_i x^i$. It suffices to show that for any weight k, c_i is divisible by 3, whenever $i \geqslant 1$. Although it is hard to compute or express the explicit formula of the p^{th}-Hecke operator, from computer calculation, we conjecture that for $p = 3$, the matrix representations of T_p satisfy the properties listed in the following theorem, which implies that Conjecture 2.5 holds for $p = 3$.

Theorem 2.6. *Let M be a $n \times n$ matrix, i.e.*

$$M = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{bmatrix}$$

Suppose M has the following properties:

1. $3 \mid m_{ii}$, *for all* $i = 1, 2, \dots n$.
2. *Let* $l_i = ord_3(i)$. *If* $l_i = 0$, *then* $3 \mid m_{ij}$, *for all* $j = 1, 2, \dots, n$. *If* $l_i \geqslant 1$, *then* $3 \mid m_{ij}$, *for all* $j \not\equiv \frac{i}{3} \pmod{3^{l_i}}$

Then for the polynomial $det(I - Mx) = \sum_{i=0}^{n} c_i x^i$, c_i *is divisible by* 3 *for all* $i \geqslant 1$.

Proof. For any i, the coefficient c_i is determined by the following formula:

$$c_i = (-1)^i \cdot \sum_{\substack{1 \leqslant u_1 < u_2 \cdots < u_i \leqslant n; \\ \sigma \in S_i}} sgn(\sigma) \cdot m_{u_1, \sigma(u_1)} \cdot m_{u_2, \sigma(u_2)} \cdots m_{u_i, \sigma(u_i)},$$

where S_i is the symmetric group $Sym(u_1, u_2 \dots u_i)$ and $sgn(\sigma)$ is the sign of permutation σ.

By the formula above, we know $c_1 = -(m_{11} + m_{22} + \cdots + m_{nn}) = -tr(M)$. Since $3 \mid m_{ii}$ for all i, $3 \mid c_1$.

To show $3 \mid c_2$, it suffices to show that for every $1 \leqslant u_1 < u_2 \leqslant n$ and $\sigma \in S_2$, $3 \mid m_{u_1, \sigma(u_1)} \cdot m_{u_2, \sigma(u_2)}$. It is obvious that S_2 only contains the identity e and the permutation $(u_1 u_2)$, which interchanges u_1 and u_2. If σ is the identity, then $3 \mid m_{u_1, u_1} \cdot m_{u_2, u_2}$ by property 1. So we just need to show that for all $1 \leqslant u_1 < u_2 \leqslant n$, $3 \mid m_{u_1, u_2} \cdot m_{u_2, u_1}$.

Suppose there exists $1 \leqslant u_1 < u_2 \leqslant n$ such that $3 \nmid m_{u_1, u_2} \cdot m_{u_2, u_1}$. Then both m_{u_1, u_2} and m_{u_2, u_1} are not divisible by 3. By property 2, we have $l_{u_1}, l_{u_2} \geqslant 1$. Suppose at least one of l_{u_1} and l_{u_2} are equal to 1. Without loss of generality, we assume $l_{u_1} = 1$. It implies that $3 \mid u_1$ but $9 \nmid u_1$. In order to have $3 \nmid m_{u_1, u_2}$, u_2 must be congruent to $\frac{u_1}{3} \pmod 3$. Since $9 \nmid u_1$, u_2 is congruent to either 1 or 2 (mod 3). Thus $l_{u_2} = 0$, which implies that $3 \mid m_{u_2, u_1}$. Contradiction. Hence, we must have $l_{u_1}, l_{u_2} \geqslant 2$.

Similarly, suppose at least one of l_{u_1} and l_{u_2} are equal to 2. Without loss of generality, assume $l_{u_1} = 2$. Then $9 \mid u_1$ but $27 \nmid u_1$. In order to have $3 \nmid m_{u_1, u_2}$, u_2 must be congruent to $\frac{u_1}{3} \pmod 9$. However, since $l_{u_1} = 2$, l_{u_2} must be less than or equal to 1. It follows that $3 \mid m_{u_2, u_1}$. Hence, we must have $l_{u_1}, l_{u_2} \geqslant 3$.

By continuing this process, we obtain that for all $1 \leqslant u_1 < u_2 \leqslant n$ such that $3 \mid m_{u_1, u_2} \cdot m_{u_2, u_1}$. Therefore, $3 \mid c_2$. The proof of the general case is similar but very technical. So we omit the proof here. One can show that $3 \mid c_i$ for all $i \geqslant 1$ by the similar argument and induction.

□

Also from Figure 2, one may notice that all the Newton polygons are bounded below. Now let's still fix the prime p and consider quadratic lower bounds of the generic Newton polygon. Assuming Conjecture 2.5 holds, we already know two vertices lying on the x-axis, i.e. (0,0) and $(\lfloor \frac{p-2}{3} \rfloor, 0)$. Since a quadratic polynomial can be determined by only 3 points, another interesting question is whether we can find a quadratic lower bound which depends on p and hits the zero points of the generic Newton polygon. Although it is still complicated to prove that a specific polynomial is a lower bound for all weight $k \in \mathbb{N}$, we can at least calculate the first several k's by Magma and obtain the following conjecture.

Conjecture 2.7. *For congruence subgroup* $\Gamma_0(3)$ *and prime number* $p \geqslant 3$, $y = \frac{1}{p-1} x (x - \lfloor \frac{p-2}{3} \rfloor)$ *is a quadratic lower bound of the generic Newton polygon.*

It is easy to check that y hits the zero points (0,0) and $(\lfloor \frac{p-2}{3} \rfloor, 0)$. However, we are just claiming that y is a quadratic lower bound. It may not the "greatest lower bound" which is the lower bound that hits at least 3 vertices on the generic Newton polygon. For example, when $p = 3$, $y = \frac{3}{2} x^2 + \frac{1}{2} x$ is the conjectured greatest lower bound.

2.3 Newton Polygons for other congruence subgroups

In this section, we give more conjectures about the two questions mentioned before: the length of zero slope and quadratic lower bound, but consider Hecke polynomials in different congruence subgroups Γ.

Conjecture 2.8. *For prime $p \geqslant 3$,*

1. *if $\Gamma = \Gamma_1(3)$, then the length of zero slope is $\lfloor \frac{p-2}{3} \rfloor$;*
2. *if $\Gamma = \Gamma_0(4) = \Gamma_1(4)$, then the length of zero slope is $\lfloor \frac{p-2}{2} \rfloor$;*
3. *if $\Gamma = \Gamma_0(5)$, then the length of zero slope is $\lfloor \frac{p+1}{4} \rfloor + \lfloor \frac{p-1}{4} \rfloor$;*
4. *if $\Gamma = \Gamma_1(5)$, then the length of zero slope is $p-2$.*

Conjecture 2.9. *For prime $p \geqslant 3$,*

1. *if $\Gamma = \Gamma_1(3)$, $y = \frac{1}{p-1} x(x - \lfloor \frac{p-2}{3} \rfloor)$ is a quadratic lower bound of the generic Newton polygon.*
2. *if $\Gamma = \Gamma_0(4) = \Gamma_1(4)$, $y = \frac{1}{p+1} x(x - \lfloor \frac{p-2}{2} \rfloor)$ is a quadratic lower bound of the generic Newton polygon.*

3 Appendix

3.1 Magma Code

The following Magma code gives all vertices of Newton polygons for $p = 3$, $\Gamma = \Gamma_1(3)$, as weight k varies from 1 to 100.

```
R<x> := PolynomialRing(Integers());
p := 3;
for k in [1..100] do
   S := CuspForms(Gamma1(3),k);
     P := HeckePolynomial(S,p);
     P := ReciprocalPolynomial(P);
     NP := NewtonPolygon(P,p);
     AllVertices(NP);
end for;
```

The following Magma code determines the divisibility of each entry in the Hecke matrix for $p = 3$, $\Gamma' = \Gamma_0(3)$, as weight k varies from 1 to 100.

```
p:= 3;
for k in [1..100] do
    M:= CuspForms(Gamma0(3),k);
    d:= Dimension(M);
    T:= HeckeOperator(M,p);
    for i in [1..d] do
        for j in [1..d] do
            T[i,j]:= T[i,j] mod p;
        end for;
    end for;
    print k;
    print T;
end for;
```

3.2 Sage Code

The following Sage code plots the graph of Newton polygons for $p = 3$, $\Gamma = \Gamma_1(3)$, as weight k varies from 1 to 30.

```
p = 3
G = Gamma1(3)
N = 30

from sage.geometry.newton_polygon import NewtonPolygon

def hecke_poly(k):
    W = CuspForms(G,k)
    d = W.dimension()
    H = W.hecke_matrix(p)
    I = matrix.identity(d)
    U = I - H*x
    Q = U.determinant()
    return Q
```

```
K = Qp(p)
R.<t> = K[]

print "p = ",p,"    -----  Newton slopes of Hecke"
E = []

for k in [1..N]:
    hecke = hecke_poly(k)
    L = hecke.coefficients(sparse=False)
    p_hecke = R(L)
    NP = p_hecke.newton_slopes()
    NP_half = []
    for i in [0..len(NP)/2-1]:
        NP_half.append(-NP[i])
    NP12 = NewtonPolygon(NP_half).plot()
    E.append(NP12)
sum(E)
```

Here the Hecke operator $U = I - Hx$, since $p = 3$ is divisible by 3. If p doesn't divide 3, then $U = I - Hx + p^{(k-1)}x^2 I$.

References

[1] Wells Johnson, *p-adic proofs of congruences for the Bernoulli numbers*, J. Number Theory **7** (1975), 251–265. MR 0376512

[2] Bernd C. Kellner, *On irregular prime power divisors of the Bernoulli numbers*, Math. Comp. **76** (2007), no. 257, 405–441. MR 2261029

[3] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003

[4] ———, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136