Alternative Proof of the Iwasawa Main Conjecture

Vivian Yu

February 23, 2023

Previously, we have discussed the proof of Iwasawa Main Conjecture following Mazur and Wiles using deep techniques from algebraic geometry. In this talk, we will discuss an alternative proof by Rubin using Kolyvagin's Euler System.

1 Notations

We will first begin by introducing some notations.
Fix a rational prime $p > 2$. For every integer $n \geq 0$, let

$$K_n = \mathbb{Q}(\zeta_{p^{n+1}}), \quad K_\infty = \cup_n K_n$$

Put

$$\Delta = \mathrm{Gal}(K_0/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \quad \textit{and} \quad \Gamma = \mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p,$$

then $\mathrm{Gal}(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$. For $n \geq 1$, write C_n for the p-part of the ideal class group of K_n, E_n for the group of global units of K_n, and $\mathscr{E}_n$ for the group of cyclotomic units of K_n. Write U_n for the group of local units of the completion of K_n above p which are congruent to 1 modulo the maximal ideal, and let $\bar{E}_n$ and V_n denote the closures of $E_n \cap U_n$ and $\mathscr{E}_n \cap U_n$ in U_n. Define the following inverse limits with respect to the norm maps:

$$C_\infty = \varprojlim C_n, \quad E_\infty = \varprojlim \bar{E}_n, \quad V_\infty = \varprojlim V_n, \quad U_\infty = \varprojlim U_n.$$

For $n \leq \infty$, Ω_n be the maximal abelian p-extension of K_n unramified outside primes above p. Write $X_n = \mathrm{Gal}(\Omega_n/K_n)$.

Define the Iwasawa algebra

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(K_n/K_0)] \cong \mathbb{Z}_p[[T]]$$

For every character χ of Δ, define the χ-idempotent

$$\varepsilon_\chi = \frac{1}{p-1} \sum_{\delta \in \Delta} \chi^{-1}(\delta)\delta$$

If Y is a $\mathbb{Z}_p[\Delta]$-module, write $Y(\chi) = \varepsilon_\chi Y$.

2 Formulation of the Main Conjecture over $\mathbb{Q}$

There are several equivalent formulations of the Main Conjecture. The one we will be proving is the following:

Theorem 2.1. *For all even characters χ of Δ, we have the following identity of characteristic ideals:*

$$\mathrm{char}(C_\infty(\chi)) = \mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$$

3 Definition and Properties of Kolyvagin's Euler System

Fix a positive integer m and let $F = \mathbb{Q}(\zeta_m)^+$. Let $\mathscr{S}$ denote the set of positive square free integers divisible only by primes $l \equiv \pm 1 \mod m$ (i.e., by those l which split completely in $F/\mathbb{Q}$). For every $r \in \mathscr{S}$, write

$$G_r = \mathrm{Gal}(F(\zeta_r)/F) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$$

and write $\mathbf{N}_r = \sum_{\tau \in G_r} \tau \in \mathbb{Z}[G_r]$. Because of the natural isomorphism $G_r = \prod_{l|r} G_l$, we have the relation $\mathbf{N}_r = \prod_{l|r} \mathbf{N}_l$. If $l \equiv \pm 1 \mod m$ and $l \nmid r$, the we identify G_l with $\mathrm{Gal}(F(\zeta_{rl})/F(\zeta_r))$, and we write Frob_l for the Frobenius of l in G_r. For every prime $l \equiv \pm 1 \mod m$, fix a generator σ_l of G_l. Define

$$\mathbf{D}_l = \sum_{i=1}^{l-2} i\sigma_l^i \in \mathbb{Z}[G_l].$$

It is easy to see that $\mathbf{D}_l$ satisfies

$$(\sigma_l - 1)\mathbf{D}_l = (l-1) - \mathbf{N}_l.$$

For $r \in \mathscr{S}$, define

$$\mathbf{D}_r = \prod_{l|r} \mathbf{D}_l \in \mathbb{Z}[G_r]$$

Fix a primitive m-th root of unity ζ_m and, for each prime $l \equiv \pm 1$, a primitive l-th root of unity ζ_l. For $r \in \mathscr{S}$ define the Euler system ξ_r of level r by:

$$\xi_r = \left(1 - \zeta_m \prod_{l|r} \zeta_l\right)\left(1 - \zeta_m^{-1} \prod_{l|r} \zeta_l\right)$$

These algebrain integers satisfy the following:

ES1. $\xi_r \in F(\zeta_r)^\times$.

ES2. ξ_r is a cyclotomic unit if $r > 1$.

ES3. $\mathbf{N}_l \xi_r = (\mathrm{Frob}_l - 1)\xi_{r/l}$.

ES4. $\xi_r \equiv \xi_{r/l}$ mod every prime above l.

Proof. **ES1** is clear from definition. **ES2** follows from the classification of cyclotomic units ($\zeta_m = \zeta_m^{m+1}$). **ES3** follows from the fact that

$$\prod_{\eta, \eta^p = 1} (\xi\eta - 1) = \xi^p - 1$$

Here ξ is a cyclotomic unit. **ES4** follows from the fact that $\zeta_l \equiv 1$ modulo all primes above l. □

Fix an odd integer M and define

$$\mathscr{S}_M = \{r \in \mathscr{S} \mid \ r \text{ is divisible only by primes } l \equiv 1 \mod M\}.$$

Now we move on to construct Kolyvagin's derivative classes from the Euler system.

Lemma 3.1. For every $r \in \mathscr{S}_M$ there is a $\kappa_r \in F^\times/(F^\times)^M$ such that

$$\kappa_r \equiv \mathbf{D}_r \xi_r \mod (F(\zeta_r)^\times)^M$$

Proof. We omit the details of the proof but κ_r is of the form

$$\kappa_r = \mathbf{D}_r \xi_r / \beta^M$$

for some $\beta \in F(\zeta_r)^\times$. In fact, κ_r is obtained from $\mathbf{D}_r \xi_r$ under the following sequence of isomorphisms:

$$\mathbf{D}_r \xi_r \in [(F(\zeta_r)^\times)/(F(\zeta_r)^\times)^M]^{G_r} \cong H^1(G_{F(\zeta_r)}, \mu_M)^{G_r} \cong H^1(G_F, \mu_M) \cong F^\times/(F^\times)^M.$$

□

Each κ_r is a principal ideal of F modulo M-th powers of ideals, which can be viewed as a relation in the ideal class group of F if M is big enough. These relations will be used to bound the size of the ideal class group. To do this, we must understand the prime factorizations of these ideals and also how to choose r so as to get useful relations.

Let $\mathcal{O}_F$ denote the ring of integers of F, and write $\mathscr{I} = \bigoplus_\lambda \mathbb{Z}\lambda$ for the group of fractional ideals of F written additively. For every rational prime l, write $\mathscr{I}_l = \bigoplus_{\lambda | l} \mathbb{Z}\lambda$. Therefore, $\mathscr{I} = \bigoplus_l \mathscr{I}_l$. If $y \in F^\times$, let $(y) \in \mathscr{I}$ denote the principal ideal generated by y and let $(y)_l \in \mathscr{I}_l$, $[y] \in \mathscr{I}/M\mathscr{I}$, and $[y]_l \in \mathscr{I}_l/M\mathscr{I}_l$ be the natural projections of (y). Note that $[y]$ and $[y]_l$ are also well defined for $y \in F^\times/(F^\times)^M$.
Let $G = \mathrm{Gal}(F/\mathbb{Q})$.

Lemma 3.2. Suppose l splits completely in F and $l \equiv 1 \mod M$. There is a unique G-equivariant surjection

$$\varphi_l : (\mathcal{O}_F/l\mathcal{O}_F)^\times \to \mathscr{I}_l/M\mathscr{I}_l$$

such that $\varphi_l((1-\sigma_l)x) = [\mathbf{N}_l x]_l$.

Remark 3.0.1. Note that φ_l can be extended to $\{y \in F^\times/(F^\times)^M \mid [y]_l = 0\}$. The Galois cohomological formulation of this Lemma is more enlightening.

The following proposition is due to Kolyvagin and it deals with the prime factorization of (κ_r)

Proposition 3.1. *Suppose $r \in \mathscr{I}_M$ and l is a rational prime.*

(i) If $l \nmid r$, then $[\kappa_r]_l = 0$.

(ii) Otherwise, $[\kappa_r]_l = \varphi_l(\kappa_{r/l})$.

The next Theorem is an application of the Chebotarev Theorem. Together with the proposition above, we will be able to construct all the relations we need in the ideal class group of F. As usual we fix a rational prime $p > 2$ and let C denote the p-part of the ideal class group of F.

Theorem 3.1. *Suppose we are given a class $\mathfrak{c} \in C$, $M \in \mathbb{Z}$ a power of p, a finite G-submodule W of $F^\times/(F^\times)^M$, and a Galois-equivariant map*

$$\psi : W \to \mathbb{Z}/M\mathbb{Z}[G].$$

Then there are infinitely many primes λ of F such that

(i) $\lambda \in \mathfrak{c}$

(ii) If l is the rational prime below λ, then $l \equiv 1 \mod M$ and l splits completely in $F/\mathbb{Q}$.

(iii) $[w]_l = 0$ *for all $w \in W$, and there is a $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that $\varphi_l(w) = u\psi(w)\lambda$ for all $w \in W$.*

4 An Example of Applying Kolyvagin's Method

Proposition 3.1 and Theorem 3.1 were used to bound the χ-part of the p-part of the class group of $F = \mathbb{Q}(\zeta_p)^+$.

5 Preparation for the proof of the Main Conjecture

Now we introduce some tools from Iwasawa theory that will help us with the proof of the main conjecture. In order to use the relations we construct for the ideal class group, we need to know more about the structure of C_n and $\bar{E}_n$ as $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-modules. For any fixed n we know very little, but C_∞ and E_∞ has nice Λ-module structure that can be decent to the n-th level using control theorems.

For every n, let $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ and let I_n denote the ideal of Λ generated by $\gamma^{p^n} - 1$, where γ is the topological generator of Γ. Write

$$\Lambda_n = \Lambda/I_n \cong \mathbb{Z}_p[\mathrm{Gal}(K_n/K_0)].$$

For Y a Λ-module, write

$$Y_{\Gamma_n} = Y/I_nY = Y \otimes_\Lambda \Lambda_n.$$

We study the natural maps induced by projection:

$$X_\infty(\chi)_{\Gamma_n} \to X_n(\chi), \quad C_\infty(\chi)_{\Gamma_n} \to C_n(\chi), \quad U_\infty(\chi)_{\Gamma_n} \to U_n(\chi)$$
$$E_\infty(\chi)_{\Gamma_n} \to \bar{E}_n(\chi), \quad V_\infty(\chi)_{\Gamma_n} \to V_n(\chi)$$

The second one is an isomorphism for all χ, the first, third, and fifth are isomorphisms when χ is nontrivial and even. For the fourth one, under the same condition for χ, the kernel of cokernal are finite and bounded independently of n. The following are some corollaries of the control theorems that we will be using in the proof of the Main Conjecture.

For every character χ of Δ, fix a generator $h_\chi \in \Lambda$ of $\mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$.

Proposition 5.1. *Suppose χ is even and $\chi \neq 1$. There is an ideal $\mathscr{A}$ of finite index in Λ such that for every $\eta \in \mathscr{A}$ and every n, there is a map $\theta_{n,\eta} : \bar{E}_n(\chi)$ such that $\theta_{n,\eta}(V_n(\chi)) = \eta h_\chi \Lambda_n$.*

We already know that $C_\infty(\chi)$ is Λ-torsion and by the structure theorem of Λ-modules pseudo-isomorphic to a module of the form

$$\bigoplus_{i=1}^{k} \Lambda/f_i\Lambda$$

Writing $f_\chi = \prod_{i=1}^k f_i$, we have $\mathrm{char}(C_\infty(\chi)) = f_\chi \Lambda$.

Proposition 5.2. *Let $f_1, \cdots, f_k$ be as above. There is an ideal $\mathscr{B}$ of finite index in Λ and for every n there are classes $\mathfrak{c}_1, \ldots, \mathfrak{c}_k \in C_n(\chi)$ such that the annihilator $\operatorname{Ann}(\mathfrak{c}_i) \subset \Lambda_n$ of $\mathfrak{c}_i$ in $C_n(\chi)/(\Lambda_n \mathfrak{c}_1 + \cdots + \Lambda_n \mathfrak{c}_{i-1})$ satisfies $\mathscr{B} \operatorname{Ann}(\mathfrak{c}_i) \subset f_i \Lambda_n$.*

Lemma 5.1. Let f_χ, h_χ be as above.

(i) For every n, $\Lambda_n/f_\chi\Lambda_n$ and $\Lambda_n/h_\chi\Lambda_n$ are finite.

(ii) There is a positive constant c such that for all n,

$$c^{-1} \leq \frac{\#C_n(\chi)}{\#\Lambda_n/f_\chi\Lambda_n} \leq c, \quad c^{-1} \leq \frac{\#\bar{E}_n(\chi)/V_n(\chi)}{\#\Lambda_n/h_\chi\Lambda_n} \leq c$$

(iii) If $\chi = 1$, then f_χ and h_χ are units.

6 Proof of the Main Conjecture

The proof of the Main Conjecture will be similar to the inductive technique used in the example, except that elements of group rings will be used in place of numbers.

In general, M will be a large power of p. For the proof we fix n and write

$$C := C_n \quad E := E_n \quad V := V_n$$

Let $F := K_n^+ = \mathbb{Q}(\zeta_{p^{n+1}})^+$. When χ is even, we can identify $C(\chi)$ and the χ-component of the ideal class group of F. Let l be a rational prime splitting completely in F. If λ is a prime of F above l, then

$$\mathscr{I}_l(\chi) := \varepsilon_\chi(\mathscr{I}_l \otimes \mathbb{Z}_p)$$

is free of rank 1 over Λ_n, generated by

$$\lambda(\chi) := \varepsilon_\chi \lambda.$$

Define

$$\nu_\lambda = \nu_{\lambda,\chi} : F^\times \to \Lambda_n \quad st.\ \nu_\lambda(w)\lambda(\chi) = \varepsilon_\chi(w)_l$$

Since $\mathscr{I}$ is a free Λ_n-module, ν_λ is well-defined. We write $\bar{\nu}_\lambda : F^\times/(F^\times)^M \to \Lambda_n/M\Lambda_n$ as the corresponding map of ν_λ satisfying $\bar{\nu}_\lambda(w)\lambda(\chi) = \varepsilon_\chi[w]_l$.

For $r \in \mathscr{S}_M$, let $\kappa_r \in F^\times/(F^\times)^M$ be as defined above. The following lemma helps us define a map that will be used in the proof later.

Lemma 6.1. Suppose $r \in \mathscr{S}_M$, $l \mid r$, and λ is a prime of F above l. Let B be the subgroup of the ideal class group C generated by the primes of F dividing r/l. Write $\mathfrak{c} \in C(\chi)$ for the class of $\lambda(\chi)$ and write W for the Λ_n-submodule of $F^\times/(F^\times)^M$ generated by $\varepsilon_\chi\kappa_r$.
If $\eta, f \in \Lambda_n$ are such that the annihilator $\operatorname{Ann}(\mathfrak{c}) \subset \Lambda_n$ of $\mathfrak{c}$ in $C(\chi)/B(\chi)$ satisfies

(i) $\eta \operatorname{Ann}(\mathfrak{c}) \subset f\Lambda_n$,

(ii) $\Lambda_n/f\Lambda_n$ is finite,

(iii) $M \geq \#C(\chi)\#\frac{\mathscr{I}_l(\chi)/M\mathscr{I}_l(\chi)}{\Lambda_n[\varepsilon_\chi\kappa_r]_l}$,

then there is a $\mathrm{Gal}(K_n/K_0)$-equivariant map $\psi : W \to \Lambda_n/M\Lambda_n$ such that

$$f\psi(\varepsilon_\chi\kappa_r) = \eta\bar{\nu}_\lambda(\kappa_r).$$

Proof. The proof is by construction. □

Recall that

$$\mathrm{char}(E_\infty(\chi)/V_\infty(\chi)) = h_\chi\Lambda, \quad \mathrm{char}(C_\infty(\chi)) = f_\chi\Lambda,$$

where $f_\chi = \prod_{i=1}^k f_i$.

Theorem 6.1. *For every even character χ of Δ, we have*

$$\mathrm{char}(C_\infty(\chi)) \mid \mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$$

Proof. When $\chi = 1$, we know from Lemma 5.1 that h_χ and f_χ are both units and the divisibility holds.

Thus, from now on we assume $\chi \neq 1$. Recall that κ_1 is represented by $\xi = (\zeta_{p^n} - 1)(\zeta_{p^n}^{-1} - 1) \in F^\times$ and $\xi(\chi) := \xi^{\varepsilon_\chi}$ generates $V_n(\chi)$. Let $\mathfrak{c}_1, \cdots, \mathfrak{c}_k \in C(\chi)$ be as in Proposition 5.2. Let $\mathfrak{c}_{k+1} \in C(\chi)$ be any element. Fix an ideal $\mathscr{C}$ of finite index in Λ satisfying both Proposition 5.1 and Proposition 5.2. Let $\eta \in \mathscr{C}$ be such that $\Lambda_m/\eta\Lambda_m$ is finite for all m. Let $\theta = \theta_{n,\eta} : \bar{E}(\chi) \to \Lambda_n$ be the map in Proposition 5.1 with this choice of η. WLOG we can normalize θ so that

$$\theta(\xi(\chi)) = \eta h_\chi.$$

According to Lemma 5.1, we can find an integer h such that $p^h \geq \Lambda_n/h_\chi\Lambda_n$. We also require $p^h \geq \Lambda_n/\eta\Lambda_n$. Fix $M = p^{n+(k+1)h}\#C(\chi)$.

We will be applying Theorem 3.1 inductively to choose primes λ_i of F lying above l_i for $1 \leq i \leq k+1$ satisfying:

(a) $\lambda_i \in \mathfrak{c}_i, \quad l_i \equiv 1 \mod M$,

(b) $\bar{\nu}_{\lambda_1}(\kappa_{l_1}) = u_1\eta h_\chi$, $f_{i-1}\bar{\nu}_{\lambda_i}(\kappa_{r_i}) = u_i\eta\bar{\nu}_{\lambda_{i-1}}(\kappa_{r_{i-1}})$ for $2 \leq i \leq k+1$,

where $r_i = \prod_{j\leq i} l_j$ and $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$.

For the first step take $\mathfrak{c} = \mathfrak{c}_1$, $W = (E/E^M)(\chi)$, and

$$\psi : W \to \bar{E}(\chi)/\bar{E}(\chi)^M \xrightarrow{\theta} \Lambda_n/M\Lambda_n \xrightarrow{\varepsilon_\chi} \varepsilon_\chi\mathbb{Z}/M\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$$

Let λ_1 be any prime satisfying Theorem 3.1 with this data, and l_1 the rational prime below λ_1. Theorem 3.1 says they satisfy (a). By Theorem 3.1 and Proposition 3.1, for some $u_1 \in (\mathbb{Z}/M\mathbb{Z})^\times$,

$$\begin{aligned}\bar{\nu}_{\lambda_1}(\kappa_{l_1})\lambda_1(\chi) = \varepsilon_\chi[\kappa_{l_1}]_{l_1} = \varepsilon_\chi\varphi_{l_1}(\kappa_1) = \varepsilon_\chi u_1\psi(\kappa_1)\lambda_1 = u_1\psi(\kappa_1)\lambda_1(\chi) \\ = u_1\theta(\xi(\chi))\lambda_1(\chi) = u_1\eta h_\chi\lambda_1(\chi)\end{aligned}$$

Since $(\mathscr{I}_{l_1}/M\mathscr{I}_{l_1})(\chi)$ is free over $\Lambda_n/M\Lambda_n$, this implies (b).

Now suppose for $2 \le i \le k+1$, we have chosen $\lambda_1, \cdots, \lambda_{i-1}$ satisfying (a) and (b). We want to define λ_i. Using the recursion relation (b), we know that $\bar{\nu}_{\lambda_{i-1}}(\kappa_{r_{i-1}}) \mid \eta^{i-1}h_\chi$. Thus,

$$\#[(\mathscr{I}_{l_1}/M\mathscr{I}_{l_1})(\chi)/\Lambda_n[\kappa_{r_{i-1}}]_{l_{i-1}}] \le \#(\Lambda_n/\eta^{i-1}h_\chi\Lambda_n) \le p^{ih}$$

Let W_i be the Λ_n-submodule of $F^\times/(F^\times)^M$ generated by $\varepsilon_\chi\kappa_{r_{i-1}}$. Apply Lemma 6.1 with $r = r_{i-1}$, $l = l_{i-1}$, η as before and $f = f_{i-1}$, then Proposition 5.2 and Lemma 5.1 ensures that we have a map $\psi_i : W_i \to \Lambda_n/M\Lambda_n$ such that

$$f_{i-1}\psi_i(\varepsilon_\chi\kappa_{r_{i-1}}) = \eta\bar{\nu}_{\lambda_{i-1}}(\kappa_{r_{i-1}})$$

Let λ_i be any prime satisfying Theorem 3.1 with $\mathfrak{c} = \mathfrak{c}_i$, $W = W_i$, and $\psi = \varepsilon_\chi\psi_i$. Then (a) is satisfied. Note that we can again find $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\begin{aligned} f_{i-1}\bar{\nu}_{\lambda_i}(\kappa_{r_i})\lambda_i(\chi) &= f_{i-1}\varepsilon_\chi[\kappa_{r_i}]_{l_i} = f_{i-1}\varphi_{l_i}(\varepsilon_\chi\kappa_{r_{i-1}}) \\ &= f_{i-1}u_i\psi_i(\varepsilon_\chi\kappa_{r_{i-1}})\lambda_i(\chi) = u_i\eta\bar{\nu}_{\lambda_{i-1}}(\kappa_{r_{i-1}})\lambda_i(\chi) \end{aligned}$$

By the same reasoning, we have proven (b) for i.

From the recursive relation (b), we can conclude that in $\Lambda_n/M\Lambda_n$,

$$\eta^{k+1}h_\chi = u\left(\prod_{i=1}^{k} f_i\right)\bar{\nu}_{\lambda_{k+1}}(\kappa_{r_{k+1}})$$

for some $u \in (\mathbb{Z}/M\mathbb{Z})^\times$. Thus, $f_\chi \mid \eta^{k+1}h_\chi$ in $\Lambda_n/p^n\Lambda_n$. Since this is true for every n, we know $f_\chi \mid \eta^{k+1}h_\chi$ in Λ. We can take two η's that are coprime, which would give us $f_\chi \mid h_\chi$. (e.g., take $\mathscr{C} = \mathscr{A} \cap \mathscr{B}$, since $\mathscr{A} \cap \mathscr{B}$ has finite index, there exists a constant c such that T^c and p^c are in $\mathscr{A} \cap \mathscr{B}$. Consider $\eta_1 = T^c - p^{2c}$ and $\eta_2 = T^c - p^{3c}$).

Let $f = \prod_\chi f_\chi$ and $h = \prod_\chi h_\chi$. We want to show $f\Lambda = h\Lambda$, then it will follow from above that $f_\chi\Lambda = h_\chi\Lambda$ for each χ.
If a_n, b_n are two sequence of positive integers, we write $a_n \sim b_n$ to mean a_n/b_n is bounded above and below independent of n. We have the following:

$$\begin{aligned} \#(\Lambda/f\Lambda)_{\Gamma_n} &\sim \prod_\chi \#(\Lambda/f_\chi\Lambda)_{\Gamma_n} \sim \prod_\chi \#C_n(\chi) = \#C_n \\ \#(\Lambda/h\Lambda)_{\Gamma_n} &\sim \prod_\chi \#(\Lambda/h_\chi\Lambda)_{\Gamma_n} \sim \prod_\chi [\bar{E}_n(\chi) : V_n(\chi)] = [\bar{E}_n : V_n] \end{aligned}$$

We know that $\#C_n = [\bar{E}_n : V_n]$ from the analytic class number formula and the non-vanishing of the p-adic regulator for real cyclotomic fields. Thus, $\#(\Lambda/f\Lambda)_{\Gamma_n} \sim \#(\Lambda/h\Lambda)_{\Gamma_n}$. Since $f|h$, this implies $f\Lambda = h\Lambda$. □