UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
L—LI—1987

IWASAWA'S MAIN CONJECTURE (A SURVEY)

JAN NEKOVÁŘ, Praha

This paper is intended as an introduction into the basic ideas of cyclotomic fields theory and their relationship to both classical results and modern trends in number theory.

The origins of the subject can be traced back to works of Kummer. At first sight, his results appear completely mysterious. Indeed, how the truth of the Fermat's Last Theorem for the exponent p can be deduced from the good p-adic behaviour of Bernoulli numbers? The answer has two independent ingredients:

(A) Vanishing of certain arithmetic invariants of $\boldsymbol{Z}[\zeta_p]$ implies the FLT.

(B) These invariants are controlled by Bernoulli numbers.

A more sophisticated approach to (B) is due to Iwasawa, who investigated arithmetic of the tower $K_0 \subset K_1 \subset \dots$, where $K_n = \boldsymbol{Q}(\zeta_{p^{n+1}})$. The corresponding arithmetic object, Iwasawa's module, is then conjecturally related to a priori given p-adic analytic functions constructed first by Leopoldt and Kubota that interpolate values of Dirichlet L-functions at non-positive integers. Recently, this conjecture has been proved by Mazur and Wiles (see [4], [17]).

There exists a parallel theory for descent on abelian varieties in towers of number fields ([12], [14]). In this case Main Conjecture is closely related to the famous conjecture of Birch and Swinnerton-Dyer ([5], [8], [19], [20], [22]).

1. Classical results

Let $p > 2$ be a prime, ζ_{p^n} a primitive p^n-th root of unity, $K_n = \boldsymbol{Q}(\zeta_{p^{n+1}})$, $\Delta = G(K_0/\boldsymbol{Q})$, C_n the class group of K_n, A_n its p-primary part, ω: $(\boldsymbol{Z}/p\boldsymbol{Z})^\times \to \mu_{p-1}$ the Teichmüller character defined by $\omega(a) \equiv a \pmod p$.

Let $C_n^\pm$, $A_n^\pm$ be (± 1)-eigenspaces for the action of complex conjugation on C_n and A_n respectively. Dirichlet characters, denoted by χ, are supposed primitive, of conductor f_χ. Bernoulli polynomials and numbers are defined by generating functions:

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

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

General results available to Kummer were the following:

(1.1) Class number formula

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h R}{w |d|^{1/2}}$$

which he proved himself for a cyclotomic field K.

(1.2) Decomposition of the zeta-function of an abelian number field K

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

where characters of $G = G(K/Q)$ are identified with Dirichlet characters.

$$(1.3) \qquad L(1, \chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \bar{\chi}(a) \log |1 - \zeta^a|, \qquad \chi \neq 1 \quad \text{even}$$

$$= \pi i\, \tau(\chi) B_{1,\bar{\chi}}, \qquad \chi \quad \text{odd},$$

where $f = f_\chi$, $\zeta = \zeta_f$, $\tau(\chi) = \sum_{a=1}^{f} \chi(a) \zeta^a$.

$$(1.4) \qquad B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.$$

$$(1.5) \qquad B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right), \quad \text{if} \quad f_\chi \mid F.$$

$$(1.6) \qquad \text{For } n \geq 1 \qquad L(1-n, \chi) = -\frac{B_{n,\chi}}{n}$$

$$\text{and} \qquad B_{n,\chi} \neq 0 \quad \text{iff} \quad n \equiv \delta \bmod 2,$$

where $\delta = 0$ for χ even, 1 for χ odd $\left(\text{with the exception of } B_1 = -\frac{1}{2}\right)$.

Applying (1.2) to the fields K_0, $K_0^+ = Q(\zeta_p + \zeta_p^{-1})$ gives

$$(1.7) \qquad \# C_0^- = \frac{h_K}{h_{K^+}} = 2p \prod_{i \text{ odd}} \left(-\frac{1}{2} B_{1,\omega^i}\right),$$

since $\hat{G}(K_0/Q) = \{1, \omega, \ldots, \omega^{p-2}\}$, $\hat{G}(K_0^+/Q) = \{1, \omega^2, \ldots, \omega^{p-3}\}$.

Kummer's foundational achievements are the following:

Congruences: Let m, n be even positive integers, $p - 1 \nmid n$, $m \equiv n \pmod{p^k (p-1)}$. Then

(1.8a) $$B_{1,\omega^{n-1}} \equiv \frac{B_n}{n} (\operatorname{mod} p)$$

(1.8b) $$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} (\operatorname{mod} p^{k+1}).$$

Results on the Fermat's Last Theorem:

(1.9a) $A_0^- = 0$ iff for all even i, $2 \le i \le p-3$, $B_i \not\equiv 0 (\operatorname{mod} p)$

(1.9b) $A_0^- = 0 \Rightarrow A_0 = 0$

(1.9c) $A_0 = 0$ implies FLT for exponent p.

Note that (1.9a) is an immediate consequence of (1.7) and (1.8a).

A more detailed information on the group A_0^- is provided by the classical Stickelberger's theorem (see [2], [10], [25]):
(1.10) For any integer c prime to p the element

$$\theta_c = (c - \sigma_c)\sum_{a=1}^{p-1} \frac{a}{p} \sigma_a^{-1} \in \mathbf{Z}[G(K_0/\mathbf{Q})]$$

annihilates A_0; here σ_a: $\zeta_a \mapsto \zeta_p^a$ corresponds to a under the Artin's isomorphism $(\mathbf{Z}/p\mathbf{Z})^\times \xrightarrow{\sim} G(K_0/\mathbf{Q})$.

If Δ is a finite abelian group and $\chi \in \hat{\Delta}$ its character, put

$$\varepsilon_\chi = \frac{1}{\# \Delta} \sum_{a \in \Delta} \chi^{-1}(a)\, a \in \bar{\mathbf{Q}}[\Delta]$$

Then any $\bar{\mathbf{Q}}[\Delta]$-module M decomposes into $M = \bigoplus_{\chi \in \hat{\Delta}} \varepsilon_\chi M$ and

$$\varepsilon_\chi M = \{m \in M;\ \forall\, a \in \Delta,\ {}^a m = \chi(a) m\}.$$

The same is true if one takes any ring containing values of all χ' s and $(\# \Delta)^{-1}$ instead of $\bar{\mathbf{Q}}$. In particular, for $\Delta = G(K_0/\mathbf{Q})$, $\hat{\Delta} = \{1, \omega, \dots, \omega^{p-2}\}$ and $\varepsilon_{\omega^i} \in \mathbf{Z}_p[\Delta]$. It follows that

$$A_0^+ = \bigoplus_{i\,\text{even}} (A_0)_{\omega^i}, \quad A_0^- = \bigoplus_{i\,\text{odd}} (A_0)_{\omega^i}$$

As θ_c acts on $(A_0)_{\omega^i}$ by multiplication on $(c - \omega^i(c))B_{1,\omega^{-i}}$, Stickelberger's theorem implies that
(1.11) $(A_0)_\omega = 0$ and for i odd, $3 \le i \le p-2$, $B_{1,\omega^{-i}}$ kills $(A_0)_{\omega^i}$. but gives no information on A_0^+.

From (1.8a) and (1.11) it follows that
(1.12) (Pollaczek, Herbrand) if for some odd $i \le p-2\,(A_0)_{\omega^i} \neq 0$, then B_{p-i} is divisible by p.

It took fifty years to prove the converse:
(1.13) (Ribet [21]) If for i odd, $3 \leq i \leq p-2$, $p \backslash B_{p-i}$, then $(A_0)_{\omega^{-i}} \neq 0$. Ribet's prof required deep results on representations of $G(\bar{Q}/Q)$ related to modular forms and can be considered as a first step towards the proof of Iwasawa's Main Conjecture.

2. p-adic L-functions

Kummer's congruences (1.8) suggests that the function

$$f(n) = (1 - p^{n-1})\frac{B_n}{n} = -(1 - p^{n-1})\,\zeta(1-n)$$

might be extended to a function of a p-adic variable $s \in \boldsymbol{C}_p$. This is indeed the case; in fact, also values of Dirchlet L-series at negative integers admit p-adic interpolation. We recall two elementary constructions of p-adic L-functions.

Construction 1 (see [25]) starts with the Hurwitz function

$$\zeta(s, a) = \sum_{n=0}^{\infty} (n + a)^{-s} \quad \text{satisfying}$$

$$\zeta(1 - n, a) = -\frac{B_n(a)}{n} \quad \text{for} \quad 0 < a \leq 1, \quad n \geq 1. \tag{2.1}$$

Suppose χ is a Dirichlet character and F an integer divisible by the conductor of χ. Then (2.1) together with (1.4) imply

$$L(1 - n, \chi) = -\frac{F^{n-1}}{n}\sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) = -\frac{1}{nF}\sum_{a=1}^{F} \chi(a) a^n \sum_{i=0}^{\infty}\binom{n}{i} B_i \left(\frac{F}{a}\right)^i.$$

One is temped to substitute $1 - s$ for n in the last expression and view s as a p-adic variable. Before doing this, however, one must define what a^s would mean in this context. Note that any $a \in \boldsymbol{Z}_p^+$ can be decomposed into $a = \omega(a)\langle a\rangle$ with $\langle a\rangle \equiv 1 \pmod{p}$. The series

$$\langle a\rangle^s = \sum_{i=0}^{\infty}\binom{s}{i}(\langle a\rangle - 1)^i$$

is convergent for $|s|_p < p^{1 - \frac{1}{p+1}}$.

This justifies the following definition: let χ be a Dirichlet character with values in $\bar{\boldsymbol{Q}}_p$, F any multiple of p and f_χ. Put

$$L_p(s, \chi) = \frac{1}{(s-1)F}\sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a)\langle a\rangle^{1-s} \sum_{i=0}^{\infty}\binom{1-s}{i} B_i \left(\frac{F}{a}\right)^i. \tag{2.2}$$

Properties of $L_p(s)$ (see [10], [25]):

(L1) The series (2.2) defines a meromorphic function of $s \in \boldsymbol{C}_p$, $|s|_p < p^{1-\frac{1}{p+1}}$, the only simple pole being at $s = 1$ for $\chi = 1$ when $\operatorname*{Res}_{s=1} L_p(s, 1) = 1 - \frac{1}{p}$.

(L2) For $n \geq 1$

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

$$= -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}.$$

(L3) If $\chi \neq 1$ and $p^2 \nmid f_\chi$, then

$$L_p(s, \chi) = \sum_{i=0}^{\infty} a_i(s-1)^i, \quad |a_0|_p \leq 1, \quad p | a_i \quad \text{for} \quad i \geq 1.$$

(L4) If χ is an odd character, then, by (1.6) and (L2), $L_p(s, \chi)$ is identically zero.

If χ is even, then $L_p(1-n, \chi) \neq 0$ for all $n \geq 1$.

It may be surprising that the only information concerning Bernoulli numbers necessary for a proof of (L1)—(L4) is the theorem of Clausen- von Staudt on denominators of B_i' s. On the other hand, Kummer's congruences immediately follow from (L2) and (L3):

(a) $$B_{1,\omega^{n-1}} = -L_p(0, \omega^n) \equiv -L_p(1-n, \omega^n) \equiv \frac{B_n}{n} (\operatorname{mod} p)$$

(b) If $m \equiv n \operatorname{mod} (p-1)p^k$, then $L_p(s, \omega^m) = L_p(s, \omega^n)$ and

$$(1 - p^{m-1})\frac{B_m}{m} = -L_p(1-m, \omega^m) = -L_p(1-m, \omega^n) \equiv \text{(by (L3))}$$

$$\equiv -L_p(1-n, \omega^n) \equiv (1 - p^{n-1})\frac{B_n}{n} (\operatorname{mod} p^{k+1}).$$

p-adic *L*-functions inherit certain properties of their complex counterparts, but not all of them:

(L5) If χ is an even Dirichlet character, then

$$L_p(1, \chi) = -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f} \bar{\chi}(a) \log_p(1 - \zeta^a),$$

where $\bar{\chi} = \chi^{-1}, f = f_\chi$, $\zeta = \zeta_f$, $\tau(\chi) = \sum_{a=1}^{f} \chi(a)\zeta^a$.

(L6) If K is a totally real abelian number field, then

$$\prod_{\substack{\chi\in G\\ \chi\neq 1}}\left(1-\frac{\chi(p)}{p}\right)^{-1}L_p(1,\chi)=\frac{2^{n-1}h\,R_p}{d^{1/2}},$$

$G=G(K/\mathbf{Q})$, $n=[K:\mathbf{Q}]$ and R_p is a p-adic analogue of the regulator.

(L7) Uhlike the complex case, there is no functional equation for the p-adic L-function of the form

$$f(s)L_p(s,\chi)=h_\chi(s)g(s)L_p(1-s,\bar{\chi})$$

with f, g non-zero meromorphic, independent of χ and $h_\chi(s)$ nonvanishing.

Note that (L6) for $K=K_0^+$ tells us that

$$L_p(1,\omega^j)=\frac{2^{n-1}h^+R_p^+}{\sqrt{d^+}}$$

As for each unit η in K_0^+ one has $\log_p\eta\in\mathbf{Z}_p\otimes\mathcal{O}^+$, where $\mathcal{O}^+$ denotes the ring of integers in K_0^+, it follows that $\dfrac{R_p^+}{\sqrt{d^+}}$ is p-integral. This means, by the above formula, that $h^+=\#\,C_0^+$ is divisible by p iff $L_p(1,\omega^j)$ is, for some even j, $2\leq j\leq p-3$. By (L3) $L_p(1,\omega^j)\equiv L_p(0,\omega^j)\equiv -B_{1,\omega^{j-1}}\,(\mathrm{mod}\,p)$, hence, in view of (1.7), $p|h^+$ implies $p|h^-$, which proves Kummer's theorem (1.9b).

Construction 2 is based on p-adic integration and is due to Iwasawa, save for a language.

Let $\ldots\leftarrow X_{n-1}\xleftarrow{\pi_n}X_n\leftarrow\ldots$ be a projective system of finite sets with all π_n surjective, $X=\varprojlim X_n$ with the projective limit topology. A distribution on the space X with values in an abelian group A is a finitely additive functional ϕ on compact-open subsets of X with values in A, or, equivalently, a system (ϕ_n) of functions $\phi_n\colon X_n\to A$ satisfying

$$\phi_{n-1}(x)=\sum_{\pi_n(y)=x}\phi_n(y)$$

(indeed, if $p_n\colon X\to X_n$ is the canonical projection, then

$$\phi_n(x)=\phi(p_n^{-1}(x)))\,.$$

Distributions form an abelian group $\mathrm{Dist}\,(X,A)$. Assume that A is a subring of $\mathbf{C}_p$ complete in the p-adic norm. Then ϕ is called a measure iff there is a constant K such that $|\phi_n(x)|_p\leq K$ for all n, $x\in X_n$. If ϕ is a measure, then there is a unique A-linear continuous mapping

$$\int_X \mathrm{d}\phi\colon C(X,A)\to A_p$$

such that

$$\int_X \text{(characteristic function of U)}\ d\phi = \phi(U)$$

for all compact-open subsets U of X. Here $C(X, A)$ denotes the space of all continuous functions $f\colon X \to A$ equipped with the norm

$$\|f\| = \sup_{x \in X} |f(x)|_p .$$

In the construction of p-adic L-functions, a crucial role is played by Bernoulli distributions on the space $X = \varprojlim (\mathbf{Z}/dp^{n+1}\mathbf{Z})^\times$, where d is an integer prime to p. They are defined by the formula

$$\mathscr{B}_k(x_n) = (dp^{n+1})^{k-1} B_k\left(\left\{\frac{x_n}{dp^{n+1}}\right\}\right),$$

where $\{a\}$ denotes the fractional part of a. Though $\mathscr{B}_k$ is not a measure, it can be smoothed as follows:
take an integer c prime to dp and put

$$E_{k,c}(x_n) = \mathscr{B}_k(x_n) - c^k \mathscr{B}_k(c^{-1}x_n)$$

for $x_n \in X_n$ (c^{-1} is the inverse of c in X).

$E_{k,c}$ is a measure. Suppose χ is a p-adic (with values in $\bar{\mathbf{Q}}_p$) Dirichlet character of conductor $f_\chi = dp^m$. Denote by $x\colon X \to \mathbf{Z}_p^\times$ the canonical projection and for $a \in X$ put $\omega(a) = \omega(x(a))$, $\langle a \rangle = \langle x(a) \rangle$. One can show by tedious though elementary computations that the following fact holds:

(D1) $$E_{k,c} = kx^{k-1} E_{1,c} .$$

This has as an immediate consequence

(D2) $$\int_X \chi\omega^{-1}(a)\langle a \rangle^{k-1}\, \mathrm{d}E_{1,c} = -(1 - \chi(c)\langle c \rangle^k) L_p(1-k, \chi) .$$

Indeed, the former integral is by (D1) equal to

$$\frac{1}{k} \int \chi\omega^{-k}(a)\, \mathrm{d}E_{k,c} = \frac{1}{k}(1 - \chi\omega^{-k}(c)c^k) \int \chi\omega^{-k}\, \mathrm{d}\mathscr{B}_k =$$

(this is defined since $\chi\omega^{-k}$ is locally constant on X)

$$= \frac{1}{k}(1 - \chi(c)\langle c \rangle^k) B_{k, \chi\omega^{-k}}$$

and by (L2) we are done.

By continuity, for all $s \in \boldsymbol{C}_p$, $|s|_p < p^{1-\frac{1}{p-1}}$

$$(2.3) \qquad \int_X \chi\omega^{-1}(a)\langle a\rangle^{s-1}\,\mathrm{d}E_{1,c} = -(1-\chi(c)\langle c\rangle^s)L_p(1-s,\chi).$$

An easy argument that this integral is a function holomorphic for $|s|_p < p^{1-\frac{1}{p-1}}$, which gives an independent construction of the function $L_p(s,\chi)$ and at the same time proves properties (L1), (L2).

Iwasawa's original construction used instead of $E_{k,c}$ its Fourier transform. The general nonsense is the following:

Suppose that $X_n = \Delta \times \Gamma_n$ is an abelian group with Γ_n isomorphic to $\boldsymbol{Z}/p^n\boldsymbol{Z}$, $X = \varprojlim X_n = \Delta \times \Gamma$, $\Gamma = \varprojlim \Gamma_n \simeq \boldsymbol{Z}_p$ and the order of Δ is prime to p. Let γ_0 be a fixed generator of Γ, F a finite extension of $\boldsymbol{Q}_p$, $\mathcal{O}$ the ring of integers in F. Fourier transform associates to any distribution $\phi = (\phi_n) \in \mathrm{Dist}(X,\mathcal{O})$ the sequence

$$\hat{\phi} = (\hat{\phi}_n), \quad \hat{\phi}_n = \sum_{x\in X_n} \phi_n(x)x \in \mathcal{O}[X_n].$$

From the distribution relation it follows that

$$\hat{\phi} \in \mathcal{O}[[X]] = \varprojlim \mathcal{O}[X_n] = \mathcal{O}[\Delta] \otimes_{\mathcal{O}} \mathcal{O}[[\Gamma]],$$

where the pro-finite group ring $\mathcal{O}[[\Gamma]]$ is isomorphic to the formal power series ring $\mathcal{O}[[T]]$ via $\gamma_0 \mapsto 1+T$. If all roots of unity of order $\#\Delta$ are contained in $\mathcal{O}$, then the group ring $\mathcal{O}[\Delta] = \bigoplus_{\theta\in\hat{\Delta}} \mathcal{O}\varepsilon_\theta$ and $\hat{\phi} = (\hat{\phi}_\theta)_{\theta\in\hat{\Delta}}$, $\hat{\phi}_\theta \in \mathcal{O}[[T]]$.

It is easy to see that

(D3) $\hat{}: \mathrm{Dist}(X,\mathcal{O}) \to \mathcal{O}[\Delta] \otimes_{\mathcal{O}} \mathcal{O}[[\mathrm{T}]]$ is an isomorphism.

(D4) Regarding ϕ as a measure on $\boldsymbol{Z}_p$ via the isomorphism $s \mapsto \gamma_0^s$, $\boldsymbol{Z}_p \rightleftarrows \Gamma$, its Fourier transform is equal to

$$\hat{\phi}_\theta(T) = \int_{\Delta\times \boldsymbol{Z}_p} \theta(\delta)(1+T)^s\,\mathrm{d}\phi(\delta,s).$$

Return back to $X_n = (\boldsymbol{Z}/dp^{n+1}\boldsymbol{Z})^\times$. In this case

$$\Delta = (\boldsymbol{Z}/dp\boldsymbol{Z})^\times, \quad \Gamma = 1 + p\boldsymbol{Z}_p.$$

Fix for the moment $\theta \in \hat{\Delta}$, a character ψ of $1+p\boldsymbol{Z}_p$ of finite order, $s \in \boldsymbol{Z}_p$. Assume that $\mathcal{O}$ contains all roots of unity of order $\#\Delta$. Then it follows from (D5) that

$$(2.4) \qquad \hat{\phi}_\theta(\psi(\gamma_0)\gamma_0^s - 1) = \int_{\Delta\times\Gamma} \theta(a)\psi(a)\langle a\rangle^s\,\mathrm{d}\phi.$$

Combining (2.3) and (2.4), one obtains

$$(2.5) \qquad (\hat{E}_{1,c})_{\theta\omega^{-1}}(\psi(\gamma_0)\gamma_0^{-s} - 1) = (\psi(c)\langle c\rangle^{1-s} - 1)L_p(s, \theta\psi).$$

Set $\gamma_0 = c = 1 + p$, $\zeta\psi = \psi^{-1}(1 + p)$ (which is a p^n-th root of unity), $g_\theta(T) = = (\hat{E}_{1,1+p})_{\theta\omega^{-1}}\left(\frac{1}{1+T} - 1\right)$, $h(T) = \frac{1+p}{1+T} - 1$ and $f_\theta = g_\theta h^{-1}$. It can be shown that for $\theta \neq 1$ f_θ lies in $\mathcal{O}[[T]]$. Resuming what has been said,

(L8) If $\theta \in \hat{\Delta}$, $\theta \neq 1$ is an even character, then there exists a power series $f_\theta \in \mathcal{O}[[T]]$ such that for each character ψ of $1 + p\boldsymbol{Z}_p$ of finite order

$$L_p(s, \theta\psi) = f_\theta(\psi(1 + p)^{-1}(1 + p)^s - 1).$$

In the special case $d = 1$, formal manipulations with class number formulae and (L8) give the following result:

$$(2.6) \qquad \frac{h_n^-}{h_0^-} = \frac{\# C_n^-}{\# C_0^-} = \prod_{\substack{j=2 \\ j \text{ even}}}^{p-3} \prod_{\zeta^{p^n}=1} f_{\omega^j}(\zeta - 1) \times (p\text{-adic unit}).$$

By the Weierstrass Preparation Theorem for $f(T) = \prod_j f_{\omega^j}(T)$

$f(T) = p^\mu P(T)\,U(T)$, where $U(T)$ is a unit of $\boldsymbol{Z}_p[[T]]$ and $P(T) = T^\lambda + a_{\lambda-1}T^{\lambda-1} + \ldots + a_0$ is a distinguished polynomial, i.e. $p|a_i$ for $i = 0, \ldots, \lambda - 1$. If ζ is a primitive p^n-th root of unity, then for n large enough

$$\mathrm{ord}_p(P(\zeta - 1)) = \mathrm{ord}_p((\zeta - 1)^\lambda).$$

It follows then from (2.6) that

$$(2.7) \qquad \mathrm{ord}_p h_n^- = \mu p^n + \lambda n + \nu \qquad \text{for } n \geq n_0.$$

This is also a consequence of the general theory of $\boldsymbol{Z}_p$ — extensions, as explained below.

3. Iwasawa's theory of Z_p-extensions

Pursuing an analogy with the function field case, Iwasawa investigated arithmetic in a tower $F_0 \subset F_1 \subset \ldots \subset F_\infty = \bigcup_{n=0}^{\infty} F_n$ of number fields with $G(F_n/F_0) \simeq \simeq \boldsymbol{Z}/p^n\boldsymbol{Z}$, $G(F_\infty/F_0) = \Gamma \simeq \boldsymbol{Z}_p$. Let A_n be the p-primary part of the class group of F_n. Then A_n forms a projective system under the norm maps. Iwasawa's module of the extension F_∞/F_0 is the limit $X = \varprojlim A_n$. X is a compact module over $\Lambda = \boldsymbol{Z}_p[[\Gamma]] \simeq \boldsymbol{Z}_p[[T]]$.

Basic results of Iwasawa's theory are the following (see [2], [9], [10], [25]):

(IW1) X is a finitely generated Λ-module.

(IW2) For each Λ-module M of finite type there is a homomorphism $f\colon M \to \Lambda^r \oplus (\oplus \Lambda/p^{m_i}) \oplus (\Lambda/(g_i(T)))$ with finite kernel and cokernel (such f is called quasiisomorphism), where $g_i(T) = T^\lambda + a_{\lambda-1}T^{\lambda-1} + \ldots + a_0$ is an irreducible distinguished polynomial, $p|a_i$, $0 \leq i \leq \lambda - 1$.

(IW3) X has no free part, i.e. in the notation of (IW2) $r = 0$. In this case $g = P^{\Sigma m_i}\Pi g_i$ is independent of the quasiisomorphism chosen (up to a p-adic unit) and is called the characteristic polynomial of X. This polynomial carries allmost all information on A_n.

Of course, all this depends on a fixed generator of Γ which determines the isomorphism $\boldsymbol{Z}_p[[\Gamma]] \simeq \boldsymbol{Z}_p[[T]]$.

(IW4) Assume there is only one prime ramified in F_∞/F_0 and assume it is totally ramified. Then

$$A_n \simeq X/\omega_n X, \quad \omega_n = (1+T)^{p^n} - 1 .$$

(IW5) For n sufficiently large,

$$\# A_n = p^e n \quad \text{with} \quad e_n = \mu p^n + \lambda n + \nu,$$

where $\mu = \Sigma m_i$, $\lambda = \deg g$ in (IW3).

Under the hypotheses of (IW4), the above assertion follows from (IW3) and the computation of $M/\omega_n M$ for standard Λ-modules Λ/p^m and Λ/g.

(IW6) (Ferrero-Washington [7], see also [18]):
suppose $F_0/\boldsymbol{Q}$ is abelian and F_∞/F_0 is the cyclotomic $\boldsymbol{Z}_p$-extension. Then $\mu = 0$, thus

$$X \simeq \boldsymbol{Z}_p^\lambda \oplus \text{finite } p\text{-group} .$$

In the case of the basic cyclotomic extension $K_n = \mathrm{Q}(\zeta_{p^n+1})$ X has a decomposition $X = \bigoplus_{\theta \in \hat{\Delta}} \varepsilon_\theta X$ $(\Delta = G(K_0/\boldsymbol{Q}))$. From what has been said it follows that $\varepsilon_\theta X$ is quasiisomorphic to $\bigoplus_i \Lambda/g_i^\theta(T)$ and has a characteristic polynomial $g_\theta(T) = \prod_i g_i^\theta(T)$.

(IW7) Let i be even, $2 \leq i \leq p-3$, let $f_{\omega^i} \in \boldsymbol{Z}_p[[T]]$ be the power series associated to the p-adic L-function $L_p(s, \omega^i)$ by (L8). Then $f_{\omega^i}(T)$ kills $\varepsilon_{\omega^{1-i}}X$. This is essentially Stickelberger's theorem for all n.

(IW8) Suppose Vandiver's conjecture $A_0^+ = 0$ is true. Then $X^+ = \bigoplus_{\theta \text{even}} \varepsilon_\theta X = 0$ and $\varepsilon_{\omega^{1-i}}X = \Lambda/f_{\omega^i}(T)$ for i even, $2 \leq i \leq p-3$.

Both Vandiver's conjecture and the statement of (IW8) seem to be inaccess-

ible at the moment. Iwasawa's Main Conjecture is a weaker form of (IW8), but still a very strong generalization of all results mentioned in section 1:
(IMC): for each i even, $2 \leq i \leq p-3$, $g_{\omega^{1-i}}(T)$ and $f_{\omega^i}(T)$ generate the same ideal in Λ.

Below we shall list the most interesting consequences of the Main Conjecture:

(i) For each i odd, $i \not\equiv 1 \bmod (p-1)$

$$\varepsilon_{\omega^i}A_0 = p\text{-part of } B_{1,\omega^{-i}} = |B_{1,\omega^{-1}}|_p^{-1}.$$

(ii) Let E_0 be the group of units in K_0, let B_0 be the group generated by $\zeta = \zeta_p, \dfrac{1-\zeta^i}{1-\zeta}$ $(i = 1, \ldots, p-1)$. Then for each i even, $2 \leq i \leq p-3$

$$\varepsilon_{\omega^i}A_0 = p\text{-part of } \varepsilon_{\omega^i}(E_0/B_0)$$

(iii) For each n odd, $n \geq 1$, the order of $K_{2n}\boldsymbol{Z}$ is divisible by $w_{n+1}(\boldsymbol{Q})\zeta(-n)$, where $w_k(F)$ is the largest integer m for which $G(F(\zeta_m)/F)$ is killed by k.

This conjecture has been proved by Mazur and Wiles [17] (see also [4]). The germ of their proof can be found in [21], where (1.13) is proved: under the hypothesis that p/B_{p-i} for some odd i Ribet constructs a Galois representation ϱ: $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \to GL_2(\boldsymbol{F}_q)$ with the following properties:
$\varrho = \begin{pmatrix} 1 & * \\ 0 & \omega^i \end{pmatrix}$ with $*$ non-trivial, ϱ unramified at p, trivial on $\operatorname{Ker} \omega^i \cap$ decomposition group of p. By class field theory, fixed field of $\operatorname{Ker} \varrho$ is then a non-trivial unramified abelian p-extension corresponding to a non-zero element in $\varepsilon_{\omega^i}A_0$. ϱ comes from the representation associated to a suitable cusp form f of weight 2 for $\Gamma_1(p)$. This cusp form is an eigenform for Hecke operators and is congruent to the Eisenstein series corresponding to ω^i. Properties of ϱ then follow from the relation of Eichler and Shimura and from the study of the reduction of the factor of the Jacobian of $X_1(p)$ corresponding to the form f at p.

4. Final remarks

We have presented here only the basic facts of the theory of cyclotomic fields. More detailed information can be found in [2], [9], [10], [25]. p-adic L-functions can be defined over an arbitrary totally real number field (see [1], [6], [23]). Also the Main Conjecture can be formulated over any such a field ([2], [25]). If the field in question is abelian over $\boldsymbol{Q}$ then it has been proved in [17].

Analytic p-adic objects conjecturally related to Mazur's theory mentioned in the introduction are constructed in [11], [13], [15], [16], [24].

REFERENCES

1. Cassou—Nogues, P.: Valeurs aux entiers négatifs des fonctions zeta et fonctions zeta p-adiques. Invent. Math. 51 (1979), 29—59.
2. Coates, J.: p-adic L-functions and Iwasawa's theory. Algebraic Number Fields, ed. by A. Frohlich, 269—353. Academic Press, London, 1977.
3. Coates, J.: The arithmetic of elliptic curves with complex multiplication. Proc ICM 1978 Helsinki, 351—355.
4. Coates, J.: The work of Mazur—Wiles on cyclotomic fields, Sém. Bourbaki 1980/81, No 575, LNM 901, 220—242.
5. Coates, J.—Goldstein, C.: Some remarks on the main conjecture for elliptic curves with complex multiplication, Amer. J. Math. 105 (1983), No 2, 337—366.
6. Deligne, P.—Ribet, K.: Values of abelian L-functions at negative integers over totally real fields, Invent. Math. 59 (1980), 227—286.
7. Ferrero, B.—Washington, L.: The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. 109 (1979) 377—395.
8. Greenberg, R.: On the Birch and Swinnerton—Dyer conjecture, Invent. Math. 72 (1983), No 2, 241—265.
9. Iwasawa, K.: On Z_l-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246—326.
10. Lang, S.: Cyclotomic Fields I, II, GTM, Springer, New York, 1978, 80.
11. Lichtenbaum, S.: On p-adic L-functions associated to elliptic curves, Invent. Math. 56 (1980), 19—55.
12. Main, Yu. I.: Cyclotomic fields and modular curves, Uspekhi Mat. Nauk 26 (1971), No 6, 7—78.
13. Main, Yu. I.—Višik, M.: p-adic Hecke series of imaginary quadratic fields, Mat. Sbornik 95 (137) (1974), 357—383.
14. Mazur, B.: Rational points of abelian varieties in towers of number fields, Invent. Math. 18 (1972), 183—266.
15. Mazur, B.: On the arithmetic of spoecial values of L-functions, Invent. Math. 55 (1979), 207—240.
16. Mazur, B.—Swinerton-Dyer, H.: Arithmetic of Weil curves, Invent. Math. 25 (1974), 1—61.
17. Mazur, B.—Wiles, A.: Class fields of abelian extensions of Q, Invent. Math. 76 (1984), No 2, 179—330.
18. Oesterlé, J.: Travaux de Ferrero et Washington sur le nombre de classes d'idéaux des corps cyclotomiques, Sém. Bourbaki 1978/79, No 535, LNM 770, 170—182, Springer, 1980.
19. Perrin—Riou, B.: Groupe de Selmer d'une courbe elliptique a multiplication complexe, Compositio Math. 43 (1981), 387—417.
20. Perin—Riou B.: Descente infinite et hauter p-adic sur les courbes elliptiques a multiplications complexe, Invent. Math. 70, (1983), 369—398.
21. Ribet, K.: A modular construction of unramified p-extensions of $Q(\mu_p)$, Invent. Math. 34 (1976), 151—162.
22. Schneider, P.: Iwasawa L-functions of varieties over algebraic number fields, Invent. Math. 71 (1983), No 2, 251—293.

23. Serre, J.—P.: Formes modulaires et functions zeta p-adiques, Modular functions of one variable III, 191—268, LNM 350, Springer, 1973.

24. Tilouine, J.: Fonctions L p-adiques a deux variables et Z_p^2-extensions, C.R. Acad. Sci. Paris, t. 297, Série I, No 2, 81—84.

25. Washington, L.: Introduction into Cyclotomic Fields, GTM, Springer, 1982.

Author's address:

Jan Nekovář
Dept. Math. Analysis
Fac. Math. Phys. Charles University
Sokolovská 83
186 00 Praha 8

Received: 11. 12. 1985

SOUHRN

O IWASAWOVĚ HLAVNÍ HYPOTÉZE

Jan Nekovář Praha

Práce seznamuje se základními pojmy teorie kruhových těles, ukazuje na souvislosti s klasickými výsledky i s dosud neřešenými problémy.

РЕЗЮМЕ

ГЛАВНАЯ ГИПОТЕЗА ИВАСАВЫ

Ян Нековарж, Прага

В работе излагаются основные понятия теории круговых полей, их отношения к классическим результатам и к современным исследованиям.