Plan:

1) Iwasawa theory of cyclotomic fields

2) Proof of the main conjecture

3) Cup products of cyclotomic units

4) Relationship w/ modular symbols

$F = \mathbb{Q}(\mu_p)$, p odd prime.

$A_F = Cl_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ p-part of class gp.

<u>Def</u> p is regular if $A_F = 0$, otherwise irregular.

$\bar{\mathbb{Q}} \subset \mathbb{C}$, τ complex conj.

$A_F = A_F^+ \oplus A_F^-$, $A_F^{\pm} = \{a \in A_F \mid \tau a = \pm a\}$.

<u>Kummer</u>: 1) $A_F = 0 \Leftrightarrow A_F^- = 0$

2) <u>Conj</u> $A_F^+ = 0$ (Vandiver's conj.)

Buhler–Harvey: true for $p < 39 \cdot 2^{22}$.

<u>Def</u> n^{th} Bernoulli number $B_n = f^{(n)}(0)$

$$f(x) = \frac{x}{e^x - 1}.$$

Facts: 1) $\zeta(1-n) = -\frac{B_n}{n}$, $n \geq 1$.

2) v_p p-adic valn.

$v_p(B_n) < 0 \Leftrightarrow n \equiv 0 \bmod p-1$.

3) $n \equiv m \not\equiv 0 \bmod p-1$, $\frac{B_n}{n} \equiv \frac{B_m}{m} \bmod p$.

Consequences of analytic class # formula:

1) $A_F^- \neq 0 \Leftrightarrow p \mid B_2 B_4 \cdots B_{p-3}$

Exs $37 \mid B_{32}$, $59 \mid B_{44}$, $67 \mid B_{58}$

$691 \mid B_{12}$.

2) $|A_F^+| =$ p-part of $[E_F : C_F]$

$E_F = \mathbb{Z}[\mu_p, \frac{1}{p}]^\times$ p-units

$C_F = \langle 1-\zeta_p^i \mid 1 \leq i \leq p-1 \rangle$ cyclotomic p-units.

$\Delta = \mathrm{Gal}(F/\mathbb{Q})$, $\omega : \Delta \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mu_{p-1}(\mathbb{Z}_p)$

$A_F = \bigoplus_{i=0}^{p-2} A_F^{(i)}$, $A_F^{(i)} = \{a \in A_F \mid \delta a = \omega(\delta)^i a \ \forall \delta \in \Delta\}$.

Theorem (Herbrand–Ribet)

$k \in \mathbb{Z}$ even ≥ 2. $\quad p \mid B_k \iff A_F^{(1-k)} \neq 0$.
$k \leq p-3$

Remark: Mazur–Wiles showed

$$|A_F^{(1-k)}| = p^{v_p(B_{1,\omega^{k-1}})}, \quad B_{1,\omega^{k-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\,\omega^{k-1}(a).$$

$$B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \bmod p.$$

Iwasawa theory $\quad F_r = \mathbb{Q}(\mu_{p^r}),\ r \geq 1$

$F_\infty = \bigcup_r F_r, \quad \chi_p : \tilde{\Gamma} = \mathrm{Gal}(F_\infty/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times$
p-adic cyclotomic char.

$\tilde{\Gamma} = \Gamma \times \Delta \quad \Gamma = \mathrm{Gal}(F_\infty/F) \longrightarrow 1+p\mathbb{Z}_p \cong \mathbb{Z}_p$,

$\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty)$.

$$\tilde{\Lambda} = \mathbb{Z}_p[[\tilde{\Gamma}]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_r/F)]$$

$\Lambda = \mathbb{Z}_p[[\Gamma]], \quad \tilde{\Lambda} = \Lambda[\Delta]$.

$\Lambda \cong \mathbb{Z}_p[[T]]$ by choosing $v \in 1+p\mathbb{Z}_p \cong \mathbb{Z}_p$.
top. generator. $\quad \gamma = [v]$ group elt.

$$\gamma - 1 \longmapsto T$$

Three $\tilde{\Lambda}$-modules:

1) $A_\infty = \varinjlim A_r$, $\quad A_r = Cl_{F_r} \otimes \mathbb{Z}_p$

2) X_∞ unramified Iwasawa module
$= \mathrm{Gal}(L_\infty / F_\infty)$ for L_∞ the max'l unram. abelian pro-p extn. of F_∞.

CFT: $X_\infty \cong \varprojlim_{\text{norm}} A_r$.

3) $\mathfrak{X}_\infty$ p-ramified Iw. mod.
$= \mathrm{Gal}(M_\infty / F_\infty)$ for M_∞ ....
unramified outside p ... of F_∞.

$$\begin{tikzcd}
 & L_\infty \arrow[d, dash, "X_\infty \ni \tau"] \\
 & F_\infty \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] \arrow[uur, dash, bend left, "\mathrm{Gal} \ni \tilde{\sigma}"] & F \ni \sigma
\end{tikzcd}$$

$\tilde{\sigma}|_{F_\infty} = \sigma$

$\sigma : \tau \longmapsto \tilde{\sigma} \tau \tilde{\sigma}^{-1}$.

Relationships:

1) $X_\infty^{2} = X_\infty$ but w/ $\sigma \in \tilde{\hat{\Gamma}}$ acting by σ^{-1}.
is "pseudo-isom." to $A_\infty^\vee$ ($\tilde{\Lambda}$-mod. homom w/ finite kernel & coker.)

2) $\mathfrak{X}_\infty, X_\infty, A_\infty^\vee = \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$
are f.g. Λ-mods.
$X_\infty, A_\infty^\vee$ torsion.

3) $\mathfrak{X}_\infty^+ \cong (A_\infty^-)^\vee(1) \leftarrow$ Tate twist

Iwasawa, Ferrero-Washington:

X_∞^- contains no p-torsion (except 0).

$\rightsquigarrow X_\infty^- \hookrightarrow \bigoplus_{i=1}^{n} \Lambda/(p_i)$ p_i distinguished poly.
(monic & $\equiv T^{\deg p_i} \bmod p$).

$\mathrm{char}_\Lambda X_\infty^- = \left(\prod_{i=1}^{n} p_i\right)$.

(p-adic) L-functions:

$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$

$\rightsquigarrow$ primitive Dirichlet char. $\chi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to \overline{\mathbb{Q}}^\times$

$$\chi(p) = \begin{cases} 0 & \chi \neq 1 \\ 1 & \chi = 1. \end{cases}$$

L-series $L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$, $\operatorname{Re} s > 1$

mero. (analytic if $\chi \neq 1$) continuation to $\mathbb{C}$. $L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \in \mathbb{Q}(\chi)$
$n \geq 1$

$\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ $\quad \chi = \omega^i$ some i.

Take i even.

The values of $L_p(\chi, 1-n) :=$

$$(1 - p^{n-1} \chi\omega^{-n}(p)) L(\chi\omega^{-n}, 1-n)$$

vary "nicely": if $n \equiv m \mod p^{r-1}(p-1)$

$\rightsquigarrow$ $(\chi \neq 1)$ $L_p(\chi, 1-n) \equiv L_p(\chi, 1-m) \mod p^r$.

(Kubota–Leopoldt)

$\rightsquigarrow \exists\, L_p(\chi, s)$ cts. fn. of $s \in \mathbb{Z}_p$.

$L_p(\chi, s)$ given by a measure on $\mathbb{Z}_p^\times$

$$\Theta_n = -\sum_{a=1}^{p^n-1} \left(\frac{a}{p^n} - \frac{1}{2}\right) [a]_n^{-1} \in \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$$

gp. elt.

$$\rightsquigarrow \Theta_\infty = \varprojlim \Theta_n \in \tilde{\Lambda}.$$

$\Theta_\infty^{(1-k)} \in \Lambda$ $\quad$ k even $\not\equiv 0 \mod p-1$.

$\Theta_\infty^{(1-k)}(v^s - 1) = L_p(\omega^k, s)$.

<u>Iwasawa main conj.</u> (Mazur-Wiles):

$\mathrm{char}_\Lambda X_\infty^{(1-k)} = (f_k)$ $\quad$ k even

$$f_k = \begin{cases} \Theta_\infty^{(1-k)} & k \not\equiv 0 \mod p-1 \\ 1 & k \equiv 0 \mod p-1. \end{cases}$$

<u>Equivalent</u> <u>forms</u>:

1) $\mathrm{char}_\Lambda((A_\infty^{(1-k)})^\vee) = (h_k)$

$h_k(v^s - 1) = L_p(\omega^k, -s)$

2) $\mathrm{char}_\Lambda(\mathfrak{X}_\infty^{(k)}) = (g_k)$

$$g_k(\nu^s - 1) = L_p(\omega^k, 1-s)$$

3) $\mathcal{E}_\infty = \varprojlim \mathbb{Z}[\mu_{p^n}, \tfrac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$

$\cup$

$$\mathcal{C}_\infty = \varprojlim \langle 1 - \zeta_{p^n}^i \mid p \nmid i \rangle$$

$$\mathcal{U}_\infty = \varprojlim_n \mathbb{Q}_p(\mu_{p^n})^\times / \mathbb{Q}_p(\mu_{p^n})^{\times p^n}.$$

$$0 \to \mathcal{E}_\infty/\mathcal{C}_\infty \to \mathcal{U}_\infty/\mathcal{C}_\infty \to \mathfrak{X}_\infty \to X_\infty \to 0.$$

Thm (Iwasawa)

$$(\mathcal{U}_\infty/\mathcal{C}_\infty)^{(k)} \cong \Lambda/(g_k)$$

Main conj. $\Leftrightarrow \mathrm{char}_\Lambda(\mathcal{E}_\infty/\mathcal{C}_\infty)^{(k)} = \mathrm{char}_\Lambda X_\infty^{(k)}$.

Greenberg's conj.: $X_\infty^{(k)}$ finite.

$\Longrightarrow (\mathcal{E}_\infty/\mathcal{C}_\infty)^{(k)} = 0$.

Consequence of Greenberg's conj.:

$$X_\infty^{(1-k)} \hookrightarrow \Lambda/(f_k) \longrightarrow \text{fin.} \longrightarrow 0.$$