

§1. The Main Theorem: Notation and Statement.

Fix odd prime p . (I cannot find a statement of the Main Theorem for $p = 2$.) We write $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times 1 + p\mathbb{Z}_p$, and correspondingly $x = \tau(x) \cdot \langle x \rangle$. The function τ is called the *Teichmüller* character, and it only depends on $x \bmod p$; the function $\langle x \rangle = x/\tau(x)$ is called the *projection* of x onto Γ .

Fix a positive integer m with $m \not\equiv 2 \pmod{4}$ and $p \nmid m$, and for convenience let $q_n = mp^{n+1}$. Also fix a subfield $F \subseteq \mathbb{Q}(\mu_m)^+$ of the maximal real subfield of $\mathbb{Q}(\mu_m)$. Put $F_n = F(\mu_{p^{n+1}})$, $F_\infty = \bigcup F_n$, $\Delta = \text{Gal}(F_0/\mathbb{Q})$ (a quotient of $(\mathbb{Z}/mp)^\times$), $\Gamma_n = \text{Gal}(F_n/F_0)$, and $\Gamma = \text{Gal}(F_\infty/F_0)$. There is a natural projection map $\Gamma \rightarrow \Gamma/\Gamma^{p^n} = \Gamma_n$.

There is a canonical isomorphism $[\cdot]: 1 + p\mathbb{Z}_p \xrightarrow{\sim} \Gamma$ given by observing the action of Γ on μ_{p^∞} : for each $x \in 1 + p\mathbb{Z}_p$, $[x]$ is the unique element of Γ that satisfies $[x](\zeta) = \zeta^x$ for all $\zeta \in \mu_{p^\infty}$. (Ask yourself, what is the relation of $[\cdot]$ to the local Artin map over \mathbb{Q}_p ?) We extend the definition of this function to all of \mathbb{Z}_p^\times by projection, i.e. $[a] = [\langle a \rangle]$ for arbitrary $a \in \mathbb{Z}_p^\times$. We will write $[a]_n$ for the image of $[a]$ under the map $\Gamma \rightarrow \Gamma_n$. Throughout, we fix the topological generator $\gamma_0 = 1 + q_0 \in 1 + p\mathbb{Z}_p$ and put $\gamma = [\gamma_0]$.

Fix a nontrivial even character $\chi: \Delta \rightarrow \overline{\mathbb{Q}_p}^\times$, of conductor m or mp . One may view χ as an even character of the “first kind” of conductor m or mp , or as an even Dirichlet character of conductor m times an even power of the Teichmüller character τ .

Let $K = \mathbb{Q}_p(\chi, \tau)$ be the extension of \mathbb{Q}_p generated by the values of χ and τ , and let $\mathcal{O} = \mathcal{O}_K$ be the ring of p -adically integral elements of K . Let $\Lambda_n = \mathcal{O}[\Gamma_n]$ for $n \geq 0$, and let $\Lambda = \mathcal{O}[[\Gamma]] = \mathcal{O}[[T]]$ (under the Iwasawa isomorphism sending γ to $1 + T$). The methods in Cathy’s talk show that for any finitely generated Λ -module M , there is a quasi-isomorphism

$$M \sim \Lambda^{\oplus r} \oplus \bigoplus \Lambda/p^{m_i} \oplus \bigoplus \Lambda/f_j,$$

where the $m_i > 0$ are integers and the f_j are irreducible distinguished polynomials in Λ . We defined the numerical invariants of M to be $\text{rank}(M) = r$, $\mu(M) = \sum m_i$, and $\lambda(M) = \sum \deg f_j$, and the *characteristic ideal* of M to be the principal ideal $\text{char}(M) = p^\mu \cdot \prod f_j \cdot \Lambda$.

Further, for any $\psi: \Delta \rightarrow \overline{\mathbb{Q}_p}^\times$, define the idempotent operator

$$e_\psi = \frac{1}{\#\Delta} \sum_{\delta \in \Delta} \psi(\delta) \delta^{-1} \in \mathcal{O}[\Delta].$$

Then $\sum_\psi e_\psi = 1$, and the product $e_\psi \cdot e_{\psi'} = e_\psi$ if $\psi = \psi'$ and is 0 otherwise. We will have occasion to use the “even” and “odd” projectors,

$$e_\pm = \sum_{\psi(-1)=\pm 1} e_\psi$$

For any Λ -module M with a commuting Δ -action (i.e., a $\text{Gal}(F_\infty/\mathbb{Q})$ -module), we put $M(\psi) = e_\psi M$ and $M^\pm = e_\pm M$; both of these results are again Λ -modules. One has $M = \bigoplus M(\psi) = M^+ \oplus M^-$, and $\text{char}(M) = \prod \text{char } M(\psi) = \text{char}(M^+) \cdot \text{char}(M^-)$.

Finally we come to the two main players, and the Main Theorem which connects them.

We let $X_n = \mathcal{C}\ell(F_n)[p^\infty]$ be the p -primary subgroup of the ideal class group of F_n , and $X = \lim_{\leftarrow} X_n$.

For now, take the following claim on faith.

Fact. There exists a power series $f(\chi, T) \in \Lambda$ such that

$$L_p(\chi, s) = f(\chi, \gamma_0^s - 1)$$

for all $s \in \mathbb{Z}_p$, where $L_p(\chi, \cdot)$ is the p -adic L -function for χ as constructed by Akshay.

Granted the existence of this special power series $f(\chi, T)$, we may state the Main Theorem as follows.

Main Theorem. With the preceding notation, $\text{char } X(\tau\chi^{-1}) = f(\chi, T) \cdot \Lambda$.

This theorem was originally proved by Mazur and Wiles in a tour de force of algebraic geometry, and later proved in an entirely different (and more “elementary”) way by Kolyvagin.

The general method of proving this claim involves making use of the following two lemmas.

Lemma. Suppose $f_1, \dots, f_r, f'_1, \dots, f'_r \in \Lambda$ are such that Λ_n/f_i and Λ_n/f'_i are finite for all i and all $n \geq 0$. (This amounts to the f_i and f'_i being relatively prime to $\gamma^{p^n} - 1$ for all n .) Assume that the following two conditions hold.

- (1) $f_i \mid f'_i$ for all i .
- (2) There exists a constant $c > 0$ such that, for n sufficiently large,

$$c^{-1} \leq \frac{\prod \#(\Lambda_n/f_i)}{\prod \#(\Lambda_n/f'_i)} \leq c.$$

Then for every i , the elements f_i and f'_i generate the same principal ideal in Λ (i.e. they differ by a unit in Λ^\times):

Proof. By the Weierstrass Preparation Theorem, there exist unique $m_i, m'_i \geq 0$, distinguished $h_i, h'_i \in \mathcal{O}[T]$, and units $U_i, U'_i \in \Lambda^\times$ such that $f_i = p^{m_i} h_i U_i$ and $f'_i = p^{m'_i} h'_i U'_i$ for all i . Because of (1), we have $m_i \leq m'_i$ and $h_i \mid h'_i$ in $\mathcal{O}[T]$. Cathy showed that $m_i = \mu(\Lambda/f_i)$ and $\deg(h_i) = \lambda(\Lambda/f_i)$ are determined by $\#(\Lambda_n/f_i)$, up to a constant independent of n , for n sufficiently large (and also the respective statements for the primed quantities). Thus (2) implies that $m_i = m'_i$ and $\deg h_i = \deg h'_i$, forcing $h_i = h'_i$. Therefore, $f_i = f'_i \cdot \text{unit}$ for all i .

A similar result holds for ideals, though neither lemma is strictly more general than the other.

Lemma. Suppose $I_1, \dots, I_r, I'_1, \dots, I'_r \subseteq \Lambda$ are ideals such that Λ_n/I_i and Λ_n/I'_i are finite for all $n \geq 0$. Suppose further that

- (3) for each i we have $I_i \supseteq I'_i$, and
- (4) for all $n \geq 0$,

$$\prod \#(\Lambda_n/I_i) = \prod \#(\Lambda_n/I'_i).$$

Then $I_i = I'_i$ for all $1 \leq i \leq r$.

Proof. Let $A_{i,n} = \Lambda_n/I_i$ and $A'_{i,n} = \Lambda_n/I'_i$. Then there is a canonical surjection $A'_{i,n} \twoheadrightarrow A_{i,n}$, which shows that $\#A_{i,n}$ divides $\#A'_{i,n}$ for all i and n . If we were to have inequality for any i and n , then the condition (4) would be impossible, so we must have $A'_{i,n} \xrightarrow{\sim} A_{i,n}$ for each i and each n . Since $\Lambda/I'_i \rightarrow \Lambda/I_i$ arises from the maps $A'_{i,n} \rightarrow A_{i,n}$, which give an isomorphism of projective systems, we must have that $\Lambda/I'_i \rightarrow \Lambda/I_i$ is an isomorphism as well, forcing $I_i = I'_i$.

The claims (2) and (4), applied to various modules arising in number theory, generally result from various “analytic class number formulas.” The claims (1) and (3) require more novel or sophisticated tools (such as Shimura varieties, Euler systems, or distinguished annihilators of ideal class groups).

In the following talks, I will

- verify the Fact preceding the Main theorem, so that all of this makes sense,
- prove that (2) always holds for $F = \mathbb{Q}$, and
- show that, under a common condition, (3) and (4) hold too.

Afterwards, Abhinav will prove (1) and (2) universally.

§2. Construction of $f(\chi, T)$ as described in Fact.

The exposition in this section has been shamelessly stolen from K. Iwasawa, *Lectures on p -adic L -functions*.

To recap, p is an odd prime, $m \not\equiv 2 \pmod{4}$, $p \nmid m$, χ is even of the first kind, of conductor m or mp , and $q_n = mp^{n+1}$.

If $r \in \mathbb{R}$, then write $\{r\}$ for the smallest nonnegative real number with $r - \{r\} \in \mathbb{Z}$, i.e. $0 \leq \{r\} < 1$ and $\{r\} \equiv r \pmod{\mathbb{Z}}$. Notice that if $a \in \mathbb{Z}/N$, then $\{a/N\}$ makes sense, and is equal to a_0/N , where $0 \leq a_0 < N$ with $a_0 \equiv a \pmod{N}$.

Definition. The Stieckelberger elements are given by

$$\begin{aligned} \xi_n = \xi_n^\chi &= - \sum_{a \in (\mathbb{Z}/q_n)^\times} \left\{ \frac{a}{q_n} \right\} \cdot \tau^{-1} \chi(a) \cdot [a]_n^{-1} = -\frac{1}{q_n} \sum_{\substack{a=0 \\ (a, q_0)=1}}^{q_n-1} a \cdot \tau^{-1} \chi(a) \cdot [a]_n^{-1} \\ &= -\frac{1}{q_n} \sum_{\substack{a=0 \\ (a, q_0)=1}}^{q_n-1} \langle a \rangle \cdot \chi(a) \cdot [a]_n^{-1} \in \Lambda_n[1/p], \end{aligned}$$

and

$$\eta_n = \eta_n^\chi = (1 - \gamma_0[\gamma_0]_n^{-1}) \xi_n^\chi.$$

Proposition. The projection $\Lambda_{n+1}[1/p] \rightarrow \Lambda_n[1/p]$ takes $\xi_{n+1} \mapsto \xi_n$.

Proof. Let the projection take $\xi_{n+1} \mapsto \xi'_{n+1}$. Our claim is that $\xi'_{n+1} = \xi_n$. To see this, we evaluate the sum defining ξ'_{n+1} with $a = b + kq_n$, $0 \leq b < q_n$, $(b, q_0) = 1$, $0 \leq k < p$. Then we have, by the q_0 -periodicity of the symbols,

$$\xi'_{n+1} = -\frac{1}{q_n} \sum_b \tau^{-1} \chi(b) [b]_n^{-1} \sum_k (b + kq_n) = \xi_n - \frac{p-1}{2} \sum_b \tau^{-1} \chi(b) [b]_n^{-1}.$$

We just need the last summation to vanish. But since p is odd, $\langle -b \rangle = \langle b \rangle$, so $[-b]_n = [b]_n$. Also, χ is even and $\tau^{-1} \chi$ is odd, so that $\tau^{-1} \chi(-a) = -\tau^{-1} \chi(a)$. Thus, in the last summation, the terms with $b < q_n/2$ and the terms with $b > q_n/2$ cancel each other out. This establishes the claim.

Corollary. For $m \geq n \geq 0$, $\xi_m \mapsto \xi_n$, and $\eta_m \mapsto \eta_n$ as well.

Proposition. The element $\eta_n \in \Lambda_n[1/p]$ lies in the subring $\Lambda_n \subset \Lambda_n[1/p]$.

Proof. To see this, first notice that $\langle \gamma_0 \rangle = \gamma_0$ and (since $\gamma = 1 + q_0 \equiv 1 \pmod{mp}$) $\chi(\gamma_0) = 1$. Using these observations together with the definitions, we see that

$$\eta_n = \xi_n + \frac{1}{q_n} \sum_a \langle (1 + q_0)a \rangle \chi((1 + q_0)a) [(1 + q_0)a]_n^{-1}.$$

For each integer a with $0 \leq a < q_n$ and $(a, q_0) = 1$, let a' and a'' be those two integers that satisfy $0 \leq a' < q_n$ and $a' + a''q_n = (1 + q_0)a$. Easy to check are:

- $\tau((1 + q_0)a) = \tau(a')$
- $\chi((1 + q_0)a) = \chi(a')$
- $[(1 + q_0)a]_n = [a']_n$
- $\langle (1 + q_0)a \rangle = \tau^{-1}((1 + q_0)a) \cdot (1 + q_0)a = \tau^{-1}(a')(a' + a''q_n) = \langle a' \rangle + \tau^{-1}(a')a''q_n$
- $a \mapsto a'$ is a permutation of $(\mathbb{Z}/q_n)^\times$

Thus, substituting in, we get

$$\eta_n = \xi_n + \frac{1}{q_n} \sum_a (\langle a' \rangle + \tau^{-1}(a')a''q_n) \chi(a') [a']_n^{-1} = \sum_a a'' \tau^{-1} \chi(a') [a']_n^{-1} \in \Lambda.$$

The preceding fact did not require that χ be nontrivial. However, the following fact does.

Proposition. If χ is nontrivial, then $\xi_n \in \Lambda_n$.

Proof. We keep the notation used in the preceding proof. Note first that

- $(1 + q_0)(q_n - a) = (q_n - a') + (q_0 - a'')q_n$, so that
- $(q_n - a)' = q_n - a'$ and $(q_n - a)'' = q_0 - a''$
- $\langle q_n - a \rangle = \tau^{-1}(q_n - a) \cdot (q_n - a) = \tau^{-1}(-a)(q_n - a) = \langle a \rangle - \tau^{-1}(a)q_n$

- $\chi(q_n - a) = \chi(a)$
- $[q_n - a]_n = [a]_n$.

Writing \sum' for the sum over all $0 \leq a < q_n/2$ with $(a, q_0) = 1$, we have

$$\begin{aligned}\xi_n &= -\frac{1}{q_n} \sum'_a (\langle a \rangle \chi(a) [a]_n^{-1} + \langle q_n - a \rangle \chi(q_n - a) [q_n - a]_n^{-1}) \\ &= -\frac{2}{q_n} \sum'_a \langle a \rangle \chi(a) [a]_n^{-1} + \sum'_a \tau^{-1} \chi(a) [a]_n^{-1}.\end{aligned}$$

The last term on the right hand side lies in Λ , so it suffices to show that the first term on the right hand side does too.

Fix a value a_0 (with $(a_0, q_0) = 1$), and write \sum'' for the sum over all integers a with $0 \leq a < q_n/2$, $(a, q_0) = 1$, and also $[a]_n = [a_0]_n$. The last condition implies that $\langle a \rangle \equiv \langle a_0 \rangle \pmod{q_n}$, and so we get

$$\sum'' \langle a \rangle \chi(a) [a]_n^{-1} \equiv \left(\sum'' \chi(a) \right) \langle a_0 \rangle [a_0]_n^{-1} \pmod{q_n \Lambda_n}.$$

However, recalling that $(\mathbb{Z}/q_n)^\times = \Delta \times \Gamma_n$, the sum \sum'' runs over a set of coset representatives for $\Delta/\{\pm 1\}$. Since χ is a *nontrivial* even character of Δ , we find that the sum is zero, whence

$$\sum'' \langle a \rangle \chi(a) [a]_n^{-1} \equiv 0 \pmod{q_n \Lambda_n},$$

and thus

$$\sum'_a \langle a \rangle \chi(a) [a]_n^{-1} \equiv 0 \pmod{q_n \Lambda_n},$$

or equivalently

$$\frac{1}{q_n} \sum'_a \langle a \rangle \chi(a) [a]_n^{-1} \in \Lambda_n.$$

This shows that $\xi_n \in \Lambda$.

Suppose for the moment that χ is nontrivial. Then we have elements $\xi = \xi^\chi = \lim_{\leftarrow} \xi_n^\chi$ and $\eta = \eta^\chi = \lim_{\leftarrow} \eta_n^\chi \in \Lambda$. Using the Iwasawa isomorphism, we associate to them power series

$$\xi^\chi \leftrightarrow f(\chi, T), \quad \eta^\chi \leftrightarrow g(\chi, T) \in \mathcal{O}[[T]].$$

These two power series are related via

$$g(\chi, T) = f(\chi, T) \cdot h(T),$$

where $h(T) = 1 - \gamma_0(1 + T)^{-1}$ is the power series corresponding to the group ring element $1 - \gamma_0[\gamma_0]^{-1}$.

However, if χ is trivial, then we still get an element $\eta^\chi \in \Lambda$ and a corresponding $g(\chi, T)$, and we may define

$$f(\chi, T) = \frac{g(\chi, T)}{h(T)} \in \text{Frac } \mathcal{O}[[T]].$$

Then $f(\chi, T) \leftrightarrow \xi^\chi \in \text{Frac } \Lambda$.

Moreover, these are the power series we wished to construct, in order to verify the Fact.

Theorem. For all $s \in \mathbb{Z}_p$ (except $s = 1$ if χ is trivial), we have

$$L_p(\chi, s) = f(\chi, \gamma_0^s - 1).$$

Proof. It suffices to check this when $s = 1 - k$, with $k \geq 1$ a rational integer, and the result follows by continuity. Thus it suffices to check that, for such k ,

$$f(\chi, (1 + q_0)^{1-k} - 1) = - (1 - \tau^{-k} \chi(p)) p^{-(1-k)} \frac{B_{\tau^{-k} \chi, k}}{k}.$$

For each $t \in \mathbb{Z}_p$, there exists a unique continuous homomorphism $\phi_t: \Lambda \rightarrow \mathcal{O}$ satisfying

$$\phi_t(\gamma) = \gamma_0^t, \quad \text{i.e.} \quad \phi_t([a]) = \langle a \rangle^t \text{ for all } a \in \mathbb{Z}_p^\times.$$

For an integer $n \geq 0$, we write $\phi_{t,n}$ for the composition of ϕ_t under $\mathcal{O} \rightarrow \mathcal{O}/q_n$; this map factors through a map $\Lambda_n \rightarrow \mathcal{O}/q_n$, which we shall by abuse of notation also call $\phi_{t,n}$. Notice that if the Iwasawa isomorphism associates $\Lambda \ni \beta \leftrightarrow B(T) \in \mathcal{O}[[T]]$, then $\phi_t(\beta) = B(\gamma_0^t - 1)$.

We shall calculate the image of η_n under ϕ_t , and infer from this the image of ξ_n under ϕ_t , and deduce our desired result from this. Before we do this, we observe a few things.

- Since χ and τ are well-defined on $\mathbb{Z}/q_0 = \mathbb{Z}/mp$, we have $\tau^{-t-1} \chi(a') = \tau^{-1-t} \chi(a)$ for all appropriate a .
- By the binomial theorem,

$$(1 + q_0)^{t+1} a^{t+1} = (a' + a'' q_n)^{t+1} \equiv (a')^{t+1} + (a')^t a'' q_n (t+1) \pmod{q_n^2}.$$

- Putting the two above together and summing over a , we get

$$\begin{aligned} & (1 + q_0)^{t+1} \sum_a \tau^{-1-t} \chi(a) a^{t+1} \\ & \equiv \sum_a \tau^{-1-t} \chi(a') (a')^{t+1} + (t+1) \sum_a a'' \tau^{-1-t} \chi(a') (a')^t q_n \pmod{q_n^2}. \end{aligned}$$

- Moving the first term on the right over to the left, dividing through by q_n , and recalling that $a \mapsto a'$ is a permutation of our coset representatives, we get

$$\sum_a a'' \tau^{-1-t} \chi(a') (a')^t \equiv -\frac{1}{t+1} (1 - \gamma_0^{t+1}) \sum_a \tau^{-1-t} \chi(a) a^{t+1} \pmod{q_n}.$$

We now calculate $\phi_{-t,n}(\eta_n)$. Recall from our previous work that $\eta_n = \sum_a a'' \tau^{-1} \chi(a') [a']_n^{-1}$. Applying $\phi_{-t,n}$ to both sides of this gives

$$\begin{aligned} \phi_{-t,n}(\eta_n) &= \sum_a a'' \tau^{-1} \chi(a') \langle a' \rangle^t = \sum_a a'' \tau^{-1-t} \chi(a') a^t \\ &= -(1 - \gamma_0^{t+1}) \cdot \frac{1}{q_n} \sum_a \tau^{-1-t} \chi(a) a^{t+1} \pmod{q_n}. \end{aligned}$$

This equation allows us to readily calculate $\phi_{-t}(\eta)$. We have

$$(1+t)\phi_{-t}(\eta) = \lim_{n \rightarrow \infty} (1+t)\phi_{-t,n}(\eta_n) = -(1 - \gamma_0 \gamma_0^t) \lim_{n \rightarrow \infty} \frac{1}{q_n} \sum_a t^{-1-t} \chi(a) a^{t+1}.$$

Notice that the term $1 - \gamma_0 \gamma_0^t$ is just $\phi_{-t}(1 - \gamma_0 [\gamma_0]^{-1})$, which corresponds to $h(T) = 1 - \gamma_0(1+T)^{-1}$ under the Iwasawa isomorphism. Because of the product expression $g(\chi, T) = h(T)f(\chi, T)$, the remaining term above must be $(1+t)\phi_{-t}(\xi)$. Thus we have

$$\phi_{-t}(\xi) = -\frac{1}{t+1} \lim_{n \rightarrow \infty} \frac{1}{q_n} \sum_a \tau^{-1-t} \chi(a) a^{t+1}.$$

Recalling that $f(\chi, \gamma_0^t - 1) = \phi_t(\xi)$, and letting $t = k - 1$ for $k \geq 1$ an integer, we have

$$f(\chi, \gamma_0^{1-k} - 1) = -\frac{1}{k} \lim_{n \rightarrow \infty} \frac{1}{q_n} \sum_a \tau^{-k} \chi(a) a^k$$

Using the fact that $\tau^{-1-t} \chi(a) = 0$ for $(a, m) > 1$, we write the summation in the limit of the right hand side above as

$$\sum_{\substack{0 \leq a < q_n \\ (a, q_0) = 1}} = \sum_{\substack{0 \leq a < q_n \\ (a, p) = 1}} = \sum_{1 \leq a \leq q_n} - \sum_{\substack{1 \leq a \leq q_n \\ p|a}} = \sum_{1 \leq a \leq q_n} - \left(\tau^{-k} \chi(p) p^k \sum_{0 < a < q_{n-1}} \right).$$

In the limit, we may substitute $n = n + 1$ in the very last summation (adjusting by a power of p outside the sum), leaving us with

$$f(\chi, \gamma_0^{1-k} - 1) = -\frac{1}{k} (1 - \tau^{-k} \chi(p) p^{-(1-k)}) \lim_{n \rightarrow \infty} \frac{1}{q_n} S_{\tau^{-k} \chi}^k(q_n),$$

with

$$S_{\chi}^k(N) = \sum_{a=1}^N \chi(a) a^k.$$

Iwasawa proves in Lemma 2.1 of *Lectures on p -adic L -functions* (I don't know if Akshay covered it; it follows from elementary facts about Bernoulli polynomials) that

$$\lim_{n \rightarrow \infty} \frac{1}{q_n} S_{\tau^{-k} \chi}^k(q_n) = B_{\tau^{-k} \chi, k},$$

which, upon substitution into the preceding formula, completes the proof of the Fact.

Now that we have $f(\chi, T)$ in hand, we know that the Main Theorem makes sense.

Although I did not prove this, since it would have required more crossing t's and dotting i's than I cared for, the methods above can be extended slightly to prove the following more general fact.

Proposition. Let χ be a primitive even Dirichlet character modulo q_n , and write $\chi = \theta\pi$, where θ is primitive modulo m or q_0 (“ θ is of the first kind”), and π factors through the projection $\langle \cdot \rangle$ (“ π is of the second kind”). Let $\zeta_\pi = \pi(\gamma_0^{-1})$. Then one has

$$L_p(\chi, s) = f(\theta, \zeta_\pi \gamma_0^s - 1) \quad \text{for all } s \in \mathbb{Z}_p,$$

where $f(\theta, T)$ is the polynomial associated to θ in this section.

§3. Case $F = \mathbb{Q}$, Part I: Class Number Formula.

In this section, we work in the special case that $m = 1$, so that $F = \mathbb{Q}$ and $F_n = \mathbb{Q}(\mu_{p^{n+1}})$, and χ is just a nontrivial even character $\mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$, which we will often identify with an even power of the Teichmüller character τ . We let F_n^+ denote the maximal real subfield of F_n .

We denote $f(\chi, T)$ for the power series constructed in the preceding section, and also $g(\tau\chi^{-1}, T)$ for any power series that generates the ideal characteristic ideal $\text{char}X(\tau\chi^{-1})$. In order to ease notation, we shall write $f(T)$ or $g(T)$, respectively, for the above power series, whenever the character χ in question is clear.

The purpose of this section is to prove the content of condition (2) the lemmas of §1. We will phrase our result in such a way that under the cyclicity hypothesis of §5, we will immediately recover condition (4) of those lemmas.

More specifically, we will show that for some constant $c > 0$, one has

$$c^{-1} \leq \prod_{\chi \text{ even, nontriv}} \frac{\#\Lambda_n/f(\chi, T)}{\#\Lambda_n/g(\chi^{-1}\tau, T)} \leq c$$

for all n sufficiently large. We shall first find more convenient forms for the modules in both the numerator and the denominator in the above middle term. (It is under this restatement that we will easily recover condition (4) under they cyclicity hypothesis.)

By definition, we have $f(\chi, T) \leftrightarrow \lim_{\leftarrow} \xi_n^\chi$ under the Iwasawa isomorphism that associates $1 + T \leftrightarrow [1 + p]$. As a consequence, one has

$$\Lambda_n/f(T) = \Lambda_n/\xi_n,$$

which takes care of the numerator term. To better handle the denominator term, we have the following fact.

Proposition. There exists a constant $d > 0$ such that

$$d^{-1} \leq \frac{\#\Lambda_n/g(\chi^{-1}\tau, T)}{\#X_n(\chi^{-1}\tau)} \leq d$$

for all n sufficiently large.

Proof. Notice that there is exactly one prime above p in each F_n , and this prime is totally ramified in the \mathbb{Z}_p -extension. Therefore, by the easy case in Cathy's talk, we have $X_n = X/(\gamma^{p^n} - 1)X$, and taking eigenspaces on both sides we get

$$X_n(\chi^{-1}\tau) = X(\chi^{-1}\tau)/(\gamma^{p^n} - 1)X(\chi^{-1}\tau).$$

We conclude by comparing the λ and μ invariants of $X(\chi^{-1}\tau)$ and of $\Lambda/g(\chi^{-1}\tau, T)$ to find that there exists a constant $d > 0$ such that, for all n sufficiently large,

$$d^{-1} \leq \frac{\#\Lambda_n/g(\chi^{-1}\tau, T)}{\#X(\chi^{-1}\tau)/(\gamma^{p^n} - 1)X(\chi^{-1}\tau)} \leq d,$$

which gives us the desired result.

We need one more lemma concerning the structure of X . The proof of this lemma will be postponed until §5, since it requires Stieckelberger's Theorem.

Lemma. For all $n \geq 0$, $X_n(\tau) = 0$. Consequently,

$$\#X_n^- = \prod_{\chi \text{ even, nontriv}} \#X_n(\chi^{-1}\tau).$$

In order to prove our goal for this section, we have reduced our task to showing the following fact. (It is this fact which, under the cyclicity hypothesis, will give us property (4).)

Theorem. For all $n \geq 0$, we have

$$\#X_n^- = \prod_{\chi \text{ even, nontriv}} \#\Lambda_n/\xi_n^\chi.$$

Proof. Since both quantities above are powers of p , it suffices to compare their p -adic valuations.

Recall that e_\pm denote the projection operators onto the eigenspaces for even and odd Dirichlet characters. A simple calculation shows that $e_\pm = \frac{1}{2}(1 \pm \sigma)$, where σ denotes complex conjugation in Δ . Therefore, e_+ acts by $\frac{1}{2}\text{Norm}_{F_n/F_n^+}$ on X_n . Furthermore, since $e_+e_- = 0$, the norm map kills X_n^- . Let Y_n denote $\mathcal{C}\ell(F_n^+)[p^\infty]$. Then $e_+: X_n^+ \rightarrow Y_n$, and there is also an "inclusion" map $\iota: Y_n \rightarrow X_n$ given by considering ideals of F_n^+ as ideals of F_n . Using basic facts about Dedekind domains, we know that $e_+ \circ \iota$ acts on ideals of F_n^+ by raising to the power of $[F_n : F_n^+] = 2$. Since $(2, p) = 1$, this $e_+ \circ \iota$ induces an isomorphism of Y_n to itself: ι is injective, and e_+ is surjective. On the other hand, since e_+ is idempotent, we have $e_+|_{X_n^+} = \text{id}_{X_n^+}$, so that e_+ (or the norm map) gives an isomorphism $X_n^+ \cong Y_n$.

The upshot of the preceding paragraph is that $\#X_n^- = \#X_n/\#Y_n$, and that each of the quantities on the right hand side may be computed via the complex-analytic class number formula. In general, if K is a finite abelian extension of \mathbb{Q} , one has

$$\frac{2^r (2\pi)^s h(K) R(K)}{\#\mu_\infty(K) \sqrt{|d(K)|}} = \prod_{\chi \in \Delta^*, \chi \text{ nontriv}} L(\chi, 1).$$

Since this expression is so common, I'll let you guess what all the constants are; $\Delta = \text{Gal}(K/\mathbb{Q})$. We are going to take the formula for $K = F_n$ and divide each side by its respective side of the formula for $K = F_n^+$. In L. Washington's *Cyclotomic Fields*, chapter 4, one can find the relationships between all the above constants for $K = F_n^+, F_n$, and how they all cancel out. Applying to the result the evaluation of Dirichlet L -functions at positive integers, and taking p -adic valuations of both sides, one gets

$$v_p(\#X_n/\#Y_n) = v_p\left(\#\mu_\infty(F_n) \prod_{\psi \text{ odd}} B_{\psi,1}\right).$$

The product above runs over all odd Dirichlet characters modulo p^{n+1} . Using the fact that $\#\mu_\infty(F_n) = 2p^{n+1}$, we conclude that

$$v_p(\#X_n^-) = v_p\left(\prod_{\psi \text{ odd}} B_{\psi,1}\right) + n + 1.$$

We now turn our attention to the right hand side of the desired equation. In order to treat it, we quickly review some concepts of elementary (p -adic) linear algebra. If L is a free \mathbb{Z}_p -module of finite rank, and if $A: L \rightarrow L$ is a \mathbb{Z}_p -linear endomorphism, then one can easily show that when L/AL is finite, its order is a power of p , and moreover, $v_p(\#L/AL)$ is equal to $v_p(\det A_{\mathbb{Q}_p})$, where $A_{\mathbb{Q}_p}$ is the induced mapping of vector spaces, $L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Moreover, this determinant is unchanged if we move our attention to the induced map $A_K: L \otimes_{\mathbb{Z}_p} K \rightarrow L \otimes_{\mathbb{Z}_p} K$, where K/\mathbb{Q}_p is a finite extension of fields.

We apply these observations to $A = \xi_n$ acting on $L = \Lambda_n$, and choose K to be the extension of \mathbb{Q}_p obtained by adjoining the values of all characters of Γ_n . (For those who are keeping score, K is just $\mathbb{Q}_p(\mu_{p^n})$.) Then $\Lambda_n \otimes_{\mathbb{Z}_p} K$ decomposes as a direct sum $\bigoplus K_\rho$ of copies of K , one eigenspace for each character ρ of Γ_n . On each K_ρ , an element $x \in \Lambda_n \otimes_{\mathbb{Z}_p} K$ acts (by multiplication) by $e_\rho x = \rho(x)$, the element we get when we substitute $\rho(\gamma)$ in place of each $\gamma \in \Gamma_n$ appearing in x . In particular, the operator $\xi_{n,K}$ acts diagonally with respect to the decomposition $\Lambda_n \otimes_{\mathbb{Z}_p} K = \bigoplus K_\rho$. Therefore, we simply have

$$v_p(\#\Lambda_n/\xi_n) = v_p(\det \xi_{n,K}) = v_p\left(\prod_{\rho \in \Gamma_n^*} \rho(\xi_n)\right).$$

Recalling the definition of ξ_n , and substituting $\rho(\langle a \rangle)$ in for $[a]_n$, we get

$$\rho(\xi_n^\chi) = - \sum_{a \in (\mathbb{Z}/p^{n+1})^\times} \left\{ \frac{a}{p^{n+1}} \right\} \chi \tau^{-1} \rho^{-1}(a) = -B_{\chi \tau^{-1} \rho^{-1}, 1},$$

by the very definition of the first generalized Bernoulli number.

Putting everything above together, and reindexing over various types of characters, we have

$$v_p\left(\prod \#\Lambda_n/\xi_n^\chi\right) = v_p\left(\prod_{\psi \text{ odd, no } \tau^{-1}} B_{\psi,1}\right),$$

where the product on the left extends over all characters χ that are nontrivial even powers of τ , and the product on the right extends over all odd Dirichlet characters ψ modulo p^{n+1} whose first-kind-component is not equal to τ^{-1} .

For each integer $n \geq 0$, we define $\epsilon(n)$ by

$$\epsilon(n) = -v_p \left(\prod_{\pi} B_{\tau^{-1}\pi,1} \right),$$

where the product ranges over all characters modulo p^{n+1} that are of the second kind. Using this notation, we rewrite the preceding equations as

$$v_p \left(\prod \# \Lambda_n / \xi_n^{\chi} \right) = v_p \left(\prod_{\psi \text{ odd}} B_{\psi,1} \right) + \epsilon(n),$$

where the left product is as before, but the right product is over *all* odd Dirichlet characters modulo p^{n+1} . Comparing our work with the desired equation, we see that we have reduced our task to proving that $\epsilon(n) = n + 1$.

In order to show that $\epsilon(n) = n + 1$, we will show that $\epsilon(0) = 1$, and that for any nontrivial Dirichlet character π of the second kind that is primitive modulo p^{f+1} , one has $v_p(B_{\chi\tau^{-1},1}) = -1/p^{f-1}(p-1)$. Since there are $p^{f-1}(p-1)$ such characters, we get our desired result by induction.

The results of §2 allow us to write

$$\zeta_p(s) = f(\gamma_0^s - 1) = \frac{g(\gamma_0^s - 1)}{1 - \gamma_0^{1-s}},$$

with $g(T) \in \mathbb{Z}_p[[T]]$. Moreover, the unproven proposition at the end of that section implies that if π is a primitive character of the second kind modulo p^{f+1} , then

$$B_{\pi\tau^{-1},1} = -f(\zeta_{\pi} - 1) = -\frac{g(\zeta_{\pi} - 1)}{1 - \gamma_0/\zeta_{\pi}},$$

where ζ_{π} is a p^f th root of unity. However, it is easy to calculate that the valuation of the denominator on the right is

$$v_p(1 - \gamma_0/\zeta_{\pi}) = v_p(\zeta_{\pi} - \gamma_0) = v_p((\zeta_{\pi} - 1) + (1 - \gamma_0)) = v_p(\zeta_{\pi} - 1) = \frac{1}{p^{f-1}(p-1)}.$$

Therefore, it suffices to show that $g(\zeta_{\pi} - 1)$ is a unit. This will follow if we can show that $g(T)$ is a unit, which will result in turn if we can show that $g(0)$ is a unit. By the definition of $\epsilon(0)$, and since $v_p(1 - \gamma_0) = 1$, the claim that $g(0)$ is a unit is equivalent to showing that $\epsilon(0) = 1$. So we are left with this one calculation.

For any $a \in (\mathbb{Z}/p)^{\times}$ we have $\tau^{-1}(a) a = \langle a \rangle \equiv 1 \pmod{p}$, hence

$$\sum_{a \in (\mathbb{Z}/p)^{\times}} \tau^{-1}(a) a \equiv p - 1 \equiv -1 \pmod{p},$$

and finally

$$B_{\tau^{-1},1} = \frac{1}{p} \sum_{a \in (\mathbb{Z}/p)^\times} \tau^{-1}(a)a \equiv -\frac{1}{p} \pmod{\mathbb{Z}_p},$$

so that $v_p(B_{\tau^{-1},1}) = -1$, and $\epsilon(0) = +1$.

This completes the proof of the Theorem.

§4. Case $F = \mathbb{Q}$, Part II: Stieckelberger's Theorem.

The exposition of this section has been shamelessly stolen from L. Washington, *Introduction to Cyclotomic Fields*.

This section is aimed at proving Stieckelberger's Theorem, which underlies the divisibilities (4) of the lemmas of §1 under the cyclicity hypothesis. The underlying means is to show that a certain group ring element always annihilates the ideal class group of a cyclotomic field. The connection with our theme is that our elements ξ_n^χ from the preceding happen to be the projections of the Stieckelberger element under the various idempotent operators e_χ .

For this section, we engage in a departure from our running notation. We let $K = \mathbb{Q}(\mu_m)$ be a cyclotomic field, where m is any positive integer with $m \not\equiv 2 \pmod{4}$, and we put $G = \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m)^\times$. Denote this last isomorphism by $[b] \leftarrow b$ for $(b, m) = 1$. Also, for this section, fix a primitive m th root of unity ζ_m .

Definition. The Stieckelberger element $\theta \in \mathbb{Q}[G]$ is given by the (equivalent) formulas

$$\theta = \frac{1}{m} \sum_{a=1, (a,m)=1}^m a[a]^{-1} = \sum_{a \in (\mathbb{Z}/m)^\times} \left\{ \frac{a}{m} \right\} [a]^{-1}.$$

Stieckelberger's Theorem. Let $u \in \mathbb{Z}[G]$ be such that $u\theta \in \mathbb{Z}[G]$. Then $u\theta$ annihilates $\mathcal{Cl}(K)$.

The reason for using the auxiliary element u is that, with the denominator m appearing in θ , one cannot make a well-defined action of θ on $\mathcal{Cl}(K)$ directly. However, we should know already that this will pose little problem in our applications, because the projections $\xi_n^\chi = e_{\chi^{-1}\tau}\theta$ are known to be integral. We discuss this more in §5.

The proof of the theorem requires a couple basic properties of Gauss sums, so we make a brief digression now to prove what is needed.

Let ℓ be a rational prime not dividing m , and let \mathbb{F}_ℓ denote the finite field of ℓ elements. Fix a primitive ℓ th root of unity ζ_ℓ . For any character $\chi: \mathbb{F}_\ell^\times \rightarrow \mathbb{C}^\times$, we define its Gauss sum to be

$$g(\chi) = - \sum_{z \in \mathbb{F}_\ell} \chi(z) \zeta_\ell^z,$$

where in this definition we put $\chi(0) = 0$ even if $\chi = 1$.

We assume that the order of χ divides m , i.e. $\chi^m = 1$. If χ has order dividing m then its values are contained in K , whence $g(\chi) \in K(\mu_\ell)$.

For lack of inspiration, write $a \mapsto [a]'$ for the natural isomorphism $\mathbb{F}_\ell^\times \cong \text{Gal}(K(\mu_\ell)/K)$. Notice that $\text{Gal}(K(\mu_\ell)/\mathbb{Q}) \cong (\mathbb{Z}/m\ell)^\times = (\mathbb{Z}/m)^\times \times \mathbb{F}_\ell^\times$, and we can extend $[b] \in G$ to be an element of this group by letting it act trivially on μ_ℓ .

Lemma. With the above notation, the following statements hold.

- (a) $g(\chi)\overline{g(\chi)} = \ell$.
- (b) $g(\chi)^{[a]'} = \chi(a)^{-1}g(\chi)$, for $a \in \mathbb{F}_\ell^\times$.
- (c) $g(\chi)^{[b]} = g(\chi^b)$.
- (d) $g(\chi)^{b-[b]} \in K$, for $b \in \mathbb{Z}$ with $(b, m) = 1$.
- (e) $g(\chi)^m \in K$.

Proof. (a)

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{y,z \neq 0} \chi(yz^{-1})\zeta_\ell^{y-z} = \sum_{z,x \neq 0} \chi(x)\zeta_\ell^{zx-z} = \sum_{z \neq 0, (x=1)} \chi(1) + \sum_{x \neq 1} \chi(x) \sum_{z \neq 0} \zeta_\ell^{z(x-1)} \\ &= (\ell - 1) + \sum_{x \neq 1} \chi(x) \cdot (-1) = \ell. \end{aligned}$$

(b)

$$g(\chi)^{[a]'} = - \sum \chi(z)\zeta_\ell^{az} = -\chi(a)^{-1} \sum \chi(az)\zeta_\ell^{az} = \chi(a)^{-1}g(\chi).$$

(c)

$$g(\chi)^{[b]} = - \sum \chi(a)^b \zeta_\ell^a = g(\chi^b).$$

(d) Using (b) and (c), for $[a]' \in \text{Gal}(K(\mu_\ell)/K)$ we have

$$\left(\frac{g(\chi)^b}{g(\chi)^{[b]}} \right)^{[a]'} = \left(\frac{g(\chi)^b}{g(\chi^b)} \right)^{[a]'} = \frac{(\chi(a)^{-1})^b g(\chi)^b}{\chi^b(a)^{-1} g(\chi^b)} = \frac{g(\chi)^b}{g(\chi^b)} = \frac{g(\chi)^b}{g(\chi)^{[b]}}.$$

Since $g(\chi)^{b-[b]}$ is fixed by the Galois group, it is in the base field.

(e) Take $b = 1 + m$ in (d) and notice that $[1 + m] = [1] = \text{id}$.

This ends the digression on Gauss sums, and we now turn to Stieckelberger's theorem.

Proof of the theorem. Fix an ideal class in $\mathcal{C}\ell(K)$, and using the Čebotarev density theorem choose a prime λ in this class that is unramified and of degree 1 over \mathbb{Q} . These restrictions imply that if ℓ is the rational prime below λ , then ℓ is totally split in K , so that $\ell \equiv 1 \pmod{m}$.

We may choose a primitive root s modulo ℓ , that is an integer s such that the image of s modulo ℓ generates the multiplicative group \mathbb{F}_ℓ^\times . Let χ be character of \mathbb{F}_ℓ^\times determined by $\chi(s) = \zeta_m$; the character χ has order m . As above, let $g(\chi) \in K(\mu_\ell)$ be the Gauss sum of χ .

We calculate the factorization of the ideal $(g(\chi))$ into prime ideals. Part (a) of the preceding lemma implies that $(g(\chi))$ only involves primes of $K(\mu_\ell)$ that lie above ℓ , and it suffices to compute the valuations of $g(\chi)$ with respect to these primes.

Notice that the primes of K above ℓ are just the conjugates $[b]\lambda$, and each of these primes lies under a unique prime $[b]\Lambda$ of $K(\mu_\ell)$. (*Warning:* we are using Λ to mean a different thing here than in all other sections!) Since $K(\mu_\ell)/K$ is totally ramified of degree $\ell - 1$ at every prime λ over ℓ , we have $[b]\Lambda^{\ell-1} = [b]\lambda$ in $K(\mu_\ell)$.

Let for $b \in (\mathbb{Z}/m)^\times$, let $r_b = v_{[b]^{-1}\Lambda}(g(\chi))$. Part (e) of the lemma says that $g(\chi)^{\ell-1} \in K$. Then $\Lambda^{\ell-1} = \lambda$ implies that $r_b = v_{[b]^{-1}\lambda}(g(\chi)^{\ell-1})$. This says that, as ideals in K ,

$$(g(\chi)^{\ell-1}) = \prod_{b \in (\mathbb{Z}/m)^\times} [b]^{-1} \lambda^{r_b}.$$

This means that $\sum r_b [b]^{-1}$ annihilates $[\lambda] \in \mathcal{C}\ell(K)$. Our next step is to translate this result into a statement concerning θ .

Since $K(\mu_\ell)/K$ is totally ramified at every conjugate of λ , the element $[s]'$ is in the inertia group and hence acts trivially on the residue field. Using (b) of the lemma above, and the fact that $(\zeta_\ell - 1)^{[s]'}/(\zeta_\ell - 1) = 1 + \zeta_\ell + \cdots + \zeta_\ell^{s-1} \equiv s \pmod{[b]^{-1}\Lambda}$, one has

$$\frac{g(\chi)}{(\zeta_\ell - 1)^{r_b}} \equiv \left(\frac{g(\chi)}{(\zeta_\ell - 1)^{r_b}} \right)^{[s]'} = \frac{g(\chi)^{[s]'}}{(\zeta_\ell^s - 1)^{r_b}} \equiv \frac{g(\chi)}{(\zeta_\ell - 1)^{r_b}} \cdot \frac{\chi(s)^{-1}}{s^{r_b}} \pmod{[b]^{-1}\Lambda}.$$

By the definition of r_b , the quantity above is a unit modulo $[b]^{-1}\Lambda$, whence we have

$$s^{-r_b} \equiv \chi(s) = \zeta_m \pmod{[b]^{-1}\Lambda}.$$

Since both s^{-r_b} and ζ_m are in K , the congruence must actually hold modulo $[b]^{-1}\Lambda$. Taking $[b]$ of both, we conclude that

$$s^{-r_b} \equiv \zeta_m^b \pmod{\lambda}.$$

Since the primitive m th roots of unity are all distinct modulo λ , we may choose a $c \in (\mathbb{Z}/m)^\times$ with

$$\zeta_m \equiv s^{-\frac{\ell-1}{m}c} \pmod{\lambda}, \quad \text{or equivalently} \quad r_b \equiv \frac{\ell-1}{m}bc \pmod{\ell-1}$$

for all b . Note in particular that we must have $r_b \not\equiv 0 \pmod{\ell-1}$.

Now, since $g(\chi)$ divides ℓ , we must have $r_b = v_{[b]^{-1}\Lambda}(g(\chi)) \leq v_{[b]^{-1}\Lambda}(\ell) = \ell - 1$, and since $g(\chi)$ is integral (by definition), we must have $r_b \geq 0$. This, together with the definition of c , implies that

$$r_b = (\ell - 1) \left\{ \frac{bc}{m} \right\},$$

which in turn shows that

$$\sum_b r_b [b]^{-1} = \sum_b (\ell - 1) \left\{ \frac{bc}{m} \right\} [b]^{-1} = (\ell - 1)[c]\theta$$

annihilates $[\lambda]$, since $\lambda^{(\ell-1)[c]\theta} = (g(\chi)^{\ell-1})$. Taking $[c]^{-1}$ of both sides shows that $(\ell - 1)\theta$ annihilates $[\lambda]$.

While $(\ell - 1)\theta$ is clearly in $\mathbb{Z}[G]$ (since $\ell \equiv 1 \pmod{m}$), we now assume more generally that u is any element of $\mathbb{Z}[G]$ such that $u\theta \in \mathbb{Z}[G]$, and deduce that $u\theta[\lambda]$ is principal.

Let $\gamma = g(\chi)^{[c]^{-1}u} \in K(\mu_\ell)$, so that $\gamma^{\ell-1} = (g(\chi)^{\ell-1})^{[c]^{-1}u} \in K$ by part (e) of the lemma, and

$$(\gamma^{\ell-1}) = (g(\chi)^{\ell-1})^{[c]^{-1}u} = \lambda^{(\ell-1)\theta \cdot u} = (\lambda^{u\theta})^{\ell-1}.$$

This shows that the ideal $(\gamma^{\ell-1})$ of K is a perfect $(\ell - 1)$ th power. We plug this fact into the following lemma.

Lemma. Let L be a number field, and $x \in L^\times$ be such that the ideal (x) is a perfect n th power. Then $L(x^{1/n})/L$ is unramified away from n .

Proof. Let $(x) = I^n$. If v is a place of L that does not divide n , then let \mathcal{O}_v denote the completion of \mathcal{O}_L at v . Let $I\mathcal{O}_v = \pi_v^k \mathcal{O}_v$, where π_v is a uniformizer. Then $x = \pi_v^{nk} \cdot u$, where $u \in \mathcal{O}_v^\times$, and thus $L_v(x^{1/n}) = L_v(u^{1/n})$. Since n is prime to the characteristic of v , the polynomial $X^n - u$ has n distinct roots modulo π_v , and hence any nontrivial automorphism of $L(x^{1/n})/L$ must induce a nontrivial automorphism of the residue fields. This means that the inertia group at v is trivial, and therefore the extension is unramified at v .

Applying the above lemma to $\gamma^{\ell-1}$, we find that $K(\gamma)/K$ is unramified away from $\ell - 1$, and in particular $K(\gamma)/K$ is unramified above ℓ . But $K \subseteq K(\gamma) \subseteq K(\mu_\ell)$, and $K(\mu_\ell)/K$ is totally ramified above ℓ , so we must have $K(\gamma) = K$, i.e. $\gamma \in K$.

Therefore the quality of ideals $(\lambda^{u\theta})^{\ell-1} = (\gamma^{\ell-1}) = (\gamma)^{\ell-1}$ takes place in K . Since the ideal group of K is free abelian, we can undo the $(\ell - 1)$ th powers to conclude that

$$\lambda^{u\theta} = (\gamma),$$

and $u\theta$ kills $[\lambda] \in \mathcal{C}\ell(K)$. Applying this fact to a choice of λ in each ideal class, we find that $u\theta$ kills $\mathcal{C}\ell(K)$, as was to be shown.

§5. Case $F = \mathbb{Q}$, Part III: Cleaning Up.

We now return to the notations in this article which preceded §4. Let χ be an even Dirichlet character modulo p . Stickelberger's theorem applied to $m = p^{n+1}$ shows that if $u \in \Lambda_n[\Delta]$ is such that $u\theta$ is in $\Lambda_n[\Delta]$, then $u\theta$ annihilates X_n . In particular, $u\theta$ must annihilate $X_n(\tau\chi^{-1})$. We are going to show how to remove the u .

Writing $\text{Gal}(F_n/\mathbb{Q}) = \Delta \times \Gamma_n$, and as before $[\cdot]: (1\text{-units mod } p^{n+1}) \xrightarrow{\sim} \Gamma_n$, we must introduce the notation $[[\cdot]]: (\mathbb{Z}/p^{n+1})^\times \xrightarrow{\sim} \Delta \times \Gamma_n$ in order to avoid confusion.

Lemma. For $b \in \mathbb{Z}$ with $(b, p) = 1$, we have $(b - [[b]])\theta \in \mathbb{Z}[\Delta \times \Gamma_n]$.

Proof. Simply write

$$(b - [[b]])\theta = (b - [[b]]) \sum_{a \in (\mathbb{Z}/p^{n+1})^\times} \left\{ \frac{a}{p^{n+1}} \right\} [[a]]^{-1} = \sum_{a \in (\mathbb{Z}/p^{n+1})^\times} \left(b \left\{ \frac{a}{p^{n+1}} \right\} - \left\{ \frac{ab}{p^{n+1}} \right\} \right) [[a]]^{-1},$$

and observe that for any rational number r and integer b , $b\{r\} - \{br\} \in \mathbb{Z}$.

Next, we make the following crucial observation. On the eigenspace $X_n(\chi^{-1}\tau)$, the operator $(b - [[b]])\theta$ acts by $(b - \chi^{-1}\tau(b)[b])\xi_n^\chi$. This follows immediately from the definitions.

For the moment we take, in particular, $n = 0$ and $\psi = 1$. Choose $c = 1 + p$. Then Stieckelberger's theorem says that

$$(1 + p - \tau(1 + p))\xi_0^1 = pB_{\tau^{-1},1} \equiv -1 \pmod{p}$$

annihilates $X_0(\tau)$. This forces $X_0(\tau)$ to be trivial, and by the form of Nakayama's lemma proved in Cathy's talks, that $X(\tau) = 0$, and therefore that $X_n(\tau) = X(\tau)/([\gamma_0]^{p^n} - 1)X(\tau) = 0$ for all $n \geq 0$. This proves the fact asserted just before the proof of the theorem in §3.

From here on, we assume that χ is nontrivial. Choose a primitive $(p-1)$ th root of unity s . Since χ is nontrivial, we must have that $s \not\equiv \chi^{-1}\tau(s) \pmod{p}$. Also, $[s] = [\langle s \rangle] = [1]$, so we get $s - \chi^{-1}\tau(s)[s] \in \mathbb{Z}_p^\times \subset \Lambda_n^\times$. Since $(s - [[s]])\theta$ annihilates $X_n(\chi^{-1}\tau)$, and $s - [[s]]$ acts by a unit, we must have that $e_{\chi^{-1}\tau}\theta = \xi_n^\chi \in \Lambda_n$ annihilates $X_n(\chi^{-1}\tau)$. It is important to underscore this conclusion.

Proposition. With the notations of §3, if χ is nontrivial then ξ_n^χ annihilates $X_n(\chi^{-1}\tau)$.

We now come to the main result of my talks. This result follows quickly from the work we have done, assuming an important hypothesis.

Cyclicness Hypothesis. Assume that X_0^- is cyclic over $\Lambda_0[\Delta]$.

Note that Λ_0 is simply \mathbb{Z}_p , and on the other hand that $\Lambda_0[\Delta]$ projects onto $\Lambda_0[\Delta]^-$ before acting, so one has a couple of easy ways of rewriting the above hypothesis. If p^N is an exponent for X_0^- , then by looking modulo p^N we can rephrase our hypothesis as cyclicness over $\mathbb{Z}[\Delta]$. Nakayama's Lemma implies that the hypothesis is equivalent to X^- being cyclic over $\Lambda[\Delta]$ (or $\Lambda[\Delta]^-$).

A word might also be in order with regards to how often this hypothesis is satisfied. The amazing thing is that *this hypothesis holds in every particular example we have ever checked*. It is a conjecture of Iwasawa–Leopoldt that this is always the case. One may show, using the theory of cyclotomic units, that the cyclicity hypothesis holds whenever X_0^+ is trivial. The claim that X_0^+ is trivial is called Vandiver's conjecture, and it is generally how cyclicness is checked.

Theorem. If the cyclicness hypothesis holds, then so does the main theorem for every character χ of conductor p .

Proof. Let $C \in X^-$ be a generator. Then for every even character χ , the element $e_{\chi^{-1}\tau}C$ generates $X(\chi^{-1}\tau)$. The Λ -module map $\Lambda \rightarrow X(\chi^{-1}\tau)$ given by $x \mapsto x \cdot e_{\chi^{-1}\tau}C$ is surjective; let I_χ be its kernel. Then $X(\chi^{-1}\tau) \approx \Lambda/I_\chi$. We want to show that $I_\chi = (\xi^\chi)$.

By the above proposition, one has $\xi^\chi \in I_\chi$, so that $I_\chi \supseteq (\xi^\chi)$. This gives condition (3) of the lemma of §1.

Since there is exactly one prime above p in each F_n , and this prime is totally ramified in the \mathbb{Z}_p -extension, the easy case of Cathy's talk shows that

$$X_n(\chi^{-1}\tau) = X(\chi^{-1}\tau)/(\gamma^{p^n} - 1) = \Lambda/(I_\chi, \gamma^{p^n} - 1) = \Lambda_n/I_\chi,$$

whence

$$\prod_{\chi \text{ nontriv}} \#\Lambda_n/I_\chi = \prod_{\chi \text{ nontriv}} \#X_n(\chi^{-1}\tau) = \#X_n^- = \prod_{\chi \text{ nontriv}} \#\Lambda_n/\xi^\chi,$$

by the work done in §3. This gives condition (4) of the lemma of §1.

Applying the lemma of §1 now gives us $I_\chi = (\xi^\chi)$, and hence $X(\chi^{-1}\tau) \approx \Lambda/\xi^\chi$. But the Λ -module on the right obviously has characteristic polynomial equal to $f(\chi, T)$, which is precisely the claim of the main theorem, so we are done.