Zeros of p-adic L-functions

Yves Maurer (supervisor: Dr. Kevin Buzzard)

19th of June 2000

Abstract

The project is about calculating zeros of p-adic L-functions with Dirichlet characters. First the p-adic numbers are introduced as a natural completion of the rational numbers. Then classical L-functions are investigated and a result about their values at negative integers is introduced. This is then used to construct the p-adic analogue of classical L-functions.

Using a relatively simple formula, I developed a C program to calculate the zero for a given p. The program was run on the AP3000 Fujitsu supercomputer at Imperial College and calculated the zero to 1000 decimal places. Also included in the report are the zeros of the p-adic L-function for all irregular primes smaller than 500 up to 98 decimal places.

Acknowledgements

First I would like to thank my supervisor, Dr Kevin Buzzard for his support, ideas, inspiration and all the endless discussions. I would also like to thank him for introducing me to Number Theory through his courses.

Furthermore, I would like to thank the Imperial College Parallel Computing Centre and in particular Mr Keith Sephton for providing me with the supercomputer facilities that I needed to achieve such a high accuracy.

Thanks also to the people developing the free PARI mathematical library for C. Without it my programming efforts would have been exponentially larger.

Finally, thanks also go to all my friends who have helped me with ideas and proof-reading of the report.

Contents

Chapter 1

Introduction

This project is about computing the zeros of p-adic L-functions. Before we embark on calculating anything, we first have to understand what p-adic Numbers are and also investigate classical L-functions. P-adic Numbers were introduced by K. Hensel in a 1902 paper entitled 'über die Entwicklung der algebraischen Zahlen in Potenzreihen'. Translated, this means 'The development of algebraic numbers in power series' and that is surely one way to understand them.

Although p-adic fields arose about a hundred years ago, it took some time for them to seep through into standard mathematics. Nowadays, they are not only used in Number Theory, but also have their applications in other fields, like representation theory and algebraic topology.

L-functions arise naturally as a generalisation of the Riemann zeta function. They introduce an extra element into the formulation of the function: a Dirichlet character. The values that these functions take at negative integers have a a very special form in terms of Bernoulli numbers. Instead of working with real numbers, we will work with p-adic Numbers, so that we will consider p-adic analogues of the classical L-functions.

The Riemann Zeta function has many interesting properties and seems to encode in some way a lot of Number Theory. For example the question, *'What is the probability that two integers chosen at random are coprime'* has as answer simply Zeta(2). Using classical L-functions, you can construct class number formulae, which is a striking application. Now the p-adic L-function is a much more algebraic object that has many of these fascinating number-theoretical properties as well.

The importance of p-adic L-functions can be seen in the attempts to

solve the Birch-Swinnerton-Dyer conjecture, which is one of the Millenium Prize Problems (each worth $1 million). The p-adic version of L-functions for elliptic curves have been used to bridge the gap between algebra and analysis in one of the most successfull attacks of the problem.

One of the greatest unsolved problems in Pure Mathematics is the Generalised Riemann Hypothesis, which says that all the non-trivial zeros of an L-function have real part equal to $1/2$. Although it has not been proved yet, it has been verified for the first 200.000 cases [10]. The Riemann Hypothesis was one of the famous 23 problems for the century, announced by D. Hilbert in 1900. As it has still not been resolved, it is also one of the Millenium Prize Problems.

Surprisingly, very little is known about the zeros of the p-adic L-functions. Basing ourselves on a paper by S. Wagstaff [4] we set about computing these zeros, but found soon that a different approach was needed. There is in fact another way to compute them, based on a formula in the book by L.C. Washington [9]. So over the course of the project we will introduce this formula for the p-adic L-function and use it to calculate different zeros. The highest precision achieved up to date is 256 digits for the case $p = 37$ (Sunseri [8]).

Chapter 2

p-adic Numbers

Over the course of this chapter, we will show that any field can be completed with respect to some valuation and that the p-adics are precisely a completion of $\mathbb{Q}$ with respect to the p-adic valuation. This chapter is based on an exercise outlining the main proof in Cassels' book [2]. Some parts are also inspired by K. Mahler's exposition [6].

2.1 Valuations

Definition 2.1.1. *A* valuation *is a function from a field k to the real numbers $\mathbb{R}$ which satisfies the following axioms:*

1. $\forall b \in k$, $|b| \geq 0$, *with* $|b| = 0$ *only if* $b = 0$
2. $\forall b, c \in b$, $|bc| = |b||c|$
3. $\exists\, C \in \mathbb{R}$ *such that for* $b \in k$ *and* $|b| \leq 1$, $|1 + b| \leq C$

Example 2.1.2. *The trivial valuation is defined as follows*

$$|b|_0 = \begin{cases} 0 & \text{if } b = 0 \\ 1 & \text{otherwise} \end{cases}$$

This clearly satisfies all the axioms for a valuation.

Example 2.1.3. *Take the usual absolute value on the real numbers $\mathbb{R}$. It clearly satisfies axioms 1) and 2). If we take $C = 2$, it also satisfies axiom 3). If $|b| \leq 1$ then $-1 \leq b \leq 1$, so $0 \leq 1 + b \leq 2$ and hence $|b + 1| \leq C$.*

Corollary 2.1.4. *1.* $|1| = 1$, *as* $|1^2| = |1|$ *and* $|1^2| = |1||1|$. *But* $|1| \neq 0$, *as* $1 \neq 0$, *so* $|1| = 1$.

2. If $|a^n| = 1$, *then* $|a| = 1$.

3. $|-1| = 1$, *so* $|-a| = |a|$.

4. If k *is a finite field then then there is only the trivial valuation, as* $a^n = 1$ *for some* n, *which means by* (2) *that* $|a| = 1$ *for any* a.

Lemma 2.1.5. *If* $|\ |$ *is a valuation on a field* k *and* λ *is a real number* ≥ 0, *then* $|\ |_1 = |\ |^\lambda$ *is also a valuation.*

Proof. The function $|\ |_1$ clearly satisfies axioms 1 and 2. To satisfy axiom 3, we just take the constant $C_1 = C^\lambda$. □

Definition 2.1.6. *If two valuations are related as in Lemma 2.1.5, then they are said to be equivalent. Equivalence of valuations is easily seen to be an equivalence relation.*

Definition 2.1.7. *The triangle inequality is the following relation:*
$\forall a, b \in k$, $|a + b| \leq |a| + |b|$

Theorem 2.1.8. *A valuation satisfies the triangle inequality if and only if one can take* $C = 2$ *in axiom 3).*

Proof. Part 1
Suppose it satisfies the triangle inequality.
Then if $|b| \leq 1$, we have $|1 + b| \leq |1| + |b|$. Now $|1| + |b| = 1 + |b| \leq 2$. So we can take $C = 2$ in axiom 3).

Part 2
Suppose $C = 2$ satisfies axiom 3.

Take $a_1, a_2 \in k$ with say $|a_1| \geq |a_2|$ and $a_2 = aa_1$ so that $|a| \leq 1$. Then we get

$$|a_1 + a_2| = |a_1(1 + a)| = |a_1||1 + a| \leq 2|a_1|.$$

so for any a_1 and a_2 this means

$$|a_1 + a_2| \leq 2\max\{|a_1|, |a_2|\}.$$

by induction we get for $1 \leq j \leq 2^n$

$$|a_1 + \ldots + a_{2^n}| \leq 2^n \max|a_j|.$$

Now take $a_1, \ldots, a_N$ in k. Set n such that $2^{n-1} < N \leq 2^n$ and define $a_{N+1} = \ldots = a_{2^n} = 0$. From what we showed above, we get

$$|a_1 + \ldots + a_N| \leq 2^n \max|a_j| \leq 2N \max|a_j|.$$

So in particular, if $a_1 = a_2 = \ldots = a_N = 1$, we get for a positive integer N that $|N| \leq 2N$. So take $b, c \in k$ and let n be a positive integer. Then we get

$$\begin{aligned} |b+c|^n &= |(b+c)^n| \\ &= \left| \sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r} \right| \end{aligned}$$

So by what we showed above (as we have $n+1$ terms),

$$\begin{aligned} |b+c|^n &\leq 2(n+1)\max|\binom{n}{r} b^r c^{n-r}| \\ &\leq 2(n+1)\max|\binom{n}{r}||b^r||c^{n-r}| \end{aligned}$$

Now we use the fact that $|N| \leq 2N$ with $N = \binom{n}{r}$

$$|b+c|^n \leq 4(n+1)\max\binom{n}{r}|b|^r|c|^{n-r}$$

The maximum term is smaller than the sum of all terms (as they are ≥ 0)

$$\begin{aligned} |b+c|^n &\leq 4(n+1)\sum_{r=0}^{n}\binom{n}{r}|b|^r|c|^{n-r} \\ &= 4(n+1)(|b|+|c|)^n. \end{aligned}$$

Now take the n-th root and let n tend to infinity to get

$$|b+c| \leq |b| + |c|$$

□

Corollary 2.1.9. *Every valuation is equivalent to one satisfying the triangle inequality*

Proof. Say we have a valuation $||$ with the corresponding constant C. Then we can define the equivalent valuation $||^\lambda$ with $\lambda = \frac{\log 2}{\log C}$ whose constant is $C^{\frac{\log 2}{\log C}} = 2$. □

2.2 Field Completions

Definition 2.2.1. *Let k be a field with valuation $||$. Then a sequence $\{a_n\} = \{a_1, a_2, \dots\}$ is said to tend to b as a limit (with respect to the valuation) if for every $\epsilon > 0$, there exists an $n_0(\epsilon)$ such that $|a_n - b| < \epsilon$ for all $n > n_0(\epsilon)$.*

Example 2.2.2. *Take the sequence $\{1, 1+\frac{1}{2}, 1+\frac{1}{2}+\frac{1}{2^2}, \dots$ in the rationals. It tends to the limit $\frac{1}{1-\frac{1}{2}} = 2$ as if we fix ϵ, then we can take $n_0(\epsilon) = \frac{\log \epsilon}{\log \frac{1}{2}}$. In general, the limit of a sequence is clearly unique (If there were two limits $b \neq b'$, then take $\epsilon = \frac{|b-b'|)}{3}$, for example).*

Definition 2.2.3. *For a constant sequence, we write $\{a, a, a, \dots\} = S(a)$.*

Definition 2.2.4. *Let k be a field with valuation $||$. Then a sequence is said to be* fundamental *if for every $\epsilon > 0$, there exists an $n_1(\epsilon)$ such that $|a_m - a_n| < \epsilon$ for all $m, n > n_1(\epsilon)$. Another term for a fundamental sequence is a* Cauchy sequence.

Example 2.2.5. *Take for example the sequence $\{1, 1+1, 1+1+\frac{1}{2!}, 1+1+\frac{1}{2!}+\frac{1}{3!}, \dots\}$ in the rationals. This is just the sequence of successive approximations to the power series of e^x, evaluated at 1. This sequence is fundamental, as if $m > n$, then we can use the following inequality to get some n_1 for any $\epsilon > 0$.*

$$\begin{aligned} a_m - a_n &= \frac{1}{n!} + \ldots + \frac{1}{m!} \\ &= \frac{(m-n)! + (m-n-1)! + \ldots + 1}{m!} \\ &< \frac{m(m-n)!}{m!} \\ &= \frac{(m-n)!}{(m-1)!} \\ &\leq \frac{1}{m-1} \text{ for } n > 1. \end{aligned}$$

So for any $\epsilon > 0$, we can choose $n_1(\epsilon) = max\{\frac{1+\epsilon}{\epsilon}, 1\}$. So the series converges, but it does not have a limit in the rationals. Its limit in the reals is e. So there exist sequences, which are fundamental in some field k and do not have a limit in k.

Lemma 2.2.6. *A fundamental sequence is bounded by some constant $C > 0$. In other words, there exists $C > 0$ such that $|a_n| \leq C$ for all n.*

Proof. Fix $\epsilon > 0$ and let $q = n_1(\epsilon)$ as in Definition 2.2.4. Then for all $n > q$, we have

$$\begin{aligned} |a_n| &= |a_q + (a_n - a_q)| \\ &\leq |a_q||a_n - a_q| \\ &\leq |a_q| + \epsilon \\ &= C_1 \text{ say} \end{aligned}$$

So C_1 only depends on the sequence $\{a_n\}$ and on ϵ. So we can define the constant C required by lemma as follows

$$|a_n| \leq \max(|a_1|, \ldots, |a_{q-1}|, C_1) = C.$$

□

Definition 2.2.7. *The field k is* complete *with respect to the valuation $||$ if every fundamental sequence has a limit.*

Definition 2.2.8. *Let k be a field with valuation $||$. Then a field K is a completion of k with respect to $||$ if K is complete and there exists an isomorphism from k onto a subfield of K and k is dense in K (i.e. elements of K can be arbitrarily closely approximated by elements of k).*

An isomorphism is a bijective function $\phi(x)$ such that $\phi(xy) = \phi(x)\phi(y)$ and $\phi(x+y) = \phi(x) + \phi(y)$.

Now we will set about to prove that for any field k with some valuation, there exists a completion of k. The proof will be broken up into several steps. First, we will show that the set of fundamental sequences can be given a ring structure. Then we will define new elements which are not part of k by setting them to limits of fundamental sequences. After taking care of null sequences, we will finally define the field K, which is the completion of k.

Lemma 2.2.9. *The set F of fundamental sequences is a ring under the following definitions.*

1. $\{a_n\} + \{b_n\} = \{a_n + b_n\}$
2. $\{a_n\} - \{b_n\} = \{a_n - b_n\}$
3. $\{a_n\} \times \{b_n\} = \{a_n \times b_n\}$

Proof. As we have shown before that every valuation is equivalent to one satisfying the triangle inequality, we can assume with loss of generality that $||$ does satisfy the triangle inequality.

Let us first show closure for the operations. For addition, we get the following argument.

Fix some $\epsilon > 0$. As $\{a_n\}, \{b_n\}$ are fundamental sequences, for every $\frac{\epsilon}{2}$, there exist n_a, n_b such that $|a_m - a_n| < \frac{\epsilon}{2}$ for every $m, n > n_a$ and $|b_m - b_n| < \frac{\epsilon}{2}$ for every $m, n > n_b$. So take $n_1 = \max(n_a, n_b)$. Then for every $m, n > n_1$, we get

$$\begin{aligned} |(a_m + b_m) - (a_n + b_n)| &\leq |a_m + b_m| + |a_n + b_n| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= \epsilon \end{aligned}$$

For subtraction, the proof is exactly the same. So let us do multiplication now. As we have seen in Lemma 2.2.6, there exist $C_1 > 0$ and $C_2 > 0$ such

that $|a_n| \leq C_1$ and $|b_n| \leq C_2$. Now fix some $\epsilon > 0$. As $\{a_n\}$ is a fundamental sequence, there exists an integer n_1 such that $|a_m - a_n| < \frac{\epsilon}{2C_2}$ for all $n, m \geq n_1$. Similarly, there exists n_2 such that $|b_m - b_n| < \frac{\epsilon}{2C_1}$ for all $n, m \geq n_2$. So we get

$$\begin{aligned}
|a_m b_m - a_n b_n| &= |a_m(b_m - b_n) + (a_m - a_n)b_n| \\
&\leq |a_m||b_m - b_n| + |a_m - a_n||b_n| \\
&\leq C_1|b_m - b_n| + C_2|a_m - a_n| \\
&\leq C_1\frac{\epsilon}{2C_1} + C_2\frac{\epsilon}{2C_2} \\
&= \epsilon.
\end{aligned}$$

The remaining ring axioms are directly derived from the corresponding properties of the field k. So $+$ and $\times$ are associative, commutative and distributive. The additive and the multiplicative identity are

$$S(0) = \{0, 0, 0, \dots\}$$

$$S(1) = \{1, 1, 1, \dots\}$$

□

Note that F as defined in Lemma 2.2.9 is not a field, as it has zero divisors. For example $\{2, 0, 0, 0, \dots\} \times \{0, 1, 0, 0, \dots\} = S(0)$ but neither of the two terms is zero. So we have to take care of these zero divisors. First we have to prove a technical lemma about these sequences which tend to 0.

Lemma 2.2.10. *Let $\{a_n\}$ be a sequence which does not tend to 0, then there exists an integer n_2 and $r > 0$ such that*

$$|a_n| \geq r \text{ for all } n > n_2.$$

Proof. We will prove it by contradiction. So suppose that on the contrary for every $\epsilon > 0$ and for every integer n_2, there exists an n such that

$$|a_n| < \frac{1}{2}\epsilon$$

Now, as $\{a_n\}$ is a fundamental sequence, there exists $n_1(\frac{1}{2}\epsilon)$, such that

$$|a_m - a_n| < \frac{1}{2}\epsilon \text{ for all } m, n > n_1(\frac{1}{2}\epsilon).$$

So, if $m \geq n_1(\frac{1}{2}\epsilon)$, there exists an $n \geq n_1(\frac{1}{2}\epsilon)$ such that

$$\begin{aligned} |a_m - 0| &= |a_n + (a_m - a_n)| \\ &\leq |a_n||a_m - a_n| \\ &\leq \frac{1}{2}\epsilon + \frac{1}{2}\epsilon \\ &= \epsilon \end{aligned}$$

In other words, $\{a_n\}$ tends to 0, which contradicts our hypothesis. So there exist $r > 0$ and n_2 as required by the lemma. □

Proposition 2.2.11. *Let N be the set of sequences in F with limit 0. Then N is a maximal ideal of F.*

Proof. To prove that N is a maximal ideal of F, we will first prove that N is a prime ideal. A prime ideal satisfies the conditions

1. N is closed under addition and multiplication.
2. If $\{a_n\} \in N$ and $\{b_n\} \in F$, then $\{a_n\}\{b_n\} \in N$.
3. If $\{a_n\}\{b_n\} \in N$ then $\{a_n\} \in N$ or $\{b_n\} \in N$.

Let us first prove closure under addition. It is pretty much the same proof as for closure of F. If $\{a_n\}, \{b_n\} \in N$, then for every $\frac{\epsilon}{2}$, there exist n_1, n_2 such that $|a_n| < \frac{\epsilon}{2}$ for every $n > n_1$ and similarly for $\{b_n\}$. So if $m = \max(n_1, n_2)$, then for every $n > m$ we get

$$|a_n + b_n| \leq |a_n| + |b_n| = \epsilon$$

We will prove closure under multiplication and part 2) together now. So say that $\{a_n\} \in N$ and $\{b_n\} \in F$. So as $\{b_n\}$ is a fundamental sequence, we can find $C > 0$ such that $|b_n| < C$ by Lemma 2.2.6. Moreover, for every $\frac{\epsilon}{C} > 0$, there exists an m such that $|a_n| < \frac{\epsilon}{C}$ for every $n > m$. So finally, we get

$$\begin{aligned} |a_n b_n| &= |a_n||b_n| \\ &\leq |a_n|C \\ &\leq \frac{\epsilon}{C}C \\ &= \epsilon. \end{aligned}$$

For number 3), we just prove that if two sequences do not tend to zero, then their product does not either. So say that $\{a_n\}$ and $\{b_n\}$ do not tend to 0. By Lemma 2.2.10, there exist N, N', r, r' such that

$$|a_n| \geq r \text{ for all } n > N$$
$$|b_n| \geq r' \text{ for all } n > N'$$

So let $M = \max(N, N')$ and get

$$|a_n b_n| = |a_n||b_n| \geq rr' > 0 \text{ for } n \geq M$$

Hence $\{a_n b_n\}$ does not tend to 0.

So we conclude that if $\{a_n\}\{b_n\} \in N$ then $\{a_n\} \in N$ or $\{b_n\} \in N$.

So N satisfies the three axioms and is a prime ideal of F. In order to prove that N is maximal, we need to prove that if there is an ideal J containing N and bigger than N, then $J = F$. So suppose $\{a_n\} \in J$ such that $\{a_n\}$ does not belong to N, so it does not tend to 0. Then we can construct an inverse for $\{a_n\}$ as follows.

As $\{a_n\}$ does not tend to 0, we get by Lemma 2.2.10 that there exist n_2 and $r > 0$ such that

$$|a_n| \geq r \text{ for all } n > n_2.$$

So construct a new sequence $\{b_n\}$ as

$$b_n = \begin{cases} 0 & \text{if } 1 \leq n \leq n_2 - 1 \\ \frac{1}{a_n} & \text{if } n \geq n_2 \end{cases}$$

Then $\{b_n\}$ is a fundamental sequence, as if we fix $\epsilon > 0$, there exists $n_o(r^2\epsilon)$ such that for all $m, n > n_0(r^2\epsilon)$, we have

$$|a_m - a_n| < r^2\epsilon \text{ for all } m, n > n_0(r^2\epsilon).$$

So we get for all $m, n > \max(n_0(r^2\epsilon), n_2)$,

$$\begin{aligned}|b_m - b_n| &= |\frac{1}{a_m} - \frac{1}{a_n}| \\ &= \frac{|a_n - a_m|}{|a_n||a_m|} \\ &\leq \frac{1}{r^2}|a_m - a_n| \\ &= \frac{1}{r^2}r^2\epsilon \\ &= \epsilon.\end{aligned}$$

Now this sequence $\{b_n\}$ is indeed an inverse of $\{a_n\}$, as

$$\{a_n\}\{b_n\} = \{0, \dots, 0, 1, 1, 1, \dots\}$$

where we have n_2 zeros in the beginning. $\{0, \dots, 0, 1, 1, 1, \dots\}$ is in the same equivalence class mod N as $S(1)$, as they only differ by the sequence $\{1, \dots, 1, 0, 0, 0, \dots\}$, which tends to 0.

So $S(1) \in J$ and hence $J = F$, so that N is maximal. □

Corollary 2.2.12. *The structure K defined by $K = \frac{F}{N}$ is a field.*

Proof. As the ideal N is maximal, the ring of equivalence classes modulo N is a field and hence the result. □

So now we have constructed our bigger field K. What we are left to do is to see whether this field is indeed complete and whether there exists an isomorphism from k onto a subfield of K. Let us start with the second bit.

Lemma 2.2.13. *The function*

$$\begin{aligned}\phi : k &\to K \\ x &\mapsto \{x\} + N\end{aligned}$$

defines an isomorphism from k onto a subfield of K.

Proof. First note that if $x \neq y \in k$ then $\phi(x) \neq \phi(y)$, as $\{x - y\}$ is not a null sequence. As K is a field and by definition of addition and multiplication in F (and so in K), we get that if $x, y \in k$ then

$$\begin{aligned}\phi(x + y) &= \{x + y\} + N = \{x\} + \{y\} + N = \phi(x) + \phi(y) \\ \phi(xy) &= \{xy\} + N = \{x\}\{y\} + N = \phi(x)\phi(y)\end{aligned}$$

So ϕ is a homomorphism. The image of ϕ in K is the set $I = \{\{a\}+N | a \in k\}$. It is easy to see that ϕ is an isomorphism, as its inverse can be defined as follows

$$\begin{aligned} \phi^{-1} : I &\to k \\ \{x\} + N &\mapsto x \end{aligned}$$

Finally, it follows from k being a field, that I is a field. □

So now we are left with proving that K is complete. In order to do that, we first have to extend our valuation to K.

Lemma 2.2.14. *Take $\{a_n\} + N \in K$ such that $\{a_n\}$ converges to a in k, then*

$$|a| = \lim_{n\to\infty} |a_n|.$$

Proof. First we note that since $\{a_n\}$ converges to a, for every $\epsilon > 0$, there exists an $n_0(\epsilon)$ such that $|a_n - a| < \epsilon$ for all $n > n_0(\epsilon)$. This is just the definition of a limit, so we can write in shorter notation

$$\lim_{n\to\infty} |a_n - a| = 0$$

Now for any $x, y \in k$, we have

$$\begin{aligned} |x| &= |y + (x - y)| \\ &\leq |y| + |x - y|. \end{aligned}$$

Similarly, we get $|y| < |x| + |y - x|$. As $|x - y| = |y - x|$, this means that

$$|x - y| \geq \begin{cases} |x| - |y| \\ |y| - |x| \end{cases}.$$

So if $|\ |_\infty$ denotes the usual absolute value on the real numbers,

$$||x| - |y||_\infty \leq |x - y|.$$

This all implies that $\{|a_n|\}$ is a fundamental sequence in $\mathbb{R}$, as $\{a_n\}$ is a fundamental sequence, so for each $\epsilon > 0$, there exists an n_1 such that for all $n, m > n_1$,

$$||a_n| - |a_m||_\infty \leq |a_n - a_m| < \epsilon.$$

Now, we have to assume the real numbers are complete so that the limit of $|a_n|$ as n tends to infinity exists. As I do not try to construct the real numbers, but rather the p-adic numbers in this project, this is fine. So assuimg this limit exists, we get the following argument.

Since $|a_n| = |a + (a_n - a)| \leq |a| + |a_n - a|$, we get

$$\lim_{n\to\infty} |a_n| \leq |a|.$$

We have as well $|a| = |a_n - (a_n - a)| \leq |a_n| + |a_n - a|$, so

$$|a| \leq \lim_{n\to\infty} |a_n|.$$

So finally,

$$\lim_{n\to\infty} |a_n| = |a|.$$

□

Lemma 2.2.15. *The function* $\| \|$ *defined as*

$$\begin{aligned} \| \| : K &\to \mathbb{R} \\ \{a_n\} + N &\mapsto \lim_{n\to\infty} |a_n| \end{aligned}$$

is a valuation on K.

Proof. So we have to prove that the three axioms in the definition of a valuation hold (from Definition 2.1.1). Take two elements of K, $\{a_n\} + N = A$ and $\{b_n\} = B$. Then

$$\|A\| = \lim_{n\to\infty} |a_n| \geq 0$$

as all the $|a_n| \geq 0$. Now say that $\|A\| = 0$. Then

$$\lim_{n\to\infty} |a_n| = 0$$

so $\{a_n\}$ converges to 0 and so $\{a_n\} \in N$. Hence $A = 0_K = \{0\} + N$. So the first axiom is satisfied. For axiom 2), we have to prove

$$\|AB\| = \|A\|\|B\|$$

Now, we have

$$\begin{aligned}\|AB\| &= \lim_{n\to\infty} |a_n b_n| \\ &= \lim_{n\to\infty} |a_n||b_n|. \\ &= \lim_{n\to\infty} |a_n| \lim_{n\to\infty} |b_n|\end{aligned}$$

as both $\{|a_n|\}$ and $\{|b_n|\}$ converge in $\mathbb{R}$

$$= \|A\|\|B\|.$$

Now for axiom 3), we can take $C = 2$ as we have assumed that $|\ |$ satisfies the triangle inequality. So assuming

$$\|A\| = \lim_{n\to\infty} |a_n| \leq 1$$

we get

$$\begin{aligned}\|A + 1\| &= \lim_{n\to\infty} |a_n + 1| \\ &\leq \lim_{n\to\infty} (|a_n| + |1|) \\ &= 1 + \lim_{n\to\infty} |a_n| \\ &\leq 2.\end{aligned}$$

So $\|\ \|$ is a valuation. □

So the only thing that we still have to be prove is that K is complete with respect to the valuation $\|\ \|$. Before doing that, we will show that elements in K can be approximated arbitrarily closely by elements of k.

Lemma 2.2.16. *If $A \in K$, then A can be approximated arbitrarily closely by elements of k.*

Proof. Let $A = \{a_n\} + N$ and fix $\epsilon > 0$. As $\{a_n\}$ is a fundamental sequence, there exists w such that $|a_m - a_n| < \epsilon$ for every $m, n \geq w$. So

$$\begin{aligned}\|A - (S(a_w) + N)\| &= \|\{a_n - a_w\} + N\| \\ &= \lim_{n\to\infty} |a_n - a_w| \\ &\leq \lim_{n\to\infty} \epsilon \\ &= \epsilon.\end{aligned}$$

So the element $S(a_w) + N$ is arbitrarily close to A. As $a_w \in k$, we can say with a slight abuse of language that a_w is arbitrarily close to A. □

Theorem 2.2.17. *The field K is complete*

Proof. Let $\{A_n\}$ be a fundamental sequence in K. In other words, for each $\epsilon > 0$, there exists n_1 such that $\|A_m - A_n\| < \epsilon$ for all $m, n > n_1$. We will now construct a limit of $\{A_n\}$ which belongs to K.

Write $A_n = \{a_{n,m}\} + N$. By Lemma 2.2.16 there exists for every integer $n > 0$, an integer $w(n)$ such that

$$\|A_n - (S(a_{w(n)}) + N)\| < \frac{1}{n}$$

The sequence $\{A_n - (S(a_{w(n)}) + N)\}$ therefore tends to 0 in K. So it is a fundamental sequence. As $\{A_n\}$ is also a fundamental sequence,

$$\begin{aligned}\{A_n\} - \{A_n - (S(a_{w(n)}) + N)\} &= \{S(a_{w(n)}) + N\} \\ &= \{A\} \text{ say.}\end{aligned}$$

is also a fundamental sequence with terms $A, A, \ldots$. So its limit is $A \in K$. So every fundamental sequence in K has a limit in K and K is complete. □

2.3 p-adic Numbers

After having done all the technical things we needed to know about field completions, we can finally introduce the magical p-adic numbers. As you have probably guessed already, they are a completion of the rational numbers. In fact it can be proved that every non-trivial valuation on the rationals is equivalent to either the ordinary absolute value (in which case the completion is $\mathbb{R}$), or the p-adic valuation defined below. So in that sense, the p-adic numbers are just as important as the real numbers, and you can do pretty much everything with the p-adics that you can do with the real numbers. Note that for this construction to work, p has to be a prime. So for the remainder of the chapter, let p be a prime.

Definition 2.3.1. *Fix a prime p. Define the p-adic valuation on the field $\mathbb{Q}$ as follows. If $q \in \mathbb{Q} \setminus \{0\}$, then we can write by unique factorisation in $\mathbb{Z}$,*

$q = \frac{p^s u}{v}$ where $s \in \mathbb{Z}$ and $p \nmid u \in \mathbb{Z}$ and $p \nmid v \in \mathbb{Z}$. Then the p-adic valuation of q is

$$|q|_p = p^{-s}$$

and $|0|_p = 0$.

From now onwards, $|\ |$ will always stand for the p-adic valuation, unless specifically stated otherwise.

Lemma 2.3.2. *The function $|\ |_p$ is in fact a valuation*

Proof. So we have to prove the three axioms from Definition 2.1.1.

1. If $q \neq 0$ then $p^{-s} > 0$ and $|0| = 0$ as required.

2. For $q, r \in \mathbb{Q}$, $|q| = p^{-s}$ say and $|r| = p^{-t}$ say, then clearly $|qr| = p^{-(s+t)} = |q||r|$

3. Instead of proving it in the form as it is in the definition, we will prove that $|q + r| \leq \max(|q|, |r|)$, which is a stronger version of the triangle inequality and is called the *ultrametric inequality*. So by Theorem 2.1.8, it will be a valuation.

   Take $r, q \in \mathbb{Q}$. Assume with loss of generality that $|r| \geq |q| > 0$. Write $r = \frac{p^s u}{v}$ and $q = \frac{p^t x}{y}$ with $s, u, v, t, x, y \in \mathbb{Z}$ and $p \nmid uvxy$. Let $t - s = a$, so $a \geq 0$. Then

   $$r + q = \frac{p^s U}{V}$$

   where $V = vy \in \mathbb{Z}$ and $U = uy + p^a vx \in \mathbb{Z}$. Clearly, $p \nmid V$, but it is very well possible that $p|U$. So say that $U = p^b W$ with $b \geq 0$ and $p \nmid W$. Then

   $$|r + q| = p^{-(s+b)} \leq p^{-s} = \max(|r|, |q|)$$

□

Definition 2.3.3. *If a valuation satisfies the ultrametric inequality*

$$|q + r| \leq max(|q|, |r|)$$

then it is said to be non-archimedean.

Corollary 2.3.4. *If the valuation $||$ is non-archimedean, then the following hold*

1. $|a_1 + a_2 + \ldots + a_n| \leq max|a_j|$
2. $|a_n - a_1| \leq max|a_{j+1} - a_j|$

Proof. Part 1) is easily proved by induction on n using the definition. Part 2) is obtained by replacing a_j with $a_{j+1} - a_j$. □

Definition 2.3.5. *The p-adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to the p-adic valuation. The p-adic integers $\mathbb{Z}_p$ are a subring of $\mathbb{Q}_p$, with $\mathbb{Z}_p = \{a \text{ such that } a \in \mathbb{Q}_p \text{ and } |a| \leq 1\}$. Define ψ as the following subset of $\mathbb{Z}_p$: $\mathfrak{M} = \{a \text{ such that } a \in \mathbb{Q}_p \text{ and } |a| < 1\}$.*

Note that it is obvious that $\mathbb{Z}_p$ is a subring, as the ultrametric inequality holds.

Corollary 2.3.6. *The set $\mathfrak{M}$ is a maximal ideal of $\mathbb{Z}_p$.*

Proof. It is again easy to see by the ultrametric inequality that $\mathfrak{M}$ is an ideal. Now, if $|a| = 1$ belongs to an ideal bigger than $\mathfrak{M}$, then by definition of the p-adic valuation $|a^{-1}| = 1$ too, so $a^{-1} \in \mathbb{Z}_p$ and so the bigger ideal is just $\mathbb{Z}_p$. □

We still do not really know though what these p-adic numbers look like, so now we will introduce step by step a way to write down p-adic numbers.

Definition 2.3.7. *A valuation is* discrete *if there exists some real number $\epsilon > 0$ such that $1 - \epsilon < |a| < 1 + \epsilon \Rightarrow |a| = 1$.*

Lemma 2.3.8. *The p-adic valuation is discrete*

Proof. We can pick $\epsilon = \frac{1}{p}$. Now $|a| = p^{-s}$ for some integer s, so we have

$$1 - \frac{1}{p} < p^{-s} < 1 + \frac{1}{p}.$$

But this implies that

$$\frac{p-1}{p} < p^{-s} \Rightarrow s \leq 0$$

$$p^{-s} < \frac{p+1}{p} \Rightarrow s \geq 0.$$

So $s = 0$ and $|a| = 1$. □

Lemma 2.3.9. *The ideal $\mathfrak{M}$ is principal.*

Proof. As the p-adic valuation is discrete, the set $\{|a| : |a| < 1\}$ has an upper bound. From the definition of the p-adic valuation, we see that $|a| \leq \frac{1}{p}$ with equality for example when $a = p$. So if $|a| < 1$ then $a = pb$ for some b with $|b| \leq 1$ (so $b \in \mathbb{Z}_p$). So $\mathfrak{M}$ is a principal ideal. □

Lemma 2.3.10. *The quotient ring $\mathbb{Z}_p/\mathfrak{M}$ is isomorphic to*

$$(\mathbb{Z}/p\mathbb{Z}) = \{0, 1, \ldots, p-1\}.$$

Proof. First note that $\mathbb{Z}_p/\mathfrak{M}$ is in fact a field, as the ideal $\mathfrak{M}$ is maximal. Now define the sets

$$\alpha = \{a | a \in \mathbb{Q} \text{ and } |a| \leq 1\} \text{ and } \beta = \{a | a \in \mathbb{Q} \text{ and } |a| < 1\}.$$

Then α is clearly a ring and β an ideal of α. We will prove that $\mathbb{Z}_p/\mathfrak{M}$ is isomorphic to α/β. Clearly, $\mathbb{Z}_p \cap \mathbb{Q} = \alpha$ and $\mathfrak{M} \cap \mathbb{Q} = \beta$, so we can construct the natural map

$$\begin{aligned} \phi : \alpha/\beta &\to \mathbb{Z}_p/\mathfrak{M} \\ a + \beta &\mapsto a + \mathfrak{M} \end{aligned}$$

It is a homomorphism, as $\mathbb{Z}_p \cap \mathbb{Q} = \alpha$ and $\mathfrak{M} \cap \mathbb{Q} = \beta$, so we only need to prove that it is onto. Take any $b \in \mathbb{Z}_p$, then there exists $a \in \mathbb{Q}$ such that $|b - a| < 1$, by Lemma 2.2.16 as $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$. As $||$ is non-archimedean, $a \in \alpha$. Moreover $b - a \in \mathfrak{M}$, so that in $\mathbb{Z}_p/\mathfrak{M}$ we have $b + \mathfrak{M} = a + \mathfrak{M}$. So ϕ is an isomorphism.

Now what is a set of representatives in α/β ? Take some $q = \frac{p^s u}{v} \in \mathbb{Q}$ with $|q| \leq 1$. Then $s \geq 0$. If $s \geq 1$, then $q \in \beta$, so let us say that $s = 0$. so

$$q = \frac{u}{v}$$

$$vq = u$$

$$vq \equiv u (\text{mod } p)$$

As $p \nmid v$ and $p \nmid u$, there exists a such that

$$q \equiv a (\text{mod } p).$$

As furthermore any number in $\{1, \ldots, p-1\}$ has valuation 1 and if we use 0 to represent the class $0 + \beta$, we have shown that

$$\alpha/\beta \cong (\mathbb{Z}/p\mathbb{Z}).$$

□

Definition 2.3.11. *We say that the infinite sum*

$$\sum_{n=0}^{\infty} a_n$$

where a_n belongs to some field, converges to s *, if*

$$s = \lim_{N\to\infty} s_N \text{ with } s_N = \sum_{n=0}^{N} a_n.$$

Proposition 2.3.12. *Suppose we work in a complete field with a non-archimedean valuation. Then the infinite sum $\sum_{n=0}^{\infty} a_n$ converges if and only if $a_n \to 0$ when $n \to \infty$.*

Proof. Part 1) Suppose that $\sum_{n=0}^{\infty} a_n$ converges. Then

$$\begin{aligned}\lim_{N\to\infty} a_N &= \lim_{N\to\infty} (s_N - s_{N-1}) \\ &= \lim_{N\to\infty} s_N - \lim_{N\to\infty} s_{N-1} \\ &= s - s \\ &= 0.\end{aligned}$$

Part 2) Suppose that $a_n \to 0$ when $n \to 0$. Fix some $\epsilon > 0$, then there exists N_0 such that $|a_n| < \epsilon$ for all $n > N_0$. Let $M > N > N_0$, then

$$\begin{aligned}|s_M - s_N| &= |a_{N+1} + \ldots + a_M| \\ &\leq \max_{N<n\leq M} |a_n| \\ &< \epsilon.\end{aligned}$$

So $\{s_N\}$ is a fundamental sequence and converges as the field is complete. □

Note that this fact is not true for general valuations. In the real numbers for example, it is very well possible to construct an infinite sum whose terms tend to zero, but which goes off to infinity. For example, it is well known that

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots = \infty$$

But as the p-adic norm is non-archimedean, nothing like that can happen in the p-adic numbers. Now we have all the tools we need to be able to construct a useful notation for the p-adics.

Lemma 2.3.13. *Consider $a \in \mathbb{Z}_p$, then a can be written uniquely in the form*

$$a = \sum_{n=0}^{\infty} a_n p^n \ , \ \textit{with } a_n \in \{0, \ldots, p-1\}$$

Conversely, the right hand side always converges to an element $a \in \mathbb{Z}_p$.

Proof. The proof of the converse is easy by Proposition 2.3.12. As $|a_n p^n| = p^{-n}$, the sequence $\{a_n p^n\}$ tends to 0 as n tends to infinity, and the term with the highest norm is $a_0 p^0$ with norm 1, so it belongs to $\mathbb{Z}_p$.

Now prove the other way. Let $a \in \mathbb{Z}_p$ be given. Then there is precisely one $a_0 \in \{0, \ldots, p-1\}$ such that $|a - a_0| < 1$ by Lemma 2.3.10. So $a = a_0 + pb_1$ for some $b_1 \in \mathbb{Z}_p$. Then there is exactly one $a_1 \in \{0, \ldots, p-1\}$ such that $|b_1 - a_1| < 1$ and $b_1 = a_1 + pb_2$ for some $b_2 \in \mathbb{Z}_p$. Do this step N times to get

$$a = a_0 + a_1 p + a_2 p^2 + \ldots + a_N p^N + b_{N+1} p^{N+1}$$

with $a_i \in \{0, \ldots, p-1\}$ and $b_{N+1} \in \mathbb{Z}_p$. Now, as

$$\lim_{N \to \infty} |b_{N+1} p^{N+1}| = 0.$$

we have indeed

$$a = \sum_{n=0}^{\infty} a_n p^n.$$

□

Example 2.3.14. *Take for example the integer 7 and say we work in the 5-adic numbers. Now $|7|_5 = 1$, as 5 does not divide 7. So there exists exactly one $a_0 \in \{0, 1, 2, 3, 4\}$ such that $|7 - a_0|_5 < 1$. This is of course $a_0 = 2$. So $7 = 2 + 5 \times 1$. Now $|1|_5 = 1$, so there is $a_1 = 1$ such that $|1 - a_1|_5 < 1$ and $1 = 1 + 0 \times 5$. As $|0|_5 = 0$, we can stop here and get the following expression for 7 in the 5-adcis*

$$7 = 2 + 1 \times 5.$$

Example 2.3.15. *Now take a more complicated example. Take for example $\frac{1}{3}$ in the 5-adics. Now $|\frac{1}{3}|_5 = 1$ and so there exists exactly one $a_0 \in \{0, 1, 2, 3, 4\}$ such that $|\frac{1}{3} - a_0|_5 < 1$. So we have to find a_0 such that $1 - 3a_0$ is divisible by 5. So we solve the congruence*

$$\begin{aligned} 1 - 3a_0 &\equiv 0 && (mod\ 5) \\ -3a_0 &\equiv -1 && (mod\ 5) \\ 3a_0 &\equiv 1 && (mod\ 5) \\ a_0 &\equiv 2 && (mod\ 5) \end{aligned}$$

So $\frac{1}{3} = 2 + 5\frac{-1}{3}$ *and* $|\frac{-1}{3}|_5 = 1$. *So there exists* a_1 *such that* $|\frac{-1}{3} - a_1|_5 < 1$. *So we solve the congruence*

$$\begin{aligned} 1 + 3a_0 &\equiv 0 && (mod\ 5) \\ 3a_0 &\equiv 4 && (mod\ 5) \\ a_0 &\equiv 3 && (mod\ 5) \end{aligned}$$

So $\frac{-1}{3} = 3 + 5\frac{-2}{3}$. *Now there exists* a_2 *such that* $|\frac{-2}{3} - a_2|_5 < 1$. *We see that* $a_2 = 1$ *satisfies this. So* $\frac{-2}{3} = 1 + 5\frac{-1}{3}$. *But we already know that* $\frac{-1}{3} = 3 + 5\frac{-2}{3}$. *So from here onwards, we will only repeat* $3, 1, 3, 1, \ldots$. *So the expression for* $\frac{1}{3}$ *in the* 5*-adics is*

$$\frac{1}{3} = 2 + 3 \times 5 + 1 \times 5^2 + 3 \times 5^3 + 1 \times 5^4 + \ldots$$

Now we can extend Lemma 2.3.13 so that we can write down elements of $\mathbb{Q}_p$ as well.

Corollary 2.3.16. *Every* $a \in \mathbb{Q}_p \setminus \{0\}$ *is of the form*

$$a = \sum_{n=N}^{\infty} a_n p^n \text{ with } a_n \in \{0, 1, \ldots, p-1\} \text{ and } a_N \neq 0.$$

Proof. First, note that elements of $\mathbb{Q}_p \setminus \{0\}$ also have valuation equal to p^{-s} for some s, as the valuation is discrete. Then if $a \in \mathbb{Q}_p \setminus \{0\}$, then there exists some N such that $p^{-N}a \in \mathbb{Z}_p$, as if $|a| = p^{-s}$ then $N = s$ and $|p^{-N}a| = p^{-s+N} = 1$. □

So now we have a convenient way to write down p-adic numbers. We can relate this notation to the decimal notation for real numbers. In the reals, we have for example

$$\frac{1}{3} = 0.333333\ldots$$

In the p-adics we can write along the same lines

$$\frac{1}{3} = \ldots 31313132$$

The p-adics are written from the right to the left, as 2 is the digit corresponding to 5^0, the first 3 from the right corresponds to 5^1, ... In the results from the computation of the zero of the p-adic L-function, we use a different format of presentation though. They are presented in a table starting with the coefficient of p^0.

Now we will introduce some standard theorems about p-adic analysis that we will need later. First we will start off with a version of Hensel's Lemma, which is a generic term used for inferring the existence of a solution of an equation from the existence of an approximate solution. The version given here is analogous to Newton's method for the real numbers. Before doing that, we need to know something about derivatives of polynomials in $\mathbb{Z}_p[x]$.

Definition 2.3.17. *Let $f(x) \in \mathbb{Z}_p[x]$.*

Define $f_j(x)$ with $(j = 1, 2, \ldots)$ as follows

$$f(x+y) = f(x) + f_1(x)y + f_2(x)y^2 + \ldots$$

Then the formal derivative of f is $f'(x) = f_1(x)$.

Lemma 2.3.18. *(Hensel)*

Let $f(x) \in \mathbb{Z}_p[x]$ and let $a_o \in \mathbb{Z}_p$ be such that

$$|f(a_0)| < |f'(a_0)|^2$$

Then there exists an $a \in \mathbb{Z}_p$ such that $f(a) = 0$.

Proof. As $|f(a_0)| < |f'(a_0)|^2$, we know that there exists a $b_0 \in \mathbb{Z}_p$ such that

$$f(a_0) + b_0 f_1(a_0) = 0.$$

By definition 2.3.17, we have

$$|f(a_0+b_0)| \leq \max_{j\geq 2} |f_j(a_0)b_0^j|.$$

Since $f_j(x) \in \mathbb{Z}_p[x]$ and $a_0 \in \mathbb{Z}_p$, we have that $|f_j(a_0)| \leq 1$. As moreover $|b_0^n| \leq |b_0^2|$ for $n = 2, 3, \ldots$, we have

$$\begin{aligned} |f(a_0+b_0)| &\leq |b_0^2| \\ &= \frac{|f(a_0)|^2}{|f'(a_0)|^2} \\ &< |f(a_0)| \end{aligned}$$

as $|f(a_0)| < |f'(a_o)|^2$. In the same way, we get

$$|f_1(a_0+b_0) - f_1(a_0)| \leq |b_0| < |f_1(a_0)|.$$

Now $|q-r| < |r|$ can only happen if $|q| = |r|$, so we get

$$|f_1(a_0+b_0)| = |f_1(a_0)|.$$

Now let $a_1 = a_0 + b_0$ and repeat the same process. Then we get a sequence $\{a_n\}$ such that

$$|f_1(a_n)| = |f_1(a_0)|.$$

So we get

$$\begin{aligned} |f(a_{n+1})| &\leq \frac{|f(a_n)|^2}{|f_1(a_n)|^2} \\ &= \frac{|f(a_n)|^2}{|f_1(a_0)|^2} \end{aligned}$$

As $|f_1(a_0)| \leq 1$, we have that $|f(a_0)| < 1$. Hence

$$\lim_{n\to\infty} \frac{|f(a_n)|^2}{|f_1(a_0)|^2} = 0.$$

So,

$$\lim_{n\to\infty} f(a_n) = 0.$$

From that we get easily

$$\begin{aligned} |a_{n+1} - a_n| &= |b_n| \\ &= \frac{|f(a_n)|}{|f_1(a_n)|} \\ &= \frac{|f(a_n)|}{|f_1(a_0)|} \end{aligned}$$

So $|a_{n+1} - a_n|$ tends to 0 as $f(a_n)$ tends to 0. Define the sequence $\{b_n\}$ with $b_n = a_{n+1} - a_n$. Then b_n tends to 0 as n tends to infinity, so by proposition 2.3.12, $\{a_n\}$ tends to a limit a in $\mathbb{Z}_p$. Moreover $f(a) = 0$ by what we proved above. □

Chapter 3

Dirichlet L-series

3.1 Dirichlet Characters

Definition 3.1.1. *A Dirichlet character is a multiplicative homomorphism* $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$, *where* n *is a positive integer. In other words it is a function from* $F_n = (\mathbb{Z}/n\mathbb{Z})^\times$ *to* $\mathbb{C}^\times$ *satisfying the condition*

$\forall a, b \in F_n \ : \ \chi(ab) = \chi(a)\chi(b)$.

Notes (1) We can extend the definition of the Dirichlet character by defining it on all integers prime to n. Then $\chi(a)$ $(a \in \mathbb{Z})$ depends only on $a \ mod \ n$. We say that χ is a Dirichlet character modulo n. Further extending the definition, we put $\chi(a) = 0$ if a is not coprime to n.

(2) Take $m \in \mathbb{Z}$ such that $m|n$ and $m \neq n$ and $m > 0$. Let χ' be a character modulo m. Then χ' induces a character modulo n, χ, in the obvious way. For all integers a coprime to n (hence also coprime to m) define: $\chi(a) = \chi'(a \ mod \ m)$.

(3) If χ is a character modulo n which is not induced in this way, we say that it is *primitive*. Then n is called the *conductor* of χ. We write f_χ for the conductor of χ.

(4) If $\chi(a) = 1$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ then we say that χ is the trivial character and write $\chi = 1$.

Example 3.1.2. *(1) Let* $\chi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}^\times$ *be defined by* $\chi(1) = 1$, $\chi(2) = -1$. *Then necessarily* $\chi(2^2) = (\chi(2))^2 = 1 = \chi(4)$ *and* $\chi(2^3) = -1 = \chi(8 \ mod \ 5) = \chi(3)$. *This character is primitive since 5 is prime so it does not have proper divisors which could induce* χ.

(2) Let $\chi : (\mathbb{Z}/6\mathbb{Z})^\times \to \mathbb{C}^\times$ *be defined by* $\chi(1) = 1$ *and* $\chi(5) = -1$. *Here* χ *is induced by the character* $\chi' : (\mathbb{Z}/3\mathbb{Z})^\times$ *defined by* $\chi'(1) = 1$ *and* $\chi'(2) = -1$. *So* χ *is not primitive.*

In the course of this document, we will only consider primitive Dirichlet characters so when speaking of characters, primitive will always be implied.

Lemma 3.1.3. *Let* χ *be a character of conductor* f *such that* $\chi(a) \neq 1$ *for at least one* $a \in (\mathbb{Z}/f\mathbb{Z})^\times$ *(i.e.* $\chi \neq 1$*). Then*

$$\sum_{a=1}^{f} \chi(a) = 0.$$

Proof. Take b such that $\chi(b) \neq 1$ and $b \in (\mathbb{Z}/f\mathbb{Z})^\times$. Then $hcf(b, n) = 1$ so multiplication by b permutes the numbers $1, \ldots, f$ modulo f. Indeed, if $1 \leq a \leq f$, then

$$\begin{aligned} ab &\equiv x \mod f \\ cb &\equiv x \mod f, \end{aligned}$$

implies that $a \equiv c \mod f$. So we can write

$$\begin{aligned} \chi(b) \sum_{a=1}^{f} \chi(a) &= \sum_{a=1}^{f} \chi(a)\chi(b) \\ &= \sum_{a=1}^{f} \chi(ab) \\ &= \sum_{a=1}^{f} \chi(a). \end{aligned}$$

Hence

$$(\chi(b) - 1) \sum_{a=1}^{f} \chi(a) = 0.$$

As $\chi(b) \neq 1$ this entails that $\sum_{a=1}^{f} \chi(a) = 0$. □

Lemma 3.1.4. *If χ is a Dirichlet character, then so is χ^{-1} with $\chi^{-1}(a) = (\chi(a))^{-1}$ for a such that $hcf(a, f) = 1$.*

Proof. As $hcf(a, f) = 1$, we have $\chi(a) \neq 0$. So if $a, b \in (\mathbb{Z}/f\mathbb{Z})^\times$, then

$$\chi^{-1}(ab) = \frac{1}{\chi(ab)} = \frac{1}{\chi(a)\chi(b)} = \chi^{-1}(a)\chi^{-1}(b).$$

□

Definition 3.1.5. *The multiplication of two characters χ, ψ with conductors f_χ and f_ψ respectively is defined as the primitive character associated to γ with*

$$\begin{aligned} \gamma : (\mathbb{Z}/lcm(f_\chi, f_\psi\mathbb{Z})^\times &\to \mathbb{C}^\times \\ a &\mapsto \chi(a)\psi(a). \end{aligned}$$

Lemma 3.1.6. *Let χ, ψ be Dirichlet characters. Then*

$$\chi(a)\psi(a) = \chi\psi(a)$$

unless $\chi(a) = \psi(a) = 0$

Proof. In general, characters from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $C^\times$ can be written as a product of characters of prime power conductor. So we can restrict ourselves to the case where the conductors of χ and ψ are some power of a prime p. Now the only way that $\chi(a)\psi(a) \neq \chi\psi(a)$ is when $f_{\chi\psi} \neq f_\chi f_\psi$ and when $p \mid a$. But this means that both χ and ψ are non-trivial. Hence $\chi(a) = \psi(a) = 0$. □

3.2 L-series

Definition 3.2.1. *Let χ be a primitive Dirichlet character of conductor f. The L-series attached to χ is defined by:*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where $s \in \mathbb{C}$ and $Re(s) > 1$.

Notes (1) If $\chi = 1$ (so that $chi(a) = 1,\ \forall a$) then the L-series is just the usual Riemann zeta function.

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

(2) The L-series can be analytically continued to the whole complex plane, except possibly for a simple pole at $s = 1$ when $\chi = 1$.

(3) The L-series take really interesting values at both positive and negative integers. Later we will investigate some of those values more closely. The zeros of this family of functions have nice properties too. It can be proved that $L(n, \chi) = 0$ if $(-1)^n \neq \chi(-1)$ for negative integers n. These are called the trivial zeros of the L-function. Now are there any other zeros ? In fact there are, as for example $\frac{1}{2} + i \times 14.1347\ldots$ (From A. Odlyzko's Internet site [7]) is a zero of the Riemann Zeta function. It is conjectured that the non-trivial zeros of the analytic continuation of the L-series all have real part equal to $\frac{1}{2}$. This conjecture is called the Generalised Riemann Hypothesis and has many important consequences in Mathematics. If the conjecture is true, it implies for example that there exists a non-probabilistic primality testing algorithm which finishes in polynomial time [3].

Definition 3.2.2. *We may extend the definition a bit further and define the* Hurwitz zeta function *for* $Re(s) > 1$ *and* $0 < b \leq 1$ *as:*

$$\zeta(s, b) = \sum_{n=0}^{\infty} \frac{1}{(b+n)^s}$$

Lemma 3.2.3.

$$L(s, \chi) = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta\left(s, \frac{a}{f}\right)$$

where $Re(s) > 1$ *and* f *is the conductor of* χ.

Proof.

$$\begin{aligned}\sum_{a=1}^{f}\chi(a)f^{-s}\zeta\left(s,\frac{a}{f}\right) &= \sum_{a=1}^{f}\chi(a)f^{-s}\sum_{n=0}^{\infty}\frac{1}{(\frac{a}{f}+n)^s}\\ &= \sum_{a=1}^{f}\chi(a)\sum_{n=0}^{\infty}\frac{1}{(a+fn)^s}\\ &= \sum_{a=1}^{f}\sum_{n=0}^{\infty}\frac{\chi(a)}{(a+fn)^s}.\end{aligned}$$

change of variable: put $m = a + fn$.

$$\sum_{a=1}^{f}\sum_{n=0}^{\infty}\frac{\chi(a)}{(a+fn)^s} = \sum_{a=1}^{f}\sum_{\substack{m=a\\ m\equiv a\ (f)}}^{\infty}\frac{\chi(a)}{m^s}.$$

putting the sums together, we get:

$$\begin{aligned}\sum_{a=1}^{f}\sum_{\substack{m=a\\ m\equiv a\ (f)}}^{\infty}\frac{\chi(a)}{m^s} &= \sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}\\ &= L(s,\chi).\end{aligned}$$

□

The idea for the construction of a p-adic L-function is that we want it to be a function taking the same values as the Dirichlet L-series on the negative integers. With a few modifications, we will be able to do this. So we will now investigate the values of the L-series. Before we can do so, we first have to introduce the Bernoulli numbers as they will appear in the formula for the values that the L-series takes on at negative integers.

3.3 Bernoulli Numbers

Definition 3.3.1. *The Bernoulli numbers B_n are defined by*

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty}B_n\frac{t^n}{n!}$$

The generalised Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}$$

(e is just $exp(1)$, χ is a Dirichlet character of conductor f)

The Bernoulli polynomials $B_n(X)$ are defined by

$$\frac{te^{Xt}}{e^t-1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}$$

The Bernoulli numbers appear in many parts of mathematics. They were first introduced by Jacques Bernoulli (1654-1705) to write down infinite series expansions for hyperbolic and trigonometric functions.

Here is a list of the first few Bernoulli numbers:

B_0	B_1	B_2	B_4	B_6	B_8	B_{10}	B_{12}	B_{14}	B_{16}	B_{18}	B_{20}
1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$	$\frac{43867}{798}$	$-\frac{174611}{330}$

The B_k for k odd ($\neq 1$) are not in the table since they are zero as proved in the following lemma.

Lemma 3.3.2. *The odd Bernoulli numbers are zero (except B_1).*

Proof. The following is unchanged by substituting $-t$ for t:

$$\frac{t}{e^t-1} + \frac{t}{2} = \frac{t(e^{\frac{1}{2}t}+e^{-\frac{1}{2}t})}{2(e^{\frac{1}{2}t}-e^{-\frac{1}{2}t})}.$$

So we get the following argument

$$\frac{t}{e^t-1} + \frac{t}{2} = \frac{-t}{e^{-t}-1} + \frac{-t}{2}$$

So,

$$\begin{aligned}
-t &= \frac{t}{e^t-1} - \frac{-t}{e^{-t}-1} \\
-t &= B_0 + \frac{B_1}{1!}t + \frac{B_2}{2!}t^2 + \frac{B_3}{3!}t^3 + \frac{B_4}{4!}t^4 + \frac{B_5}{5!}t^5 \ldots \\
&\quad - (B_0 - \frac{B_1}{1!}t + \frac{B_2}{2!}t^2 - \frac{B_3}{3!}t^3 + \frac{B_4}{4!}t^4 - \frac{B_5}{5!}t^5 - \ldots) \\
-t &= -t + 2\frac{B_3}{3!}t^3 + 2\frac{B_5}{5!}t^5 + \ldots
\end{aligned}$$

So that finally, we get

$$\frac{B_3}{3!}t^3 + \frac{B_5}{5!}t^5 + \ldots = 0.$$

As the series expansion is identically equal to 0, all the coefficients have to be equal to 0 and hence the result. □

Lemma 3.3.3.

$$B_n(1-X) = (-1)^n B_n(X).$$

Proof.

$$\begin{aligned}\frac{te^{(1-X)t}}{e^t-1} &= \frac{te^{t-Xt}}{e^t-1} \\ &= \frac{te^{-Xt}}{1-e^{-t}} \\ &= \frac{(-t)e^{-Xt}}{e^{-t}-1} \\ &= \sum_{n=0}^{\infty} B_n(X)\frac{(-t)^n}{n!}.\end{aligned}$$

So $B_n(1-X) = (-1)^n B_n(X)$. □

Lemma 3.3.4.

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$$

Proof. The generating function of the Bernoulli polynomials is the product of

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

and

$$e^{Xt} = \sum_{n=0}^{\infty} X^n \frac{t^n}{n!}.$$

So the n-th term in the product is just

$$\sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i} = B_n(X).$$

□

Proposition 3.3.5. *Let F be any multiple of f where f is the conductor of χ. Then*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

Note that $B_n(a/F)$ is the Bernoulli polynomial and not Bernoulli number B_n times a/F.

Proof.

$$\begin{aligned}
\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} &= \sum_{a=1}^{F} \chi(a) \sum_{n=0}^{\infty} F^{n-1} B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} \\
&= \sum_{a=1}^{F} \frac{\chi(a)}{F} \sum_{n=0}^{\infty} B_n\left(\frac{a}{F}\right) \frac{(Ft)^n}{n!} \\
&= \sum_{a=1}^{F} \chi(a) \frac{te^{(a/F)Ft}}{e^{Ft}-1}
\end{aligned}$$

Set $g = \frac{F}{f}$ and $a = b + cf$ with $1 \le b \le f$. As the character χ is only defined modulo f, we have $\chi(a) = \chi(b)$, so we get

$$\begin{aligned}
\sum_{b=1}^{f} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf)t}}{e^{fgt}-1} &= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{fgt}-1} \sum_{c=0}^{g-1} e^{cft} \\
&= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{fgt}-1} \frac{e^{fgt}-1}{e^{ft}-1} \\
&= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{ft}-1} \\
&= \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}
\end{aligned}$$

by definition of the generalised Bernoulli numbers. Hence we get the result. □

The following theorem will only be cited and not proved, as the proof is of complex analytic nature and would take us too far afield. For a proof, see Washington [9] Chapter 4, pages 32-34.

Theorem 3.3.6. *Let n be an integer with $n \geq 1$, then*

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

And more generally

$$\zeta(1-n,b) = -\frac{B_n(b)}{n}.$$

For $0 < b \leq 1$.

3.4 Von Staudt-Clausen

In this section we will prove an interesting result about Bernoulli numbers, which says that the denominators in Bernoulli numbers cannot get arbitrarily large. This will be an important fact when we try to define the p-adic L-functions. First we will start off with a technical Lemma needed in the proof of this theorem.

Lemma 3.4.1. *Define $S_k(n) = 1^k + 2^k + \ldots + (n-1)^k$. We claim that*

$$S_k(n) = \sum_{r=0}^{k} \binom{k}{r} \frac{B_k}{k+1-r} n^{k+1-r}$$

Proof. We have

$$\begin{aligned} 1 + e^X + \ldots + e^{(n-1)X} &= \frac{e^{nX}-1}{e^X-1} \\ &= \frac{e^{nX}-1}{X}\frac{X}{e^X-1} \end{aligned} \tag{3.1}$$

Do the power series expansion on both sides. First, we see that the left-hand side gives :

$$
\begin{aligned}
&1+e^X+\ldots+e^{(n-1)X} = \\
&\quad 1+ \\
&\quad 1+X+\frac{X^2}{2!}+\frac{X^3}{3!}+\ldots+\frac{X^k}{k!}+\ldots+ \\
&\quad 1+2X+\frac{(2X)^2}{2!}+\frac{(2X)^3}{3!}+\ldots+\frac{(2X)^k}{k!}+\ldots+ \\
&\quad \ldots \\
&\quad 1+(n-1)X+\frac{((n-1)X)^2}{2!}+\frac{((n-1)X)^3}{3!}+\ldots+\frac{((n-1)X)^k}{k!}+\ldots
\end{aligned}
$$

So the coefficient of X^k in the sum is

$$\frac{1^k+2^k+\ldots+(n-1)^k}{k!}=\frac{S_k(n)}{k!} \tag{3.2}$$

Now the power series expansion for e^{nX} is just

$$1+nX+\frac{(nX)^2}{2!}+\ldots+\frac{(nX)^i}{i!}+\ldots$$

So the expansion for $\frac{e^{nX}-1}{X}$ is

$$n+\frac{n^2X}{2!}+\frac{n^3X^2}{3!}+\ldots+\frac{n^iX^{i-1}}{i!}+\ldots$$

As we have seen before, the power series for $\frac{X}{e^X-1}$ is

$$B_0+\frac{B_1}{1!}X+\frac{B_2}{2!}X^2+\ldots+\frac{B_k}{k!}X^k+\ldots$$

So the coefficient of X^k in their product is

$$B_0\frac{n^{k+1}}{(k+1)!}+\frac{B_1}{1!}\frac{n^k}{k!}+\ldots+\frac{B_i}{i!}\frac{n^{k+1-i}}{(k+1-i)!}+\ldots+\frac{B_k}{k!}n$$

We can write this as the following sum

$$\begin{aligned}&\sum_{r=0}^{k}\frac{B_r}{r!(k-r)!(k+1-r)}n^{k+1-r}\\ =&\frac{1}{k!}\sum_{r=0}^{k}\binom{k}{r}\frac{B_r}{k+1-r}n^{k+1-r}\end{aligned}\tag{3.3}$$

Now we can identify the coefficients of X^k from both sides of (3.1) by using (3.2) and (3.3) to get the result. □

Theorem 3.4.2. *(Von Staudt-Clausen)*
Let k be an even integer. Then

$$B_k+\sum_{\substack{q\ prime\\(q-1)|k}}q^{-1}\in\mathbb{Z}$$

Proof. As a first step, we prove that if $n\to 0$ p-adically (which means that $|n|_p$ tends to 0), then

$$B_k=\lim_{n\to 0}n^{-1}S_k(n).$$

Now we can say without loss of generality that n runs through the sequence $p,p^2,p^3,\ldots,p^m,\ldots$, as this sequence tends to 0 p-adically. So we let l tend to infinity in the usual sense, so that p^l tends to 0 p-adically and get

$$\begin{aligned}\lim_{l\to\infty}p^{-l}S_k(p^l)&=\lim_{l\to\infty}p^{-l}\sum_{r=0}^{k}\binom{k}{r}\frac{B_k}{k+1-r}p^{l(k+1-r)}\\ &=\lim_{l\to\infty}\sum_{r=0}^{k}\binom{k}{r}\frac{B_k}{k+1-r}p^{l(k-r)}\end{aligned}$$

Now if $r<k$, we are left with an exponent $p^{l(k-r)}$ and no matter now many times p appears in the denominator of the binomial, or in the denominator of B_r, as l tends to infinity, the $p^{l(k-r)}$ term take over in the end. So all terms with $r<k$ tend to 0 p-adically. So we get

$$\begin{aligned}\lim_{l\to\infty} p^{-l}S_k(p^l) &= \lim_{l\to\infty}\binom{k}{k}\frac{B_k}{k+1-k}p^{l(k-k)}\\ &= \lim_{l\to\infty} B_k\\ &= B_k.\end{aligned}$$

Now let us compare $p^{m-1}S_k(p^{m+1})$ and $p{-}mS_k(p^m)$. Now every integer j with $0 \le j < p^{m+1}$ is uniquely of the form

$$j = up^m + v \text{ with } 0 \le u < p \text{ and } 0 \le v < p^m$$

So we can write

$$\begin{aligned}S_k(p^{m+1}) &= \sum_{j=0}^{p^{m+1}-1} j^k\\ &= \sum_{u=0}^{p-1}\sum_{v=0}^{p^m-1}(up^m+v)^k\\ &\equiv \sum_{u=0}^{p-1}\sum_{v=0}^{p^m-1} v^k + kp^m\sum_{u=0}^{p-1}u\sum_{v=0}^{p^m-1}v^{k-1} \qquad (\text{mod } p^{2m})\\ &\equiv p\sum_{v=0}^{p^m-1} v^k + kp^m\sum_{u=0}^{p-1}u\sum_{v=0}^{p^m-1}v^{k-1} \qquad (\text{mod } p^{2m})\end{aligned}$$

by using the binomial theorem, as all other terms are multiplied by at least p^{2m}. As k is even, and as

$$2\sum_{u=0}^{p-1} u = p(p-1) \equiv 0\,(p),$$

we get by using the fact that $\sum_{v=0}^{p^m-1} v^k = S_k(p^m)$,

$$S_k(p^{m+1}) \equiv pS_k(p^m)\,(\text{mod } p^{m+1}).$$

Now divide both sides by p^{m+1} and we get

$$|p^{-m-1}S_k(p^{m+1}) - p^{-m}S_k(p^m)|_p \leq 1.$$

So by Corollary 2.3.4, it follows that for any positive integers l, m we have

$$|p^{-l}S_k(p^l) - p^{-m}S_k(p^m)|_p \leq 1.$$

Put $m = 1$ and let l tend to infinity in the usual sense, so that p^l tends to 0 p-adically. Then

$$|B_k - p^{-1}S_k(p)|_p \leq 1. \tag{3.4}$$

Let us analyse what $S_k(p)$ is congruent to modulo p. If $(p-1)$ divides k, then $i^k \equiv 1 \pmod{p}$ for all $1 \leq i < p$ as the order of i is $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. So in this case $S_k \equiv (p-1) \times 1 \equiv -1 \mod p$.

If $(p-1) \nmid k$, then let t be a primitive root modulo p. As $(p-1) \nmid k$ and the order of t is $p-1$, t^k is not congruent to 1 *mod* p. Multiplication by t mod p permutes the integers from 1 to $p-1$, as if $ta \equiv b \mod p$ and $tc \equiv b$ mod p, then $a \equiv c \mod p$. So we get modulo p,

$$\begin{aligned} S_k(p) &\equiv \sum_{j=1}^{p-1} j^k && \mod p \\ &\equiv \sum_{j=1);p-1} (tj)^k && \mod p \\ &\equiv t^k \sum_{j=1}^{p-1} j^k && \mod p \\ &\equiv t^k S_k(p) && \mod p \end{aligned}$$

So $S_k(p)(t^k - 1) \equiv 0 \mod p$. But as we said before, t^k is not congruent to $1 \mod p$, so $S_k \equiv 0 \mod p$. Putting these two cases together, we have

$$\begin{aligned} S_k(p) &= \sum_{j=0}^{p-1} j^k \\ &\equiv \begin{cases} -1 & (\text{mod } p) \text{ if } (p-1)|k \\ 0 & (\text{mod } p) \text{ otherwise} \end{cases} \end{aligned} \tag{3.5}$$

So we can put 3.4 and 3.5 together to get

$$\begin{cases} |B_k + p^{-1}|_p \leq 1 & \text{if } (p-1)|k \\ |B_k|_p \leq 1 & \text{otherwise} \end{cases} \tag{3.6}$$

Now define

$$W_k = B_k + \sum_{\substack{q \text{ prime} \\ (q-1)|k}} q^{-1}.$$

If $q \neq p$, then $|1/q|_p = 1$ by definition of the p-adic valuation. If $q = p$, then we can use the first case in 3.6 to say that $|B_k + p^{-1}|_p \leq 1$. So if we sum everything together, we can use the non-archimedean property of $|\ |_p$ to get

$$|W_k|_p \leq 1.$$

This implies that W_k has no primes in its denominator. Hence it must belong to $\mathbb{Z}$, just as the theorem states. $\square$

Chapter 4

p-adic L-functions

After introducing the p-adic numbers and proving some results about classical L-functions, we will finally introduce p-adic L-functions. The construction is not straightforward, as the usual L-series does not converge p-adically. So, as we have already pointed out before, the p-adic L-function will agree with the classical L-function on negative integers after introducing a fudge factor. As we have seen in the previous chapter, these values are algebraic over $\mathbb{Q}$, as they depend on the values of Dirichlet characters.

4.1 Results from p-adic Analysis

In this section we will introduce all the tools we need in order to be able to construct p-adic L-functions. Some of the proofs in this section are omitted, as they would take us too far afield. The results are standard results from p-adic analysis and can for example be found in Washington [9] or in Cassels [2]. First, let us remember some basic definitions.

Definition 4.1.1. *A field is* algebraically closed *if every polynomial can be factorised into linear factors.*

Definition 4.1.2. *An element of some algebraically closed field K is* algebraic *over a subfield k of K, if it is a root of a polynomial in $k[x]$.*

Lemma 4.1.3. *$\mathbb{Q}_p$ is not algebraically closed.*

Proof. First, we prove that if a polynomial with integer coefficients prime to p has no solutions mod p, then it has no solutions in $\mathbb{Q}_p$.

Say the integer polynomial $f[x]$ with coefficients prime to p has a solution a in $\mathbb{Q}_p$, then the solution is of the form

$$a = \sum_{n=N}^{\infty} a_n p^n \text{ with } a_n \in \{0, 1, \ldots, p-1\} \text{ and } a_N \neq 0.$$

Now if $N > 0$, then $a \equiv 0 \bmod p$, so there is a solution mod p. If $N \leq 0$, then a_0 is a solution mod p. So if $f[x]$ has no solutions mod p then it has no solutions in $\mathbb{Q}_p$.

For $p = 2$, consider the polynomial $X^2 + X + 1$, which is always 1 mod 2. So $\mathbb{Q}_2$ is not algebraically closed. Now if $p > 2$ is a prime, about half the numbers in $\{1, \ldots, p-1\}$ are not squares mod p. This can easily be deduced from the fact that the map $x \mapsto x^2$ is 2-to-1, as $(-x)^2 = x^2 \bmod p$. So for each p, there exists an a in $\{1, \ldots, p-1\}$ such that

$$X^2 - a \equiv 0 \pmod{p}$$

has no solution mod p, so $\mathbb{Q}_p$ is not algebraically closed. □

As $\mathbb{Q}_p$ is not algebraically closed, but we need to work with algebraic numbers, we need to consider its algebraic closure $\overline{\mathbb{Q}}_p$.

Proposition 4.1.4. *$\overline{\mathbb{Q}}_p$ is not complete.*

The proof would take us too far into the theory of cyclotomic fields, so it is not given here. For a proof please see Washington [9] Chapter 5, page 48.

Definition 4.1.5. *Let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$, then $\mathbb{C}_p$ is algebraically closed.*

Again, a proof of fact that $\mathbb{C}_p$ is algebraically closed can be found in Washington [9] Chapter 5, pages 48,49.

Definition 4.1.6. *A solution of*

$$X^{(p-1)} - 1 = 0$$

in $\mathbb{Z}_p$ is called a $(p-1)$st root of unity.

Lemma 4.1.7. *For each $a \in \mathbb{Z}_p$ such that $p \nmid a$, there exists a $(p-1)$st root (or square root for $p = 2$) of unity congruent to a mod p. This $(p-1)$st root of unity is denoted by $\omega(a)$. So $\omega(a) \equiv a$ mod p (mod 4 for $p = 2$).*

Proof. The case $p = 2$ is easily dealt with, as if $2 \nmid a$, then $a \equiv 1$ or $3 \mod 4$, so $\omega(a) = 1$ or $\omega(a) = -1 = 1 + 2 + 2^2 + \ldots$. Now say that $p > 2$. When $a \in \mathbb{Z}_p$ and $p \nmid a$, then a is congruent to one of $1, \ldots, p-1$ modulo p. As the size of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$, for each $x \in \{1, \ldots, p-1\}$, $x^{p-1} \equiv 1 \mod p$. So there exists a root x of $f(X) = X^{(p-1)} - 1$ modulo p with $x \equiv a\ (p)$.

The derivative of f is $f'(X) = (p-1)X^{(p-2)}$ and $f'(x)$ is not congruent to $0 \mod p$, as $x \neq 0$. So we have the following requirement for Hensel's Lemma,

$$|f(x)|_p < |f'(x)|_p^2.$$

Hence, by Hensel's Lemma, there exists a $(p-1)$st root of unity congruent to $a \mod p$. □

Definition 4.1.8. *For $a \in \mathbb{Z}_p$, define $\langle a \rangle = \omega^{-1}(a)a$.*

Note that then $\langle a \rangle \equiv 1 \mod p$ as $\omega^{-1}(a) \equiv 1/a \mod p$.

Definition 4.1.9. *Define the p-adic exponential function as follows*

$$exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Lemma 4.1.10. *The radius of convergence for $exp(X)$ is $|X| < p^{-1/(p-1)}$.*

Proof. Recall that as the p-adic valuation is non-archimedean, a sum converges if and only if the n-th term tends to 0 as n tends to infinity. So we have to analyse how big p-adically, the $n!$ term can get. Let $[\frac{a}{b}]$ denote the integer part of the rational $\frac{a}{b}$. As there are $[n/p^i]$ multiples of p^i less than or equal to n, the exponent v of p in the factorisation of $n!$ is (if $p^a \leq n < p^{a+1}$)

$$\begin{aligned}\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^a}\right] &\leq \frac{n}{p}+\frac{n}{p^2}+\ldots+\frac{n}{p^a}\\ &< \lim_{b\to\infty} n\sum_{a=1}^{b}\frac{1}{p^a}\\ &= n\lim_{b\to\infty}\left(\frac{1-\frac{1}{p^{b+1}}}{1-\frac{1}{p}}-1\right)\\ &= n\left(\frac{p}{p-1}-1\right)\\ &= \frac{n}{p-1}.\end{aligned}$$

Let us also find a lower bound for

$$S=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^a}\right].$$

Now as we have a terms in S, it is certainly bigger or equal to

$$\begin{aligned}\frac{n}{p}+\ldots+\frac{n}{p^a}-a &= n\left(\frac{p^{-(a+1)}-1}{p^{-1}-1}-1\right)-a\\ &= n\left(\frac{p^{-a}-p}{1-p}-\frac{1-p}{1-p}\right)-a\\ &= \frac{n-np^{-a}}{p-1}-a.\end{aligned}$$

As $p^a\leq n<p^{a+1}$, we get

$$\begin{aligned}np^{-a} &< p\\ -np^{-a} &> -p\\ \frac{n-np^{-a}}{p-1} &> \frac{n-p}{p-1}\end{aligned}$$

because $p-1\geq 1$. Moreover we have

$$a\leq\frac{\log n}{\log p}.$$

So we finally get

$$\frac{n - np^{-a}}{p-1} - a > \frac{n-p}{p-1} - \frac{\log n}{\log p}.$$

By putting the inequations together we obtain

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < v < \frac{n}{p-1}$$

where v is the exponent of p in the factorisation of $n!$. So we get for the valuation of $n!$,

$$p^{-\frac{n-p}{p-1}+\frac{\log n}{\log p}} > |n!| > p^{-\frac{n}{p-1}}.$$

First, let us see how the lower bound on $|n!|$ influences convergence for the series. For simplicity write $\alpha = \frac{n}{p-1}$. Then we get

$$\begin{aligned} |n!| &> p^{-\alpha} \\ \frac{1}{|n!|} &< p^{\alpha} \\ |\frac{X^n}{n!}| &< |X^n| p^{\alpha}. \end{aligned}$$

In order for $\frac{X^n}{n!}$ to tend to 0, as n tends to infinity, we have to have

$$\begin{aligned} |X^n| p^{\alpha} &< 1 \\ |X|^n &< p^{-\frac{n}{p-1}} \\ n \log |X| &< -\frac{n}{p-1} \log p \\ \log |X| &< -\frac{1}{p-1} \log p \\ |X| &< p^{\frac{-1}{p-1}}. \end{aligned}$$

Along the same lines, we can prove with the other inequality that if $|X| > p^{-1/(p-1)}$, then $|X^n/n!| \to \infty$ when $n \to \infty$. So the radius of convergence is in fact

$$|X| < p^{-1/(p-1)}.$$

□

Definition 4.1.11. *Define the p-adic logarithm as the power series*

$$\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}X^n}{n}.$$

The next three lemmas are not proved here, but as they are necessary for the construct of the p-adic L-function, they are cited here. For proofs please see Washington [9].

Lemma 4.1.12. *The p-adic logarithm as given in definition 4.1.11 is convergent for $|x| < 1$. There is a unique extension of $\log_p$ to all of $\mathbb{C}_p \setminus \{0\}$ such that $\log_p(p) = 0$ and $\log_p(xy) = \log_p(x) + \log_p(y)$ for all $x, y \in \mathbb{C}_p \setminus \{0\}$*

Lemma 4.1.13. *Suppose that $r < p^{-1/(p-1)} < 1$ and*

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

with $|a_n| \leq Mr^n$ for some M. Then $f(X)$ can be expressed as a power series with radius of convergence at least $R = (rp^{1(p-1)})^{-1} > 1$.

As we have defined an exponential function and a logarithm function, it makes sense now to talk about arbitrary powers of p-adic numbers. Note that before we have restricted ourselves to integer powers.

Definition 4.1.14. *Let $a \in \mathbb{Z}_p$ such that $p \nmid a$. Define*

$$\langle a \rangle^x = \exp(x \log\langle a \rangle).$$

Lemma 4.1.15. *The function $\langle a \rangle^x$ converges if $|x| < qp^{-1/(p-1)}$ where q is defined as*

$$q = \begin{cases} p, & \text{if } p \neq 2 \\ 4, & \text{if } p = 2. \end{cases}$$

4.2 p-adic L-function

This section introduces the p-adic L-function. This function was first introduced in 1964 by Kubota and Leopoldt [5]. The exposition here is closely

based on the account given in Washington [9]. There are other ways of arriving at this result which yield more insight into relationships with cyclotomic fields (see Chapter 7 of Washington [9]). For our purposes, the approach given here is better as it results in a nice formula which is the basis of the computer algorithm used in the computational part of the project.

Definition 4.2.1. *Let s be a complex variable and a, F integers with $0 < a < F$. Define the function $H(s, a, F)$ as*

$$H(s, a, F) = \sum_{\substack{m \equiv a(F) \\ m>0}}^{\infty} m^{-s}.$$

We are mainly interested by the values that H takes at negative integers.

Lemma 4.2.2. *Let n be an integer with $n \geq 1$. Then*

$$H(1-n, a, F) = -\frac{F^{n-1} B_n(\frac{a}{F})}{n}.$$

And $H(1-n, a, F) \in \mathbb{Q}$.

Proof.

$$\begin{aligned} H(s, a, F) &= \sum_{\substack{m \equiv a(F) \\ m>0}}^{\infty} m^{-s} \\ &= \sum_{n=0}^{\infty} \frac{1}{(a+nF)^s} \\ &= \sum_{n=0}^{\infty} F^{-s} \frac{1}{(\frac{a}{F}+n)^s} \\ &= F^{-s} \zeta\big(s, \frac{a}{F}\big). \end{aligned}$$

where $\zeta()$ is the Hurwitz Zeta function defined in Definition 3.2.2. Note that these steps are valid, as $0 < a < F$ so that $0 < a/F < 1$. Now we can use Theorem 3.3.6 to write

$$H(1-n, a, F) = -\frac{F^{n-1} B_n(\frac{a}{F})}{n}.$$

This expression belongs to $\mathbb{Q}$, as the Bernoulli polynomials are polynomials with rational coefficients, and everything else in the formula is rational. $\square$

As H is rational at negative integers, it also belongs to $\mathbb{Q}_p$. Now by its definition, H has a close relationship to the Hurwitz Zeta function, which in turn is closely related to the classical L-functions by the formula given in Lemma 3.2.3.

Theorem 4.2.3. *Take q as in Lemma 4.1.15. Suppose $q \mid F$ and $p \nmid a$, Then there exists a p-adic meromorphic function $H_p(s, a, F)$ with $a, F \in \mathbb{Z}$ on*

$$\{s \in \mathbb{C}_p \text{ such that } |s| < qp^{-1/(p-1)} > 1\}$$

such that

$$H_p(1-n, a, F) = \omega^{-n}(a)H(1-n, a, F) \quad \text{for} n \geq 1.$$

In particular, when $n \equiv 0 \mod (p-1)$ (or $n \equiv 0 \mod 2$ if $p = 2$), then

$$H_p(1-n, a, F) = H(1-n, a, F).$$

The function H_p is analytic except for a simple pole at $s = 1$ with residue $1/F$.

Proof. Define the function H_p as

$$H_p(s, a, F) = \frac{1}{s-1}\frac{1}{F}\langle a \rangle^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} B_j \left(\frac{F}{a}\right)^j$$

where B_j is Bernoulli number j and $\langle a \rangle$ is as defined in definition 4.1.8. First, assuming convergence, we will prove the identities given in the theorem. If $j > n$, the binomial coefficient is zero, so we get

$$\begin{aligned} H_p(1-n, a, F) &= \frac{1}{(1-n)-1}\frac{1}{F}\langle a \rangle^{1-(1-n)} \sum_{j=0}^{n} \binom{1-(1-n)}{j} B_j \left(\frac{F}{a}\right)^j \\ &= -\frac{1}{nF}\langle a \rangle^n \sum_{j=0}^{n} \binom{n}{j} B_j \left(\frac{F}{a}\right)^j \\ &= -\frac{1}{nF}\langle a \rangle^n \frac{F^n}{a^n} \sum_{j=0}^{n} \binom{n}{j} B_j \left(\frac{a}{F}\right)^{n-j}. \end{aligned}$$

By Lemma 3.3.4, we can introduce Bernoulli polynomials $B_n(X)$ to get

$$\begin{aligned} H_p(1-n,a,F) &= -\frac{F^{n-1}}{n}\left(\frac{\langle a\rangle}{a}\right)^n B_n\left(\frac{a}{F}\right) \\ &= -\frac{F^{n-1}}{n}\left(\frac{\omega^{-1}a}{a}\right)^n B_n\left(\frac{a}{F}\right) \\ &= -\frac{F^{n-1}\omega^{-n}}{n} B_n\left(\frac{a}{F}\right). \end{aligned}$$

By Lemma 4.2.2, this means that

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F).$$

Now if $n \equiv 0 \mod (p-1)$, then $\omega^{-n}(a) = 1$, as it is root of unity of order $p-1$. So in that case we have indeed

$$H_p(1-n,a,F) = H(1-n,a,F).$$

At $s = 1$, we have the residue

$$\frac{1}{F}\langle a\rangle^0 \sum_{j=0}^{\infty} \binom{0}{j} B_j \left(\frac{F}{a}\right)^j = \frac{1}{F}.$$

So let us now prove convergence in the domain $|s| < qp^{-1/(p-1)}$. Using the theorem of von Staudt-Clausen (3.4.2) proved in the previous chapter, we can say that $|B_j|_p \leq p$. Moreover, as $p \nmid a$, we have that $|a| = 1$ and from $q \mid F$ follows that $|q| \geq |F|$. This implies

$$\left|(B_j)\left(\frac{F}{a}\right)^j\right| \leq p|q|^j.$$

Using Lemma 4.1.13 with $r = |q| = \frac{1}{q}$ and $M = p$ we conclude that

$$\sum_{j=0}^{\infty} \binom{s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

is analytic on the disc $D = \{s \in \mathbb{C}_p \text{ such that } |s| < qp^{-1/(p-1)}\}$. As $qp^{-1/(p-1)} > 1$, we have $|1-s| \leq \max\{|1|, |s|\} < qp^{-1/(p-1)}$ so that D coincides with $\{s \in \mathbb{C}_p \text{ such that } |1-s| < qp^{-1/(p-1)}\}$. Hence

$$\sum_{j=0}^{\infty} \binom{1-s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

is also analytic on D. Similarly we conclude from the fact that $\langle a \rangle^s$ converges for $|s| < qp^{-1/(p-1)}$ (Lemma 4.1.15) that $\langle a \rangle^{1-s}$ is analytic in D. So $(s-1)H_p(s,a,F)$ is analytic in D, which is what we had to prove.

□

The p-adic L-function will have two parameters, s and χ, just like the complex L-series defined in definition 3.2.1. We have said before (definition 3.1.1) that Dirichlet characters are a function from $\mathbb{Z}$ to $\mathbb{C}^\times$. As we now work in $\mathbb{C}_p$, we regard the values of $\chi(a)$ to lie in $\mathbb{C}_p$. This works because $\mathbb{C}_p$ and $\mathbb{C}$ are algebraically isomorphic (see Washington [9] Chapter 5,page 49) and $\chi(a)$ lies in some algebraic extension of $\mathbb{Q}$.

Lemma 4.2.4. *The function $\omega(a)$ is a multiplicative homomorphism from $\mathbb{Z}$ to $\mathbb{C}_p$ with conductor q.*

Proof. First remark that $\omega(a)$ is only defined modulo q so the conductor is indeed q. The case $p = 2$ is obvious, so we can restrict ourselves to elements of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Now $\omega(a)$ is defined to be the $p-1$st root of unity congruent to a. So $\omega(ab) \equiv ab \mod p$ is the unique $p-1$st root of unity congruent to ab. As the product of two roots of unity of order $p-1$ is also of order $p-1$, $\omega(a)\omega(b)$ is a $p-1$st root of unity. Moreover it is congruent to $ab \mod p$. Hence $\omega(ab) = \omega(a)\omega(b)$ □

Theorem 4.2.5. *Let χ be a Dirichlet character of conductor f and let F be any multiple of q (as in Lemma 4.1.15) and f. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s,\chi)$ on $\{s \in \mathbb{C}_p$ such that $|s| < qp^{-1/(p-1)}\}$ with*

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} \text{ for } n \geq 1.$$

If $\chi = 1$ ($\chi(a) = 1 \forall a$) then $L_p(s,1)$ is analytic except for a pole at $s = 1$ with residue $(1-1/p)$.

Moreover the formula for $L_p(s,\chi)$ is

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Proof. First we show that the analytic properties hold, then we prove that the given formula does indeed give the desired values at $1-n$ for $n \geq 1$. We have

$$\begin{aligned}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(s,a,F) &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\frac{1}{s-1}\frac{1}{F}\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j\\ &= L_p(s,\chi).\end{aligned}$$

As $L_p(s,\chi)$ is the sum of meromorphic functions defined on $D = \{s \in \mathbb{C}_p \text{ such that } |s| < qp^{-1/(p-1)} > 1\}$, it is also meromorphic in D. The residue at $s=1$ is

$$R = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\frac{1}{F}.$$

If $\chi = 1$, then this sum is equal to

$$\begin{aligned}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\frac{1}{F} &= \frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}1\\ &= \frac{1}{F}\left(F - \frac{F}{p}\right)\\ &= 1 - \frac{1}{p}.\end{aligned}$$

If $\chi \neq 1$, we can write

$$R = \frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb).$$

As F is a multiple of f, the first sum is zero by Lemma 3.1.3. If $p \mid f$, then $\chi(pb) = 0$, as $hcf(pb, f) > 1$, so the second sum is also zero. Now if $p \nmid f$, then $f \mid (F/p)$ so again by Lemma 3.1.3 the second sum is zero. Hence if $\chi \neq 1$, the residue is 0, so that $L_p(s, \chi)$ has no pole at $s = 1$ and is analytic.

Now let us verify the identity for $L_p(1 - n, \chi)$ $(n \geq 1)$. We have by theorem 4.2.3

$$\begin{aligned} L_p(1-n,\chi) &= \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a) H_p(1-n,a,F) \\ &= \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\omega^{-n}(a) H(1-n,a,F). \end{aligned}$$

Now use lemma 4.2.2 to get

$$\begin{aligned} L_p(1-n,\chi) &= -\sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\omega^{-n}(a)\frac{F^{n-1}B_n(a/F)}{n} \\ &= -\frac{1}{n}F^{n-1}\sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\omega^{-n}(a) B_n\left(\frac{a}{F}\right). \end{aligned}$$

We can use lemma 3.1.6 to multiply the two characters χ and ω^{-n} as $\omega^{-n}(a) \neq 0$ to get

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{1}{n}F^{n-1}\sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi\omega^{-n}(a) B_n\left(\frac{a}{F}\right) \\ &= -\frac{1}{n}F^{n-1}\sum_{a=1}^{F} \chi\omega^{-n}(a) B_n\left(\frac{a}{F}\right) \\ &\quad + \frac{1}{n}F^{n-1}\sum_{b=1}^{F/p} \chi\omega^{-n}(bp) B_n\left(\frac{bp}{F}\right). \end{aligned}$$

Now the second part of the sum can be rewritten as

$$\frac{1}{n}F^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(bp)B_n\left(\frac{bp}{F}\right)$$
$$=\frac{1}{n}\chi\omega^{-n}(p)p^{n-1}\left(\frac{F}{p}\right)^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(b)B_n\left(\frac{b}{F/p}\right).$$

So we can use proposition 3.3.5 on both parts of the sum to get

$$L_p(1-n,\chi)=-\frac{1}{n}(B_{n,\chi\omega^{-n}}-\chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}$$
$$=-\frac{1}{n}(1-\chi\omega^{-n}(p)p^{n-1})B_{n,\chi\omega^{-n}}.$$

Hence the result. □

So we do indeed have this p-adic function which agrees with the classical L-function on negative integers except for the fudge factor $(1-\chi\omega^{-n}(p)p^{n-1})$. This factor is called the Euler factor at p for $L(s,\chi\omega^{-n})$. So theorem 4.2.5 now provides with an easy formula to calculate the power series of $L_p(s,\chi)$.

Chapter 5

Programming Details

5.1 Preliminaries

We restrict ourselves to the case of teichmuller characters and irregular primes. The teichmuller character of index i is defined as $\chi(a) = \omega(a)^i$. An irregular prime is a prime which divides some Bernoulli number B_k with $0 \leq k \leq p-1$. The only interesting case for teichmuller characters is when $i = k-1$, as it can be proved that for other values of i, $L_p(s, \chi)$ is a p-adic unit and hence has no zeros.

5.2 Overall Strategy

The overall strategy is to first compute the p-adic L-function for some prime p and some teichmuller character with index `index`. The function is expressed as a power series in the variable s with ac terms, so that ac is the accuracy we want. Then Hensel's Lemma is used to compute the zero of the resulting power series.

The algorithm to express the L-function as a power series is based on the formula given in Washington [9], namely

$$L_p(s, \chi) = \frac{1}{p}\frac{1}{s-1}\sum_{a=1}^{p-1}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}B_j\left(\frac{p}{a}\right)^j.$$

The program calculates the sums in the same order as the formula. Each processor is assigned the task to calculate the inner sum for a few values of a.

If we have for example 16 processors, and the prime p is 37, then processors 0 to 11 will calculate the inner sum for 2 values of a and processors 12 to 15 do it for 3 values of a. If the total task cannot be evenly distributed amongst the processors, then the higher burden is placed on the processors with higher id, as processor 0 will do all the remaining work alone.

The Bernoulli numbers are precomputed for each processor in the array *bernvec*, so that they do not have to be calculated again for a different a. The calculation of the inner sum is quite straightforward. A sensible optimization I did was to keep track of the binomial coefficient and multiply it by the required value for each iteration of the inner sum, instead of just using the PARI function `binomial()`.

After the processors have finished summing up their part of the series, they all transfer the results to processor 0, which sums up the final series. The result is divided by p and $s-1$ to give the final form of the L-function. Then the function `do_Hensel()` is invoked, which calculates the zero. It does so by first finding a solution $sol \ mod \ p^3$ and then using the following recursion

$$sol_{i+1} = sol_i - \frac{L_p(sol_i)}{L'_p(sol_i)}$$

5.3 The PARI Library

As the program uses a lot of mathematical functions which have already been implemented by other people in highly optimized ways, I thought it would be best to use one of those libraries. The particular one I used was the PARI library which is developed at the University of Bordeaux and can be downloaded freely from ftp://megrez.math.u-bordeaux.fr/pub/pari. It has a lot of functions for use in Number Theory already built in, which helped me considerably.

The PARI variables have data type `GEN` in the C programming language. A `GEN` can be either an integer (of any size), a real (not used here), a series or a p-adic number. Functions are provided for addition, multiplication, division, logarithms, ... with any type of `GEN`'s. Moreover there are functions for calculating a derivative (as used in Hensel's Lemma) and for substituting a value for a variable in a series or polynomial.

The only thing that requires a bit of attention when programming in PARI is memory management. The `GEN`'s are not regular pointers, but rather

indices in a huge array which PARI uses to store its variables. When a calculation is done, the result is stored below all other variables in the array. The variable `AVMA` keeps track of where the last variable ends. So if we want to delete the result from an operation, we store `AVMA` in a temporary variable `ltop` before the operation and then after, set `AVMA` to `ltop` again. If however, we would like to keep the result and discard any intermediate results, we have to use the function `gerepile()`. This function frees all the space used by intermediate variables and moves the result (usually the last variable put into the array) into the space made free. For a more thorough explanation please refer to the PARI programming tutorial [1].

5.4 The MPI library

As I ran the program on the Fujitsu AP3000 supercomputer, I had to use the MPI (Message Passing Interface) library to send variables from one processor to another. Each processor has its own memory and the only way to communicate between different processes is to send messages. These messages can be of any length and just need the target processor's id. The main functions involved are `sendstruc()` and `recvstruc()` which send PARI objects from one processor to another. Because these structures are stored as a continous chunk of memory on the PARI stack, transfer is relatively straightforward.

There is one problem though. Inside the structures are pointers to other parts of the structure. A p-adic number for example has for example a pointer to three integers, namely the prime, the base integer and the p-adic valuation. These pointers have to be translated after the structure has been tranferred from one processor to another, as the exact memory location will certainly be different on the two processors.

In order to correct these pointers, we have to translate the pointers according to the new memory location. This translation is done at the end of `recvstruc()`. This took me quite some time to get right, as the PARI library is generally accessed through high-level mathematical functions and there is no documentation on the nitty gritty bits of how memory management works in detail. Essentially, I worked my way through the freely available code of the PARI library and pieced the address translation together myself.

5.5 Precision Issues

As with all computations, we have to analyze the precision to which we get the value of the zero by running the program. In our case it is quite straightforward. By setting the variable `ac`, we control the number of terms in the series expansion of $L_p(s,\chi)$ and the number of terms in the inner summation. Remember the formula for $L_p(s,\chi)$,

$$L_p(s,\chi) = \frac{1}{p}\frac{1}{s-1}\sum_{a=1}^{p-1}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}B_j\left(\frac{p}{a}\right)^j.$$

The main problem in terms of powers of p in the denominator of a term is the binomial coefficient. As we showed in the proof of the radius of convergence of the exponential function, we have

$$v < \frac{n}{p-1},$$

where v is the exponent of p in the factorisation of $j!$. So in term j in the inner summation, we get to precision $j-v$ with respect to the binomial term. Now B_j has p at most once in its denominator. So the inner sum is computed to a p-adic precision of $ac - ac/(p-1) - 1$. Now F/a, $\langle a\rangle$ and $\chi(a)$ are not divisible by p. We still have the $1/p$ term on the outside. So in total, if we do the calculations to accuracy `ac`, we get a precision of

$$ac - ac/(p-1) - 2.$$

So to calculate the zero for $p = 37$ to 1000 "decimal places", we have to set `ac` to 1029. As I did the calculations for the other primes with `ac` set to 100, I get for $p > 100$ an accuracy of 100-2=98 digits. If $p < 100$, we get 97 digits.

Chapter 6

Appendix

6.1 Appendix A : Program Listing

```
// Program to calculate the Zero of a p-adic L-function
// It runs on multiprocessor machines (if MULTI is defined)
// and can be compiled to run on single-processor as well.
// It uses the PARI library to do the mathematical
// calculations and the MPI library to handle inter-process
// communication if it's running on a multi-processor
// machine.

#include <stdio.h>
#include <memory.h>

#define MULTI

#ifdef MULTI
#include "mpi.h"
#endif

#include "pari.h"

#define PUSED (top-avma)/sizeof(long)
#define DEBUG 1

#ifdef MULTI
void sendstruc(GEN x, long ltop, long lbot, int dest) {
  /* Need to transmit the following things :
     size of data structure
     reference pointer to see how pointers have
```

```
                          to be adjusted (ltop)
     pointer to x
     data of x
  */

  long *siz,*ptrtop,*ptrx,size;

  siz=(long *) malloc(sizeof(long));
  ptrtop=(long *) malloc(sizeof(long));
  ptrx=(long *) malloc(sizeof(long));

  size=(ltop-lbot)/sizeof(long);
  *siz=size;
  *ptrtop=ltop;
  *ptrx=(long) x;

  /* Send the size, the base pointer and the data structure */
  MPI_Send(siz,1,MPI_LONG,dest,99,MPI_COMM_WORLD);
  MPI_Send(ptrtop,1,MPI_LONG,dest,98,MPI_COMM_WORLD);
  MPI_Send(ptrx,1,MPI_LONG,dest,97,MPI_COMM_WORLD);
  MPI_Send((long *)lbot,size,MPI_LONG,dest,96,MPI_COMM_WORLD);

  free(siz);
  free(ptrtop);
}

GEN recvstruc(int sender) {
  long *siz,ltop,lbot,*ptrtop,*ptrx,dec;
  MPI_Status status;
  GEN x,ll,a,b;

  /* Recieve x from the other processor */
  siz=(long *) malloc(sizeof(long));
  ptrtop=(long *) malloc(sizeof(long));
  ptrx=(long *) malloc(sizeof(long));
  MPI_Recv(siz,1,MPI_LONG,sender,99,MPI_COMM_WORLD,&status);
  MPI_Recv(ptrtop,1,MPI_LONG,sender,98,MPI_COMM_WORLD,&status);
  MPI_Recv(ptrx,1,MPI_LONG,sender,97,MPI_COMM_WORLD,&status);

  ltop=avma;
  avma=((long) ltop)-(*siz)*sizeof(long);
  lbot=avma;
  dec=ltop-*ptrtop;
  x=(long *) (*ptrx+dec);
  MPI_Recv((long *)lbot,*siz,
```

```
          MPI_LONG,sender,96,MPI_COMM_WORLD,&status);

  /* Now comes the hard bit :
     translating the addresses inside x.
     This is based on the code of gerepile
     from the pari library
  */

  ll=(long *)lbot;
  while (ll < (GEN)ltop)
  {
    const long tl=typ(ll);
    if (! is_recursive_t(tl)) {
      ll+=lg(ll);
      continue;
    }
    a = ll+lontyp[tl];
    if (tl==t_POL) {
      b=ll+lgef(ll); ll+=lg(ll);
    } else {
      ll+=lg(ll); b=ll;
    }
    for (; a<b; a++) {
      *a+=dec;
    }
  }
  free(siz);
  free(ptrx);
  return x;
}

#endif

#ifndef MULTI

typedef long MPI_Status;
int MPI_COMM_WORLD=1;

void MPI_Init(void *a,void *b) {
}

void MPI_Finalize(void) {
}

void MPI_Comm_rank(int cw,int *myrank) {
```

```
  *myrank=0;
}

void MPI_Comm_size(int cw,int *mysize) {
  *mysize=1;
}

void sendstruc(GEN x, long ltop, long lbot, int dest) {
  printf("Shouldn't happen\n");
}

GEN recvstruc(int sender) {
  GEN x;
  printf("Strange\n");
  x=stoi(0);
  return x;
}

#endif

long pcoeff(GEN a,long i) {
  GEN c,p;
  long ltop,coeff;

  c=(long *)a[4];
  if (i<=valp(a)) return 0;
  ltop=avma; i=i-valp(a);
  p=(long *) a[2];
  while (i>1) {
    c=gdivmod(c,p,NULL);
    i--;
  }
  coeff=gtolong(gmod(c,p));
  avma=ltop;
  return coeff;
}

void print_padic(GEN a,long prec) {
  long i;

  for (i=1;i<prec;i++) {
    printf("%4li",pcoeff(a,i));
  }
  printf("\n");
}
```

```
GEN do_Hensel(GEN Lfunc,long Lvar,long p,long ac) {
  /* Lfunc : p-adic L function normalised and truncated
     Lvar  : the main variable number of Lfunc
     p     : the prime we work with
     ac    : accuracy
  */
  GEN dLfunc,sol,acoeff,bcoeff;
  long ltop,ltop1,i,aval,bval;

  ltop=avma;
  /* Calculate the starting value for using Hensel's Lemma
     If the function is
     (0+a1*37+a2*37^2...)+(b0+b1*37...)*T+(0+...)*T^2+...
     Then the starting value is
     -(a1*37+a2*37^2)/(b0+b1*37)   mod p^3
  */
  printf("%li\n",pcoeff((long *)Lfunc[2],2));
  acoeff=(long *)Lfunc[2];
  bcoeff=(long *)Lfunc[3];
  aval=pcoeff(acoeff,2)+pcoeff(acoeff,3)*p;
  bval=pcoeff(bcoeff,2);
  sol=gcvtop(gneg(gdiv(gmodulss(aval,p*p),
              gmodulss(bval,p*p))),stoi(p),ac);
  sol=gerepileupto(ltop,sol);

  if (DEBUG==1) {
    printf("Starting value : ");
    output(sol);
  }

  /* Set the right precision for the solution p-adic number */
  setprecp(sol,ac);

  /* dLfunc is the derivative of the polynomial Lfunc
     with respect to the variable Lvar */
  dLfunc=deriv(Lfunc,Lvar);

  /* Now use Hensel's Lemma to find a solution */
  ltop1=avma;
  for (i=1;i<13;i++) {
    sol=gsub(sol,gdiv(gsubst(Lfunc,Lvar,sol),
                      gsubst(dLfunc,Lvar,sol)));
    sol=gerepileupto(ltop1,sol);
  }
```

```
  sol=gerepile(ltop,avma,sol);
  return sol;
}

int main(int argc,char **argv)
{
  int myrank,mysize,i;
  long int_p,              // The prime in long format
    int_index,             // Character index
    int_a,                 // Counter
    s,                     // variable "s"
    ac,                    // Accuracy of calculation
    out_top,               // AVMA pointer outside main loop
    in_top,                // AVMA pointer outside inner loop
    ltop,                  // local use of AVMA
    mylength,              // number of steps for processor
    lbound,                // lower bound for a
    ubound,                // upper bound for a
    global_timer,          // Time since start of program
    tim;                   // Local timer
  GEN p,                   // The prime in PARI format
    a,                     // Counter in PARI format
    teich_a,               // Teichmuller of a
    pa,                    // p/a
    bvec,                  // Array with Bernoulli numbers
    out_sum,               // The outer sum accumulator
    out_term,              // The outer term
    in_sum,                // The inner sum accumulator
    in_term,               // Inner term
    x,                     // The value for which Lp is 0
    bin,                   // binomial coefficient
    mins,                  // 1-s
    bincoeff,              // binomial coefficient
    *gptr[2];              // pointer to array of 2 Gens for
                           // memory management

  MPI_Init( &argc, &argv );
  MPI_Comm_rank( MPI_COMM_WORLD, &myrank );
  MPI_Comm_size( MPI_COMM_WORLD, &mysize );

  /* Initialise the Pari system with 400 MB of Memory */
  pari_init(400000000,100000);
  global_timer=timer();

  /* accuracy of the calculation */
```

```
ac=1029;
/* int_p is the prime we work with */
int_p=37;
/* int_index is the index of the cyclotomic character */
int_index=31;

/* Construct the basic PARI variables we'll need */
s=fetch_user_var("s");    // our variable will be called s
bin=polx[s];              // construct polynomial "s"
p=stoi(int_p);            // Set p to the prime
out_sum=stoi(0);          // The sum starts at 0

precdl=ac;                // set the series precision to ac
/* Calculate all Bernoulli numbers needed
   Remark : this is quick (approx. 155 secs) so
   it is calculated once for every processor */
bvec=bernvec(ac);

if (DEBUG==1) {
  tim=timer(); global_timer+=tim;
  if (myrank==0) {
    printf("Calculation of Bernoulli numbers took %li ms\n",
           tim);
  }
  printf("Memory used now : %li longs\n",PUSED);
}

/* Separate the task for the different processors
   The total sum is from 1 to int_p-1  */

mylength=(int_p-1)/mysize;
lbound=myrank*mylength+1;
if (myrank>=(mysize-((int_p-1)%mysize))) {
  mylength++;
  lbound+=(myrank-(mysize-((int_p-1)%mysize)));
}
ubound=lbound+mylength;
if (DEBUG==1) {
  printf("Processor %i going from %li to %li\n",
         myrank,lbound,ubound-1);
}

/* Now for the outside loop where a goes
   from lbound to ubound
*/
```

```
out_top=avma;
for (int_a=lbound;int_a<ubound;int_a++) {
  mins=gsubsg(1,bin);               // mins is "1-s"
  a=stoi(int_a);                    // PARI version of a
  /* Calculate the X(a)<a>^(1-s) term */
  ltop=avma;
  teich_a=teich(gcvtop(a,p,ac));
  out_term=gtrunc(gmul(gpowgs(teich_a,int_index+1),
                       gpow(gdivsg(int_a,teich_a),mins,ac)));
  out_term=gerepileupto(ltop,out_term);

  /* prepare the calculation of the inner sum */
  pa=gdiv(p,a);                      // pa is p/a
  /* The binomial coefficient starts at 1 */
  bincoeff=stoi(1);

  /* Calculate the extra B1 term which is missed in the loop
     because the loop goes over the even Bernoulli numbers
     (as the odd Bi are 0 except B1) */
  ltop=avma;
  in_sum=gmul(gmul(bernfrac(1),binome(mins,1)),pa);
  in_sum=gerepileupto(ltop,in_sum);

  /* Now do the inner sum
     We go from 0 to ac/2 as the odd Bi are 0 */
  in_top=avma;
  for (i=0;i<=(ac/2);i++) {
    /* Inner term is Bj*binomial(1-s,j)*(p/a)^j with j=2*i
       we have to take bvec[i+1] since PARI just stores
       the non-zero Bernoulli numbers and we calculated
       the B1 term already before the loop */
    ltop=avma;
    in_term=gmul(gmul((long *) bvec[i+1],bincoeff),
                 gpowgs(pa,i*2));
    in_term=gerepileupto(ltop,in_term);

    /* compute new form of binomial coefficient */
    ltop=avma;
    bincoeff=gmul(gmul(gsubgs(gsubsg(1,bin),i*2),
                       gsubgs(gsubsg(1,bin),i*2+1)),
                  gdivgs(bincoeff,(i*2+1)*(i*2+2)));
    bincoeff=gerepileupto(ltop,bincoeff);

    /* Add the new term to the inner sum */
    in_sum=gadd(in_sum,in_term);
```

```
    /* And clean up the stack */
    gptr[0]=&bincoeff;
    gptr[1]=&in_sum;
    gerepilemany(in_top,gptr,2);
  }
  /* Multiply the inner sum with the outer term and
     add everything to the outer sum */
  out_sum=gadd(gmul(out_term,in_sum),out_sum);
  out_sum=gerepileupto(out_top,out_sum);
  if (DEBUG==1) {
    tim=timer(); global_timer+=tim;
    printf("%2li  %4li:%2li:%2li    ",int_a,
      tim/60000,(tim/1000)%60,tim%1000);
    printf("(Memory used : %li)\n",PUSED);
  }
}
if (DEBUG==1) {
  printf("Finished : total time : %li s     ",
         global_timer/1000);
  printf("(Memory used : %li)\n",PUSED);
}

/* Now processor 0 does the rest of the work alone
   So we send the intermediate results to processor 0
*/

if (myrank!=0) {
  sendstruc(out_sum,out_top,avma,0);
  MPI_Finalize();
  return 0;
}

/* So processor 0 is the only one performing
   the following code */

/* Now recieve the sums from the other processors */
ltop=avma;
for (i=1;i<mysize;i++) {
  in_sum=recvstruc(i);
  out_sum=gadd(out_sum,in_sum);
  out_sum=gerepileupto(out_top,out_sum);
}

/* Now divide the sum by (s-1) and by p to have
```

```
     the final form of Lp(s,X) */
  out_sum=gdiv(gdiv(out_sum,p),gsubgs(bin,1));

  if (DEBUG==1) {
    printf("Truncating\n");
  }
  out_sum=gtrunc(out_sum);
  out_sum=gerepileupto(top,out_sum);

  if (DEBUG==1) {
    tim=timer(); global_timer+=tim;
    printf("Calculating Zero\n");
  }
  x=do_Hensel(out_sum,s,int_p,ac);
  print_padic(x,ac);

  /* Now apply the Wagstaff normalisation by substituting
     -log(1+T)/log(1+p+O(p^ac)) for s in -L
  */
  printf("Now Applying normalisation\n");
  p=gcvtop(stoi(int_p+1),stoi(int_p),ac);
  x=gpow(p,gneg(x),ac);
  x=gsubgs(x,1);
  x=gerepileupto(top,x);
  print_padic(x,ac);
  printf("\n");
  output(x);

  if (DEBUG==1) {
    tim=timer(); global_timer+=tim;
    printf("Calculation of zero time :  %4li:%2li:%2li\n",
           tim/60000,(tim/1000)%60,tim%1000);
    printf("Total time : %4li:%2li:%2li\n",
       global_timer/60000,
           (global_timer/1000)%60,
           global_timer%1000);
  }

  MPI_Finalize();

  return 0;
}
```

6.2 Results

So finally, here are the tables of the zeros of $L_p(s, \chi)$, for different values of p and different characters χ. The characters used are the Teichmuller characters of index i, such that p divides Bernoulli number B_{i+1}.

The main result of this project, the zero for $p = 37$ and $i = 31$ was computed on the Fujitsu AP3000 Supercomputer at Imperial College London. The program used 16 processors and it took 1 day, 14 hours and 58 minutes to complete. The other tables were computed using a Pentium II-300 and a Cyrix-133+ under Linux. They took between 10 minutes for the smaller primes and 3 hours for the big ones. This increase in computing time is due to the fact that we have to compute the inner sum p times. Moreover the computation of the inner sum takes longer for large primes too. Internally in PARI, p-adic integers are represented as usual integers, along with some other information, so if p is large, an integer representing a p-adic number mod p^{100} will be large too. So computing sums and multiplications takes longer than for small primes.

The format of the tables is quite intuitive. The entries are the coefficients of the power series expansion of the root of $L_p(s, \chi)$. So if we write

$$s = \sum_{n=0}^{\infty} s_n p^n,$$

then the entries are the s_n. The column number and row number (printed in bold above, respectively left of the table) are added together to give the exponent of p for which the entry is the coefficient of.

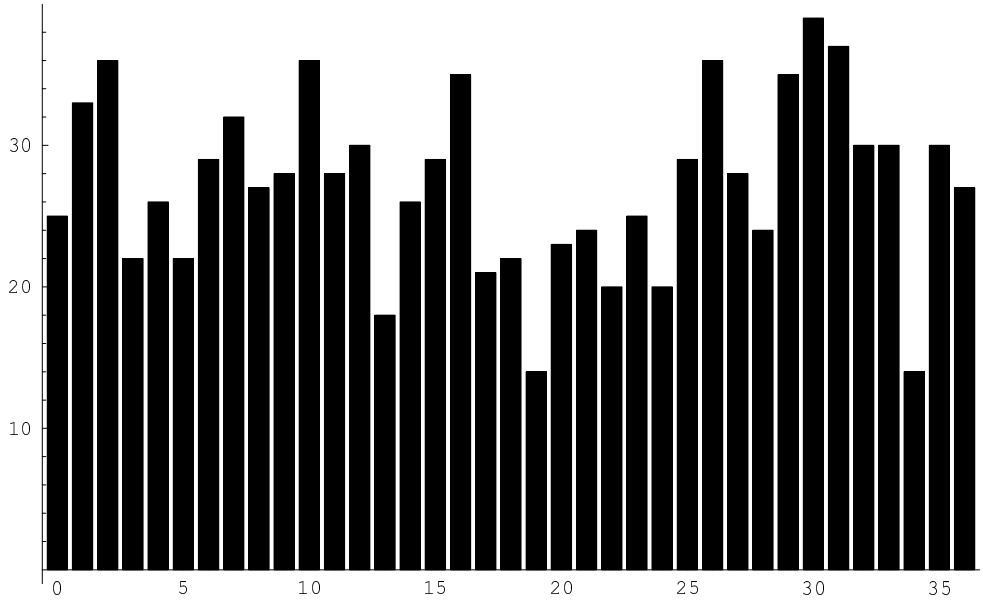

Figure 6.1: distribution of digits for p=37, i=31

As figure 6.1 shows the digits for $p = 37, i = 31$ are distributed not that evenly. Notably, there seems to be a lack of the digits 19 and 34. However these fluctuations can probably be explained by the fact that we only have 1000 data points. In the mean, each digit is represented 27 times and the variance is nearly 40 (38.77).

There is not much point plotting graphs like this for the other zeros as well because we clearly do not have enough digits to get a sensible graph.

6.2.1 Appendix B : Results for $p = 37$ and $i = 31$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	13	20	30	8	11	12	9	24	18	3
10	29	8	33	14	10	25	1	26	0	12
20	30	1	2	1	36	0	21	18	16	17
30	32	1	31	9	26	6	31	2	35	6
40	9	26	32	2	12	8	6	33	36	18
50	27	20	22	25	8	2	27	0	15	17
60	35	13	0	15	28	15	15	7	7	35
70	35	9	10	11	25	36	28	17	29	32
80	26	18	1	13	31	17	17	16	27	28
90	29	10	27	31	23	8	35	34	11	9
100	30	16	5	24	23	33	21	8	15	13
110	36	15	16	34	2	32	26	33	15	36
120	15	11	1	26	9	7	9	1	35	1
130	24	11	8	30	25	8	23	13	8	1
140	16	36	10	26	16	9	4	30	31	32
150	10	14	0	12	10	20	2	12	10	36
160	7	21	7	33	21	13	1	29	36	22
170	0	33	14	26	20	2	20	25	12	14
180	22	31	7	12	33	3	15	32	16	31
190	12	19	18	26	31	32	26	14	30	13
200	24	35	32	27	5	32	7	4	32	30
210	16	20	35	31	19	2	12	4	16	7
220	36	19	35	2	13	18	32	8	30	30
230	2	26	23	21	5	6	29	11	25	1
240	34	28	1	19	11	22	20	36	5	11
250	24	1	21	7	15	35	36	31	2	33
260	33	25	15	14	23	6	7	12	27	4
270	2	4	25	6	12	9	25	30	6	1
280	10	22	14	14	19	2	5	8	3	30
290	14	30	30	31	6	3	21	4	2	20
300	26	36	31	36	29	1	0	7	20	2
310	20	2	24	36	27	6	30	28	20	30
320	4	36	13	25	8	27	10	7	21	20

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
330	18	31	23	30	21	35	16	22	36	14
340	0	33	0	35	33	12	30	24	35	19
350	32	34	6	3	31	35	12	5	23	16
360	24	24	26	14	26	4	30	6	14	8
370	29	12	27	26	28	28	29	22	1	3
380	10	2	15	3	0	30	10	14	25	19
390	15	14	21	6	14	23	24	27	16	26
400	4	24	9	14	27	0	11	23	26	23
410	9	25	17	23	10	24	4	35	35	5
420	22	28	2	31	36	31	31	5	29	5
430	17	28	29	11	21	9	27	4	30	19
440	7	26	16	17	15	6	26	10	12	29
450	9	23	1	4	29	21	5	5	25	0
460	3	16	34	5	11	9	21	13	18	28
470	16	36	32	27	1	16	6	11	27	25
480	31	4	35	11	7	32	22	14	16	2
490	4	26	22	1	30	25	28	6	21	2
500	18	33	8	9	31	34	29	29	13	20
510	4	4	14	17	30	30	27	8	20	8
520	16	9	11	24	6	3	2	16	35	1
530	28	33	36	14	1	14	4	27	18	28
540	24	25	33	7	9	12	30	35	20	36
550	7	11	34	33	33	12	5	32	11	2
560	1	18	26	5	24	25	20	11	16	16
570	30	8	33	10	5	23	32	35	9	20
580	24	33	25	32	23	16	10	23	9	0
590	26	33	24	29	11	18	0	19	4	2
600	15	26	3	6	27	11	26	18	3	22
610	0	26	2	2	31	29	21	30	33	10
620	9	32	7	10	13	27	29	31	19	32
630	0	17	7	10	5	23	2	20	11	26
640	28	31	25	31	24	32	13	16	35	25
650	17	3	18	18	12	22	31	30	14	35
660	21	31	10	15	16	31	4	8	23	4
670	1	16	35	28	4	5	17	10	2	30
680	31	12	7	10	14	33	28	35	1	29
690	17	36	26	12	7	0	22	13	25	25

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
700	1	6	31	8	2	12	10	0	17	3
710	32	21	12	16	26	32	30	29	35	21
720	29	29	35	36	12	34	31	16	10	27
730	3	30	8	12	29	26	28	30	0	2
740	9	15	1	11	22	29	17	36	31	6
750	3	24	31	33	10	30	29	9	9	6
760	10	34	29	26	16	30	26	21	25	3
770	28	15	20	10	7	6	13	7	8	27
780	1	17	31	30	9	30	29	23	16	21
790	18	6	7	16	19	33	34	12	10	25
800	22	9	35	5	18	6	12	6	33	18
810	20	25	35	32	24	2	11	2	35	17
820	22	27	7	34	11	23	36	20	18	28
830	16	32	1	21	10	21	32	34	16	16
840	31	29	31	0	12	23	0	36	34	15
850	22	8	15	1	33	9	29	23	22	11
860	14	36	28	8	13	31	6	0	26	19
870	0	16	4	2	7	29	9	20	11	16
880	23	30	28	17	8	1	4	17	15	5
890	5	29	17	15	31	18	10	12	2	18
900	12	27	13	4	7	14	7	20	30	14
910	25	27	13	10	33	10	10	30	15	26
920	11	8	17	32	32	15	29	15	26	6
930	26	15	4	33	5	6	10	0	11	15
940	2	32	33	28	26	23	3	27	6	3
950	7	10	23	32	33	3	35	1	27	29
960	27	0	3	15	14	7	15	31	22	7
970	29	9	32	6	27	4	3	7	22	28
980	7	1	21	25	29	2	3	36	11	34
990	25	23	25	19	5	2	27	10	29	8

6.2.2 Appendix C : Results for other primes

Prime 59 and Index 43

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	31	9	15	55	40	51	5	11	30	10
10	41	21	11	16	3	32	25	51	44	47
20	10	17	30	2	28	3	2	44	10	18
30	2	22	9	15	55	22	9	29	9	13
40	1	16	58	15	56	54	54	54	13	24
50	48	14	35	26	58	37	4	18	34	24
60	37	35	37	16	41	40	32	35	12	30
70	45	7	56	11	38	7	45	52	16	16
80	54	45	50	20	1	29	30	7	45	5
90	16	56	37	25	33	0	15			

Prime 67 and Index 57

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	59	51	7	0	64	30	58	62	28	42
10	15	25	45	38	4	26	43	29	18	47
20	3	42	55	32	2	28	48	61	22	50
30	25	15	38	59	2	58	47	51	51	64
40	63	49	32	56	43	47	21	29	40	49
50	54	64	52	25	17	57	60	64	64	38
60	51	15	5	26	12	16	33	49	21	50
70	23	63	31	34	53	10	55	21	46	41
80	20	28	14	27	15	42	53	53	30	52
90	13	52	29	59	47	18	60			

Prime 101 and Index 67

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	91	100	88	14	57	94	36	6	35	21
10	86	72	63	33	67	65	38	54	96	60
20	79	3	35	88	60	90	11	23	29	66
30	75	65	85	7	20	16	84	5	14	28
40	79	47	50	63	53	99	83	62	37	30
50	63	44	90	81	35	43	27	95	17	57
60	75	53	37	1	27	47	2	56	15	39
70	93	61	23	58	8	15	26	16	68	80
80	46	60	45	82	22	33	3	18	36	80
90	82	45	47	8	61	81	59	77		

Prime 103 and Index 23

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	82	84	71	94	58	68	35	40	7	95
10	67	10	6	28	56	41	36	0	41	19
20	89	26	95	17	6	66	60	12	73	38
30	64	27	38	64	4	91	31	24	17	41
40	6	94	29	80	100	91	31	86	41	37
50	39	1	74	22	61	93	64	27	64	34
60	39	54	4	31	101	98	37	34	98	66
70	19	22	70	75	55	64	32	66	56	10
80	85	21	84	76	62	57	36	97	91	43
90	63	102	31	74	87	38	59	74		

Prime 131 and Index 21

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	72	64	16	31	35	102	55	49	90	2
10	94	68	39	60	35	80	115	14	24	96
20	109	70	52	33	64	73	66	97	72	55
30	91	15	81	51	99	38	72	48	98	119
40	59	81	82	100	46	50	29	14	88	9
50	2	55	111	84	40	100	21	54	51	72
60	87	67	18	59	33	64	85	89	90	14
70	77	42	5	30	14	116	54	84	101	55
80	100	114	28	127	6	42	52	55	88	113
90	65	73	127	66	19	123	19	18		

Prime 149 and Index 129

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	94	142	90	83	71	105	97	39	49	8
10	144	90	12	77	77	36	81	53	79	116
20	24	85	145	109	11	13	79	95	61	148
30	98	45	61	17	116	130	20	38	10	6
40	57	100	1	99	23	60	148	59	5	40
50	136	55	49	10	12	42	23	60	103	139
60	129	145	44	139	135	82	0	102	92	122
70	29	18	14	76	56	118	147	62	3	64
80	98	65	138	91	134	62	108	54	17	40
90	67	75	6	12	78	105	106	2		

Prime 157 and Index 109

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	121	86	54	108	104	4	60	136	9	123
10	11	44	18	39	102	142	59	132	79	98
20	23	46	36	121	56	138	13	69	110	64
30	66	125	28	86	103	75	18	120	22	96
40	134	0	124	84	93	96	131	128	90	82
50	123	38	10	7	23	72	148	17	149	131
60	69	76	94	2	69	83	128	22	100	141
70	138	35	54	34	34	7	43	24	29	105
80	92	155	132	65	124	10	43	37	94	110
90	114	47	115	17	132	140	50	34		

Prime 157 and Index 61

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	136	104	79	118	39	88	86	2	89	129
10	22	21	90	96	38	7	55	125	30	108
20	142	31	27	18	26	48	16	82	0	149
30	62	150	89	38	62	72	78	30	36	148
40	92	77	141	93	19	46	147	80	21	28
50	116	66	18	59	25	7	87	134	36	92
60	135	147	47	106	33	1	131	34	89	104
70	151	74	126	110	22	16	30	142	151	77
80	0	88	72	113	81	10	14	122	17	115
90	138	36	63	51	11	99	154	22		

Prime 233 and Index 83

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	90	224	203	10	214	115	25	72	122	121
10	29	154	22	0	53	207	44	76	214	210
20	169	33	226	38	42	90	104	193	23	22
30	52	122	210	212	28	192	111	177	219	92
40	140	99	167	72	76	54	89	99	136	132
50	98	15	153	205	14	3	75	205	164	179
60	184	78	96	92	2	24	151	12	56	148
70	17	71	221	140	39	28	111	228	211	45
80	9	22	215	19	39	149	179	203	195	135
90	57	105	17	63	60	96	27	136		

Prime 257 and Index 163

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	229	38	113	172	215	31	206	182	57	153
10	168	77	157	75	219	13	239	164	211	49
20	52	216	111	80	77	175	7	229	40	241
30	20	147	186	108	102	142	218	212	187	122
40	95	148	57	124	138	155	149	232	196	65
50	68	36	123	130	232	240	250	131	250	31
60	49	225	199	163	245	123	14	57	253	56
70	189	175	104	255	91	142	125	256	110	174
80	115	12	25	67	87	182	125	170	64	205
90	174	56	22	184	108	19	17	242		

Prime 263 and Index 99

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	99	204	11	218	95	160	102	49	175	197
10	135	111	72	113	73	232	242	60	237	67
20	163	153	10	121	8	220	66	179	145	257
30	204	169	200	196	196	95	139	261	30	34
40	145	217	187	34	49	168	236	173	155	72
50	99	219	224	69	244	206	9	250	242	239
60	114	93	188	151	20	90	253	210	18	257
70	91	177	222	56	130	146	129	34	123	216
80	46	14	107	235	231	101	108	244	134	254
90	148	112	7	101	220	200	151	228		

Prime 271 and Index 83

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	193	8	225	40	224	81	255	28	113	127
10	7	217	257	20	185	156	134	160	124	252
20	232	42	125	207	58	83	225	88	215	62
30	184	232	188	143	45	122	162	242	23	6
40	140	2	7	130	225	147	224	152	77	24
50	233	236	148	170	234	246	35	166	238	186
60	118	206	7	23	189	124	34	135	174	264
70	222	33	266	0	218	122	31	68	9	169
80	13	217	145	140	253	236	237	25	43	134
90	11	125	58	66	173	201	97	118		

Prime 283 and Index 19

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	246	133	55	249	113	150	13	114	19	31
10	136	204	151	199	121	44	278	235	166	30
20	196	70	159	241	200	180	170	114	106	23
30	45	156	243	144	42	38	84	215	71	273
40	241	36	196	133	36	99	52	116	109	23
50	244	278	142	230	273	226	34	267	163	53
60	99	160	278	21	254	266	206	153	57	248
70	57	258	203	54	141	25	202	220	135	84
80	5	30	235	125	13	274	96	254	210	154
90	153	168	133	180	279	55	94	259		

Prime 293 and Index 155

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	75	138	213	51	199	144	1	41	179	236
10	163	88	195	17	223	69	143	16	148	142
20	86	32	259	148	75	81	254	104	171	204
30	94	103	170	204	142	289	133	25	144	177
40	114	2	273	137	78	16	27	109	175	95
50	49	174	255	100	218	149	156	236	158	203
60	277	9	84	231	216	2	45	57	184	55
70	12	48	266	138	93	188	268	13	254	63
80	122	234	107	227	57	133	239	291	180	123
90	166	271	91	241	211	72	96	198		

Prime 307 and Index 87

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	290	163	124	121	238	35	0	274	93	128
10	262	37	74	279	242	249	165	17	117	200
20	146	36	63	79	231	26	17	131	183	7
30	201	33	106	146	46	294	196	188	142	257
40	82	267	225	84	301	202	115	241	278	276
50	170	70	172	12	242	280	29	32	94	224
60	260	130	223	105	121	7	95	303	104	261
70	74	264	148	226	149	234	95	56	261	19
80	33	14	73	300	26	303	282	112	118	127
90	235	185	133	133	101	233	77	230		

Prime 311 and Index 291

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	224	289	136	250	234	30	40	59	148	95
10	215	161	169	197	46	221	232	52	56	208
20	194	243	66	261	207	179	186	28	5	217
30	294	57	120	255	37	142	112	270	225	31
40	3	79	265	259	158	120	98	64	124	255
50	149	16	189	262	193	154	59	91	204	209
60	122	127	250	245	280	94	235	134	35	204
70	90	72	18	260	131	200	95	196	194	253
80	87	215	190	269	232	179	211	163	140	53
90	108	267	283	65	264	182	299	145		

Prime 347 and Index 279

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	181	136	247	156	304	227	31	271	54	76
10	72	197	145	85	316	5	216	282	179	163
20	30	98	168	108	2	181	142	84	316	325
30	24	305	252	134	27	1	26	74	118	95
40	165	185	202	168	11	306	199	272	232	81
50	184	2	322	10	154	265	115	269	100	79
60	209	45	3	299	111	297	157	267	76	106
70	297	103	337	314	178	64	233	337	45	35
80	297	289	63	340	335	201	212	139	108	53
90	77	156	175	224	28	210	248	177		

Prime 353 and Index 185

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	5	310	218	20	137	288	197	239	264	210
10	141	156	44	341	105	214	77	254	111	200
20	304	344	345	239	26	333	184	25	222	259
30	219	123	194	73	10	339	78	275	179	106
40	270	58	79	268	339	75	101	324	41	116
50	277	158	132	178	131	228	236	231	280	232
60	11	193	58	314	149	196	240	63	139	280
70	350	121	50	115	193	42	200	134	239	199
80	43	172	234	112	67	160	203	87	279	22
90	315	120	341	83	243	348	9	85		

Prime 353 and Index 299

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	235	118	14	13	93	311	86	258	317	35
10	104	20	343	242	300	199	167	145	153	291
20	98	67	26	339	29	73	30	123	230	319
30	141	159	238	258	146	87	280	44	252	234
40	133	74	331	61	168	98	57	139	319	264
50	200	292	180	145	331	112	4	70	36	232
60	344	272	288	111	58	217	71	7	236	114
70	77	122	154	142	248	104	3	332	169	284
80	205	227	93	47	304	323	123	281	310	244
90	314	151	0	15	340	164	83	333		

Prime 379 and Index 99

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	143	35	190	147	368	175	198	212	350	235
10	233	60	75	362	221	33	197	176	327	135
20	216	358	111	53	194	2	226	179	98	51
30	300	338	8	195	228	268	76	298	203	18
40	305	351	158	168	259	76	246	196	111	115
50	146	177	173	127	177	37	323	16	213	174
60	340	310	261	149	72	68	212	80	6	215
70	43	224	90	235	16	70	175	355	83	290
80	133	47	301	296	46	57	40	183	294	164
90	359	24	156	46	296	225	117	270		

Prime 379 and Index 173

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	191	231	182	107	149	236	122	286	245	348
10	89	349	366	27	66	65	99	33	91	360
20	294	145	374	119	142	351	121	321	2	50
30	15	20	183	87	65	286	5	62	373	39
40	291	333	286	85	71	290	345	177	122	253
50	303	168	257	378	209	214	252	143	188	273
60	14	323	114	206	299	295	235	63	356	326
70	231	230	139	97	58	351	180	18	165	222
80	198	274	286	337	12	128	235	341	79	325
90	344	100	78	255	178	225	252	34		

Prime 389 and Index 199

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	155	68	337	207	228	189	214	355	307	156
10	194	207	154	95	140	341	228	256	288	44
20	106	86	295	192	343	218	26	63	363	321
30	238	176	348	136	331	37	334	201	39	69
40	280	281	288	129	210	365	203	254	343	360
50	310	184	13	143	208	291	78	223	280	254
60	276	26	18	77	341	130	317	297	270	55
70	53	289	384	12	61	20	269	203	365	298
80	184	9	241	23	241	288	239	136	80	36
90	286	99	368	305	320	188	48	52		

Prime 401 and Index 381

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	283	263	86	385	373	149	188	189	34	97
10	43	35	399	385	129	161	271	287	298	388
20	202	169	12	272	155	336	384	199	331	205
30	253	309	341	344	181	317	265	356	150	174
40	378	64	364	46	152	64	195	248	292	4
50	355	149	131	197	304	268	76	35	391	360
60	240	354	126	135	98	230	2	120	329	238
70	390	376	57	205	282	384	15	360	94	113
80	275	321	215	251	200	388	59	320	296	58
90	3	336	215	375	337	284	141	12		

Prime 409 and Index 125

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	264	363	312	74	111	162	297	15	88	323
10	238	226	103	397	391	316	303	377	151	144
20	71	179	77	124	224	88	117	21	97	311
30	220	66	92	139	360	357	239	320	15	238
40	203	254	81	60	386	408	122	163	70	14
50	38	37	164	82	217	134	64	168	247	144
60	280	319	33	80	168	320	26	34	396	118
70	166	299	273	69	174	9	125	312	78	144
80	310	146	283	400	252	302	36	392	97	292
90	69	40	99	366	381	129	148	6		

Prime 421 and Index 239

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	112	211	315	132	376	39	178	23	212	150
10	152	208	26	381	291	292	393	41	156	56
20	379	417	304	3	363	60	181	106	84	304
30	356	328	370	155	293	207	176	156	45	144
40	139	264	306	54	400	198	323	206	208	13
50	302	81	346	105	317	195	60	354	347	332
60	296	154	133	91	235	78	75	281	388	286
70	19	122	298	80	30	154	293	172	66	286
80	246	232	284	414	97	91	60	306	173	61
90	65	298	148	54	17	257	95	37		

Prime 433 and Index 365

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	41	369	29	295	219	306	18	366	308	160
10	92	198	20	17	379	181	327	332	3	21
20	127	97	238	317	23	216	144	6	418	29
30	152	60	295	371	63	432	73	279	193	228
40	74	299	426	219	178	166	398	259	159	302
50	132	11	59	308	126	172	391	155	337	222
60	411	404	392	216	292	214	318	28	190	263
70	338	73	10	310	45	108	94	166	18	24
80	306	96	199	189	432	89	222	9	200	114
90	151	405	202	276	69	1	424	233		

Prime 461 and Index 195

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	228	159	111	289	291	68	454	396	202	354
10	317	411	408	236	212	175	417	176	451	428
20	440	399	2	202	45	217	235	273	286	6
30	375	296	231	358	402	280	158	103	328	336
40	416	137	434	250	56	445	372	427	172	349
50	131	74	179	55	129	299	247	46	124	244
60	92	294	339	134	249	174	204	272	202	145
70	142	113	240	387	304	375	348	329	215	184
80	209	263	5	174	45	355	155	242	224	181
90	344	446	324	123	373	286	123	133		

Prime 463 and Index 129

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	247	28	183	295	106	374	210	401	356	368
10	0	205	424	8	282	195	39	269	389	60
20	437	416	9	372	163	189	455	246	412	396
30	406	21	296	326	208	114	212	220	341	207
40	116	410	416	296	83	21	195	297	381	71
50	67	120	220	114	444	268	178	407	241	203
60	61	4	428	34	92	321	400	153	5	439
70	125	352	202	162	211	422	95	270	19	404
80	305	333	410	119	264	357	389	446	426	54
90	68	211	203	41	371	378	153	444		

Prime 467 and Index 193

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	90	46	292	264	218	448	392	225	22	228
10	402	314	350	91	197	113	51	147	318	1
20	347	452	319	217	100	447	153	377	127	167
30	434	282	202	183	399	356	394	170	132	249
40	284	243	172	237	327	80	39	79	19	264
50	409	394	136	67	110	360	351	87	261	399
60	173	295	26	388	13	84	63	256	101	116
70	109	453	209	433	269	55	402	136	346	244
80	325	434	187	38	257	131	383	172	159	374
90	57	405	193	49	464	327	119	384		

Prime 467 and Index 93

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	126	174	338	272	4	179	107	438	291	394
10	343	115	165	256	278	185	85	168	40	131
20	350	306	14	393	207	400	373	161	237	221
30	2	375	206	428	80	284	140	17	298	208
40	74	317	306	99	55	27	284	419	384	249
50	166	33	454	301	356	53	109	117	237	292
60	7	303	377	448	424	189	131	136	355	400
70	94	182	24	114	61	365	100	54	116	451
80	324	356	379	80	229	319	314	427	178	302
90	365	174	396	444	252	78	212	251		

Prime 491 and Index 291

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	418	80	417	136	99	67	27	138	25	79
10	171	73	37	347	346	44	110	160	323	343
20	400	339	289	19	457	424	150	331	382	344
30	234	411	153	151	217	72	248	33	138	455
40	283	2	27	201	46	170	367	88	130	432
50	186	108	194	411	255	173	412	62	238	162
60	432	213	194	213	56	484	197	86	183	375
70	347	487	208	120	131	179	36	455	323	281
80	360	76	41	32	467	444	360	183	417	472
90	412	278	317	401	468	199	38	326		

Prime 491 and Index 335

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	416	245	25	340	176	309	15	309	95	341
10	69	463	314	335	132	400	202	129	222	282
20	146	431	123	272	77	310	360	116	208	112
30	83	53	392	370	458	357	185	51	6	103
40	104	490	64	173	484	362	455	426	272	417
50	60	137	216	25	363	46	292	458	3	230
60	345	474	122	383	420	193	201	446	188	9
70	380	62	484	397	290	10	174	159	278	374
80	344	54	16	154	246	27	343	421	266	43
90	223	42	342	459	37	228	362	115		

Prime 491 and Index 337

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	213	100	437	489	418	312	303	155	410	257
10	363	349	383	320	231	85	164	210	395	405
20	60	280	272	434	5	149	57	0	63	455
30	319	60	416	244	237	419	158	460	250	158
40	327	245	313	312	365	459	121	10	384	433
50	226	435	375	356	7	47	160	99	96	446
60	449	394	186	484	109	104	41	166	315	35
70	354	246	389	466	266	166	278	335	58	303
80	213	146	17	242	361	147	152	107	144	328
90	150	51	117	437	43	89	211	134		

Bibliography

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. Pari-gp. ftp://megrez.math.u-bordeaux.fr/pub/pari.

[2] J.W.S. Cassels. *Local Fields*. Cambridge University Press, 1986.

[3] Harden. http://www.math.niu.edu/ rusin/known-math/97/grh.

[4] Samuel S. Wagstaff Jr. Zeros of p-adic L-functions. *Mathematics of Computation*, 29(132), 1975.

[5] T. Kubota and H.W. Leopoldt. Eine p-adische theorie der zetawerte. *Journal für reine angewandte Mathematik*, 214, 1964.

[6] K. Mahler. *Introduction to p-adic numbers and their functions*. Cambridge University Press, 1973.

[7] Andrew M. Odlyzko. The first 100 (non trivial) zeros of the riemann zeta function. http://www.lacim.uqam.ca/piDATA/zeta100.html.

[8] R. Sunseri. *Zeros of p-adic L-functions and densities relating to Bernoulli numbers*. PhD thesis, University of Illinois, 1979.

[9] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1991.

[10] Eric Weisstein. Mathworld. http://mathworld.wolfram.com/.