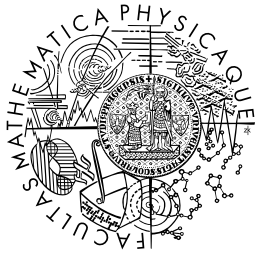

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Anh Dung Le

Bernoulli numbers and regular primes

Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D.
Study programme: Mathematics
Study branch: General mathematics

Prague 2017

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In Prague 20.07.2017 Anh Dung Le

Title: Bernoulli numbers and regular primes

Author: Anh Dung Le

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The aim of this work is to study the relation between regular primes and regular Bernoulli numbers (or just simply Bernoulli numbers). By the class number formula we connect the class number to the values of Dirichlet L-series. We then compute certain values of Dirichlet L-series in terms of generalized Bernoulli numbers. In order to investigate the relations between two types of Bernoulli numbers we define the p-adic Dirichlet L-series. In the end we get a congruence between the class number and Bernoulli numbers modulo p. Since the regular primes are those which divide the corresponding class numbers this is precisely our goal.

Keywords: Bernoulli number, regular prime, ideal class group, cyclotomic field

I would like to thank my supervisor Vítězslav Kala for his inspiring and useful advice. I am very grateful for his patience and the time he devoted to me during the preparation of this thesis.

Contents

Introduction

In 1847, Gabriel Lamé outlined a proof of Fermat's Last Theorem based on factoring the equation $x^p + y^p = z^p$ in $\mathbb{C}$, specifically the cyclotomic field based on the p-th roots of unity. His proof failed, however, because it assumed incorrectly that such complex numbers can be factored uniquely into primes, similar to integers. This gap was pointed out immediately by Joseph Liouville, who later read a paper that demonstrated this failure of unique factorisation, written by Ernst Kummer. Using the general approach outlined by Lamé, Kummer proved both cases of Fermat's Last Theorem for all regular prime numbers. However, he could not prove the theorem for the exceptional primes (irregular primes) that conjecturally occur approximately 39% of the time; the only irregular primes below 100 are 37, 59 and 67.

An odd prime number p is defined to be regular if it does not divide the class number of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity, Ernst Kummer (Kummer 1850) showed that an equivalent criterion for regularity is that p does not divide the numerator of any of the Bernoulli numbers B_k for $k = 2, 4, 6, \ldots, p-3$. In this thesis we focus on one implication of this theorem in 3.27, namely if p satisfies the criterion if and only $p \mid h^-$, the relative class number of $\mathbb{Q}(\zeta_p)$, the quotient between the class numbers h and h^+ of $\mathbb{Q}(\zeta_p)$ and its maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, respectively. The second implication can be proved by showing $p \mid h^- \Leftrightarrow p \mid h$ which is beyond the scope of this thesis. The proof can be found in the end of chapter 5 Washington [1].

In the first chapter we introduce the basic concepts that we will use throughout this thesis, in particular properties of finite extensions of $\mathbb{Q}$ (or number fields) and their rings of integers. We find out that the rings of integers are Dedekind domains and there exists unique factorization of ideals into prime ideals. The normal uniqueness of factorization does not hold here and the extent of how this unique factorization fails is measured by a number called class number. We then define the cyclotomic fields, the number fields of our main focus, and Dirichlet characters. The Dirichlet characters $\widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$ provide us valuable information about $\mathbb{Q}(\zeta_n)$.

In the second chapter we introduce two generalizations of Riemann zeta functions $\zeta(s)$, the Dirichlet L-series $L(s, \chi)$, which contain a Dirichlet character χ in the nominator, and Dedekind zeta function $\zeta_K(s)$, which are defined in a number field K. These two functions are related by Theorem 2.7. By class number formula the class number of K appears in the residue of $\zeta_K(s)$ at the simple pole $s = 1$ and the values of $L(s, \chi)$ can be computed in terms of generalized Bernoulli numbers (Theorem 2.5 and Theorem 2.20 (without proof)). This gives us a connection between the class number and generalize Bernoulli numbers.

In the last chapter we establish the tie between the ordinary Bernoulli numbers and generalized Bernoulli numbers modulo a prime p. In order to achieve this goal we introduce p-adic L-functions and investigate their properties by p-adic analysis. The desired congruences between ordinary and generalized Bernoulli numbers then emerge from Corollary 3.26.

1. Cyclotomic fields and Dirichlet characters

1.1 Basics from algebraic number theory

Definition 1.1. Let K be a field. We say that K is a number field of degree d if it is a finite extension of $\mathbb{Q}$ of degree d, i.e. d-dimensional vector space over $\mathbb{Q}$

Definition 1.2. Let K be a number field. By its ring of integers $\mathcal{O}_K$ we mean a subring of K consisting of all roots of polynomials with integer coefficients in K.

Definition 1.3. A ring A is integrally closed if it is its own integral closure in its field of fractions K.

Definition 1.4. A Dedekind domain is an integral domain A such that

1. A is Noetherian
2. A is integrally closed
3. every nonzero prime ideal is maximal

Theorem 1.5. *Let A be a Dedekind domain. Every proper nonzero ideal $\mathfrak{P}$ of A can be written in the form*

$$\mathfrak{P} = \mathfrak{P}_1^{r_1} \dots \mathfrak{P}_n^{r_n}$$

with the $\mathfrak{P}_i$ distinct prime ideals and the $r_i > 0$; the $\mathfrak{P}_i$ and the r_i are uniquely determined.

For proof see Milne [3, Theorem 3.7].

Definition 1.6. A fractional ideal of A is a nonzero A-submodule $\mathfrak{a}$ of K such that

$$d\mathfrak{a} \stackrel{\text{def}}{=} \{da \mid a \in \mathfrak{a}\}$$

is contained in A for some nonzero $d \in A$, i.e., it is a nonzero A-submodule of K, whose elements have a common denominator.

Every nonzero element b of K defines a fractional ideal

$$(b) \stackrel{\text{def}}{=} bA \stackrel{\text{def}}{=} \{ba \mid a \in A\}$$

A fractional ideal of this type is said to be principal.

The product of two fractional ideals is defined in the same way as for normal ideals

$$\mathfrak{ab} = \{ \sum_{\text{finite sum}} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

This is again a fractional ideal: it is obviously an A-module, and if $d\mathfrak{a} \subset A$ and $e\mathfrak{b} \subset A$, then $de\mathfrak{ab} \subset A$. For principal fractional ideals $(a)(b) = (ab)$.

Theorem 1.7. *Let A be a Dedekind domain. The set $Id(A)$ of fractional ideals is a group, in fact, it is the free abelian group on the set of nonzero prime ideals.*

For proof see Milne [3, Theorem 3.20].

Definition 1.8. We define the ideal class group $Cl(A)$ of A to be the quotient $Cl(A) = Id(A) = P(A)$ of $Id(A)$ by the subgroup of principal ideals. The class number of A is the order of $Cl(A)$ (when finite). In the case that A is the ring of integers $\mathcal{O}_K$ in a number field K, we often refer to $Cl(\mathcal{O}_K)$ as the ideal class group of K, and its order as the class number of K.

Theorem 1.9. *Let K be a number field, then the class number of K is finite.*

For proof see Milne [3, Theorem 4.4].

Theorem 1.10. *Let A be a Dedekind domain with the field of fractions K, and let B be the integral closure of A in a finite separable extension L of K. Then B is a Dedekind domain.*

For proof see Milne [3, Theorem 3.29].

Definition 1.11. Let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathfrak{a}$ a nonzero (integral) ideal of $\mathcal{O}_K$. The absolute norm of $\mathfrak{a}$ is

$$N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|\,.$$

By convention, the norm of the zero ideal is taken to be zero.

Definition 1.12. Let A be a Dedekind domain with field of fractions K, and let B be the integral closure of A in a finite separable extension L of K. A prime ideal p of A will factor in B:

$$pB = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}, e_i \geq 1$$

If any of the numbers e_i is greater than 1, then we say that p is ramified in B (or L). The number e_i is called the ramification index. We say $\mathfrak{P}$ divides p (written $\mathfrak{P} \mid p$) if $\mathfrak{P}$ occurs in the factorization of p in B. We then write $e(\mathfrak{P}/p)$ for the ramification index and $f(\mathfrak{P}/p)$ for the degree of the field extension $[B/\mathfrak{P} : A/p]$ (called the residue class degree, note that A/p can be embedded into $B/\mathfrak{P}$ by the map $a \pmod p \mapsto a \pmod{\mathfrak{P}}$). A prime p is said to split (or split completely) in L if $e_i = f_i = 1$ for all i, and it is said to be inert in L if pB is a prime ideal (so $g = 1 = e$).

Theorem 1.13. *Let m be the degree of L over K, and let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the prime ideals dividing p; then*

$$\sum_{i=1}^{g} e_i f_i = m$$

If L is Galois over K, then all the ramification numbers are equal, and all the residue class degrees are equal, and so

$$efg = m$$

For proof see Milne [3, Theorem 3.34].

1.2 Cyclotomic fields and Dirichlet characters

Definition 1.14. The n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ (where $n > 2$) is obtained by adjoining a primitive n-th root of unity ζ_n to the rational numbers.

Definition 1.15. A prime p is called regular if p divides the class number of $\mathbb{Q}(\zeta_n)$. Otherwise p is called irregular.

Theorem 1.16. *$\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$.*

For proof see Washington [1, Theorem 2.6].

Lemma 1.17. *If α is an algebraic integer all of whose conjugates have absolute value 1, then α is a root of unity.*

Proof. The coefficients of the irreducible polynomials for all powers of α are in $\mathbb{Z}$ which can be given bounds depending only on the degree of α over $\mathbb{Q}$. It follows that there are only finitely many irreducible polynomials which can have a power of α as a root. Therefore there are only finitely many distinct powers of α. The lemma follows. □

Theorem 1.18. *Let ϵ be a unit of $\mathbb{Z}[\zeta_p]$. Then there exist $\epsilon_1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $r \in \mathbb{Z}$ such that $\epsilon = \zeta^r \epsilon_1$.*

For proof see Washington [1, Proposition 1.5].

Definition 1.19. A Dirichlet character is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$.

If $n \mid m$ then χ induces a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore we could also regard χ as being defined mod m or mod n, since both are essentially same map. It is convenient to choose n minimal and call it the conductor of χ, denoted f or f_χ.

It is convenient to classify characters into two types: if $\chi(-1) = 1$ then χ is called even; if $\chi(-1) = -1$ then χ is called odd. Moreover we can regard χ as a map $\mathbb{Z} \to \mathbb{C}$ by letting $\chi(a) = 0$ if $(a, f_\chi) \neq 1$. In this case it is important to make a convention regarding the modulus of definition of χ. We shall always regard χ as being defined modulo its conductor. Such characters are called primitive.

Lemma 1.20. *Let χ be Dirichlet of conductor f then*

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

Proof. Since $\chi(a) = 0$ for $gcd(a, f) \neq 1$ we only need to consider residues a coprime to f . Let $b \neq 1$ be a natural number coprime to f then $b \cdot (\mathbb{Z}/f\mathbb{Z})^\times$ is the same set as $(\mathbb{Z}/f\mathbb{Z})^\times$. Therefore

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

and the conclusion follows. □

In the following, when we talk of the characters of $(\mathbb{Z}/n\mathbb{Z})^\times$, or of the characters mod n, we shall be including the characters of conductor dividing n, for example the trivial character of conductor 1. This set of characters with multiplication forms a group denoted by $\widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$.

The convention that all characters are primitive plays a part in the multiplication of characters. Let χ and ψ be Dirichlet characters of conductors f_χ and f_ψ. Since $lcm(f_\chi, f_\psi)$ is the common period of χ and ψ, we have the following homomorphism

$$\gamma : (\mathbb{Z}/lcm(f_\chi, f_\psi)\mathbb{Z})^\times \to \mathbb{C}^\times$$

defined by $\gamma(a) = \chi(a)\psi(a)$. Then $\chi\psi$ is the primitive character associated to γ.

It is sometimes advantageous to think of Dirichlet characters as being characters of Galois groups of cyclotomic fields $\mathbb{Q}(\zeta_n)$, if we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$. In general, let χ be a character mod n, hence a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let K be the fixed field of the kernel of χ. Then $K \subset \mathbb{Q}(\zeta_n)$, and if n is minimal then $n = f_\chi$. The field K depends only on χ and is called the field belonging to χ.

More generally, let X be a finite group of Dirichlet characters. let n be the least common multiple of the conductors of the characters in X, so X is a subgroup of the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let H be the intersection of the kernels of these characters and let K be the fixed field of H. The field K is called the field belonging to X and if X is cyclic and generated by χ, then K is precisely the same as the field belonging to χ mentioned above.

In the statements below we consider only finite abelian groups G.

Lemma 1.21. *If G is a finite abelian group, then $G \cong \widehat{G}$.*

For proof see Washington [1, Lemma 3.1].

Corollary 1.22. *$\widehat{\widehat{G}} \cong G$ "canonically", so we can equate $\widehat{\widehat{G}}$ with G.*

For proof see Washington [1, Corollary 3.2].

Remark. An element g of G can be considered an element of $\widehat{\widehat{G}}$ in the following way

$$g(\chi) \stackrel{def}{=} \chi(g),\ \forall \chi \in \widehat{G}$$

Definition 1.23. Now let H be a subgroup of G (Since we consider a finite abelian group G, H is always normal). Let

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(h) = 1, \forall h \in H\}.$$

Lemma 1.24. *We have a natural isomorphism $H^\perp \cong \widehat{(G/H)}$.*

Proof. Consider the map $\phi : H^\perp \to \widehat{(G/H)}$ by $\phi(\chi)(g + H) = \chi(g)$ for $\chi \in H^\perp$. The map $\phi(\chi)$ is well-defined, i.e. it does not depend on the choice of the

representative g for the equivalence class $g+H$, because $\chi(H)=\{1\}$. The map is injective, because if $\phi(\chi)$ is trivial on (G/H) then

$$\chi(g)=\phi(\chi)(g+H)=1$$

so χ is trivial on G. Let $\chi'\in\widehat{(G/H)}$ and consider $\chi(g)\overset{def}{=}\chi'(g+H)$. Clearly g is a well-defined character of G, which is trivial on H, so $g\in H^\perp$ and ϕ is surjective, thus a group isomorphism. By the first isomorphism theorem we have $H^\perp\cong\widehat{(G/H)}$. □

Lemma 1.25. $\widehat{H}\cong\widehat{G}/H^\perp$.

For proof see Washington [1, Proposition 3.3].

Lemma 1.26. $(H^\perp)^\perp=H$ *(here we equate* $\widehat{\widehat{G}}=G$*).*

For proof see Washington [1, Proposition 3.4].

Remark. From the remark below Corollary 1.22 $g\in(H^\perp)^\perp\Leftrightarrow 1=g(\chi)=\chi(g)$, so

$$(H^\perp)^\perp=\{g\in G\mid\chi(g)=1\forall\chi\in H^\perp\}$$

or the intersection of the kernels of χ in $H^\perp$.

Lemma 1.27. *Consider* $X\subset\widehat{Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})}$ *a finite group of Dirichlet characters and* $K\subset\mathbb{Q}(\zeta_n)$ *the field belonging to* X*. It is well-known that each* $\sigma\in Gal(K/\mathbb{Q})$ *can be extended to* $(\widehat{\sigma})\in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$*. Then the following map is a group isomorphism*

$$\begin{aligned}\phi:X&\to\widehat{(Gal(K/\mathbb{Q})}\\ \chi&\mapsto(\sigma\mapsto\chi(\widehat{\sigma}))\end{aligned}$$

In certain sense X *is precisely the set of homomorphism* $Gal(K/\mathbb{Q})\to\mathbb{C}^\times$.

Proof. By definition K is the fixed field of

$$X^\perp=\{g\in\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\mid\chi(g)=1,\forall\chi\in X\}$$

then $X^\perp=\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$ by Galois theory. Therefore

$$\begin{aligned}Y&\overset{\text{Lemma 1.26}}{=}(Y^\perp)^\perp=\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)^\perp\overset{\text{Lemma 1.24}}{=}\\&=(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\widehat{\mathbb{Q})/\mathrm{Gal}}(\mathbb{Q}(\zeta_n)/K))\overset{\text{Galois theory}}{=}\widehat{\mathrm{Gal}(K/\mathbb{Q})}\end{aligned}$$

□

Remark. It follows that we have a one-one correspondence between subgroups of $\mathrm{Gal}(\widehat{\mathbb{Q}(\zeta_n)}/\mathbb{Q})$ and subfields of $\mathbb{Q}(\zeta_n)$.

We now show how ramification indices maybe computed in terms of characters. Let $n=\prod p^a$. Corresponding to the decomposition

$$(\mathbb{Z}/n\mathbb{Z})^\times\cong\prod(\mathbb{Z}/p^a\mathbb{Z})^\times$$

we may write any character χ defined mod n as

$$\chi = \prod \chi_p$$

where χ_p is a character defined mod p^a. This can be seen from the character multiplication homomorphism $\widehat{(\mathbb{Z}_n)^\times} \times \widehat{(\mathbb{Z}_m)^\times} \to \widehat{(\mathbb{Z}_{mn})^\times}$, where m, n are coprime. This map is an isomorphism because it is injective and by Lemma 1.21 both sides are finite groups of the same size.

Lemma 1.28. *If $gcd(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$.*

Proof. We know that $f_{\chi\psi} \neq f_\chi f_\psi$, then in the above isomorphism $\chi\psi$ would decompose into a product of different characters than in the decomposition of $f_\chi f_\psi$, which is a contradiction. □

Theorem 1.29. *Let χ and ψ be primitive Dirichlet characters, if $\chi(a) \neq 0$ or $\psi \neq 0$ then $\chi(a)\psi(a) = \chi\psi(a)$.*

Proof. If both $\chi(a)$ and $\psi(a)$ are non-zero then $gcd(f_\chi f_\psi), a) = 1$, hence the conductor of $\chi\psi$ is also coprime to a and the conclusion follows.

If $\psi(a) = 0$ then $\chi(a) \neq 0$. Clearly there exists a prime $p|a$ such that $\psi(a) = 0$. Obviously $\chi(p) \neq 0$ and if $\chi\psi(p) = 0$ then $\chi\psi(a) = 0$, so it is enough to prove for p. Let $f_\chi = p^b m$, where $p \not| m$ then $\chi = \chi_1\chi_2$ with conductors p^b and m, respectively, by $gcd(p^b, m) = 1$ and Lemma 1.28. Since $f_{\chi_2\psi} \mid f_{\chi_2} f_\psi$ we have $gcd(p, f_{\chi_2\psi}) = 1$ and again by Lemma 1.28 $f_{\chi\psi} = p f_{\chi_2\psi}$. Therefore $p|f_{\chi\psi}$ and $\chi\psi(p) = 0$. □

Definition 1.30. If X is a group of Dirichlet characters, then we let

$$X_p = \{\chi_p \mid \chi \in X\}$$

Theorem 1.31. *Let X be a group of Dirichlet characters and K the associated field. Let p be a prime number with ramification index e in K. Then $e = |X_p|$.*

For proof see Washington [1, Theorem 3.5].

Corollary 1.32. *Let χ be a Dirichlet character and K the associated field. Then p ramifies in K if and only if $\chi(p) = 0$ (equivalently $p \mid f_\chi$).*
More generally, let L be the field associated with a group X of Dirichlet characters. Then p is unramified in $L/\mathbb{Q}$ if and only if $\chi(p) \neq 0$ for all $\chi \in X$.

For proof see Washington [1, Corollary 3.6] Corollary 3.6.

Theorem 1.33. *Let X be a group of Dirichlet characters, K the associated field. Let*

$$Y = \{\chi \in X \mid \chi(p) \neq 0\},\ Z = \{\chi \in X \mid \chi(p) = 1\}$$

Then

$$e = [X : Y],\ f = [Y : Z],\ \text{and } g = [Z : 1]$$

are the ramification index for p in K, the residue class degree, and the number of primes lying above p, respectively. In fact

$$X/Y \cong \text{ the inertia group, } X/Z \cong \text{ the decomposition group}$$
$$Y/Z \cong \text{ is cyclic of order } f$$

For definition of the inertia group see Milne [3, page 130], the decomposition group see Milne [3, page 139] and for proof see Washington [1, Theorem 3.7].

Theorem 1.34 (Conductor-Discriminant Formula)**.** *Let K be the number field associated to the group X of Dirichlet characters. Then the discriminant of K is given by*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi$$

where r_2 is the number of conjugate pairs of complex embedding $K \to \mathbb{C}$.

For proof see Washington [1, Theorem 3.11] and chapter 4 page 35.

2. Analytic number theory

2.1 Dirichlet L-series

Throughout this chapter χ will denote a Dirichlet character of conductor f.

Definition 2.1. The L-series with complex variable s attached to χ is defined by:

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

The series converges when $\mathrm{Re}(s) > 1$, where $\mathrm{Re}(s)$ denotes the real part of s because

$$|n^s| = \left|e^{(\mathrm{Re}(s)+i\mathrm{Im}(s))\log(n)}\right| = \left|e^{\mathrm{Re}(s)\log(n)}\right| \cdot \left|e^{i(\mathrm{Im}(s)log(n))}\right| = \left|e^{\mathrm{Re}(s)log(n)}\right| = n^{\mathrm{Re}(s)}$$

Hence it guarantees the absolute convergence of the L-series

$$\sum_{n=1}^{\infty} \left|\frac{\chi(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{Re(s)}}$$

For $\chi = 1$ this is the usual Riemann zeta function. It is well known that $L(s,\chi)$ may be continued analytically to the whole complex plane, except for a simple pole at $s = 1$ when $\chi = 1$. See Garrett [7].

Let $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$ be the gamma function, $\tau(\chi) = \sum_{a=1}^{f} \chi(a)e^{2\pi ia/f}$ be a Gauss sum and $\delta = 0$ if $\chi(-1) = 1, \delta = 1$ if $\chi(-1) = -1$. Then we have a functional equation (see Garrett [7])

$$\left(\frac{f}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) = W_\chi \left(\frac{f}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\bar{\chi})$$

More generally, we may define the Hurwitz zeta function

$$\zeta(s,b) = \sum_{n=0}^{\infty} \frac{1}{(b+n)^s},\ \mathrm{Re}(s) > 1,\ 0 < b \leq 1$$

Then

$$\sum_{a=1}^{f} \chi(a) f^{-s} \zeta\left(s, \frac{a}{f}\right) = \sum_{a=1}^{f} \sum_{n=0}^{\infty} \frac{\chi(a)}{f^s\left(n+\frac{a}{f}\right)^s} = \sum_{a=1}^{f} \sum_{n=0}^{\infty} \frac{\chi(a+nf)}{(fn+a)^s} = L(s,\chi)$$

Later on we will be interested in the values of $L(s,\chi)$, where s is a non-positive integer. To describe $L(1-n,\chi)$ explicitly we need to define the generalized Bernoulli numbers.

2.2 Bernoulli numbers

Definition 2.2. The ordinary Bernoulli numbers B_n are defined by

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

where the right hand side is the Taylor expansion of the function on the left hand side. For the generalized Bernoulli numbers $B_{n,\chi}$

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

Remark. For a nontrivial Dirichlet character χ it is easy to see that the defining relation for the $B_{n,\chi}$ is an even function of t when χ is even and odd when χ is odd. Therefore

$$B_{n,\chi} = 0 \text{ if } n \not\equiv \delta \pmod 2$$

Note that when $\chi = 1$ we have $f = 1$, therefore:

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

so $B_{n,1} = B_n$ except for $n = 1$, when we have $B_{1,1} = \frac{1}{2}$ and $B_1 = -\frac{1}{2}$.

We also need the Bernoulli polynomials $B_n(X)$ defined by:

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

.

Lemma 2.3. *For $n \in \mathbb{N}_0$ we have*

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

Proof.

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

The last equality follows from two Taylor expansions. Comparing the coefficients on both sides we get

$$\frac{B_n(X)}{n!} = \sum_{i=0}^{n} \frac{B_i}{i!} \frac{X^{n-i}}{(n-i)!} = \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$$

which is what we want. □

Theorem 2.4. *Let F be any multiple of f. Then*

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

Proof.

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

where the last equality follows from the definition 2.2 for the general Bernoulli numbers with Ft plugged into t and a/F plugged into X. Let $g = F/f$ and $a = b + cf$. Let b run from 1 to f and c run from 0 to $g-1$ respectively. Each a between 1 and F corresponds to exactly one pair of b and c. Also note that $\chi(a) = \chi(b)$ because the conductor is f. After expressing a, F in terms of b, c, f, g we have:

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

and the result follows. □

Theorem 2.5. *$L(1-n, \chi) = -(B_{n,\chi}/n), n \geq 1$. More generally*

$$\zeta(1-n, b) = -B_n(b),\ 0 < b \leq 1.$$

For proof see Washington [1, Theorem 4.2].

2.3 Class number

Definition 2.6. Let K be a number field. Its Dedekind zeta function $\zeta_K(s)$ is defined for complex numbers s with real part $\mathrm{Re}(s) > 1$

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{(N_{K/\mathbb{Q}}(I))^s}$$

where I ranges through the non-zero ideals of the ring of integers $\mathcal{O}_K$ of K and $N_{K/\mathbb{Q}}(I)$ denotes the absolute norm of I (which is equal to both the index $[\mathcal{O}_K : I]$ or equivalently the cardinality of quotient ring $\mathcal{O}_K/I$.

The Dedekind zeta function $\zeta_K(s)$ of K has an Euler product which is a product over all the prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$

$$\zeta_K(s) = \prod_{\mathfrak{P} \subseteq \mathcal{O}_K} \frac{1}{1 - (N_{K/\mathfrak{Q}}(\mathfrak{P}))^{-s}},\ \text{for } \mathrm{Re}(s) > 1.$$

This is the expression in analytic terms of the uniqueness of prime factorization of the ideals I in $\mathcal{O}_K$, since it is a Dedekind domain. It is well known that $\zeta_K(s)$ may be continued analytically to the whole complex plane, except for a simple pole at $s = 1$.

Theorem 2.7. *Let X be a group of Dirichlet characters, K the associated field, and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$$

Proof. Let n be the least common multiple of the conductors of the characters of X, then $K \subset \mathbb{Q}(\zeta_n)$ and $X \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, X is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, hence K is a Galois extension. Let p be a prime in $\mathbb{Z}$. Since K is a Galois extension by Theorem 3.34 (Milne [3]) the prime ideals in the decomposition of (p) in K have the same ramification index e and residue class degree f. Suppose

$$(p) = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$$

is the prime factorization of p in K, $N\mathfrak{P} = p^f$. Then $\zeta_K(s)$ contains the factor

$$\prod_{\mathfrak{P}|p} (1 - (N\mathfrak{P})^{-s})^{-1} = (1 - p^{-fs})^{-g}$$

We will prove it is equal to $\prod_{\chi \in X}(1 - \chi(p)p^{-s})^{-1}$, the Euler factors corresponding to p in $L(s, \chi)$. Since each prime ideal $\mathfrak{P}$ appears in the decomposition of only one prime p in $\mathbb{Z}$ this would prove our theorem. Those χ with $\chi(p) = 0$ do not contribute so we ignore them. By Theorem 1.33, Y/Z is cyclic of order f, where Y is the group of those $\chi \in X$ with $\chi(p) \neq 0$ and Z consists of those with $\chi(p) = 1$. As χ runs through a set of coset representatives for Y/Z, $\chi(p)$ runs through all f-th roots of unity (since if $\chi_1(p) = \chi_2(p)$ then $\chi_1\chi_2^{-1}(p) = 1$, which means it is 1 in Y/Z). Each coset has g elements. Since:

$$\prod_{a=0}^{f-1} (1 - \zeta_f^a p^{-s}) = (1 - p^{-fs})$$

and the result follows.

□

Corollary 2.8. $L(1, \chi) \neq 0$

Proof. Let K be the field belonging to χ. It is well known that the zeta function of K has a simple pole $s = 1$. Let b be the order of χ. Then

$$\zeta_K(s) = \prod_{a=0}^{b-1} L(s, \chi^a) = \zeta(s) \prod_{a=1}^{b-1} L(s, \chi^a)$$

Since both $\zeta(s)$ and $\zeta_K(s)$ has a simple pole at $s = 1$, none of the factors $L(s, \chi^a)$ can vanish at $s = 1$. This completes the proof. □

Definition 2.9. Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. Let $b_1, \dots, b_n$ be an integral basis of $\mathcal{O}_K$ (i.e. a basis as a Z-module), and let $\{\sigma_1, \dots, \sigma_n\}$ be the set of embeddings of K into the complex numbers. The discriminant of K is the square of the determinant of the n by n matrix B whose (i, j)-entry is $\sigma_i(b_j)$.

Definition 2.10. Let K be a number field and r_1, r_2 are the numbers of real embeddings and conjugate pairs of imaginary embeddings to $\mathbb{C}$, respectively. Let $r = r_1 + r_2 - 1$ and let $\epsilon_1, \ldots, \epsilon_r$ be a set of independent units of K. Write the embeddings of K to $\mathbb{C}$ as $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_r, \overline{\sigma_r}$, where $\sigma_j, 1 \leq j \leq r_1$, is real, and $\sigma_j, \overline{\sigma_j}, r_1 + 1 \leq j \leq r + 1$, is a pair of complex embeddings. Finally let $\delta_j = 1$ if σ_j is real and $\delta_j = 2$ if σ_j is complex. The regulator is define to be

$$R_K(\epsilon_1, \ldots, \epsilon_r) = |det(\delta_j \log |\sigma_i(\epsilon_j)|)|_{1 \leq i,j \leq r}$$

Note that we omit one σ_j. Since the norm of each ϵ is ± 1, the sum of all $\sigma_i, 1 \leq i \leq r + 1$, of $\delta_i \log |\sigma_i(\epsilon_j)|$ is 0. Since we take the absolute value of the determinant, the possible sign change from omitting different σ does not happen.

If $\epsilon_1, \ldots, \epsilon_r$ is a basis for the group of units of K modulo roots of unity, then $R_K(\epsilon_1, \ldots, \epsilon_r) = R_K$ is called the regulator of K. Again, the fact that we took the absolute value of the determinant makes R_K independent of the choice of basis and ordering of the σ's.

The zeta function of a field K has residue at the simple pole $s = 1$ with residue (see Osserman [8])

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}}$$

where r_1, r_2 are defined as usual, h is the class number of K, R is the regulator, w is the number of roots of unity in K, and d is the discriminant. Suppose K belongs to a group X of Dirichlet characters. Using Theorem 2.7, and the fact that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, we obtain

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi)$$

Definition 2.11. A field is called totally real if all its embeddings into $\mathbb{C}$ lie in $\mathbb{R}$ and totally imaginary if none of its embeddings lie in $\mathbb{R}$. A CM-field is a totally imaginary quadratic extension K of a totally real number field K^+.

Lemma 2.12. *Let K be a CM-field, then $K^+ = K \cap \mathbb{R}$.*

Proof. Clearly $K^+ \subset K \cap \mathbb{R}$, but $[K : K^+] = 2$ a prime, so any intermediate field must be K or K^+. Since K is totally imaginary, $K \cap \mathbb{R}$ must be K^+. □

Lemma 2.13. *Let K be a CM-field and $\phi, \psi : K \to \mathbb{C}$ be two embeddings. Then $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$ In other words complex conjugation on $\mathbb{C}$ induces an automorphism on the field K which is independent of the embedding into $\mathbb{C}$.*

Proof. First note that $\phi(K)/\phi(K^+)$ is quadratic, hence normal (since if $\phi(K)$ contains a root of a quadratic polynomial over $\phi(K^+)$ then the second root lies in $\phi(K)$ as well). Since K^+ is totally real, $\phi(K^+)$ lies in $\mathbb{R}$ and complex conjugation fixes $\phi(K^+)$. Therefore from normality of $\phi(K)/\phi(K^+)$ we get $\bar{\phi}(K) = \phi(K)$. In particular $\phi^{-1}(\bar{\phi})$ is defined.

Clearly both $\phi^{-1}(\bar{\phi})$ and $\psi^{-1}(\bar{\psi})$ are automorphisms of K and both fix K^+ since it is totally real. Since K is totally imaginary, neither automorphism can be the identity. Therefore they must be equal since $\mathrm{Gal}(K/K^+)$ has order 2. $\square$

Remark. Consequently, when working with CM-fields we may talk about $\bar{\alpha}$ and $|\alpha|^2 = \alpha\bar{\alpha}$, which are well-defined and independent of the embedding.

Example. Cyclotomic extensions $\mathbb{Q}(\zeta_n)$ are CM-field because they are totally imaginary quadratic extension of totally real number fields $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Theorem 2.14. *Let K be a CM-field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h. The quotient h^- is called the relative class number.*

For proof see Washington [1, Theorem 4.10].

Theorem 2.15. *Let K be a CM-field and let E be its unit group. Let E^+ be the unit group of K^+ and let W be the group of roots of unity in K. Then*

$$Q \stackrel{def}{=} [E : WE^+] = 1 \text{ or } 2$$

Proof. Define $\phi : E \to W$ by $\phi(\epsilon) = \epsilon/\bar{\epsilon}$. Since K is a CM-field, by Lemma 2.13 $\bar{(\epsilon^\sigma)} = (\bar{\epsilon})^\sigma$ for all embeddings σ, we have $|\phi(\epsilon)^\sigma| = 1$ for all σ, hence by Lemma 1.17 $\phi(\epsilon)$ is a root of unity and ϕ is well-defined. If $\epsilon \in W \subset E$, then $\phi(\epsilon) = \epsilon/\bar{\epsilon} = \epsilon^2$, thus $W^2 \subset \phi(E)$ and we can define a map $\psi : E \to W/W^2$ induced by ϕ, i.e. the composition of *phi* with the natural projection from W to W/W^2. Suppose $\epsilon = \zeta\epsilon_1$, where $\zeta \in W$ and $\epsilon_1 \in E^+$, thus ϵ_1 is a real number. Then

$$\phi(\epsilon) = \frac{\zeta\epsilon_1}{\overline{\zeta\epsilon_1}} = \frac{\zeta\epsilon_1}{\zeta^{-1}\epsilon_1} = \zeta^2$$

so $\epsilon \in \mathrm{Ker}(\psi)$. Conversely, suppose $\phi(\epsilon) = \zeta^2 \in W^2$. Then $\epsilon_1 = \zeta^{-1}\epsilon = \zeta^{-1}\zeta^2\bar{\epsilon} = \zeta\bar{\epsilon} = \overline{\zeta\epsilon} = \bar{\epsilon}_1$ Then ϵ_1 is real, hence by Lemma 2.12 belongs to E^+. It follows that $Ker(\psi) = WE^+$. Since $|W/W^2| = 2$, we are done. Note that if $\phi(E) = W$ then $Q = 2$ and if $\phi(E) = W^2$ then $Q = 1$. $\square$

Corollary 2.16. *Let $K = \mathbb{Q}(\zeta_n)$. Then $Q = 1$ if n is a prime power and $Q = 2$ if n is not a prime power.*

Proof. Conside $\epsilon \in E$. Suppose n is an odd prime power and. Then from Theorem 1.18 there exists $\epsilon_1 \in E^+$ and $r \in \mathbb{Z}$ such that $\epsilon = \zeta_n^r\epsilon_1$. Hence

$$\frac{\epsilon}{\bar{\epsilon}} = \frac{\zeta\epsilon_1}{\overline{\zeta\epsilon_1}} = \frac{\zeta\epsilon_1}{\zeta^{-1}\epsilon_1} = \zeta^2 \in W^2$$

so $\psi(E) \subset W^2$ and $Q = 1$. For $p = 2$ we cannot use Lemma 1.5. Suppose ϵ is a unit in $\mathbb{Q}(\zeta_{2^m})$ such that $\epsilon/\bar{\epsilon} = \zeta = \zeta_{2^m}^s \notin W^2$, then s is odd and ζ is a primitive $2^m th$ root of unity since ζ_{2^m} has order 2^m. The imaginary unit $i = \zeta_{2^m}^{2^{m-2}} \in \mathbb{Q}(\zeta_{2^m})$. Let N denote the norm from $\mathbb{Q}(\zeta_{2^m})$ to $Q(i)$. Consider $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q})$, then $\sigma(\zeta) = \zeta^a$ for odd a between 0 and 2^m, then σ fixes $\mathbb{Q}(i)$ if and only if $i^a = \sigma(i) = i$, which is equivalent to $a \equiv 1 \pmod 4$, thus

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}(i)) = \{\zeta_{2^m} \to \zeta_{2^m}^a \mid 0 < a < 2^m, a \equiv 1 \pmod 4\}$$

Then by Milne [3, Corollary 2.20] on the properties of norm $N(\zeta) = \zeta^b$, where

$$b = \sum_{\substack{0<a<2^m \\ a\equiv 1 \pmod 4}} a = \sum_{j=0}^{2^{m-2}-1} (1+4j) = 2^{m-2} + 2^{m-1}(2^{m-2}-1) \equiv$$
$$\equiv 2^{m-2} \pmod{2^{m-1}}$$

Therefore ζ^a is a primitive 4-th root of 1. It follows that $N(\epsilon)/\overline{N(\epsilon)} = \pm i$. But $N(\epsilon)$ is a unit of $\mathbb{Q}(i)$, since its inverse is $N(\epsilon^{-1})$, therefore the only possibilities are ± 1 or $\pm i$. None of these gives $N(\epsilon)/\overline{N(\epsilon)} = \pm i$, so we have a contradiction. So $Q = 1$ for $\mathbb{Q}(\zeta_{2^m})$.
Now assume n is not a prime power. By Proposition 2.8, $1 - \zeta_n$ is a unit. Then

$$\psi(1-\zeta_n) = \frac{1-\zeta_n}{1-\overline{\zeta_n}} = \frac{\zeta_n(\overline{\zeta_n}-1)}{1-\overline{\zeta_n}} = -\zeta_n$$

Suppose $-\zeta_n \in W^2$. Then $-\zeta_n = (\pm\zeta_n^r)^2 = \zeta_n^{2r}$, so $-1 = \zeta_n^{2r-1}$. Clearly n is even, otherwise -1 would not be a power of ζ_n, so $n \equiv 0 \pmod 4$. Since $-1 = \zeta_n^{n/2}$, we have $n/2 \equiv 2r-1 \pmod n$, therefore $n/2 \equiv -1 \pmod 2$, which is impossible. It follows that $-\zeta_n \notin W^2$, so $Q = 2$. This completes the proof. □

Lemma 2.17. *Let $\epsilon_1, \dots, \epsilon_r$ be independent units of a number field K which generate a subgroup A of the units of K modulo roots of unity, and let $\eta_1, \dots, \eta_r$ generate a subgroup B. If $A \subset B$ is of finite index then*

$$[B : A] = \frac{R_K(\epsilon_1, \dots, \epsilon_r)}{R_K(\eta_1, \dots, \eta_r)}$$

Proof. We may write

$$\epsilon_i = \left(\prod_{l=1}^{r} \eta_l^{a_{il}}\right) \cdot (\text{root of unity}), \text{ with } a_i l \in \mathbb{Z}$$

Therefore

$$\delta_j \log|\epsilon_i^{\sigma_j}| = \sum_{l=1}^{r} a_{il}\delta_j \log|\eta_l^{\sigma_j}|$$

Consequently as matrix multiplication (the subscripts under the lines just mean we are working with matrices)

$$(\delta_j \log|\epsilon_i^{\sigma_j}|) = \underset{1\le i,j\le r}{(a_{il})}\ (\delta_j \log|\eta_i^{\sigma_j}|)$$
$$R(\epsilon_1, \dots, \epsilon_r) = |det\ \underset{1\le i,j\le r}{(a_{il})}\ |R(\eta_1, \dots, \eta_r)$$

Since $A \subset B$ are free modules over $\mathbb{Z}$, a PID, by Drapal [6, I.6.3] there exist bases $x_1, \dots, x_r$ of A, $y_1, \dots, y_r$ of B with $x_i = y_i^{d_i}$, which implies $\log|x_i| = |d_i| \log|y_i|$. Therefore $[B : A] = |\prod_{i=1}^r d_i|$. Consider the $r \times r$ integral matrices (of the exponents) M, N corresponding to the change of bases from $\eta_1, \dots, \eta_r$ to $y_1, \dots, y_r$, $x_1, \dots, x_r$ to $\epsilon_1, \dots, \epsilon_r$. These matrices have determinant ± 1 because they have integral inverses. Moreover

$$|det\ \underset{1\le i,j\le r}{(a_{il})}\ | = |det(N\ \underset{1\le i,j\le r}{(a_{il})}\ M)| = |det(\text{dial}(d_1, \dots, d_r))| = [B : A]$$

This completes the proof of the lemma. □

Theorem 2.18. *Let K be a CM-field and K^+ its maximal real subfield. Then*

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q}2^r, \text{ where } r = \frac{1}{2}deg(K/\mathbb{Q}) - 1$$

Proof. Since K is CM-field, thus by definition a totally imaginary field, so $r_1 = 0, r_2 = \deg(K/\mathbb{Q})$ and $r = \frac{1}{2}\deg(K/\mathbb{Q}) - 1$ is by Dirichlet unit theorem (Milne [3, Theorem 5.1]) indeed the rank of the free abelian group of units in K modulo roots of unity. Let $\epsilon_1, \ldots, \epsilon_r$ be a basis of for the group of units of K^+ modulo roots of unity, then

$$R_K(\epsilon_1, \ldots, \epsilon_r) = 2^r R_{K^+1}(\epsilon_1, \ldots, \epsilon_r)$$

Since in the definition of the regulator each $\delta_i = 1$ for K^+, a totally real field, and each $\delta_i = 2$ for K, a totally imaginary field. On the other hand by Theorem 2.15 $\epsilon_1, \ldots, \epsilon_r$ form a basis for a subgroup of index Q in the units of K modulo roots of unity. Therefore by Lemma 2.17

$$QR_K = R_K(\epsilon_1, \ldots, \epsilon_r = 2^r R_{K^+}(\epsilon_1, \ldots, \epsilon_r) = 2^r R_{K^+}$$

and the conclusion follows. □

Theorem 2.19. *Let K be a CM-field, X its associated group of Dirichlet characters then*

$$\prod_{\chi \in X} \tau(\chi) = \begin{cases} \sqrt{|d(K)|}, & \text{if } K \text{ is totally real} \\ i^{deg(K/\mathbb{Q})/2}\sqrt{|d(K)|}, & \text{if } K \text{ is complex} \end{cases}$$

For proof see Washington [1, Corollary 4.6].

Theorem 2.20.

$$L(1, \chi) = \pi i \frac{\tau(\chi)}{f} B_{1,\bar{\chi}} = \pi i \frac{\tau(\chi)}{f} \frac{1}{f} \sum_{a=1}^{f} \bar{\chi}(a)a \text{ if } \chi(-1) = -1$$

Theorem 2.21. *Let K be a CM-field, X its associated group of Dirichlet characters and h^- the relative class number. Then*

$$h^-(K) = Qw \prod_{\chi \text{ odd}} (-\frac{1}{2}B_{1,\chi}).$$

Proof. Let X be the group of Dirichlet characters and K the associated field. We assume K is totally complex, so half of the characters in X are odd and half are even. Let $n = \deg(K/\mathbb{Q})$. Then by class number formula:

$$\frac{2^{n/2}h(K^+)R_{K^+}}{2\sqrt{|d(K^+)|}} = \prod_{\substack{\chi \in X \\ \chi \text{ even} \\ \chi \neq 1}} L(1, \chi),$$

and

$$\frac{(2\pi)^{n/2}h(K)R_K}{2\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi),$$

Dividing, we obtain

$$\frac{\pi^{n/2}h^-(K)2^{n/2}}{Qw\sqrt{|d(K)/d(K^+)|}} = \prod_{\chi \text{ odd}} L(1,\chi)$$

Now $L(1,\chi) = (\pi i\tau(\chi)/f_\chi)B_{1,\bar{\chi}}$ for χ odd thanks to Theorem 2.20, and by the Conductor-discriminant formula 1.34 $\sqrt{|d(K)/d(K^+)|} = (\prod_{\chi \text{ odd}} f_\chi)^{1/2}$. Also by Theorem 2.19

$$\prod_{\chi \text{ odd}} \tau(\chi) = i^{n/2}\sqrt{|d(K)/d(K^+)}.$$

Putting everything together, we obtain the desired result

$$h^-(K) = Qw \prod_{\chi \text{ odd}} (-\frac{1}{2}B_{1,\chi}).$$

□

3. p-adic L-functions

3.1 p-adic analysis

Definition 3.1. An absolute value or (multiplicative) valuation on a field K is a function $|\cdot| : K \to \mathbb{R}$ such that

1. $|x| > 0$ except that $|0| = 0$
2. $|x||y| = |xy|$
3. $|x + y| \leq |x| + |y|$

If the third condition is strengthened to $|x+y| \leq \max\{|x|, |y|\}$, then $|\cdot|$ is called a nonarchimedean absolute value.

Example. For any prime number p, we have the p-adic absolute value on $\mathbb{Q}$. Let $e \in mathbbR^+, a/b = r \in \mathbb{Q}$, where $a, b \in \mathbb{Z}, b \neq 0$. Then

$$|r|_p = \left(\frac{1}{e}\right)^{\mathrm{ord}_p(r)} = \left(\frac{1}{e}\right)^{\mathrm{ord}_p(a)-\mathrm{ord}_p(b)}$$

Normally we normalize this by taking $e = p$, thus in this chapter we will denote

$$|r|_p = \left(\frac{1}{p}\right)^{\mathrm{ord}_p(r)}$$

Similarly, for any prime ideal $\mathfrak{P}$ in a number field K, we have a normalized $\mathfrak{P}$-adic absolute value

$$|\mathfrak{a}| = \left(\frac{1}{N\mathfrak{P}}\right)^{\mathrm{ord}_{\mathfrak{P}}(\mathfrak{a})}$$

Definition 3.2. Let K be a field with a nontrivial absolute value. A sequence $(a_n)_{n=0}^{\infty}$ of elements in K is called a Cauchy sequence if, for every $\epsilon > 0$, there is an N such that

$$|a_n - a_m| < \epsilon, \forall m, n > N$$

The field K is said to be complete if every Cauchy sequence has a limit in K. (The limit is necessarily unique.)

Theorem 3.3. *Let K be a field with an absolute value $|\,|$. Then there exists a complete valued field $(\widehat{K}, |\,|)$ and a homomorphism $K \to \widehat{K}$ preserving the absolute value that is universal in the following sense: every homomorphism $K \to L$ from K into a complete valued field $(L, |\,|)$ preserving the absolute value, extends uniquely to a homomorphism $\widehat{K} \to L$.*

For proof see Mile [3] Theorem 7.23.

Example. For $K = \mathbb{Q}$ and absolute value $|\,|_p$ we denote the completion by $\mathbb{Q}_p$.

Definition 3.4. Define

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

to be the unit disk of $\mathbb{Q}_p$. It is easy to show that Z_p is a ring which contains a unique maximal ideal

$$\mathfrak{m} = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$$

Definition 3.5. Let $\overline{\mathbb{Q}_p}$ denote the algebraic closure of $\mathbb{Q}_p$. By Milne [3] Corollary 7.40. the absolute value $|\,|_p$ on $\mathbb{Q}_p$ can be uniquely extended to $|\,|_p$ on $\overline{\mathbb{Q}_p}$. By Washington [1] Proposition 5.1. $\overline{\mathbb{Q}_p}$ is not complete. Let $\mathbb{C}_p$ be its completion. Fortunately $\mathbb{C}_p$ is algebraically closed, which we will prove below.

From now on unless stated otherwise we will only work with the absolute value $|\,|_p$, so we will omit the subscript.

Lemma 3.6 (Krasner)**.** *Suppose K is a complete field with respect to a non-archimedean valuation. Let $\alpha, \beta \in \overline{K}$, the algebraic closure of K, with α separable over $K(\beta)$. Finally, suppose that for all conjugates $\alpha_i \neq \alpha$ of α we have:*

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

Then $K(\alpha) \subset K(\beta)$. In other words, if β is sufficiently close to α then $\alpha \in K(\beta)$ (here we use the extension of the absolute value from K to $\overline{K}$, such an extension exists and is unique from Milne [3] Corollary 7.40).

Proof. Consider the extension $K(\alpha, \beta)/K(\beta)$ and let $L/K(\beta)$ be the Galois closure. Let $\sigma \in \mathrm{Gal}(L/K(\beta))$. If $|\cdot|$ is an absolute value on L, then $|\sigma(\cdot)|$ is also an absolute value because

1. $|\sigma(0)| = |0| = 0$ and if $x \in L/\{0\}$ then $\sigma(x) \neq 0, |\sigma(x)| \neq 0$
2. $|\sigma(xy)| = |\sigma(x)\sigma(y)| = |\sigma(x)||\sigma(y)|$
3. $|\sigma(x+y)| = |\sigma(x) + \sigma(y)| \leq |\sigma(x)| + |\sigma(y)|$

By Milne [3] Theorem 7.38 the extension of the absolute value on L is unique, hence $|\sigma(x)| = |x| \,\forall x \in L$. Then

$$|\beta - \sigma(\alpha)| = |\sigma(\beta) - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha| < |\alpha_1 - \alpha|$$

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

$$|\alpha - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\}|\alpha_1 - \alpha|$$

It follows that $\sigma(\alpha) = \alpha_i$ for all conjugates α_i of α, so $\alpha = \sigma(\alpha)$, which means α is fixed by all $\sigma \in \mathrm{Gal}(L/K(\beta))$, hence $\alpha \in K(\beta)$. □

Theorem 3.7. *$\mathbb{C}_p$ is algebraically closed.*

Proof. Suppose $\alpha \neq 0$ is algebraic over $\mathbb{C}_p$ and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be its irreducible 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 coefficient b_i are close to those a_i of $f(x)$ such that $g(\alpha)$ is arbitrarily small.

$$|g(\alpha)| = |g(\alpha) - f(\alpha)| = \left|\sum_{i=0}^{n}(b_i - a_i)\alpha^i\right| \leq \max_{0\leq i\leq n}\left\{\left|(b_i - a_i)\alpha^i\right|\right\}$$

Suppose $\beta_1, \ldots, \beta_n$ are roots of $g(x)$. They lie in $\overline{\mathbb{Q}_p} \subset \mathbb{C}_p$. Then

$$g(\alpha) = \prod_{i=1}^{n}(\alpha - \beta_i)$$

We see that $|\alpha - \beta|$ is small for some root β of $g(x)$. In particular, we can choose $g(x)$ and then β so that $|\beta - \alpha| < |\alpha_i - \alpha|$, where α_i's are the conjugates of α. By Lemma 3.6 $\alpha \in \mathbb{C}_p(\beta) = \mathbb{C}_p$. The proof is complete. □

From now on unless otherwise stated we shall be working in $\mathbb{C}_p$, which may be regarded as the p-adic analogue of the complex numbers. We next introduce the p-adic exponential and logarithm functions. The following results of infinite sequences are easy to prove or they can be found in Conrad [9].

Theorem 3.8. *Let $(x_n)_{n=1}^{\infty}$ an infinite sequence in $\mathbb{C}_p$, then*

$$\sum_{n=1}^{\infty} x_n \text{ converges } \Leftrightarrow \lim_{n\to\infty} x_n = 0$$

Theorem 3.9. *Let $\sum_{n=1}^{\infty} x_n$ converges then*

$$\left|\sum_{n=0}^{\infty} x_n\right| \leq \max_{0\leq n} |a_n|$$

Theorem 3.10. *Let $\sum_{n=1}^{\infty} x_n$ converges then there exist $m_0 \in \mathbb{N}$ such that for all $m \geq m_0$ we have*

$$\left|\sum_{n=0}^{\infty} x_n\right| = \left|\sum_{n=0}^{m} x_n\right|$$

Definition 3.11. The exponential function is defined by the power series

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

By Theorem 3.8 this series converges if and only if $x^n/n! \to 0$ for $n \to \infty$. Since from 1 to n there are $\lfloor n/p \rfloor$ multiples of p, $\lfloor n/p^2 \rfloor$ multiples of p^2 and so on, we can see that

$$\mathrm{ord}_p(n!) = \sum_{i=0}^{\infty} \lfloor \frac{n}{p^i} \rfloor$$

Note that the sum is finite because for $p^i > n$ we have $\lfloor \frac{n}{p^i} \rfloor = 0$. Suppose $p^a \leq n \leq p^{a+1}$. Now we can estimate the value of $\mathrm{ord}_p(n!)$

$$\mathrm{ord}_p(n!) \leq \sum_{i=0}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}$$

$$\mathrm{ord}_p(n!) = \sum_{i=0}^{a} \lfloor \frac{n}{p^i} \rfloor \geq \sum_{i=0}^{a} \left(\frac{n}{p^i} - 1 \right) = \frac{n(1-p^{-a}}{p-1} - a > \frac{n-p}{p-1} - \frac{\log n}{\log p}$$

Therefore

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} \leq \mathrm{ord}_p(n!) \leq \frac{n}{p-1}$$

It follows that $|x^n/n!| \to 0$ as $n \to \infty$ if $|x| < p^{-1/(p-1)}$ and $|x^n/n| \to \infty$ if $|x| > p^{-1/(p-1)}$. Therefore $\exp(x)$ has radius of convergence $p^{-1/(p-1)}$.

Definition 3.12. The logarithm function is defined by the power series

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

Since the exponent of p in n is at most $\log n / \log p$, we find that the series has radius of convergence 1.

Theorem 3.13. *There exists a unique extension of log_p to all of $\mathbb{C}_p^\times$ such that $log_p(p) = 0$ and $log_p(xy) = log_p(x) + log_p(y)$ for all $x, y \in \mathbb{C}_p^\times$.*

Proof. $\mathbb{C}_p$ contains the algebraic closure of $\mathbb{Q}_p$, hence also the algebraic closure of $\mathbb{Q}$. Consider $\mathbb{Q} \subset \mathbb{C}$. The algebraic closure of $\mathbb{Q}$ is unique up to an isomorphism that fixes every element of $\mathbb{Q}$, thus we can embed $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$. For each rational number r define the power p^r of p to be the positive real r-th power of p in $\mathbb{Q}$. This choice ensures $p^r p^s = p^{r+s}$ for all rational numbers r, s. Denote by $p^{\mathbb{Q}}$ the set of p^r, $r \in \mathbb{Q}$.

Let $\alpha \in \mathbb{C}_p^\times$. $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$, so we can choose $\alpha_1 \in \overline{\mathbb{Q}_p}$ such that $|\alpha_1 - \alpha| < |\alpha|$, which gives us the following equality:

$$|\alpha_1| = |\alpha_1 - \alpha + \alpha| = \max(|\alpha_1 - \alpha|, |\alpha|) = |\alpha|$$

By Milne [3] Theorem 7.38 we have $|\alpha_1| = (p^{1/e})^n$ for some integer n where e is the ramification index of $\mathbb{Q}_p(\alpha_1)/\mathbb{Q}_p$. Therefore $|\alpha| = p^r$ for some $r \in \mathbb{Q}$ and $|\alpha p^{-r}| = 1$.

Now suppose $\alpha p^{-r} = \beta \in \mathbb{C}_p^\times, |\beta| = 1$. Choose $\beta_1 \in \overline{\mathbb{Q}_p}$ such that $|\beta_1 - \beta| < 1$, then $|\beta_1 - \beta| < |\beta|$, thus:

$$|\beta_1| = |\beta_1 - \beta + \beta| = \max(|\beta_1 - \beta|, |\beta|) = |\beta| = 1$$

so β_1 is a unit of the finite extension $\mathbb{Q}_p(\beta_1)/\mathbb{Q}_p$. Let $\mathcal{O}$ be the integral closure of Z_p in $\mathbb{Q}_p(\beta_1)$. According to Milne [3] Theorem 7.38 there is a unique prime ideal $\mathfrak{P} \subset \mathcal{O}$ lying above p which is the local uniformizing parameter of the extended absolute value on $\mathbb{Q}_p(\beta_1)$. The residue field $\mathcal{O}/\mathfrak{P}$ has characteristics p and p^f elements, where f is the residue class degree. The equivalence class of β_1 in $\mathcal{O}/\mathfrak{P}$ is a nonzero element because $|\beta_1| = 1$, so $\beta_1 \notin \mathfrak{P}$. Then β_1 is a root of the equation $x^{p^n-1} - 1 = 0$ in $\mathcal{O}/\mathfrak{P}$. The exponent $p^n - 1$ is coprime to p, so β_1 is a single root and via Hensel's lemma there is a (p^n-1)-th root of unity ω in $\mathcal{O}$ such that $\omega \equiv \beta_1 \pmod{\mathfrak{P}}$. It follows that $|\beta_1 - \omega| < 1$ and

$$|\beta\omega^{-1} - 1| = |\beta - \omega| = |\beta - \beta_1 + \beta_1 - \omega| \leq \max(|\beta - \beta_1|, |\beta_1 - \omega|) < 1$$

Since p^n-1 is coprime to p such roots of unity are distinct modulo $\mathfrak{P}$, therefore the choice of ω is unique. Let W denote the group of all roots of unity of order prime to p in $\mathbb{C}_p^\times$. From the decomposition $\alpha = p^r \times \omega \times \beta\omega^{-1}$. We have proved that:

$$\mathbb{C}_p^\times = p^{\mathbb{Q}} \times W \times U_1$$

where

$$U_1 = \{x \in \mathbb{C}_p \mid |x-1| < 1\}$$

Now let $\alpha = p^r\omega x, x \in U_1$. Define $\log_p \alpha = \log_p x$. Since $x \in U_1$, $\log_p x$ is defined by the power series. Clearly this extension satisfies the desired properties.

Suppose $f(\alpha)$ gives another extension. We have $f(1) = f(1) + f(1)$, thus $f(1) = 0$. If $\omega^N = 1$ then

$$\begin{aligned} f(\alpha) = \frac{1}{N} f(\alpha^N) = \frac{1}{N}(f(p^{rN}) + f(1) + f(x^N)) = \\ = \frac{1}{N}(0 + 0 + Nf(x)) = f(x) = \log_p x \end{aligned}$$

Therefore the extension is unique. This completes the proof of the proposition. □

Lemma 3.14. *If $|x| < p^{-1/(p-1)}$ then $|\log_p(1+x)| = |x|$ and if $|x| \leq p^{-1/(p-1)}$ then $|log_p(1+x)| \leq |x|$.*

Proof. If $n \in \mathbb{N}, n < p$ then $|n| = 1$, and in general $|n| = 1/p^{v_p(n)} \geq 1/n$. Therefore, if $|x| < p^{-1/(p-1)} < 1$ we have

$$\left|\frac{x^n}{n}\right| = |x|^{n-1} \cdot |x| < |x| \text{ if } 2 \leq n < p$$

and

$$\left|\frac{x^n}{n}\right| < np^{(1-n)/(p-1)}|x| \leq |x| \text{ if } n \geq p$$

since $np^{(1-n)/(p-1)} = 1$ for $n = p$ and $np^{(1-n)/(p-1)}$ is decreasing for $n \geq p$. Therefore

$$\left|\sum_{n=2}^{\infty} \frac{(-1)^{n+1}x^n}{n}\right| \leq \max_{2\leq n} \left|\frac{x^n}{n}\right| < |x|$$

hence

$$|\log_p(1+x)| = \left|x + \sum_{n=2}^{\infty} \frac{(-1)^{n+1}x^n}{n}\right| = |x|$$

For the second part note that in this case the equalities are not strict and the conclusion follows similarly. This completes the proof. □

Theorem 3.15. $\log_p x = 0 \Leftrightarrow$ *x is a rational power of p times a root of unity (of arbitrary order).*

Proof. Suppose $x = p^r\omega$, where $r \in \mathbb{Q}$ and $\omega \in W$. Choose $N \in \mathbb{N}$ such that $Nr \in \mathbb{N}$ and $\omega^N = 1$. Then

$$\log_p x = \frac{1}{N}(\log_p p^{rN} + \log_p \omega^N) = \frac{1}{N}(0+0) = 0$$

Conversely, suppose $\log_p x = 0$. Since $\mathbb{C}_p^\times = p^{\mathbb{Q}} \times W \times U_1$ from Theorem 3.13 and the first two components are nullified by $\log_p$, we may assume $x = 1+y$ with $|y| < 1$. Let $N \in \mathbb{N}$ be large enough that $|y^{p^N}| < p^{-1/(p-1)}$. Then

$$x^{p^N} = (1+y)^{p^N} = 1 + p^N y + \cdots + \binom{p^N}{j} y^j + \cdots + y^{p^N}.$$

From Legendre's formula we can easily prove $p|\binom{p^N}{j}$, thus all the middle terms have absolute value at most $|py| < |p| \leq p^{-1/(p-1)}$, and by the choice of N we have $|y^{p^N}| < p^{-1/(p-1)}$. Therefore $|x^{p^N} - 1| < p^{-1/(p-1)}$ and from Lemma 3.14

$$|x^{p^N} - 1| = |\log_p(x^{p^N} - 1 + 1)| = |\log_p(x^{p^N})| = 0$$

Therefore x is a p^N-th root of unity. This completes the proof. □

Theorem 3.16. *If $|x| < p^{-1/(p-1)}$ then*

$$\log_p \exp(x) = x$$

and

$$\exp \log_p(1+x) = 1 + x$$

Proof. Both are formal power series identities, so we need only check convergence. $\exp(x)$ converges for $|x| < p^{-1/(p-1)}$, so it remains to show that $|\exp(x) - 1| < 1$. Because $v_p(n!) < n/(p-1)$ we have $|n!| > p^{-n/(p-1)}$, thus

$$\left|\frac{x^n}{n!}\right| < |x|^n p^{\frac{n}{p-1}} < p^{\frac{-n}{p-1} + \frac{n}{p-1}} = 1$$

If $|\exp(x) - 1| = 0$ then $|\exp(x) - 1| < 1$ holds trivially, because from Theorem 3.10 there exists $k \in \mathbb{N}$ such that

$$|\exp(x) - 1| = \left|\sum_{n=1}^{k} \frac{x^n}{n!}\right| \leq \max_{1 \leq n \leq k} \left|\frac{x^n}{n!}\right| < 1$$

so $\log_p \exp(x)$ converges. For the second identity $|x| < p^{-1/(p-1)} < 1$, so $\log_p(1+x)$ converges and we still need to check $|\log_p(1+x)| < p^{-1/(p-1)}$, which follows from Lemma 3.14. □

Lemma 3.17. *Let $P_i(x) = \sum_{n=0}^{\infty} a_{n,i} x^n, i = 0, 1, 2 \ldots$ be a sequence of power series which converge in a fixed subset D of $\mathbb{C}_p$ and suppose:*

i $a_{n,i} \to a_{n,0}$ as $i \to \infty$ for each n, and

ii $\forall x \in D$ and $\forall \epsilon > 0$ there exists an n_0 such that $|\sum_{n \geq n_0}^{\infty} a_{n,i} x^n| < \epsilon$ uniformly in $i (= 0, 1, 2, \ldots)$.

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

Proof. Given ϵ and x choose n_0 as above. For each $n < n_0$ there exists $j_n \in \mathbb{N}$ such that $|a_{n,0} - a_{n,i}||x^n| < \epsilon, \forall i \geq j_n$. Let $j = \max_{1 \leq n < n_0}\{j_n\}$ then $\forall i \geq j$:

$$\begin{aligned} |P_0(x) - P_i(x)| &= \left| \sum_{1 \leq n < n_0} (a_{n,0} - a_{n,i}) x^n + \sum_{n \geq n_0} a_{n,0} x^n - \sum_{n \geq n_0} a_{n,i} x^n \right| \\ &\leq \max_{n < n_0}\{|a_{n,0} - a_{n,i}||x^n|, |\sum_{n \geq n_0} a_{n,0} x^n|, |\sum_{n \geq n_0} a_{n,i} x^n|\} < \epsilon \end{aligned}$$

□

Theorem 3.18. *Suppose $r < p^{-1/(p-1)} < 1$ and*

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

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

Proof. Let

$$P_i(x) = \sum_{n \leq i} a_n \binom{x}{n} = \sum_{n \leq i} a_{n,i} x^n,\ i = 1, 2, 3, \ldots$$

Then

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

so

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

Also

$$|a_{n,i} - a_{n,i+k}| = \left| a_{i+1} \frac{\text{integer}}{(i+1)!} + \cdots + a_{i+k} \frac{\text{integer}}{(i+k)!} \right| \leq MR^{-(i+1)} \to 0 \text{ as } i \to \infty$$

Therefore $\{a_{n,i}\}_{i=1}^{\infty}$ is a Cauchy sequence. Let $a_{n,0} = \lim_{i \to \infty} a_{n,i}$. Then $|a_{n,0}| \leq MR^{-n}$. Let $P_0(x) = \sum_{n=0}^{\infty} a_{n,0} x^n$, so P_0 converges in $D = \{x \in \mathbb{C}_p \mid |x| < R$, because:

$$|a_{n,0} x^n| \leq M \left(\frac{|x|}{R} \right)^n \to 0 \text{ as } n \to \infty$$

The polynomials $P_1, P_2, \ldots$ of course also converge in D. Finally, if $x \in D$ then

$$\left| \sum_{n \geq n_0} a_{n,i} x^n \right| \leq \max_{n \geq n_0} \{ MR^{-n} |x|^n \} \to 0 \text{ as } n_0 \to \infty$$

uniformly in i. Therefore $\lim_{i \to \infty} P_i(x) = P_0(x)$ by Theorem 3.17, so $f(x)$ can be expressed as a power series, hence analytic. □

Theorem 3.19 (von Staudt-Clausen)**.** *Let n be even and positive. Then*

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z}$$

where the sum is over those primes p such that $p - 1$ divides n. Consequently pB_n is p-integral, i.e. lies in $\mathbb{Z}_p$ for all p.

Proof. We will use mathematical induction. The base case $B_2 = \frac{1}{6}$ can be verified manually . We assume that the statement true for all even $m < n$ and $n > 2$ is even. In particular $pB_m \in \mathbb{Z}_{\text{ı}}$ for all $m < n$ because if m is even then the statement

follows from the assumption, otherwise $B_0 = 1, B_1 = -1/2$ and $B_m = 0$ for odd $m \geq 3$. From Theorem 2.4 with $\chi = 1$, hence f_χ, and $F = p$ we have

$$\begin{aligned} B_n = B_{n,1} &= p^{n-1} \sum_{a=1}^{p} B_n\left(\frac{a}{p}\right) \overset{\text{Lemma 2.3}}{=} \\ &= p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} \left(\frac{a}{p}\right)^{n-j} (B_j) = \\ &= \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (pB_j) a^{n-j} p^{j-2} \equiv \\ &\equiv \sum_{a=1}^{p} (pB_0) a^n p^{-2} + n(pB_1) a^{n-1} p^{-1} + (pB_n) p^{n-2} \pmod{\mathbb{Z}_p} \end{aligned}$$

where the last congruence holds because $(pB_j)a^{n-j}p^{j-2}$ is p-integral for $2 \leq j \leq n$ from the induction assumption. Since $B_1 = -\frac{1}{2}$ we have $p \neq 2 \Rightarrow B_1 \in \mathbb{Z}_p$. If $p = 2$, then since n is even, $nB_1 \in \mathbb{Z}_2$, therefore we may omit the term with B_1. Using $B_0 = 1$ we obtain:

$$B_n = \sum_{a=1}^{p} (pB_0) a^n p^{-2} + (pB_n) p^{n-2} \equiv p^n B_n + \frac{1}{p} \sum_{a=1}^{p} a^n \pmod{\mathbb{Z}_p}$$

$$(1 - p^n) B_n \equiv \frac{1}{p} \sum_{a=1}^{p} a^n \pmod{\mathbb{Z}_p}$$

Now if $(p-1) \mid n$ then $a^n \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$ from Fermat's Little Theorem, thus:

$$(1 - p^n) B_n \equiv \frac{p-1}{p} \pmod{\mathbb{Z}_p}$$

Since $1 - p^n$ is a unit in Z_p whose inverse is congruent to $1 \pmod{p}$ we have $B_n \equiv -\frac{1}{p} \pmod{\mathbb{Z}_p}$.

For the second case $p - 1 \nmid n$ consider a primitive root g modulo p, i.e. $p-1$ is the smallest positive integer such that $g^{p-1} \equiv 1 \pmod{p}$, then $g^0, g^1, \ldots, g^{p-2}$ is a complete nonzero residue class modulo p

$$\sum_{a=1}^{p} a^n \equiv \sum_{a=1}^{p-1} a^n \equiv \sum_{k=0}^{p-2} g^{kn} \equiv \frac{g^{(p-1)n} - 1}{g^n - 1} \pmod{p}$$

Note that $g^{(p-1)n} - 1 \equiv 0 \pmod{p}$ and $g^n - 1 \not\equiv 0 \pmod{p}$, since g is a primitive root and $p - 1 \nmid n$. Hence $B_n \in \mathbb{Z}_p$ for $p - 1 \nmid n$.

Now consider $B_n + \sum_{p-1|n} \frac{1}{p}$. By the above, this is in $\mathbb{Z}_p$ for every p, so there are no primes in the denominator. Therefore it must be an integer. □

3.2 p-adic L-function

Definition 3.20. Let $q = p$, if $p \neq 2$ and $q = 4$, if $p = 2$. Given $a \in \mathbb{Z}_p, p \nmid a$, there exists a unique $\phi(q)$-th root of unity $\omega(a) \in \mathbb{Z}_p$ such that

$$a \equiv \omega(a) \pmod{q}$$

and let

$$\langle a\rangle = \omega(a)^{-1}a$$

The function ω is also called Teichmüller character. We may define

$$\langle a\rangle^x = \exp(x\log_p\langle a\rangle)$$

Since $|\log_p\langle a\rangle|| \le |a-1| \le |q| = 1/q$ by Lemma 3.14, this converges if $|x| < qp^{-1/(p-1)}$

Remark. We define q differently for $p=2$, because if $q=2$ then $|2|_2$ would not be strictly less than $2^{-1/(2-1)}$ the convergence radius of $\exp(x)$ and the functions $\langle a\rangle^x$ would not have nice properties.

Then let's define the following function

$$H(s,a,F) = \sum_{\substack{m\equiv a \pmod F \\ m>0}} m^{-s} = \sum_{n=0}^{\infty}\frac{1}{(a+nF)^s} = F^{-s}\zeta\left(s,\frac{a}{F}\right)$$

where s is a complex variable, a and F are integers with $0<a<F$, and $\zeta(s,b)$ is the Hurwitz zeta function defined in the previous chapter. The Hurwitz zeta function can be analytically extended to the whole complex plane except at a simple pole $s=1$. Then:

$$H(1-n,a,F) \overset{\text{Theorem2.5}}{=} -\frac{F^{n-1}B_n(a/F)}{n} \in \mathbb{Q} \text{ for } n\in\mathbb{N}$$

Now we will define the p-adic analogue of $H(s,a,F)$.

Theorem 3.21. *Suppose $q \mid F$ and $p \nmid a$ (a and F as above). Then there exists a p-adic meromorphic function $H_p(s,a,F)$ on*

$$\{s\in\mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$$

such that

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F), \forall n\in\mathbb{N}$$

In particular, when $n\equiv 0 \pmod{p-1}$ if p is odd, or $\pmod 2$ if $p=2$, then $\omega^{-n}=1$ and

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

The function H_p is analytic in s except for a simple pole at $s=1$ with residue $\frac{1}{F}$.

Proof. Let

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

Assume convergence for the moment. Let $s=1-n, n\in\mathbb{N}$, note that $\binom{n}{j}$ is 0 for $j>n$. Then

$$\begin{aligned}
H_p(1-n,a,F) &= \frac{-1}{nF}\langle a\rangle^n\sum_{j=0}^{n}\binom{n}{j}\left(\frac{F}{a}\right)^j(B_j)\\
&= -\frac{F^n\langle a\rangle^n a^{-n}}{Fn}\sum_{j=0}^{n}\binom{n}{j}\left(\frac{a}{F}\right)^{n-j}(B_j)\\
&\overset{\text{Lemma2.3}}{=} -\frac{F^{n-1}\omega^{-n}(a)}{n}B_n\left(\frac{a}{F}\right)\\
&= \omega^{-n}H(1-n,a,F), \text{ as desired}
\end{aligned}$$

At $s = 1$, we have residue (note that $\binom{0}{0} = 1$)

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

It remains to prove the convergence. By von Staudt-Clausen Theorem 3.19 we have $|B_j| \leq p$, thus combined with $q \mid F, p \nmid a$ we obtain $|(F/a)^j B_j| \leq p|q|^j$. Therefore, by Theorem 3.18 with $x = 1 - s$, $r = |q| = \frac{1}{q}$, thus $R = qp^{-1/(p-1)}$, we find that

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

is analytic on $D = \{s \in \mathbb{C}_p \mid |1-s| < qp^{-1/(p-1)}\}$. Similarly $\langle a\rangle^{1-s}$ is also analytic on D. We will prove that D is the same set as $D' = \{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$. Put $u = qp^{-1/(p-1)}$, since $u > 1$ we obtain

$$|s| < u \Rightarrow |1 - s| \leq \max\{|1|, |s|\} < u$$

Thus $D' \subset D$ and similarly $D \subset D'$. This completes the proof. □

Let χ be a p-adic Dirichlet character, i.e. with the codomain $\mathbb{C}_p$. For a given order the group of characters is still the same as with the codomain $\mathbb{C}$, since the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}_p$ is isomorphic to the usual algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Also, observe that $\omega(a)$ is a p-adic Dirichlet character of conductor q and order $\phi(q)$.

Theorem 3.22. *Let χ be a Dirichlet character of conductor f and let F be any multiple of q and f. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ such that*

$$L_p(1 - n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \forall n \in \mathbb{N}$$

If $\chi = 1$ then $L_p(s, 1)$ is analytic except for a simple pole at $s = 1$ with residue $(1 - 1/p)$. In fact, we have the formula:

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

Proof. We show that the formula gives the desired function. By Theorem 3.21

$$L_p(s, \chi) = \sum_{a=1, p\nmid a}^{F} \chi(a) H_p(s, a, F)$$

Each $H_p(s, a, F)$ is analytic except at $s = 1$, where it has the residue $1/F$ so the residue of $L_p(s, \chi)$ at $s = 1$ is $\sum_{a=1, p\nmid a}^{F} \chi(a)(1/F)$. If $\chi = 1$ then since $q|F$ we have $p|F$, hence the number of multiples of p from 1 to F is exactly F/p and the sum is equal to $(1/F)(F - F/p) = 1 - 1/p$. If $\chi \neq 1$ then the sum is

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

By Lemma 1.20 the first sum is 0. If $p \mid f$ then $\chi(p) = 0$. If $p \nmid f$ then since $f|F$ we also have $f|(F/p)$, so again by Lemma 1.20 the second sum is 0. Therefore $L_p(s, \chi)$ has no pole at $s = 1$ if $\chi \neq 1$.

Note that if $p \nmid a$, then $\omega^{-n}(a) \neq 0$, hence by Lemma 1.29 $\chi(a)\omega^{-n}(a) = \chi\omega^{-n}(a)$. If $n \in \mathbb{N}$ then by Theorem 3.21 we obtain

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

By Theorem 2.4 with F and the character $\chi\omega^{-n}$ the first sum is $-B_{n,\chi\omega^{-n}}/n$. If $p \mid f_{\chi\omega^{-n}}$ then $\chi\omega^{-n}(pb) = 0$ and the whole expression $\chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}$ is also zero. Otherwise since $f_{\chi\omega^{-n}} \mid f_\chi f_{\omega^{-n}} = fp$ we have $f_{\chi\omega^{-n}} \mid f \mid F$. Again by Theorem 2.4 with F/p and character $\chi\omega^{-n}$ after factoring out $\chi(p)$ the second sum is equal to $\chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}$. Overall we get the following

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{1}{n}(B_{n,\chi\omega^{-n}} - \chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}) \\ &= -\frac{1}{n}(1 - \chi\omega^{-n}(p)p^{n-1})B_{n,\chi\omega^{-n}} \end{aligned}$$

□

Theorem 3.23. *Suppose $\chi \neq 1$ and $pq \neq f_\chi$. Then*

$$L_p(s,\chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

with $|a_0| \leq 1$ and $p|a_i$ for all $i \in \mathbb{N}$.

Proof. We may choose F as in Theorem 3.22 so that $q|F$ but $pq \nmid F$. Also we may assume χ is even since everything is 0 otherwise by Remark 2.2.
Consider $a \in \mathbb{N}$ such that $a \nmid p$. If $j \geq 6$ then by Theorem 3.19 and

$$\left|\frac{B_j}{j!}\frac{F^{j-1}}{a^j}\right| \leq p^{j/(p-1)} \cdot p \cdot \frac{1}{q^{j-1}} \leq \frac{1}{q}$$

The last inequality hold because if p is 2 then q is 4 and the total exponent of p is $j + 1 - 2(j-1) = 3 - j \leq -2$. If p is odd then $p = q$ and the total exponent of p is $j/(p-1) + 1 - (j-1) \leq j/2 - j + 2 = 2 - j/2 \leq -1$. A check of the cases

$j = 3, 4, 5$ shows that the inequality holds for $j \geq 3$. Therefore all coefficients in the power series expansion of

$$\frac{1}{F}\sum_{j\geq 3}\binom{1-s}{j}\left(\frac{F}{a}\right)(B_j)$$

are divisible by p. Now we look at the terms for $j \leq 2$ individually. If $j = 0$, then the denominator is F. If $j = 1$, then there is no denominator. Finally if $j = 2$, then the denominator is 2. Overall they can have possibly q but not pq, in the denominator. Similarly

$$\langle a\rangle^{1-s} = \exp((1-s)\log_p\langle a\rangle) = \sum_{j=0}^{\infty}\frac{1}{j!}(1-s)^j(\log_p\langle a\rangle)^j$$

Since $|\langle a\rangle - 1| \leq 1/q < p^{-1/(p-1)}$ by Lemma 3.14 we obtain $|\log_p\langle a\rangle| = |\langle a\rangle - 1| \leq 1/q$, thus

$$\left|\frac{(\log_p\langle a\rangle)^j}{j!}\right| \leq \frac{1}{q^j}\cdot p^{j/(p-1)}$$

If $p = 2$ then the total exponent of p is $j - 2j = -j$. If p is odd then the total exponent of p is $j/(p-1) - j \leq j/2 - j = -j/2$, thus all the coefficients are in $\mathbb{Z}_p$, and they are divisible by pq for $j \geq 2$ (if $p = 3$ the bound $-3/2$ implies the bound -2 since the coefficients are in $\mathbb{Z}_p$, hence the power of p is an integer). Therefore we need only consider

$$\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)(1+(1-s)\log_p\langle a\rangle)\left(\frac{1}{F} - \frac{1-s}{2a} + \frac{(1-s)(1-s-1)F}{12a^2}\right)$$

Since the products of other terms contributes multiples of p to the coefficients of $(s-1)^j$. We find that

$$a_0 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{1}{F}\log_p\langle a\rangle - \frac{1}{2a} - \frac{F}{12a^2}\right) \pmod p$$

We already know $q \mid \log_p\langle a\rangle$ and since $pq \nmid F$ we have $(\log_p\langle a\rangle)/F$ and $F/12$ are in $\mathbb{Z}_p$. If p is odd then $1/2a$ is also in $\mathbb{Z}_p$ for $a \nmid p$. If $p = 2$ then since $a \equiv \omega(a) \pmod 4$ and $\omega^{-1}(a) \neq 0 \overset{\text{Theorem1.29}}{\Rightarrow} \chi(a)\omega^{-1}(a) = \chi\omega^{-1}(a)$ we have

$$\sum_{\substack{a=1\\ p\nmid a}}^{F}\frac{\chi(a)}{a} \equiv \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\omega^{-1}(a) \equiv \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\omega^{-1}(a) \equiv 0 \pmod q$$

The last congruence follows from the same argument we used in Theorem 3.22 and $\chi\omega^{-1} \neq 1$ because χ is an even character and ω is an odd character. This shows that $|a_0| \leq 1$. Next, we have

$$a_1 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{F}{12a^2} - \frac{\log_p\langle a\rangle}{2a} - \frac{F\log_p\langle a\rangle}{12a^2}\right) \pmod p$$

From the arguments mentioned above clearly $F \log_a \langle a \rangle / 12a^2$ and $\log_p \langle a \rangle / 2a$ are divisible by p. If $p \geq 5$ then $F/12 \in p\mathbb{Z}_p$, so $p \mid a_1$. If $p = 2$ or 3 then $F/12 \in \mathbb{Z}_p$. But $a^2 \equiv 1 \pmod{p}$ if $p \nmid a$ so by Lemma 1.20

$$\sum_{\substack{a=1 \\ p \nmid a}}^{F} \frac{\chi(a)}{a^2} \equiv \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a) \equiv 0 \pmod{p}$$

Again we have $p \mid a_1$. Finally

$$a_2 \equiv -\sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a)(\log_p \langle a \rangle) \frac{F}{12a^2} \equiv 0 \pmod{p}$$

and this completes the proof. □

Corollary 3.24. *Suppose $\chi \neq 1, pq \nmid f$. Let $m, n \in \mathbb{Z}$ (co kdyz p je 2). Then*

$$L_p(m, \chi) \equiv L_p(n, \chi) \pmod{p},$$

and both numbers are p-integral.

Proof. By Theorem 3.23 both numbers are congruent to a_0. Moreover $|a_0| \leq 1$ which implies they both belong to $\mathbb{Z}_p$. □

Corollary 3.25 (Kummer's congruences)**.** *Suppose $m \equiv n \not\equiv 0 \pmod{p-1}$ are positive even integers. Then*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}$$

More generally, if m and n are positive even integers with $m \equiv n \pmod{(p-1)p^a}$ and $n \not\equiv 0 \pmod{p-1}$, then

$$(1 - p^{m-1}) \frac{B_m}{m} \equiv (1 - p^{n-1}) \frac{B_n}{n} \pmod{p^{a+1}}$$

Proof. Since $m \equiv n \pmod{p-1}$ we have $\omega^m = \omega^n$ and $L_p(s, \omega^m) = L_p(s, \omega^n)$, thus by Theorem 3.23

$$\begin{aligned} L_p(1 - m, \omega^m) &= a_0 + a_1(-m) + a_2(-m)^2 + \ldots \equiv \\ &\equiv a_0 + a_1(-n) + a_2(-n)^2 + \ldots = \\ &= L_p(1 - n, \omega^m) = L_p(1 - n, \omega^n) \pmod{p^{a+1}} \end{aligned}$$

Finally by Theorem 3.22

$$(1 - p^{m-1}) \frac{B_m}{m} = L_p(1 - m, \omega^m) \equiv L_p(1 - n, \omega^n) \equiv (1 - p^{n-1}) \frac{B_n}{n} \pmod{p^{a+1}}$$

□

Corollary 3.26. *Suppose n is odd, $n \not\equiv -1 \pmod{p-1}$. Then*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}$$

and both sides are p-integral.

Proof. Since $n \not\equiv -1 \pmod{p-1}$ we have $\omega^{n+1} \neq 1$. Also $\omega^n(p) = 0$ since n is odd, hence not divisible by $p-1$. Therefore by Theorem 3.22 and Corollary 3.24

$$\begin{aligned} B_{1,\omega^n} =& (1-\omega^n(p))B_{1,\omega^n} = -L_p(0,\omega^{n+1}) \equiv \\ \equiv& -L_p(1-(n+1),\omega^{n+1}) = (1-p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \pmod{p} \end{aligned}$$

The p-integrality also follows from Corollary 3.24. □

Theorem 3.27. *Let p be an odd prime and let h_p^- be the relative class number of $\mathbb{Q}(\zeta_p)$. Then $p \mid h_p^- \Leftrightarrow p$ divides the numerator of B_j for some $j = 2, 4, \ldots, p-3$.*

Proof. Let ω be a generator of $Gal(\widehat{\mathbb{Q}(\zeta_p)}/\mathbb{Q}) \cong (\widehat{\mathbb{Z}/p\mathbb{Z}})^\times$. The odd characters corresponding to $\mathbb{Q}(\zeta_p)$ are $\omega, \omega^3, \ldots, \omega^{p-2}$. Therefore, by Theorem 2.21 ($Q = 1$ by Corollary 2.16, and $w = 2p$, because there are $2p$ roots of unity in $\mathbb{Q}(\zeta_p)$, indeed they are precisely $\zeta, \zeta^2, \ldots, \zeta^p, -\zeta, \ldots, -\zeta^p$)

$$h_p^- = 2p \prod_{\substack{j=1 \\ j\text{odd}}}^{p-2} \left(-\frac{1}{2}B_{1,\omega^j}\right)$$

First note that $B_1(x) = x - 1/2, \sum_{a=1}^{p-1} \omega^{-1}(a) = 0$ and by Theorem 2.4 with $n = 1, F = p$

$$\begin{aligned} B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} &= p^{1-1} \sum_{a=1}^{p} \omega^{-1}(a) B_1\left(\frac{a}{p}\right) = \\ &= \frac{1}{p}\sum_{a=1}^{p} a\omega^{-1}(a) - \frac{1}{2}\sum_{a=1}^{p-1}\omega^{-1}(a) \equiv \frac{p-1}{p} \pmod{\mathbb{Z}_p} \end{aligned}$$

Therefore $(2p)(-\frac{1}{2}B_{1,\omega^{p-2}}) \equiv 1 \pmod{p}$, so we have

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^j}\right) \pmod{p}$$

By Corollary 3.26 this may be rewritten as

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{1}{2}\frac{B_{j+1}}{j+1}\right) \pmod{p}$$

and the theorem follows immediately.

□

Corollary 3.28. *If a prime p divides the numerator of B_j for some $j = 2, 4, \ldots, p-3$. Then p is irregular.*

Bibliography

[1] L. C. Washington: *Introduction to cyclotomic fields*, GTM 83.

[2] B.Mazur: *How can we construct abelian Galois extensions of basic number fields*, Bull. Amer. Math. Soc. 48 (2011), 155-209.

[3] J. S. Milne: *Algebraic Number Theory*, `http://www.jmilne.org/math/CourseNotes/ant.html`

[4] M. R. Murty, J. Esmonde: *Problems in Algebraic Number Theory*, GTM 190.

[5] S. Lang: *Algebraic Number Theory*, GTM 110.

[6] A. Drápal: *Komutativní okruhy*, `http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf`

[7] Paul Garrett*Analytic continuation, functional equation: examples*,

[8] Brian Osserman*The analytic class number formula 1*, `https://www.math.ucdavis.edu/~osserman/classes/254a/lectures/19.pdf`

[9] Keith Conrad*Infinite series in p-adic fields*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/infseriespadic.pdf`