THE CYCLOTOMIC ZETA FUNCTION

1. Dirichlet Characters

Let $N$ be a positive integer. A Dirichlet character modulo $N$ is defined initially as a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times.$$  

Any such character determines a least positive divisor $M$ of $N$ such that the character factors as

$$\chi = \chi_o \circ \pi_M : (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\pi_M} (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi_o} \mathbb{C}^\times.$$  

The integer $M$ is the conductor of $\chi$, and the character $\chi_o$ is primitive. Note that if $n \in \mathbb{Z}$ is not coprime to $N$ but is coprime to $M$ then $\chi_o(n + M\mathbb{Z})$ is defined and nonzero. Perhaps confusingly at first, we also use the symbol $\chi$ to denote $\chi_o$ lifted to a multiplicative function on the integers,

$$\chi : \mathbb{Z} \rightarrow \mathbb{C}, \quad \chi(n) = \begin{cases} \chi_o(n + M\mathbb{Z}) & \text{if } \gcd(n, M) = 1, \\ 0 & \text{if } \gcd(n, M) > 1. \end{cases}$$  

Thus (the lifted) $\chi(n)$ need not equal (the original) $\chi(n + N\mathbb{Z})$, and in particular $\chi(n)$ need not equal 0 even when $\gcd(n, N) > 1$.

Especially, if $N > 1$ then the trivial character $1$ modulo $N$ has conductor $M = 1$, and the trivial character $1_o$ modulo 1 is identically 1 on $(\mathbb{Z}/1\mathbb{Z})^\times = \{0\}$, and this character lifts to the constant function 1(n) = 1 for all $n \in \mathbb{Z}$, even though the original character 1 modulo $N$ is undefined on the coset $N\mathbb{Z}$ in $\mathbb{Z}/N\mathbb{Z}$.

Fix a rational prime $p$.

- Let $p^d \parallel N$ and $N_p = N/p^d$ and $e = \phi(p^d)$.
- Let $f$ denote the order of $p + N_p\mathbb{Z}$ in $(\mathbb{Z}/N_p\mathbb{Z})^\times$.
- Let $g = \phi(N_p)/f = \phi(N)/(ef)$.

Note that $N_p = N$ and $e = 1$ for all primes $p$ other than the finitely many prime divisors of $N$. For $k = 0, \ldots, f - 1$, there exist Dirichlet characters modulo $N_p$ that take $p$ to $\zeta_f^k$, where $\zeta_f = e^{2\pi i/f}$. The number of such characters is $g$, independently of $k$. Any Dirichlet character modulo $N$ that is not defined modulo $N_p$ takes $p$ to 0. That is, for $k = 0, \ldots, f - 1$, there exist $g$ Dirichlet characters modulo $N$ that take $p$ to $\zeta_f^k$, and any Dirichlet character modulo $N$ that does not take $p$ to $\zeta_f^k$ for some $k$ takes $p$ to 0.

2. Cyclotomic Arithmetic

Again let $N$ be a positive integer. Let $\zeta_N = e^{2\pi i/N}$, and consider the cyclotomic number field

$$K = \mathbb{Q}(\zeta_N).$$  

For any rational prime $p$, again let $p^d \parallel N$ and let $N_p = N/p^d$. Then $p$ factors in $\mathcal{O}_K$ as

$$p\mathcal{O}_K = (p_1 \cdots p_g)^e,$$
where all the primes lying over $p$ have

- ramification degree $e = \phi(p^d) = p^d - (p - 1)$,
- inertial degree $f = \text{ord}_p(p + N_p \mathbb{Z})$ in $(\mathbb{Z}/N_p \mathbb{Z})^\times$,
- and decomposition index $g = \phi(N_p)/f = \phi(N)/(ef)$,
- so that altogether $efg = \phi(N)$.

The rational primes that ramify are precisely the prime divisors of $N$, except that 2 does not ramify if $2 \mid N$ but $4 \nmid N$. In the exceptional case $N = 2 \mod 4$, in fact $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N/2})$, so if we avoid redundant cyclotomic extensions $\mathbb{Q}(\zeta_N)$ where $N = 2 \mod 4$ then the primes that ramify are exactly the prime divisors of $N$.

### 3. Cyclotomic Galois Theory, Briefly

The Galois group of $K = \mathbb{Q}(\zeta_N)$ over $\mathbb{Z}$ is

$$G = \{ \zeta_N \mapsto \zeta_N^a : a + NZ \in (\mathbb{Z}/N\mathbb{Z})^\times \}.$$ 

The fact that the Galois group is a subgroup of $G$ is clear. On the other hand, showing that the Galois group is all of $G$ is not entirely trivial, though it can be made elementary. We freely make the identifications

$$G = (\mathbb{Z}/N\mathbb{Z})^\times = (\mathbb{Z}/N_p\mathbb{Z})^\times \times (\mathbb{Z}/p^d\mathbb{Z})^\times.$$ 

Fix a rational prime $p$. The inertia and decomposition subgroups of $p$ in $G$ are

$$I_p = \{1\} \times (\mathbb{Z}/p^d\mathbb{Z})^\times, \quad D_p = \langle p + N_p \mathbb{Z} \rangle \times (\mathbb{Z}/p^d\mathbb{Z})^\times.$$ 

Thus $|I_p| = e$ and $|D_p| = ef$.

The inertia field $K_{I,p}$ and the decomposition field $K_{D,p}$ of $p$ are the intermediate fields of $K/\mathbb{Q}$ corresponding to the inertia and decomposition subgroups of $G$. Thus $\mathbb{Q} \subset K_{D,p} \subset K_{I,p} \subset K$. The decomposition field is so named because $p$ decomposes there as $p \mathcal{O}_D = p_{1,D} \cdots p_{g,D}$ (the $p_{i,D}$ are ideals), and for each $i$ there is no residue field growth, meaning that $[\mathcal{O}_D/p_{i,D} : \mathbb{Z}/p\mathbb{Z}] = 1$, and visibly there is no ramification. The inertia field is so named because each $p_{i,D}$ remains inert in $\mathcal{O}_I$, which is to say that $p_{i,D} \mathcal{O}_I$ takes the form $p_{i,I}$ rather than decomposing further, but here there is residue field growth, specifically $[\mathcal{O}_I/p_{i,I} : \mathcal{O}_D/p_{i,D}] = f$, and again there is no ramification. Finally, each $p_{i,I}$ ramifies in $\mathcal{O}_K$ as $p_{i,I}/\mathcal{O}_K = p_{i,I}^e$ but with no further decomposition and with no further residue field growth, $[\mathcal{O}_K/p_{i,I} : \mathcal{O}_I/p_{i,I}] = 1$.

### 4. The Dedekind Zeta Function and its Euler Product

The ring of integers of $K$ is $\mathcal{O}_K = \mathbb{Z}[\zeta_N]$.

Define the norm of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ to be

$$N\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|.$$ 

Thus we tacitly assert without proof that the quotient is finite. We further assert without proof that the norm is strongly multiplicative, and that

$$Np = p^f \quad \text{where} \quad p \mid p \text{ and } f \text{ is the inertial degree as above.}$$
**Definition 4.1.** The Nth cyclotomic Dedekind zeta function is

\[ \zeta_K(s) = \sum_a N^{-s} = \prod_p (1 - Np^{-s})^{-1}, \quad \text{Re}(s) > 1. \]

The sum is taken over nonzero ideals of \( \mathcal{O}_K \), and the product is taken over maximal ideals.

For any \( p \), compute that

\[ \prod_p (1 - Np^{-s})^{-1} = (1 - p^{-fs})^{-g} = \prod_{k=0}^{f-1} (1 - \zeta_K^k p^{-s})^{-g} = \prod_{\chi} (1 - \chi(p)p^{-s})^{-1}, \]

where the product is taken over all characters \( \chi \) modulo \( N \), each character understood to be the underlying primitive character extended to a multiplicative function on \( \mathbb{Z} \). As discussed above, \( \chi(p) = \zeta_K^k \) for \( g \) characters \( \chi \) modulo \( N \), independently of \( k \), these characters being defined modulo \( Np \) while the characters \( \chi \) modulo \( N \) that are not defined modulo \( Np \) take \( p \) to 0 and thus contribute a trivial factor of 1 to the last product in the previous display. Overall, then, we have

\[ \zeta_K(s) = \prod_p \prod_{\chi} (1 - \chi(p)p^{-s})^{-1} = \prod_{\chi} \prod_p (1 - \chi(p)p^{-s})^{-1}, \]

which is to say that the Nth cyclotomic Dedekind zeta function factors as the product of all Dirichlet L-functions modulo \( N \),

\[ \zeta_K(s) = \prod_{\chi} L(\chi, s). \]

One consequence of these calculations is as follows. It is known that the function \( L(1, s) = \zeta(s) \), which is initially defined only for \( \text{Re}(s) > 1 \), extends to a meromorphic function on \( \{\text{Re}(s) > 0\} \) whose only singularity is a simple pole at \( s = 1 \), and it is known that \( L(\chi, s) \) for \( \chi \neq 1 \) is analytic on \( \{\text{Re}(s) > 0\} \). Thus \( \zeta_N(s) \) is meromorphic on \( \{\text{Re}(s) > 0\} \) with its only possible pole at \( s = 1 \). Recall that \( \prod_p (1 - Np^{-s})^{-1} = (1 - p^{-fs})^{-g} \), and estimate for any positive real \( s \) that

\[ (1 - p^{-fs})^{-g} = \left( \sum_{n=0}^{\infty} p^{-nf_N} \right)^{g} \geq \sum_{n=0}^{\infty} p^{-nf_N} \geq \sum_{n=0}^{\infty} p^{-n\phi(N)s} = (1 - p^{-\phi(N)s})^{-1}. \]

Multiplying over \( p \) gives

\[ \zeta_N(s) \geq \zeta(\phi(N)s), \quad s > 0. \]

Thus \( \zeta_N(s) \) must have a pole at \( s = 1 \): if it didn’t then it would converge for all \( s > 0 \), but the displayed inequality shows that it diverges at \( s = 1/\phi(N) \). The fact that \( \zeta_N(s) \) has a pole at \( s = 1 \) is the crux of Dirichlet’s proof that there are infinitely many primes in any credible arithmetic progression.

The Dedekind zeta function of \( K \) is the generating function for a representation number function,

\[ \zeta_K(s) = \sum_{n=1}^{\infty} |\{a : Na = n\}| n^{-s}. \]
On the other hand, let $d = \phi(N)$. Then
\[
\prod_{\chi} L(\chi, s) = \sum_{n=1}^{\infty} \left[ \sum_{n_1 \cdots n_d = n} \chi_1(n_1) \cdots \chi_d(n_d) \right] n^{-s}.
\]
And so
\[
|\{a : Na = n\}| = \sum_{n_1 \cdots n_d = n} \chi_1(n_1) \cdots \chi_d(n_d).
\]
In particular, for any prime $p$,
\[
|\{p : Np = p\}| = \sum_{\chi} \chi(p).
\]
The previous display is nothing other than the second orthogonality relation,
\[
\sum_{\chi} \chi(p) = \begin{cases} 
\phi(N_p) & \text{if } p \equiv 1 \pmod{N_p}, \\
0 & \text{otherwise}.
\end{cases}
\]
That is, the second orthogonality relation is a special case of a cyclotomic counting formula.