AMS/IP

Studies in Advanced Mathematics

Volume 27

Introduction to *p*-adic Analytic Number Theory

M. Ram Murty

American Mathematical Society • International Press

Introduction to *p*-adic Analytic Number Theory

Shing-Tung Yau, General Editor

2000 *Mathematics Subject Classification.* Primary 11–01, 11–02, 11E95, 11Sxx.

The quote on page v from Swami Vivekananda is reprinted with permission, from the *Complete Works of Swami Vivekananda*, Vol. 2, p. 227, Advaita Ashrama 5, Dehi Entally Road, Kolkatta 700 014, India. © Advaita Ashrama.

Library of Congress Cataloging-in-Publication Data

Murty, Maruti Ram.
Introduction to p-adic number theory / M. Ram Murty.
p. cm. — (AMS/IP studies in advanced mathematics, ISSN 1089-3288 ; v. 27)
Includes bibliographical references and index.
ISBN 0-8218-3262-X (alk. paper)
1. Number theory. 2. p-adic analysis. I. Title. II. Series.

QA241 M85 2002
512′.74—dc21 2002025584

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to `reprint-permission@ams.org`.

© 2002 by the American Mathematical Society and International Press. All rights reserved.
The American Mathematical Society and International Press retain all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: `http://www.ams.org/`
Visit the International Press home page at URL: `http://www.intlpress.com/`

10 9 8 7 6 5 4 3 2 1 07 06 05 04 03 02

One life runs through all like a continuous chain,
of which all these various forms represent the links,
link after link, extending almost infinitely,
but of the same one chain.

Vivekananda

Contents

	Preface	**ix**
1	**Historical Introduction**	**1**
2	**Bernoulli Numbers**	**9**
3	**p-adic Numbers**	**25**
4	**Hensel's Lemma**	**43**
5	**p-adic Interpolation**	**57**
6	**p-adic L-functions**	**71**
7	**p-adic Integration**	**87**
8	**Leopoldt's Formula for $L_p(1, \chi)$**	**99**
9	**Newton Polygons**	**113**
10	**An Introduction to Iwasawa Theory**	**135**
	Bibliography	**145**
	Index	**148**

Preface

Following Hensel's discovery in 1897 of the p-adic numbers, Ostrowski's theorem of 1918 classifying all the possible norms that one can define on the rational numbers has been the starting point of what is now called the adelic perspective. Loosely speaking, this means that the rational numbers should not be thought of as merely a subset of the real numbers but rather as a subset of a spectrum of topological fields obtained by completing the rational number field with respect to each of the possible norms. This adelic perspective has been a unifying theme in number theory ever since its conception in the 20th century. From this vantage point, all completions of the rationals must be treated "equally." It would seem then that what is traditionally called analytic number theory looks at only one completion, and ignores the non-archimedean (or p-adic) completions. In the latter half of the 20th century, this restricted viewpoint was enlarged through the foundational work of Kubota and Leopoldt and later by Iwasawa who established much of the groundwork of a p-adic analytic number theory. Thus, the search for p-adic incarnations of the classical zeta and L-functions is of relatively recent origin and has been a useful motif in the study of special values of various L-functions and their arithmetic significance. This perspective has also been a fertile program of research, largely inspired by the method of analogy with the archimedean context. As such, it is an exciting program to discover to what extent p-adic analogues of classical theorems and in some cases, the classical methods, exist.

This monograph is a modest introduction to the p-adic universe. Its aim is to acquaint the non-expert to the basic ideas of the theory and to invite the novice to engage in a fecund field of research. It grew out of a course given to senior undergraduates and graduate students at Queen's University during the fall semester of 2000-2001. That course was based on notes of a shorter course given at the Harish-Chandra Research Institute on p-adic analytic number theory from December 22, 1999 till January 12, 2000.

The prerequisites have been kept to a minimum. My goal is to introduce the novice student to a beautiful chapter in number theory. A background in basic algebra, analysis, elementary number theory and at least one course in complex analysis should suffice to understand the first nine chapters. The last chapter requires a little bit more background and is intended to give some inspiration for studying the subject at a deeper level. There are more than a hundred exercises in the book and their level varies. Most of them are routine and the students in the course were able to keep pace by doing them.

I would like to thank Alina Cojocaru, Fernando Gouvêa. Hershy Kisilevsky, Yu-Ru Liu, Kumar Murty, D.S. Nagaraj, and Lawrence Washington for their careful and critical reading of preliminary versions of these lecture notes. I also thank the students and post-doctoral fellows at Queen's who participated in the seminar and course out of which the monograph was born.

M. Ram Murty
Kingston, Ontario, Canada
January 2002

Chapter 1

Historical Introduction

There is a remarkable historical parallel between the proof of the prime number theorem and Fermat's Last Theorem. The prime number theorem is the assertion that the number of primes $p \leq x$, denoted $\pi(x)$, is asymptotic to $x/\log x$ as $x \to \infty$. Fermat's Last Theorem (FLT) predicts that the equation

$$x^p + y^p = z^p$$

for odd primes p has no non-trivial integer solutions. This was recently resolved by the work of Wiles and Ribet using a galaxy of ideas and techniques that can be traced to diverse areas of mathematics, most notably, number theory, algebraic geometry and representation theory.

It was in 1860 that Riemann wrote his fundamental (and only) paper in number theory outlining how one should prove the prime number theorem. The main tool, he wrote, should be the use of the ζ-function, defined as

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

as a function of a *complex* variable s. Riemann observes that the above series which converges absolutely for $Re(s) > 1$ is connected to prime numbers via the Euler product:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{1.1}$$

where the product is over prime numbers p. (1.1) can be viewed as an analytic formulation of the unique factorization theorem in the ring of integers $\mathbb{Z}$. In the same paper, Riemann shows that $\zeta(s)$ admits an analytic continuation for all complex values of $s \in \mathbb{C}$ apart from $s = 1$ where it has a simple pole. Moreover, he derives the functional equation

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

He then writes down, without proof, a remarkable explicit formula for $\pi(x)$ in terms of the zeros of the ζ function and explains that the main term $x/\log x$

really comes from the simple pole at $s = 1$. As is well-known, Riemann suggested that all the zeros ρ of $\zeta(s)$ in the region $0 \leq Re(s) \leq 1$ satisfy $Re(\rho) = 1/2$. This Riemann hypothesis is still an unsolved problem.

Most of Riemann's statements were simply assertions and his paper came to be viewed as a program to prove the prime number theorem. In fact, in the three decades after Riemann's paper had appeared, Hadamard had developed his theory of entire functions largely with the goal of proving the prime number theorem. Finally, in 1895, Hadamard and de la Vallée Poussin had independently proved the prime number theorem.

The key ingredients in their work were the analytic continuation of $\zeta(s)$ and the non-vanishing of $\zeta(s)$ on $Re(s) = 1$.

It is rather striking that around the same time, Kummer was developing his fundamental ideas on cyclotomic fields. His celebrated theorem that FLT holds for all primes p which are coprime to the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ was proved in a series of papers beginning in 1847. But how does one determine if p divides the class number h_p of $\mathbb{Q}(\zeta_p)$. Kummer derived a very beautiful criterion for this.

Define the Bernoulli numbers B_n by the power series

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

Then, $B_{2k+1} = 0$ for $k \geq 1$ and

$$B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_4 = -1/30, \quad B_6 = 1/42,$$

$$B_8 = -1/30, \quad B_{10} = 5/66, \quad B_{12} = -691/2730, \quad B_{14} = 7/6, ...$$

Earlier, Euler showed that $B_{2k} \neq 0$ and related them to the value of $\zeta(2k)$. Kummer proved that p divides h_p if and only if p divides the numerator of some B_k, $k = 2, 4, 6, ..., p-3$. For example,

$$x^{13} + y^{13} = z^{13}$$

has no non-trivial integral solutions because 13 does not divide the numerators of B_{2k} for $k \leq 5$.

A prime p is called a *regular* prime if p is coprime to h_p. It is still unknown if there are infinitely many such primes. Kummer derived his criterion for regularity by proving his famous congruences for the Bernoulli numbers: if

$n \not\equiv 0 (\bmod p-1)$ and $m \equiv n (\bmod p^a(p-1))$ with m, n even, then

$$(1.2) \qquad (1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} (\bmod p^{a+1}).$$

For $a = 0$, the Kummer congruences take the simpler form

$$(1.3) \qquad \frac{B_m}{m} \equiv \frac{B_n}{n} (\bmod p)$$

whenever $m \equiv n \not\equiv 0 (\bmod p-1)$, with m, n even.

Building on Kummer's work, Hensel developed systematically the theory of p-adic number fields in the early 1900's. He discovered the p-adic norm on the field of rational numbers and completed the field with respect to this norm. The full significance of this construction did not become clear until Ostrowski proved in 1918 his celebrated theorem, that essentially the only norms that can be defined on $\mathbb{Q}$ are the p-adic norms and the usual norm given by the absolute value. The familiar construction of the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ from the rational numbers can be imitated in the p-adic context. This gives rise to the field of p-adic numbers $\mathbb{Q}_p$ and after taking algebraic closure and then completions we get $\mathbb{C}_p$, the p-adic analogue of the complex numbers.

With the development of class field theory and the adelic viewpoint in place, it became clear that number theory should be studied at all completions simultaneously. This has been a guiding principle in the 50's and 60's in representation theory. It served, and still serves, as a useful beacon in number theory as well.

A significant development of this point of view was the interpretation of the Kummer congruences by Kubota and Leopoldt in 1964, more than 100 years after Riemann's 1860 paper. They discovered that the congruences imply the existence of a p-adic analogue of the Riemann ζ function.

Beginning with the observation that

$$\zeta(1-k) = -\frac{B_k}{k}$$

and the Kummer congruences, they showed the existence of a p-adic analytic function $\zeta_p(s)$ such that

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

Kubota and Leopoldt extended these constructions to define p-adic analogues of classical Dirichlet L-functions. Iwasawa discovered in the 1960's that cyclotomic fields and in particular, the growth of the p-part of the class groups of $\mathbb{Q}(\zeta_{p^n})$ can be efficiently studied through the analysis of the p-adic L-functions. In

the 1960's, Leopoldt discovered his famous class number formula for $L_p(1,\chi)$ generalizing to the p-adic context the classical formula of Dirichlet. This paved the way for further generalizations, namely to the study of elliptic curves, and special values of L-functions attached to modular forms. These generalizations figure prominently in the work of Wiles[Wi], for instance.

Despite the fact that FLT has been solved, there are still many unresolved issues emanating from Kummer's work. First and foremost is the existence of infinitely many regular primes. Siegel [Si] outlined a heuristic argument to indicate that the number of such primes $p \leq x$ is asymptotic to

$$\frac{x}{\sqrt{e}\log x}$$

as $x \to \infty$. Treating the $(p-3)/2$ Bernoulli numbers B_k for $k = 2, 4, ..., (p-3)$ as independent, and assuming the probability that p divides the numerator of B_k is $1/p$, we would expect that the probability that p is regular should be

$$\left(1 - \frac{1}{p}\right)^{(p-3)/2}$$

which tends to $1/\sqrt{e}$ as p tends to infinity. More generally, let $i(p)$ be the index of irregularity, namely the number of B_j, $j = 2, 4, ..., p-3$ whose numerators are divisible by p. The same heuristic reasoning leads to the prediction that the number of primes $p \leq x$ such that $i(p) = k$ is

$$\frac{x}{2^k k! \sqrt{e}\log x}$$

as x tends to infinity.

Then there is the Kummer - Vandiver conjecture that p is coprime to the class number of the maximal real subfield of $\mathbb{Q}(\zeta_p)$ which has still not been settled.

There is also a famous criterion of Wieferich indicating that if $2^{p-1} \not\equiv 1 (\bmod p^2)$ then the first case of FLT is true. It is still unknown at present if there are infinitely many primes p satisfying this condition or infinitely many not. Silverman [S] proved that if one assumes the ABC conjecture, there are infinitely many such primes. In these lectures, we will derive related results using p-adic methods. For instance, we will prove that $2^{p-1} \equiv 1 (\bmod p^2)$ if and only if the numerator of

$$1 + \frac{1}{2} + ... + \frac{1}{(p-1)/2}$$

is divisible by p, and this will then be related to the p-adic Hurwitz zeta function.

Since Silverman's theorem alluded to above is simple and elegant, we present it here as a means of motivating our study. First, let us recall the ABC conjecture. This says that for any $\epsilon > 0$, there is an absolute constant $\kappa(\epsilon)$ such that whenever there are three mutually coprime integers A, B, C, satisfying $A + B = C$, we have

$$\max(|A|, |B|, |C|) \leq \kappa(\epsilon) \left(\prod_{p|ABC} p \right)^{1+\epsilon}.$$

It is easy to see that this conjecture implies, for example, that FLT holds for sufficiently large p. This conjecture was formulated by Masser and Oesterlé [MO] around 1980. It has been shown by the author and Mai [MaMu] that it is equivalent to the degree conjecture in the theory of elliptic curves. Goldfeld and Szpiro [GS] (see also the correction by Rajan [Ra]) showed that it is essentially a conjecture about the estimation of the size of Shafarevich-Tate groups attached to elliptic curves over $\mathbf{Q}$.

Recall that a number m is called squarefull if whenever $p|m$ we have $p^2|m$. We begin by writing

$$2^n - 1 = u_n v_n$$

where u_n is squarefree and v_n is squarefull, $(u_n, v_n) = 1$. Note that if $p|u_n$, for some n, then

$$2^{p-1} \not\equiv 1 (\bmod p^2). \tag{1.4}$$

(Thus, primes satisfying (1.4) can be characterized as the prime divisors of the sequence u_n.) To see this, let d be the order of 2 mod p. Then, $de = p-1$ for some e and $dt = n$ for some t. Writing $2^d = 1 + kp$ we see that $2^n \equiv 1 + ktp (\bmod p^2)$ so that $(k, p) = 1$. Thus,

$$2^{p-1} = (1 + kp)^e \equiv 1 + kep (\bmod p^2)$$

and

$$2^{p-1} \not\equiv 1 (\bmod p^2).$$

By the ABC conjecture applied to $(2^n - 1) + 1 = 2^n$, with $A = 2^n - 1$, $B = 1$ and $C = 2^n$, we obtain

$$u_n v_n \ll (u_n v_n^{1/2})^{1+\epsilon}$$

so that $v_n \ll 4^{n\epsilon}$. It immediately follows that $u_n \to \infty$. Thus, there are infinitely many primes p such that

$$2^{p-1} \not\equiv 1 (\bmod p^2).$$

Moreover, for q prime, the sequence u_q is mutually coprime (see Exercise 1) and hence the number of such primes $p \leq x$ is at least

$$\gg \frac{\log x}{\log \log x}.$$

Now we consider the question of whether $u_n \to \infty$ can be proved unconditionally. If $n = 2k \geq 5$, we get

$$2^{2k} - u_{2k}v_{2k} = 1.$$

As v_{2k} is squarefull, we can write it as (see Exercise 2)

$$v_{2k} = a_{2k}^2 b_{2k}^3$$

and one can show that (see Exercise 3)

$$2^k - a_{2k}b_{2k}\sqrt{u_{2k}b_{2k}}$$

is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{u_{2k}b_{2k}})$. This leads to the question of whether, given a real quadratic field $\mathbb{Q}(\sqrt{D})$, the fundamental unit

$$\epsilon_D = t_D + u_D\sqrt{D}$$

satisfies $u_D \equiv 0 (\bmod D)$. We will return to this question and related questions later in these lectures.

We begin at a very elementary level and consider the problem of p-adic interpolation. This means that given a sequence of integers (say) a_k, does there exist a p-adically continuous function such that $f(k) = a_k$. The classical example of this problem involves the sequence of factorials $a_k = k!$ and the discovery of the Γ-function by Euler solves the interpolation problem over $\mathbb{C}$. We will begin our study with the p-adic analogue of the Γ function and use it to prove various results about congruences for binomial coefficents. We will also relate these results to Gauss sums, Jacobi sums via a result of Gross and Koblitz.

Then we will derive results concerning the p-adic ζ-function and L - functions. From this, we will derive Kummer's criterion for regularity. After discussing p-adic Hurwitz zeta functions, we will reconsider the Wieferich criterion in this context. We will also touch briefly upon the main theorems of Iwasawa theory concerning the growth of the p-part of the ideal class group of $\mathbb{Q}(\zeta_{p^n})$.

It is curious how Iwasawa came to construct his p-adic L-functions as characteristic polynomials of the Frobenius automorphism of the $\mathbb{Z}_p$ extension defined by the union of the cyclotomic fields $\mathbb{Q}(\zeta_{p^n})$. In this, he was motivated by the success of the theory of zeta functions of function fields over finite fields as developed by Weil. In fact, there is a letter from Weil to Artin in 1941 in Weil's collected papers. On the last page of that letter, Weil gives the starting idea of what is now called Iwasawa theory. Perhaps Weil mentioned this idea to Iwasawa when the latter was at the Institute in the late 1940's. In any case, Iwasawa's construction was an important step towards the understanding of the ζ-function of number fields.

More precisely, if h_n denotes the class number of $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$, let p^{e_n} be the highest power of p dividing h_n. In 1958, Iwasawa [Iw] proved that there exist integers λ, μ and ν, independent of n, such that

$$e_n = \lambda n + \mu p^n + \nu$$

for all n sufficiently large. He conjectured that $\mu = 0$ and this was subsequently proved by Ferrero and Washington [FW] in 1979. Thus, $e_n = \lambda n + \nu$.

In the course of proving his theorem, Iwasawa noticed that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$$

can be identified with the additive group $\mathbb{Z}_p$ of p-adic integers and that the topological generator

$$\gamma_0 : \zeta_{p^n} \mapsto \zeta_{p^n}^{1+p}$$

of the Galois group plays the role analogous to the Frobenius automorphism that generates $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. If A_n denotes the p-Sylow subgroup of the class group of K_n, the norm mapping from K_n to K_{n-1} induces a map from A_n to A_{n-1}. Let

$$X = \varprojlim A_n$$

be the inverse limit. Iwasawa felt that X (or more precisely, a piece of X) should play the role of a curve encountered in algebraic geometry over finite fields. X can be viewed as a module over the group ring

$$\varprojlim \mathbb{Z}[\mathrm{Gal}(K_n/K_0)] = \Lambda(\text{say}).$$

Iwasawa conjectured that the p-adic zeta function (that we will discuss in later chapters) attached to the totally real field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ should essentially be the characteristic polynomial of γ_0. Hence, the zeros of these p-adic zeta functions can be interpreted as eigenvalues of γ_0. This conjecture of Iwasawa (the "main" conjecture) was proved by Mazur and Wiles [MW] in 1980 using very delicate techniques from algebraic geometry. Thus, we have here another situation where the "Hilbert-Pólya" dream is realized, namely, the zeros of a zeta function are interpreted as the eigenvalues of an operator.

Exercises

1. For q prime, show that the sequence $u_q = 2^q - 1$ is a mutually coprime sequence. That is, show that u_q and $u_{q'}$ are coprime for distinct primes q and q'.
2. Show that any squarefull number can be written as a^2b^3.
3. Suppose that $2^{2n} - 1 = dy^2$ with d squarefree. Show that $2^n - y\sqrt{d}$ is a fundamental unit of $\mathbb{Q}(\sqrt{d})$. (Hint: see Exercise 8.3.3 of [EM].)

Chapter 2

Bernoulli Numbers

The Bernoulli numbers first made their appearance in a posthumous work *Ars Conjectandi* (1713) of Jacob Bernoulli (1654-1705). In that work, Bernoulli addressed the problem of finding a general formula for the sum

$$s_k(n) = 1^k + 2^k + \cdots + (n-1)^k.$$

However, the earliest known work that attacks the problem of finding a closed formula for $s_k(n)$ is the *Aryabhatiya* of Aryabhata (see [Cl, p. 38]) in the 5th century A.D. There, he derives the formulas for $k = 1, 2$ and 3. His writing reveals he was aware of the general method for deriving such formulas.

Recall that the Bernoulli numbers are defined by the power series

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

Consider the power series

$$\begin{aligned} \sum_{k=0}^{\infty} \frac{s_k(n) t^k}{k!} &= \sum_{k=0}^{\infty} \frac{t^k}{k!} \Big(\sum_{j=0}^{n-1} j^k \Big) \\ &= \sum_{j=0}^{n-1} e^{tj} = \frac{e^{nt} - 1}{e^t - 1}. \end{aligned}$$

Writing

$$\begin{aligned} \frac{e^{nt} - 1}{e^t - 1} &= \frac{e^{nt} - 1}{t} \frac{t}{e^t - 1} \\ &= \Big(\sum_{i=1}^{\infty} \frac{n^i t^{i-1}}{i!} \Big) \Big(\sum_{j=0}^{\infty} \frac{B_j t^j}{j!} \Big) \end{aligned}$$

and comparing coefficients of t^k on both sides gives the formula

$$(k+1) s_k(n) = \sum_{i=0}^{k} \binom{k+1}{i} B_i n^{k+1-i}.$$

By writing

$$\binom{k+1}{i} = \frac{k+1}{k+1-i}\binom{k}{i}$$

and changing variables, we get

$$s_k(n) = \sum_{i=0}^{k} \binom{k}{i} B_{k-i} \frac{n^{i+1}}{i+1}. \tag{2.1}$$

Thus, we see that $s_k(n)$ is a polynomial in n of degree $k+1$ involving the Bernoulli numbers as its coefficients.

We now define the n-th Bernoulli polynomial as

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

Then,

$$s_k(n) = \frac{1}{k+1}\Big(B_{k+1}(n) - B_{k+1}\Big).$$

It is also easy to see that we have the generating function

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

Since

$$\frac{t}{2} + \sum_{k=0}^{\infty} \frac{B_k t^k}{k!} = \frac{t}{2} + \frac{t}{e^t - 1} = \frac{t(e^t+1)}{2(e^t-1)}$$

and the right hand side is an even function of t, we deduce that $B_k = 0$ for k odd and ≥ 3.

In 1734, Euler discovered the beautiful formula

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

and more generally the formula

$$\sum_{n=-\infty}^{\infty}{}' \frac{1}{n^k} = -\frac{(2\pi\sqrt{-1})^k B_k}{k!}, \quad k \geq 2,$$

where the dash on the summation means we omit $n = 0$. For odd k, both sides of the equation are zero so we get no information about the values of $\zeta(s)$ for odd integers. However, for even k, we get a very elegant formula.

Euler's formula was based on the result

$$\sin \pi t = \pi t \prod_{n=1}^{\infty} \left(1 - \frac{t^2}{n^2}\right),$$

which can be viewed as analogous to the factorization of a polynomial in terms of its zeros. Taking logarithmic derivatives of both sides, we deduce the formula

$$\frac{\pi t \cos \pi t}{\sin \pi t} = 1 - 2\sum_{k=1}^{\infty} \zeta(2k) t^{2k}.$$

On the other hand, the left hand side is

$$\begin{aligned} \frac{\pi t i(e^{i\pi t} + e^{-i\pi t})}{e^{i\pi t} - e^{-i\pi t}} &= \frac{\pi t i(e^{2\pi i t} + 1)}{e^{2\pi i t} - 1} \\ &= \pi t i + \frac{2\pi i t}{e^{2\pi i t} - 1} \\ &= \pi t i + \sum_{k=0}^{\infty} \frac{B_k (2\pi i)^k t^k}{k!} \end{aligned}$$

from which Euler's formula is easily derived.

Several consequences can be deduced from this. First, $(-1)^k B_{2k} < 0$ for $k \geq 0$, so that the B_{2k}'s alternate in sign. Since $\zeta(2k) \to 1$ as $k \to \infty$, we also deduce that

$$|B_{2k}| \sim \frac{2(2k)!}{(2\pi)^{2k}}.$$

In particular, using the obvious inequality $e^k > k^k/k!$, we deduce that

$$|B_{2k}| > 2(k/\pi e)^{2k}$$

so that

$$|B_{2k}/2k| \to \infty \tag{2.2}$$

as $k \to \infty$.

In view of the functional equation for the Riemann zeta function, Euler's formula can be rewritten in a simpler way as

$$\zeta(1-k) = -\frac{B_k}{k}, \tag{2.3}$$

and it is this formulation that gains significance in the 1964 work of Kubota and Leopoldt .

There is an amusing way of deriving (2.3). We have

$$\begin{aligned}\sum_{k=0}^{\infty}\zeta(-k)\frac{t^k}{k!} &= \sum_{k=0}^{\infty}\Big(\sum_{n=1}^{\infty}n^k\Big)\frac{t^k}{k!}\\ &= \sum_{n=1}^{\infty}e^{nt} = \frac{e^t}{1-e^t}\\ &= -1-\frac{1}{e^t-1}\end{aligned}$$

from which (2.3) easily follows. Of course, none of the sums above are convergent and the argument is not rigorous. However, the argument can be made rigorous in the following way.

Recall that the Γ-function is defined for $Re(s) > 0$ by the integral

$$\Gamma(s) = \int_0^{\infty} e^{-x}x^{s-1}dx.$$

By integration by parts, we see that $\Gamma(s)$ satisfies the functional equation $\Gamma(s+1) = s\Gamma(s)$ which can be used to derive the meromorphic continuation of it for all $s \in \mathbb{C}$. By an application of Stirling's formula and the calculus of residues, we have

$$e^{-x} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} x^{-s}\Gamma(s)ds,$$

since $\Gamma(s)$ has simple poles at $s = -k$ for $k = 0, 1, 2, \ldots$ and residue $(-1)^k/k!$ at $s = -k$. If now $F(s) = \sum_{n=1}^{\infty} a_n/n^s$ is a Dirichlet series absolutely convergent for $Re(s) > 1$, then we get

$$\sum_{n=1}^{\infty} a_n e^{-nx} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} x^{-s}F(s)\Gamma(s)ds.$$

In particular,

$$\sum_{n=1}^{\infty} e^{-nx} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} x^{-s}\zeta(s)\Gamma(s)ds.$$

The left hand side is

$$\frac{1}{e^x-1}.$$

By moving the line of integration to the left to $-\infty$, the right hand side becomes

$$\frac{1}{x} + \sum_{k=0}^{\infty}\frac{x^k(-1)^k\zeta(-k)}{k!}. \tag{2.4}$$

Moreover, by the functional equation and Stirling's formula,

$$|\zeta(-k)| \le Ce^{k\log k}.$$

As $k! \sim e^{k \log k - k + O(\log k)}$, we deduce that the power series in (2.4) converges in a small enough disc so that we can compare coefficients and deduce (2.3).

This argument can be extended to obtain similar results for the Dirichlet L-functions, and Hurwitz zeta functions. The precise details are contained in a paper by the author and Marilyn Reece [MR].

Though the 'naive' derivation above leads to the correct formula but requires complex analysis, analytic continuation and functional equation of the ζ-function for its justification, it is possible to derive the analytic continuation and derive (2.3) in a much more elementary fashion as described in [MR]. Recall that the Riemann ζ-function, originally defined by the Dirichlet series

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

for $Re(s) > 1$. Let us denote by $[x]$ the number of positive integers less than or equal to x. By partial summation,

$$\zeta(s) = s \int_1^{\infty} \frac{[x]}{x^{s+1}} dx = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{x\}}{x^{s+1}} dx,$$

where $\{x\}$ denotes the fractional part of x. This gives the analytic continuation of $\zeta(s)$ for $Re(s) > 0$. We can now proceed inductively. Writing

$$\int_1^{\infty} \frac{\{x\}}{x^{s+1}} dx = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{x-n}{x^{s+1}} dx = \sum_{n=1}^{\infty} \int_0^1 \frac{u du}{(u+n)^{s+1}}$$

and integrating the last integral by parts, we get

$$\sum_{n=1}^{\infty} \int_0^1 \frac{u du}{(u+n)^{s+1}} = \frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{(n+1)^{s+1}} + \frac{(s+1)}{2} \int_1^{\infty} \frac{\{x\}^2}{x^{s+2}} dx$$

and the latter integral converges for $Re(s) > -1$. That is,

$$\zeta(s) = \frac{s}{s-1} - \frac{s}{2}(\zeta(s+1) - 1) - \frac{s(s+1)}{2} \int_1^{\infty} \frac{\{x\}^2}{x^{s+2}} dx$$

from which we infer that $\zeta(0) = -1/2$. Thus, inductively, we deduce

$$\zeta(s) = 1 + \frac{1}{s-1} - \sum_{r=1}^{m} \frac{s(s+1)\cdots(s+r-1)}{(r+1)!} \Big(\zeta(s+r) - 1\Big)$$

$$- \frac{s(s+1)\cdots(s+m)}{(m+1)!} \sum_{n=1}^{\infty} \int_0^1 \frac{u^{m+1} du}{(u+n)^{s+m+1}}$$

and the infinite sum on the right hand side converges for $Re(s) > -m$. This derivation, though not well-known, is not new. For example, it is found in [Ap]. However, the idea of deriving the special values of $\zeta(1-k)$ from it, seems to have not been noticed before. Indeed, if in the above, we put $s = 1-m$, and note that for $r = m$, $\zeta(s+m)$ has a simple pole at $s = 1-m$, we obtain the recurrence

$$\zeta(1-m) = 1 - \frac{1}{m} + \frac{(-1)^m}{m(m+1)} - \sum_{r=1}^{m-1}(-1)^r\binom{m-1}{r}\frac{1}{r+1}\Big(\zeta(1-m+r)-1\Big).$$

By integrating the expression

$$(1-x)^{m-1} = \sum_{r=0}^{m-1}\binom{m-1}{r}(-1)^r x^r$$

we deduce

$$\frac{1-(1-x)^m}{m} = \sum_{r=0}^{m-1}\binom{m-1}{r}(-1)^r\frac{x^{r+1}}{r+1}.$$

Putting $x = 1$ gives

$$\frac{1}{m} = \sum_{r=0}^{m-1}\binom{m-1}{r}\frac{(-1)^r}{r+1}$$

so that we obtain:

Theorem 2.1 *For positive integers m,*

$$m\zeta(1-m) = \frac{(-1)^m}{(m+1)} - m\sum_{r=1}^{m-1}(-1)^r\binom{m-1}{r}\frac{1}{r+1}\zeta(1-m+r).$$

Since

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}\frac{B_k t^k}{k!},$$

we easily deduce the recurrence

$$\sum_{k=0}^{n}\binom{n}{k}\frac{B_{n-k}}{k+1} = 0$$

for $n \geq 1$. Our goal now is to prove:

Theorem 2.2 *For $k \geq 2$,*

$$\zeta(1-k) = -\frac{B_k}{k}.$$

To this end, we will apply induction using Theorem 2.1. Since

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

is an even function, the Bernoulli numbers for odd subscripts ≥ 3 vanish, and we can rewrite the above equation as

$$\zeta(1-k) = (-1)^{k-1}\frac{B_k}{k}.$$

Then, by induction, we see that the right hand side of the formula in Theorem 2.1 becomes

$$\frac{(-1)^m}{m+1} + (-1)^m \sum_{r=1}^{m-2} \binom{m}{r} \frac{B_{m-r}}{r+1} - (-1)^{m-1}\zeta(0).$$

It is immediate that this reduces to

$$\frac{(-1)^m}{m+1} - (-1)^m\Big(B_m + B_1 + \frac{B_0}{m+1}\Big) - \frac{(-1)^m}{2} = (-1)^{m-1}B_m$$

by virtue of the fact that $\zeta(0) = -1/2$. The result is now immediate.

Our goal now is to derive the Kummer congruences and lay the foundations for the p-adic interpolation of the Riemann zeta function. We will say that a rational number a/b with $(a,b) = 1$ is p-integral if p is coprime to b. Given any rational number r, we can write it as $p^u a_1/b_1$ with $(p, a_1 b_1) = 1$ which determines the integer u uniquely. We define $\mathrm{ord}_p r$ to be u. Sometimes we also use the notation $v_p(r)$ to designate u. We now begin with:

Lemma 2.3 *Let p be a prime number. Then pB_k is p-integral.*

Proof. We induct on k. We set $n = p$ in (2.1) and write it as

$$s_k(p) = pB_k + \sum_{i=1}^{k} \binom{k}{i} (pB_{k-i}) \frac{p^i}{i+1}.$$

Since $p^i \geq 2^i \geq i+1$, we see that $\mathrm{ord}_p(p^i/i+1) \geq 0$ and by induction, each of pB_{k-i} is p-integral in the sum. Since $s_k(p)$ is an integer, it follows that pB_k is p-integral. ∎

Corollary 2.4 *Let $B_k = U_k/V_k$ with $(U_k, V_k) = 1$. Then V_k is squarefree.*

Proof. If $p^2|V_k$ for some prime p, then pB_k will still have a denominator divisible by p. ∎

We can sharpen the argument of Lemma 2.3 to deduce

Lemma 2.5 *If k is even and ≥ 2, then*

$$pB_k \equiv s_k(p)(\bmod p).$$

Proof. If k is even and ≥ 4, then $k-1$ is odd and ≥ 3 so that

$$s_k(p) = pB_k + p\sum_{i=2}^{k}\binom{k}{i}(pB_{k-i})\frac{p^{i-1}}{i+1}.$$

By an easy argument (see Exercise 3) as before, $p^{i-1}/(i+1)$ is p-integral and by Lemma 2.3, we obtain $s_k(p) \equiv pB_k(\bmod p)$, for $k \geq 4$. For $k = 2$, $B_2 = 1/6$ and the result is verified directly. ∎

We also have the elementary:

Lemma 2.6 *If $(p-1)\nmid k$, then $s_k(p) \equiv 0(\bmod p)$. If $(p-1)|k$, then $s_k(p) \equiv -1(\bmod p)$.*

Proof. Let g be a primitive root mod p. Then, if $p-1$ does not divide k,

$$s_k(p) \equiv \sum_{j=0}^{p-2}(g^j)^k \equiv \frac{g^{k(p-1)}-1}{g^k-1}(\bmod p)$$

and the numerator is 0 mod p. In the case $(p-1)|k$, we find by Fermat's little theorem that the sum $s_k(p) \equiv p-1 \equiv -1(\bmod p)$ as desired. ∎

We can now deduce the famous

Theorem 2.7 (von Staudt - Clausen) *For k even,*

$$B_k + \sum_{(p-1)|k}\frac{1}{p} \in \mathbb{Z}.$$

Proof. If $p-1$ does not divide k, then Lemma 2.6 implies that $s_k(p) \equiv 0(\bmod p)$ so that by Lemma 2.5, p does not divide V_k, the denominator of B_k. If $p-1$ divides k, then again by Lemma 2.6, $s_k(p) \equiv -1(\bmod p)$ so that by

Lemma 2.5, we get $pB_k \equiv -1 (\bmod p)$. Therefore, p necessarily divides V_k. Thus, the primes dividing V_k are precisely those primes p such that $p-1|k$. Hence,

$$B_k + \frac{1}{p}$$

is p-integral for every p such that $(p-1)|k$ which completes the proof. ∎

Remark. It is suggestive to think of B_k as having 'simple poles' at primes p such that $(p-1)|k$ and the sum in the theorem can be viewed as the 'polar' part of B_k. Also observe that $6|V_k$ for all even $k \geq 2$.

We now deduce the Voronoi congruences from which the Kummer congruences will follow. It seems that Voronoi proved them while a student in 1889.

Theorem 2.8 *Let k be even and ≥ 2. Then,*

$$V_k s_k(n) \equiv U_k n \pmod{n^2}.$$

Proof. As before, we write from (2.1),

$$s_k(n) = B_k n + \Big(\sum_{i=2}^{k} \binom{k}{i} B_{k-i} \frac{n^{i-1}}{i+1}\Big) n^2. \tag{2.5}$$

The sum

$$\sum_{i=4}^{k} \binom{k}{i} (B_{k-i} n) \frac{n^{i-2}}{i+1}$$

is p-integral for $p \geq 3$ since $p^{i-2} \geq 3^{i-2} \geq 1 + 2(i-2) = 2i - 3 \geq i + 1$. To prove the theorem, we study p-integrality of the expression for primes $p|n$. Also for $p \geq 5$, the term corresponding to $i = 2$ is

$$\binom{k}{2} B_{k-2} \frac{n}{3}$$

is p-integral. Multiplying the equation (2.5) by V_k and recalling that $6|V_k$, we see that

$$V_k \binom{k}{2} B_{k-2} \frac{n}{3}$$

is 3-integral when $3|n$. Finally, note that $2^{i-2} \geq (i+1)/2$ for $i \geq 4$ so that

$$V_k \Big(\sum_{i=4}^{k} \binom{k}{i} (B_{k-i} n) \frac{n^{i-2}}{i+1}\Big)$$

is 2-integral when $2|n$ since $2|V_k$. In addition,

$$V_k\binom{k}{2}B_{k-2}\frac{n}{3}$$

is clearly 2-integral. Therefore, we see that the sum in brackets in (2.5) when multiplied by V_k is p-integral for all $p|n$. This completes the proof. ∎

Theorem 2.9 (Voronoi, 1889) *Let n be a natural number and $(a,n)=1$. Then,*

$$(a^k-1)s_k(n) \equiv kna^{k-1}\sum_{j=1}^{n-1}[ja/n]j^{k-1} \pmod{n^2}.$$

Proof. For each j satisfying $1 \le j < n$, write $ja = q_jn + r_j$ where $0 \le r_j < n$. Then, $q_j = [ja/n]$ and we have

$$\begin{aligned}(ja)^k &\equiv r_j^k + kq_jnr_j^{k-1} \pmod{n^2}\\ &\equiv r_j^k + kq_jn(ja)^{k-1} \pmod{n^2}.\end{aligned}$$

As j ranges over the integers from 1 to $n-1$ so does r_j because $(a,n)=1$. Therefore, summing the above congruence from $j=1$ to $n-1$ gives the required result. ∎

Corollary 2.10

$$(a^k-1)U_k \equiv kV_ka^{k-1}\sum_{j=1}^{n-1}[ja/n]j^{k-1} \pmod{n}. \tag{2.6}$$

Proof. Obvious from Theorem 2.8 and Theorem 2.9. ∎

Theorem 2.11 (Adams congruences) *If $p-1$ does not divide k, then B_k/k is p-integral.*

Proof. If $p^t|k$, then by Corollary 2.10 with $n=p^t$, we deduce, $(a^k-1)U_k \equiv 0 \pmod{p^t}$. Choosing a to be a primitive root mod p, we can ensure that p is coprime to a^k-1 so that U_k is divisible by p^t. ∎

Theorem 2.12 (Kummer congruences) *Let $k \ge 2$ be even, p prime such that $p-1$ does not divide k. If $k \equiv k' \pmod{\phi(p^e)}$, then*

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \pmod{p^e}.$$

Proof. Let $t = \mathrm{ord}_p k$ and write $B_k = U_k/V_k$ as before. In (2.6), we set $n = p^{e+t}$ to get

$$(a^k - 1)U_k \equiv kV_k a^{k-1} \sum_{j=1}^{p^{e+t}-1} [ja/p^{e+t}]j^{k-1} (\mathrm{mod}\, p^{e+t}).$$

Since $(p-1)\nmid k$, V_k and p are coprime. By Theorem 2.11, $p^t | U_k$ so that

$$(a^k - 1)\frac{B_k}{k} \equiv a^{k-1} \sum_{j=1}^{p^{e+t}-1} [ja/p^{e+t}]j^{k-1} (\mathrm{mod}\, p^e). \tag{2.7}$$

We begin with the case $e = 1$. On the right hand side of the above congruence, we can omit those j divisible by p since $e = 1$. Since $k \equiv k' (\mathrm{mod}\, p-1)$, we find $j^{k-1} \equiv j^{k'-1} (\mathrm{mod}\, p)$ for j coprime to p. Choosing a to be a primitive root (mod p), we deduce

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} (\mathrm{mod}\, p).$$

When $e > 1$, we write

(2.8)

$$\sum_{j=1}^{p^{e+t}-1} [ja/p^{e+t}]j^{k-1} = \sum_{\substack{j=1 \\ (j,p)=1}}^{p^{e+t}-1} [ja/p^{e+t}]j^{k-1} + p^{k-1} \sum_{j=1}^{p^{e+t-1}-1} [ja/p^{e+t-1}]j^{k-1}.$$

The congruence (2.7) with e replaced by $e-1$ gives for $k \geq 2$,

$$p^{k-1}(a^k - 1)\frac{B_k}{k} \equiv p^{k-1} a^{k-1} \sum_{j=1}^{p^{e+t-1}-1} [ja/p^{e+t-1}]j^{k-1} (\mathrm{mod}\, p^e)$$

so that (2.8) becomes

$$(1 - p^{k-1})(a^k - 1)\frac{B_k}{k} \equiv a^{k-1} \sum_{\substack{j=1 \\ (j,p)=1}}^{p^{e+t}-1} [ja/p^{e+t}]j^{k-1} (\mathrm{mod}\, p^e).$$

For $k \equiv k' (\mathrm{mod}\, \phi(p^e))$, we deduce the desired congruences. This completes the proof of the theorem. ∎

Remark. The value

$$(1 - p^{k-1})\frac{B_k}{k}$$

can be interpreted as $\zeta(1-k)$ with the p-Euler factor removed.

A prime p will be called *regular* if it does not divide any of the numerators of the B_k with k even and $\leq p-3$. (Later, we will prove Kummer's theorem that

this is equivalent to p being coprime to the class number of the p-th cyclotomic field.) If p is not regular, we will call it irregular. It is still unknown if there are infinitely many regular primes. We have, however, the following.

Theorem 2.13 *There are infinitely many irregular primes.*

Proof. Suppose not. Let $p_1, ..., p_s$ be the set of irregular primes. Let k be even and set $n = k(p_1 - 1)...(p_s - 1)$ if $s \geq 1$. Otherwise, set $n = k$. By (2.2), $|B_n/n| \to \infty$ as $k \to \infty$ so we can choose k sufficiently large so that $|B_n/n| > 1$. Let p be a prime so that $\mathrm{ord}_p(B_n/n) > 0$. By von Staudt-Clausen theorem (Theorem 2.7), we have $(p-1) \nmid n$. Thus, $p \neq p_i$ for $1 \leq i \leq s$ and $p \neq 2$. We now show that p is irregular. Indeed, let $n \equiv m (\mathrm{mod}\, p-1)$ with $m < (p-1)$ since $p-1$ does not divide n. Moreover, m is even because n is even. By the Kummer congruences,

$$\frac{B_n}{n} \equiv \frac{B_m}{m} (\mathrm{mod}\, p)$$

so that $\mathrm{ord}_p(B_m/m) > 0$. Hence, $\mathrm{ord}_p(B_m) > 0$ as claimed. This completes the proof. ∎

The prime 691 is irregular since it divides the numerator of B_{12}. The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, and 157 which in fact divides the numerators of two distinct Bernoulli numbers B_{2k} with $k \leq 77$.

Exercises

1. Let p be prime and define for each non-zero rational number $v_p(x)$ by the equation $x = p^{v_p(x)} x_1$ where x_1 is a rational number coprime to p. Define the p-adic metric by $||x|| = p^{-v_p(x)}$ and set $||0|| = 0$. Show that

$$||x + y|| \leq \max(||x||, ||y||).$$

2. With $|| \cdot ||$ as in the previous exercise, does the limit $\lim_{n \to \infty} ||n!||$ exist? What is the limit?

3. Prove that

$$v_p\left(\frac{p^{i-1}}{i+1}\right) \geq 0$$

for $i \geq 2$.

4. Prove that
$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k(x)t^k}{k!},$$
where $B_k(x)$ denotes the k-th Bernoulli polynomial. Deduce that
$$B_k(1-x) = (-1)^k B_k(x).$$

5. Let A be an abelian group. The **exponent** of A is defined to be the smallest positive integer e such that $x^e = 1$ for all $x \in A$. If e is the exponent of A, show that A has an element of order e.

6. Let p be prime and let $1 \leq a \leq p-1$. Set $F(a) = (a^{p-1} - 1)/p$. Prove that
$$F(ab) \equiv F(a) + F(b) \pmod{p}.$$

7. Prove the following generalization of Wilson's theorem:
$$(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$$
for $1 \leq k \leq p-1$.

8. If p is an odd prime, show that $2^{p-1} \equiv 1 \pmod{p^2}$ if and only if the numerator of
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1}$$
is divisible by p.

9. With F as in Exercise 6, show that
$$F(a+pt) \equiv F(a) - a't \pmod{p}$$
where $aa' \equiv 1 \pmod{p}$.

10. Let $[x]$ denote the greatest integer less than or equal to x. For $1 \leq a \leq p-1$, show that
$$\frac{a^p - a}{p} \equiv \sum_{j=1}^{p-1} \frac{1}{j} \left[\frac{aj}{p}\right] \pmod{p}.$$

11. Let $n = 2k+1$ be an odd positive integer. Prove by induction that

$$\sin nx = P_n(\sin x), \qquad \frac{\cos nx}{\cos x} = Q_{n-1}(\sin x),$$

for polynomials P_n and Q_n of degree at most n, with integer coefficients. [Hint: apply induction.]

12. Show that for $n = 2k+1$ an odd positive integer, we have

$$\frac{\sin nx}{n \sin x} = 1 + a_1 \sin x + a_2 \sin^2 x + \cdots a_{2k} \sin^{2k} x$$

for certain rational numbers a_i.

13. Using the previous exercise, show that for $n = 2k+1$,

$$\frac{\sin nx}{n \sin x} = \prod_{r=1}^{k} \left(1 - \frac{\sin^2 x}{\sin^2 \frac{\pi r}{n}}\right).$$

Deduce that

$$\frac{\sin \pi x}{n \sin(\pi x/n)} = \prod_{r=1}^{k} \left(1 - \frac{\sin^2 \frac{\pi x}{n}}{\sin^2 \frac{\pi r}{n}}\right).$$

14. Let $n = 2k+1$. Show that

$$\prod_{r=1}^{k} \left(1 - \frac{\sin^2 \frac{\pi x}{n}}{\sin^2 \frac{\pi r}{n}}\right) \left(1 - \frac{x^2}{r^2}\right)^{-1} \to 1$$

as $k \to \infty$.

15. From the previous exercise, deduce that

$$\frac{\sin \pi x}{\pi x} = \prod_{r=1}^{\infty} \left(1 - \frac{x^2}{r^2}\right).$$

16. For $0 < x \leq 1$, define the Hurwitz ζ-function by the series

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

First, prove that the series converges for $Re(s) > 1$. Then, by noting that

$$-\frac{1}{x^s} + \zeta(s,x) - \zeta(s) = \sum_{n=1}^{\infty} \left(\frac{1}{(n+x)^s} - \frac{1}{n^s} \right),$$

and writing the summand as

$$\frac{1}{n^s} \left(\left(1 + \frac{x}{n}\right)^{-s} - 1 \right)$$

show that

$$-\frac{1}{x^s} + \zeta(s,x) - \zeta(s) = \sum_{r=1}^{\infty} \binom{-s}{r} \zeta(s+r) x^r.$$

Deduce that $(s-1)\zeta(s,x)$ extends to an entire function of s and that

$$\lim_{s \to 1} (s-1)\zeta(s,x) = 1.$$

17. Deduce from the previous exercise that

$$\zeta(1-k,x) = -\frac{B_k(x)}{k}$$

for every integer $k \geq 1$.

18. With the notation of Exercise 6, show that

$$\sum_{a=1}^{p-1} F(a) \equiv \frac{(p-1)!+1}{p} \pmod{p},$$

for p prime.

19. Show that

$$s_{p-1}(p) \equiv pB_{p-1} \pmod{p^2}$$

for p a prime, and $s_k(p) = 1^k + 2^k + \cdots (p-1)^k$, as usual.

20. Deduce from the previous exercises that $(p-1)! + 1 \equiv 0 \pmod{p^2}$ if and only if the numerator of

$$B_{p-1} + \frac{1}{p} - 1$$

is divisible by p.

Chapter 3

p-adic Numbers

A *norm* on a field F is a map $||\cdot|| : F \to \mathbb{R}_+$ such that
(i) $||x|| = 0$ if and only if $x = 0$;
(ii) $||xy|| = ||x||||y||$;
(iii) $||x + y|| \leq ||x|| + ||y||$ (triangle inequality).

We can always define a 'trivial' norm by setting $||0|| = 0$ and $||x|| = 1$ for $x \neq 0$. We usually discard this norm and study non-trivial norms. Let us also make one more 'trivial' remark. Note that in a field F where $0 \neq 1$ (that is, the additive identity does not coincide with the multiplicative identity), we have by (ii) that $||1|| = 1$. Thus, $||-1||^2 = 1$ so that $||-1|| = 1$. Therefore $||-x|| = ||x||$.

Given a norm, we can define a metric on F by setting the distance between x and y as $d(x, y) = ||x - y||$. The usual absolute value is a norm on $\mathbb{Q}$ and the corresponding metric is the usual distance function. But we can construct other norms on $\mathbb{Q}$ in the following way. Let p be a prime number and for each rational number $x \neq 0$, write $x = p^{v_p(x)}x_1$ where x_1 is a rational number coprime to p (that is, when x_1 is written in lowest terms, both the numerator and denominator are coprime to p). Define the p-adic absolute value of x, denoted $|x|_p$ as

$$|x|_p = p^{-v_p(x)}.$$

For $x = 0$, we set $|0|_p = 0$. It is easily checked that $|\cdot|_p$ is a norm on $\mathbb{Q}$. In fact, (iii) is satisfied in the sharper form

$$|x + y|_p \leq \max(|x|_p, |y|_p), \tag{3.1}$$

as is easily verified. Equality holds in (3.1) whenever $|x|_p \neq |y|_p$. This property is often phrased as the theorem that "all p-adic triangles are isosceles" or somewhat metaphorically as "the stronger one wins" since $|x|_p > |y|_p$ implies $|x+y|_p = |x|_p$. Observe that in this metric, the sequence $p^n \to 0$ as $n \to \infty$. Thus, the norm measures divisibility by powers of p and is therefore ideal in the study of congruences. It allows us to bring the notions of analysis into the study of congruences.

Two metrics d_1 and d_2 are said to be *equivalent* if they induce the same

topology on F. Two norms are said to be *equivalent* if their induced metrics are equivalent.

If $0 < c < 1$ and p is prime, we can define for $x \neq 0$,

$$||x|| = c^{v_p(x)},$$

and $||0|| = 0$. It is then easy to see that this norm is equivalent to $|\cdot|_p$.

We have the following celebrated theorem of Ostrowski which says that up to equivalence the only norms on $\mathbb{Q}$ are the p-adic norms or the usual norm given by absolute value.

Theorem 3.1 (Ostrowski, 1918) *Every non-trivial norm $||\cdot||$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or the usual absolute value.*

Proof. Case (1): suppose that $||n|| \leq 1$ for all integers n. Since the norm is non-trivial, there is an n such that $||n|| < 1$. Moreover, since $||-n|| = ||n||$, we may assume n is positive. Let n_0 be the least such positive n. Then n_0 must be prime by property (ii). Say $n_0 = p$. If q is a prime $\neq p$, then we claim that $||q|| = 1$. If not, then $||q|| < 1$ and for sufficiently large N, $||q^N|| < 1/2$. Similarly, for sufficiently large M, $||p^M|| < 1/2$. Since p^M and q^N are coprime, we can find integers u and v such that

$$up^M + vq^N = 1.$$

Hence,

$$1 = ||up^M + vq^N|| \leq ||u||||p^M|| + ||v||||q^N|| < 1/2 + 1/2 = 1,$$

a contradiction. Therefore, $||q|| = 1$. Write then $c = ||p||$. Then, $||n|| = c^{v_p(n)}$ and this metric is equivalent to $|\cdot|_p$. Case (2): suppose there is a natural number n such that $||n|| > 1$. Let n_0 be the least such. Then $n_0 > 1$. Write $||n_0|| = n_0^\alpha$ for some α. Given a natural number n, let us write it in base n_0:

$$n = a_0 + a_1 n_0 + \cdots + a_s n_0^s, \quad 0 \leq a_i < n_0,$$

with $a_s \neq 0$. Notice that $||a_i|| \leq 1$, by the definition of n_0. By the triangle inequality,

$$\begin{aligned}
||n|| &\leq ||a_0|| + ||a_1 n_0|| + \cdots + ||a_s n_0^s|| \\
&\leq ||a_0|| + ||a_1||n_0^\alpha + \cdots + ||a_s||n_0^{\alpha s} \\
&\leq 1 + n_0^\alpha + \cdots + n_0^{\alpha s} \\
&\leq n_0^{\alpha s}\Big(1 + \frac{1}{n_0^\alpha} + \frac{1}{n_0^{2\alpha}} + \cdots\Big) \\
&\leq n_0^{\alpha s}\Big(1 + \frac{1}{2^\alpha} + \frac{1}{2^{2\alpha}} + \cdots\Big) = C n_0^{\alpha s},
\end{aligned}$$

by the choice of n_0 and with C a constant independent of n_0. Since $n \geq n_0^s$, we deduce for all natural numbers n,

$$||n|| \leq Cn^\alpha,$$

for some absolute constant $C \geq 1$. Thus, $||n^N|| \leq Cn^{N\alpha}$ and so $||n|| \leq C^{1/N}n^\alpha$. Letting $N \to \infty$ gives $||n|| \leq n^\alpha$ for all natural numbers n. We can also deduce the reverse inequality. Since $n_0^{s+1} > n \geq n_0^s$, we have

$$\begin{aligned} ||n_0^{s+1}|| &= ||n + n_0^{s+1} - n|| \\ &\leq ||n|| + ||n_0^{s+1} - n|| \end{aligned}$$

by the triangle inequality. Thus,

$$\begin{aligned} ||n|| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \\ &\geq n_0^{(s+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\ &\geq C_1 n^\alpha \end{aligned}$$

for some constant C_1. Arguing as before, we deduce that $||n|| \geq n^\alpha$. Thus, $||n|| = n^\alpha$ which is equivalent to the usual absolute value. ∎

Given a field F with norm $||\cdot||$, let R be the set of all sequences $\{a_n\}_{n=1}^\infty$, $a_n \in F$, which are Cauchy with respect to the norm $||\cdot||$. One can define addition and multiplication of sequences pointwise, by setting

$$\{a_n\}_{n=1}^\infty + \{b_n\}_{n=1}^\infty = \{a_n + b_n\}_{n=1}^\infty$$

$$\{a_n\}_{n=1}^\infty \times \{b_n\}_{n=1}^\infty = \{a_n b_n\}_{n=1}^\infty.$$

Then, $(R, +, \times)$ is a commutative ring. Moreover, the subset $\mathfrak{m}$ of R consisting of null Cauchy sequences, that is sequences converging to zero, is a maximal ideal. Consequently, $R/\mathfrak{m}$ is a field.

We can embed F in R via the map $a \mapsto (a, a, ...)$ which is clearly a Cauchy sequence. We can therefore view F as a subfield of $R/\mathfrak{m}$. $R/\mathfrak{m}$ is called the completion of F with respect to $||\cdot||$. In case, $F = \mathbb{Q}$ with the usual absolute value, this construction gives the field of real numbers. If $F = \mathbb{Q}$, with norm $|\cdot|_p$, we get the field, designated $\mathbb{Q}_p$, of p-adic numbers.

We can extend the concept of norm to $\mathbb{Q}_p$ in the following way. Given any sequence $a = \{a_n\}_{n=1}^\infty$ in $\mathbb{Q}_p$ (or more precisely an equivalence class of

sequences), we observe that $\{|a_n|_p\}_{n=1}^{\infty}$ is a Cauchy sequence of real numbers and as $\mathbb{R}$ is complete, the sequence has a limit. So we define

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

It is easily checked that this is well-defined. Moreover, $\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$. Indeed, let $\{a^{(j)}\}_{j=1}^{\infty}$ be a Cauchy sequence of equivalence classes in $\mathbb{Q}_p$. We must show that there is a Cauchy sequence to which it converges. To do this, observe that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ (exercise). Thus, we can find rational numbers $\lambda^{(j)}$ so that

$$\lim_{n\to\infty} |a^{(j)} - \lambda^{(j)}|_p = 0,$$

where we interpret $\lambda^{(j)}$ as the constant sequence in $\mathbb{Q}_p$. It is now not hard to show that the sequence of rational numbers $\lambda^{(j)}$ is a Cauchy sequence in $\mathbb{Q}$ and letting λ denote the element of $\mathbb{Q}_p$ corresponding to this sequence we deduce that

$$\lim_{j\to\infty} a^{(j)} = \lambda.$$

We leave the details as an exercise.

The set

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

is a subring of $\mathbb{Q}_p$ called the ring of p-adic integers. Sometimes, we write $|\cdot|$ for $|\cdot|_p$ when it is clear from the context that we are speaking of the p-adic norm.

The subset

$$\mathfrak{m} = \{x \in \mathbb{Z}_p : |x|_p < 1\}$$

is a maximal ideal of $\mathbb{Z}_p$. Thus every element x of $\mathfrak{m}$ satisfies $v_p(x) \geq 1$ and so we deduce $\mathfrak{m} = p\mathbb{Z}_p$. Moreover, every non-trivial ideal of $\mathbb{Z}_p$ is a power of $\mathfrak{m}$. (Commutative rings with only one maximal ideal are called *local rings*. $\mathbb{Z}_p$ is thus a local ring.)

Given $x \in \mathbb{Q}$ satisfying $|x|_p \leq 1$ and any natural number i, we can find a positive integer a_i satisfying $0 \leq a_i < p^i$ such that $|x - a_i| \leq p^{-i}$. Indeed, write $x = a/b$ with $(a, b) = 1$. As $|x|_p \leq 1$, p and b are coprime, so we can find integers u and v such that $ub + vp^i = 1$. Let $a_i = ua$. Then

$$|a_i - x|_p = |ua - x|_p = \left|ua - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |ub - 1|_p \leq p^{-i}.$$

We can translate a_i by a multiple of p^i to ensure $0 \leq a_i < p^i$ and the above inequalities are not altered.

These observations imply that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Thus, we can think of elements of $\mathbb{Z}_p$ as formal power series

$$\sum_{n=0}^{\infty} b_n p^n, \quad 0 \leq b_n \leq p-1.$$

Given any $x \in \mathbb{Q}_p$, we can find p^N such that $|p^N x|_p \leq 1$ so that every element of $\mathbb{Q}_p$ can be thought of as a formal series

$$\sum_{n=-N}^{\infty} b_n p^n, \quad 0 \leq b_n \leq p-1.$$

This p-adic expansion of x is easily checked to be unique.

These remarks allow us to infer a few of the basic topological aspects of $\mathbb{Z}_p$ and $\mathbb{Q}_p$. For example, recall that a topological space X is called locally compact if every point of X has a compact neighborhood. It is not difficult to see that $\mathbb{Q}_p$ is locally compact and $\mathbb{Z}_p$ is compact. Indeed, $\mathbb{Z}_p$ is complete since it is a closed subset of a complete field. It is also totally bounded since for any $\epsilon = p^{-n}$, the p^n balls

$$a + p^n \mathbb{Z}_p, \qquad a = 0, 1, 2, ..., p^n - 1$$

cover $\mathbb{Z}_p$. Now given any $x \in \mathbb{Q}_p$, we can find some N so that $p^N x \in \mathbb{Z}_p$ which has a compact neighborhood and thus x has one.

It is useful to observe the analogy with Laurent series and the field of meromorphic functions of a complex variable. At each point $z \in \mathbb{C}$, a meromorphic function has a Laurent expansion which is unique. This suggests that if a rational number has denominator divisible by p, we can think of it as a p-adic number having a 'pole' at p. This analogy has been a guiding force for much of the development in p-adic number theory.

Now we consider the convergence of p-adic infinite series. The p-adic metric is much simpler to deal with than the usual absolute value for this study as the following theorem shows.

Theorem 3.2 *A p-adic series*

$$\sum_{n=1}^{\infty} c_n, \quad c_n \in \mathbb{Q}_p,$$

converges if and only if $|c_n|_p \to 0$ as $n \to \infty$.

Proof. It is clear that if the series converges, then $|c_n|_p \to 0$ since the usual proof carries over. Now suppose $|c_n|_p \to 0$. Let

$$s_N = \sum_{n=1}^{N} c_n.$$

Since $\mathbb{Q}_p$ is complete, it suffices to show that $\{s_N\}_{N=1}^{\infty}$ is Cauchy. We have for $M > N$,

$$\begin{aligned} |s_M - s_N|_p &= |c_{N+1} + \cdots + c_M|_p \\ &\leq \max(|c_{N+1}|_p, \ldots, |c_M|_p) \end{aligned}$$

which goes to 0 as $N \to \infty$. This completes the proof. ∎

For example, the sequence

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

converges (to $(1-p)^{-1}$). Also, the series

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

converges. It is still unknown if this number is a p-adic irrational. That is, can we show that it is an element of $\mathbb{Q}_p \backslash \mathbb{Q}$? By contrast, we have

$$\sum_{n=0}^{\infty} n \cdot n! = -1 \tag{3.2}$$

because

$$\sum_{n=0}^{N} n \cdot n! = (N+1)! - 1,$$

as an easy induction argument shows. Taking p-adic limits gives us (3.2).

We can also consider the convergence of double series of the form

$$\sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{mn}.$$

Suppose that for every m,

$$\lim_{n \to \infty} a_{mn} = 0.$$

Suppose further that $\lim_{m\to\infty} a_{mn} = 0$ uniformly in n. That is, for each n, and given $\epsilon > 0$, there is an $N = N(\epsilon)$ (independent of n) such that

$$m \geq N \Rightarrow |a_{mn}|_p < \epsilon.$$

With these hypotheses, it is easy to see that

$$a_{mn} \to 0 \quad \text{as} \quad \max(m,n) \to \infty.$$

This observation allows us to prove that

Theorem 3.3 *Let $a_{mn} \in \mathbb{Q}_p$ and suppose that for every m, $\lim_{n\to\infty} a_{mn} = 0$. Suppose further that $\lim_{m\to\infty} a_{mn} = 0$ uniformly in n. Then both series*

$$\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right) \quad \textit{and} \quad \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_{mn}\right)$$

converge and their sums are equal.

Proof. By our observation above, we see that both sums converge, since for $m, n \geq \max(N, N_1) = N_0$ (say) we have

$$\left|\sum_{j=0}^{\infty} a_{mj}\right|_p < \epsilon \quad \textit{and} \quad \left|\sum_{k=0}^{\infty} a_{kn}\right|_p < \epsilon.$$

It is also clear that using (3.1), we have

$$\left|\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right) - \sum_{m=0}^{N_0}\left(\sum_{n=0}^{N_0} a_{mn}\right)\right|_p$$

$$= \left|\sum_{m=0}^{N_0}\left(\sum_{n=N_0+1}^{\infty} a_{mn}\right) + \sum_{m=N_0+1}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right)\right|_p < \epsilon.$$

Similarly,

$$\left|\sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_{mn}\right) - \sum_{n=0}^{N_0}\left(\sum_{m=0}^{N_0} a_{mn}\right)\right|_p < \epsilon$$

by reversing m and n in the previous inequality. Hence, for any $\epsilon > 0$,

$$\left|\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right) - \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_{mn}\right)\right|_p$$

$$\leq \max\left(\left|\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right) - S\right|_p, \left|S - \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_{mn}\right)\right|_p\right) \leq \epsilon$$

with

$$S = \sum_{n=0}^{N_0} \sum_{m=0}^{N_0} a_{mn}.$$

This completes the proof. ∎

As in the case of real analysis, one can consider power series of the form

$$f(x) = \sum_{n=1}^{\infty} a_n x^n \tag{3.3}$$

and determine its radius of convergence. By Theorem 3.2, we see that the series in (3.3) has radius of convergence given by

$$\rho = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}},$$

where we use the usual conventions when the limit is 0 or ∞, so that $0 \le \rho \le \infty$. That is, if $\rho = 0$, $f(x)$ converges only when $x = 0$. If $\rho = \infty$, $f(x)$ converges for all $x \in \mathbb{Q}_p$. Notice that any series

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

converges in $|x|_p < 1$ if the coefficients a_n lie in $\mathbb{Z}_p$.

Even though convergence of series has been reduced to a simple criterion by the previous theorem, the p-adic analogues of classical functions cannot be so easily extended. For example, consider the series

$$\mathrm{Exp}(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Since

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} [n/p^j],$$

we see that $\mathrm{Exp}\,(x)$ converges for $|x|_p < r_p = p^{-1/(p-1)}$. Moreover, observing that

$$\mathrm{ord}_p((p^m)!) = \frac{p^m - 1}{p - 1}$$

shows that $\rho = p^{-1/(p-1)}$ is the radius of convergence for $\mathrm{Exp}(x)$. (This comment is not quite accurate. For $x \in \mathbb{Q}_p$, the p-adic metric will take only integral powers of p and not rational powers. Thus, if $p \neq 2$, there is no element x in $\mathbb{Q}_p$ such that $|x|_p = r_p$. Later, when we define the metric for extensions of $\mathbb{Q}_p$, we

will see that r_p does occur as the norm of an element in some extension field of $\mathbb{Q}_p$.) If we let $D = \{x \in \mathbb{Z}_p : \quad |x|_p < p^{-1/(p-1)}\}$, then the p-adic exponential is well-defined for $x \in D$. Moreover, if $x, y \in D$, then $x + y \in D$ (by virtue of the stronger inequality (3.1)) and we have

$$\mathrm{Exp}(x+y) = \mathrm{Exp}(x)\mathrm{Exp}(y)$$

as is easily checked by a formal multiplication of power series.

By contrast, the series

$$-\log_p(1-x) := \sum_{n=1}^{\infty} \frac{x^n}{n}$$

converges in the larger region $|x|_p < 1$ because $\mathrm{ord}_p(n) \leq [\log n / \log p]$ and the convergence in question is easily checked. (The notation $\log_p$ indicates the p-adic logarithm and **not** the natural logarithm to the base p.) Thus, the p-adic logarithm $\log_p(x)$ can be defined via the power series above for $|x-1|_p < 1$. One can also verify the identity

$$\log_p(xy) = \log_p(x) + \log_p(y)$$

as an identity of formal power series, for x, y in the same disc.

One must be a bit cautious with these 'formal power series' discussions since there are subtleties involved. We do not elaborate upon these here, but refer the reader to Theorem 4.3.3 of [G]. However, in the above context, the arguments can be rigorously justified.

Here is a curious consequence of the above. It follows that the series

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

converges in the 2-adic number field $\mathbb{Q}_2$. To what? To $-\log_2(-1)$ of course. But then, $-2\log_2(-1) = -\log_2(-1)^2 = -\log_2 1 = 0$. Thus, for each integer $M > 0$, there is a natural number n such that the numerator of the partial sum

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n}$$

is divisible by 2^M. (This is certainly not obvious and the reader is asked to prove it directly using elementary number theory. See Exercise 5 below.) In other words,

$$\sum_{n=1}^{\infty} \frac{2^n}{n} = 0 \qquad \text{in} \quad \mathbb{Q}_2.$$

One can ask if a similar result holds in $\mathbb{Q}_p$ with 2 replaced by a prime p or any other number divisible by p. We will see below that this is not the case. In fact, we will prove that

$$v_p\left(p+\frac{p^2}{2}+\frac{p^3}{3}+\cdots+\frac{p^n}{n}\right)$$

is bounded for all n.

We may also consider the binomial series

$$B_a(x) := (1+x)^a = \sum_{n=0}^{\infty}\binom{a}{n}x^n = \sum_{n=0}^{\infty}\frac{a(a-1)\cdots(a-n+1)}{n!}x^n.$$

Recall that when x is a complex number, and $a \in \mathbb{R}$ or $\mathbb{C}$, the series converges for $|x| < 1$ and diverges if $|x| > 1$ (unless a is a non-negative integer). In the p-adic case, the answer depends on p-adic valuation of a. If $|a|_p > 1$, then $|a-i|_p = |a|_p$ for each integer i so that it follows that the above series converges for $|x|_p < r_p/|a|_p$. If $|a|_p \leq 1$, then it is easy to see that

$$\left|\frac{a(a-1)\cdots(a-n+1)}{n!}\right|_p \leq 1$$

so that the series converges for $|x|_p < 1$.

One can use this observation to construct the "Artin-Hasse exponential," which is similar to the exponential function defined above but has a larger region of convergence. It is based on an elementary observation. Recall that the Möbius function of elementary number theory is defined as $\mu(1) = 1$, $\mu(n) = 0$ if $p^2|n$ for some prime p and $\mu(n) = (-1)^r$ if n is composed of r distinct prime numbers. It has the characteristic property

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

If we set

$$f(x) = \prod_{n=1}^{\infty}(1-x^n)^{-\mu(n)/n}$$

and formally expand $\log f(x)$ as a power series, rearrange terms, we see that $f(x) = \exp(x)$ as a formal identity. The n-th factor in the product converges in the region $|x|_p < 1$ provided n is coprime to p. This suggests that we consider instead

$$E_p(x) = \prod_{\substack{n=1 \\ (n,p)=1}}^{\infty}(1-x^n)^{-\mu(n)/n}.$$

Now the binomial series $B_{-\mu(n)/n}(-x^n)$ converges in $|x|_p < 1$ and the infinite product makes sense as all the coefficients are in $\mathbb{Z}_p$. Thus the series obtained

from the product for $E_p(x)$ converges in $|x|_p < 1$. Proceeding formally as above, we find

$$E_p(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots\right).$$

It is curious that Wilson's theorem can be recovered from this. As all the coefficients of $E_p(x)$ are p-integral, the coefficient of x^p in particular is p-integral. This coefficient is

$$\frac{1}{p!} + \frac{1}{p} = \frac{1 + (p-1)!}{p!}$$

which must be p-integral. Hence, $(p-1)! + 1$ is divisible by p.

There is an important theorem called Strassman's theorem which gives us an upper bound for the number of $\mathbb{Z}_p$-zeros of a p-adic power series. In fact, the argument can be generalised to treat zeros in larger discs of the form $p^{-n}\mathbb{Z}_p$.

Theorem 3.4 (Strassman's theorem) *Let*

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

be a non-zero power series with $a_n \in \mathbb{Q}_p$. Suppose $a_n \to 0$ as $n \to \infty$ so that $f(x)$ converges for $x \in \mathbb{Z}_p$. Let N be defined by the conditions

$$|a_N|_p = \max_n |a_n|_p \qquad \textit{and} \qquad |a_n|_p < |a_N|_p \qquad \textit{for} \quad n > N.$$

Then, the function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ given by $x \mapsto f(x)$ has at most N zeros.

Proof. We induct on N. For $N = 0$, we have $|a_0|_p > |a_n|_p$ for $n \geq 1$. If $f(r) = 0$ for some $r \in \mathbb{Z}_p$, we have

$$-a_0 = a_1 r + a_2 r^2 + \cdots$$

so that

$$|a_0|_p \leq \max_{n \geq 1} |a_n r^n|_p \leq \max_{n \geq 1} |a_n|_p,$$

a contradiction. This proves the theorem for $N = 0$. Now assume $N \geq 1$. If $r \in \mathbb{Z}_p$ is a zero of $f(x)$, we can write

$$\begin{aligned} f(x) = f(x) - f(r) &= \sum_{n=1}^{\infty} a_n (x^n - r^n) \\ &= (x - r) \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} a_n x^j r^{n-1-j}. \end{aligned}$$

By Theorem 3.3, we can re-arrange our series:

$$f(x) = (x - r) \sum_{n=0}^{\infty} b_n x^n$$

where

$$b_n = \sum_{k=0}^{\infty} a_{n+1+k} r^k.$$

Observe that for every n,

$$|b_n|_p \leq \max_{k \geq 0} |a_{n+1+k}|_p \leq |a_N|_p$$

and that

$$|b_{N-1}|_p = |a_N + a_{N+1} r + \cdots|_p = |a_N|_p$$

so that if $n \geq N$, we have

$$|b_n|_p \leq \max_{k \geq 0} |a_{n+1+k}|_p \leq \max_{j \geq N+1} |a_j|_p < |a_N|_p.$$

Thus,

$$g(x) = \frac{f(x)}{x - r}$$

satisfies the hypotheses of the theorem with N replaced by $N-1$. By induction, $g(x)$ has at most $N - 1$ zeros in $\mathbb{Z}_p$ so that $f(x)$ has at most N zeros in $\mathbb{Z}_p$. ∎

One can use Strassman's theorem to determine zeros of

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

Since the power series converges only in $|x|_p < 1$, we cannot use Theorem 3.4 directly. We therefore consider

$$-\log_p(1 - px) = \sum_{n=1}^{\infty} \frac{p^n}{n} x^n.$$

If $p \neq 2$, we see that

$$\max_{n \geq 1} \left| \frac{p^n}{n} \right|_p = |p|_p$$

so that $-\log_p(1 - px)$ has at most one zero in $|x|_p \leq 1$. But $x = 0$ is a zero in this disc and so we deduce that the only $\mathbb{Z}_p$-zeros of $\log_p(1 - px)$ is $x = 0$. If $p = 2$, we see that $-\log_2(1 - 2x)$ has at most two zeros in $|x|_2 \leq 1$. $x = 0$ and $x = 1$ are the two zeros. (Compare this with the example above as well as Exercise 5.)

Let us make a few general remarks. It is not difficult to show that a p-adic power series represents a continuous function in its region of convergence. The notion of a p-adic derivative of a function is clear. We define it as

$$\lim_{n\to\infty} \frac{f(x+p^n)-f(x)}{p^n}$$

when this limit exists and denote it by $f'(x)$. An elementary verification shows, for instance, that the derivative of $f(x) = x^n$ is nx^{n-1} for non-negative integers n. It is also clear that if $f(x)$ is a convergent power series, we can differentiate term by term thus $f'(x)$ is given by a convergent power series in this region. (There is something to check and we leave the verification to the reader as an elementary exercise.)

Now for a fixed natural number a, consider the function $f(x) = a^x$. Naturally, we will interpret this to be $(1+a-1)^x = B_x(a-1)$ which converges and defines a continuous function for $|a-1| < 1$. In the complex analytic case, the derivative of $f(x)$ is easily computed to be $(\log a)a^x$. A similar result holds in the p-adic case, although the proof of this is not trivial. It requires us to discuss the derivatives of functions of the form

$$\binom{x}{h}$$

which we will not do here. Observe, however that if an analogous result holds, then, we derive the interesting formula:

$$\log_p a = \lim_{n\to\infty} \frac{a^{p^n}-1}{p^n}$$

which can be interpreted as the p-adic derivative of a^x at $x = 0$. Thus, quotients of the form $(a^{p^n}-1)/p^n$ behave like the logarithm.

We already witnessed this phenomenon in the Fermat quotient. In the next chapter, we will see a theoretical basis for this behaviour. For the moment, this maybe a good place to discuss the Fermat quotient in the light of what we have done:

$$F(a) = \frac{a^{p-1}-1}{p}$$

defined for $1 \le a \le p-1$. $F(a)$ has similar properties to the p-adic logarithm defined above, and there is a good reason for this, as will be shown later. For instance,

$$F(ab) \equiv F(a) + F(b) (\bmod p)$$

because

$$\begin{aligned}(ab)^{p-1} &= a^{p-1}b^{p-1} \\ &= (1+pF(a))(1+pF(b)) \\ &\equiv 1+p(F(a)+F(b)) (\bmod p^2).\end{aligned}$$

One can relate the Fermat quotient to sums of 'Voronoi' type studied in the previous chapter. Observe that

$$F(a+pt) \equiv F(a) - \overline{a}t (\bmod p) \tag{3.4}$$

where $a\overline{a} \equiv 1 (\bmod p)$. Indeed,

$$\begin{aligned}
(a+pt)^{p-1} &\equiv a^{p-1} + p(p-1)ta^{p-2} (\bmod p^2) \\
&\equiv 1 + pF(a) + p(p-1)ta^{p-1}\overline{a} (\bmod p^2) \\
&\equiv 1 + pF(a) + p(p-1)t\overline{a}(1+pF(a)) (\bmod p^2) \\
&\equiv 1 + p(F(a) + (p-1)t\overline{a}) (\bmod p^2)
\end{aligned}$$

from which (3.4) is deduced. [One should think of this as 'Taylor series' of $F(a)$ in a small disc.]

Now

$$\sum_{j=1}^{p-1} F(aj) \equiv \sum_{j=1}^{p-1} F(a) + \sum_{j=1}^{p-1} F(j) (\bmod p)$$

since $F(aj) \equiv F(a) + F(j) (\bmod p)$. Thus,

$$F(a) \equiv \sum_{j=1}^{p-1} F(j) - \sum_{j=1}^{p-1} F(aj) (\bmod p).$$

Now write $aj = pq_j + r_j$ with $1 \le r_j \le p-1$. Then

$$F(aj) = F(r_j + pq_j) \equiv F(r_j) - \overline{r_j}q_j (\bmod p)$$

by (3.4). As j runs through 1 to $p-1$, so does r_j. Therefore,

$$F(a) \equiv \sum_{j=1}^{p-1} \frac{q_j}{r_j} \equiv \sum_{j=1}^{p-1} \left[\frac{ja}{p}\right] \frac{1}{ja} (\bmod p)$$

from which we deduce:

Theorem 3.5 *For $1 \le a \le p-1$,*

$$\frac{a^p - a}{p} \equiv \sum_{j=1}^{p-1} \left[\frac{ja}{p}\right] \frac{1}{j} (\bmod p).$$

In particular, observe that for odd primes p

$$\frac{2^p - 2}{p} \equiv \sum_{p/2<j<p} \frac{1}{j} (\bmod p).$$

Now,

$$\sum_{1\le j<p} \frac{1}{j} \equiv 0 (\bmod p)$$

so that

$$-\frac{2^p-2}{p} \equiv \sum_{j<p/2} \frac{1}{j} (\bmod p).$$

Thus, $p^2|(2^p-2)$ if and only if the numerator of

$$1+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}$$

is divisible by p.

Since $F(uv) \equiv F(u)+F(v)(\bmod p)$, we find

$$\sum_{a=1}^{p-1} F(a) \equiv F((p-1)!)(\bmod p).$$

By Wilson's theorem, we have for some integer t

$$\{(p-1)!\}^{p-1} \equiv (-1+tp)^{p-1} \equiv 1-tp(p-1)(\bmod p^2)$$

for odd primes p. It is now easily deduced that

$$\sum_{a=1}^{p-1} F(a) \equiv \frac{(p-1)!+1}{p} (\bmod p).$$

The left hand side of the above congruence is

$$\frac{s_{p-1}(p)-(p-1)}{p}$$

in the notation of the previous chapter. By (2.5), we find

$$s_{p-1}(p) \equiv pB_{p-1}(\bmod p^2)$$

so that we have proved:

Theorem 3.6 $(p-1)!+1 \equiv 0(\bmod p^2)$ *if and only if the numerator of*

$$B_{p-1}+\frac{1}{p}-1$$

is divisible by p.

Remark. Note that by the von Staudt-Clausen theorem, the number $B_{p-1}+1/p$ is p-integral. It is as if we have removed the 'pole' and the criterion of the

theorem is given in terms of the constant term of the 'Laurent' expansion of B_{p-1}.

The quotient

$$W_p = \frac{(p-1)!+1}{p}$$

is called Wilson's quotient and it is unknown if there are infinitely many primes p such that $W_p \equiv 0 (\bmod p)$. It is curious that the Bernoulli number B_{p-1} does not enter into Kummer's criterion for regularity but enters here.

Exercises

1. Prove that if a has p-adic expansion $a_0 + a_1 p + a_2 p^2 + \cdots$, then $-a$ has p-adic expansion $(p - a_0) + (p - 1 - a_1)p + (p - 1 - a_2)p^2 + \cdots$.

2. Show that $\sum_{n=0}^{\infty} n! x^n$ converges in $\mathbb{Q}_p$ for $|x|_p < 1$.

3. Suppose that

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

is a convergent p-adic series. Prove that

$$\left| \sum_{n=1}^{\infty} a_n \right|_p \leq \max_{n \geq 1} |a_n|_p.$$

4. Show that

$$\sum_{n=0}^{\infty} \frac{B_n x^n}{n!}$$

converges in $\mathbb{Q}_p$ for $|x|_p < r_p$.

5. Prove that the power of 2 dividing the numerator of the rational number

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots \frac{2^n}{n}$$

is $\geq n - (\log n / \log 2)$.

6. Show that $\sum_{n=0}^{\infty} n^k p^n$ converges in $\mathbb{Q}_p$ to a p-adic rational number.

7. Let n be a positive integer, and let $n = a_0 + a_1 p + \cdots a_k p^k$ be its expansion in base p. Let $s = a_0 + a_1 + \cdots + a_k$ be the sum of its digits in the expansion. Show that
$$v_p(n!) = \frac{n-s}{p-1}.$$
[Hint: work out the fractional part of n/p^i in terms of the digits.]

8. If x is in $\mathbb{Q}_p$ and
$$x = \sum_{n=-N}^{\infty} a_n p^n, \qquad 0 \le a_n \le p-1$$
is its p-adic expansion, with the sequence $\{a_n\}_{n=0}^{\infty}$ eventually periodic, show that x is rational. (That is, $x \in \mathbb{Q}$.)

9. Prove the converse of the assertion in the previous exercise. That is, if x is rational, its p-adic expansion is eventually periodic. [Hint: it suffices to prove the theorem for $x = a/b$ with $(p, ab) = 1$. By exercise 1, we may suppose that a is negative and b is positive. By Euler's theorem, $p^{\phi(b)} - 1 = bb'$ for some b'. Now consider, $x = ab'/bb'$.]

10. Prove the p-adic version of Eisenstein's irreducibility criterion: let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be in $\mathbb{Z}_p[x]$. Suppose that $|a_i|_p < 1$ for $i = 0, 1, ..., n-1$ and that $|a_0|_p = 1/p$. Prove that $f(x)$ is irreducible in $\mathbb{Q}_p[x]$.

Chapter 4

Hensel's Lemma

Recall that $\mathbb{R}$ is not algebraically closed since $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. We will show below that $\mathbb{Q}_p$ is not algebraically closed. In the case of the reals, we have that adjoining $\sqrt{-1}$ to $\mathbb{R}$ gives us a quadratic extension of $\mathbb{R}$ which is algebraically closed. In contrast, the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is of infinite degree over $\mathbb{Q}_p$. Moreover, it is not complete with respect to the extension of the p-adic norm. By completing it (via the usual method outlined in the previous chapter) we obtain $\mathbb{C}_p$, the p-adic analogue of the complex numbers $\mathbb{C}$, which turns out to be both algebraically closed and complete. The study of $\mathbb{C}_p$ in the literature falls under the heading of rigid analytic spaces and we will not discuss this theory in this monograph. Our investigation will be confined to $\mathbb{Q}_p$.

We begin with the important theorem:

Theorem 4.1 (Hensel's lemma) *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$. Write $f'(x)$ for its formal derivative. If $f(x) \equiv 0 (\bmod p)$ has a solution a_1 satisfying $f'(a_1) \not\equiv 0 (\bmod p)$ then there is a unique p-adic integer a such that $f(a) = 0$ and $a \equiv a_1 (\bmod p)$.*

Proof. We prove inductively that if

$$f(x) \equiv 0 (\bmod p^n)$$

has a solution a_n then it can be lifted uniquely to $a_{n+1} (\bmod p^{n+1})$ such that

$$f(a_{n+1}) \equiv 0 (\bmod p^{n+1})$$

and $a_{n+1} \equiv a_n (\bmod p^n)$. Indeed, writing $a_{n+1} = p^n t + a_n$ we require

$$f(p^n t + a_n) \equiv 0 (\bmod p^{n+1}).$$

Writing $f(x) = \sum_i c_i x^i$, we get

$$\begin{aligned} f(p^n t + a_n) &= \textstyle\sum_i c_i (a_n + p^n t)^i \\ &\equiv \textstyle\sum_i c_i (a_n^i + i p^n t a_n^{i-1}) (\bmod p^{n+1}) \\ &\equiv f(a_n) + p^n t f'(a_n) (\bmod p^{n+1}). \end{aligned}$$

We need to solve for t in the congruence

$$p^n t f'(a_n) + f(a_n) \equiv 0 (\bmod p^{n+1}).$$

Since $f(a_n) \equiv 0 (\bmod p^n)$ this reduces to

$$t f'(a_n) \equiv -(f(a_n)/p^n)(\bmod p)$$

which has a unique solution t (mod p) because $a_n \equiv a_1 (\bmod p)$ and $f'(a_1) \not\equiv 0 (\bmod p)$. Moreover, the sequence $\{a_n\}_{n=1}^{\infty}$ is a Cauchy sequence whose limit is the required solution. Since a_{n+1} is a unique lifting (mod p^{n+1}) of $a_n (\bmod p^n)$, the uniqueness of the limit solution is clear. This completes the proof of the theorem.

If K is an algebraic number field, and $\mathfrak{p}$ a prime ideal, it is clear how we can define the field of $\mathfrak{p}$-adic integers of K. It is also clear that Hensel's lemma can be extended to this setting. One natural way of defining the $\mathfrak{p}$-adic norm of an element $x \in K$, $x \neq 0$ is to set

$$|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_p(x)}$$

where $N(\mathfrak{p})$ is the norm of the ideal $\mathfrak{p}$ and $v_p(x)$ is the power of $\mathfrak{p}$ appearing in the factorization of the principal ideal (x). The field obtained by completing K with respect to $|\cdot|_{\mathfrak{p}}$ is denoted $K_{\mathfrak{p}}$. (We caution the reader that other normalizations of the metric are possible and are used in the literature. For instance, if $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$, and we define

$$||\pi|| = p^{-1/e}$$

where p is the rational prime below $\mathfrak{p}$ and $p = \pi^e u$, with u coprime to p, then we obtain an equivalent metric.) The ring

$$O_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : \quad |x|_{\mathfrak{p}} \leq 1\}$$

is called the ring of $\mathfrak{p}$-adic integers. If p is the rational prime below $\mathfrak{p}$, we can view $K_{\mathfrak{p}}$ as an extension of $\mathbb{Q}_p$. Moreover, one can show that every finite extension of $\mathbb{Q}_p$ is obtained in this way and for such extensions, the residue field $O_{\mathfrak{p}}/\mathfrak{p}$ is a finite field.

Remark. The main thrust of Hensel's lemma is that solving equations in $\mathbb{Z}_p$ is equivalent to solving equations (mod p^n) for all positive integers n. Since we have the natural maps (projections)

$$\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

one can view $\mathbb{Z}_p$ as the inverse (or projective) limit of the system $\{\mathbb{Z}/p^n\mathbb{Z}\}$. Note that in the above construction of the root,

$$a_{n+1} \equiv a_n - \frac{f(a_n)}{f'(a_n)} (\bmod p^{n+1})$$

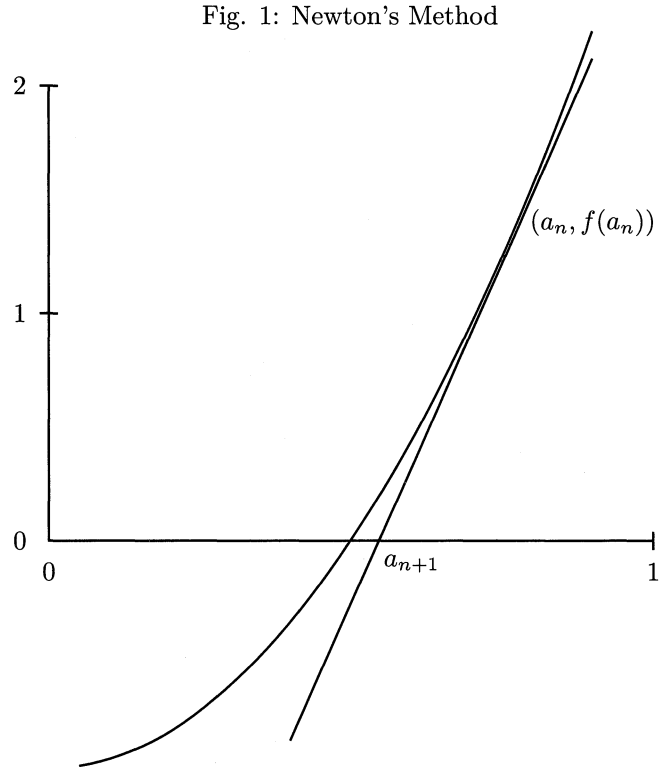
This formula bears a striking resemblance to Newton's method.

Indeed, Hensel's lemma can be viewed as the p-adic analogue of the classical method of Newton for approximating real roots of a differentiable function. Let us briefly recall this method. If $f(x)$ has a root α, one chooses a point a_n in the neighbourhood of α such that $f'(a_n) \neq 0$. The line through the point $(a_n, f(a_n))$ having slope $f'(a_n)$ intersects the x-axis at a_{n+1} (say) which gives a better approximation than a_n, one hopes, to the root α. Then, we have (see Fig. 1)

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

which has a close resemblance to the sequence $\{a_n\}$ we constructed in the p-adic version. Newton's method does not always lead to a real root (see Exercise 1).

Fig. 1: Newton's Method



An application of Theorem 4.1 enables us to see that if p is odd, then the congruence $x^2 \equiv 1 (\bmod p^n)$ has only 2 solutions $x = \pm 1$ for all $n \geq 1$. If $p = 2$ and $n \geq 2$, Hensel's lemma cannot be applied to study $x^2 \equiv 1 (\bmod 2^n)$ since

the derivative of $x^2 - 1$ mod 2 is zero. The congruence $x^2 \equiv 1 (\bmod 2^n)$ has four solutions, if $n > 2$, namely $x = \pm 1, 2^{n-1} \pm 1$. Indeed, $2^n | (x-1)(x+1)$ implies exactly one of $x-1$ or $x+1$ is divisible by 4. Hence, either $2||(x-1)$ or $2||x+1$ (where the notation $p||n$ means that $p|n$ and n/p is coprime to p). In the former case, $x \equiv -1 (\bmod 2^{n-1})$ so that $x = 2^{n-1}t - 1$ for some t. If t is even, we get $x \equiv -1 (\bmod 2^n)$. If t is odd, we get $x \equiv 2^{n-1} - 1 (\bmod 2^n)$. In the case $2||x+1$, $x \equiv 1 (\bmod 2^{n-1})$ so that $x = 2^{n-1}t + 1$. If t is even, we get $x \equiv 1 (\bmod 2^n)$ and if t is odd, we get $x \equiv 2^{n-1} + 1 (\bmod 2^n)$. Notice that $x^2 \equiv 1 (\bmod 4)$ has exactly 2 solutions which can be lifted uniquely to $\mathbb{Q}_2$. (Compare with Exercise 10.)

Consider now the polynomial $f(x) = x^m - 1$ with $m|p-1$. Then $f(x) \equiv 0 (\bmod p)$ has m distinct solutions since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ and for each of these solutions, the conditions of Hensel's lemma are verified so that each of them can be lifted to $\mathbb{Q}_p$. In particular, if $p > 2$ and $m = p-1$, we see that for each $1 \le i \le p-1$, there is a number $\omega(i) \in \mathbb{Z}_p$ such that $\omega(i) \equiv i (\bmod p)$ and $\omega(i)^{p-1} = 1$. The $\omega(i)$ are called the Teichmüller representatives of the residue classes mod p. The map

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p$$

given by $x \mapsto \omega(x)$ defines a multiplicative character called the Teichmüller character. For $x \in \mathbb{Z}_p^\times$, we define $\omega(x)$ to be $\omega(x \bmod p)$. It is easy to see that every $x \in \mathbb{Z}_p^\times$ can be written uniquely as $x = \omega(x)\langle x \rangle$ with $\langle x \rangle \in 1 + p\mathbb{Z}_p$ (and in fact, if $p = 2$, in $1 + 4\mathbb{Z}_2$.) Notice that for $p \neq 2$,

$$\omega(x) = \lim_{n \to \infty} x^{p^n},$$

(because $a \equiv b (\bmod p)$ implies $a^{p^n} \equiv b^{p^n} (\bmod p^{n+1})$ as is easily verified by induction, so that)

$$\omega(x) = \omega(x)^{p^n} = \frac{x^{p^n}}{\langle x \rangle^{p^n}}$$

and the denominator goes to 1 as $n \to \infty$.

For $p = 2$, we let $\omega(a)$ be the unique square root of 1 such that $\omega(a) \equiv a (\bmod 4)$, the existence of which was established above.

For $1 \le a \le p-1$, let us write

$$\omega(a) = a + a_1 p + a_2 p^2 + \cdots$$

as a p-adic integer and determine a_1. Since $\omega(a)^{p-1} = 1$, we must have

$$1 = (a + a_1 p + a_2 p^2 + \cdots)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}(a_1 p) \pmod{p^2}$$

so that

$$a_1 \equiv \frac{a^p - a}{p} (\bmod p).$$

Thus, the Fermat quotient $F(a) = (a^{p-1} - 1)/p$ occurs in the second coefficient of the p-adic expansion of $\omega(a)$. That is,

$$\omega(a) \equiv a(1 + F(a)p)(\bmod p^2).$$

There is a polynomial version of Hensel's lemma that is useful and it is proved in a similar way. We state it as:

Theorem 4.2 (Polynomial form of Hensel's lemma) *Suppose $f(x) \in \mathbb{Z}_p[x]$ and there exist $g_1, h_1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ such that*

$$f(x) \equiv g_1(x)h_1(x)(\bmod p)$$

with $(g_1, h_1) = 1$, g_1 monic. Then there exist polynomials $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $g(x) \equiv g_1(x)(\bmod p)$, $h(x) \equiv h_1(x)(\bmod p)$ with $g(x)$ monic and

$$f(x) = g(x)h(x).$$

Let us also note that either an application of Theorem 4.1 or 4.2 shows that $\mathbb{Q}_p$ is not algebraically closed. In fact, it has algebraic extensions of every degree. For example, by a p-adic version of the Eisenstein criterion (see Exercise 10 in Chapter 3), the polynomial $x^n - p$ is irreducible in $\mathbb{Q}_p[x]$. One can also see that $\mathbb{Q}_p$ has algebraic extensions of every degree by noting that the number of monic irreducible polynomials mod p of degree n is given by the formula

$$\frac{1}{n}\sum_{d|n} \mu(d)p^{n/d} \geq 1,$$

where μ denotes the Möbius function. We can lift an irreducible polynomial mod p to a polynomial in $\mathbb{Z}_p[x]$ which must still be irreducible in $\mathbb{Z}_p[x]$.

Before we begin a study of functions of $\mathbb{Q}_p$, let us make several remarks. If K is a finite extension of $\mathbb{Q}_p$, it is clear how the norm should be extended to K. We set for $\alpha \in K$,

$$|\alpha|_p = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]},$$

where $N_{K/\mathbb{Q}_p}(\alpha)$ denotes the norm of α (which, as always, is the product of the conjugate roots of the minimal polynomial of α over $\mathbb{Q}_p$).

Theorem 4.3 *$|\cdot|_p$ is a non-archimedean norm on K.*

Proof. It is clear that $|x|_p = 0$ if and only if $x = 0$. It is also clear that $|xy|_p = |x|_p|y|_p$ since the norm is multiplicative. To prove the stronger triangle inequality, namely,

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

(say, without loss of generality, $|x|_p \leq |y|_p$) we see that upon dividing by y, it suffices to prove that for $z \in K$, and $|z|_p \leq 1$, we have

$$|z + 1|_p \leq 1.$$

This will follow if we can show

$$|z|_p \leq 1 \Rightarrow |z - 1|_p \leq 1$$

because

$$|z|_p \leq 1 \Rightarrow |-z|_p \leq 1 \Rightarrow |-z-1|_p = |z+1|_p \leq 1.$$

Therefore, it suffices to show that

$$|N_{K/\mathbb{Q}_p}(z)|_p \leq 1 \Rightarrow |N_{K/\mathbb{Q}_p}(z-1)|_p \leq 1.$$

This reduces to showing

$$N_{K/\mathbb{Q}_p}(z) \in \mathbb{Z}_p \Rightarrow N_{K/\mathbb{Q}_p}(z-1) \in \mathbb{Z}_p.$$

Now, we must use a bit of algebraic number theory. Clearly, $\mathbb{Q}_p(z) = \mathbb{Q}_p(z-1)$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be the minimal polynomial of z in $\mathbb{Q}_p[x]$. The minimal polynomial for $z - 1$ is then

$$f(x+1) = x^n + (a_{n-1} + n)x^{n-1} + \cdots + (1 + a_{n-1} + \cdots a_1 + a_0).$$

Notice that $N_{K/\mathbb{Q}_p}(z) = (-1)^n a_0$, and

$$N_{K/\mathbb{Q}_p}(z-1) = (-1)^n(1 + a_{n-1} + \cdots a_1 + a_0).$$

We now use the polynomial form of Hensel's lemma. If all the coefficients of $f(x)$ are in $\mathbb{Z}_p$, we are done. So assume that $a_0 \in \mathbb{Z}_p$ but some $a_i \notin \mathbb{Z}_p$. Choose m to be the smallest exponent such that $p^m a_i \in \mathbb{Z}_p$ for all i and "clear denominators":

$$g(x) = p^m f(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

with $b_i = p^m a_i$. Since $f(x)$ is monic, $b_n = p^m$ and we also know that $b_0 = p^m a_0$. By assumption, at least one of the b_i is not divisible by p. Thus,

$$g(x) \equiv (b_n x^{n-k} + \cdots + b_k)x^k (\bmod p),$$

where $k \geq 1$ is the smallest index such that b_k is not divisible by p. By Theorem 4.2, this factorization extends to $\mathbb{Z}_p[x]$, which means that $g(x) = p^m f(x)$ is reducible, a contradiction, since $f(x)$ is the minimal polynomial of z. This completes the proof of the stronger triangle inequality. ∎

Let us make a few more remarks that are easily verified. First, as $K \simeq \mathbb{Q}_p^n$, it is evident that K is complete with respect to this extended norm. Second, if $\sigma : K \to K$ is an automorphism of K, we see that $|x|_p = |\sigma(x)|_p$ as the norms of x and $\sigma(x)$ are the same.

If we define for $x \in K$, $x \neq 0$, the function $v_p(x)$ by $|x|_p = p^{-v_p(x)}$, this extends to K the definition of v_p defined earlier for $x \in \mathbb{Q}_p^\times$. The map $v_p : K^\times \to \mathbb{Q}$ is a homomorphism into the additive group of rational numbers, whose image is easily seen to be of the form $(1/e)\mathbb{Z}$ for some divisor e of $n = [K : \mathbb{Q}_p]$ (see Exercise 7). e is called the **ramification index** of K over $\mathbb{Q}_p$. We say that $K/\mathbb{Q}_p$ is *unramified* if $e = 1$, *ramified* if $e > 1$, and *totally ramified* if $e = n$. An element $\pi \in K$ is called a *uniformizer* if $v_p(\pi) = 1/e$.

The ring

$$O_K = \{x \in K : \quad |x|_p \leq 1\}$$

now plays the analogous role of $\mathbb{Z}_p$, and the maximal ideal

$$\mathfrak{p} = \{x \in K : \quad |x|_p < 1\}$$

plays the role of $p\mathbb{Z}_p$. Sometimes, the role of p is played by a uniformizer. All of our previous theorems extend to K such as Hensel's lemma and Strassman's theorem (see Exercises 5 and 6). The notion of a Teichmüller representative (which depended on the residue field) is also easily extended.

Let us look at an important special case. Let ζ_p denote a primitive p-th root of unity and let $K = \mathbb{Q}_p(\zeta_p)$. By Exercise 2, $[K : \mathbb{Q}_p] = p - 1$. By Exercise 3, $N_{K/\mathbb{Q}_p}(1 - \zeta_p) = p$ and therefore

$$|\zeta_p - 1|_p = p^{-1/(p-1)} = r_p,$$

where r_p was defined in the previous chapter in connection with the radius of convergence of the exponential power series. (Now we see elements that actually have this absolute value.) Thus, K is totally ramified and $\pi = 1 - \zeta_p$ is a uniformizer.

As remarked above, our earlier theorems on p-adic power series extend to finite extensions of $\mathbb{Q}_p$ (see Exercise 6). Thus, we may consider the Exp and $\log_p$ functions in this setting. Consider the problem of finding the roots of $\log_p x$ in $K = \mathbb{Q}_p(\zeta_p)$. Let $\pi = 1 - \zeta_p$ be a uniformizer. Applying Strassman's theorem

shows that the power series

$$-\log_p(1-\pi x) = \sum_{n=1}^{\infty} \frac{\pi^n x^n}{n}$$

has at most p zeroes (see Exercise 8). Since $1, \zeta_p, ..., \zeta_p^{p-1}$ are roots of $\log_p x = 0$, we have found them all.

This result has now the curious consequence that the power of p dividing the numerator of the rational number

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\pi + \frac{\pi^2}{2} + \cdots + \frac{\pi^n}{n}\right)$$

tends to infinity as n tends to infinity. (Notice that this is the norm of an algebraic number over the field of rational numbers.) One can also derive a lower bound for this power of p of the form

$$n - c\log n,$$

for some constant $c > 0$ depending upon p. This can be viewed as a generalization of Exercise 5 in the previous chapter which corresponds to the case $p = 2$.

The above discussion extends the metric to any finite extension of $\mathbb{Q}_p$. It is thus clear that the metric can be extended to $\overline{\mathbb{Q}}_p$. However, we have the important theorem:

Theorem 4.4 *$\overline{\mathbb{Q}}_p$ is not complete.*

Proof. For each n coprime to p, let $f(n)$ be a primitive n-th root of unity. If p divides n, let $f(n) = 1$. Now consider the convergent series

$$\sum_{n=1}^{\infty} f(n)p^n.$$

If $\overline{\mathbb{Q}}_p$ were complete, the series would converge to some $\alpha \in \overline{\mathbb{Q}}_p$. Thus, α would lie in some finite extension K of $\mathbb{Q}_p$ (say). Observe that $f(1) = 1 \in K$. Suppose we have shown that $f(n) \in K$ for all $n < m$. We will show by induction that $f(m) \in K$ also. If m is divisible by p, there is nothing to prove. So we may suppose p is coprime to m. By the induction hypothesis,

$$\beta := p^{-m}\Big(\alpha - \sum_{n=1}^{m-1} f(n)p^n\Big) \in K.$$

Observe that

$$\beta = f(m) + pf(m+1) + p^2 f(m+2) + \cdots .$$

Let $\mathfrak{p}$ denote the maximal ideal of $\mathcal{O}_K = \{x \in K : \quad |x|_p \leq 1\}$. Then, $\beta \equiv f(m) (\mathrm{mod}\, \mathfrak{p})$ so that the equation $x^m - 1 = 0$ has a solution mod $\mathfrak{p}$ because $f(m)$ is a primitive m-th root of unity. By Hensel's lemma we can lift this solution to K. Since p is coprime to m, all the m-th roots of unity are distinct mod $\mathfrak{p}$ (see Exercise 3) and it follows that $f(m) \in K$. This proves that $f(n) \in K$ for all n. That is, all the roots of unity of order prime to p lie in K. Since the roots of unity of order prime to p are distinct mod $\mathfrak{p}$, we thus get infinitely many residue classes mod p which is a contradiction since $K/\mathbb{Q}_p$ is a finite extension.■

Now let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$ with respect to the p-adic absolute value. Thus, for $\alpha \in \overline{\mathbb{Q}}_p$ we define

$$|\alpha|_p = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}$$

and it is easily checked that this is well-defined. The definition is motivated by the fact that we expect norms to be preserved under isomorphism. Thus, $|\alpha|_p = |\sigma(\alpha)|_p$ for any automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We can extend the norm to $\mathbb{C}_p$ as before and it turns out that $\mathbb{C}_p$ is algebraically closed and $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$. To establish this, we will need an important lemma, known as Krasner's lemma, that basically says that if $\alpha \in \mathbb{C}_p$ is sufficiently close to $\beta \in \mathbb{C}_p$ and algebraic over $\mathbb{Q}_p(\beta)$, then $\alpha \in \mathbb{Q}_p(\beta)$.

Lemma 4.5 (Krasner's lemma) *Suppose K is a complete field with respect to a non-archimedean norm $|\cdot|_p$. Let $\alpha, \beta \in \overline{K}$, with α separable over $K(\beta)$. Suppose for all $K(\beta)$-conjugates $\alpha_i \neq \alpha$ of α we have*

$$|\beta - \alpha|_p < |\alpha_i - \alpha|_p.$$

Then, $K(\alpha) \subseteq K(\beta)$.

Proof. Consider $K(\alpha, \beta)/K(\beta)$ and let $L/K(\beta)$ be the Galois closure. Let $\sigma \in \mathrm{Gal}(L/K(\beta))$. Then,

$$\sigma(\beta - \alpha) = \beta - \sigma(\alpha).$$

Thus,

$$|\beta - \sigma(\alpha)|_p = |\beta - \alpha|_p < |\alpha_i - \alpha|_p,$$

for all $\alpha_i \neq \alpha$. Therefore,

$$|\alpha - \sigma(\alpha)|_p \leq \max(|\alpha - \beta|_p, |\beta - \sigma(\alpha)|_p) < |\alpha_i - \alpha|_p \quad \forall \alpha_i \neq \alpha.$$

If $\sigma(\alpha) \neq \alpha$, this is a contradiction. Thus, $\sigma(\alpha) = \alpha$ for all σ and $\alpha \in K(\beta)$ as desired. ■

We can now prove:

Theorem 4.6 *$\mathbb{C}_p$ is algebraically closed.*

Proof. Let $K = \mathbb{C}_p$ and $|\cdot|_p$ its p-adic norm. Suppose α is algebraic over K. Let $f(x)$ be its minimal polynomial in $\mathbb{C}_p[x]$. Since $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, we may choose a monic $g(x) \in \overline{\mathbb{Q}}_p[x]$ whose coefficients are sufficiently close to those of $f(x)$. Thus, $g(\alpha) = g(\alpha) - f(\alpha)$ is very small in terms of the p-adic norm. Writing $\beta = \beta_1$ with β_1 sufficiently close to α, and

$$g(x) = \prod_j (x - \beta_j)$$

we see that $|\beta - \alpha|_p < |\alpha_i - \alpha|_p$ for all conjugates $\alpha_i \neq \alpha$. By Krasner's lemma, $K(\alpha) \subseteq K(\beta) = \mathbb{C}_p(\beta) = \mathbb{C}_p$ since $\beta \in \overline{\mathbb{Q}}_p \subseteq \mathbb{C}_p$. Hence, $\alpha \in \mathbb{C}_p$. This completes the proof. ∎

Much of our previous discussion about convergence of series and power series extends to $\mathbb{C}_p$. For example, the p-adic exponential for

$$\operatorname{Exp}(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converges in $|x|_p < r_p = p^{-1/(p-1)}$. The p-adic logarithm defined by

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

is well defined for $|x|_p < 1$. These two functions are inverses of each other in the smaller domain $|x|_p < r_p$. This is clear as identities of formal power series. To prove this rigorously, we need to estimate the functions and make sure they are in the stated domain of definition. Thus, we need to show

$$|x|_p < r_p \Rightarrow |\operatorname{Exp}(x) - 1|_p < 1$$

and

$$|x|_p < r_p \Rightarrow |\log_p(1+x)|_p < r_p.$$

To verify the first inequality, note that $v_p(x) > 1/(p-1)$ implies that for $n \geq 2$,

$$v_p(x^{n-1}/n!) = (n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} = \frac{s-1}{p-1} \geq 0,$$

where s is the sum of the digits in the p-adic expansion of n. (See Exercise 7, Chapter 3.) Thus, $|x^{n-1}/n!|_p < 1$ and so $|x^n/n!|_p < |x|_p$ from which we deduce $|\operatorname{Exp}(x) - 1|_p = |x|_p < r_p$. Therefore, $\log_p(\operatorname{Exp}(x))$ can be expanded as a power

series and we are allowed to interchange summations to deduce that this equals x.

To verify that $\operatorname{Exp}(\log_p(1+x)) = 1+x$, we need to estimate the absolute value of $\log_p(1+x)$ for $|x|_p < r_p$. Indeed,

$$\begin{aligned} v_p((-1)^{n+1}x^n/n) - v_p(x) &= (n-1)v_p(x) - v_p(n) \\ &> \frac{n-1}{p-1} - v_p(n) = (n-1)\left(\frac{1}{p-1} - \frac{v_p(n)}{n-1}\right). \end{aligned}$$

If $n = p^a n_1$ with n_1 coprime to p, we have

$$\frac{v_p(n)}{n-1} = \frac{a}{p^a n_1 - 1} \leq \frac{a}{p^a - 1} = \frac{a}{(p-1)(p^{a-1} + \cdots + p + 1)} \leq \frac{1}{p-1},$$

so that $|x^n/n|_p < |x|_p$ for $n > 1$. This means $|\log_p(1+x)|_p = |x|_p < r_p$ is in the domain of definition for Exp.

Following Iwasawa, we now show that the logarithm can be extended to all of $\mathbb{C}_p^\times = \mathbb{C}_p \backslash \{0\}$.

Theorem 4.7 (Iwasawa) *There is a unique extension of* $\log_p$ *such that* $\log_p(xy) = \log_p(x) + \log_p(y)$ *for all* $x, y \in \mathbb{C}_p^\times$ *and* $\log_p p = 0$.

Proof. We begin by proving that every element x of $\mathbb{C}_p^\times$ can be written as $p^r wu$ where w is a root of unity of order prime to p and u is in $\mathbb{C}_p$ satisfies $|u-1|_p < 1$. There are a few things to check. Let us observe that the extended norm on $\overline{\mathbb{Q}}_p$ can take on only rational powers of p. Since $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, and the norm is non-archimedean, we see the same is true for $\mathbb{C}_p$. Thus, if $r = \operatorname{ord}_p(x) = a/b \in \mathbb{Q}$, let p^r denote any root of $x^b - p^a = 0$. Then, $x = p^r x_1$ with x_1 of norm 1. We can find $y_1 \in \overline{\mathbb{Q}}_p$ so that $|x_1 - y_1|_p < 1$. Then, as $|x_1|_p = 1$, again by the non-archimedean property of the metric, $|y_1|_p = 1$. Since y_1 is algebraic, by the Hensel lemma construction, let $\omega(y_1)$ denote the unique Teichmüller representative of y_1 and set $u = y_1/\omega(y_1)$. Thus, any element of $\mathbb{C}_p^\times$ can be written as $p^r wu$. This is unique up to p-power roots of unity ζ for which $\log_p \zeta = 0$. We then define the logarithm by

$$\operatorname{Log} x = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}(u-1)^n}{n}.$$

This is well-defined since we have set logarithms of roots of unity to be 0. ∎

With this extended logarithm, let us observe an interesting connection to the Fermat quotients. (Henceforth, we may use the notation 'Log' to indicate the p-adic logarithm and omit the p if it is clear which prime is meant. Sometimes, we

may write 'log' also when there is no cause for confusion.) Notice that $p^2|\mathrm{Log}\, a$ (with $\mathrm{Log}\, a \neq 0$) if and only if the Fermat quotient satisfies $F(a) \equiv 0 (\mathrm{mod}\, p)$. This is because

$$\mathrm{Log}\, a = \frac{1}{p-1}\mathrm{Log}\, a^{p-1} = \frac{1}{p-1}\mathrm{Log}\,(1+pF(a)) \equiv \frac{pF(a)}{p-1}(\mathrm{mod}\, p^2).$$

As stated in Chapter 3, the notion of a derivative is easily extended. As before, we define the derivative of a continuous function f to be

$$f'(x) = \lim_{h\to 0} \frac{f(x+h)-f(x)}{h},$$

provided this limit exists. In the p-adic metric, this means

$$f'(x) = \lim_{n\to\infty} \frac{f(x+p^n)-f(x)}{p^n},$$

provided this limit exists. Thus, for example, the derivative of x^m is mx^{m-1}.

The p-adic logarithm has nicer properties than the usual logarithm. It is locally analytic on $\mathbb{C}_p^\times$ (in the sense that given $x_0 \in \mathbb{C}_p^\times$ it has a convergent power series expansion valid in a sufficiently small neighbourhood of x_0). Since this series can be differentiated term by term, we find that

$$\frac{d}{dx}\mathrm{Log}\, x = \frac{1}{x}$$

for $x \in \mathbb{C}_p^\times$.

For $a \in \mathbb{Z}_p$, let us compute the derivative of $f(x) = a^x$ at $x = 0$. We need to compute the limit

$$\lim_{n\to\infty} \frac{a^{p^n}-1}{p^n}.$$

As we noted above, $\mathrm{Log}\, a = (\mathrm{Log}\, a^{p-1})/(p-1)$ so that it suffices to compute the limit for $a \equiv 1 (\mathrm{mod}\, p)$. Writing $a = 1+tp$ we have by the binomial theorem,

$$\begin{aligned}(1+tp)^{p^n} &= 1+\sum_{k=1}^{p^n} \frac{p^n(p^n-1)\cdots(p^n-(k-1))}{k!}(pt)^k \\ &\equiv 1+\sum_{k=1}^{p^n} \frac{p^n(-1)^{k-1}(k-1)!}{k!}(pt)^k (\mathrm{mod}\, p^{2n+1})\end{aligned}$$

from which it is clear that

$$\frac{a^{p^n}-1}{p^n} \equiv \mathrm{Log}\, a\ (\mathrm{mod}\, p^{n+1}).$$

Thus, the derivative of a^x at $x = 0$ is $\operatorname{Log} a$.

Let us make one more observation concerning the p-adic logarithm. If $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ then as $|\sigma(x)|_p = |x|_p$ for all $x \in \overline{\mathbb{Q}}_p$, we may extend σ to a continuous automorphism of $\mathbb{C}_p$. By continuity,

$$\operatorname{Log}(1+\sigma(x)) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}\sigma(x)^n}{n} = \sigma\Big(\sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}\Big) = \sigma\Big(\operatorname{Log}(1+x)\Big).$$

Thus, $\operatorname{Log}\sigma(\alpha) = \sigma(\operatorname{Log}\alpha)$ for $\alpha \in \mathbb{C}_p^\times$. In particular, for $\alpha \in \overline{\mathbb{Q}}_p$, we have $\operatorname{Log}\alpha \in \overline{\mathbb{Q}}_p$ and in fact in $\mathbb{Q}_p(\alpha)$.

Exercises

1. In Newton's method, consider the problem of finding a real root of $f(x) = x^3 - x$. If $a_n = 1/\sqrt{5}$, show that $a_{n+1} = -1/\sqrt{5}$ and $a_{n+2} = 1/\sqrt{5}$. Thus, the sequence generated by the initial value $a_0 = 1/\sqrt{5}$ does not converge.

2. Let p be prime. Show that the p-th cyclotomic polynomial $\Phi_p(x)$ given by
$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$
is irreducible in $\mathbb{Q}_p[x]$.

3. Let ζ_m be a primitive m-th root of unity. Show that
$$m = \prod_{j=1}^{m-1}(1 - \zeta_m^j).$$

4. Given that Eisenstein polynomials factor mod p (see Chapter 3, Exercise 10), why can't we use Hensel's lemma in the form of Theorem 4.2 to factor them in $\mathbb{Z}_p$?

5. (Hensel's lemma for finite extensions) Let $K/\mathbb{Q}_p$ be a finite extension and π be a uniformizer. Let $f(x) \in O_K[x]$. Suppose there is an $a_0 \in O_K$ such that $f(a_0) \equiv 0 (\operatorname{mod} \pi)$ and $f'(a_0) \not\equiv 0 (\operatorname{mod} \pi)$, where $f'(x)$ is the (formal) derivative of $f(x)$. Then, there is a unique $a \in O_K$ such that $a \equiv a_0 (\operatorname{mod} \pi)$ and $f(a) = 0$.

6. Prove that Strassman's theorem extends to finite extensions of $\mathbb{Q}_p$.

7. Let $K/\mathbb{Q}_p$ be a finite extension. Prove that the image of the map $v_p : K^\times \to \mathbb{Q}_p$ is of the form $(1/e)\mathbb{Z}$ for some e dividing $n = [K : \mathbb{Q}_p]$.

8. Let p be prime and ζ_p a primitive p-th root of unity. Set $K = \mathbb{Q}_p(\zeta_p)$ and $\pi = 1 - \zeta_p$. Prove that $|\pi^n/n|_p$ is largest when $n = p$.

9. Show that $x^3 = 2$ has a solution in $\mathbb{Q}_5$.

10. Prove the following generalization of Hensel's lemma: let $f(x) \in \mathbb{Z}_p[x]$. Write $f'(x)$ for its formal derivative. Suppose for some non-negative integer N and some integer a_0, we have $f(a_0) \equiv 0 (\bmod p^{2N+1})$ but $f'(a_0) \equiv 0 (\bmod p^N)$, $f'(a_0) \not\equiv 0 (\bmod p^{N+1})$. Show that there is a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_0 (\bmod p^{N+1})$.

Chapter 5

p-adic Interpolation

We will consider first continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$ and begin with the p-adic analogue of the classical problem of interpolating the factorials. Recall that

$$\int_0^\infty e^{-x} x^n dx = n!$$

and so the problem of finding a continuous $f(s)$ taking the value of $n!$ for $s = n$ is solved by setting

$$f(s) = \int_0^\infty e^{-x} x^s dx$$

which is the familiar gamma function $\Gamma(s+1)$.

The p-adic analogue of this problem has no solution since $n! \to 0$ (in the p-adic metric) as $n \to \infty$ in the "usual" metric. This suggests that it may be more natural to consider

$$\prod_{\substack{j \leq n \\ (j,p)=1}} j$$

as the p-adic analogue of the factorials.

If we are given a sequence of integers $\{a_k\}_{k=1}^\infty$ we can ask: when does there exist a continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ such that $f(k) = a_k$? Since $\mathbb{Z}_p$ is compact, such a function must be uniformly continuous and bounded. Thus, a necessary condition is that for each m, there must exist an integer $N = N(m)$ such that

$$k \equiv k' (\bmod p^N) \quad \Rightarrow \quad a_k \equiv a_{k'} (\bmod p^m). \tag{5.1}$$

That is, whenever k and k' are close p-adically, then a_k and $a_{k'}$ should be close p-adically. Conversely, if (5.1) is satisfied, and

$$\sup_n |a_n|_p$$

is bounded, then we can define a continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ as follows. For $x \in \mathbb{Z}_p$, let n_i be a sequence of integers tending to x and define

$$f(x) = \lim_{i \to \infty} f(n_i).$$

The limit exists by virtue of (5.1). Moreover, if n_i' is any other sequence tending to x, it is easy to see that

$$\lim_{i\to\infty} f(n_i) = \lim_{i\to\infty} f(n_i')$$

so that the function is well-defined. Thus, the interpolation problem reduces to checking (5.1). We state these observations as:

Theorem 5.0 *Suppose that a sequence of numbers $f(k), k = 0, 1, 2, \ldots$ is p-adically bounded and satisfies the following condition. For each natural number m, there is a natural number $N = N(m)$ such that*

$$k \equiv k' (\bmod p^N) \quad \Rightarrow \quad f(k) \equiv f(k') (\bmod p^m).$$

Then, there is a continuous function $\tilde{f} : \mathbb{Z}_p \to \mathbb{Z}_p$ such that $\tilde{f}(k) = f(k)$.

As an application of the above theorem, notice that if $n \equiv 1 (\bmod p)$, the function $f(k) = n^k$ can be p-adically interpolated since the condition (5.1) is easily verified. We will show below that, in fact, $f(s) = n^s$ is a p-adically analytic function for $s \in \mathbb{C}_p$ satisfying $|s|_p < p^{\frac{p-2}{p-1}}$. This region is larger than the unit disc for odd primes p.

Let us, for now, consider the sequence

$$a_k = \prod_{\substack{j<k \\ (j,p)=1}} j$$

and see if property (5.1) is satisfied. The verification, it turns out, is essentially Wilson's theorem. We must compare the p-adic distance between a_{k+p^s} and a_k. Observe that

$$a_{k+p^s} = \Big(\prod_{\substack{j \le p^s \\ (j,p)=1}} j \Big) \Big(\prod_{\substack{p^s < j < k+p^s \\ (j,p)=1}} j \Big)$$

and the first factor is just the product of a complete set of coprime residues mod p^s. In such a product, we can pair up a residue class with its inverse residue class, provided they are distinct. When a residue class x coincides with its own inverse (mod p^s), we have $x^2 \equiv 1 (\bmod p^s)$. For odd p, the only solutions of

$$x^2 \equiv 1 (\bmod p^s),$$

are $x = \pm 1$, as is evident from Hensel's lemma, so that we get

$$\begin{aligned} a_{k+p^s} &\equiv -\prod_{\substack{p^s < j < k+p^s \\ (j,p)=1}} j \pmod{p^s} \\ &\equiv -a_k \pmod{p^s}. \end{aligned}$$

Thus, if we make a slight sign adjustment in our definition of a_k, we can p-adically interpolate them.

Accordingly, following Morita, (see [Ro, p. 368]) we define the p-adic gamma function for $p \neq 2$ as: $\Gamma_p(0) := 1$, and

$$\Gamma_p(n) = (-1)^n \prod_{\substack{j<n \\ (j,p)=1}} j.$$

Our calculation above shows that

$$\Gamma_p(k + p^s) \equiv \Gamma_p(k) (\bmod p^s).$$

Thus, the existence of a continuous function $\Gamma_p(x)$ for $x \in \mathbb{Z}_p$ is established.

Recall the classical theorem of Weierstrass that a continuous function on a closed interval can be uniformly approximated by polynomials. The p-adic analogue of this is Mahler's theorem. This theorem says that given any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$, there are numbers c_k in $\mathbb{Q}_p$ such that

$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} c_k.$$

Thus the sequence of partial sums of this series gives the desired polynomial approximations for $f(x)$.

We begin with a few preliminary observations from combinatorial analysis. Our proof of Mahler's theorem will follow a treatment due to Bojanic [Bo].

If

$$\begin{aligned} n &= a_0 + a_1 p + a_2 p^2 + \cdots \\ k &= b_0 + b_1 p + b_2 p^2 + \cdots \end{aligned}$$

are the p-adic expansions of n and k respectively, it is easily seen that for p prime,

$$\binom{n}{k} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2} \cdots (\bmod p).$$

In particular,

$$\binom{p^n}{k} \equiv 0 (\bmod p)$$

for $1 \leq k \leq p^n - 1$.

Let us also recall the binomial inversion formula, which we leave to the reader as a simple exercise to verify directly:

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k \tag{5.2}$$

if and only if

$$a_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} b_k. \tag{5.3}$$

Now fix a positive integer m. If we set $a_k = (-1)^k$ for $k = m$ and 0 otherwise, then the above binomial inversion formula gives the 'orthogonality' relation:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{k}{m} = \begin{cases} (-1)^m & \text{if } n = m \\ 0 & \text{otherwise.} \end{cases} \tag{5.4}$$

If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous, let

$$a_n(f) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(k). \tag{5.5}$$

By (5.2), we have

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} a_k(f).$$

This suggests how we can solve the interpolation problem. Given a sequence $f(0), f(1), f(2), \ldots$, define $a_n(f)$ by (5.5) and set

$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} a_k(f). \tag{5.6}$$

If we can show that this is a p-adically convergent series, we are done. Observe that

$$\binom{x}{n} = \begin{cases} x(x-1)\cdots(x-n+1)/n! & \text{if } n \geq 1 \\ 1 & \text{if } n = 0 \end{cases}$$

is a continuous function of a p-adic variable and takes integer values for $x \in \mathbb{Z}$. Thus, by continuity,

$$\left| \binom{x}{n} \right|_p \leq 1$$

for all $x \in \mathbb{Z}_p$. The key idea in Mahler's theorem is to show that $|a_k(f)|_p \to 0$ as $k \to \infty$ whenever (5.1) is satisfied.

To this end, let us define the 'difference' operators Δ^n by

$$\Delta^n f(x) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(x+k).$$

Thus,

$$\begin{aligned} \Delta f(x) &= f(x+1) - f(x), \\ \Delta^2 f(x) &= f(x+2) - 2f(x+1) + f(x), \\ \cdots & \quad \cdots \end{aligned}$$

Clearly, Δ^n is a linear operator. We will use:

Lemma 5.1

$$\Delta^n f(x) = \sum_{j=0}^{m} \binom{m}{j} \Delta^{n+j} f(x-m).$$

Proof. It suffices to show that

$$f(x) = \sum_{j=0}^{m} \binom{m}{j} \Delta^j f(x-m)$$

and the result can be obtained by applying Δ^n to both sides of the equation. But

$$\begin{aligned} \sum_{j=0}^{m} \binom{m}{j} \Delta^j f(x-m) &= \sum_{j=0}^{m} \binom{m}{j} \sum_{k=0}^{j} \binom{j}{k} (-1)^{j-k} f(x-m+k) \\ &= \sum_{k=0}^{m} (-1)^k f(x-m+k) \sum_{j=0}^{m} \binom{m}{j} \binom{j}{k} (-1)^j. \end{aligned}$$

By (5.4), the inner sum is zero unless $k = m$ in which case it is $(-1)^m$. The result is now immediate. ∎

Lemma 5.2 *For any sequence $f(0), f(1), f(2), f(3), \ldots$ define*

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k).$$

Then,

$$\sum_{j=0}^{m} \binom{m}{j} a_{n+j}(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+m).$$

Proof. For $m = 0$, this is clear. By Lemma 5.1,

$$\Delta^n f(m) = \sum_{j=0}^{m} \binom{m}{j} \Delta^{n+j} f(0).$$

But

$$\Delta^n f(m) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(m+k)$$

and

$$\Delta^n f(0) = a_n(f)$$

so the result is now clear. ∎

Theorem 5.3 (Mahler, 1961) *Suppose $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous. Let*

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k).$$

Then $a_n(f) \to 0$ as $n \to \infty$ and so the series

$$\sum_{k=0}^{\infty} \binom{x}{k} a_k(f)$$

converges uniformly in $\mathbb{Z}_p$. Moreover,

$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} a_k(f).$$

Remark. This is the p-adic analogue of the classical theorem of Weierstrass that any continuous function on $[-1, 1]$ can be uniformly approximated by polynomials.

Proof. Since $\mathbb{Z}_p$ is compact and f is continuous, it is uniformly continuous. Hence, given any positive integer s, there exists a positive integer t such that for $x, y \in \mathbb{Z}_p$,

$$|x - y|_p \leq p^{-t} \quad \Rightarrow \quad |f(x) - f(y)|_p \leq p^{-s}.$$

In particular,

$$|f(k + p^t) - f(k)|_p \leq p^{-s}$$

for $k = 0, 1, 2, \ldots$ Since f is continuous on $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is compact, it is bounded there. Without loss of generality, say that $|f(x)|_p \leq 1$ for all $x \in \mathbb{Z}_p$. Then,

$|a_n(f)|_p \leq 1$ for all n. By Lemma 5.2, and the formula for a_n given there, we have

$$a_{n+p^t}(f) = -\sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j}(f) + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \{f(k+p^t) - f(k)\}.$$

Since p divides each of the binomial coefficients in the first sum, we find

$$\begin{aligned} |a_{n+p^t}(f)|_p &\leq \max_{1 \leq j < p^t} \{p^{-1}|a_{n+j}(f)|_p, p^{-s}\} \\ &\leq p^{-1} \quad \text{for } n \geq p^t \end{aligned}$$

because $|a_n(f)|_p \leq 1$. Replacing n by $n + p^t$ in the penultimate inequality, we get

$$|a_n(f)|_p \leq p^{-2} \quad \text{for } n \geq 2p^t.$$

Repeating the argument $(s-1)$ times gives

$$|a_n(f)|_p \leq p^{-s} \quad \text{for } n \geq sp^t.$$

Thus, $a_n(f) \to 0$ as $n \to \infty$. Hence, the series

$$\sum_{k=0}^{\infty} \binom{x}{k} a_k(f)$$

converges to $f(x)$ as both are continuous and equal on a dense set and as

$$\left|\binom{x}{k}\right|_p \leq 1$$

for $x \in \mathbb{Z}_p$. ∎

Corollary 5.4 *Let $\{a_n\}$ be any sequence in $\mathbb{C}_p$. Define*

$$b_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k.$$

Then, there exists a continuous function $f : \mathbb{Z}_p \to \mathbb{C}_p$ such that $f(n) = a_n$ if and only if $b_n \to 0$ as $n \to \infty$.

Proof. This is clear from Mahler's theorem. ∎

We would like to consider the question of convergence for $x \in \mathbb{C}_p$. Under certain conditions, it is possible to show that the above series extends to an analytic function for $|x|_p < R$ with $R > 1$. In deriving such a result, we follow an approach due to Washington.

Lemma 5.5 *Let $P_i(x) = \sum_{n=0}^{\infty} a_{n,i}x^n$ be a sequence of power series which converge in some fixed subset D of $\mathbb{C}_p$. Suppose for each n, $a_{n,i} \to a_{n,0}$ as $i \to \infty$ and for each $x \in D$ and $\epsilon > 0$ there is an $n_0 = n_0(x, \epsilon)$ such that*

$$\Big| \sum_{n \geq n_0} a_{n,i}x^n \Big| < \epsilon$$

uniformly in i. Then $\lim_{i\to\infty} P_i(x) = P_0(x)$ for all $x \in D$.

Proof. Given ϵ and x, choose n_0 as above. Then,

$$|P_0(x) - P_i(x)| \leq \max_{n<n_0}\{\epsilon, |a_{n,0} - a_{n,i}|_p |x|_p^n\} = \epsilon$$

for i sufficiently large. ∎

Theorem 5.6 *Suppose $r < p^{-1/(p-1)} < 1$ and for $x \in \mathbb{C}_p$,*

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

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

Remark. Notice that $R > 1$ so the theorem gives us a wider region of convergence of the series.

Proof. Let us consider the partial sums

$$P_i(x) = \sum_{n \leq i} \binom{x}{n} a_n = \sum_{n \leq i} a_{n,i}x^n.$$

Then,

$$a_{n,i} = a_n \frac{\text{integer}}{n!} + a_{n+1}\frac{\text{integer}}{(n+1)!} + \cdots$$

so that

$$|a_{n,i}|_p \leq \max_{j \geq n} |a_j/j!|_p \leq \max_{j \geq n} Mr^j p^{j/(p-1)} \leq MR^{-n}$$

since $\text{ord}_p j! \leq j/(p-1)$. Also,

$$\begin{aligned} |a_{n,i} - a_{n,i+k}|_p &= \Big| a_{i+1}\frac{\text{integer}}{(i+1)!} + \cdots + a_{i+k}\frac{\text{integer}}{(i+k)!} \Big|_p \\ &\leq MR^{-(i+1)} \to 0 \end{aligned}$$

as $i \to \infty$. Thus, $\{a_{n,i}\}_{i=1}^{\infty}$ is a Cauchy sequence. Let $a_{n,0} = \lim_{i\to\infty} a_{n,i}$. Then, $|a_{n,0}|_p \leq MR^{-n}$. Now set

$$P_0(x) = \sum_{n=0}^{\infty} a_{n,0} x^n.$$

Then, P_0 converges for $x \in \mathbb{C}_p$, with $|x|_p < R$. As the P_i are polynomials, they converge in

$$D = \{x \in \mathbb{C}_p : \quad |x|_p < R\}.$$

In addition, for $|x|_p < R$, we have

$$\Big| \sum_{n \geq n_0} a_{n,i} x^n \Big| \leq \max_{n \geq n_0} MR^{-n} |x|_p^n \to 0$$

as $n_0 \to \infty$ uniformly in i. Thus, $|P_0(x) - P_i(x)|_p \leq \epsilon$ uniformly for $|x|_p < R$. This completes the proof. ∎

By Mahler's theorem,

$$f(x) = \sum_{n=0}^{\infty} \binom{x}{n} a_f(n)$$

is a continuous function on $\mathbb{Z}_p$ whenever (5.1) is satisfied. If, in addition, the sequence $a_n = f(n)$ satisfies the growth condition of Theorem 5.6, then we get a p-adic analytic continuation of $f(x)$ to a wider domain. Theorem 5.6 can be sharpened, as we show below in Theorem 5.7. This sharper version can be used to show that $\Gamma_p(x)$ does not admit a power series expansion which converges for $x \in \mathbb{C}_p$ satisfying $|x|_p \leq 1$. (See exercise 6 below.)

Theorem 5.7 *Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be a continuous function with Mahler series*

$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} c_k.$$

Then, f is the restriction of an analytic power series

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

with $a_n \to 0$ if and only if $|c_k/k!|_p \to 0$ as $k \to \infty$.

Proof. The vector space of polynomials has the natural basis

$$1, x, x^2, \ldots$$

But we can also use the basis

$$1, (x)_1, (x)_2, ...,$$

where $(x)_k = x(x-1)...(x-k+1)$. We have the formulas

$$(x)_n = \sum_{k=0}^{n} s(n,k)x^k$$

where $s(n,k)$ are the Stirling numbers of the first kind. We also have

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k$$

where $S(n,k)$ are called the Stirling numbers of the second kind. They have a combinatorial interpretation as the number of partitions of a set of n elements into k blocks. That is, $S(n,k)$ is the number of equivalence relations on a set of n elements with exactly k equivalence classes. Hence, if we write $f(x) = \sum_n a_n x^n$, we can also write it as $\sum_k b_k(x)_k$. Since the Stirling numbers are integers, we have

$$\sup_n |a_n|_p = \sup_k |b_k|_p.$$

But $c_k = k!b_k$ and so the result follows. ∎

In the next chapter, we will use Theorem 5.6 to get a p-adic continuation of the Riemann zeta function and more generally the Dirichlet L-functions.

Notice that if $n \equiv 1 (\bmod p)$, then

$$n^s = (1+(n-1))^s = \sum_{k=0}^{\infty} \binom{s}{k} (n-1)^k$$

and we see that an application of Theorem 5.6 gives a p-adic continuation of n^s.

Let us return to $\Gamma_p(x)$ for p odd. Notice that from the definition of Γ_p, we have

$$\Gamma_p(n+1) = \begin{cases} -n\Gamma_p(n) & \text{if } (n,p)=1 \\ -\Gamma_p(n) & \text{if } (n,p) \neq 1 \end{cases}$$

for any natural number n. Thus,

$$\Gamma_p(x+1) = h_p(x)\Gamma_p(x)$$

where

$$h_p(x) = \begin{cases} -x & \text{if } |x|_p = 1 \\ -1 & \text{if } |x|_p < 1. \end{cases}$$

The 2-adic Γ function can be defined by setting

$$\Gamma_2(n) = (-1)^n \prod_{\substack{1 \le j \le n \\ (j,2)=1}} j$$

and this can be extended to a continuous function on $\mathbb{Z}_2$. Indeed,

$$\Gamma_2(n+2^s) = \Gamma_2(n) \prod_{\substack{0 \le j < 2^s \\ (n+j,2)=1}} (n+j).$$

The product above is the product of a complete set of coprime residue classes mod 2^s and it reduces to the product of elements of order 2. By our remark (made earlier in Chapter 4), the solutions of $x^2 \equiv 1 (\bmod 2^s)$ are precisely $1, -1, 2^{s-1}+1$ and $2^{s-1}-1$ for $s \ge 2$. Thus,

$$\Gamma_2(n+2^s) \equiv \Gamma_2(n) (\bmod 2^s)$$

and the existence of Γ_2 follows from Mahler's theorem.

Recall the classical formula

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin \pi x}$$

for $0 < x < 1$. The following is a p-adic analogue of this result.

Theorem 5.8 *If p is an odd prime, then for $x \in \mathbb{Z}_p$, we have*

$$\Gamma_p(x)\Gamma_p(1-x) = (-1)^{\ell(x)}$$

where $\ell(x)$ is defined as the element of $\{1, 2, ..., p\}$ satisfying $\ell(x) \equiv x (\bmod p)$.
Proof. We have

$$\begin{aligned} 1 = \Gamma_p(0) &= \Gamma_p(-1)h_p(-1) \\ &= \Gamma_p(-2)h_p(-2)h_p(-1) \end{aligned}$$

and so on. Thus,

$$\Gamma_p(-n) \prod_{j=1}^{n} h_p(-j) = 1$$

for any natural number n. Also $h_p(-j) = -1$ if $p|j$ and j otherwise. Thus,

$$\Gamma_p(-n)\Gamma_p(n+1)(-1)^{[n/p]+n+1} = 1.$$

Writing $n-1$ instead of n, we get

$$\Gamma_p(n)\Gamma_p(1-n) = (-1)^{n+[(n-1)/p]}.$$

If $n = a_0 + a_1 p + a_2 p^2 + \cdots$ is the p-adic expansion of n, then

$$[(n-1)/p] = [((a_0 - 1) + a_1 p + \cdots)/p].$$

First suppose $a_0 \neq 0$. Then,

$$[(n-1)/p] = a_1 + a_2 p + \cdots$$

so that $n - p[(n-1)/p] = a_0 = \ell(n)$. Clearly

$$(-1)^{n+[(n-1)/p]} = (-1)^{n-p[(n-1)/p]} = (-1)^{\ell(n)}$$

and the formula is proved in this case. If $a_0 = 0$,

$$n - 1 = (p-1) + b_1 p + \cdots$$

and

$$[(n-1)/p] = b_1 + b_2 p + \cdots$$

which gives

$$n - p[(n-1)/p] = p = \ell(n)$$

as claimed. The result for $x \in \mathbb{Z}_p$ follows by continuity. ∎

Consider the special case $x = 1/2$ for $p \neq 2$. Then,

$$\Gamma_p(1/2)^2 = (-1)^{\ell(1/2)}.$$

But $\ell(1/2) = \ell((p+1)/2) = (p+1)/2$ so we get

$$\Gamma_p(1/2)^2 = \begin{cases} 1 & \text{if } p \equiv 3 (\bmod 4) \\ -1 & \text{if } p \equiv 1 (\bmod 4). \end{cases}$$

Thus, unlike the complex case where $\Gamma(1/2) = \sqrt{\pi}$ is a transcendental number, we find that for odd primes p, $\Gamma_p(1/2)$ is algebraic.

In case $p \equiv 3 (\bmod 4)$, we can say more. From the above, $\Gamma_p(1/2) = \pm 1$. The sign depends on the parity of the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Indeed, let $r_1, r_2, \ldots$ be the R quadratic residues mod p which are less than $p/2$, $r_1', r_2', \ldots$ the quadratic residues greater than $p/2$, and $n_1, n_2, \ldots$ the N non-residues mod p which are less than $p/2$. Then,

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &\equiv r_1 r_2 \ldots n_1 n_2 \ldots \pmod p \\ &\equiv r_1 r_2 \ldots (p - r_1')(p - r_2') \cdots \pmod p \\ &\equiv (-1)^N r_1 r_2 \ldots r_1' r_2' \ldots \pmod p \\ &\equiv (-1)^N \pmod p \end{aligned}$$

since the product of all the quadratic residues is $\equiv 1 (\bmod p)$. Now, $R + N = (p-1)/2$. If $h(-p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$ and $(\cdot/p)$ is the Legendre symbol, we have by Dirichlet's class number formula, (see [W, p. 45, Ex. 4.5(c)])

$$h(-p)\left(2 - \left(\frac{2}{p}\right)\right) = R - N.$$

By Exercise 9

$$\Gamma_p(1/2)\left(\frac{p-1}{2}\right)! \equiv 1 \pmod p$$

so that the "sign" of $\Gamma_p(1/2)$ is determined by the parity of the class number $h(-p)$.

Gross and Koblitz obtained a nice formula for the classical Gauss and Jacobi sums in terms of the p-adic gamma function. This enabled them to derive the classical theorem of Stickelberger, giving the ideal factorization of the Gauss sums, in a more precise form. Using their theorem, Gross and Koblitz show that $\Gamma_p(a/N)$ is algebraic whenever $N|p-1$ but the proof of this fact uses p-adic cohomology. It would be nice to find a more elementary proof. It would also be nice to resolve the algebraicity of $\Gamma_p(a/N)$ in general.

Exercises

1. Prove that
$$-\Gamma_p(n+1) = (-1)^n \frac{n!}{[n/p]!p^{[n/p]}}$$
where $[x]$ denotes the greatest integer less than or equal to x.

2. Prove that if $0 \le j < p$ and m are non-negative integers, then
$$\Gamma_p(mp+j+1) = (-1)^{mp+j+1}\frac{(mp+j)!}{m!p^m}.$$

3. Show that
$$\sum_{m=0}^{\infty} \Gamma_p(mp+j+1)\frac{x^{mp+j}}{(mp+j)!} = (-1)^{j+1}x^j \exp(-x^p/p).$$

4. If $f : \mathbb{Z}_p \to \mathbb{C}_p$ is a continuous function with Mahler series
$$f(x) = \sum_{k=0}^{\infty} \binom{x}{k} c_k$$

show that

$$\sum_{k=0}^{\infty} c_k \frac{x^k}{k!} = e^{-x} \sum_{n=0}^{\infty} f(n) \frac{x^n}{n!}.$$

5. Let

$$\Gamma_p(x+1) = \sum_{k=0}^{\infty} \binom{x}{k} a_k$$

be the Mahler series of $\Gamma_p(x+1)$. Show that

$$\sum_{k=0}^{\infty} (-1)^{k+1} \frac{a_k x^k}{k!} = \frac{1-x^p}{1-x} \exp\left(x + \frac{x^p}{p}\right).$$

Hint: Write

$$\sum_{n=0}^{\infty} \Gamma_p(n+1) \frac{x^n}{n!} = \sum_{0 \le j < p} \sum_{m=0}^{\infty} \Gamma_p(mp+j+1) \frac{x^{mp+j}}{(mp+j)!}.$$

6. Show that $\Gamma_p(x+1)$ cannot be extended to a $\mathbb{C}_p$-analytic function in the domain $|x|_p \le 1$. (Hint: use the previous exercise and Theorem 5.7)

7. Let $x = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$. Prove that

$$\Gamma_p(x) \equiv \Gamma_p(a_0 + a_1 p + \cdots + a_n p^n) (\bmod p^{n+1}).$$

8. Let $p = kf + 1$ be prime and $a \le k$. Show that

$$-\frac{a}{k} \equiv af(1 + p + p^2 + \cdots + p^n) (\bmod p^{n+1}).$$

Deduce that

$$\Gamma_p\left(1 - \frac{a}{k}\right) \equiv \Gamma_p\left(1 + af + afp + \cdots + afp^n\right) (\bmod p^{n+1}).$$

9. With notation as in the previous exercise, prove that

$$\Gamma_p\left(1 - \frac{a}{k}\right) \equiv (-1)^{af+1} (af)! (\bmod p)$$

and

$$\Gamma_p\left(\frac{a}{k}\right) \equiv \frac{1}{(af)!} (\bmod p).$$

10. Deduce Theorem 5.6 from Theorem 5.7.

Chapter 6

p-adic L-functions

Let f be a natural number and χ be a primitive Dirichlet character mod f. (Sometimes, we may write f_χ for f to make its dependence on the character explicit.) We extend χ to all natural numbers by

$$\chi(n) = \begin{cases} \chi(n \bmod f) & \text{if } (n,f)=1 \\ 0 & \text{otherwise .} \end{cases}$$

The Dirichlet series, given by

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

is well-known to converge for $Re(s) > 0$ if $\chi \neq \chi_0$, the trivial character. Moreover, it extends to an entire function and satisfies a functional equation of the following form.

Define the Gauss sum

$$\tau(\chi) = \sum_{b(\bmod f)} \chi(b) e^{2\pi i b/f}$$

and set

$$\xi(s,\chi) = \pi^{-s/2} f^{s/2} \Gamma(\frac{s+a}{2}) L(s,\chi)$$

where $a = 0$ or 1 according as $\chi(-1) = 1$ or -1. (We say χ is even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$.) Then,

$$\xi(s,\chi) = w_\chi \xi(1-s,\overline{\chi})$$

where $w_\chi = \tau(\chi)/i^a f^{1/2}$. Here, $\overline{\chi}$ is the complex conjugate character of χ. One can also write the functional equation in an asymmetrical form:

$$L(1-s,\overline{\chi}) = \sqrt{\frac{2}{\pi}} \frac{f^{1/2}}{\tau(\chi)} \Big(\frac{2\pi}{f}\Big)^{\frac{1}{2}-s} \Big(\cos\frac{\pi s}{2}\Big) \Gamma(s) L(s,\chi)$$

if $\chi(-1) = 1$, and

$$L(1-s,\overline{\chi}) = -(2\pi)^{-1/2} \frac{i f^{1/2}}{\tau(\chi)} \Big(\frac{2\pi}{f}\Big)^{\frac{1}{2}-s} \Big(\sin\frac{\pi s}{2}\Big) \Gamma(s+1) L(s,\chi)$$

for $\chi(-1) = -1$, as is easily derived by an application of

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

and Legendre's duplication formula:

$$\Gamma(2s)\sqrt{\pi} = 2^{2s-1}\Gamma(s)\Gamma(s+\frac{1}{2}).$$

This allows us to derive the estimate for $k \in \mathbb{N}$,

$$|L(-k,\chi)| \leq Ck!(f/2\pi)^{2k}$$

if $\chi(-1) = 1$ and

$$|L(-k,\chi)| \leq C(k+1)!(f/2\pi)^{k}$$

if $\chi(-1) = -1$, for a certain positive constant C which is $O(\sqrt{f})$.

As hinted in Chapter 2, we can deduce the formula

$$\sum_{n=1}^{\infty} \chi(n)e^{-nx} = \sum_{k=0}^{\infty} \frac{L(-k,\chi)(-x)^k}{k!} \tag{6.1}$$

by considering the vertical line integral

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} L(s,\chi)\Gamma(s)x^{-s}ds$$

and moving the path of integration to $Re(s) = -\infty$. The left hand side of (6.1) can be simplified as follows:

$$\begin{aligned}
\sum_{n=1}^{\infty} \chi(n)e^{-nx} &= \sum_{b(\mathrm{mod}\, f)} \chi(b) \sum_{n\equiv b(\mathrm{mod}\, f), n>0} e^{-nx} \\
&= \sum_{b(\mathrm{mod}\, f)} \chi(b)\Big(\sum_{r=0}^{\infty} e^{-(fr+b)x}\Big) \\
&= \sum_{b(\mathrm{mod}\, f)} \chi(b)\frac{e^{-bx}}{1-e^{-fx}} \\
&= \sum_{b(\mathrm{mod}\, f)} \chi(b)\frac{e^{(f-b)x}}{e^{fx}-1}
\end{aligned}$$

Recall that

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

where $B_k(x)$ denotes the k-th Bernoulli polynomial. Observe that

$$\frac{e^{(f-b)x}}{e^{fx}-1} = \frac{e^{(1-b/f)fx}}{e^{fx}-1}$$

can be expanded as

$$\sum_{k=0}^{\infty} \frac{B_k(1-\frac{b}{f})x^{k-1}f^{k-1}}{k!}.$$

When we substitute this series in the calculation above, we get

$$\sum_{n=1}^{\infty} \chi(n)e^{-nx} = \sum_{k=0}^{\infty}\Big(\sum_{b(\mathrm{mod}\, f)} \chi(b)B_k\Big(1-\frac{b}{f}\Big)\Big)\frac{(fx)^{k-1}}{k!}.$$

Notice that for $k=0$, $B_0(x)=1$ and as

$$\sum_{b(\mathrm{mod}\, f)} \chi(b) = 0,$$

the polar term (that is, the term corresponding to $k=0$) disappears. We deduce

$$L(1-n,\chi) = \frac{(-f)^{n-1}}{n} \sum_{b(\mathrm{mod}\, f)} \chi(b)B_n\Big(1-\frac{b}{f}\Big).$$

Also note that

$$\frac{te^{(1-x)t}}{e^t-1} = \frac{(-t)e^{x(-t)}}{e^{-t}-1}$$

so that

$$B_k(1-x) = (-1)^k B_k(x)$$

and we deduce

$$L(1-n,\chi) = -\frac{f^{n-1}}{n} \sum_{b(\mathrm{mod}\, f)} \chi(b)B_n\Big(\frac{b}{f}\Big). \tag{6.2}$$

Defining the generalized Bernoulli numbers $B_{n,\chi}$ by the formula

$$B_{n,\chi} = f^{n-1} \sum_{b(\mathrm{mod}\, f)} \chi(b)B_n\Big(\frac{b}{f}\Big),$$

we can rewrite (6.2) as

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \tag{6.3}$$

which can be thought of as a generalisation of the corresponding result (Theorem 2.2) derived for the Riemann zeta function in Chapter 2.

This formula can also be deduced without contour integration by making use of exercises 16 and 17 in Chapter 2. In those exercises, we defined the Hurwitz zeta function as

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

for $0 < x \leq 1$. By noting that

$$-\frac{1}{x^s} + \zeta(s,x) - \zeta(s) = \sum_{n=1}^{\infty} \left(\frac{1}{(n+x)^s} - \frac{1}{n^s} \right)$$

and writing the summand as

$$\frac{1}{n^s} \left(\left(1 + \frac{x}{n}\right)^{-s} - 1 \right),$$

we use the binomial theorem to deduce

$$-\frac{1}{x^s} + \zeta(s,x) - \zeta(s) = \sum_{r=1}^{\infty} \binom{-s}{r} \zeta(s+r) x^r.$$

From this expression, we easily deduce that $(s-1)\zeta(s,x)$ extends to an entire function and that

$$\lim_{s \to 1} (s-1)\zeta(s,x) = 1.$$

Indeed, for all r sufficiently large, $\zeta(s+r)$ is absolutely bounded so that the series involving the binomial coefficients is easily seen to converge. Putting $s = 1-k$ in the penultimate expression gives

$$\zeta(1-k,x) = -\frac{B_k(x)}{k}$$

for every integer $k \geq 1$.

A Dirichlet L-function can be written as a linear combination of Hurwitz zeta functions. (In fact, historically, Hurwitz introduced his zeta function for the explicit purpose of deriving an analytic continuation of the L-series $L(s,\chi)$.) Indeed,

$$L(s,\chi) = \sum_{b (\mathrm{mod}\, f)} \chi(b) \sum_{n \equiv b (\mathrm{mod}\, f)} \frac{1}{n^s},$$

and the inner sum is really

$$f^{-s} \sum_{j=0}^{\infty} \frac{1}{\left(j + \frac{b}{f}\right)^s} = f^{-s} \zeta(s, b/f).$$

Therefore,

$$L(s,\chi) = f^{-s} \sum_{b (\mathrm{mod}\, f)} \chi(b) \zeta(s, b/f)$$

from which we deduce the analytic continuation of $L(s,\chi)$. As a consequence of the above formula, we also deduce (6.3).

Also note that

$$\begin{aligned}\sum_{b(\bmod f)} \chi(b)B_n\Big(\frac{b}{f}\Big) &= (-1)^n \sum_{b(\bmod f)} \chi(b)B_n\Big(1-\frac{b}{f}\Big)\\ &= (-1)^n\chi(-1) \sum_{b(\bmod f)} \chi(f-b)B_n\left(\frac{f-b}{f}\right)\\ &= (-1)^n\chi(-1) \sum_{b(\bmod f)} \chi(b)B_n\Big(\frac{b}{f}\Big)\end{aligned}$$

so that

$$L(1-n,\chi) = (-1)^n\chi(-1)L(1-n,\chi).$$

Thus, if χ and n have opposite parity, then $L(1-n,\chi)=0$. If they have the same parity, the functional equation shows that for $n \geq 1$,

$$|L(n,\chi)| = |\tau(\chi)|\Big(\frac{2\pi}{f}\Big)^n \left|\frac{B_{n,\overline{\chi}}}{n!}\right|.$$

Since $L(n,\chi) \neq 0$ for $n \geq 1$, it follows that $B_{n,\chi} \neq 0$ in this case.

Notice that if χ is odd, $B_{1,\chi} \neq 0$ comes from the non-vanishing of $L(1,\chi)$. This means that for $\chi(-1) = -1$,

$$B_{1,\chi} = \frac{1}{f}\sum_{a=1}^{f} \chi(a)a \neq 0$$

and no elementary proof of this simple fact is known.

For $n \geq 1$ therefore, $L(1-n,\chi) \neq 0$ if and only if $\chi(-1) = (-1)^n$. That is, $L(1-n,\chi) \neq 0$ if and only if χ and n have the same parity.

The significance of the equation (6.2) lies in the fact that the right hand side is essentially a linear combination of terms of the form

$$\sum_{k=0}^{n} \binom{n}{k}(f/b)^k B_k$$

which makes sense when n is replaced by a p-adic variable and $p|f$.

More precisely, we define the p-adic Hurwitz zeta function for $p|F$:

$$H_p(s,b,F) = \frac{1}{s-1}\frac{1}{F}\langle b\rangle^{1-s}\sum_{k=0}^{\infty}\binom{1-s}{k}(F/b)^k B_k.$$

This will be the p-adic analogue of the classical Hurwitz zeta function:

$$H(s,b,F) = \sum_{n=0}^{\infty}\left(n+\frac{b}{F}\right)^{-s} \qquad 0 < b \le F.$$

Let

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

Then:

Theorem 6.1 *Suppose $q|fF$ and $(a,p)=1$. Then, $H_p(s,a,F)$ is analytic for $s \neq 1$ and $s \in \mathbb{C}_p$ satisfying $|s|_p < qp^{-1/(p-1)}$. At $s=1$, it has a simple pole with residue $1/F$.*

Proof. We apply Theorem 5.6 to the series

$$\sum_{k=0}^{\infty}\binom{s}{k}(F/b)^k B_k. \tag{6.4}$$

Observe that by the von Staudt-Clausen theorem, we have for odd p,

$$|(F/b)^k B_k|_p \le p^{-(k-1)} = p(1/p)^k$$

so that we can take $r = 1/p$ and $M = p$ in Theorem 5.6. A stronger estimate holds for $p = 2$. In either case, (6.4) converges in

$$D = \{s \in \mathbb{C}_p : \quad |s|_p < qp^{-1/(p-1)}\}.$$

Since $1 \in D$ and any point of a p-adic disc is its 'center', D is the same as the set

$$\{s \in \mathbb{C}_p : \quad |1-s|_p < qp^{-1/(p-1)}\}.$$

This proves that

$$\sum_{k=0}^{\infty}\binom{1-s}{k}(F/b)^k B_k$$

is analytic in D. We have already remarked that $\langle b\rangle^s$ is analytic in D and hence so is $\langle b\rangle^{1-s}$. It is clear that at $s=1$, $H_p(s,b,F)$ has a simple pole at $s=1$ with residue $1/F$. This completes the proof. ∎

We can now construct the p-adic L-functions.

Theorem 6.2 *Let χ be a Dirichlet character of conductor f and let F be a multiple of q and f. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s,\chi)$ defined on*

$$D = \{s \in \mathbb{C}_p : \quad |s|_p < qp^{-1/(p-1)}\}$$

such that

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

where ω is the Teichmüller character. If $\chi = 1$, then $L_p(s,1)$ is analytic in D except for a simple pole at $s = 1$ with residue $(1-1/p)$. In fact, we have the formula

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)\langle a\rangle^{1-s}\sum_{k=0}^{\infty}\binom{1-s}{k}(F/a)^k B_k.$$

Proof. The formula for $L_p(s,\chi)$ given by

$$L_p(s,\chi) = \sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)H_p(s,a,F)$$

is analytic in D by the previous theorem, apart from $s = 1$. At $s = 1$, $L_p(s,\chi)$ has residue

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

If $\chi = 1$ the sum is $(1-1/p)$. If $\chi \neq 1$, the sum can be rewritten as

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

The first sum is 0. If $p|f$, then $\chi(pb) = 0$ for all b and the second sum is 0. If $(p,f) = 1$, then $f|(F/p)$ so again the second sum is 0. Moreover,

$$\begin{aligned} L_p(1-n,\chi) &= \sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)H_p(1-n,a,F) \\ &= -\frac{1}{nF}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)\langle a\rangle^n\sum_{k=0}^{n}\binom{n}{k}(F/a)^k B_k. \end{aligned}$$

The inner sum can be rewritten as

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}(F/a)^k B_k &= \sum_{k=0}^{n}\binom{n}{k}(F/a)^{n-k}B_{n-k}\\ &= (F/a)^n\sum_{k=0}^{n}\binom{n}{k}(a/F)^k B_{n-k}.\end{aligned}$$

Using the Teichmüller character, we can rewrite this as

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

If $p|f_{\chi\omega^{-n}}$ then $\chi\omega^{-n}(pb)=0$. Otherwise, $f_{\chi\omega^{-n}}|(F/p)$. By Exercise 1, the first term is $-B_{n,\chi\omega^{-n}}/n$ and the second term is $\chi(p)\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}/n$. Hence,

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

which completes the proof of Theorem 6.2. ∎

Thus, $L_p(s,\chi)$ interpolates the numbers

$$(1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n}).$$

If χ is an odd character, then n and $\chi\omega^{-n}$ have opposite parities and $L_p(s,\chi)$ is identically zero. If χ is even, then n and $\chi\omega^{-n}$ have the same parity and so $B_{n,\chi\omega^{-n}}\neq 0$ by a remark made earlier. Thus, $L_p(s,\chi)$ is not the zero function in this case.

We can now derive a generalization of the Kummer congruences from the following theorem.

Theorem 6.3 *Suppose $\chi\neq 1$ and $pq\nmid f_\chi$. Then*

$$L_p(s,\chi)=a_0+a_1(s-1)+a_2(s-1)^2+\cdots$$

with $|a_0|_p\leq 1$ and $p|a_i$ for $i\geq 1$.

Remark. Note that since $L_p(s,\chi)$ has radius of convergence greater than 1, we can set $s=n$ such that $(n-1,p)=1$. The convergence of the Laurent

expansion shows that $a_i \to 0$ as $i \to \infty$. Thus, we have the conclusion of the theorem for i sufficiently large.

Proof. We may choose F as in Theorem 6.2 so that $q|F$ but $pq \nmid F$. Also, we may suppose that χ is even for otherwise $L_p(s,\chi)$ is identically zero. Notice that if $j \geq 6$, then

$$\left|\frac{B_j}{j!}\frac{F^{j-1}}{a^j}\right|_p \leq p^{j/(p-1)}(p/q^{j-1}) \leq 1/q.$$

For $j = 3, 4, 5$, the same inequality holds. Therefore all the coefficients of the power series

$$\frac{1}{F}\sum_{j\geq 3}\binom{1-s}{j}(F/a)^j B_j$$

are divisible by p. Also the terms for $j \leq 2$ have possibly a q in the denominator but not pq. Similarly,

$$\langle a\rangle^{1-s} = \sum_{j=0}^{\infty}\frac{(1-s)^j}{j!}\Big(\mathrm{Log}\,\langle a\rangle\Big)^j$$

has all its coefficients in $\mathbb{Z}_p$ and they are divisible by pq for $j \geq 2$ since $q|\mathrm{Log}\,\langle a\rangle$. Thus, we need only consider the sum

$$\frac{1}{s-1}\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)\Big(1+(1-s)\mathrm{Log}\,\langle a\rangle\Big)\Big(\frac{1}{F}-\frac{1-s}{2a}+\frac{(1-s)(-s)F}{12a^2}\Big).$$

We find

$$a_0 \equiv -\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)\Big(\frac{1}{F}\mathrm{Log}\,\langle a\rangle-\frac{1}{2a}-\frac{F}{12a^2}\Big)(\mathrm{mod}\,p).$$

Now $(1/F)\mathrm{Log}\,\langle a\rangle$ and $F/12$ are in $\mathbb{Z}_p$. Since $a \equiv \omega(a)(\mathrm{mod}\,q)$,

$$\frac{1}{2}\sum_a\frac{\chi(a)}{a} \equiv \frac{1}{2}\sum_a \chi\omega^{-1}(a) \equiv 0(\mathrm{mod}\,\frac{1}{2}q),$$

since χ is even and ω is odd, $\chi\omega^{-1} \neq 1$ The last term involving F is clearly zero mod p for $p \geq 5$. For $p = 2$ or 3, $a^2 \equiv 1(\mathrm{mod}\,2)$ for $p \nmid a$ and the result is clear that the sum vanishes mod p. Next,

$$a_1 = \sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)\Big(\frac{F}{12a^2}-\frac{\mathrm{Log}\,\langle a\rangle}{2a}-\frac{F\mathrm{Log}\,\langle a\rangle}{12a^2}\Big)(\mathrm{mod}\,p).$$

All these terms are divisible by p if $p \geq 5$. If $p = 2$ or 3, then $F/12 \in \mathbb{Z}_p^\times$ and $a^2 \equiv 1$ so that

$$\sum_{(a,p)=1}\chi(a)a^{-2} \equiv \sum_{(a,p)=1}\chi(a) \equiv 0(\mathrm{mod}\,p).$$

Finally,

$$a_2 = -\sum_{(a,p)=1} \chi(a)(\mathrm{Log}\,\langle a\rangle)\frac{F}{12a^2} \equiv 0 (\mathrm{mod}\, p).$$

This completes the proof. ∎

Corollary 6.4 *If $\chi \neq 1$, then*

$$L_p(1,\chi) \equiv -\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)\mathrm{Log}\,\langle a\rangle (\mathrm{mod}\, p).$$

Corollary 6.5 *Suppose $\chi \neq 1$, $pq \nmid f$. Let $m, n \in \mathbb{Z}$ then*

$$L_p(m,\chi) \equiv L_p(n,\chi)(\mathrm{mod}\, p).$$

and both numbers are p-integral.

Both sides are congruent to a_0 in the notation of the Theorem.

Corollary 6.6 (Kummer congruences) *Suppose $m \equiv n \not\equiv 0 (\mathrm{mod}\, p-1)$ are positive even integers. Then*

$$\frac{B_m}{m} \equiv \frac{B_n}{n}(\mathrm{mod}\, p).$$

More generally, if $m \equiv n (\mathrm{mod}\, \phi(p^a)), n \not\equiv 0 (\mathrm{mod}\, p-1)$, then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n}(\mathrm{mod}\, p^a).$$

Proof. Consider $L_p(s,\omega^m) = L_p(s,\omega^n)$. Then,

$$L_p(1-m,\omega^m) = -(1-p^{m-1})\frac{B_m}{m}$$

and similarly for n. Also, as $p|a_i$ for $i \geq 1$, we have

$$\begin{aligned} L_p(1-m,\omega^m) &= a_0 + a_1(-m) + a_2(-m)^2 + \cdots \\ &\equiv a_0 + a_1(-n) + a_2(-n)^2 + \cdots (\mathrm{mod}\, p^a) \\ &\equiv L_p(1-n,\omega^n)(\mathrm{mod}\, p^a) \end{aligned}$$

from which the result follows. ∎

Theorem 6.7 *Suppose n is odd, $n \not\equiv -1 (\bmod p-1)$, then*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} (\bmod p)$$

and both sides are p-integral.

Proof. Since $n \not\equiv -1 (\bmod p-1)$, we have $\omega^{n+1} \neq 1$. Also, $\omega^n(p) = 0$, since ω^n is not the trivial character. Therefore,

$$\begin{aligned} B_{1,\omega^n} &= (1-\omega^n(p))B_{1,\omega^n} \\ &= -L_p(0,\omega^{n+1}) \\ &\equiv -L_p(1-(n+1),\omega^{n+1}) (\bmod p) \\ &\equiv (1-p^n)\frac{B_{n+1}}{n+1} (\bmod p) \\ &\equiv \frac{B_{n+1}}{n+1} (\bmod p). \end{aligned}$$

p-integrality follows from Corollary 6.5. ∎

In Chapter 2, we defined the notion of a regular prime. Recall that a prime p is called *regular* if it does not divide the numerators of the Bernoulli numbers B_k with k even and less than or equal to $p-3$. The non-vanishing of $L_p(1,\chi)$ is a theorem of Brumer and its proof uses the p-adic analog of the theory of linear forms in logarithms studied in transcendental number theory. We will not be able to prove this theorem in these lectures. However, in the case of a regular prime p, the result can be established easily by our discussion above. We have:

Theorem 6.8 *If p is a regular prime, and k is an even integer with $k \not\equiv 0 (\bmod p-1)$, then $L_p(1,\omega^k) \not\equiv 0 (\bmod p)$. In particular, $L_p(1,\omega^k) \neq 0$.*

Proof. By Theorem 6.2

$$L_p(1-k,\omega^k) \equiv (1-p^{k-1})\frac{B_k}{k} (\bmod p).$$

But, by Corollary 6.5,

$$\begin{aligned} L_p(1,\omega^k) &\equiv L_p(1-k,\omega^k) (\bmod p) \\ &\not\equiv 0 (\bmod p) \end{aligned}$$

since p is a regular prime. ∎

Let us also note that we can derive Kummer's criterion for regularity as the non-vanishing (mod p) of a special value of $L_p(s,\chi)$. Let h_p^+ be the class number of the maximal real subfield of $\mathbb{Q}(\zeta_p)$, namely, $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$. Then, the class number h_p of $\mathbb{Q}(\zeta_p)$ factors as $h_p = h_p^+ h_p^-$. By the theory of Dedekind zeta functions and Dirichlet's class number formula, we can write the integer h_p^- as

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-2} \Big(-\frac{1}{2} B_{1,\omega^j} \Big).$$

Note that

$$B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} (\operatorname{mod} \mathbb{Z}_p)$$

so that

$$-(2p)\Big(\frac{B_{1,\omega^{p-2}}}{2}\Big) \equiv 1 (\operatorname{mod} p).$$

Hence,

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \Big(-\frac{1}{2} B_{1,\omega^j} \Big) (\operatorname{mod} p).$$

By Corollary 6.7,

$$B_{1,\omega^j} \equiv \frac{B_{j+1}}{j+1} (\operatorname{mod} p),$$

so we deduce:

Theorem 6.9 *$p \nmid h_p^-$ if and only if p does not divide the numerators of B_{2k} for $1 \le k \le (p-3)/2$.*

Remark. Kummer proved that $p|h_p$ if and only if $p|h_p^-$ and thereby established his famous criterion for regularity via Theorem 6.9. There is a famous conjecture of Vandiver that p is always coprime to h_p^+ and this conjecture is still open.

We will now examine the question of whether there are infinitely many primes p such that

$$2^{p-1} \not\equiv 1 (\operatorname{mod} p^2),$$

in the context of p-adic L-functions. If χ is a Dirichlet character (mod p), then by Corollary 6.4

$$L_p(1,\chi) = -\frac{1}{p} \sum_{a=1}^{p-1} \chi(a) \operatorname{Log} \langle a \rangle (\operatorname{mod} p).$$

By a calculation derived in Chapter 3, we have

$$\operatorname{Log}\langle a\rangle \equiv pF(a)(\operatorname{mod} p)$$

where $F(a)$ is the Fermat quotient. Thus we obtain:

Theorem 6.10 *If χ is a non-trivial Dirichlet character (mod p), then*

$$L_p(1,\chi) = -\sum_{a=1}^{p-1}\chi(a)\Big(\frac{a^{p-1}-1}{p}\Big)(\operatorname{mod} p).$$

Recall that we proved

$$W_p = \frac{(p-1)!+1}{p} \equiv \sum_{a=1}^{p-1} F(a)(\operatorname{mod} p).$$

Thus, by the orthogonality relations, we obtain

Theorem 6.11

$$\frac{a^{p-1}-1}{p} + W_p \equiv \sum_{\chi\neq 1}\chi^{-1}(a)L_p(1,\chi)(\operatorname{mod} p).$$

In particular, setting $a = 1$ gives:

Corollary 6.12

$$W_p \equiv \sum_{\chi\neq 1} L_p(1,\chi)(\operatorname{mod} p).$$

In particular, we deduce that $2^{p-1} \equiv 1(\operatorname{mod} p^2)$ if and only if a certain linear combination of the values $L_p(1,\chi)$ vanishes mod p.

We conclude this chapter by making an additional remark which is of independent interest that relates congruences for certain binomial coefficients with the Wieferich congruence. For example, it is easily seen that (say by (3.4))

$$F(p-a) = F(a) + a^{p-2}(\operatorname{mod} p).$$

Wilson's theorem can be generalized to (see Exercise 7 in Chapter 2)

$$(p-k)!(k-1)! \equiv (-1)^k(\operatorname{mod} p).$$

Putting $k = (p+1)/2$ gives for odd primes p,

$$((p-1)/2)!^2 \equiv (-1)^{(p+1)/2} (\bmod p).$$

Now by (3.4), we deduce

$$W_p = \sum_{a=1}^{p-1} F(a) = 2 \sum_{a=1}^{(p-1)/2} F(a) + \sum_{a=1}^{(p-1)/2} \frac{1}{a} \pmod p.$$

Since

$$\sum_{a=1}^{(p-1)/2} F(a) \equiv F\left(\left(\frac{p-1}{2}\right)!\right) \pmod p \equiv \frac{((p-1)/2)!^{p-1} - 1}{p} \pmod p,$$

writing

$$((p-1)/2)!^2 = kp + e, \quad e = (-1)^{(p+1)/2},$$

we get

$$\frac{(kp+e)^{(p-1)/2} - 1}{p} \equiv k(\frac{p-1}{2})e \pmod p$$

so that

$$W_p \equiv -ek + \sum_{a=1}^{(p-1)/2} \frac{1}{a} \pmod p.$$

This proves:

Theorem 6.13

$$W_p \equiv \sum_{a=1}^{(p-1)/2} \frac{1}{a} - e\Big(\frac{((p-1)/2)!^2 - e}{p}\Big) \pmod p.$$

In other words,

$$\frac{(p-1)! + ((p-1)/2)!^2 e}{p} \equiv \sum_{a=1}^{(p-1)/2} \frac{1}{a} \pmod p.$$

In view of Theorem 3.3, we deduce the interesting:

Corollary 6.14 $2^p \equiv 2 (\bmod p^2)$ *if and only if*

$$\binom{p-1}{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \pmod{p^2}.$$

There are other approaches in the literature dealing with the continuation of p-adic L-functions. One approach, due to Mazur, tries to mimic the classical method of expressing ζ-functions as Mellin transforms of certain functions. From this point of view, Mazur constructs a p-adic distribution μ on $\mathbb{Z}_p$ and derives a p-adic integration theory to show that

$$(1-p^{k-1})\zeta(1-k) = \int_{\mathbb{Z}_p} x^{k-1} d\mu.$$

The Kummer congruences are then easily deduced from this formula as a consequence of the classical Fermat and Euler theorems. It also gives the p-adic continuation of the Riemann zeta function. This will be taken up in the next chapter.

It would be interesting to study special values of p-adic L-functions at other points. In chapter 8, we discuss $L_p(1,\chi)$ and its relationship to class numbers of algebraic number fields. Nothing is known about the meaning of $L_p(n,\chi)$ for $n \geq 2$ though there seems to be some relationship to K-theory.

A classical formula of Lerch gives

$$L'(0,\chi) = B_{1,\chi} \log f + \sum_{a=1}^{f} \chi(a) \log \Gamma(a/f).$$

In 1979, Ferrero and Greenberg derived a p-adic analog of this formula: if χ is even and $\chi\omega^{-1}$ has conductor f, then

$$L_p'(0,\chi) = (1-\chi\omega^{-1}(p))B_{1,\chi\omega^{-1}} \mathrm{Log}\, f + \sum_{a=1}^{f} \chi\omega^{-1}(a) \mathrm{Log}\, \Gamma_p(a/f).$$

Using the Gross-Koblitz formula relating Gauss sums to the p-adic Gamma function, they were able to deduce that $L_p'(0,\chi) \neq 0$ if $\chi\omega^{-1}(p) = 1$. Note that $L_p(0,\chi) = 0$ in this case.

A useful program of research is to derive p-adic analogues of classical formulas involving Dirichlet L-functions.

Exercises

1. Let χ be a Dirichlet character of conductor f. Let F be any multiple of f. Show that

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

Hint: show that

$$\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

2. Using the expression for $L_p(s,\chi)$ given in Theorem 6.2, show that

$$L_p(1,\chi) = \frac{1}{F} \sum_{\substack{a=1 \\ (a,p)=1}}^{F} \chi(a) \left(-\log_p\langle a\rangle + \sum_{j=1}^{\infty} \frac{B_j}{j} \left(\frac{-f}{a}\right)^j \right).$$

3. Let p be prime and note that $\chi = \omega^{(p-1)/2}$ is the quadratic character mod p given by the Legendre symbol. Using Corollary 6.5 and Theorem 6.2, show that

$$L_p(1,\chi) \equiv 2B_{(p-1)/2} (\operatorname{mod} p),$$

where B_k denotes the k-th Bernoulli number.

4. Show that

$$L_p(s,1) = \left(1 - \frac{1}{p}\right) \frac{1}{s-1} + a_0 + a_1(s-1) + \cdots$$

with $a_i \in \mathbb{Z}_p$ for $i \geq 0$.

5. Show that if $p^g(p-1)|i$ then $p^g|(B_i - 1/p - 1)$.

Chapter 7

p-adic Integration

One of the essential properties of classical zeta and L-functions is that they can all be written as a Mellin transform. That is, they can be expressed as an integral of the form

$$\int_1^\infty \frac{A(x)}{x^{s+1}} dx,$$

where $A(x)$ is a piecewise continuous function or more precisely, a step function. Our goal in this chapter is to introduce a p-adic integration theory so that the p-adic zeta and L-functions introduced in the earlier chapters can be written as some form of p-adic Mellin transforms. This approach, due to Mazur, is capable of considerable generalization and power. For instance, the Kummer congruences are an immediate consequence of such a derivation. The method can also be applied to define p-adic analogues of L-functions attached to elliptic curves and modular forms.

There are several ways to set up an integration theory for functions on $\mathbb{Z}_p$ or $\mathbb{Q}_p$. Before we explore these ways, let us recall the notion of an integral. The classical Riemann or Lebesgue integral is a linear functional from a vector space of integrable functions to $\mathbb{R}$ or $\mathbb{C}$. Thus, as a prelude to the study p-adic integration, let us investigate the more general notion of a p-adic linear functional (or a p-adic distribution).

Recall that in the p-adic topology, all sets (or "intervals") of the form

$$a + p^N \mathbb{Z}_p$$

are both closed and open. We will develop an integration theory over such sets. More precisely, let X be a compact-open subset of $\mathbb{Q}_p$ (such as an "interval" or $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$). A *p-adic distribution* μ on X is a $\mathbb{Q}_p$-linear functional on the $\mathbb{Q}_p$-vector space of locally constant functions on X. (Recall that a function f is *locally constant* if for every $x \in X$ there is a neighbourhood U such that $f(U)$ is a single element of $\mathbb{Q}_p$.) Any locally constant function is a linear combination of functions of the form $c\chi_U$ with c a constant and χ_U being the characterstic function of U. We will write $\mu(U)$ for $\mu(\chi_U)$. Locally constant functions will play the same role for p-adic integration as the step functions play in the theory of Riemann integration.

An equivalent definition is that a p-adic distribution μ on X is an additive map from the set of compact-open sets in X to $\mathbb{Q}_p$. Thus, if $U \subseteq X$ is a disjoint union of compact-open sets $U_1, U_2, ..., U_n$, then

$$\mu(U) = \mu(U_1) + \cdots + \mu(U_n).$$

A typical "interval" in $\mathbb{Q}_p$ is of the form

$$a + p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \quad |x - a|_p \leq p^{-n}\}.$$

In fact, the collection of such sets for $a \in \mathbb{Q}_p$ is a basis of open sets for $\mathbb{Q}_p$. Thus, a distribution is determined by its values on such "intervals". The following theorem makes this idea more precise and establishes the fundamental property of distributions on $\mathbb{Q}_p$.

Theorem 7.1 *Every map μ from the set of "intervals" of X to $\mathbb{Q}_p$ satisfying*

$$\mu(a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^n + p^{n+1}\mathbb{Z}_p) \tag{7.1}$$

whenever $a + p^n\mathbb{Z}_p \subseteq X$, extends uniquely to a p-adic distribution on X and conversely.

Proof. Since every compact-open $U \subseteq X$ can be written as a finite disjoint union of intervals, say $U = \cup_i I_i$, we can define

$$\mu(U) = \sum_i \mu(I_i).$$

We must check that this is well-defined. Indeed, if $U = \cup_i I_i$ and $U = \cup J_i$, where I_i and J_i are "intervals", we can refine both of these decompositions to $\cup_{ij} I_{ij}$ where the I_{ij} are intervals. The result is now clear. Uniqueness is also evident. ∎

The theorem allows us to define $\int_X f d\mu$ for locally constant functions. Indeed, writing f as a linear combination of characteristic functions χ_{U_i},

$$f = \sum_i c_i \chi_{U_i}$$

with U_i compact-open sets, we define

$$\int_X f d\mu = \sum_i c_i \mu(U_i).$$

Here are some examples of distributions. First, we have the *Haar distribution* given by

$$\mu_{Haar}(a + p^n\mathbb{Z}_p) = \frac{1}{p^n}.$$

It is easy to see that the property in Theorem 7.1 is satisfied. This is the unique distribution (up to a constant) which is translation invariant.

The *Dirac distribution* $\mu^{(a)}$ for $a \in \mathbb{Z}_p$ is defined as

$$\mu^{(a)}(U) = \begin{cases} 1 & \text{if } a \in U \\ 0 & \text{otherwise.} \end{cases}$$

Clearly,

$$\int_X f d\mu^{(a)} = f(a).$$

The *Bernoulli distribution* is defined for each positive integer k as

$$\mu_k(a + p^n\mathbb{Z}_p) = p^{n(k-1)}B_k(a/p^n),$$

where $B_k(x)$ is the k-th Bernoulli polynomial introduced in Chapter 2. We must verify that (7.1) holds. That is, we must prove that

$$p^{n(k-1)}B_k(a/p^n) = \sum_{b=0}^{p-1} p^{(n+1)(k-1)}B_k((a + bp^n)/p^{n+1}).$$

After multiplying both sides of this equation by $p^{-n(k-1)}$, the identity to be proved follows from

$$B_k(px) = p^{k-1}\sum_{b=0}^{p-1} B_k\left(x + \frac{b}{p}\right) \tag{7.2}$$

which is easily deduced from the power series generating function for the Bernoulli polynomials as follows. Recall that

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

Therefore,

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

on one hand. On the other hand, the right hand side of (7.2) is the coefficient of t^k in the power series expansion of

$$p^{k-1}\sum_{b=0}^{p-1} \frac{te^{(x+b/p)t}}{e^t - 1} = \frac{p^{k-1}te^{xt}}{e^t - 1}\sum_{b=0}^{p-1} e^{bt/p} = \frac{p^{k-1}te^{xt}}{e^t - 1}\cdot\frac{e^t - 1}{e^{t/p} - 1} = \frac{p^k(t/p)e^{px(t/p)}}{e^{(t/p)} - 1},$$

and the coefficient of t^k on the right hand side is $B_k(px)$, as required.

Therefore, μ_k is a p-adic distribution. Observe that $\mu_k(\mathbb{Z}_p) = B_k$. One can construct other distributions. An especially important one is obtained by fixing z to be a fixed $(p-1)$-th root of unity and defining

$$\nu_z(a + p^N\mathbb{Z}_p) = \frac{z^a}{1 - z^{p^N}}.$$

Notice that the denominator is $1 - z^{p^N} = 1 - z$. We leave the verification of (7.1) as an exercise (exercise 3).

A distribution μ of X is called a *measure* if there is a constant B such that

$$|\mu(U)|_p \leq B$$

for all compact-open $U \subseteq X$. Thus, in the above examples, only the Dirac distribution is a measure. Neither the Haar distribution nor the Bernoulli distribution qualifies for a measure. We will show later how one can "regularize" the Bernoulli distribution to obtain a measure.

The interest in measures is that one can develop a suitable integration theory as the following theorem shows.

Theorem 7.2 *Let μ be a p-adic measure on X and let $f : X \to \mathbb{Q}_p$ be a continuous function. Then the "Riemann sums"*

$$S_N := \sum_{\substack{0 \leq a < p^N \\ a + p^N\mathbb{Z}_p \subseteq X}} f(x_{a,N})\mu(a + p^N\mathbb{Z}_p)$$

(where the sum is taken over all a for which $a + p^N\mathbb{Z}_p \subseteq X$ and $x_{a,N}$ is chosen in the "interval" $a + p^N\mathbb{Z}_p$) converge to a limit in $\mathbb{Q}_p$ as $N \to \infty$. This limit does not depend on the choice of the $\{x_{a,N}\}$.

Proof. We first show that the sequence $\{S_N\}$ is Cauchy. Writing X as a finite union of intervals, we can choose N large enough so that every interval $a + p^N\mathbb{Z}_p$ is contained in X or disjoint from X. Let $M > N$. By the additivity of μ, we can rewrite S_N as

$$S_N = \sum_{\substack{0 \leq a < p^M \\ a + p^M\mathbb{Z}_p \subseteq X}} f(x_{\tilde{a},N})\mu(a + p^M\mathbb{Z}_p)$$

where $\tilde{a}$ denotes the least non-negative residue of a mod p^N. Let $\epsilon > 0$. By the continuity of f, we may assume that N is large enough so that $|f(x) - f(y)|_p \leq \epsilon$

whenever $x \equiv y (\bmod p^N)$ since continuity implies uniform continuity as X is compact. Then,

$$\begin{aligned} |S_N - S_M|_p &= \left| \sum_{\substack{0 \le a < p^M \\ a + p^M \mathbb{Z}_p \subseteq X}} (f(x_{\tilde{a},N}) - f(x_{a,M}))\, \mu(a + p^M \mathbb{Z}_p) \right|_p \\ &\le \max_a \left(|f(x_{\tilde{a},N}) - f(x_{a,M})|_p \cdot |\mu(a + p^M \mathbb{Z}_p)|_p \right) \\ &\le B\epsilon, \end{aligned}$$

since $x_{\tilde{a},N} \equiv x_{a,M} (\bmod p^N)$. Thus the "Riemann sums" have a limit. It is also clear that the limit is independent of the $\{x_{a,N}\}$. This completes the proof of the theorem. ∎

When a function f satisfies the hypothesis of the theorem, we will denote the limit of the Riemann sums by the symbol

$$\int_X f d\mu.$$

If we choose $x_{a,N} = a$, then the integral is seen to be equivalent to the limit

$$\lim_{N \to \infty} \sum_{0 \le a < p^N} f(a) \mu(a + p^N \mathbb{Z}_p).$$

We now introduce the Mazur measure. Let $\alpha \in \mathbb{Z}_p$. We let $(\alpha)_N$ be the rational integer between 0 and $p^N - 1$ that is congruent to $\alpha (\bmod p^N)$. Notice that if

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots,$$

then

$$(\alpha)_N = a_0 + a_1 p + \cdots + a_{N-1} p^{N-1}.$$

Therefore,

$$\frac{(\alpha)_N}{p^N} = \frac{\alpha}{p^N} - \left[\frac{\alpha}{p^N} \right],$$

where we interpret the last term as

$$\left[\frac{\alpha}{p^N} \right] = a_N + a_{N+1} p + \cdots.$$

If μ is a distribution and $\alpha \in \mathbb{Q}_p$, it is clear that $\alpha\mu$ is again a distribution. If $\alpha \in \mathbb{Z}_p^\times$, then μ' defined by $\mu'(U) = \mu(\alpha U)$ is again a distribution. Now let α be

any rational integer coprime to p and unequal to 1. We define the "regularized" Bernoulli distribution by setting

$$\mu_{k,\alpha}(U) = \mu_k(U) - \alpha^{-k}\mu_k(\alpha U)$$

for any compact open set U. It turns out that $\mu_{k,\alpha}$ is a measure. We first verify this for $k = 1$.

Clearly,

$$\begin{aligned}\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) &= \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{(\alpha a)_N}{p^N} - \frac{1}{2}\right) \\ &= \frac{(1/\alpha) - 1}{2} + \frac{a}{p^N} - \frac{1}{\alpha}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right),\end{aligned}$$

where $[\cdot]$ indicates the greatest integer function. Thus,

$$\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) = \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{(1/\alpha) - 1}{2}.$$

Since $\alpha \in \mathbb{Z}_p^\times$, $1/\alpha \in \mathbb{Z}_p$ and $((1/\alpha) - 1)/2 \in \mathbb{Z}_p$ if $p \neq 2$. If $p = 2$, then $\alpha^{-1} \equiv 1 (\bmod 2)$ and $(\alpha^{-1} - 1)/2 \in \mathbb{Z}_p$ in this case also. Thus, $\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) \in \mathbb{Z}_p$, and hence

$$|\mu_{1,\alpha}(a + p^N\mathbb{Z}_p)|_p \leq 1.$$

Since every compact-open set U is a finite disjoint union of intervals of the form $a + p^N\mathbb{Z}_p$, it follows from the non-archimedean property of the p-adic norm that $|\mu_{1,\alpha}(U)|_p \leq 1$.

To prove that $\mu_{k,\alpha}$ is a measure for every positive integer k, we need the following lemma.

Lemma 7.3 *Let d_k be the least common multiple of the denominators of the coefficients of $B_k(x)$. Then,*

$$d_k\mu_{k,\alpha}(a + p^N\mathbb{Z}_p) \equiv d_k k a^{k-1}\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) \pmod{p^N}.$$

Proof. The Bernoulli polynomial begins as

$$x^k - \frac{k}{2}x^{k-1} + \cdots$$

as is easily checked. Now, by definition,

$$d_k\mu_{k,\alpha}(a + p^N\mathbb{Z}_p) = d_k p^{N(k-1)}\left(B_k\left(\frac{a}{p^N}\right) - \alpha^{-k}B_k\left(\frac{(\alpha a)_N}{p^N}\right)\right).$$

The polynomial $d_k B_k(x)$ has integral coefficients whose first two terms are

$$d_k x^k - d_k(k/2)x^{k-1}.$$

Since $x = a/p^N$ has denominator p^N, and we are multiplying by $p^{N(k-1)}$, the terms after x^{k-2} will be divisible by p^N when we substitute $x = a/p^N$. Thus, $d_k \mu_{k,\alpha}(a + p^N)$ is congruent (mod p^N) to

$$d_k p^{N(k-1)} \left(\frac{a^k}{p^{Nk}} - \alpha^{-k} \left(\frac{(\alpha a)_N}{p^N} \right)^k - \frac{k}{2} \left(\frac{a^{k-1}}{p^{N(k-1)}} - \alpha^{-k} \left(\frac{(\alpha a)_N}{p^N} \right)^{k-1} \right) \right).$$

This expression can be simplified (modulo p^N) to d_k times

$$\left(\frac{a^k}{p^N} - \frac{p^{N(k-1)}}{\alpha^k} \left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N} \right] \right)^k - \frac{k}{2} \left(a^{k-1} - \frac{p^{N(k-1)}}{\alpha^k} \left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N} \right] \right)^{k-1} \right) \right).$$

This reduces to (modulo p^N)

$$d_k \left(\frac{a^k}{p^N} - \alpha^{-k} \left(\frac{\alpha^k a^k}{p^N} - k\alpha^{k-1} a^{k-1} \left[\frac{\alpha a}{p^N} \right] \right) - \frac{k}{2} \left(a^{k-1} - \alpha^{-k}(\alpha^{k-1} a^{k-1}) \right) \right).$$

Thus, $d_k \mu_{k,\alpha}(a + p^N \mathbb{Z}_p)$ is congruent to

$$d_k k a^{k-1} \left(\frac{1}{\alpha} \left[\frac{\alpha a}{p^N} \right] + \frac{\alpha^{-1} - 1}{2} \right) \pmod{p^N}.$$

We conclude that

$$d_k \mu_{k,\alpha}(a + p^N \mathbb{Z}_p) \equiv d_k k a^{k-1} \mu_{1,\alpha}(a + p^N \mathbb{Z}_p) \pmod{p^N}.$$

This completes the proof. ∎

The lemma immediately implies that $\mu_{k,\alpha}$ is a measure for α a p-adic unit. Notice that $\mu_k(\mathbb{Z}_p) = B_k$ and $\mu_k(p\mathbb{Z}_p) = p^{k-1} B_k$. Since α is coprime to p, $\alpha \mathbb{Z}_p = \mathbb{Z}_p$ so that $\mu_k(\alpha \mathbb{Z}_p) = \mu_k(\mathbb{Z}_p) = B_k$ and $\mu_k(\alpha p \mathbb{Z}_p) = \mu_k(p\mathbb{Z}_p) = p^{k-1} B_k$. We deduce that

$$\mu_{k,\alpha}(\mathbb{Z}_p) = (1 - \alpha^{-k}) B_k,$$

and

$$\mu_{k,\alpha}(\mathbb{Z}_p^*) = \mu_{k,\alpha}(\mathbb{Z}_p) - \mu_{k,\alpha}(p\mathbb{Z}_p) = (1 - \alpha^{-k})(1 - p^{k-1}) B_k.$$

From the previous lemma, we deduce immediately that

$$\int_X d\mu_{k,\alpha} = k \int_X x^{k-1} d\mu_{1,\alpha},$$

for any compact-open set X of $\mathbb{Z}_p$.

Putting these observations together, we have:

Theorem 7.4 (Mazur, 1972)

$$-(1-p^{k-1})B_k/k = \frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}d\mu_{1,\alpha}.$$

As we saw in earlier chapters, the left hand side can be interpreted as

$$(1-p^{k-1})\zeta(1-k)$$

which can be extended to give the p-adic zeta function. Thus, Mazur's theorem should be viewed as expressing the p-adic zeta function as a kind of "Mellin transform". In fact, Mazur's theorem immediately gives the p-adic continuation of the zeta function, as well as the Kummer congruences, in one stroke. Thus, we have

Corollary 7.5 (Kummer congruences) *If* $(p-1)\nmid i$ *and* $i \equiv j (\bmod p^n(p-1))$, *then*

$$(1-p^{i-1})\frac{B_i}{i} \equiv (1-p^{j-1})\frac{B_j}{j} (\bmod p^{n+1}).$$

Proof. Let α be a primitive root mod p. Since $p-1$ does not divide i, we have $\alpha^i \not\equiv 1 (\bmod p)$ so that $\alpha^{-i}-1$ is a p-adic unit. By Euler's theorem,

$$\alpha^{-i}-1 \equiv \alpha^{-j}-1 (\bmod p^{n+1})$$

and

$$\int_{\mathbb{Z}_p^\times} x^{i-1}d\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{j-1}d\mu_{1,\alpha} \quad (\bmod p^{n+1}),$$

from which the Kummer congruences follow. ∎

We can also deduce the p-integrality B_i/i whenever $p-1$ does not divide i from the same theorem. Indeed,

$$|B_i/i|_p = |\alpha^{-i}-1|_p^{-1}|1-p^{i-1}|_p^{-1}\left|\int_{\mathbb{Z}_p^\times} x^{i-1}d\mu_{1,\alpha}\right|_p.$$

The first two factors before the integral are coprime to p and therefore their p-adic absolute values are 1. Thus,

$$|B_i/i|_p = \left|\int_{\mathbb{Z}_p^\times} x^{i-1}d\mu_{1,\alpha}\right|_p \leq 1,$$

because $|\mu_{1,\alpha}(U)|_p \leq 1$ for all compact open subsets U. This completes the proof.

The von Staudt-Clausen theorem can be derived as well from this result. Recall that this asserts that if $(p-1)|i$, and i is even, then

$$pB_i \equiv -1 \pmod{p}.$$

Indeed, if we let

$$s_m(p) = 1^m + 2^m + \cdots (p-1)^m,$$

then by an earlier result in Chapter 2,

$$(m+1)s_m(p) = \sum_{k=0}^{m} \binom{m+1}{k} B_k p^{m+1-k}.$$

Therefore,

$$pB_m = s_m(p) - \sum_{k=0}^{m-1} \frac{1}{m+1} \binom{m+1}{k} B_k p^{m+1-k}$$

which is equal to

$$s_m(p) - \frac{p^{m+1}}{m+1} - \sum_{k=1}^{m-1} \binom{m}{k-1} \frac{B_k}{k} p^{m+1-k}.$$

By our previous discussion, $|B_k/k|_p \leq 1$ if $p-1$ does not divide k. We now write $m = (p-1)t$ and induct on t. For $t = 1$,

$$pB_{p-1} = s_{p-1} - p^{p-1} - \sum_{k=1}^{p-2} \binom{p-1}{k-1} \frac{B_k}{k} p^{p-k} \equiv -1 \pmod{p},$$

by Fermat's little theorem. The general result can now be deduced by an easy induction argument.

We can use Theorem 7.4 to give the p-adic continuation of the Riemann zeta function. Fix $s_0 \in \{0, 1, 2, ..., p-2\}$. For $s \in \mathbb{Z}_p$ ($s \neq 0$ if $s_0 = 0$), let us define

$$\zeta_{p,s_0}(s) = \frac{1}{\alpha^{-(s_0+(p-1)s)} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1} d\mu_{1,\alpha}. \tag{7.3}$$

This integral makes sense because,

$$\alpha^{-s_0+(p-1)s} = \alpha^{-s_0}(\alpha^{p-1})^{-s}$$

and $\alpha^{p-1} \equiv 1 \pmod{p}$. The same reasoning applies to the integrand.

Theorem 7.6 *For p and s_0 fixed as above, the function $\zeta_{p,s_0}(s)$ is a continuous function of s that does not depend on the choice of $\alpha \in \mathbb{Z}, (\alpha, p) = 1$ and $\alpha \neq 1$, that appears in the definition (7.3).*

Proof. The continuity of the integral is clear. It only remains to show that it is independent of α. If $\beta \in \mathbb{Z}$, with $\beta \neq 1$, $(\beta, p) = 1$, then the two functions

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

and

$$\frac{1}{\beta^{-s_0+(p-1)s} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1} d\mu_{1,\beta}$$

agree whenever $s_0 + (p-1)s = k$ is an integer greater than 0 since in both cases the value of the function is $-(1 - p^{k-1})B_k/k$. That is, both functions agree on the set of non-negative integers. Since this set is dense in $\mathbb{Z}_p$, the two continuous functions are equal. This completes the proof. ∎

Similar results can be derived for the Dirichlet L-functions as well. We refer the reader to the monograph of Koblitz [K2] for the details. To accomodate Dirichlet characters of conductor d, one considers integration on the space $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}_p$ instead of $\mathbb{Z}_p$ alone.

Exercises

1. Let X be a compact-open subset of $\mathbb{Q}_p$. Prove that a function $f : X \to \mathbb{Q}_p$ is locally constant if and only if it is a linear combination of characteristic functions of compact-open sets.

2. Show that $\mu_k(\mathbb{Z}_p^\times) = (1 - p^{k-1})B_k$.

3. Let z be a fixed $(p-1)$-th root of unity. Show that

$$v_z(a + p^N\mathbb{Z}_p) := \frac{z^a}{1 - z^{p^N}}$$

defines a measure on $\mathbb{Z}_p$.

4. Evaluate

$$\int_{\mathbb{Z}_p^\times} f(x) d\mu_{1,\alpha}$$

when $f(x) = \sum_{i=0}^n a_i x^i$.

5. (Manin) Show that Theorem 7.2 is valid for any distribution μ that satisfies
$$|p^N \mu(a + p^N \mathbb{Z}_p)|_p \to 0$$
as $N \to \infty$ and any function $f : X \to \mathbb{Q}_p$ satisfying the "Lipschitz condition": there is a positive constant $C \in \mathbb{R}$ such that for all $x, y \in X$,
$$|f(x) - f(y)|_p \leq C|x - y|_p.$$

6. Let p be an odd prime. If we define
$$\mu(a + p^n \mathbb{Z}_p) = (-1)^{S(a)}$$
where $S(a)$ denotes the sum of the p-adic digits in a, show that μ is a measure on $\mathbb{Z}_p$. Prove that
$$\int_{\mathbb{Z}_p} f(x) d\mu = 0$$
for any function f satisfying $f(-x) = -f(x)$ for all $x \in \mathbb{Z}_p$.

7. Prove that a p-adic distribution μ is a measure if and only if for some $a \in \mathbb{Z}_p$, the distribution $a\mu$ takes values in $\mathbb{Z}_p$. Show that the set of measures on a compact-open subset X of $\mathbb{Q}_p$ is a $\mathbb{Q}_p$-vector space.

8. Let X be a compact-open subset of $\mathbb{Q}_p$. If $f : X \to \mathbb{Q}_p$ is a continuous function such that $|f(x)|_p \leq A$ for all $x \in X$, and if $|\mu(U)|_p \leq B$ for all compact-open U contained in X,then
$$\left| \int_X f d\mu \right| \leq AB.$$
Deduce that if $f, g : X \to \mathbb{Q}_p$ are two continuous functions satisfying
$$|f(x) - g(x)|_p \leq \epsilon \quad \forall x \in X,$$
then
$$\left| \int_X f d\mu - \int_X g d\mu \right|_p \leq B\epsilon.$$

9. Let $p > 2$, $f(x) = 1/x$ and $\alpha = 1 + p$. Prove that
$$\int_{\mathbb{Z}_p^\times} f d\mu_{1,\alpha} \equiv -1 (\bmod p).$$
[Hint: Use the previous exercise with $g(x) = 1/a_0(x)$, where $a_0(x)$ is the first digit in the p-adic expansion of x. Thus, $f(x) \equiv g(x) (\bmod p)$ and $g(x)$ is locally constant.]

Chapter 8

Leopoldt's Formula for $L_p(1, \chi)$

In 1965, Leopoldt derived a p-adic analogue of the classical formula of Dirichlet for $L(1, \chi)$. Our goal in this chapter is to derive this formula.

In Chapter 6, we introduced the Gauss sum

$$\tau(\chi) = \sum_{b (\mathrm{mod}\, f)} \chi(b) e^{2\pi i b/f}.$$

It is well-known and easy to show that (see Exercise 1)

$$\chi(a)\tau(\overline{\chi}) = \sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i a b/f}. \tag{8.1}$$

We also need to recall the notion of primitive and imprimitive characters. Clearly, a Dirichlet character χ mod f has the property that $\chi(n+f) = \chi(n)$ for all integers n. The smallest positive integer f_χ such that $\chi(n + f_\chi) = \chi(n)$ for all integers n is called the *conductor* of χ. If the conductor of χ is f, we say that χ is a *primitive character* mod f. Otherwise, we call it an *imprimitive character* mod f. Imprimitive characters are obtained from primitive characters mod d for some proper divisor d of f in the natural way. Namely, if ψ is a character (mod d), we can extend ψ to a character mod f by simply setting $\psi(n) := \psi(n \bmod d)$. It is an easy exercise to characterize the conductor of χ in the following way. χ has conductor f if and only if for every divisor $d|f$, there is a $b \equiv 1 (\mathrm{mod}\, d)$ such that $\chi(b) \neq 1$ (see exercise 2).

From (8.1), we may deduce that

$$\sum_{a \bmod f} |\chi(a)\tau(\chi)|^2 = \sum_{b_1, b_2 \bmod f} \overline{\chi}(b_1)\chi(b_2) \sum_{a \bmod f} e^{2\pi i a(b_1 - b_2)/f}$$

and the inner sum is easily summed as a geometric progression and equals f when $b_1 \equiv b_2 (\mathrm{mod}\, f)$ and 0 otherwise. We deduce that

$$|\tau(\chi)|^2 = f.$$

Furthermore, note that setting $a = -1$ in (8.1), we obtain that

$$\chi(-1)\tau(\overline{\chi}) = \sum_{b=1}^{f} \overline{\chi}(b) e^{-2\pi i ab/f}$$

so that

$$\chi(-1)\tau(\overline{\chi}) = \overline{\tau(\chi)}.$$

Thus, $\tau(\overline{\chi}) = \chi(-1)f/\tau(\chi)$, a formula which will be useful below.

Before we prove Leopoldt's formula, let us recall the classical formula of Dirichlet. In the derivation below, we will ignore questions of convergence and relegate to the exercises their rigorous justification, which can be easily done by invoking a partial summation argument. Consider for $\chi \neq 1$,

$$\begin{aligned} L(1,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) e^{2\pi i an/f} \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) \Big(\sum_{n=1}^{\infty} \frac{e^{2\pi i an/f}}{n} \Big) \\ &= -\frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) \log(1-\zeta_f^a), \quad \zeta_f = e^{2\pi i/f}. \end{aligned}$$

Since $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)} = \chi(-1)f/\tau(\chi)$, we get

Theorem 8.1 (Dirichlet, 1850)

$$L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log(1-\zeta_f^a) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log(1-\zeta_f^{-a}).$$

This formula can be simplified further. However, it is the p-adic analogue of the above formula that Leopoldt derives. Now $\log(1-\zeta_f^a) + \log(1-\zeta_f^{-a}) = 2\log|1-\zeta_f^a|$. Thus, if χ is even,

$$L(1,\chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log|1-\zeta_f^a|.$$

For odd χ, we can use the functional equation to get (using (6.3))

$$\begin{aligned} L(1,\chi) &= \frac{\tau(\chi)\pi}{if} L(0,\overline{\chi}) \\ &= \frac{\pi i \tau(\chi)}{f} B_{1,\overline{\chi}}. \end{aligned}$$

This proves:

Corollary 8.2 *We have for $\chi \neq 1$,*

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{f^2} \sum_{a=1}^{f} \overline{\chi}(a) a \qquad \text{if } \chi(-1) = -1,$$

$$L(1,\chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log|1-\zeta_f^a| \qquad \text{if } \chi(-1) = 1.$$

A special case of Theorem 8.1 is worth considering. Let p be a prime $\equiv 1 (\bmod 4)$. Let h be the class number of $\mathbb{Q}(\sqrt{p})$ and χ the quadratic character (Legendre symbol) $(\bmod\, p)$. Let $\epsilon > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then, by Dirichlet's class number formula (see for example Exercise 10.5.2 in [EM, p. 136]),

$$2h \log \epsilon = -\sum_{a=1}^{p-1} \chi(a) \log(1-\zeta^a)$$

since $\chi(-1) = 1$ (see Exercise 8 below) and $\tau(\chi) = \sqrt{p}$ (see Exercise 5.5.14 in [M, p. 81]).

There is a famous conjecture of Ankeny, Artin and Chowla concerning the fundamental unit ϵ of $\mathbb{Q}(\sqrt{p})$. If we write $\epsilon = (t + u\sqrt{p})/2$, they conjecture that $u \not\equiv 0 (\bmod\, p)$. We will see below the connection between this conjecture and p-adic L-functions.

We now consider p-adic analogues of the second formula (since $L_p(s,\chi) \equiv 0$ for χ odd).

Theorem 8.3 (Leopoldt, 1965) *Let χ be a non-trivial even Dirichlet character of conductor f. Then,*

$$L_p(1,\chi) = -\Big(1 - \frac{\chi(p)}{p}\Big) \frac{\tau(\chi)}{f} \sum_{a=1}^{f} \chi^{-1}(a) \mathrm{Log}\,(1-\zeta_f^{-a}).$$

The first question that arises is whether $L_p(1,\chi) = 0$. In 1967, Brumer developed the p-adic analogue of Baker's theory of linear forms in logarithms and as a consequence obtained the non-vanishing of $L_p(1,\chi)$.

To prove Theorem 8.3, we will follow Washington [W], who says that his proof is essentially a shortened and simplified version of Leopoldt's proof. Let p be a prime number, χ a Dirichlet character of conductor $f > 1$, and ζ a fixed primitive f-th root of unity. Set

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

Choose a positive integer N such that $(N, fp) = 1$ and $\chi(N) \neq 1$. Let $\{\lambda\}$ be the set of all N-th roots of unity (in some algebraic closure of the p-adic field $\mathbb{Q}_p$). We will denote by $B_{n,\chi}$ the generalized Bernoulli number defined in Chapter 6. We will also denote by $\overline{\chi}(a)$ the quantity $\chi(a)^{-1}$ if $(a, f) = 1$ and 0 otherwise.

Lemma 8.4

$$-(\chi(N)N^n - 1)B_{n,\chi} = n\sum_{i=1}^{n}\sum_{\lambda\neq 1}\sum_{a=1}^{f} \frac{\overline{\chi}(a)\tau(\chi)}{fi(\lambda\zeta^a - 1)^i}\sum_{j=1}^{i}(-1)^{i-j}\binom{i}{j} j^n.$$

Proof. Let

$$g(X) = \sum_{b=1}^{f} \chi(b)X^{b-1}.$$

We have the partial fraction expansion:

$$\frac{g(X)}{X^f - 1} = \sum_{a=1}^{f} \frac{c_a}{X - \zeta^a}$$

so that

$$c_a = \operatorname*{Res}_{X=\zeta^a} \frac{g(X)}{X^f - 1} = \lim_{X\to\zeta^a} \frac{(X - \zeta^a)}{X^f - 1} g(X) = \frac{g(\zeta^a)\zeta^a}{f}.$$

Thus,

$$\begin{aligned}\sum_{b=1}^{f}\frac{\chi(b)te^{bt}}{e^{ft}-1} &= te^t\frac{g(X)}{X^f-1}\bigg|_{X=e^t}\\ &= te^t\sum_{a=1}^{f}\frac{\zeta^a}{f}\frac{g(\zeta^a)}{X-\zeta^a}\bigg|_{X=e^t}\\ &= te^t\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^t-\zeta^a},\end{aligned}$$

by (8.1) used with $\overline{\chi}$ instead of χ. Recall that (see Exercise 1, Chapter 6)

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

Therefore,

$$\begin{aligned}\sum_{n=0}^{\infty}(\chi(N)N^n-1)B_{n,\chi}\frac{t^n}{n!} &= \chi(N)\sum_{b=1}^{f}\frac{\chi(b)Nte^{bNt}}{e^{fNt}-1}-\sum_{b=1}^{f}\frac{\chi(b)te^{bt}}{e^{ft}-1}\\ &= \chi(N)e^{Nt}Nt\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^{Nt}-\zeta^a}-te^t\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^t-\zeta^a}.\end{aligned}$$

In the first sum on the right hand side, we may replace a by aN since $(N,f)=1$. Thus,

$$\sum_{n=0}^{\infty}(\chi(N)N^n-1)B_{n,\chi}\frac{t^n}{n!}=e^{Nt}Nt\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^{Nt}-\zeta^{aN}}-te^t\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^t-\zeta^a}.$$

Now,

$$X^N-\zeta^{aN}=\prod_{\lambda}(X-\lambda\zeta^a)$$

so that logarithmic differentiation gives

$$\frac{NX^{N-1}}{X^N-\zeta^{aN}}=\sum_{\lambda}\frac{1}{X-\lambda\zeta^a},$$

and the above simplifies to

$$te^t\frac{\tau(\chi)}{f}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)}{e^t-\lambda\zeta^a}.$$

Writing

$$e^t - \lambda\zeta^a = (1-\lambda\zeta^a)\left(1 - \frac{e^t-1}{\lambda\zeta^a - 1}\right)$$

we obtain that the sum can be rewritten as

$$\sum_{\lambda\neq 1}\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\frac{te^t}{1-\lambda\zeta^a}\sum_{i=0}^{\infty}\left(\frac{e^t-1}{\lambda\zeta^a-1}\right)^i$$

$$= \frac{\tau(\chi)}{f}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\overline{\chi}(a)\frac{te^t}{1-\lambda\zeta^a}\sum_{i=0}^{\infty}\frac{1}{(\lambda\zeta^a-1)^i}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}e^{jt}$$

$$= -\frac{\tau(\chi)}{f}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{i=0}^{\infty}\frac{1}{(\lambda\zeta^a-1)^{i+1}}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}\sum_{m=i}^{\infty}\frac{(j+1)^m t^{m+1}}{m!}$$

since $(e^t-1)^i$ has a power series expansion starting with t^i, the summation over m above can begin at $m=i$ as all the earlier terms must vanish. This simplifies to

$$-\frac{\tau(\chi)}{f}\sum_{\lambda\neq 1}\sum_{m=0}^{\infty}\frac{t^{m+1}}{m!}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{i=0}^{m}\frac{1}{(\lambda\zeta^a-1)^{i+1}}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}(j+1)^m.$$

We may rewrite the inner two sums as

$$\sum_{i=1}^{m+1}\frac{1}{(\lambda\zeta^a-1)^i}\sum_{j=0}^{i-1}\binom{i-1}{j}(-1)^{i-1-j}(j+1)^m$$

and observe that

$$\binom{i-1}{j} = \binom{i-1}{i-(j+1)} = \binom{i}{j+1}\frac{j+1}{i}$$

so that our expression becomes

$$-\frac{\tau(\chi)}{f}\sum_{\lambda\neq 1}\sum_{m=0}^{\infty}\frac{t^{m+1}}{m!}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{i=1}^{m+1}\frac{1}{i(\lambda\zeta^a-1)^i}\sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^{m+1}.$$

The lemma now follows by comparing coefficients of t^n. ∎

Now we can prove Theorem 8.3. We will make use of Euler's theorem

$$a^{\phi(p^n)} \equiv 1 (\operatorname{mod} p^n) \quad (a,p)=1$$

in the weaker form of a p-adic limit:

$$\lim_{n\to\infty} a^{\phi(p^n)} = 1,$$

or as $|a^{\phi(p^n)}-1|_p \le p^{-n}$ which is needed in Exercise 5. Thus,

$$(\chi(N)-1)L_p(1,\chi) = \lim_{n\to\infty}(\chi(N)N^{\phi(p^n)}-1)L(1-\phi(p^n),\chi)$$

which is by Theorem 6.2 equal to

$$-\lim_{n\to\infty}(\chi(N)N^{\phi(p^n)}-1)(1-\chi(p)p^{\phi(p^n)-1})\frac{B_{\phi(p^n),\chi}}{\phi(p^n)}.$$

By Lemma 8.4, this is equal to

$$\lim_{n\to\infty}\sum_{i=1}^{\phi(p^n)}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fi(\lambda\zeta^a-1)^i}\sum_{j=1}^{i}(-1)^{i-j}\binom{i}{j}j^{\phi(p^n)}$$

so that by Euler's theorem this is

$$= \lim_{n\to\infty}\sum_{i=1}^{\phi(p^n)}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fi(\lambda\zeta^a-1)^i}\sum_{\substack{j=1\\(p,j)=1}}^{i}(-1)^{i-j}\binom{i}{j}. \tag{8.2}$$

This step needs a little justification (see Exercise 5). Since

$$\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}=0$$

the innermost sum in (8.2) is

$$-\sum_{\substack{j=0\\p|j}}^{i}(-1)^{i-j}\binom{i}{j}.$$

Putting this fact in (8.2), (and henceforth writing log to denote $\log_p$ where there is no confusion in notation) and using p-th roots of unity to filter indices j divisible by p, shows that $(\chi(N)-1)L_p(1,\chi)$ equals

$$\begin{aligned}
&= -\lim_{n\to\infty}\sum_{i=1}^{\phi(p^n)}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fi(\lambda\zeta^a-1)^i}\frac{1}{p}\sum_{w^p=1}\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}w^j\\
&= -\lim_{n\to\infty}\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fp}\sum_{w}\sum_{i=1}^{\phi(p^n)}\frac{1}{i}\left(\frac{w-1}{\lambda\zeta^a-1}\right)^i\\
&= \sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fp}\sum_{w}\log\left(1-\frac{w-1}{\lambda\zeta^a-1}\right)
\end{aligned}$$

since $(\lambda\zeta^a)^{fp}\neq 1$ and thus, $(\lambda\zeta^a)^p\neq 1$. We therefore have

$$|(w-1)/(\lambda\zeta^a-1)|_p<1$$

so that the series for the logarithm converges. Taking into account the sum over the p-th roots of unity, we obtain that the limit in question is

$$\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fp}\log\left(\prod_{w^p=1}\frac{\lambda\zeta^a-w}{\lambda\zeta^a-1}\right)$$

$$=\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{fp}\left(\log(\lambda^p\zeta^{ap}-1)-p\log(\lambda\zeta^a-1)\right).$$

If $p|f$, we may by the definition of the conductor f, choose $b\equiv 1(\bmod f/p)$ such that $\chi(b)\neq 1$ and $(b,f)=1$ (see Exercise 2). Thus,

$$\begin{aligned}\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^{ap}-1) &= \sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^{apb}-1)\\ &= \chi(b)\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^{ap}-1)\end{aligned}$$

and as $\chi(b)\neq 1$, the above sum vanishes and we deduce that if $p|f$,

$$(\chi(N)-1)L_p(1,\chi)=-\sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{f}\log(\lambda\zeta^a-1).$$

If $(p,f)=1$, then

$$\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^{ap}-1)=\chi(p)\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^a-1).$$

As λ runs through non-trivial N-th roots of unity, so does λ^p, and we can write

$$\chi(p)\sum_{\lambda\neq 1}\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda^p\zeta^a-1)=\chi(p)\sum_{\lambda\neq 1}\sum_{a=1}^{f}\overline{\chi}(a)\log(\lambda\zeta^a-1).$$

In either case, we obtain

$$\begin{aligned}(\chi(N)-1)L_p(1,\chi) &= \sum_{\lambda\neq 1}\sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{f}\left(\frac{\chi(p)}{p}-1\right)\log(\lambda\zeta^a-1)\\ &= \sum_{a=1}^{f}\frac{\overline{\chi}(a)\tau(\chi)}{f}\left(\frac{\chi(p)}{p}-1\right)\log\frac{\zeta^{aN}-1}{\zeta^a-1}\\ &= (\chi(N)-1)\left(\frac{\chi(p)}{p}-1\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\log(\zeta^a-1).\end{aligned}$$

Since $\chi(N) \neq 1$ and $\log(\zeta^a - 1) = \log(1 - \zeta^{-a})$, we obtain

$$L_p(1,\chi) = -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\log(1-\zeta^{-a}),$$

which is Leopoldt's theorem. ∎

The above derivation also gives us a new analytic expression for $L_p(s,\chi)$:

Theorem 8.5 *Suppose $\chi \neq 1$, $f \neq p$, and ζ is a primitive$f$-th root of unity. Then, for $s \in \mathbb{Z}_p$, we have*

$$L_p(s,\chi) = -\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{i=1}^{\infty}\frac{1}{i(\zeta^a-1)^i}\sum_{\substack{j=1\\(p,j)=1}}^{i}\binom{i}{j}(-1)^{i-j}\langle j\rangle^{1-s}.$$

Proof. We have $L_p(s,\chi) = \lim_{n\to\infty} L_p(1-n,\chi)$ where $n = (p-1)m \to \infty$ and $m \to (1-s)/(p-1)$ p-adically. So

$$L_p(s,\chi) = -\lim_{n\to\infty}(1-\chi(p)p^{n-1})\frac{B_{n,\chi}}{n} = \lim_{n\to\infty}\frac{B_{n,\chi}}{n}.$$

By Exercise 6, we have

$$\frac{B_{n,\chi}}{n} = -\frac{\tau(\chi)}{f}\sum_{a=1}^{f-1}\sum_{i=1}^{n}\frac{\overline{\chi}(a)}{i(\zeta^a-1)^i}\sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^n.$$

Since

$$\lim_{n\to\infty} j^n = \lim_{n\to\infty}(\omega(j)\langle j\rangle)^n = \lim_{n\to\infty}\langle j\rangle^n = \langle j\rangle^{1-s}$$

for $(p,j) = 1$, the result follows. The justification of the termwise evaluation of the limit is the same as indicated in Exercise 5. ∎

We can use Theorem 8.3 to prove:

Theorem 8.6 (Ankeny, Artin and Chowla, 1952) *Let p be a prime $\equiv 1 \pmod 4$. Let h be the class number of $\mathbb{Q}(\sqrt{p})$ and $\epsilon = (t+u\sqrt{p})/2 > 1$ be its fundamental unit. Then,*

$$\frac{uh}{t} \equiv B_{(p-1)/2} \pmod p$$

where B_k denotes the k-th Bernoulli number.

Proof. By our remark following Theorem 8.1, we have

$$2h\log\epsilon = -\sum_{a=1}^{p-1}\chi(a)\log(1-\zeta_p^a)$$

so that

$$\epsilon^{-2h} = \prod_{a=1}^{p-1}(1-\zeta_p^a)^{\chi(a)}.$$

In $\overline{\mathbb{Q}}_p$ we may choose ζ_p, ϵ and $\sqrt{p}$ so that $\tau(\chi)=\sqrt{p}$ and the above relation holds. Fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$. Since the above inequality holds in $\overline{\mathbb{Q}}$, it holds in $\mathbb{C}_p$. Taking p-adic logarithms, we get

$$\begin{aligned}
2h\mathrm{Log}\,\epsilon &= -\sum_{a=1}^{p-1}\chi(a)\mathrm{Log}\,(1-\zeta_p^a)\\
&= -\frac{\tau(\chi)\sqrt{p}}{p}\sum_{a=1}^{p-1}\chi(a)\mathrm{Log}\,(1-\zeta_p^a)\\
&= \left(1-\frac{\chi(p)}{p}\right)^{-1}\sqrt{p}L_p(1,\chi)\\
&= \sqrt{p}L_p(1,\chi)
\end{aligned}$$

by Theorem 8.3. Now, $\chi=\omega^{(p-1)/2}$ since χ is a quadratic character of conductor p. By Corollary 6.5 and Theorem 6.2, we obtain

$$\begin{aligned}
L_p(1,\chi) &\equiv L_p(1-\frac{p-1}{2},\chi)\\
&\equiv \left(1-p^{(p-1)/2}\right)\frac{B_{(p-1)/2}}{(p-1)/2}\\
&\equiv 2B_{(p-1)/2}(\mathrm{mod}\,p).
\end{aligned}$$

By Exercise 7, $\mathrm{Log}\,r\equiv 0(\mathrm{mod}\,p)$ for any rational number r so that

$$\begin{aligned}
\mathrm{Log}\,\epsilon &= \mathrm{Log}\,(t/2)+\mathrm{Log}\left(1+\frac{u}{t}\sqrt{p}\right)\\
&\equiv \frac{u}{t}\sqrt{p}(\mathrm{mod}\,p)
\end{aligned}$$

so that

$$\frac{hu}{t}\equiv B_{(p-1)/2}(\mathrm{mod}\,p),$$

which completes the proof. ∎

As mentioned earlier, the Ankeny-Artin-Chowla (AAC) conjecture predicts that $u \not\equiv 0 (\bmod p)$. One can show (see for example, Exercise 6.5.8 on p. 77 of [EM]) that $h < \sqrt{p}$. Thus, the significance of the conjecture is that if $u \not\equiv 0 (\bmod p)$, the congruence determines h. Moreover, we see that $u \not\equiv 0 (\bmod p)$ is equivalent to the numerator of $B_{(p-1)/2}$ being coprime to p. In particular, if p is regular, then the AAC conjecture is true. However, we still do not know if their conjecture is true for infinitely many primes.

If p is a prime of the form n^2+1, and $n > 2$, then one can show that $\epsilon = n + \sqrt{n^2+1}$ is a fundamental unit of $\mathbb{Q}(\sqrt{p})$ (see Exercise 9). Hence for such primes, the AAC conjecture is true.

Some heuristic reasoning can be given against the conjecture. If we view the numerator of $B_{(p-1)/2}$ as a random number, then the probability that it is divisible by p is $1/p$. Thus, the expected number of primes $p \leq x$ with $p \equiv 1 (\bmod 4)$ and p dividing the numerator of $B_{(p-1)/2}$ is

$$\sum_{\substack{p \leq x \\ p \equiv 1 (\bmod 4)}} \frac{1}{p} \sim \frac{1}{2} \log \log x.$$

This heuristic reasoning predicts that the AAC conjecture is false. For $p < 6,270,713$, the conjecture has been verified. However, this range is too small a range for any tangible counterexample to show up.

This conjecture is quite analogous to the existence of primes p such that

$$2^{(p-1)} \not\equiv 1 (\bmod p^2). \tag{8.3}$$

As we saw in Chapter 1, the ABC conjecture predicts that there are infinitely many p for which (8.3) holds. Recall that this would follow if had the following. Writing, $2^n - 1 = u_n v_n$ with $(u_n, v_n) = 1$, u_n squarefree and v_n squarefull, it suffices to show that $u_n \to \infty$ as $n \to \infty$.

Now we consider the question of whether $u_n \to \infty$ can be proved unconditionally. If $n = 2k \geq 5$, we get

$$2^{2k} - u_{2k} v_{2k} = 1.$$

As v_{2k} is squarefull, we can write it as

$$v_{2k} = a_{2k}^2 b_{2k}^3$$

and one can show that

$$2^k - a_{2k} b_{2k} \sqrt{u_{2k} b_{2k}}$$

is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{u_{2k}b_{2k}})$. Thus, this leads to the question of whether, given a real quadratic field $\mathbb{Q}(\sqrt{D})$, the fundamental unit

$$\epsilon_D = t_D + u_D\sqrt{D}$$

satisfies $u_D \equiv 0 (\bmod D)$.

We conclude by noting that by an old theorem of Brahmagupta (8th century AD) (see [We, p. 19]) there are infinitely many such quadratic fields. The Ankeny- Artin-Chowla conjecture predicts that for $D = p \equiv 1 (\bmod 4)$, this should not happen. Heuristic reasoning would suggest however that it is a sparse phenomena much like the case primes not satisfying (8.3).

Returning to $L_p(1,\chi)$ and the problem of its non-vanishing, we introduce the p-adic regulator. Let K be a number field. Fix an embedding of $\mathbb{C}_p$ into $\mathbb{C}$. Then any embedding of K into $\mathbb{C}_p$ becomes an embedding into $\mathbb{C}$, and hence may be considered real or complex depending on the image of K. Let r_1 be the number of real embeddings and $2r_2$ the number of complex embeddings for K in the customary notation. We list these, as usual, as

$$\sigma_1, ...\sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, ...\sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$$

and set $r = r_1 + r_2 - 1$. Let $\delta_i = 1$ if σ_i is real and 2 if σ_i is complex. Let $\epsilon_1, ..., \epsilon_r$ be independent units of K. Then, we define

$$R_{K,p}(\epsilon_1, ..., \epsilon_r) = \det(\delta_i \mathrm{Log}\,(\sigma_j \epsilon_j))_{1\le i,j\le r}.$$

Of course, this may depend upon the embedding of $\mathbb{C}_p$ into $\mathbb{C}$ but this will not affect its p-adic valuation which is what we will be interested in. Also, the regulator defined is only up to sign.

If $\{\epsilon_1, ..., \epsilon_r\}$ is a basis for the units of K modulo roots of unity, then we define $R_p(K)$ to be

$$R_{K,p}(\epsilon_1, ..., \epsilon_r)$$

to be the p-adic regulator of K. We state:

Theorem 8.7 (Leopoldt) *Let K be a totally real abelian number field of degree n corresponding to a group X of Dirichlet characters. Let $h(K)$ be the class number of K and d_K its discriminant. Then,*

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d_K}} = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi)$$

up to signs.

If we define the p-adic ζ-function of K as

$$\zeta_{K,p}(s) = \prod_{\chi \in X} L_p(s,\chi)$$

then we obtain

$$\lim_{s\to 1}(s-1)\zeta_{K,p}(s) = \frac{2^{n-1}h(K)R_p(K)}{\sqrt{d_K}}.$$

Thus, if $R_p(K) \neq 0$, then $\zeta_{K,p}(s)$ has a simple pole at $s = 1$ with a residue which is the p-adic analogue of the residue in the complex case. As mentioned earlier, Brumer proved that $R_p(K) \neq 0$. The notion of the p-adic zeta function can still be defined in the case K is an arbitrary totally real number field and it is an unsolved problem to show $R_p(K) \neq 0$ in this case.

Exercises

1. Let χ be a non-trivial character mod f. Show that

$$\chi(a)\tau(\overline{\chi}) = \sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i ab/f}.$$

2. Let χ be a primitive character mod f. Show that for any proper divisor d of f, there is a $b \equiv 1 (\bmod d)$ such that $\chi(b) \neq 1$.

3. Prove that

$$\sum_{n=1}^{\infty} \frac{e^{2\pi i an/f}}{n}$$

converges to $\log(1 - e^{2\pi a/f})$ whenever $(a, f) = 1$.

4. Justify the derivation of the formula for $L(1,\chi)$ at the beginning of this chapter.

5. Justify the limit process in formula (8.2). You will have to determine precisely the power of p that may enter into the denominators of the expression in (8.2).

6. Let $\chi \neq 1$ be a Dirichlet character of conductor $f \neq p$. Let ζ be a primitive f-th root of unity. Prove the following variation of Lemma 8.4:

$$\frac{B_{n,\chi}}{n} = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f-1} \sum_{i=1}^{n} \frac{\overline{\chi}(a)}{i(\zeta^a - 1)^i} \sum_{j=1}^{i} \binom{i}{j} (-1)^{i-j} j^n.$$

7. If $r \in \mathbb{Q}$, show that $\operatorname{Log} r \equiv 0 (\operatorname{mod} p)$.

8. Let p be a prime $\equiv 1 (\operatorname{mod} 4)$ and χ the unique character $(\operatorname{mod} p)$ of order 2. Show that $\chi(-1) = 1$.

9. Suppose $n^2 + 1$ is squarefree with $n > 2$. Show that $\epsilon = n + \sqrt{n^2+1}$ is the fundamental unit of $\mathbb{Q}(\sqrt{n^2+1})$.

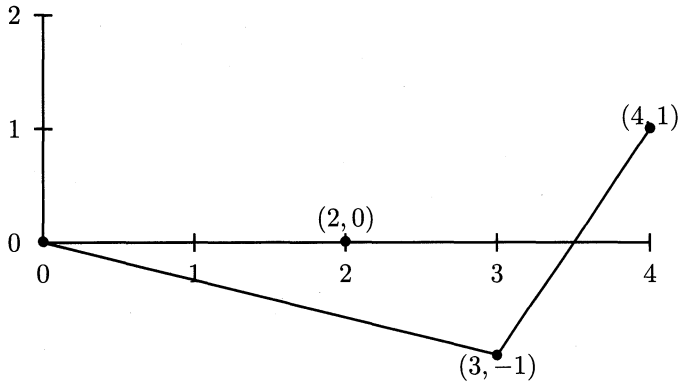
10. Let D be squarefree and $\equiv 1 (\operatorname{mod} 4)$. Suppose that $\epsilon = (a + b\sqrt{D})/2 > 1$ is the fundamental unit of $\mathbb{Q}(\sqrt{D})$. If $(u+v\sqrt{D})/2$ is any other unit, show that $b|v$.

Chapter 9

Newton Polygons

Let $f(x) = 1 + \sum_{i=1}^{n} a_i x^i \in \mathbb{C}_p[x]$ be a polynomial of degree n with coefficients in $\mathbb{C}_p$ and constant term 1. We look at the set of points in $\mathbb{R}^2$ consisting of $(0,0)$ and $(i, \mathrm{ord}_p a_i)$, $1 \leq i \leq n$. If $a_i = 0$, we think of $\mathrm{ord}_p a_i = \infty$ and usually omit that point. The *Newton polygon* of $f(x)$ is defined as the "convex hull" of this set of points. More precisely, it is constructed by taking the vertical line through $(0,0)$ and rotating it counter-clockwise, with $(0,0)$ as the center, until it hits any of the points $(i, \mathrm{ord}_p a_i)$, say $(i_1, \mathrm{ord}_p a_{i_1})$, and then taking the new point $(i_1, \mathrm{ord}_p a_{i_1})$ as the center and rotating the line further until it hits another one of the points $(i, \mathrm{ord}_p a_i)$, say $(i_2, \mathrm{ord}_p a_{i_2})$, until we reach $(n, \mathrm{ord}_p a_n)$. For example, the Newton polygon for $f(x) = 1 + x^2 + (1/3)x^3 + 3x^4 \in \mathbb{C}_3[x]$ is given by the following graph:

Fig. 2: Newton Polygon for $f(x) = 1 + x^2 + \frac{1}{3}x^3 + 3x^4 \in \mathbb{C}_3[x]$



The *vertices* of a Newton polygon are defined to be $(i_j, \mathrm{ord}_p a_{i_j})$, where the slopes change. If a segment joins (a, b) to (c, d), its *slope* is defined as $(d-b)/(c-a)$ and the *length* of the slope is simply $(c-a)$.

Theorem 9.1 *Let*

$$f(x) = \left(1 - \frac{x}{\alpha_1}\right)\left(1 - \frac{x}{\alpha_2}\right)\cdots\left(1 - \frac{x}{\alpha_n}\right)$$

be the factorization of $f(x)$ in terms of its roots $\alpha \in \mathbb{C}_p$. Let $\lambda_i = \mathrm{ord}_p(1/\alpha_i)$. If λ is a slope of length m of the Newton polygon of $f(x)$, then precisely m of the λ_i are equal to λ.

Remark. In other words, the slopes of the Newton polygon of f "are" (counting multiplicity) the p-adic ordinals of the reciprocal roots of $f(x)$.

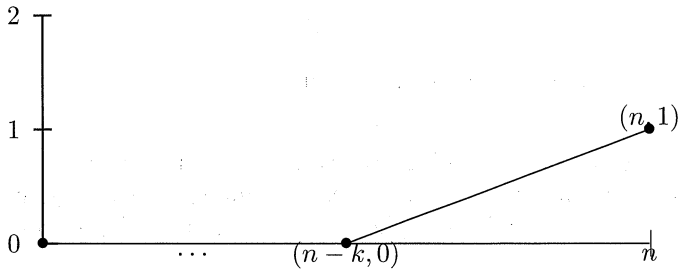
Proof. We may suppose the α_i to be arranged so that $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Suppose for the sake of definiteness, $\lambda_1 = \lambda_2 = \cdots = \lambda_r < \lambda_{r+1}$. We will show that the first segment of the Newton polygon is the segment joining $(0,0)$ to $(r, r\lambda_1)$. Recall that each a_i is $(-1)^i$ times the i-th symmetric polynomial of the roots $1/\alpha_j$'s. The p-adic ordinal of such a product is at least $i\lambda_1$ so that the p-adic ordinal of a_i is at least $i\lambda_1$. Therefore, the point $(i, \mathrm{ord}_p a_i)$ is on or above the point $(i, i\lambda_1)$, that is, on or above the line joining $(0,0)$ to $(r, r\lambda_1)$. Now look at a_r. It can be written as various products of r of the $1/\alpha_j$'s, with exactly one term having p-adic ordinal $r\lambda_1$. All of the other products have p-adic ordinal greater than $r\lambda_1$. By the property of the p-adic norm, (or by the "isosceles triangle principle") we deduce that $\mathrm{ord}_p a_r = r\lambda_1$.

Now suppose $i > r$. As before, all of the products of i of the $1/\alpha_j$'s have p-adic ordinal $> i\lambda_1$. Therefore, $\mathrm{ord}_p a_i > i\lambda_1$. By the definition of the construction of the Newton polygon, this means that the first segment is the line joining $(0,0)$ to $(r, r\lambda_1)$. The remainder of the proof is completely analogous and we leave it as an exercise. ∎

Theorem 9.1 has many interesting consequences. First, let us observe that if $f(x) \in \mathbb{Q}_p[x]$ is irreducible, then all the roots of f have the same p-adic norm. Therefore, the Newton polygon of an irreducible polynomial in $\mathbb{Q}_p[x]$ consists of one line segment with slope of length equal to the degree of f. In particular, if the Newton polygon does not consist of a single line segment, then necessarily, the polynomial is reducible in $\mathbb{Q}_p[x]$. (The same logic applies if $f(x) \in K[x]$ where K is a finite extension of $\mathbb{Q}_p$.) The converse, however, is not true (see Exercise 1). Another interesting consequence of it is the familiar Eisenstein irreducibility criterion. Notice that if the Newton polygon of a polynomial consists of a single line segment joining $(0,0)$ to (n, m) with m coprime to n, then the polynomial is irreducible. Indeed, any root α of $f(x)$ has $\mathrm{ord}_p \alpha = m/n$. If $f(x)$ factored as a product of two polynomials of smaller degree, then at least

one root α would have $\mathrm{ord}_p\alpha$ equal to a fraction with denominator strictly smaller than n which contradicts Theorem 9.1. In particular, if f is Eisenstein, its Newton polygon consists of a single line segment joining $(0,0)$ to $(n,1)$. By the above reasoning, it is irreducible.

Fig. 3: Newton Polygon for almost Eisenstein polynomials



One more case is worth noting. We may consider 'almost' Eisenstein polynomials of the form $f(x) = 1+a_1x+a_2x^2+\cdots+a_nx^n$, with integer coefficients (or coefficients in $\mathbb{Z}_p$) such that $p|a_{n-i}$ for $0 \le i \le k-1$ and $p^2 \nmid a_n$, then $f(x)$ has an irreducible factor of degree $\ge k$. (This appears as Exercise 3.3.11 in [EM, p.35].) This result can also be deduced p-adically from Theorem 9.1 as follows. In fact, more can be deduced from the Newton polygon which has the form illustrated in Figure 3. It has two slopes $1/k$ and 0, of lengths k and $n-k$ respectively. By Theorem 9.1, the roots of $f(x)$ can be partitioned into two groups, one group consisting of p-adic units and the other not. The group consisting of roots which are not p-adic units give rise to a factor which is p-Eisenstein. If $p \nmid a_{n-k}$, then $f(x)$ has an irreducible factor of degree k.

We now want to extend this theory to power series. The natural way to proceed is to consider a power series

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i \in \mathbb{C}_p[[x]]$$

and define the Newton polygon of $f(x)$ to be the "limit" of the Newton polygons of polynomials formed from the partial sums:

$$f_n(x) = 1 + \sum_{i=1}^{n} a_i x^i.$$

We could describe this as before. First plot all the points $(i, \mathrm{ord}_p a_i)$ and "rotate" the vertical line through $(0,0)$ counterclockwise until it hits some point

$(i_1, \mathrm{ord}_p a_{i_1})$, then break the line at that point and rotate with that point as the center and so forth.

In this construction, three possibilities arise. First, we may get infinitely many segments of finite length. For example, if

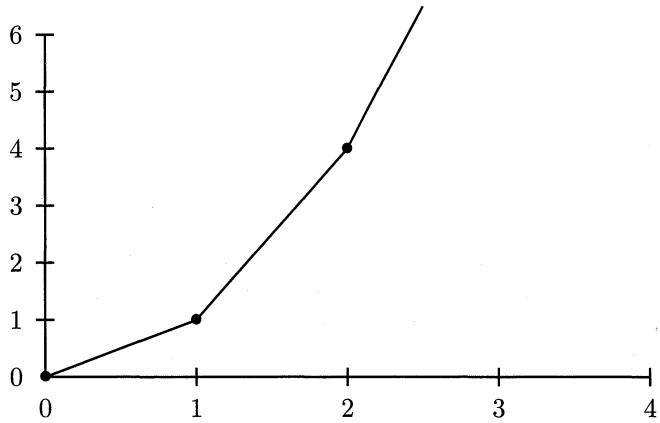
$$f(x) = 1 + \sum_{i=1}^{\infty} p^{i^2} x^i,$$

the Newton polygon given in Figure 4 is of this type.

Second, at some point, the line we are rotating hits infinitely many points, forcing us to stop. In such a case, the Newton polygon has only finitely many line segments. For example, for $f(x) = \sum_{i=1}^{\infty} x^i$, the polygon consists of the x-axis.

A third possibility is that the line we are rotating has not hit any of the points $(i, \mathrm{ord}_p a_i)$ which are farther out, but if rotated any further, the line would "miss" some points. This is seen in the example, $f(x) = 1 + \sum_{i=1}^{\infty} px^i$.

Fig. 4: Newton Polygon of $f(x) = 1 + \sum_{i=1}^{\infty} p^{i^2} x^i$.



In the case of polynomials, the Newton polygon is useful since we can see at a glance where its roots are located. It turns out that in the case of power series also, similar information is given by the Newton polygon. In many cases, such information is sharper than that given by Strassman's theorem that we met in Chapter 3.

Theorem 9.2 *Let b equal the supremum of all the slopes of the Newton polygon of*

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i \in \mathbb{C}_p[[x]].$$

Then, the radius of convergence of $f(x)$ is p^b. If $b = +\infty$, then $f(x)$ converges for all $x \in \mathbb{C}_p$.

Proof. Let $|x|_p = p^c$, with $c < b$. Then, $\mathrm{ord}_p x = -c$. Now, $\mathrm{ord}_p(a_i x^i) = \mathrm{ord}_p a_i - ci$. Since b is the supremum of all the slopes and $c < b$, it is clear that, sufficiently far out, $(i, \mathrm{ord}_p a_i)$ lies arbitrarily far above (i, ci). That is, $\mathrm{ord}_p(a_i x^i) \to \infty$ as $x \to \infty$ so that the series converges. If $|x|_p = p^c$ with $c > b$, then the same reasoning shows $\mathrm{ord}_p(a_i x^i) = \mathrm{ord}_p a_i - ci$ is negative for infinitely many values of i so that the series for $f(x)$ does not converge. Therefore, the radius of convergence is exactly p^b. ∎

Let us make a few remarks about convergence on the boundary. It is not hard to see that such convergence can only take place when the Newton polygon is of the third type described above. The reason for this is that if $|x|_p = p^b$, then we need, $\mathrm{ord}_p a_i - bi \to \infty$ as $i \to \infty$ for convergence to take place. In case the Newton polygon is of type 1 or 2, $\mathrm{ord}_p a_i$ gets very close to bi. Even if the polygon has type 3, convergence can only take place if $\mathrm{ord}_p a_i - bi \to \infty$. For

example, this is the case if

$$f(x) = 1 + \sum_{i=1}^{\infty} p^i x^{p^i}$$

whose Newton polygon is the horizontal line from $(0,0)$ consisting of the positive x-axis. (See Exercise 4.)

Another remark worth making concerns how the Newton polygon changes under a variable change. Let $c \in \mathbb{C}_p$ have $\mathrm{ord}_p c = \lambda$. Let $f(x)$ be a given power series and set $g(x) = f(x/c)$. The Newton polygon of g is obtained from that of f by subtracting the line $y = \lambda x$ which passes through $(0,0)$ from the polygon of f. To see this, write

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i$$

$$g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i$$

and observe that $\mathrm{ord}_p b_i = \mathrm{ord}_p a_i - \lambda i$ from which the result is clear.

Lemma 9.3 *Suppose that λ_1 is the first slope of the Newton polygon of*

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i.$$

Let $c \in \mathbb{C}_p$ have $\mathrm{ord}_p c = \lambda \leq \lambda_1$. Suppose that $f(x)$ converges in $|x|_p \leq p^\lambda$. Let $g(x) = (1 - cx)f(x)$. Then, the Newton polygon of $g(x)$ is obtained by joining $(0,0)$ to $(1,\lambda)$ and then translating the Newton polygon of $f(x)$ by 1 to the right and λ upward. If $f(x)$ has last slope λ_f and converges on $|x|_p \leq p^{\lambda_f}$ then $g(x)$ also converges in the same disc.

Remark. In other words, the Newton polygon of $g(x)$ is obtained by 'joining' the Newton polygon of $1 - cx$ to the Newton polygon of $f(x)$. Observe that the convergence is assured if $\lambda < \lambda_1$ or if the Newton polygon of f has more than one segment.

Proof. We first reduce the proof to the case $c = 1$, $\lambda = 0$. Suppose the lemma holds in this case. Then $f_1(x) = f(x/c)$ and $g_1(x) = (1 - x)f_1(x)$ satisfy the conditions of the lemma with c, λ, λ_1 replaced by $1, 0, \lambda_1 - \lambda$ respectively. Since the lemma holds in this case, we obtain the Newton polygon of $g_1(x)$ and the convergence in the disc $|x|_p \leq p^{\lambda_f - \lambda}$ when f converges in the disc $|x|_p \leq p^{\lambda_f}$. As $g(x) = g_1(cx)$, by the remarks made earlier about how the Newton polygon

changes under variable change, we get the Newton polygon of g. Therefore it suffices to prove the lemma for $c = 1$ and $\lambda = 0$.

Let $g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i$. Since $g(x) = (1-x)f(x)$, $b_{i+1} = a_{i+1} - a_i$, for $i \geq 0$. Now,

$$\mathrm{ord}_p(b_{i+1}) \geq \min(\mathrm{ord}_p a_{i+1}, \mathrm{ord}_p a_i)$$

with equality if and only if $\mathrm{ord}_p a_{i+1} \neq \mathrm{ord}_p a_i$. Since $(i, \mathrm{ord}_p a_i)$ and $(i, \mathrm{ord}_p a_{i+1})$ lie on or above the Newton polygon of $f(x)$, so does $(i, \mathrm{ord}_p b_{i+1})$. If $(i, \mathrm{ord}_p a_i)$ is a vertex, then $\mathrm{ord}_p a_{i+1} > \mathrm{ord}_p a_i$ so that $\mathrm{ord}_p b_{i+1} = \mathrm{ord}_p a_i$. This means that the Newton polygon of $g(x)$ must have the shape described in the lemma as far as the last vertex of the Newton polygon of $f(x)$. It now remains to show that in the case when the Newton polygon has a final infinite slope λ_f, so does $g(x)$. Moreover, we need to show that if $f(x)$ converges on $|x|_p = p^{\lambda_f}$, then so does $g(x)$. Since $\mathrm{ord}_p b_{i+1} \geq \min(\mathrm{ord}_p a_{i+1}, \mathrm{ord}_p a_i)$, it immediately follows that $g(x)$ converges when $f(x)$ does. We must rule out the possiblity that the Newton polygon has slope $\lambda_g > \lambda_f$. Indeed, if it did have such a slope, then for some large i, the point $(i+1, \mathrm{ord}_p a_i)$ would lie below the Newton polygon of $g(x)$. Then, for all $j \geq i+1$, $\mathrm{ord}_p b_j > \mathrm{ord}_p a_i$ which implies $\mathrm{ord}_p a_{i+1} = \mathrm{ord}_p a_i$ for all $j > i$. This contradicts the assumed convergence of $f(x)$ in $|x|_p \leq 1$. ∎

Lemma 9.4 *Let $f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i$ have Newton polygon with first slope λ_1. Suppose that $f(x)$ converges in $|x|_p \leq p^{\lambda_1}$ and that the line through $(0,0)$ with slope λ_1 passes through a point $(i, \mathrm{ord}_p a_i)$. Then, there exists an x_0 for which $\mathrm{ord}_p x_0 = -\lambda_1$ and $f(x_0) = 0$.*

Remark. Notice that both the conditions imposed on f are automatic if the Newton polygon has more than one slope.

Proof. For simplicity, we first consider $\lambda_1 = 0$ and reduce the general case to this one. Thus, $\mathrm{ord}_p a_i \geq 0$ with $\mathrm{ord}_p a_i \to \infty$ as $i \to \infty$. Let N be the greatest i for which $\mathrm{ord}_p a_i = 0$. This N is the length of the first segment (of slope 0) unless the Newton polygon of f has only one horizontal line. Set

$$f_n(x) = 1 + \sum_{i=1}^{n} a_i x^i.$$

By Theorem 9.1, $f_n(x)$ has precisely N roots $x_{n,1}, \ldots, x_{n,N}$ with $\mathrm{ord}_p x_{n,i} = 0$ for $n \geq N$. Define a sequence $\{x_n\}_{n=N}^{\infty}$ inductively by $x_N = x_{N,1}$ and for $n \geq N$, let x_{n+1} be any one of $x_{n+1,1}, \ldots, x_{n+1,N}$ with $|x_{n+1,i} - x_n|_p$ minimal. Thus, $|x_{n+1,i} - x_n|_p \geq |x_{n+1} - x_n|_p$ for $1 \leq i \leq n+1$. We claim that the sequence $\{x_n\}$ is Cauchy and its limit has the desired properties. Indeed, let S_n denote the set of roots of $f_n(x)$. Then, for $n \geq N$,

$$\begin{aligned}|f_{n+1}(x_n) - f_n(x_n)|_p &= |f_{n+1}(x_n)|_p \quad \text{since } f_n(x_n) = 0, \\ &= \prod_{\alpha \in S_{n+1}} \left|1 - \frac{x_n}{\alpha}\right|_p = \prod_{i=1}^{N} \left|1 - \frac{x_n}{x_{n+1,i}}\right|_p\end{aligned}$$

because for $\alpha \in S_{n+1}$ with $\mathrm{ord}_p \alpha < 0$, we have

$$\left|1 - \frac{x_n}{\alpha}\right|_p = 1.$$

Thus,

$$\begin{aligned}|f_{n+1}(x_n) - f_n(x_n)|_p &= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \quad \text{since } |x_{n+1,i}|_p = 1, \\ &\geq |x_{n+1} - x_n|_p^N \quad \text{by choice of } x_{n+1}\end{aligned}$$

so that $|x_{n+1} - x_n|_p^N \leq |a_{n+1} x_n^{n+1}|_p = |a_{n+1}|_p$. Since $\mathrm{ord}_p a_i \to \infty$, we deduce that the sequence $\{x_n\}$ is Cauchy. Put $x_0 = \lim_{n\to\infty} x_n$. Then, $f(x_0) = \lim_{n\to\infty} f(x_n)$. In addition

$$\begin{aligned}|f_n(x)|_p &= |f_n(x) - f_n(x_n)|_p \\ &= |x - x_n|_p \left|\sum_{i=1}^{n} a_i \left(\frac{x^i - x_n^i}{x - x_n}\right)\right|_p \\ &\leq |x - x_n|_p\end{aligned}$$

since $|a_i|_p \leq 1$ and $|(x^i - x_n^i)/(x - x_n)|_p \leq 1$. Therefore

$$|f_n(x_0)|_p \leq |x_0 - x_n|_p$$

and letting $n \to \infty$, we see that $f(x_0) = 0$. This completes the proof in the case $\lambda_1 = 0$. For the general case, let $z \in \mathbb{C}_p$ be any number such that $\mathrm{ord}_p z = \lambda_1$. Such a z exists since we may take the i-th root of a_i for which $(i, \mathrm{ord}_p a_i)$ lies on the line through $(0,0)$ with slope λ_1. Set $g(x) = f(x/z)$. Then $g(x)$ satisfies the conditions of the lemma with $\lambda_1 = 0$. By what has already been proved, there is an x_0' with $\mathrm{ord}_p x_0' = 0$ and $g(x_0') = 0$. If we let $x_0 = x_0'/z$ then, $\mathrm{ord}_p x_0 = -\lambda_1$ and $f(x_0) = 0$. This completes the proof of the lemma. ∎

Lemma 9.5 *Let*

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i \in \mathbb{C}_p[[x]]$$

converge and have value 0 at $x = \alpha$. Let

$$g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i$$

be obtained from $f(x)$ by dividing it by $1 - x/\alpha$. Then, $g(x)$ converges in $|x|_p \leq |\alpha|_p$.

Proof. Let

$$f_n(x) = 1 + \sum_{i=1}^{n} a_i x^i.$$

Then,

$$b_i = \frac{1}{\alpha^i} + \frac{a_1}{\alpha^{i-1}} + \cdots + \frac{a_{i-1}}{\alpha} + a_i,$$

so that $b_i\alpha^i = f_i(\alpha)$. Hence, $|b_i\alpha^i|_p = |f_i(\alpha)|_p \to 0$ as $i \to \infty$ since $f(\alpha) = 0$. Therefore $g(x)$ converges in the region indicated. ∎

We are now ready to prove the p-adic version of a classical theorem in algebraic geometry known as the Weierstrass preparation theorem. The classical version gives a factorization of a formal power series as a polynomial and an invertible formal power series. This factorization is then used to show that the ring of formal power series over any field is a unique factorization domain. A variant of the theorem (see Chapter 10) can then be used to show that the ring of formal power series over $\mathbb{Z}_p$, namely, $\mathbb{Z}_p[[x]]$, is a unique factorization domain. More generally, the same applies to $\mathcal{O}[[x]]$ where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$. One can then develop a structure theory of finitely generated modules over such rings and use it to study the growth of class numbers in cyclotomic fields and analyse the zeros of p-adic L-functions. One consequence of the theory (as we shall see in Chapter 10) is that a p-adic L-function has only finitely many zeros.

Theorem 9.6 *Let*

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i$$

converge in $|x|_p \leq p^\lambda$. Let N be the total horizontal length of all the segments of the Newton polygon of f having slope $\leq \lambda$, if this length is finite. Otherwise, if $f(x)$ has last slope λ, let N be the largest i such that $(i, \mathrm{ord}_p a_i)$ lies on the last segment. (Such an i must exist because the series for f converges on $|x|_p = p^\lambda$.) Then, there is a polynomial $h(x)$ of degree N and a power series

$$g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i$$

which converges and is non-zero in $|x|_p \leq p^\lambda$ *such that*

$$h(x) = f(x)g(x).$$

The polynomial $h(x)$ *is uniquely determined by these properties and its Newton polygon coincides with* f *upto* $(N, \mathrm{ord}_p a_N)$.

Proof. We induct on N. For $N = 0$, we must show that the power series for $g(x) = 1/f(x)$ converges and is non-zero in $|x|_p \leq p^\lambda$. By changing variables (as before in the proof of Lemma 9.3), we can reduce to the case $\lambda = 0$. Write

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i.$$

Then $N = 0$ implies $\mathrm{ord}_p a_i > 0$. Since $f(x)$ converges in $|x|_p \leq 1$, we have $\mathrm{ord}_p a_i \to \infty$ as $i \to \infty$. Write

$$g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i.$$

The relation $f(x)g(x) = 1$ implies for $i \geq 1$,

$$b_i = -\left(b_{i-1}a_1 + b_{i-2}a_2 + \cdots b_1 a_{i-1} + a_i\right).$$

From this, we deduce, by an easy induction on i, that $\mathrm{ord}_p b_i > 0$. To complete the proof, we must show $\mathrm{ord}_p b_i \to \infty$ as $i \to \infty$. Since $\mathrm{ord}_p a_i \to \infty$, we can, for any given M, choose m so that $i > m$ implies $\mathrm{ord}_p a_i > M$. If $i > m$, we may write

$$b_i = -\left(b_{i-1}a_1 + \cdots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \cdots + a_i\right),$$

from which we see that the terms $b_{i-j}a_j$, $j > m$ have $\mathrm{ord}_p(b_{i-j}a_j) \geq \mathrm{ord}_p a_j > M$. If we let

$$v = \min(\mathrm{ord}_p a_1, \mathrm{ord}_p a_2, ..., \mathrm{ord}_p a_m) > 0,$$

we see that the terms with $j \leq m$ have $\mathrm{ord}_p(b_{i-j}a_j) \geq \mathrm{ord}_p(b_{i-j}) + v$. This suggests another induction argument. Namely, we will prove by induction on n that $i > nm$ implies $\mathrm{ord}_p b_i > \min(M, nv)$, from which will follow the desired conclusion that $\mathrm{ord}_p b_i \to \infty$. To prove the claim, we induct on n. For $n = 0$, the result is clear. For $i > nm$ and $j \leq m$, we see that $i - j > (n-1)m$ and so by induction,

$$\mathrm{ord}_p(b_{i-j}) > \min(M, (n-1)v).$$

Thus,

$$\begin{aligned} \mathrm{ord}_p(b_{i-j}a_j) &\geq \mathrm{ord}_p(b_{i-j}) + v \\ &> \min(M, (n-1)v) + v \\ &> \min(M, nv). \end{aligned}$$

This completes the proof for $N = 0$.

Now suppose $N \geq 1$ and that the theorem holds for $N-1$. Let $\lambda_1 \leq \lambda$ be the first slope of the Newton polygon of $f(x)$. Using Lemma 9.4, we can find an α such that $f(\alpha) = 0$ and $\mathrm{ord}_p \alpha = -\lambda_1$. Let

$$\begin{aligned} f_1(x) &= f(x)\left(1 + x/\alpha + (x/\alpha)^2 + \cdots\right) \\ &= 1 + \textstyle\sum_{i=1}^{\infty} a_i' x^i. \end{aligned}$$

By Lemma 9.5, $f_1(x)$ converges in $|x|_p \leq p^{\lambda_1}$. Let $c = 1/\alpha$ so that $f(x) = (1-cx)f_1(x)$. If the Newton polygon of $f_1(x)$ has first slope $\lambda_1' < \lambda_1$, then it would follow by Lemma 9.4 that $f_1(x)$ has a root with p-adic ordinal $-\lambda_1'$ and then, so would $f(x)$, which is not the case. Hence, $\lambda_1' \geq \lambda_1$. By Lemma 9.3, the Newton polygon of $f_1(x)$ is the same as the one for $f(x)$ minus the segment from $(0,0)$ to $(1, \lambda_1)$. Moreover, Lemma 9.3 tells us that if $f(x)$ converges in $|x|_p \leq p^{\lambda}$ then so does $f_1(x)$. Thus, $f_1(x)$ satisfies the conditions of the theorem with N replaced by $N-1$. By induction, there is a polynomial

$$h_1(x) \in 1 + x\mathbb{C}_p[x]$$

of degree $N-1$ and a series $g(x) \in 1 + x\mathbb{C}_p[[x]]$ which converges in $|x|_p \leq p^{\lambda}$ such that

$$h_1(x) = f_1(x)g(x).$$

Multiplying both sides of this equation by $(1-cx)$ and setting $h(x) = (1-cx)h_1(x)$ gives the final result. Finally, since f has precisely N zeros in $|x|_p \leq p^{\lambda}$, it follows that $h(x)$ is unique, since its zeros must be the same as the N zeros of $f(x)$. ∎

Corollary 9.7 *If a segment of the Newton polygon of*

$$f(x) \in 1 + x\mathbb{C}_p[[x]]$$

has finite length N and slope λ, then there are precisely N values of α for which $f(\alpha) = 0$ and $\mathrm{ord}_p \alpha = -\lambda$.

Observe that in Theorem 9.6, we can also write

$$f(x) = h(x)G(x)$$

where $G(x) \in 1 + x\mathbb{C}_p[[x]]$, and $h(x)$ is a polynomial of degree N. (Sometimes, the theorem is also stated in this form in the literature.) In addition, the proof also shows that if we write

$$G(x) = 1 + d_1 x + d_2 x^2 + \cdots$$

then $|d_n| p^{mn} < 1$, for all n so that $|G(x) - 1|_p < 1$.

An important consequence of Theorem 9.6 is the p-adic analogue of the Weierstrass and Hadamard factorization theorem for entire functions. Indeed let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

be a power series which converges for all $x \in \mathbb{C}_p$. This implies (see Exercise 10) that

$$\mathrm{ord}_p(a_n)/n \to \infty.$$

We may suppose $a_0 \neq 0$ (otherwise, we can factor out a power of x and consider the quotient which has a non-zero constant term). By dividing by a_0, we can assume that

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots .$$

We can consider this series for $|x|_p \leq 1$ and apply Theorem 9.6 to deduce

$$f(x) = h_1(x) G_1(x)$$

where $h_1(x)$ is a polynomial and $G_1(x)$ does not vanish in $|x|_p \leq 1$. Since $\mathbb{C}_p$ is algebraically closed, we can factor $h_1(x)$ into linear factors

$$h_1(x) = \prod_{i=1}^{N} (1 - \lambda_i x),$$

with $|G_1(x) - 1|_p < 1$. We can now consider larger discs of the form $|x|_p \leq p^m$. This is easily done by changing variables. Set $f_1(x) = f(x/p)$. Applying Theorem 9.6 to $f_1(x)$ gives

$$f_1(x) = \tilde{h}_2(x) \tilde{G}_2(x)$$

with $|\tilde{G}_2(x) - 1|_p < 1$. Thus,

$$f(x) = \tilde{h}_2(px) \tilde{G}_2(px) = h_2(x) G_2(x)$$

where $|G_2(x) - 1|_p < 1/p$. In this way, we obtain successively

$$f(x) = h_m(x) G_m(x)$$

with $h_m(x)$ a polynomial consisting of zeros of $f(x)$ lying in the disc $|x|_p \leq p^m$ and $|G_m(x) - 1|_p \leq p^{-m}$. That is

$$\lim_{m \to \infty} G_m(x) = 1.$$

This proves:

Theorem 9.8 *Let $f(x)$ be a power series defining an entire function in $\mathbb{C}_p$. Then, $f(x)$ can be written uniquely as*

$$f(x) = a x^r \prod_{i=1}^{\infty} (1 - \lambda_i x)$$

where $a \in \mathbb{C}_p$, r is a non-negative integer and λ_i ranges through reciprocals of zeros of $f(x)$, which form a sequence tending to zero.

For example, the theorem implies

$$f(x) = \prod_{n=1}^{\infty}(1 - p^n x)$$

defines an entire function in $\mathbb{C}_p$.

Exercises

1. Give an example of a polynomial in $\mathbb{Q}_p[x]$ which is reducible but whose Newton polygon consists of a single line segment.

2. Determine the Newton polygon of $f(x) = 1 + x^2 + px^4 + p^3x^6$. Deduce that $f(x)$ is reducible in $\mathbb{Q}_p[x]$.

3. Find the Newton polygon of

$$\prod_{i=1}^{p^2}(1 - ix).$$

4. Show that the Newton polygon of the power series

$$f(x) = 1 + \sum_{i=1}^{\infty} p^i x^{p^i}$$

consists of the horizontal line from $(0, 0)$ to $+\infty$. Determine its radius of convergence and show that it converges on the 'circumference' of convergence.

5. Find the Newton polygon of

$$\mathrm{Exp}\,(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

6. Find the Newton polygon of

$$\frac{1-p^2x}{1-px}.$$

7. If $f(x)$ is a power series which converges in $|x|_p \leq r$ and has infinitely many zeros, show that f is identically zero.

8. Let K be a finite extension of $\mathbb{Q}_p$. Suppose that

$$f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i, \qquad a_i \in K$$

converges in $|x|_p \leq p^\lambda$. Show that in Theorem 9.6, we may take $h(x) \in K[x]$ and $g(x) \in K[[x]]$.

9. Deduce Strassman's theorem (Theorem 3.4) from Theorem 9.6. In fact, deduce the following sharper version: if

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots$$

converges in $|x|_p \leq 1$, let N be defined by

$$|a_N|_p = \max_n |a_n|_p, \quad |a_n|_p < |a_N|_p \text{ for } n > N.$$

Then $f(x)$ has exactly N zeros in $\mathbb{C}_p$ lying in the closed disc $|x|_p \leq 1$.

10. If

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

converges for all $x \in \mathbb{C}_p$, show that

$$\frac{\mathrm{ord}_p a_n}{n} \to \infty$$

as $n \to \infty$, and conversely.

Appendix: Newton Polygons and Galois Groups

We begin by reviewing some basic facts from algebraic number theory that will be relevant in the computation of Galois groups of polynomials, in particular over the rational number field. We will show how these facts can be used to determine the Galois groups of trinomials such as $x^n + ax + b$ and the truncated exponential polynomials, such as

$$f_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!},$$

using the theory of Newton polygons discussed in Chapter 9. It turns out that the Newton polygons contain information about inertia groups(defined below) and this knowledge can be used to determine the Galois group.

Let us recall some properties about decomposition groups, the proofs of which can be found in Janusz [J] or Cassels [C]. Let L/K be a finite Galois extension of algebraic number fields with Galois group G. It is clear that G has a natural action on the prime ideals of L. For each prime ideal $\wp$ of L, we define the **decomposition group** of $\wp$, denoted $D(\wp)$, as

$$\{\sigma \in G \ : \quad \sigma\wp = \wp\}.$$

It is known that $\mathfrak{p}$ splits completely in L if and only if $D(\wp)$ is trivial. If O_K is the ring of integers of K, it is evident that $\wp \cap O_K = \mathfrak{p}$ is a prime ideal of K. The finite field $O_L/\wp$ can be viewed as a finite field extension of $O_K/\mathfrak{p}$ in a natural way and we have a natural map

$$D(\wp) \to \mathrm{Gal}((O_L/\wp)/(O_K/\mathfrak{p}))$$

given by the action

$$\overline{\sigma}(x + \wp) := \sigma(x) + \wp, \quad \sigma \in D(\wp),$$

which is easily seen to be well-defined. One can show that this map is surjective and the kernel of this map, denoted $I(\wp)$, is called the **inertia group** of $\wp$. Thus we have an isomorphism

$$\mathrm{Gal}((O_L/\wp)/(O_K/\mathfrak{p})) \simeq D(\wp)/I(\wp).$$

If we let $L_\wp$ be the completion of L at $\wp$, then it is a well-known fact that

$$\mathrm{Gal}(L_\wp/K_\mathfrak{p}) \simeq D(\wp).$$

We say that $\mathfrak{p}$ is **ramified** in L if $I(\wp)$ is non-trivial for some $\wp|\mathfrak{p}$. If L/K is abelian, we sometimes write $D(\mathfrak{p})$ and $I(\mathfrak{p})$ to denote $D(\wp)$ and $I(\wp)$ for any $\wp|\mathfrak{p}$ since they are all equal.

Let us suppose that O_L has an O_K-basis. Recall that we may define the **relative discriminant** $D_{L/K}$ as

$$\det(\mathrm{Tr}_{L/K}(w_i w_j))$$

where $w_1, ..., w_n$ is an O_K basis of O_L, and $\mathrm{Tr}_{L/K}$ is the trace map. A classical theorem of Dedekind states that $\mathfrak{p}$ is ramified in L if and only if $\mathfrak{p}|D_{L/K}$. If $L^{I(\wp)}$ denotes the subfield of L fixed by $I(\wp)$, then it is known that $\wp$ is unramified in this field.

If we specialize our discussion to the case that K is the rational number field, we can deduce that the Galois group G is generated by the inertia groups $I(\wp)$ as $\wp$ ranges over the prime ideals of L. Indeed, if H is the subgroup generated by all the inertia groups, and L^H is the subfield left fixed by H, then L^H is unramified over the rationals. But by a famous theorem of Minkowski, there are no such proper extensions. Thus, $L^H = \mathbb{Q}$ so that $H = G$. Therefore, the strategy is to use p-adic considerations to deduce facts about inertia groups from which we can infer the structure of the Galois group.

We recall a few functorial properties of decomposition groups. If

$$L \supset M \supset K$$

is a tower of fields such that $H = \mathrm{Gal}(L/M)$, and $P = \wp \cap O_M$, then $D(P) = D(\wp) \cap H$. If $H \lhd G$, then M/K is Galois with group $\simeq G/H$ so that $D(P)$ can be viewed as the set of cosets σH where $\sigma \in D(\wp)$.

An example may elucidate the above discussion. We use it as an opportunity to provide a proof of the celebrated law of quadratic reciprocity using ramification theory.

Theorem A.1 (The law of quadratic reciprocity) *Let p and q be odd prime numbers and set $q^* = (-1)^{(q-1)/2}q$. Then p is a square mod q if and only if q^* is a square mod p.*

Proof. Consider $L = \mathbb{Q}(\zeta_q)$, where q is an odd prime and ζ_q denotes a primitive q-th root of unity. Its discriminant is easily computed as $(-1)^{(q-1)/2}q^{q-2}$. Thus, the only prime that ramifies in L is q. The Galois group of $L/\mathbb{Q}$ is $(\mathbb{Z}/q\mathbb{Z})^*$. Moreover, $D(p)$ is cyclic generated by the automorphism σ_p whose action on ζ_q is given by $\sigma_p(\zeta_q) = \zeta_q^p$. This group has a subgroup H of index 2 consisting of

squares. The subfield M fixed by this subgroup must be a quadratic extension ramified only at q. Thus, it must be $\mathbb{Q}(\sqrt{q^*})$ where $q^* = (-1)^{(q-1)/2}q$. By the functorial properties noted above, the decomposition group of P is the group of cosets σH. Thus, $D(P)$ is trivial if and only if σ_p is a square mod p. That is, $D(p)$ is trivial if and only if p is a square mod q. On the other hand, the Galois group of $\mathbb{Q}_p(\sqrt{q^*})$ over $\mathbb{Q}_p$ is either trivial or of order 2 according as q^* is a square mod p or not(by an application of Hensel's lemma). Thus,

$$\left(\frac{p}{q}\right) = 1 \text{ if and only if } \left(\frac{q^*}{p}\right) = 1.$$

This is precisely the law of quadratic reciprocity. ∎

We will now use these ideas to compute the Galois group of trinomials of the form $x^n + ax + b$. Our motivation for this study is prompted by a conjecture of Williams and Uchiyama (see Osada [O]). For each prime p, they defined $a_n(p)$ as the smallest positive value of a such that $x^n + x + a$ is irreducible mod p and conjectured that

$$\liminf_{p\to\infty} a_n(p) = \delta_n$$

where $\delta_n = 1$ for $n = 2$ or $n \not\equiv 2 (\bmod 3)$, $\delta_n = 2$ for even $n > 2$ and $n \equiv 2 (\bmod 3)$, $\delta_n = 3$ for odd n satisfying $n \equiv 2 (\bmod 3)$. If we can show that the Galois group of $x^n + x + \delta_n$ is S_n, the symmetric group on n letters, then by an application of the Chebotarev density theorem (see [MM]), we can deduce that there are infinitely many primes p for which $x^n + x + \delta_n$ is irreducible mod p, from which the conjecture easily follows.

We will make use of several facts from group theory that will enable us to establish the Galois groups of certain trinomials. First, recall that if $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, then the Galois group, viewed as a permutation group on the roots, is a transitive permutation group. We will show below that a transitive permutation group on n elements which is generated by transpositions is the full symmetric group S_n.

Lemma A.2 *If G is a transitive permutation group on the finite set Ω and generated by transpositions, then G is* $\mathrm{Sym}(\Omega)$.

Proof. Let Ω' be a maximal subset of Ω such that $\mathrm{Sym}(\Omega') \subseteq G$. As G is generated by transpositions, it suffices to show that every transposition of G lies in $\mathrm{Sym}(\Omega')$. Let $(x\ y)$ be a transposition of G not in $\mathrm{Sym}(\Omega')$. Either both x, y do not lie in Ω' or one of them does and the other doesn't. Suppose the latter, with $x \in \Omega'$ and $y \notin \Omega'$. In that case, by the transitivity of $\mathrm{Sym}(\Omega')$, we find that conjugating $(x\ y)$ appropriately, $(z\ y)$ lies in G for any $z \in \Omega'$. Thus, we can enlarge Ω' by adding y and this contradicts the maximality of Ω'. Thus, for any transposition, $(x\ y)$, either both x, y lie in Ω' or both of them don't.

Thus G stabilizes Ω'. But, G is transitive so that $\Omega' = \Omega$. This completes the proof. ∎

Selmer [Se] has proved that if $n \not\equiv 2 (\bmod 3)$, then $x^n + x + 1$ is irreducible. The proof is not simple. One can however show by a simple argument that $x^n + x + 3$ is always irreducible. Indeed, if it factored non-trivially,

$$x^n + x + 3 = (x^r + \cdots + c_1 x + c_0)(x^s + \cdots + b_1 x + b_0)$$

we get $1 = c_1 b_0 + c_0 b_1$ and $3 = c_0 b_0$. Thus, without loss of generality, we can suppose $c_0 = \pm 1$ and $b_0 = \pm 3$. If $\alpha_1, \cdots, \alpha_n$ are the roots of $x^n + x + 3$, we cannot have $|\alpha_i| \leq 1$ for any i for otherwise,

$$3 = |\alpha_i^n + \alpha_i| \leq 1 + 1 = 2,$$

a contradiction. Thus, $|\alpha_i| > 1$ which means that $|c_0| > 1$ as c_0 is a product of some subset of the roots. This is a contradiction.

It is not difficult to compute the discriminant of trinomials such as $x^n + ax + b$. An easy computation (see Exercise 3) shows that it is

$$(-1)^{\binom{n}{2}} \left(b^{n-1} n^n + a^n (1-n)^{n-1}\right).$$

We can now prove:

Theorem A.3 *Suppose $x^n + x + 1$ is irreducible over $\mathbb{Q}$. Then it has Galois group S_n, the symmetric group on n letters.*

Proof. Now if $f(x) = x^n + x + b$, the congruence $f(x) \equiv 0 (\bmod p)$ can have at most a double root because if r is such a root, we would need $r^n + r + b \equiv 0 (\bmod p)$ and $nr^{n-1} + 1 \equiv 0 (\bmod p)$. It is easily seen that we can find a unique solution for r provided $(p, n(n-1)) = 1$. Now a double root can exist only for primes dividing the discriminant (see Exercise 4). In the case $b = 1$, this means that for primes dividing the discriminant, we must necessarily have $(p, n(n-1)) = 1$ so there is at most a double root mod p. Thus, $f(x) = (x-c)^2 h(x) (\bmod p)$ where $h(c) \not\equiv 0 (\bmod p)$ and $h(x)$ is separable. By Hensel's lemma, we can lift this factorization to $\mathbb{Q}_p$:

$$f(x) = G(x) H(x)$$

where $G(x) \equiv (x-c)^2 (\bmod p)$ and $H(x) \equiv h(x) (\bmod p)$. Let K be the splitting field of f over $\mathbb{Q}$ and $\mathfrak{p}$ a prime above p. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. We know that $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) = D(\mathfrak{p})$ is the decomposition group at p. Now $K_{\mathfrak{p}}$ contains the splitting field of $f(x)$ over $\mathbb{Q}_p$. Let L be the splitting field of $G(x)$, L' the splitting field of $H(x)$ over $\mathbb{Q}_p$, so that $K_{\mathfrak{p}}$ contains the compositum of L and L'. Since $L'/\mathbb{Q}_p$ is unramified, the ramification can come

only from the extension $K_{\mathfrak{p}}/L'$ which is at most quadratic. This extension is generated by at most a transposition. Thus, the inertia groups are all generated by transpositions. By Lemma A.2, this means that the Galois group is the full symmetric group. ∎

The above reasoning can be extended to show that if $f(x) \in \mathbb{Z}[x]$, such that the discriminant $D(f)$ of f is squarefree, and $f(x)$ is irreducible, then $\mathrm{Gal}(f)$ is the full symmetric group on n letters where $n = \deg f$.

We will now apply some of these ideas to prove a theorem of Schur, namely:

Theorem A.4 *The Galois group of the polynomial*

$$f_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

over $\mathbb{Q}$ is the alternating group A_n if $4|n$ and the full symmetric group S_n otherwise.

Proof. We will follow Coleman [Co]. Our strategy will be to show that $\mathrm{Gal}(f_n) \supseteq A_n$ in all cases. The result then follows from the fact that $\mathrm{Gal}(f_n) \subseteq A_n$ if and only if the discriminant $D(f_n)$ is a perfect square. We begin with the discriminant calculation.

Recall that if f is a monic polynomial $f(x) = (x - a_1) \cdots (x - a_n)$, then

$$D(f) = (-1)^{\binom{n}{2}} \prod_{i \neq j} (a_i - a_j) = (-1)^{\binom{n}{2}} \prod_i f'(a_i).$$

Set $F_n(x) = n! f_n(x)$, so that F_n is monic. Thus,

$$D(F_n) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} n F_{n-1}(a_i)$$

because $F_n'(x) = nF_{n-1}(x)$. Moreover, $f_n(x) = f_{n-1}(x) + x^n/n!$ so that $0 = f_n(a_i) = f_{n-1}(a_i) + a_i^n/n!$. Thus,

$$D(F_n) = (-1)^{\binom{n}{2}} n!^n.$$

We deduce that $D(f_n)$ is not a perfect square if $n \equiv 2 (\mathrm{mod}\, 4)$ since in that case, $D(f_n) < 0$. If n is divisible by 4, $D(f_n)$ is a perfect square. If n is odd, we have by Chebycheff (see [EM, p. 10, Ex. 1.4.19], a prime p satisfying the inequality $n/2 < p < n$ so that $n!^n$ is not a perfect square. Hence, $D(f_n)$ is a perfect square if and only if $4|n$.

Now we recall facts about Newton polygons proved in Chapter 9. For $a \in \overline{\mathbb{Q}}_p$, $\mathrm{ord}_p a$ is defined by the equation $|a|_p = p^{-\mathrm{ord}_p a}$. The p-adic Newton polygon of

$$f(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

is defined as the "convex hull" of the points

$$(0,0), (1, \mathrm{ord}_p a_1), \cdots, (n, \mathrm{ord}_p a_n).$$

The points of "breakage" are called the vertices of the polygon. If we let $(x_0, y_0) = (0,0)$, $(x_1, y_1), \cdots, (x_s, y_s)$ be the vertices then, the numbers

$$\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$$

are called the slopes. Recall from Chapter 9 that $f(x)$ factors over $\mathbb{Q}_p$ as

$$f(x) = f_1(x) \cdots f_s(x)$$

with degree of f_i equal to $x_i - x_{i-1}$ and all the roots α_i of f_i have $\mathrm{ord}_p \alpha_i = -(y_i - y_{i-1})/(x_i - x_{i-1})$. In particular, if the p-adic Newton polygon has "breaks", then it is reducible over $\mathbb{Q}_p$.

Let us look at the 2-adic Newton polygon of $f_7(x)$. Notice that it has breaks at the vertices $(0,0), (4,3), (6,4), (7,4)$. Observe that if we write $7 = 2^2 + 2 + 1$, the x-co-ordinates of the vertices are the "partial sums" of the 2-adic expansion of 7: 2^2, $2^2 + 2$, $2^2 + 2 + 1$. More generally, if we write $n = b_1 p^{n_1} + b_2 p^{n_2} + \cdots$, $n_1 > n_2 > \cdots$ $1 \leq b_i \leq p - 1$, then the x-co-ordinates of the vertices are (see Exercise 5)

$$\begin{aligned} x_1 &= b_1 p^{n_1} \\ x_2 &= b_1 p^{n_1} + b_2 p^{n_2} \\ &\cdot \\ &\cdot \\ x_i &= b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_i p^{n_i} \end{aligned}$$

so that the slopes are

$$m_i = -\frac{p^{n_i} - 1}{p^{n_i}(p-1)}.$$

These slopes will tell us something about the orders of the inertia groups. More precisely, if d divides the denominators of all the slopes of the p-adic Newton polygon of f, then d divides the degree of each irreducible factor of f over $\mathbb{Q}_p$.

In the case of $f_n(x)$, we deduce immediately that p^{n_s} divides the degree of each irreducible factor of f over $\mathbb{Q}_p$. Now suppose that $p^m | n$. Writing $n =$

$b_1p^{n_1} + \cdots + b_sp^{n_s}$, we see that $n_s \geq m$ so that p^m divides the degree of each irreducible factor of $f_n(x)$. If $p^k \leq n$, then $k \leq n_1$. Hence p^k divides the denominator of the first slope. Thus, p^k divides the degree of any extension of $\mathbb{Q}_p$ formed by adjoining a root of f_n with valuation $-m_1$. We can deduce from this that $f_n(x)$ is irreducible over $\mathbb{Q}$. Indeed, write

$$n = \prod_{p \leq n} p^{n_p}.$$

By the preceding discussion, p^{n_p} divides the degree of the splitting field of $f_n(x)$ over $\mathbb{Q}$. Hence n divides the degree of the splitting field of $f_n(x)$ so that $f_n(x)$ is irreducible.

Since $f_n(x)$ is irreducible over $\mathbb{Q}$, its Galois group is transitive. Now, if p is a prime satisfying $n/2 < p < n$, then $p||n$ so that the splitting field of $f_n(x)$ over $\mathbb{Q}$ is divisible by p. Thus, the Galois group G has an element of order p. This must be a p-cycle. By a theorem of Jordan, G contains A_n. Finally, by the lemma, we complete the proof. ∎

We conclude by noting that the same argument works to show that $\sum_{j=0}^{n} a_j x^j/j!$ with $a_j = \pm 1$, has Galois group G which contains the alternating group A_n.

Exercises

1. Prove that $x^n + x + 1$ is reducible when $n \equiv 2 (\bmod 3)$ for $n > 2$.
2. Prove that $x^n + x + 2$ is irreducible over $\mathbb{Q}$.
3. Show that the discriminant of $x^n + ax + b$ is given by
$$(-1)^{\binom{n}{2}}(b^{n-1}n^n + a^n(1-n)^{n-1})$$
4. If $f(x) \in \mathbb{Z}[x]$, show that if the congruence $f(x) \equiv 0 (\bmod p)$ has a double root mod p then $p|D(f)$.
5. Prove that the x-co-ordinates of the p-adic Newton polygon of
$$f_n(x) + 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$
are given by
$$x_i = b_1p^{n_1} + b_2p^{n_2} + \cdots + b_ip^{n_i}$$
where
$$n = b_1p^{n_1} + b_2p^{n_2} + \cdots, \quad n_1 > n_2 > \cdots$$
and $1 \leq b_i \leq p - 1$.

Chapter 10

An Introduction to Iwasawa Theory

As mentioned in the previous chapter, the Weierstrass preparation theorem implies that $F[[x]]$, the ring of formal power series over a field is a unique factorization domain. The proof of this fact can be modified to show that $\mathcal{O}[[x]]$ is a unique factorization domain whenever $\mathcal{O}$ is a complete local ring, such as $\mathbb{Z}_p$. It is customary in Iwasawa theory to designate by Λ, the ring $\mathbb{Z}_p[[x]]$. Then, the p-adic Weierstrass preparation theorem can be used to show that for any $f(x) \in \Lambda$, f not zero, we can write it uniquely as

$$f(x) = p^{\mu} P(x) U(x)$$

where $\mu \geq 0$, $U(x)$ is a unit in Λ and $P(x)$ is a polynomial of the form

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad p|a_i, \quad 0 \leq i \leq n-1.$$

Such polynomials are called *distinguished.* For instance, Eisenstein polynomials are distinguished.

Manin noticed that a "semi-Euclidean" algorithm holds for the ring Λ. This fact can then be used to derive a variant of the p-adic preparation theorem. This can, in turn, be used to study the structure of Λ and finitely generated modules over Λ. We follow Manin below.

Lemma 10.1 *Let $f, g \in \Lambda = \mathbb{Z}_p[[x]]$ and assume $f = a_0 + a_1 x + \cdots$, with $p|a_i$ for $0 \leq i \leq n-1$, $p \nmid a_n$. Then, we can write*

$$g(x) = q(x)f(x) + r(x),$$

with $q \in \Lambda$, and $r \in \mathbb{Z}_p[x]$ is a polynomial of degree at most $n-1$.

Proof. We first prove uniqueness which means we must consider the equation $qf + r = 0$. If $q, r \neq 0$, we may suppose that either $p \nmid r$ or $p \nmid q$. Reducing mod p gives that $p|r$ since $qf \pmod p$ is a power series whose first term begins with $q(0)a_n x^n$. Since $p \nmid f$, we deduce that $p|q$, a contradiction.

The existence is a little more involved. We define the "head" and "tail" operators H and T given by

$$H\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{n-1} b_i x^i,$$

and

$$T\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=n}^{\infty} b_i x^{i-n}.$$

Clearly H and T are $\mathbb{Z}_p$-linear. Notice that
(i) $T(x^n h(x)) = h(x) \quad \forall h(x) \in \mathbb{Z}_p[[x]]$;
(ii) $T(h(x)) = 0$ if and only if $h(x)$ is a polynomial of degree $\leq n-1$.

Also observe that since $p \nmid a_n$, $T(f)$ is a unit in Λ. In our notation, we want to find a q such that

$$T(g) = T(qf).$$

Since $f = H(f) + x^n T(f)$, we can write this as

$$T(g) = T(qH(f)) + T(qx^n T(f)) = T(qH(f)) + qT(f),$$

by property (i). Since $T(f)$ is invertible, setting $Z = qT(f)$, we can rewrite this as

$$T(g) = T\left(\frac{H(f)}{T(f)} Z\right) + Z = \left(1 + T \circ \frac{H(f)}{T(f)}\right) Z.$$

Since $H(f) \equiv 0 (\bmod p)$, we can invert the operator and get

$$Z = \left(1 + T \circ \frac{H(f)}{T(f)}\right)^{-1} T(g),$$

from which q can be obtained because $T(f)$ is invertible. This completes the proof. ∎

Theorem 10.2 (p-adic Weierstrass preparation theorem) *Any power series* $f \in \Lambda$,

$$f(x) = a_0 + a_1 x + \cdots$$

with $p | a_i$ *for* $0 \leq i \leq n-1$, $p \nmid a_n$ *can be written uniquely as*

$$f(x) = (x^n + b_{n-1} x^{n-1} + \cdots + b_0) u$$

where $p | b_i$ *and* u *is a unit in* Λ.

Proof. By Lemma 10.1, we can write uniquely

$$x^n = qf + r,$$

where r is a polynomial of degree less than n. If we write

$$q = c_0 + c_1 x + \cdots$$

we obtain by comparing coefficients of x^n on both sides of the equation,

$$c_0 a_n \equiv 1 (\bmod p).$$

Since $p \nmid a_n$, we find $p \nmid c_0$ so that q is invertible in Λ. Therefore,

$$f = q^{-1}(x^n - r).$$

Since $f \equiv a_n x^n + \cdots (\bmod p)$, we must have $r \equiv 0 (\bmod p)$. This proves existence. Uniqueness is immediate. ∎

Theorem 10.3 *Λ is a unique factorization domain whose irreducible elements are p and the irreducible distinguished polynomials. The prime ideals of Λ are 0, (p), (p, x) and $(P(x))$, where $P(x)$ is a distinguished irreducible polynomial. Λ is a local ring. The ideal (p, x) is the unique maximal ideal.*

Remark. Thus, Λ is almost a principal ideal domain. It is also immediate that Λ is Noetherian.

Recall that finitely generated modules over principal ideal domains admit a beautiful structure theorem. Namely, any such module is isomorphic to a direct sum of a finite number of cyclic submodules. Iwasawa discovered a similar structure theorem for finitely generated Λ-modules. To describe this, we define two Λ-modules M and M' to be *pseudo-isomorphic* (written $M \sim M'$) if there is a homomorphism $M \to M'$ with finite kernel and cokernel. This relation is not reflexive (see Exercise 3). However, one can show that for finitely generated *torsion* Λ-modules that $M \sim M'$ if and only if $M' \sim M$.

The structure theorem for finitely generated Λ-modules is:

Theorem 10.4 (Iwasawa) *Let $\Lambda = \mathbb{Z}_p[[x]]$ and M a finitely generated Λ-module. Then,*

$$M \sim \Lambda^r \oplus (\Lambda/(p^{n_1}) \oplus \cdots \oplus \Lambda/(p^{n_s})) \oplus (\Lambda/(f_1(x)^{m_1}) \oplus \cdots \oplus \Lambda/(f_t(x)^{m_t})),$$

where the r, n_i, m_j are non-negative integers and $f_j(x)$ are distinguished and irreducible.

Remark. Thus, M is pseudo-isomorphic to a direct sum of cyclic submodules. This is similar to the case that M is a finitely generated module over a PID,

except that isomorphism has been replaced by pseudo-isomorphism. A proof modelled along classical lines can be found in several books such as [W, p. 270-276].

Iwasawa applied his theorem to study the growth of the p-part of the ideal class groups of the cyclotomic extensions $\mathbb{Q}(\zeta_{p^n})$. More generally, suppose we have a tower of number fields

$$K_0 \subset K_1 \subset \cdots \subset K_\infty = \cup_{n=0}^{\infty} K_n$$

with $\mathrm{Gal}(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}$. (For example, $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ is one such tower.) Then,

$$\mathrm{Gal}(K_\infty/K_0) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p.$$

The extension K_∞/K_0 is called a $\mathbb{Z}_p$-extension (or sometimes, a Γ-extension). Let p^{e_n} be the exact power of p dividing the class number of K_n. Iwasawa proved:

Theorem 10.5 (Iwasawa, 1958) *There exist integers $\mu \geq 0, \lambda \geq 0$ and ν such that*

$$e_n = \mu p^n + \lambda n + \nu,$$

for all sufficiently large n.

Remark. μ, λ and ν are usually called the Iwasawa invariants of the $\mathbb{Z}_p$ extension K_∞/K_0. They may depend on p but are independent of n.

Proof. (Sketch) Let $\Gamma = \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p$. This is a pro-cyclic group. Let L_n be the maximal unramified abelian p-extension of K_n. By class field theory, $X_n = \mathrm{Gal}(L_n/K_n)$ is isomorphic to A_n, the p-Sylow subgroup of the ideal class group of K_n. Let $L_\infty = \cup_{n=1}^{\infty} L_n$ and $X = X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$. Each L_n is Galois over K_0 since L_n is maximal, so that L_∞/K_0 is Galois. Let $G = \mathrm{Gal}(L_\infty/K_0)$. The idea is to make X into a Γ-module, and therefore, a Λ-module. Iwasawa [Iw] shows that this can be done, and that it is finitely generated and Λ-torsion. By the structure theorem, it is pseudo-isomorphic to a direct sum of modules of the form

$$\Lambda/(p^k) \qquad \text{and} \qquad \Lambda/(P(x)^k).$$

One can study the structure of X_n from the structure of X. For instance, if K_∞/K_0 is a $\mathbb{Z}_p$-extension in which exactly one prime is ramified and totally ramified (like in the case $K_0 = \mathbb{Q}(\zeta_p)$ and $K_\infty = \cup_{n\geq 1}\mathbb{Q}(\zeta_{p^{n+1}})$ where only p is ramified and totally ramified), one can show

$$A_n \simeq X_n \simeq X/((1+x)^{p^n} - 1)X.$$

By Exercise 2, $\Lambda/(f)$ is infinite for any $f \in \Lambda$. Since A_n is finite, we must therefore have $r = 0$. Thus, X is pseudo-isomorphic to a direct sum of modules:

$$X \sim \left(\oplus_{i=1}^{s} \Lambda/(p^{k_i})\right) \oplus \left(\oplus_{j=1}^{t} \Lambda/(g_j(x))\right)$$

where each $g_j(x)$ is distinguished (but not necessarily irreducible). Since $(1+x)^{p^n} - 1$ is distinguished, we can apply the division algorithm to deduce that (see Exercise 5) for n large,

$$\left|\Lambda/(p^{k_i}, (1+x)^{p^n} - 1)\right| = p^{k_i p^n}.$$

Thus, these quotients contribute μp^n, where $\mu = \sum_{i=1}^{s} k_i$ to e_n. To deal with the other factors, note that $(1+x)^{p^n} = 1 + p(\text{polynomial}) + x^{p^n}$ so that if $g_j(x)$ has degree d_j, then

$$x^{d_j} \equiv p(\text{polynomial})(\bmod g_j)$$

since g_j is distinguished. By induction,

$$x^k \equiv p(\text{poly.})(\bmod g_j)$$

for $k \geq d_j$. Therefore, if $p^n \geq d_j$, then

$$(1+x)^{p^n} \equiv 1 + p(\text{poly.})(\bmod g_j).$$

Thus,

$$(g_j(x), (1+x)^{p^n} - 1) = (g_j(x), p(\text{poly.})),$$

from which it is not hard to see (by an application of Lemma 10.1) that

$$\left|\Lambda/(g_j(x), (1+x)^{p^n} - 1)\right| = p^{d_j n},$$

for n sufficiently large. These terms therefore give a contribution of λn with $\lambda = \sum_j d_j$ to e_n. Putting it all together, we obtain $e_n = \mu p^n + \lambda n + \nu$ with ν bounded. This completes our sketch of the proof. ∎

Iwasawa conjectured for cyclotomic $\mathbb{Z}_p$-extensions (that is, extensions $K_\infty \subseteq \cup_n K_0(\zeta_{p^n})$) we must have $\mu = 0$. He constructed non-cyclotomic $\mathbb{Z}_p$-extensions which have $\mu > 0$. His conjecture has now been proved if $K_0/\mathbb{Q}$ is abelian by Ferrero and Washington [FW]. It is still open in the general case. As a consequence of the Ferrero-Washington theorem, we have:

Corollary 10.6 *Let h_n be the class number of $\mathbb{Q}(\zeta_{p^{n+1}})$. Let p^{e_n} be the power of p dividing h_n. Then, there are constants $\lambda \geq 0$ and ν such that $e_n = \lambda n + \nu$ for all n sufficiently large.*

Remark. In other words, thanks to the fact that $\mu = 0$, the growth of the power of p in h_n is linear in n. It is interesting to observe that by using analytic

class number formulas or the Brauer-Siegel theorem, such a sharp estimate on the growth of the p-part cannot be deduced (see Exercises 7 and 8).

If F is a number field and we consider a $\mathbb{Z}_p$-extension of F, then some results are known. For example, Iwasawa proved that if F has class number coprime to p and there is only one prime in F lying above p, then any $\mathbb{Z}_p$ extension of F has $\mu = \lambda = \nu = 0$. In particular, if p is a regular prime, the class number of $\mathbb{Q}(\zeta_{p^{n+1}})$ is coprime to p for all natural numbers n.

Iwasawa derived a "Wieferich-type" congruence involving the Bernoulli numbers whenever $\mu \neq 0$. More precisely, he showed that if $\mu > 0$, then there is an even integer $2 \leq j \leq p-3$ such that p divides the numerator of B_j and

$$\frac{B_{j+p-1}}{j+p-1} \equiv \frac{B_j}{j} (\operatorname{mod} p^2),$$

where the second condition is recognized as a stronger congruence than the one implied by the Kummer congruences. The converse, however, does not hold. It can happen that the stronger Kummer congruence holds. For example,

$$\frac{B_{16}}{16} - \frac{B_4}{4} = -\frac{7 \cdot 13^2}{2^5 \cdot 5 \cdot 17}$$

so that the "stronger" Kummer congruence holds for the pair $(p, j) = (13, 4)$. Still, the above criterion allows one to check that $\mu = 0$ for all primes $p < 8,000,000$ for the classical cyclotomic $\mathbb{Z}_p$-tower.

The motivation for making the conjecture that $\mu = 0$ comes from algebraic geometry. We will try and describe it below.

The inspiration comes from the situation in function fields. Recall that if $\mathbb{F}_q$ is a finite field, we may consider the function field $\mathbb{F}_q(x)$ which in many ways is analogous to the field of rational numbers. We may consider a finite algebraic extension $k = \mathbb{F}_q(x, y)$ of $\mathbb{F}_q(x)$ and think of it as analogous to a finite extension of the rational numbers. Such an extension is given by a curve of the form $f(x, y) = 0$ and we may consider the zeta function of k which can be written as

$$\zeta_k(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where $P(x)$ is a polynomial $\in \mathbb{Z}[x]$ of degree $2g$, with g being equal to the genus of the curve.

If we wanted to construct a $\mathbb{Z}_p$-extension in the function field case, the natural tower to consider is

$$\mathbb{F}_q \subset \mathbb{F}_{q^p} \subset \cdots \subset \mathbb{F}_{q^{p^n}} \subset \cdots$$

so that if $k_n = k\mathbb{F}_{q^{p^n}}$, then we have the tower

$$k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset k_\infty$$

is also a $\mathbb{Z}_p$-extension. It turns out that the zeta function of k_n can be written as (see [W, p.129])

$$\zeta_{k_n}(s) = \frac{P_n(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where

$$P_n(x) = \prod_{j=1}^{2g}(1-\alpha_j^{p^n}x^{p^n}) = \prod_{\zeta^{p^n}=1} P(\zeta x).$$

Several facts are known about $P(x)$ and we review them now.

(a) $P(x) = \prod_{j=1}^{2g}(1-\alpha_j x)$, $\quad |\alpha_j| = q^{1/2}$ (Riemann hypothesis for curves);
(b) $P(1) = \prod_{j=1}^{2g}(1-\alpha_j) = h(k)$, the class number of k;
(c) $h(k_n) = \prod_{j=1}^{2g}(1-\alpha_j^{p^n}) = h_0 \prod_{\zeta^{p^n}=1,\zeta\neq 1} P(\zeta)$.

It easily follows from (c) that if p^{e_n} is the exact power of p dividing $h(k_n)$, then $e_n = \lambda n + \nu$, (see Exercises 9 and 10) with $\lambda \leq 2g$. In particular, $\mu = 0$. Similarly, if $\ell \neq p$ is another prime, and ℓ^{f_n} is the exact power of ℓ dividing $h(k_n)$, then f_n is bounded. By analogy, we may conjecture a similar result in the number field case. Washington [W2] proved that if $k/\mathbb{Q}$ is abelian, then f_n is bounded for the cyclotomic $\mathbb{Z}_p$-extensions.

The function field case also suggests that the Iwasawa invariant λ is analogous to the genus of a curve. Motivated by this analogy, Kida [K] derived for the λ-invariant the analog of the Riemann-Hurwitz formula for the genus of a curve. This formula has some nice applications to the study of zeros of p-adic L-functions.

There is a further analogy that motivated Iwasawa and this has to do with the Riemann hypothesis. The Galois group of $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is procyclic generated by the Frobenius automorphism ($x \mapsto x^p$). The Frobenius automorphism acts on the $\overline{\mathbb{F}}_p$ points of the curve and thus on its Jacobian. $P(x)$ above is essentially the characteristic polynomial of the Frobenius automorphism acting on the Jacobian of C. This interpretation of the zeta function was an essential factor in the resolution of the Riemann hypothesis for the zeta functions of curves.

Returning to the case of $\mu = 0$, we note that A_n is approximately $(\mathbb{Z}/p^n\mathbb{Z})^\lambda$. One can construct a direct system by defining a map $A_n \to A_m$ for $n < m$ given by sending the class of an ideal $\mathfrak{a}$ to the class of the ideal generated by $\mathfrak{a}$ in the

ring of integers of F_m, so that

$$\lim_{\rightarrow} A_n \sim (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda.$$

This reminds one of the p-power torsion of the Jacobian of a curve or more generally for an abelian variety. Perhaps, the p-adic zeta function can be written as a "characteristic polynomial or power series" of some topological generator of $\mathbb{Z}_p$ acting on X. It was this analogy that motivated Iwasawa to formulate the so-called "main conjecture."

More precisely, let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of $\mathbb{Q}(\zeta_p)$. We can define the p-adic zeta function of K as

$$\zeta_{K,p}(s) = \prod_{\substack{\chi \text{ even} \\ f_\chi | p}} L_p(s, \chi).$$

Iwasawa proved that there is a formal power series

$$A(x) = \prod_{\substack{\chi \text{ even} \\ f_\chi | p}} f(x, \chi) \quad \in \mathbb{Z}_p[[x]]$$

such that

$$\zeta_{K,p}(s) = \frac{A((1+p)^s - 1)}{h((1+p)^s - 1)},$$

with $h(x) = (x-p)/(x+1)$. This is analogous to the formula for the zeta function of a curve with $A(x)$ playing the role of $P(x)$. It is possible to interpret $A(x)$ as the "characteristic polynomial" of some generator of $\mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p$. $A(x)$ is essentially the characteristic polynomial of X_∞ and this fact came to be known as the "main conjecture of Iwasawa theory."

More precisely, with X as above, we note that complex conjugation acts on each A_n and therefore on X. Let

$$X^- = \{x \in X : \quad \overline{x} = -x\}.$$

This group plays the analogous role of the Jacobian of a curve in Iwasawa theory. Then X^- is a Λ-module which is Noetherian and torsion and so by the structure theorem,

$$X^- \sim \oplus_j \Lambda/(f_j(x)^{a_j}).$$

Let $F(x) = \prod_j f_j(x)^{a_j}$. The main conjecture states that there is a unit $u(x) \in \Lambda$ such that $A(x) = F(x)u(x)$. This was first proved in 1980 by Mazur and Wiles using high-powered techniques from algebraic geometry. Later work of Thaine, Rubin and Kolyvagin has led to simpler proofs (see Rubin's appendix to Lang [L]).

Mazur extended Iwasawa theory to study the Mordell-Weil groups of elliptic curves (and more generally of abelian varieties) in $\mathbb{Z}_p$-extensions. In 1970, he made the following conjecture. Suppose A is an abelian variety over a number field F. Assume that p is a prime such that A has good, ordinary reduction at all primes of F lying above p. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ extension. Then $A(F_\infty)$ is finitely generated.

He succeeded in proving this conjecture under the assumption that $A(F)$ and $\mathbf{III}_A(F)_p$ are both finite. Here, $\mathbf{III}_A(F)_p$ denotes the p-primary subgroup of the Tate-Shafarevich group of A over F. These investigations have had significant applications towards the proof of the Birch and Swinnerton-Dyer conjectures in the theory of elliptic curves.

Since the p-adic L-functions have now been interpreted as some form of characteristic polynomials of some operator, it may be interesting to study their zeros and inquire into their significance. It is fair to say that the study of the zeros of p-adic L-functions is still in its infancy. Washington [W3] has done some work on this question and has related it to the Buniakowski-Schinzel hypothesis about the existence of primes in polynomial sequences. It is possible that sieve theory may have some application to such questions and shed further light on the matter.

Exercises

1. Let K be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}$ its ring of integers. Prove Lemma 10.1 with Λ replaced by $\mathcal{O}[[x]]$.

2. Let $f \in \Lambda$. Using Theorem 10.3, show that $\Lambda/(f)$ is infinite. (Hint: By the structure theorem, it suffices to consider the two cases $f = p$ and f distinguished and irreducible. In the former case, $\Lambda/(p) \simeq \mathbb{F}_p[x]$ and the latter case, apply the division algorithm.)

3. Show that pseudo-isomorphism is not reflexive. Namely, show that $M \sim M'$ does not imply $M' \sim M$. (Hint: notice that $(p, x) \sim \Lambda$. If $\Lambda \sim (p, x)$, consider the image f of 1 under this map. Now apply the previous exercise.)

4. Prove Theorem 10.2 (Weierstrass preparation theorem) directly by writing

$$u = c_0 + c_1 x + \cdots$$

and solving the system of equations that result from

$$f(x) = (x^n + b_{n-1}x^{n-1} + \cdots + b_0)u.$$

5. Let $f(x)$ be distinguished of degree n. Show that

$$|\mathbb{Z}_p[[x]]/(p^m, f(x))| = p^{mn}.$$

6. If $f(x)$ is distinguished, show that $f(x)^m$ is distinguished.

7. Let d_m denote the discriminant of $\mathbb{Q}(\zeta_m)$ and d_m^+ the discriminant of $\mathbb{Q}(\zeta_m+\zeta_m^{-1})$. . Show that $\log|d_m| \sim \phi(m)\log m$ and $\log|d_m^+| \sim \frac{1}{2}\phi(m)\log m$ as $m\to\infty$.

8. Let h_n be the class number of $\mathbb{Q}(\zeta_{p^{n+1}})$ and h_n^+ the class number of its totally real subfield. It is known that $h_n = h_n^+ h_n^-$ for some integer h_n^-. The Brauer-Siegel theorem (see [W, p. 44]) implies

$$\log h_n^- \sim \frac{p^n(p-1)}{4}(n+1)\log p$$

as $n\to\infty$. Write $h_n = p^{e_n}h_n'$ with h_n' coprime to p. Using the Brauer-Siegel theorem and Iwasawa's theorem, show that h_n' tends to infinity as $n\to\infty$.

9. Let $r = \mathrm{ord}_p(\alpha - 1)$. If $r \geq 1$, show that $\mathrm{ord}_p(\alpha^{p^n} - 1) = r + n$.

10. If $\mathrm{ord}_p(\alpha - 1) = 0$, show that $\mathrm{ord}_p(\alpha^{p^n} - 1) = 0$. Deduce that

$$\mathrm{ord}_p\left(\prod_{j=1}^{2g}(\alpha_j^{p^n} - 1)\right) = \lambda n + \nu$$

with $\lambda = \#\{j : \mathrm{ord}_p(\alpha_j - 1) > 0\} \leq 2g$ and ν bounded.

Bibliography

[Ap] T. Apostol, Introduction to Analytic Number Theory, Undergraduate Texts in Mathematics, Springer-Verlag, 1976.

[Bo] R. Bojanic, A simple proof of Mahler's theorem on approximation of continuous functios of a p-adic variable by polynomials, *J. Number Theory,* **6** (1974)pp. 412-415.

[C] J. Cassels, Local Fields, *London Mathematical Society Student Texts,* **3**, Cambridge University Press., 1986.

[Cl] W. E. Clark, The Aryabhatiya of Aryabhata, University of Chicago Press, Chicago, Illinois, 1930.

[Co] R. Coleman, On the Galois groups of the exponential Taylor polynomials, *Enseign. Math.,* **33**(2) (1987), no. 3-4, 183-189.

[EM] J. Esmonde and M. Ram Murty, Problems in Algebraic Number Theory, GTM, Vol. 190, Springer-Verlag, 1999.

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Annals of Math.,* **109** (1979) pp. 377-395.

[G] F. Gouvêa, p-adic Numbers, Universitext, Springer, 1997.

[GS] D. Goldfeld and L. Szpiro, Bounds for the order of the Tate-Shafarevich group, *Comp. Math.,* **97** (1995), no.1-2, pp. 71-87.

[Gr] R. Greenberg, Iwasawa theory, Past and Present, in *Advanced Studies in Pure Mathematics,* **30** (2001), pp. 335-385.

[Iw] K. Iwasawa, On some properties of Γ-finite modules, *Annals of Math.,* **70**(2) (1959), pp. 530-561.

[J] G.J. Janusz, Algebraic Number Fields, Second Edition, *Graduate Texts in Mathematics,* **7**, American Math. Society, Providence, Rhode Island, 1996.

[K] N. Koblitz, p-adic Numbers, p-adic Analysis and Zeta Functions, Vol. 58, Springer-Verlag, 1977.

[K2] N. Koblitz, p-adic analysis: a short course on recent work, *London Math. Society Lecture Notes,* **46** (1980), Cambridge University Press, Cambridge, New York.

[Ki] Y. Kida, ℓ-extensions of CM fields and cyclotomic invariants, *Journal of Number Theory,* **12** (1980), pp. 519-528.

[L] S. Lang, Cyclotomic Fields, second edition, Springer-Verlag, 1990.

[MW] B.Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.,* **76** (1984), no. 2, 179-330.

[MO] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, *Sem. Bourbaki,* **694**, Astérisque 161-162, S.M.F., (1988), pp. 165-186.

[MaMu] L. Mai and M. Ram Murty, The Phragmén-Lindelöf theorem and modular elliptic curves, *Contemp. Math.,* **166** (1994), pp. 335-340, American Math. Society, Providence, R.I.

[M] M. Ram Murty, Problems in Analytic Number Theory, GTM/RIM, Vol. 206, Springer-Verlag, 2001.

[MM] M. Ram Murty and V. Kumar Murty, Non-vanishing of L-functions and Applications, *Progress in Mathematics,* **157**, Birkhaüser-Verlag, 1997.

[MR] M. Ram Murty and Marilyn Reece, A simple derivation of $\zeta(1-k) = -B_k/k$, *Functiones et Approximatio,* **28** (2000), 141-154.

[O] H. Osada, The Galois groups of the polynomials $x^n + ax^l + b$, *J. Number Theory,* **5** (1987), no. 2, 230-238.

[Ra] C. S. Rajan, On the size of the Shafarevich-Tate group of elliptic curves over function fields, *Comp. Math.,* **105** (1997), no. 1, pp. 29-41.

[Ro] A. Robert, A course in p-adic analysis, GTM, Vol. 198, Springer-Verlag, 2000.

[Se] E. Selmer, On the irreducibility of certain trinomials, *Math. Scand.,* **4** (1956), 287-302.

[Si] C. L. Siegel, Zu zwei Bemerkungen Kummers, *Nachr. Akad. Wiss., Göttingen, Math.-Phys. Kl.* (1964), no. 6, 51-57. (See also, *Gesammelte Abhandlungen,* Springer-Verlag, Berlin, 1966, Vol. 3, 436-442.)

[S] J. H. Silverman, Wieferich's criterion and the *abc*-conjecture, *J. Number Theory,* **30** (1988), no. 2, 226-237.

[W] L. Washington, Introduction to Cyclotomic Fields, GTM, Vol. 83, Second Edition, Springer-Verlag, 1997.

[W2] L. Washington, The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, *Inv. Math.,* **49** (1978), 87-97.

[W3] L. Washington, A family of cubic fields and zeros of 3-adic L-functions, *Journal of Number Theory,* **63** (1997), no. 2, 408-417.

[We] A. Weil, Number Theory, An Approach Through History, From Hammurapi to Legendre, Birkhaüser, 1984.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Annals of Math.*, **141**(2) (1995), no. 3, 443-551.

Index

p-adic Γ-function, 67
p-adic integers, 33
p-adic interpolation, 65
p-adic Weierstrass preparation theorem, 159, 161
p-adic distribution, 103
p-adic regulator, 130

ABC conjecture, 5
Adams congruences, 22
Ankeny, 120, 127
Artin, 120, 127
Artin-Hasse exponential, 40
Aryabhata, 11

Bernoulli distribution, 105
Bernoulli numbers, 2, 11
Bernoulli polynomial, 12, 85, 106
Birch, 168
Brahmagupta, 129
Brauer-Siegel theorem, 170
Brumer, 120, 131

Cauchy sequences, 32
Chebotarev density theorem, 152
Chowla, 120, 127
Clausen, 20
Coleman, 154
completion, 32
conductor, 117
cyclotomic polynomial, 63

decomposition group, 149
Dirac distribution, 105
Dirichlet, 118
Dirichlet character, 83
discriminant, 153

Eisenstein polynomials, 159
Eisenstein's criterion, 48, 135
elliptic curves, 4
equivalent norms, 30
Euler, 13
Euler product, 1
exponential function, 37, 60

Fermat quotient, 43, 98
Fermat's Last Theorem, 1, 2
Ferrero, 8, 100, 164
Frobenius automorphism, 167
functional equation, 84
functional equation of $\zeta(s)$, 2
fundamental unit, 120

Galois group, 149
Gauss sum, 83, 117
generalized Bernoulli number, 121
Greenberg, 100
Gross and Koblitz, 7, 79, 100

Haar distribution, 105
Hensel, 3
Hensel's lemma, 49, 51, 64
Hensel's lemma for polynomials, 54
Hurwitz ζ-function, 5, 27, 86

imprimitive character, 117
index of irregularity, 5
inertia group, 150
irregular primes, 23
Iwasawa, 4, 162
Iwasawa's logarithm, 61

Jacobian, 167

Kida, 166
Koblitz, 114
Krasner's lemma, 59
Kubota, 14
Kubota and Leopoldt, 4
Kummer congruences, 3, 20, 22, 92, 111
Kummer criterion, 46, 95
Kummer-Vandiver conjecture, 5

Laurent series, 34
Leopoldt, 14, 117, 120
local ring, 33, 159

locally analytic, 62
locally compact, 34
locally constant, 104
logarithm, 38, 61

Möbius function, 40, 54
Mahler's theorem, 68
Manin, 114, 159
Mazur, 9, 99, 103, 168
Mazur measure, 108, 111
measure, 106
Mellin transform, 99, 103
Minkowski's theorem, 150

Newton polygon, 133, 155
Newton's method, 51, 63
norm, 29

Ostrowski, 3
Ostrowski's theorem, 30

prime number theorem, 2
primitive character, 117
pseudo-isomorphic, 162

quadratic reciprocity, 151

radius of convergence, 37
ramification index, 56
ramified prime, 56, 150
regular prime, 3
regularized measure, 107
regulator, 130
relative discriminant, 150
Riemann, 1
Riemann ζ function, 1, 16
Riemann hypothesis, 2
Riemann hypothesis for curves, 166
Riemann-Hurwitz formula, 166

Schur, 154
Shafarevich-Tate groups, 6
Siegel, 4
squarefull number, 6
Stickelberger, 79
Stirling numbers, 75
Strassman's theorem, 41, 42
Swinnerton-Dyer, 168
symmetric group, 153

Teichmüller representative, 53
Tiechmüller character, 53
totally ramified, 56
trinomials, 153

uniformizer, 56, 57
unramified, 56

Vandiver, 96
von Staudt, 20
von Staudt-Clausen theorem, 46, 112
Voronoi congruences, 20
Voronoi's theorem, 21

Washington, 8, 164
Wieferich, 98
Wieferich criterion, 5
Wiles, 4, 9
Wilson's theorem, 25, 41, 67, 98

Titles in This Series

27 **M. Ram Murty,** Introduction to p-adic Analytic Number Theory, 2002

26 **Raymond Chan, Yue-Kuen Kwok, David Yao, and Qiang Zhang, Editors,** Applied Probability, 2002

25 **Donggao Deng, Daren Huang, Rong-Qing Jia, Wei Lin, and Jian Zhong Wong, Editors,** Wavelet Analysis and Applications, 2002

24 **Jane Gilman, William W. Menasco, and Xiao-Song Lin, Editors,** Knots, Braids, and Mapping Class Groups—Papers Dedicated to Joan S. Birman, 2001

23 **Cumrun Vafa and S.-T. Yau, Editors,** Winter School on Mirror Symmetry, Vector Bundles and Lagrangian Submanifolds, 2001

22 **Carlos Berenstein, Der-Chen Chang, and Jingzhi Tie,** Laguerre Calculus and Its Applications on the Heisenberg Group, 2001

21 **Jürgen Jost,** Bosonic Strings: A Mathematical Treatment, 2001

20 **Lo Yang and S.-T. Yau, Editors,** First International Congress of Chinese Mathematicians, 2001

19 **So-Chin Chen and Mei-Chi Shaw,** Partial Differential Equations in Several Complex Variables, 2001

18 **Fangyang Zheng,** Complex Differential Geometry, 2000

17 **Lei Guo and Stephen S.-T. Yau, Editors,** Lectures on Systems, Control, and Information, 2000

16 **Rudi Weikard and Gilbert Weinstein, Editors,** Differential Equations and Mathematical Physics, 2000

15 **Ling Hsiao and Zhouping Xin, Editors,** Some Current Topics on Nonlinear Conservation Laws, 2000

14 **Jun-ichi Igusa,** An Introduction to the Theory of Local Zeta Functions, 2000

13 **Vasilios Alexiades and George Siopsis, Editors,** Trends in Mathematical Physics, 1999

12 **Sheng Gong,** The Bieberbach Conjecture, 1999

11 **Shinichi Mochizuki,** Foundations of p-adic Teichmüller Theory, 1999

10 **Duong H. Phong, Luc Vinet, and Shing-Tung Yau, Editors,** Mirror Symmetry III, 1999

9 **Shing-Tung Yau, Editor,** Mirror Symmetry I, 1998

8 **Jürgen Jost, Wilfrid Kendall, Umberto Mosco, Michael Röckner, and Karl-Theodor Sturm,** New Directions in Dirichlet Forms, 1998

7 **D. A. Buell and J. T. Teitelbaum, Editors,** Computational Perspectives on Number Theory, 1998

6 **Harold Levine,** Partial Differential Equations, 1997

5 **Qi-keng Lu, Stephen S.-T. Yau, and Anatoly Libgober, Editors,** Singularities and Complex Geometry, 1997

4 **Vyjayanthi Chari and Ivan B. Penkov, Editors,** Modular Interfaces: Modular Lie Algebras, Quantum Groups, and Lie Superalgebras, 1997

3 **Xia-Xi Ding and Tai-Ping Liu, Editors,** Nonlinear Evolutionary Partial Differential Equations, 1997

2.2 **William H. Kazez, Editor,** Geometric Topology, 1997

2.1 **William H. Kazez, Editor,** Geometric Topology, 1997

1 **B. Greene and S.-T. Yau, Editors,** Mirror Symmetry II, 1997