A journey though Iwasawa theory

Niels Ketelaars

Leiden University

3 July 2023

Let p be an odd prime.

Let p be an odd prime.
At the dawn of algebraic number theory ($\sim$1850), Ernst Kummer was interested in the class numbers of the fields $\mathbf{Q}(\zeta_p)$.

Let p be an odd prime.
At the dawn of algebraic number theory ($\sim$1850), Ernst Kummer was interested in the class numbers of the fields $\mathbf{Q}(\zeta_p)$.

THEOREM (Kummer). The class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$ is divisble by p if and only if p divides the numerator of one of the *Bernoulli numbers* $B_2, B_4, \ldots, B_{p-3}$.

Let p be an odd prime.
At the dawn of algebraic number theory ($\sim$1850), Ernst Kummer was interested in the class numbers of the fields $\mathbf{Q}(\zeta_p)$.

THEOREM (Kummer). The class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$ is divisble by p if and only if p divides the numerator of one of the *Bernoulli numbers* $B_2, B_4, \ldots, B_{p-3}$.

The Bernoulli numbers are defined by

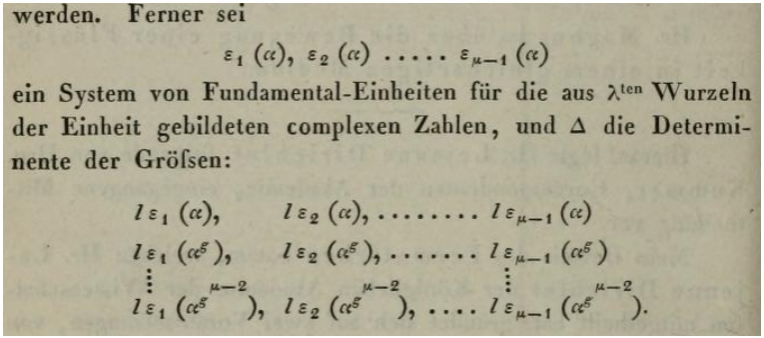
$$\frac{t}{e^t - 1} = \sum_{k \geq 0} B_k \frac{t^k}{k!}.$$

werden. Ferner sei

$$\varepsilon_1(\alpha),\ \varepsilon_2(\alpha)\ \ldots\ldots\ \varepsilon_{\mu-1}(\alpha)$$

ein System von Fundamental-Einheiten für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen, und Δ die Determinente der Größen:

$$\begin{array}{llll} l\,\varepsilon_1(\alpha), & l\,\varepsilon_2(\alpha), & \ldots\ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha) \\ l\,\varepsilon_1(\alpha^g), & l\,\varepsilon_2(\alpha^g), & \ldots\ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha^g) \\ \vdots & & & \vdots \\ l\,\varepsilon_1(\alpha^{g^{\mu-2}}), & l\,\varepsilon_2(\alpha^{g^{\mu-2}}), & \ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha^{g^{\mu-2}}). \end{array}$$



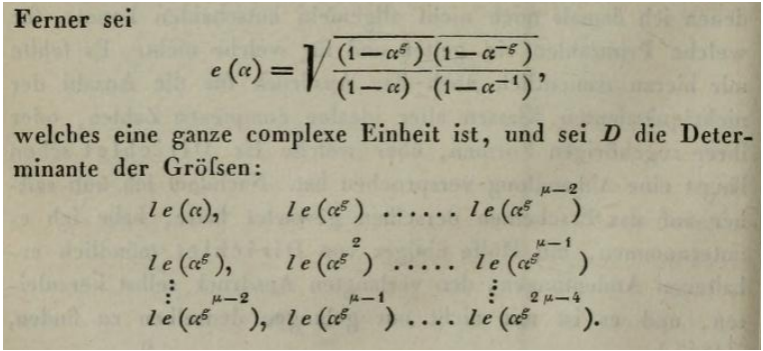
werden. Ferner sei

$$\varepsilon_1(\alpha),\ \varepsilon_2(\alpha)\ \ldots\ldots\ \varepsilon_{\mu-1}(\alpha)$$

ein System von Fundamental-Einheiten für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen, und Δ die Determinente der Grösen:

$$\begin{array}{llll} l\,\varepsilon_1(\alpha), & l\,\varepsilon_2(\alpha), \ldots\ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha) \\ l\,\varepsilon_1(\alpha^g), & l\,\varepsilon_2(\alpha^g), \ldots\ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha^g) \\ \vdots & & \vdots \\ l\,\varepsilon_1(\alpha^{g^{\mu-2}}), & l\,\varepsilon_2(\alpha^{g^{\mu-2}}), \ldots\ldots & l\,\varepsilon_{\mu-1}(\alpha^{g^{\mu-2}}). \end{array}$$

Here $\alpha = \zeta_p$, and g is a primitive root modulo p.
Thus $\Delta = \mathrm{Reg}(\mathbf{Z}[\zeta_p]^\times)$.

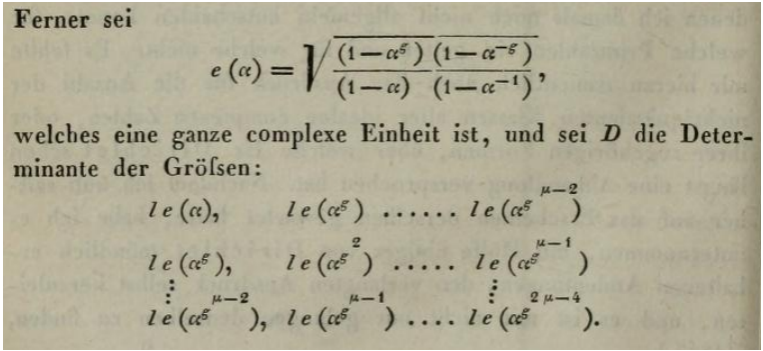


Ferner sei

$$e(\alpha) = \sqrt{\frac{(1-\alpha^{\varepsilon})}{(1-\alpha)}\frac{(1-\alpha^{-\varepsilon})}{(1-\alpha^{-1})}},$$

welches eine ganze complexe Einheit ist, und sei D die Determinante der Grösen:

$$\begin{array}{llll} le(\alpha), & le(\alpha^{\varepsilon}) & \ldots\ldots & le(\alpha^{\varepsilon^{\mu-2}}) \\ le(\alpha^{\varepsilon}), & le(\alpha^{\varepsilon^{2}}) & \ldots\ldots & le(\alpha^{\varepsilon^{\mu-1}}) \\ \vdots & & & \vdots \\ le(\alpha^{\varepsilon^{\mu-2}}), & le(\alpha^{\varepsilon^{\mu-1}}) & \ldots\ldots & le(\alpha^{\varepsilon^{2\mu-4}}). \end{array}$$



Ferner sei

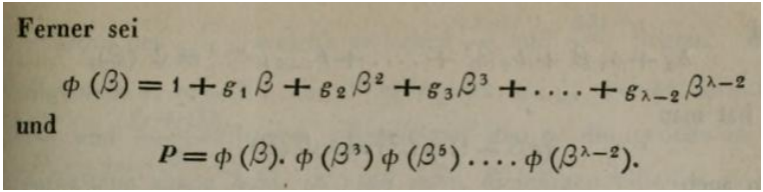
$$e(\alpha) = \sqrt{\frac{(1-\alpha^g)(1-\alpha^{-g})}{(1-\alpha)(1-\alpha^{-1})}},$$

welches eine ganze complexe Einheit ist, und sei D die Determinante der Grölsen:

$$\begin{array}{llll} le(\alpha), & le(\alpha^g) & \ldots\ldots & le(\alpha^{g^{\mu-2}}) \\ le(\alpha^g), & le(\alpha^{g^2}) & \ldots\ldots & le(\alpha^{g^{\mu-1}}) \\ \vdots & & & \\ le(\alpha^{g^{\mu-2}}), & le(\alpha^{g^{\mu-1}}) & \ldots\ldots & le(\alpha^{g^{2\mu-4}}). \end{array}$$

$$e(\alpha) = \sqrt{\frac{(1-\zeta_p^g)(1-\zeta_p^{-g})}{(1-\zeta_p)(1-\zeta_p^{-1})}}$$

D is the regulator of the subgroup of units generated by the Galois conjugates of $e(\alpha)$.

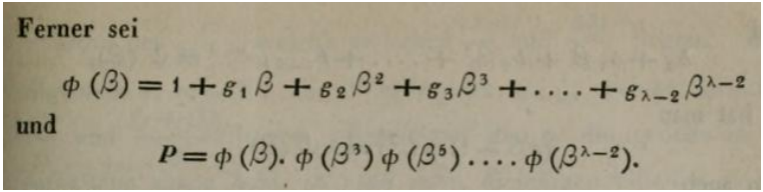


Ferner sei

$$\phi(\beta) = 1 + g_1\beta + g_2\beta^2 + g_3\beta^3 + \ldots + g_{\lambda-2}\beta^{\lambda-2}$$

und

$$P = \phi(\beta).\,\phi(\beta^3)\,\phi(\beta^5)\ldots\phi(\beta^{\lambda-2}).$$


Ferner sei

$$\phi(\beta) = 1 + g_1\beta + g_2\beta^2 + g_3\beta^3 + \ldots + g_{\lambda-2}\beta^{\lambda-2}$$

und

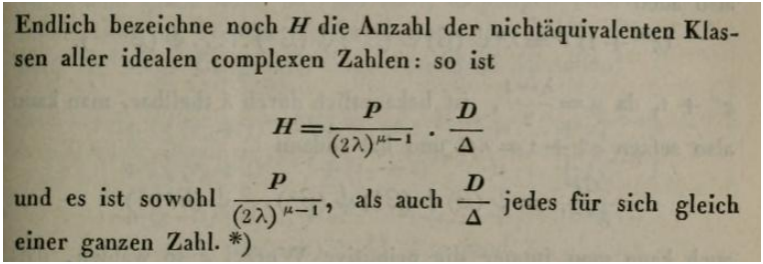
$$P = \phi(\beta).\,\phi(\beta^3)\,\phi(\beta^5)\ldots\phi(\beta^{\lambda-2}).$$

The product P is essentially the product of the Bernoulli numbers $B_2, \ldots, B_{p-3}$.

Endlich bezeichne noch H die Anzahl der nichtäquivalenten Klassen aller idealen complexen Zahlen: so ist

$$H = \frac{P}{(2\lambda)^{\mu-1}} \cdot \frac{D}{\Delta}$$

und es ist sowohl $\frac{P}{(2\lambda)^{\mu-1}}$, als auch $\frac{D}{\Delta}$ jedes für sich gleich einer ganzen Zahl. *)

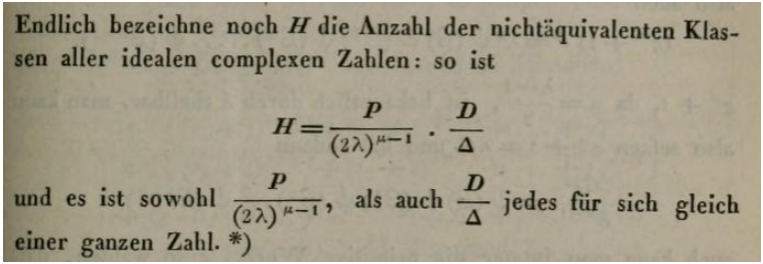


Endlich bezeichne noch H die Anzahl der nichtäquivalenten Klassen aller idealen complexen Zahlen: so ist

$$H = \frac{P}{(2\lambda)^{\mu-1}} \cdot \frac{D}{\Delta}$$

und es ist sowohl $\frac{P}{(2\lambda)^{\mu-1}}$, als auch $\frac{D}{\Delta}$ jedes für sich gleich einer ganzen Zahl. *)

$$\frac{(2\pi)^{(p-1)/2}}{2p^{p/2}} \mathrm{Reg}(\mathbf{Z}[\zeta_p]^\times) h = \prod_{\chi \neq 1} L(\chi, 1)$$



Endlich bezeichne noch H die Anzahl der nichtäquivalenten Klassen aller idealen complexen Zahlen: so ist

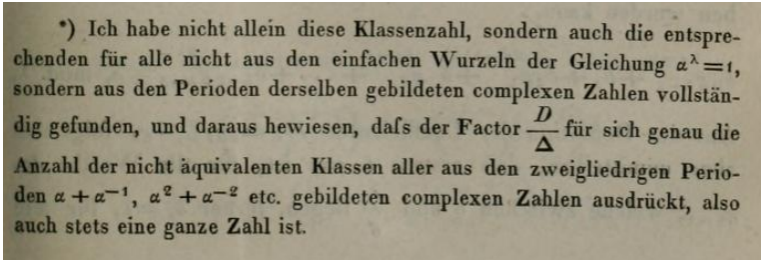
$$H = \frac{P}{(2\lambda)^{\mu-1}} \cdot \frac{D}{\Delta}$$

und es ist sowohl $\frac{P}{(2\lambda)^{\mu-1}}$, als auch $\frac{D}{\Delta}$ jedes für sich gleich einer ganzen Zahl. *)

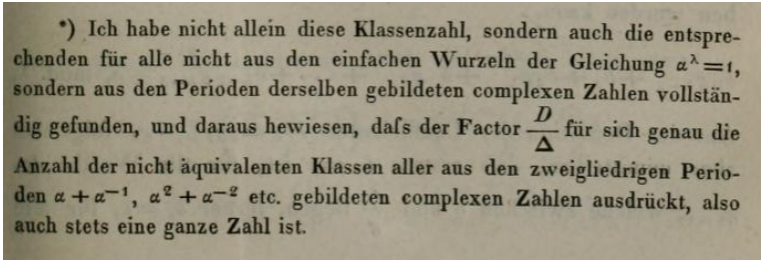
$$\frac{(2\pi)^{(p-1)/2}}{2p^{p/2}} \mathrm{Reg}(\mathbf{Z}[\zeta_p]^\times) h = \prod_{\chi \neq 1} L(\chi, 1)$$

The values $L(\chi, 1)$ at odd characters are given by Bernoulli numbers, and for even characters we have

$$L(\chi, 1) = \frac{-1}{G(\chi^{-1})} \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \chi^{-1}(a) \log\left(1 - \zeta_p^a\right)$$

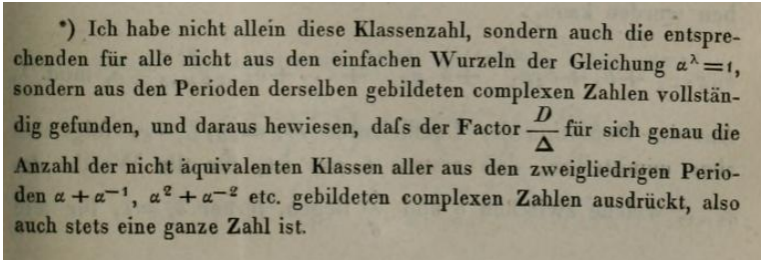


*) Ich habe nicht allein diese Klassenzahl, sondern auch die entsprechenden für alle nicht aus den einfachen Wurzeln der Gleichung $\alpha^\lambda = 1$, sondern aus den Perioden derselben gebildeten complexen Zahlen vollständig gefunden, und daraus hewiesen, dafs der Factor $\frac{D}{\Delta}$ für sich genau die Anzahl der nicht äquivalenten Klassen aller aus den zweigliedrigen Perioden $\alpha + \alpha^{-1}$, $\alpha^2 + \alpha^{-2}$ etc. gebildeten complexen Zahlen ausdrückt, also auch stets eine ganze Zahl ist.



*) Ich habe nicht allein diese Klassenzahl, sondern auch die entsprechenden für alle nicht aus den einfachen Wurzeln der Gleichung $\alpha^\lambda = 1$, sondern aus den Perioden derselben gebildeten complexen Zahlen vollständig gefunden, und daraus hewiesen, dafs der Factor $\frac{D}{\Delta}$ für sich genau die Anzahl der nicht äquivalenten Klassen aller aus den zweigliedrigen Perioden $\alpha + \alpha^{-1}$, $\alpha^2 + \alpha^{-2}$ etc. gebildeten complexen Zahlen ausdrückt, also auch stets eine ganze Zahl ist.

Kummer notes that the factor D/Δ(= index of the cyclotomic units in the full unit group) is also equal to the class number h^+ of $\mathbf{Q}(\zeta_p)^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$.



*) Ich habe nicht allein diese Klassenzahl, sondern auch die entsprechenden für alle nicht aus den einfachen Wurzeln der Gleichung $\alpha^\lambda = 1$, sondern aus den Perioden derselben gebildeten complexen Zahlen vollständig gefunden, und daraus hewiesen, dafs der Factor $\frac{D}{\Delta}$ für sich genau die Anzahl der nicht äquivalenten Klassen aller aus den zweigliedrigen Perioden $\alpha + \alpha^{-1}$, $\alpha^2 + \alpha^{-2}$ etc. gebildeten complexen Zahlen ausdrückt, also auch stets eine ganze Zahl ist.

Kummer notes that the factor D/Δ(= index of the cyclotomic units in the full unit group) is also equal to the class number h^+ of $\mathbf{Q}(\zeta_p)^+ = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Kummer later remarks in a letter to Kronecker that h^+ seems to always be coprime to p. This has been verified for all $p < 2^{31}$.

Let A be the p-power torsion subgroup of $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. It comes equipped with a natural action of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$.

Let A be the p-power torsion subgroup of $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. It comes equipped with a natural action of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$.

Let $\omega\colon (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ be the unique character with $a \equiv \omega(a) \bmod p$, and write $A(i) = \{a \in A \mid \sigma a = \omega^i(\sigma)a \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

Let A be the p-power torsion subgroup of $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. It comes equipped with a natural action of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$.

Let $\omega\colon (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ be the unique character with $a \equiv \omega(a) \bmod p$, and write $A(i) = \{a \in A \mid \sigma a = \omega^i(\sigma)a \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

THEOREM (Herbrand). Let i odd. If $A(i) \neq 0$, then p divides the numerator of B_{p-i}.

Let A be the p-power torsion subgroup of $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$. It comes equipped with a natural action of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$.

Let $\omega\colon (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ be the unique character with $a \equiv \omega(a) \bmod p$, and write $A(i) = \{a \in A \mid \sigma a = \omega^i(\sigma)a \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

THEOREM (Herbrand). Let i odd. If $A(i) \neq 0$, then p divides the numerator of B_{p-i}.

Questions:

1. Is the converse true?
2. Is the order of $A(i)$ equal to the exact power of p dividing B_{p-i}?

In 1959, Iwasawa proved the following result regarding the class numbers of the fields $\mathbf{Q}(\zeta_{p^n})$.

In 1959, Iwasawa proved the following result regarding the class numbers of the fields $\mathbf{Q}(\zeta_{p^n})$.

THEOREM (Iwasawa). Let $h_n = \#\operatorname{Cl}(\mathbf{Q}(\zeta_{p^n}))$. Then there exist integers μ, λ, ν such that

$$\operatorname{ord}_p h_n = \mu p^n + \lambda n + \nu$$

for all $n \gg 0$.

In 1959, Iwasawa proved the following result regarding the class numbers of the fields $\mathbf{Q}(\zeta_{p^n})$.

THEOREM (Iwasawa). Let $h_n = \#\operatorname{Cl}(\mathbf{Q}(\zeta_{p^n}))$. Then there exist integers μ, λ, ν such that

$$\operatorname{ord}_p h_n = \mu p^n + \lambda n + \nu$$

for all $n \gg 0$.

Main important idea: $\Gamma := \operatorname{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}(\zeta_p)) \cong \mathbf{Z}_p$.

In 1959, Iwasawa proved the following result regarding the class numbers of the fields $\mathbf{Q}(\zeta_{p^n})$.

THEOREM (Iwasawa). Let $h_n = \#\operatorname{Cl}(\mathbf{Q}(\zeta_{p^n}))$. Then there exist integers μ, λ, ν such that

$$\operatorname{ord}_p h_n = \mu p^n + \lambda n + \nu$$

for all $n \gg 0$.

Main important idea: $\Gamma := \operatorname{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}(\zeta_p)) \cong \mathbf{Z}_p$.

Each $\mathscr{Y}_n := p-$power torsion of $\operatorname{Cl}(\mathbf{Q}(\zeta_{p^n}))$ is naturally a $\mathbf{Z}_p[\Gamma/\Gamma^{p^n}]$ module, so $\mathscr{Y}_\infty = \varprojlim \mathscr{Y}_n$ is naturally a module over $\Lambda(\Gamma) = \varprojlim \mathbf{Z}_p[\Gamma/\Gamma^{p^n}]$ (in fact, finitely generated and torsion).

The ring $\Lambda(\Gamma)$ is isomorphic to $\mathbf{Z}_p[[T]]$, which is a 2-dimensional complete regular local ring. Established structure theory for modules over such rings implies the following:

The ring $\Lambda(\Gamma)$ is isomorphic to $\mathbf{Z}_p[[T]]$, which is a 2-dimensional complete regular local ring. Established structure theory for modules over such rings implies the following:

THEOREM. There exists a map with finite kernel and cokernel from $\mathscr{Y}_\infty$ to a module of the form

$$\bigoplus_{i=1}^{s} \mathbf{Z}_p[[T]]/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \mathbf{Z}_p[[T]]/(f_j^{n_j})$$

where each f_j is a *distinguished* irreducible polynomial.

The ring $\Lambda(\Gamma)$ is isomorphic to $\mathbf{Z}_p[[T]]$, which is a 2-dimensional complete regular local ring. Established structure theory for modules over such rings implies the following:

THEOREM. There exists a map with finite kernel and cokernel from $\mathscr{Y}_\infty$ to a module of the form

$$\bigoplus_{i=1}^{s} \mathbf{Z}_p[[T]]/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \mathbf{Z}_p[[T]]/(f_j^{n_j})$$

where each f_j is a *distinguished* irreducible polynomial.

Iwasawa's result holds now with $\mu = \sum_i m_i$ and $\lambda = \sum_j n_j \deg(f_j)$.

The ring $\Lambda(\Gamma)$ is isomorphic to $\mathbf{Z}_p[[T]]$, which is a 2-dimensional complete regular local ring. Established structure theory for modules over such rings implies the following:

THEOREM. There exists a map with finite kernel and cokernel from $\mathscr{Y}_\infty$ to a module of the form

$$\bigoplus_{i=1}^{s} \mathbf{Z}_p[[T]]/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \mathbf{Z}_p[[T]]/(f_j^{n_j})$$

where each f_j is a *distinguished* irreducible polynomial.

Iwasawa's result holds now with $\mu = \sum_i m_i$ and $\lambda = \sum_j n_j \deg(f_j)$.

We call $p^\mu \prod_j f_j^{n_j}$ the characteristic polynomial of the module $\mathscr{Y}_\infty$.

In 1964, Kubota and Leopoldt found a p-adic analogue of the Dirichlet L-function

$$L_p(\chi, \cdot)\colon \mathbf{Q}_p \to \mathbf{C}_p$$

that interpolates the values of the complex L-function at negative integers.

In 1964, Kubota and Leopoldt found a p-adic analogue of the Dirichlet L-function

$$L_p(\chi, \cdot)\colon \mathbf{Q}_p \to \mathbf{C}_p$$

that interpolates the values of the complex L-function at negative integers.

These functions are quite simple, in the sense that there are power series $f_i \in \mathbf{Z}_p[[T]]$ such that

$$f_i((1+p)^{1-s} - 1) = L_p(\omega^i, s)$$

THEOREM. Let $h_n^- = h_n/h_n^+$. Write $f_i = p^{\mu_i} P_i U_i$ with $P_i \in \mathbf{Z}_p[[T]]$ distinguished of degree λ_i and $U_i \in \mathbf{Z}_p[[T]]^\times$. Then for all $n \geq 1$ with $\max \lambda_i < p^{n-1} - p^{n-2}$,

$$\operatorname{ord}_p h_n^- = \mu p^n + \lambda n + \nu,$$

where $\mu = \sum_i \mu_i$ and $\lambda = \sum_i \lambda_i$.

THEOREM. Let $h_n^- = h_n/h_n^+$. Write $f_i = p^{\mu_i} P_i U_i$ with $P_i \in \mathbf{Z}_p[[T]]$ distinguished of degree λ_i and $U_i \in \mathbf{Z}_p[[T]]^\times$. Then for all $n \geq 1$ with $\max \lambda_i < p^{n-1} - p^{n-2}$,

$$\operatorname{ord}_p h_n^- = \mu p^n + \lambda n + \nu,$$

where $\mu = \sum_i \mu_i$ and $\lambda = \sum_i \lambda_i$.

In fact, we know that $\mu = 0$ for all p, and for all $p < 2^{31}$ we have $\nu = 0$ and the formula holds for all n.

THEOREM. Let $h_n^- = h_n/h_n^+$. Write $f_i = p^{\mu_i} P_i U_i$ with $P_i \in \mathbf{Z}_p[[T]]$ distinguished of degree λ_i and $U_i \in \mathbf{Z}_p[[T]]^\times$. Then for all $n \geq 1$ with $\max \lambda_i < p^{n-1} - p^{n-2}$,

$$\operatorname{ord}_p h_n^- = \mu p^n + \lambda n + \nu,$$

where $\mu = \sum_i \mu_i$ and $\lambda = \sum_i \lambda_i$.

In fact, we know that $\mu = 0$ for all p, and for all $p < 2^{31}$ we have $\nu = 0$ and the formula holds for all n.

Question: What is the relation between the characteristic polynomial of $\mathscr{Y}_\infty$ and the power series f_i?

Write $\mathscr{Y}_\infty(i) = \{y \in \mathscr{Y}_\infty \mid \sigma y = \omega^i(\sigma)y \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

Write $\mathscr{Y}_\infty(i) = \{y \in \mathscr{Y}_\infty \mid \sigma y = \omega^i(\sigma)y \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

THEOREM (Mazur–Wiles). Let $i \not\equiv 0 \bmod p-1$ odd. The characteristic polynomial of $\mathscr{Y}_\infty(i)$ is (up to a unit) equal to

$$f_{p-i}\left(\frac{1+p}{1+T} - 1\right).$$

Write $\mathscr{Y}_\infty(i) = \{y \in \mathscr{Y}_\infty \mid \sigma y = \omega^i(\sigma)y \text{ for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$.

THEOREM (Mazur–Wiles). Let $i \not\equiv 0 \bmod p-1$ odd. The characteristic polynomial of $\mathscr{Y}_\infty(i)$ is (up to a unit) equal to

$$f_{p-i}\left(\frac{1+p}{1+T} - 1\right).$$

COROLLARY. Let i odd. Then

$$\mathrm{ord}_p \#A(i) = \mathrm{ord}_p(B_{p-i}).$$