A brief introduction to p-adic numbers.

Reference: J.P Serre, A Course in Arithmetic, Springer Chapter II

Let p be a prime number.
For $n \in \mathbb{Z} \setminus \{0\}$, we denote by $v_p(n)$ the biggest integer m such that $p^m \mid n$. We set $v_p(0) = +\infty$.

We therefore have a map $v_p : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ such that:

rk 1) $v_p(n) = +\infty \iff n = 0$;

rk 2) $v_p(nm) = v_p(n) + v_p(m)$;

rk 3) $v_p(n+m) \geq \inf(v_p(n), v_p(m))$.

Let $x \in \mathbb{Q}$, write $x = \frac{a}{b}$ $a, b \in \mathbb{Z}, b \neq 0$. We set:

$$v_p(x) = v_p(a) - v_p(b).$$

One can show that $v_p(x)$ is well-defined. We have a map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ satisfying rk 1), rk 2), rk 3).

Let $(x_n)_{n \geq 0}$ be a sequence of elements in $\mathbb{Q}$.
We say that $(x_n)_{n \geq 0}$ p-adically converges to $\ell \in \mathbb{Q}$ if:

$\forall N \in \mathbb{N}, \quad \exists m \geq 0, \quad \forall n \geq m, \quad v_p(x_n - \ell) \geq N.$

We say that $(x_n)_{n \geq 0}$ is a p-adic Cauchy sequence if:

$\forall N \in \mathbb{N}, \quad \exists m \geq 0, \quad \forall n, n' \geq m, \quad v_p(x_n - x_{n'}) \geq N.$

If $(x_n)_{n \geq 0}$ is p-adically convergent then it is a p-adic Cauchy sequence.

T.S.V.R →

Example:

$\forall n \geq 0, \quad x_n = (p-1) + (p-1)p + \dots + (p-1)p^n$

We have $x_n = (p-1)(1 + \dots + p^n)$

$$= (p-1)\frac{p^{n+1}-1}{p-1}$$

$$= 1 + p^{n+1}$$

then:

$$v_p(x_n - (-1)) = n+1.$$

therefore $(x_n)_{n \geq 0}$ p-adically converges to -1.

We denote by $\mathbb{Q}_p$ the p-adic completion of $\mathbb{Q}$. We have:

- $\mathbb{Q}$ is dense in $\mathbb{Q}_p$
- $\mathbb{Q}_p$ is a field
- $\mathbb{Q}_p$ is complete (i.e. every p-adic Cauchy sequence of elements in $\mathbb{Q}$ converges in $\mathbb{Q}_p$)

We have a map $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{+\infty\}$ extending $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ and satisfying $v(1)$, $v(2)$, $v(3)$.

Lemma. $\forall n \geq 0, \; x_n \in \mathbb{Q}_p$

then $\sum_{n \geq 0} x_n$ converges in $\mathbb{Q}_p \iff \lim_n x_n = 0$

Proof. $\Leftarrow$

let $N \geq 0$. $\exists\, m \geq 0, \; \forall n \geq m \; v_p(x_n) \geq N$

Set $S_n = x_0 + x_1 + \dots + x_n$. then for $n, n' \geq m$,

$$v_p(S_n - S_{n'}) = v_p(x_{n'+1} + \dots + x_{n+1})$$

$$\geq \min(v_p(x_{n'+1}), \dots, v_p(x_{n+1}))$$

$$\geq N.$$

therefore s_n is a Cauchy sequence and thus converges in $\mathbb{Q}_p$. $\square$

We let $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$. Then $\mathbb{Z}_p$ is a principal ideal domain and its ideals are:

$$\{0\}, \quad p^n \mathbb{Z}_p \quad n \geq 0.$$

Furthermore the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induces an isomorphism of rings:

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}_p$$

this implies that if $x \in \mathbb{Z}_p$, x can uniquely write:

$$x = \sum_{i \geq 0} a_i p^i \qquad a_i \in \{0, \dots, p-1\}.$$

<u>theorem</u> (Hensel's Lemma)

let $F(x) \in \mathbb{Z}_p[x]$ be a monic polynomial

let $g(x), h(x) \in \mathbb{F}_p[x]$ be monic polynomials and relatively prime such that:

$$F(x) \equiv g(x)\, h(x) \quad (p\mathbb{Z}_p[x])$$

then there exist $G(x), H(x)$ monic polynomials in $\mathbb{Z}_p[x]$ such that:

$$G(x) \equiv g(x) \quad (p\mathbb{Z}_p[x])$$

$$H(x) \equiv h(x) \quad (p\mathbb{Z}_p[x])$$

$$F(x) = G(x)\, H(x).$$

<u>Example</u>: $p \geq 3$.

$$x^2 - (1+p) \equiv (x-1)(x+1) \quad (p).$$

thus there exists $\alpha \in \mathbb{Z}_p$, $\alpha \equiv 1 \ (p)$, such that:

$$x^2 - (1+p) = (x-\alpha)(x+\alpha).$$

Observe that if $n = 3$ then $\alpha = -2$ let's suppose that $n \geq 5$, we want to show that $\alpha \notin \mathbb{Q}$.

If $\alpha \in \mathbb{Q}$ then since α is integral over $\mathbb{Z}$, we get $\alpha \in \mathbb{Z}$, $\alpha \equiv 1 \ (n)$ and $\alpha \neq 1$.

then $|\alpha| \geq n-1$.

this implies that $(n-1)^2 \leq 1+n$ which is impossible for $n \geq 5$.

We assume that $p \geq 3$.

<u>Lemma.</u>

Let $a, b \in \mathbb{Z}_{p^n}$, $a \equiv b \ (p^n \mathbb{Z}_p)$.

Then:

$$a^p \equiv b^p \ (p^{n+1} \mathbb{Z}_p)$$

Proof.

$$a = b + p^n c \qquad c \in \mathbb{Z}_p$$

Thus,

$$a^p = b^p + p^{np} c^p + \sum_{k=2}^{p-2} \binom{p}{k} b^k (p^n c)^{p-k}$$
$$\equiv b^p \ (p^{n+1}). \ \square$$

<u>Corollary.</u>

Let $a \in \mathbb{Z}_p^\times$. Then $(a^{p^n})_{n \geq 0}$ converges in $\mathbb{Z}_p$.

Proof.

$$\equiv 0 \ (p$$

Fix $N \in \mathbb{N}$. Then:

$$n \geq n_0 \qquad a^{p^n} - a^{p^{n_0 N}} = a^{p^{n_0 N}} (a^{p^n - p^{n_0 N}} - 1)$$

By the lemma: $a^{p^n - p^N} \equiv 1 \quad (p^{N+1})$

Thus if $m, n \geq n_0$:

$$a^{p^n} - a^{p^m} = a^{p^n} - a^{p^N} + a^{p^N} - a^{p^m}$$
$$\equiv 0 \ (p^{N+1})$$

Therefore $(a^{p^n})_{n \geq 0}$ is a Cauchy sequence and therefore it converges. $\square$

For $a \in \mathbb{Z}_p^\times$, we set:

$$\omega_p(a) = \lim_n a^{p^n}$$

Observe that $\omega_p(a) \in \mathbb{Z}_p^\times$, $\omega_p(a) \equiv a \ (p\mathbb{Z}_p)$ and $\omega_p(a)^{p-1} = 1$.

Lemme. $\forall\ a, b \in \mathbb{Z}_p^\times$,

$$\omega_p(a) = \omega_p(b) \iff a \equiv b \ (p\mathbb{Z}_p)$$

Proof.

If $\omega_p(a) = \omega_p(b)$ then:

$$\begin{aligned} a &\equiv \omega_p(a) \ (p) \\ &\equiv \omega_p(b) \ (p) \\ &\equiv b \ (p) \end{aligned}$$

Reciprocally let's assume that $a \equiv b \ (p\mathbb{Z}_p)$.

then:

$$\forall\ n \geq 0 \qquad a^{p^n} \equiv b^{p^n} \ (p^{n+1}\mathbb{Z}_p)$$

thus:

$$\begin{aligned} \omega_p(a) &= \lim_n a^{p^n} \\ &= \lim_n b^{p^n} \\ &= \omega_p(b). \ \square \end{aligned}$$

Lemme. $\omega_p : \mathbb{Z}_p^\times \longrightarrow N_{p-1} \subset \mathbb{Z}_p^\times$ is a surjective group homomorphism and induces an isomorphism of groups:

$$\omega_p : (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} N_{p-1}$$

Proof. By Hensel's lemma $N_{p-1} \subset \mathbb{Z}_p^\times$.

We have:

$$\begin{aligned} \omega_p(ab) &= \lim_n (ab)^{p^n} \\ &= \lim_n a^{p^n} b^{p^n} \\ &= \omega_p(a)\,\omega_p(b). \ \square \end{aligned}$$

$\omega_p : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow N_{p-1}$ is called the p-adic Teichmüller character.

References: L. Washington, Introduction to cyclotomic Fields, Springer chapter 5

T. Arakawa, T. ~~Kaneko~~ IBUKIYAMA, M. Kaneko, Bernoulli Numbers and Zeta functions, Springer. chapter 1/2/3/4

Bernoulli Numbers & Zeta Values. (1)

The nth Bernoulli number $B_n \in \mathbb{Q}$ is defined as follows:

$$\frac{t}{e^t-1} = \sum_{n\geq 0} B_n \frac{t^n}{n!} \in \mathbb{Q}[[t]],$$

where $e^t = \sum_{n\geq 0} \frac{t^n}{n!} \in \mathbb{Q}[[t]]$.

Exercise 1

a) Prove that $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$.

b) Prove that $\forall n \geq 1$, $B_{2n+1} = 0$

Let x be another indeterminate and let's set:

$$\frac{t e^{xt}}{e^t-1} = \sum_{n\geq 0} B_n(x) \frac{t^n}{n!} \in \mathbb{Q}[x][[t]],$$

where $B_n(x) \in \mathbb{Q}[x]$ is the nth Bernoulli polynomial.

Exercise 2.

a) Prove that $B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_i x^{n-i}$

b) Prove that $B_n(1-x) = (-1)^n B_n(x)$

c) Prove that, $\forall n \geq 1$, $B_n'(x) = n B_{n-1}(x)$

d) Prove that $\forall n \geq 1$, $B_n(0) = B_n(1) = B_n$.

Lemma Let h be a prime number and let $n \geq 2$, $n \equiv 0 (2)$.

We have:

$$B_n = h^{n-1} \sum_{a=1}^{h} B_n\left(\frac{a}{h}\right).$$

Proof

$$\sum_{n\geq 0} h^{n-1} \sum_{a=1}^{h} B_n\left(\frac{a}{h}\right) \frac{t^n}{n!}$$

$$= \sum_{a=1}^{h} \sum_{n\geq 0} h^{n-1} B_n\left(\frac{a}{h}\right) \frac{t^n}{n!}$$

T.S.V.P.

$$= \sum_{a=1}^{n} \frac{t\, e^{\frac{a}{n} nt}}{e^{nt}-1}$$

$$= \frac{t}{e^{nt}-1} \sum_{a=1}^{n} (e^t)^a$$

$$= \frac{t}{e^{nt}-1} \cdot \frac{e^{(n+1)t} - e^t}{e^t-1}$$

$$= \frac{t e^t}{e^t-1} = t + \frac{t}{e^t-1}$$

$$= t + \sum_{m\geq 0} B_m \frac{t^m}{m!} \cdot \square$$

<u>Theorem</u> (von Staudt - Clausen)

$$\forall n \geq 1, \quad B_{2n} + \sum_{\substack{p \text{ prime} \\ p-1 \mid 2n}} \frac{1}{p} \in \mathbb{Z}$$

Proof.

Let p be a prime number. We will prove by induction on n that:

$$\forall n \geq 2,\ n \equiv 0 (2), \qquad B_n \equiv \begin{cases} -\frac{1}{p} \ (\mathbb{Z}_p) & p-1 \mid n \\ 0 \ (\mathbb{Z}_p) & \text{else} \end{cases}$$

The case $n=2$: $B_2 = \frac{1}{6}$.

thus $B_2 \in \mathbb{Z}_p$ if $p \geq 5$

$$B_2 + \frac{1}{2} = \frac{1}{6} + \frac{1}{2} = \frac{4}{6} = \frac{2}{3} \in \mathbb{Z}_2$$

$$B_2 + \frac{1}{3} = \frac{1}{6} + \frac{1}{3} = \frac{3}{6} = \frac{1}{2} \in \mathbb{Z}_3.$$

therefore the assertion is true for $n=2$.

By our Lemma:

$$B_n = p^{n-1} \sum_{a=1}^{p} B_n\left(\frac{a}{p}\right)$$

$$= p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} B_j \left(\frac{a}{p}\right)^{n-j}$$

$$= \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} p B_j\, a^{n-j}\, p^{j-2}$$

By our induction hypothesis for $j<n$, $p B_j \in \mathbb{Z}_p$.

Thus:

$$B_n \equiv \sum_{a=1}^{p} \left(p a^n p^{-2} + n p B_1 a^{n-1} p^{-2} + p B_n p^{n-2}\right) (\mathbb{Z}_p)$$

$$\equiv p^n B_n + \frac{1}{p} \sum_{a=1}^{p} a^n \quad (\mathbb{Z}_p).$$

Finally, we get:

$$(1-p^n) B_n \equiv \frac{1}{p} \sum_{a=1}^{p} a^n \quad (\mathbb{Z}_p)$$

<u>Exercise 3</u>

Let $\mathbb{F}_q$ be a finite field having q elements and let $n \geq 1$ be an integer. Prove that:

$$\sum_{\alpha \in \mathbb{F}_q^\times} \alpha^n = \begin{cases} -1 & \text{if } n \equiv 0 \ (q-1) \\ 0 & \text{otherwise.} \end{cases}$$

By the above exercise,

$$(1-p^n) B_n \equiv \begin{cases} -\frac{1}{p} \ (\mathbb{Z}_p) & \text{if } n \equiv 0 \ (p-1) \\ 0 \ (\mathbb{Z}_p) & \text{otherwise.} \end{cases}$$

We conclude that $B_n \in \mathbb{Z}_p$ if $p-1 \nmid n$, since $1-p^n \in \mathbb{Z}_p^\times$.

If $p-1 \mid n$:

$$B_n \equiv -\frac{1}{p(1-p^n)} \quad (\mathbb{Z}_p)$$

$$\equiv -\frac{1}{p} \sum_{k \geq 0} (p^n)^k \quad (\mathbb{Z}_p)$$

$$\equiv -\frac{1}{p} \ (\mathbb{Z}_p) \quad \text{if } p-1 \mid n.$$

We conclude that for every prime number ℓ:

$$B_n + \sum_{p,\, p-1 \mid n} \frac{1}{p} \in \mathbb{Z}_\ell$$

the result follows. $\square$

T.S.V.P.

Exercise 4

Let $n \geq 2$, $n \equiv 0 \pmod 2$. Let's write:

$$B_n = \frac{U_n}{V_n} \qquad U_n, V_n \in \mathbb{Z}, \quad V_n \geq 1 \quad (U_n, V_n) = 1.$$

Prove that: $V_n = \prod_{k,\, k-1 \mid n} k$

Bernoulli Numbers & Zeta Values (2)

$$\frac{t}{e^t-1} = \sum_{n\geq 0} B_n \frac{t^n}{n!} \in \mathbb{Q}[[t]] \qquad \forall n\geq 0,\ B_n\in\mathbb{Q}.$$

<u>Theorem</u> (von Staudt - Clausen)

$\forall n\geq 2,\ n\equiv 0\ (2),\qquad B_n + \sum_{p,\ p-1\mid n} \frac{1}{p} \in \mathbb{Z}.$

<u>Remark.</u>

$\forall n\geq 2,\ n\equiv 0\ (2),\quad B_n\neq 0.$

Indeed, if $B_n=0$ then $\sum_{p,\ p-1\mid n}\frac{1}{p}\in\mathbb{Z}$. But:

$$\nu_2\Big(\sum_{p,\ p-1\mid n}\frac{1}{p}\Big) = -1 < 0$$

this is a contradiction!

<u>Proposition.</u> Let p be an odd prime.

Let $r,s\in\mathbb{Z}_p$ and $\varphi(t)\in\mathbb{Z}_p[[t]]$.

Write:

$$\varphi(e^{rt}-e^{st}) = \sum_{m\geq 0} A_m \frac{t^m}{m!} \in \mathbb{Q}_p[[t]]$$

Then:

i) $\forall m\geq 0,\quad A_m\in\mathbb{Z}_p.$

(ii) $\forall\ m\geq, a\geq 1,$

$$A_{m+(p-1)p^{a-1}} \equiv A_m\ (p^a).$$

<u>Proof.</u> Write $\varphi(t) = \sum_{k\geq 0} a_k t^k \qquad a_k\in\mathbb{Z}_p.$

We have: $\varphi(e^{rt}-e^{st}) = \sum_{k\geq 0} a_k (e^{rt}-e^{st})^k$

$$= \sum_{k\geq 0} a_k \sum_{\ell=0}^{k} \binom{k}{\ell}(-1)^{\ell} e^{st\ell} e^{r(k-\ell)t}$$

T.S.V.P.

thus:

$$\varphi(e^{rt}e^{st}) = \sum_{h\geq 0}\sum_{l=0}^{h} (-1)^l a_h \binom{h}{l} e^{(r(h-l)+sl)t}$$

then take m-th derivative and set $t=0$:

$$A_m = \sum_{h\geq 0}\sum_{l=0}^{h} (-1)^l a_h \binom{h}{l} (r(h-l)+sl)^m$$

Remark that since $(e^{rt}-e^{st})^k \equiv 0\ (t^k)$, we get for:

$$h > m, \quad \sum_{l=0}^{k} (-1)^l a_h \binom{h}{l} (r(h-l)+sl)^m = 0$$

In particular $A_m \in \mathbb{Z}_h$

Now, let $m \geq a \geq 1$:

$$A_{m+(h-1)h^{a-1}} - A_m$$

$$= \sum_{h\geq 0}\sum_{l=0}^{h} (-1)^l a_h \binom{h}{l} (r(h-l)+sl)^m \left((r(h-l)+sl)^{(h-1)h^{a-1}} - 1\right)$$

If $h \mid (r(h-l)+sl) \Rightarrow (r(h-l)+sl)^m \equiv 0\ (h^a)$ since $m \geq 0$

If $h \nmid (r(h-l)+sl) \Rightarrow (r(h-l)+sl)^{h-1} \equiv 1\ (h)$

$$\Rightarrow (r(h-l)+sl)^{(h-1)h^{a-1}} \equiv 1\ (h^a)$$

therefore:

$$A_{m+(h-1)h^{a-1}} - A_m \equiv 0\ (h^a). \ \square$$

<u>Theorem</u> (Kummer Congruences).

Let p be an odd prime.

a) Let $n \geq 2$, $n \equiv 0 (2)$, $n \not\equiv 0 (p-1)$. Then $\frac{B_n}{n} \in \mathbb{Z}_p$.

b) Let $m, n \in \mathbb{Z}$, $n \geq m \geq a \geq 1$, $n \equiv m \, (-(p-1) p^{a-1})$, $m \not\equiv 0 (p-1)$.
Then:

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \quad (p^a)$$

<u>Proof</u>. Let $c \in \mathbb{Z}_p^\times$, $c \neq 1$

We have:

$$(1+t)^c = \sum_{n \geq 0} \frac{c(c-1)\cdots(c-n+1)}{n!} t^n \in \mathbb{Q}_p[[t]]$$

But $\frac{c(c-1)\cdots(c-n+1)}{n!} \in \mathbb{Z}_p \quad \forall c \in \mathbb{Z}_p$. Thus:

$$(1+t)^c \in \mathbb{Z}_p[[t]].$$

Let $\varphi(t) = \frac{1}{t} - \frac{c}{(1+t)^c - 1}$.

Observe that $(1+t)^c - 1 = ct + t^2 f \qquad f \in \mathbb{Z}_p[[t]]$

Thus:

$$\frac{c}{(1+t)^c - 1} = \frac{c}{ct(1+t^2 g)} \qquad g = \frac{f}{c} \in \mathbb{Z}_p[[t]]$$

Therefore $\frac{c}{(1+t)^c - 1} = \frac{1}{t} \sum_{n \geq 0} (tg)^n$

$$\equiv \frac{1}{t} \quad (\mathbb{Z}_p[[t]]).$$

We conclude that:

$$\varphi(t) \in \mathbb{Z}_p[[t]]$$

Now, $\varphi(e^t - 1) = \frac{1}{e^t - 1} - \frac{c}{e^{ct} - 1}$

$$= \frac{1}{t}\left(\frac{t}{e^t - 1} - \frac{ct}{e^{ct} - 1}\right)$$

T.S.V.P. →

$$= \frac{1}{t} \sum_{n \geq 0} (1-c^n) B_n \frac{t^n}{n!}$$

$$= \sum_{n \geq 1} (1-c^n) \frac{B_n}{n} \frac{t^{n-1}}{(n-1)!}$$

By the previous Proposition:

$$\forall c \in \mathbb{Z}_n^\times, \quad (1-c^n) \frac{B_n}{n} \in \mathbb{Z}_n$$

Let's select $c \in \mathbb{Z}_n^\times$ such that $c^m \not\equiv 1 \ (n)$ $(m \not\equiv 0 \ (n-1))$.
Then $(1-c^m) \in \mathbb{Z}_n^\times$ and thus:

$$\frac{B_m}{m} \in \mathbb{Z}_n.$$

Now, let $m \geq a \geq 1$. By the previous Proposition:

$$\left(1 - c^{m+(n-1)n^{a-1}}\right) \frac{B_{m+(n-1)n^{a-1}}}{m+(n-1)n^{a-1}} \equiv (1-c^m) \frac{B_m}{m} \ (n^a)$$

But:

$$\left(1 - c^{m+(n-1)n^{a-1}}\right) \equiv (1-c^m) \ (n^a),$$

and $(1-c^m) \in \mathbb{Z}_n^\times$ for a good choice of c $(m \not\equiv 0 \ (n-1))$.

Thus $$\frac{B_{m+(n-1)n^{a-1}}}{m+(n-1)n^{a-1}} \equiv \frac{B_m}{m} \ (n^a).$$

Thus:

$$\forall k \geq 1, \quad \frac{B_{m+k(n-1)n^{a-1}}}{m+k(n-1)n^{a-1}} \equiv \frac{B_m}{m} \ (n^a).$$

We conclude that:

$$\frac{B_m}{m} \equiv \frac{B_m}{m} \ (n^a). \quad \square$$

Liouville's Theorem

Let $f : \mathbb{C} \to \mathbb{C}$ be an entire function. Let's suppose that there exists $M \in [0, +\infty[$ such that:

$$\forall z \in \mathbb{C}, \ |f(z)| \leq M.$$

Then there exists $c \in \mathbb{C}$ such that $\forall z \in \mathbb{C}, \ f(z) = c$.

Theorem.

$$\sin(\pi t) = \pi t \prod_{n \geq 1} \left(1 - \frac{t^2}{n^2}\right) \in \mathbb{R}[[t]].$$

Proof.

$$\forall z \in \mathbb{C}, \quad \sin(\pi z) = \frac{e^{iz\pi} - e^{-iz\pi}}{2i}$$

$$= \sum_{n \geq 1} (-1)^{n-1} \frac{\pi^{2n+1} z^{2n+1}}{(2n+1)!}$$

$$= \pi z - \frac{(\pi z)^3}{3!}$$

Thus
$$\frac{\pi^2}{\sin(\pi z)^2} = \frac{\pi^2}{\pi^2 z^2 \left(1 - \frac{\pi^2 z^2}{3!} + \cdots\right)^2}$$

$$= \frac{1}{z^2} + \text{regular at } z$$

In fact $\sin(\sin(\pi z + n))^2 = \sin(\pi z)^2 \quad \forall n \in \mathbb{Z}$, we get:

$$\frac{\pi^2}{\sin(\pi z)^2} = \frac{1}{(z+n)^2} + \text{regular at } (z+n)$$

But $\frac{\pi^2}{\sin(\pi z)^2}$ has only poles at $n \in \mathbb{Z}$.

We get:

$$f(z) = \frac{\pi^2}{\sin(\pi z)^2} - \sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^2} \quad \text{has no poles}$$

and therefore is an entire function on $\mathbb{C}$.

T.S.V.P. →

Let's prove that $f(z) = f(z+1)$.

Furthermore, it is not difficult to verify that f is bounded on $\{x+iy,\ x\in[0,1],\ |y|\leq N\}$ N any natural number. By the periodicity of f, we get that f is bounded on $\{x+iy,\ x\in\mathbb{R},\ |y|\leq N\}$ for any N.

But $\lim_{|y|\to+\infty} f(x+iy)=0$. Thus f is bounded on $\mathbb{C}$.

Therefore by Liouville's Theorem, f is constant. Thus $f=0$.

We therefore have:

$$\frac{\pi^2}{\sin(\pi z)^2} = \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2}$$

We remark it has:

$$\frac{\pi^2}{\sin(\pi z)^2} = \frac{1}{z^2} + \sum_{n\geq 1} \frac{1}{(z-n)^2} + \frac{1}{(z+n)^2}$$

the left hand side is the derivative of:

$$-\pi\cot(\pi z)$$

the right hand side is the derivative of:

$$-\frac{1}{z} + \sum_{n\geq 1} -\frac{1}{z-n} - \frac{1}{z+n}$$

thus $\pi\cot(\pi z) = \text{cste} + \frac{1}{z} + \sum_{n\geq 1} \frac{1}{z-n} + \frac{1}{z+n}$

But since the functions are odd, cste $=0$. therefore we have proved:

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{n\geq 1} \frac{1}{z-n} + \frac{1}{z+n}$$

Observe that:

$$d\log \sin \pi z = \frac{\pi \cos(\pi z)}{\sin(\pi z)}$$

$$= \pi \cot(\pi z)$$

$n \geq 1$ $$d\log\left(1 - \frac{z^2}{n^2}\right) = \frac{-\frac{2}{n^2} z}{1 - z^2/n^2}$$

$$= \frac{2z}{z^2 - n^2}$$

$$= \frac{1}{z-n} + \frac{1}{z+n}$$

Therefore:

$$d\log \sin \pi z = d\log\left(z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right)\right)$$

We get:

$$\log \sin(\pi z) = cst + \log\left(z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right)\right)$$

Thus:

$$\sin \pi z = e^{cst} \; z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right).$$

But $\sin \pi z = \pi z \mod z^2$. Thus: $e^{cst} = \pi$.

Therefore:

$$\sin \pi z = z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right). \quad \square$$

Recall that $\forall s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \in \mathbb{C}$$

$$= \prod_n \left(1 - \frac{1}{n^s}\right)^{-1}$$

T.S.V.P.

Theorem (L. Euler)

$\forall k \geq 1,$ $$\frac{\zeta(2k)}{(2i\pi)^{2k}} = -\frac{1}{2}\frac{B_{2k}}{(2k)!}$$

Proof

We have:

$$\sin(t) = t \prod_{n\geq 1}\left(1 - \frac{t^2}{n^2\pi^2}\right) \in \mathbb{Q}[[t]].$$

Let's take the logarithmic derivative and multiply by t:

$$\frac{t\cos(t)}{\sin(t)} = 1 - 2\sum_{n\geq 1}\frac{t^2}{n^2\pi^2 - t^2}$$

$$= 1 - 2\sum_{m\geq 1}\zeta(2m)\frac{t^{2m}}{(2\pi)^{2m}}$$

But $\cos(t) = \dfrac{e^{it}+e^{-it}}{2}$ $\quad \sin t = \dfrac{e^{it}-e^{-it}}{2i}$

Thus: $$t\frac{\cos(t)}{\sin(t)} = it + \frac{2it}{e^{2it}-1}$$

$$= it + \sum_{n\geq 0} B_n \frac{(2it)^n}{n!}$$

$$= 1 + \sum_{\substack{n\geq 2\\ n\equiv 0(2)}} 2^n \frac{B_n}{n!}(-1)^n t^n$$

Thus:

$$\zeta(2m)/(2\pi)^{2m} = (-1)^{2m-1}\, 2^{2m-1}\frac{B_{2m}}{2m!}$$

$$\frac{\zeta(2m)}{(2i\pi)^{2m}} = -\frac{1}{2}\frac{B_{2m}}{2m!}. \quad \square$$

<u>Corollary.</u>

Let $n \geq 1$. Then:

$$|B_{2n}| > 2\left(\frac{n}{\pi e}\right)^{2n}$$

In particular $\lim_{n \to +\infty} \frac{|B_{2n}|}{2n} = +\infty$.

<u>Proof.</u>

We have

$$|B_{2n}| = \frac{2n!}{(2\pi)^{2n}} 2\,\zeta(2n) > \frac{2n!}{(2\pi)^{2n}} 2$$

Now:

$$e^{2n} > \frac{(2n)^{2n}}{2n!}$$

thus: $2n! > \left(\frac{2n}{e}\right)^{2n}$

Therefore:

$$|B_{2n}| > 2\left(\frac{n}{\pi e}\right)^{2n}$$

thus:

$$\frac{|B_{2n}|}{2n} > \frac{1}{\pi e}\left(\frac{n}{\pi e}\right)^{2n-2}$$

And we get:

$$\lim_{n \to +\infty} \frac{|B_{2n}|}{2n} = +\infty. \quad \square$$

Let p be an odd prime number.

For $p \geq 1$, $p \equiv 0(2)$, $2 \leq k \leq p-3$ we have:

$$B_k \in \mathbb{Z}_p.$$

The prime number p is called regular if:

$$\prod_{\substack{k=2 \\ k \equiv 0(2)}}^{p-3} B_k \not\equiv 0(p)$$

p is called irregular otherwise.

T.S.V.P. →

Conjecture. There exist infinitely many regular primes.
(It is believed that 61% of the prime numbers are regular)

Example. 37 is the first irregular prime, we have:

$$B_{32} \equiv 0 \ (37).$$

A list of irregular primes:

37, 59, 67, 101, 103, 131, 149, 157, 233 ...

Let $i(n) = |\{2 \leq k \leq n-3,\ k \equiv 0 (2),\ B_k \equiv 0 \ (n)\}|$ the index of irregularity of n.

Then n is regular $\Leftrightarrow i(n) = 0$

$i(37) = 1$, $i(59) = 1$, $i(67) = 1$, $i(101) = 1$, $i(103) = 1$
$i(131) = 1$, $i(149) = 1$, $i(157) = 2$, $i(233) = 1$, ...

Conjecture. $\lim_{n \to \infty} i(n) = +\infty$.

Conjecture (K. Kamano - D. Zagier)
Let $N \geq 3$, $N \equiv 1 (2)$. There exist infinitely many prime numbers n such that $B_{n-N} \not\equiv 0 (n)$.

<u>Theorem</u> There exist infinitely many regular primes.

<u>Proof.</u>
Let S be the set of irregular primes and let's suppose that S is finite. Write $S = \{p_1, p_2, \dots, p_r\}$.
Let $m = N(p_1 - 1)\cdots(p_r - 1)$ where $N \equiv 0 (2)$ and N is large enough such that:

$$|B_m| / m > 1$$

Let p be a prime number dividing the numerator of $\frac{B_m}{m}$.
By the von Staudt-Clausen Theorem:

$$p \neq p_i \quad i = 1, \dots, r \quad \text{since } p_i - 1 \mid m$$

$$p - 1 \nmid m$$

(thus p is odd)

Let $n \in \{2, \dots, p-3\}$ such that $n \equiv m \ (p-1)$.
By the Kummer congruences:

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \ (p)$$

Thus:

$$B_n \equiv 0 \ (p) \quad \text{and} \quad p \in S.$$

This is a contradiction. $\square$

One can prove by analytic techniques:

<u>Theorem</u> Let $p \equiv 3 (4)$. Then $B_{\frac{p+1}{2}} \equiv 0 (p)$

Let $p \equiv 1 (4)$ and let $K = \mathbb{Q}(\sqrt{p})$.

Then there exists $\varepsilon > 1$ such that $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$

Recall that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \frac{\sqrt{p} - 1}{2}$. Thus one can write:

$$\varepsilon = \frac{t + u\sqrt{p}}{2} \qquad t, u \in \mathbb{Z}.$$

It is obvious that $t \not\equiv 0 \ (p)$.

Let h_K be the ideal class number of K.

<u>Theorem</u> (Ankeny–Artin–Chowla)

$$h_K \frac{u}{t} \equiv B_{\frac{p-1}{2}} \pmod{p}.$$

By analytic techniques one can prove that $h_K < \sqrt{p}$.

Thus $u \equiv 0 \pmod{p} \iff B_{\frac{p-1}{2}} \equiv 0 \pmod{p}$

<u>Open Problem</u>

Let $p \equiv 1 \pmod{4}$. Is it true that $B_{\frac{p-1}{2}} \not\equiv 0 \pmod{p}$?

The Hasse-Arf theorem (1)

$\zeta_n = e^{2i\pi/n}$ $\qquad$ n : odd prime number

$K = \mathbb{Q}(\zeta_n) = \mathbb{Q}[\zeta_n] = \bigoplus_{k=0}^{n-2} \mathbb{Q}\,\zeta_n^k$

$\mathcal{O}_K = \mathbb{Z}[\zeta_n] = \bigoplus_{k=0}^{n-2} \mathbb{Z}\,\zeta_n^k$

$\Delta = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma : K \to K \mid \sigma \text{ isomorphism of fields}\}$.

One has:

$$\Delta \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

For $a \in \mathbb{Z} \setminus n\mathbb{Z}$, let $\sigma_a \in \Delta$ such that $\sigma_a(\zeta_n) = \zeta_n^a$.

We have:

$x \in K$, $x = \sum_{k=0}^{n-2} x_k \zeta_n^k$ $\qquad$ $x_k \in \mathbb{Q}$,

$$\sigma_a(x) = \sum_{k=0}^{n-2} x_k\, \sigma_a(\zeta_n^k)$$
$$= \sum_{k=0}^{n-2} x_k\, \zeta_n^{ak}.$$

Observe that $\forall s \in \Delta$, $s(\mathcal{O}_K) = \mathcal{O}_K$.

Let ℓ be a prime number $\ell \equiv 1\ (n)$.

Then $X^n - 1$ divides $X^{\ell-1} - 1$ in $\mathbb{F}_\ell[X]$. Recall that:

$$X^{\ell-1} - 1 = \prod_{\alpha \in \mathbb{F}_\ell^\times} X - \alpha$$

Let $c \in \mathbb{Z}$, $c \in \{2, \dots, \ell-1\}$ such that $c^n \equiv 1\ (\ell)$.

Let:

$$\mathfrak{L} = (\zeta_n - c, \ell) \quad \text{ideal of } \mathcal{O}_K.$$

Then $\ell \in \mathfrak{L}$ and $\zeta_n \equiv c\ (\mathfrak{L})$. Thus:

$$\mathcal{O}_K/\mathfrak{L} \simeq \mathbb{F}_\ell.$$

In particular $\mathfrak{L}$ is a maximal ideal of $\mathcal{O}_K$.

We have:

$$\sigma_a^{-1}(\zeta_n) \equiv c \quad (\sigma_a^{-1}(\mathfrak{L}))$$

Let $a, b \in \mathbb{Z}$, $ab \equiv 1\ (n)$.

We opt:

$$\zeta_n^b \equiv c \quad (\sigma_a^{-2}(\mathfrak{l})).$$

Thus $$\zeta_n^{ab} = \zeta_n \equiv c^a \quad (\sigma_a^{-2}(\mathfrak{l})).$$

Now: $$\sigma_a^{-2}(\mathfrak{l}) = (\zeta_n^b - c, \ell)$$

But $$\zeta_n^b - c \equiv \zeta_n^b - c^{ab} \quad (\ell)$$
$$\equiv (\zeta_n - c^a)(\zeta_n^{b-1} + \dots + (c^a)^{b-1})(\ell)$$

then $\sigma_a^{-2}(\mathfrak{l}) \subset (\zeta_n - c^a, \ell)$. But these two ideals are maximal, thus:

$$\sigma_a^{-2}(\mathfrak{l}) = (\zeta_n - c^a, \ell).$$

Let's assume that:

$$\sigma_a^{-2}(\mathfrak{l}) = \sigma_b^{-2}(\mathfrak{l})$$
$$\Rightarrow \quad \zeta_n - c^a \in \sigma_b^{-2}(\mathfrak{l})$$
$$\Rightarrow \quad (\zeta_n - c^a)(\zeta_n - c^b) \in \sigma_b^{-2}(\mathfrak{l})$$
$$\Rightarrow \quad c^b - c^a \in \sigma_b^{-2}(\mathfrak{l})$$
$$\Rightarrow \quad c^b - c^a \in \sigma_b^{-2}(\mathfrak{l}) \cap \mathbb{Z} = \ell\mathbb{Z}$$
$$\Rightarrow \quad c^b \equiv c^a \ (\ell)$$
$$\Rightarrow \quad a \equiv b \ (h)$$
$$\Rightarrow \quad \sigma_a = \sigma_b$$

Thus: $$\ell\mathcal{O}_K = \prod_{a=1}^{h-1} \sigma_a^{-2}(\mathfrak{l}).$$

Let I be the set of non zero fractional ideals of $\mathcal{O}_K$, i.e.

$$a \in I \iff \exists\, x \in K^\times,\ x a \text{ ideal of } \mathcal{O}_K,\ x a \neq \{0\}.$$

Since $\mathcal{O}_K$ is a Dedekind domain, every $a \in I$ can be uniquely written:

$$a = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

$\mathfrak{p}$ runs through the maximal ideals of $\mathcal{O}_K$, $n_{\mathfrak{p}} \in \mathbb{Z}$, $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$.

Here $\mathfrak{p}^{-2}$ is the unique fractional ideal of I such that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.
We have that I is a $\mathbb{Z}[\Delta]$ module:

$$\sum_{\delta \in \Delta} n_\delta\, \delta \cdot a = \prod_{\delta \in \Delta} \delta(a)^{n_\delta}$$

Let P be the subgroup of I consisting of principal ideals, $P = \{x\,\mathcal{O}_K,\ x \in K^\times\}$. Then P is also a $\mathbb{Z}[\Delta]$ module. Thus:

$$Cl(K) := I/P \text{ is a } \mathbb{Z}[\Delta] \text{ module } (*)$$

Furthermore $Cl(K)$ is finite.

<u>Theorem</u> (Čebotarev)
Let $\sigma \in Cl(K)$. Then there exist infinitely many prime ideals $\mathfrak{l}$ of $\mathcal{O}_K$ such that:
1) $\mathfrak{l} \cap \mathbb{Z} = l\mathbb{Z}$, l prime number, $l \equiv 1\ (n)$;
2) $\mathfrak{l} \in \sigma$.

Let l be a prime number, $l \equiv 1\ (n)$.
Let $s \in \mathbb{F}_l^\times$ such that $\langle s \rangle = \mathbb{F}_l^\times$.
Let $\chi_l : \mathbb{F}_l^\times \to \mathbb{C}^\times$ such that:

$$\chi_l(s) = \xi_n.$$

We set:

$$g(\chi_\ell) = -\sum_{b=1}^{\ell-1} \chi_\ell(b)\, \zeta_\ell^{b} \in K(\zeta_\ell) \quad \text{where } \zeta_\ell = e^{2i\pi/\ell}$$

<u>Proposition.</u>

1) $g(\chi_\ell)\,\overline{g(\chi_\ell)} = \ell$

2) $g(\chi_\ell)^{\ell-2} \in \mathcal{O}_K$

<u>Proof.</u>

1) We have:

$$g(\chi_\ell)\, g(\overline{\chi_\ell})$$

$$= \sum_{b,b'} \chi_\ell(b)\, \overline{\chi_\ell}(b')\, \zeta_\ell^{b-b'}$$

$$= \sum_{b,b'} \chi_\ell(bb'^{-1})\, \zeta_\ell^{(bb'^{-1})b'}$$

$$= \sum_{c,b'} \chi_\ell(c)\, \zeta_\ell^{(c-1)b'}$$

$$= \ell - 1 + \sum_{c\neq 1} \sum_{b'} \chi_\ell(c)\, \zeta_\ell^{(c-1)b'}$$

$$= \ell - 1 + \sum_{c\neq 1} \chi_\ell(c)\, \mathrm{Tr}_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\zeta_\ell^{c-1})$$

$$= \ell - 1 - \sum_{c\neq 1} \chi_\ell(c)$$

$$= \ell - 1 - (-1)$$

$$= \ell$$

2) By denoting this term:

$$\mathrm{Gal}(K(\zeta_\ell)/K) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_\ell)\cap K)$$

$$= \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$$

let $\tau \in \mathrm{Gal}(K(\zeta_\ell)/K)$, $\tau(\zeta_\ell) = \zeta_\ell^{c}$ $c \in \mathbb{Z}\setminus \ell\mathbb{Z}$.

We have:

$$\tau(g(\chi_\ell)) = -\sum_{b=1}^{\ell-1} \chi_\ell(b)\, \zeta_\ell^{bc}$$

thus $\tau(g(\chi_\ell)) = -\sum_{c} \zeta_\ell^{bc}\, \chi_\ell(bc)\, \bar{\chi}_\ell(c)$

$$= \bar{\chi}_\ell(c)\; g(\chi_\ell).$$

therefore: $\tau(g(\chi_\ell)^{\ell-2})$

$$= \tau(g(\chi_\ell))^{\ell-2}$$

$$= (\bar{\chi}_\ell(c))^{\ell-2}\, g(\chi_\ell)^{\ell-2}$$

$$= g(\chi_\ell)^{\ell-2}$$

this being true for any $\tau \in Gal(K(\zeta_\ell)/K)$. We get:

$$g(\chi_\ell)^{\ell-2} \in K.$$

But $g(\chi_\ell)$ is an algebraic integer, thus:

$$g(\chi_\ell)^{\ell-2} \in \mathcal{O}_K. \quad \square$$

(*) let $\mathbb{Q}[\Delta]$ be the commutative ring defined as follows:

$$\mathbb{Q}[\Delta] = \bigoplus_{\delta \in \Delta} \mathbb{Q}\delta \quad \text{as a } \mathbb{Q}\text{ vector space}$$

$$(\sum x_\delta \delta)(\sum y_{\delta'} \delta')$$

$$= \sum_{\tau \in \Delta} \Big(\sum_{\delta\delta' = \tau} x_\delta y_{\delta'} \Big) \tau$$

Then $\mathbb{Z}[\Delta] = \bigoplus_{\delta \in \Delta} \mathbb{Z}\delta$ is a commutative subring of $\mathbb{Q}[\Delta]$.

We set:

$$\theta = \frac{1}{h} \sum_{a=2}^{h-2} a\, \sigma_a^{-2} \in \mathbb{Q}[\Delta].$$

<u>Theorem</u>

let $\mathfrak{l}$ be a principal ideal of $\mathcal{O}_K$ above ℓ. Then there exists $\sigma_c \in \Delta$ such that:

$$g(\chi_\ell)^{\ell-2}\, \mathcal{O}_K = (\ell-1)\, \sigma_c \theta \cdot \mathfrak{l}.$$

Proof.

$$\begin{array}{ccccc} L = K(\xi_\ell) & \mathfrak{L} & \mathcal{O}_L = \mathbb{Z}[\xi_m, \xi_\ell] = \mathbb{Z}[\xi_{m\ell}] & & \xi_{m\ell} = e^{2i\pi/m\ell} \\ | & & | & & \\ K & \mathfrak{l} & \mathcal{O}_K \quad \mathbb{Z}[\xi_m] & & \\ | & & | & & \\ \mathbb{Q} & \ell & \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} & & \end{array}$$

We have an isomorphism of groups:

$$Cl(\mathbb{Q}(\xi_m, \xi_\ell)/\mathbb{Q}(\xi_\ell)) \simeq Cl(\mathbb{Q}(\xi_m)/\mathbb{Q})$$

We have:

$$\mathfrak{L}^{\ell-1} = \ell \mathcal{O}_L$$

We deduce that $\{ s(\mathfrak{L}) \mid s \in \Delta \}$ is exactly the set of primes of $\mathcal{O}_L$ above ℓ.

We have $g(\chi_\ell)^{\ell-1} g(\overline{\chi_\ell})^{\ell-1} = \ell^{\ell-1}$ thus in the decomposition of $g(\chi_\ell)^{\ell-1}\mathcal{O}_K$ into prime ideals, only the ideals above ℓ appear. Therefore:

$$g(\chi_\ell)^{\ell-1}\mathcal{O}_K = \sum_{a=1}^{h-1} r_a \sigma_a^{-1}\mathfrak{L} \qquad r_a \in \{0, \dots, \ell-1\}$$

Let $\tau \in Cl(K(\xi_\ell)/K)$, $\tau(\xi_\ell) = \xi_\ell^s$. Then $\tau(\mathfrak{L}) = \mathfrak{L}$.

We have:

$$\tau(g(\chi_\ell)) = \overline{\chi_\ell}(s)\, g(\chi_\ell).$$

Now:

$$\frac{\xi_\ell^s - 1}{\xi_\ell - 1} \equiv s \quad (\sigma_a^{-1}\mathfrak{L})$$

We get:

$$\frac{g(\chi_\ell)}{(\xi_\ell - 1)^{r_a}} \equiv \frac{\tau(g(\chi_\ell))}{\tau((\xi_\ell - 1)^{r_a})} \quad (\sigma_a^{-1}\mathfrak{L})$$

$$\equiv \frac{g(\chi_\ell)\, \overline{\chi_\ell}(s)^{-1}}{(\xi_\ell - 1)^{r_a}\, s^{r_a}} \quad (\sigma_a^{-1}\mathfrak{L})$$

Thus:

$$\chi_c(s) \equiv s^{-ra} \; (\sigma_a^{-1}\alpha)$$

i.e.

$$\xi_n \equiv s^{-ra} \; (\sigma_a^{-1}\mathfrak{c}). \qquad \sigma_a^{-1}\alpha \cap \mathcal{O}_K = \sigma_a^{-1}\mathfrak{c}.$$

Finally: $\xi_n^{a} \equiv s^{-ra} \; (\mathfrak{c})$.

But $\xi_n \equiv s^{-\frac{\ell-1}{n}c} \; (\mathfrak{c})$ for some c prime to n.

Thus: $ra \equiv \frac{\ell-1}{n} ca \; (\ell-1)$.

But $ra \in \{0,\dots,\ell-1\}$, thus:

$$ra = (\ell-1)\left\{\frac{ac}{n}\right\}.$$

Now

$$\sum_{a=2}^{n-1} (\ell-1)\left\{\frac{ac}{n}\right\} \sigma_a^{-1}$$

$$= (\ell-1)\,\sigma_c \,\frac{1}{n}\sum_{a=2}^{n-1} a\,\sigma_a^{-1}$$

$$= (\ell-1)\,\sigma_c\,\theta. \quad \square$$

<u>Theorem.</u> (Stickelberger's theorem)

Let $\beta \in \mathbb{Z}[\Delta]$ such that $\beta\theta \in \mathbb{Z}[\Delta]$.

Then,

$$\beta\theta \,.\, \mathcal{C}(K) = \{0\}.$$

<u>Proof.</u> Let $\mathfrak{p} \in \mathcal{C}(K)$. Select, by Čebotarev, $\mathfrak{c} \in \mathfrak{p}$, $\mathfrak{c} \cap \mathbb{Z} = \ell\mathbb{Z}$, $\ell \equiv 1 \; (n)$.

~~Let~~ ~~$\chi =$~~ Then: $g(\chi)^{\ell-2}\mathcal{O}_K = (\ell-1)\,\sigma_c\,\theta\,\mathfrak{c}$.

for some $\sigma_c \in \Delta$.

Let:

$$\gamma = g(x_\ell)^{\pi_\ell^{-2}\beta} \in K(\zeta_\ell).$$

We have:

$$\gamma^{\ell-1} \in K.$$

Furthermore:

$$\gamma^{\ell-1}\mathcal{O}_K = (\beta.\mathcal{O}\,\mathfrak{l})^{\ell-1}$$

this implies that $K(\gamma)/K$ is unramified above every prime ideal of K above ℓ.

But $K(\gamma) \subset K(\zeta_\ell)$ and $K(\zeta_\ell)/K$ is totally ramified at every prime of $\mathcal{O}_K$ above ℓ.

thus $K(\gamma) = K$, i.e. $\gamma \in K$. thus:

$$\beta.\mathcal{O}.\mathfrak{l} = \gamma\mathcal{O}_K.$$

In other words:

$$\beta.\mathcal{O}.\sigma = 0.$$

this holds for every $\sigma \in \mathcal{C}(K)$. $\square$

p is an odd prime.

Let's give some basic facts about $\mathbb{Z}_p[\Delta]$-modules.

$$\mathbb{Q}_p[\Delta] = \bigoplus_{\delta \in \Delta} \mathbb{Q}_p \delta \quad \text{as } \mathbb{Q}_p\text{-vector space}$$

$$\left(\sum x_\delta \cdot \delta\right)\left(\sum y_{\delta'} \cdot \delta'\right) = \sum_{\tau} \left(\sum_{\delta\delta' = \tau} x_\delta y_{\delta'}\right) \tau$$

thus $\mathbb{Q}_p[\Delta]$ is a commutative $\mathbb{Q}_p$-algebra and $\mathbb{Z}_p[\Delta] = \bigoplus_{\delta \in \Delta} \mathbb{Z}_p \delta$ is a subring of $\mathbb{Q}_p[\Delta]$.

Note that: $\theta = \frac{1}{p} \sum_{a=1}^{p-1} a \sigma_a^{-1} \in \mathbb{Q}_p[\Delta] \setminus \mathbb{Z}_p[\Delta]$.

Recall that $(p-1) \sum_{n \geq 0} p^n = 1$ thus $p-1 \in \mathbb{Z}_p^\times$.

Let:

$$\hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times) \simeq \Delta$$

For $\chi \in \hat{\Delta}$, we set:

$$e_\chi = \frac{1}{p-1} \sum_{\delta \in \Delta} \chi^{-1}(\delta)\, \delta \in \mathbb{Z}_p[\Delta].$$

<u>Proposition.</u>

a) $\forall\, \chi, \chi' \in \hat{\Delta}$, $e_\chi e_{\chi'} = \delta_{\chi,\chi'}\, e_\chi$.

b) $\forall\, \delta \in \Delta$, $\delta e_\chi = \chi(\delta)\, e_\chi$

c) $1 = \sum_{\chi \in \hat{\Delta}} e_\chi$ (here $1 = \sigma_1 \in \Delta$).

<u>Proof.</u>

b) $$\delta e_\chi = \frac{1}{p-1} \sum_{\delta' \in \Delta} \chi^{-1}(\delta')\, \delta\delta'$$

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

$$= \chi(\delta)\, e_\chi$$

a)

T.S.V.P.

If $\chi \in \hat{\Delta}$, $\chi \neq 1$. We have:

$\exists\, s_0 \in \Delta$, $\chi(s_0) \neq 1$. thus:

$$\chi(s_0) \sum_{s \in \Delta} \chi(s) = \sum_{s \in \Delta} \chi(s s_0) = \sum_{s \in \Delta} \chi(s)$$

Therefore $(\chi(s_0) - 1) \sum_{s \in \Delta} \chi(s) = 0 \implies \sum_{s \in \Delta} \chi(s) = 0$.

Now,

$$e_{\chi'} e_{\chi}$$

$$= \frac{1}{n-2} \sum_{s \in \Delta} \chi'(s)^{-1} s\, e_{\chi}$$

$$= \frac{1}{n-2} \sum_{s \in \Delta} \chi'(s)^{-1} \chi(s)\, e_{\chi}$$

$$= \left(\frac{1}{n-2} \sum_{s \in \Delta} (\chi \chi'^{-1})(s) \right) e_{\chi}$$

$$= \begin{cases} e_{\chi} & \chi = \chi' \\ 0 & \text{si } \chi \neq \chi' \end{cases}$$

c) let $s \in \Delta$, $s \neq 1$. $\exists\, \chi_0 \in \hat{\Delta}$, $\chi_0(s) \neq 1$.

We have:

$$\chi_0(s) \sum_{\chi \in \hat{\Delta}} \chi(s) = \sum_{\chi \in \hat{\Delta}} \chi\chi_0(s) = \sum_{\chi \in \hat{\Delta}} \chi(s)$$

$$\implies (\chi(s) - 1) \left(\sum_{\chi \in \hat{\Delta}} \chi(s) \right) = 0$$

$$\implies \sum_{\chi \in \hat{\Delta}} \chi(s) = 0.$$

Now $\sum_{\chi \in \hat{\Delta}} e_{\chi}$

$$= \sum_{\chi \in \hat{\Delta}} \frac{1}{n-2} \sum_{s \in \Delta} \chi(s)\, s^{-1}$$

$$= \sum_{s \in \Delta} \frac{1}{n-2} \left(\sum_{\chi \in \hat{\Delta}} \chi(s) \right) s^{-1}$$

$$= 1 \qquad \square$$

Let M be a $\mathbb{Z}_n[\Delta]$-module.

We set:

$$\forall \chi \in \hat{\Delta},\quad M(\chi) = \{m \in M \mid \forall s \in \Delta,\ s.m = \chi(s)\, m\}.$$

<u>Theorem.</u>

a) $M(\chi) = e_\chi M$

b) $M = \bigoplus_{\chi \in \hat{\Delta}} M(\chi)$ (direct sum of $\mathbb{Z}_n$-modules)

<u>Proof.</u>

We have $1 = \sum_{\chi \in \hat{\Delta}} e_\chi$ thus:

$$M = \sum_{\chi \in \hat{\Delta}} e_\chi M.$$

Let $z \in e_\chi M$, $z = e_\chi m$ $m \in \Delta$. We have:

$$s.z = s e_\chi m = \chi(s) e_\chi m = \chi(s)\, z.$$

We therefore get:

$$e_\chi M \subset M(\chi).$$

Let $m = \sum_{\chi \in \hat{\Delta}} m_\chi$, $m_\chi \in e_\chi M$.

~~Then~~:

Let's assume that $m = 0$. Then:

$$0 = e_\chi m$$

$$= \sum_{\psi \in \hat{\Delta}} e_\chi m_\psi$$

$$= \sum_{\psi \in \hat{\Delta}} e_\chi e_\psi m'_\psi \qquad m_\psi = e_\psi m'_\psi$$

$$= e_\chi e_\chi m'_\chi$$

$$= m_\chi$$

thus:

$$M = \bigoplus_{\chi \in \hat{\Delta}} e_\chi M.$$

let $m \in M(\chi)$.

$$s\, e_\psi m$$
$$= \psi(s)\, e_\psi m$$
$$= \chi(s)\, e_\psi m$$

thus:

$$(\chi(s) - \psi(s))\, e_\psi m = 0 \quad \forall s \in \hat{\Delta}.$$

this implies that $e_\psi m = 0$ $\psi \neq \chi$. therefore:

$$M(\chi) \subset e_\chi M$$

and finally $e_\chi M = M(\chi)$. $\square$

Examples.

1) $M = \mathbb{Z}_n[\Delta]$ viewed as a $\mathbb{Z}_n[\Delta]$ module.

$\forall \chi \in \hat{\Delta}$, $e_\chi M = \mathbb{Z}_n e_\chi$.

thus $M = \bigoplus_{\chi \in \hat{\Delta}} \mathbb{Z}_n e_\chi$

2) $M = \mathbb{Z}_n$ viewed as a $\mathbb{Z}_n[\Delta]$ module with trivial action of Δ.

$\forall \chi \in \hat{\Delta}$, $\chi \neq 1$ $\quad M(\chi) = e_\chi M = 0$

If $\chi = 1$,

$$M(1) = e_\chi M = \mathbb{Z}_n.$$

Remark. let $(M, +)$ be a finite Abelian p-group.
then M is not finally a $\mathbb{Z}_p$-module.
If $p^N = |M|$, we get:

$$\forall m \in M, \quad \sum_{i \geq 0} x_i p^i \cdot m = \sum_{i=0}^{N-1} x_i p^i \cdot m$$

Furthermore there exist $0 \leq e_1 \leq e_2 \leq \dots \leq e_r$ such that:

$$M \simeq \mathbb{Z}_p / p^{e_1} \mathbb{Z}_p \times \dots \times \frac{\mathbb{Z}_p}{p^{e_r} \mathbb{Z}_p}$$

$\mathrm{Ann}_{\mathbb{Z}_p} M = p^{e_r} \mathbb{Z}_p$ $\qquad \mathrm{Filt}_{\mathbb{Z}_p} M = p^{e_1 + \dots + e_r} \mathbb{Z}_p$

the Herbrand-Ribet theorem (2)

p: an odd prime.

$$X = \hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times) = \mathbb{F}_p^\times$$

Since $\forall a \in \mathbb{Z}\setminus p\mathbb{Z}$, $\omega_p(\sigma_a) := \omega_p(a) \equiv a\,(p)$.

We have:

$$o(\omega_p) = p-1.$$

Thus,

$$X = \langle \omega_p \rangle = \{ \omega_p^k,\ 0 \le k \le p-1 \}.$$

Since $\omega_p(-1)^2 = 1$ and $\omega_p(-1) \equiv -1\,(p)$. We get.

$$\omega_p(-1) = -1.$$

We set:

$$X_{odd} = \{ \chi \in X \mid \chi(-1) = -1 \}$$
$$= \{ \omega_p^n,\ 1 \le n \le p-2,\ n \equiv 1\,(2) \}.$$

Let $\chi \in X$,

$$e_\chi \theta$$
$$= e_\chi \left(\frac{1}{p} \sum_{a=2}^{p-2} a\, \sigma_a^{-2} \right)$$
$$= \left(\frac{1}{p} \sum_{a=2}^{p-2} \chi^{-2}(a)\, a \right) e_\chi$$

Thus $\forall \chi \in X$, we set,

$$B_{1,\chi} = \frac{1}{p} \sum_{a=2}^{p-2} \chi^{-2}(a)\, a \in \mathbb{Q}_p.$$

We have:

$$\forall \chi \in X,\quad e_\chi \theta = B_{1,\chi^{-2}}\, e_\chi.$$

Remark. If $\chi = 1$,

$$B_{1,\chi} = \frac{1}{p} \sum_{a=2}^{p-2} a = \frac{p-1}{2}$$

T.S.V.P. →

Lemma $\forall \chi \in X$.

$$B_{1,\chi} \equiv \begin{cases} 0 \ (\mathbb{Z}_h) & \chi \neq \omega_h^{-2} \\ -\frac{1}{h} \ (\mathbb{Z}_h) & \chi = \omega_h^{-2} \end{cases}$$

Proof.

Write $\chi = \omega_h^{n}$ $\quad n \in \{0, \dots, h-1\}$.

We have:

$$\sum_{a=1}^{h-1} \chi(a)\, a$$

$$\equiv \sum_{a=1}^{h-1} a^{n+1} \ (h)$$

$$\equiv \begin{cases} 0 \ (h) & n+1 \not\equiv 0 \ (h-1) \quad \text{i.e. } \chi \neq \omega_h^{-2} \\ -1 \ (h) & n+1 \equiv 0 \ (h-1) \quad \text{i.e. } \chi = \omega_h^{-2}. \end{cases}$$

The lemma follows. $\square$

Lemma. Let $\chi \in X$, $\chi \neq 1$ and $\chi(-1) = 1$.

then: $B_{1,\chi} = 0$.

Proof.

$$B_{1,\chi} = \frac{1}{h} \sum_{a=1}^{h-1} \chi(a)\, a$$

$$= \frac{1}{h} \sum_{a=1}^{h-1} \chi(h-a)\,(h-a)$$

$$= -\frac{1}{h} \sum_{a=1}^{h-1} \chi(-a)\, a \qquad \chi \neq 1$$

$$= -\frac{1}{h} \sum_{a=1}^{h-1} \chi(a)\, a \qquad \chi(-1) = 1$$

$$= -B_{1,\chi}. \qquad \square$$

Remark. $\chi \in X$, $\chi \neq 1$.

$s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$,

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

$$= \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

One can show that $L(s,\chi)$ can be analytically continued to a holomorphic function on $\mathbb{C}$. Furthermore,

$$L(1,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n} \in \mathbb{C}^\times.$$

One can prove that if $\chi \in X_{odd}$, we have:

$$\frac{L(1,\chi)\, \tau(\chi^{-1})}{2i\pi} = -\frac{1}{2} B_{1,\chi^{-1}}$$

where $\tau(\chi^{-1}) = \sum_{a=1}^{n} \overline{\chi}(a)\, e^{2i\pi a/n} \in \mathbb{C}^\times$.

Thus $\forall\, \chi \in X_{odd}$, $B_{1,\chi} \neq 0$.

<u>Open Problem</u>: Give an algebraic proof of the fact that $B_{1,\chi} \neq 0$ $\forall\, \chi \in X_{odd}$.

Let $\chi \in X$ odd set $\tau(\chi) = \sum_{a=1}^{n} \chi(a)\, \zeta_n^a$. (recall let $\zeta_n = e^{2i\pi/n}$)

<u>Proposition</u>. $\forall\, \chi \in X$, $\chi \neq 1$, we have:

$$\tau(\chi)\, \overline{\tau(\chi)} = n$$

Proof.

$$(n-1)\, \tau(\chi)\, \overline{\tau(\chi)} = \sum_{b=1}^{n} \chi(b)\, \overline{\chi}(b)\, \tau(\chi)\, \overline{\tau(\chi)}$$

$$= \sum_{b=1}^{n} \overbrace{\left(\sum_{a=1}^{n} \chi(a)\, e^{2i\pi ab/n}\right)\left(\sum_{c=1}^{n} \overline{\chi}(c)\, e^{-2i\pi cb/n}\right)}^{\overline{\chi}(b)\,\tau(\chi)}$$

$$= \sum_{a,c} \chi(a)\, \overline{\chi}(c) \sum_{b} e^{2i\pi b(a-c)/n}$$

$$= \sum_{\substack{a=c \\ a}} 1 = n. \quad \square$$

Proposition.

$\chi \in X_{odd}$.

$$\sum_{a=2}^{n} \frac{\overline{\chi}(a)}{\zeta_n^a - 1} = B_{1,\chi}\, \tau(\chi^{-1}).$$

Proof.

Let $\alpha(\chi) = \tau(\overline{\chi^{-1}}) \sum_{a=2}^{n} \frac{\overline{\chi}(a)}{\zeta_n^a - 1}$.

We have,

$$\alpha(\chi) = \sum_{a,b} \chi(b)\, \zeta_n^{-b}\, \frac{\overline{\chi}(a)}{\zeta_n^a - 1}$$

$$= \sum_{a,b} \chi(b)\overline{\chi}(a) \frac{\zeta_n^{-b}}{\zeta_n^a - 1}$$

$$= \sum_{a,b \in \mathbb{F}_n^\times} \chi(ba^{-1}) \frac{\zeta_n^{-ba^{-1}a}}{\zeta_n^a - 1}$$

$$= \sum_{a,c \in \mathbb{F}_n^\times} \chi(c) \frac{\zeta_n^{-ca}}{\zeta_n^a - 1}$$

$$= -\sum_{a,c \in \mathbb{F}_n^\times} \chi(c) \frac{\zeta_n^{ca}}{\zeta_n^a - 1}$$

$$= \sum_{a,c \in \mathbb{F}_n^\times} \chi(c) \frac{\zeta_n^{ac} - 1}{\zeta_n^a - 1} \qquad \chi \neq 1$$

$$= -\sum_{a,c \in \mathbb{F}_n^\times} \chi(c) \left(1 + (\zeta_n^a) + \cdots + (\zeta_n^a)^{c-1}\right)$$

$$= -\sum_{c \in \mathbb{F}_n^\times} \chi(c) \sum_{a \in \mathbb{F}_n^\times} \left(1 + (\zeta_n^a) + \cdots + (\zeta_n^a)^{c-1}\right)$$

$$= -\sum_{c \in \mathbb{F}_n^\times} \chi(c) \sum_{a \in \mathbb{F}_n^\times} \left(\zeta_n^a + \cdots + (\zeta_n^a)^{c-1}\right)$$

$$= -\sum_{c \in \mathbb{F}_n^\times} \chi(c) \cdot -(c-1)$$

$$= \sum_{c \in \mathbb{F}_n^\times} c\,\chi(c)$$

$$= n\, B_{1,\chi}.$$

$$= \tau(\chi^{-1})\, \tau(\overline{\chi^{-1}})\, B_{1,\chi} \qquad \square$$

Let $E = \mathbb{Q}_n(\zeta_n)$.

Then $E/\mathbb{Q}_n$ is a Galois extension and:

$$\Delta \simeq \mathrm{Gal}(E/\mathbb{Q}_n).$$

$$E = \bigoplus_{k=0}^{n-2} \mathbb{Q}_n \zeta_n^k$$

$x \in E$, $x = \sum_{k \geq 0} x_k \zeta_n^k$ $\qquad \sigma_a(x) = \sum_{k=0}^{n-2} x_k \sigma_a(\zeta_n)^k$

$$= \sum_{k=0}^{n-2} x_k \zeta_n^{ak}$$

$$R = \mathbb{Z}_n[\zeta_n] = \bigoplus_{k=0}^{n-2} \mathbb{Z}_n \zeta_n^k$$

R is a discrete valuation ring, its maximal ideal is:

$$\mathfrak{m} = (\zeta_n - 1) R.$$

In particular:

$$nR = \mathfrak{m}^{n-1}$$

$$R/\mathfrak{m}R \simeq \mathbb{F}_n$$

R ~~ad~~ is a $\mathbb{Z}_n[\Delta]$-module. Let $\chi \in X$, then:

$$e_\chi \zeta_n = \frac{1}{n-1} \tau(\chi^{-1})$$

Since R is complete in the $\mathfrak{m}$-adic topology, $\forall\, h(x) \in \mathbb{Z}_n[[X]]$, $\forall\, z \in \mathfrak{m}$, $h(z) \in R$.

<u>Theorem</u> (J. Tate)

There exists $\lambda \in R$, $\lambda^{n-2} = -n$ and there exists $g(x) \in \mathbb{Z}_n[[X]]$ such that:

1) $g(\lambda) = \zeta_n$.

2) $g(x) \equiv \exp(x) \quad (x^{n-1})$

3) $\forall a \in \mathbb{Z} \setminus n\mathbb{Z}$, $\sigma_a(\lambda) = \omega_n(a)\lambda$.

~~Proof~~

3) $\sigma_a(\lambda^{n-2}) = \sigma_a(\lambda)^{n-2} = \sigma_a(-n) = -n$.

Thus $\sigma_a(\lambda) = N\lambda \quad N \in N_{n-2}$.

But $g(\lambda) = \xi_n$ thus:

$$\sigma_a(g(\lambda)) = g(\sigma_a(\lambda)) = \xi_n^a = g(\lambda)^a.$$

Since $g(x) \equiv x \ (x^2)$, we get:

$$g(\lambda)^a \equiv a\lambda \ (\lambda^2)$$

thus:

$$\sigma_a(\lambda) \equiv a\lambda \ (\lambda^2)$$

We get: $N \equiv a \ (m)$ since $\lambda \in m_0$.

thus $N \equiv a \ (n)$ since $m_0 \cap \mathbb{Z}_n = n\mathbb{Z}_n$

thus $N = \omega_n(a)$. $\square$

<u>Proposition.</u>

$\chi \in X$, $\chi = \omega_h^n$ $\quad 1 \leq n \leq h-2$.

We have:

$$\tau(\chi^{-1}) \equiv -\frac{\lambda^n}{n!} \quad (hR)$$

Proof.

$$c_\chi \, \varepsilon_h = \frac{1}{h-2} \tau(\chi^{-1}) \equiv -\tau(\chi^{-1}) \quad (hR)$$

Now, $e_\chi \varepsilon_h = \frac{1}{h-2} \sum_a \chi^{-1}(a) \, \sigma_a(\varepsilon_h)$

$$= \frac{1}{h-2} \sum_a \chi^{-1}(a) \, \sigma_a(\gamma(\lambda))$$

$$\equiv \frac{1}{h-2} \sum_a \chi^{-1}(a) \, \sigma_a\left(\sum_{k=0}^{h-2} \frac{\lambda^k}{k!}\right) \quad (hR)$$

$$\equiv \frac{1}{h-2} \sum_a \chi^{-1}(a) \sum_{k=0}^{h-2} \frac{\omega_h(a)^k \lambda^k}{k!} \quad (hR)$$

$$\equiv \sum_{k=0}^{h-2} \frac{\lambda^k}{k!} \left(\frac{1}{h-2} \sum_{a \in} \omega_h^{k-n}(a)\right) \quad (hR)$$

$$\equiv \frac{\lambda^n}{n!} \quad (hR). \quad \square$$

<u>Theorem.</u> $\chi = \omega_h^n$, $1 \leq n \leq h-4$, $n \equiv 1 \ (2)$.

then:

$$B_{1,\chi} \equiv \frac{B_{n+1}}{n+1} \quad (h)$$

Proof.

We have:

$$\frac{\lambda}{\varepsilon_{h-2}} = \frac{\lambda}{\gamma(\lambda)} \equiv \sum_{k=0}^{h-3} B_k \frac{\lambda^k}{k!} \quad (hR)$$

then:

$$\frac{1}{\varepsilon_{h-2}} \equiv \frac{1}{\lambda} + \sum_{k=2}^{h-3} \frac{B_k}{k} \frac{\lambda^{k-1}}{(k-1)!} \quad (m_0^{h-2})$$

Here we use $\lambda R = m_0$ since $\frac{\lambda}{\varepsilon_{h-2}} \equiv 1 \ (m_0)$.

thus:

$$e_\chi \frac{1}{\varepsilon_{h-2}} \equiv e_\chi \frac{1}{\lambda} + \sum_{k=2}^{h-3} \frac{B_k}{k} e_\chi \frac{\lambda^{k-1}}{(k-1)!} \quad (m_0^{h-2})$$

T.S.V.P.

$i \in \mathbb{Z}$

$$e_\chi \lambda^i = \left(\frac{1}{h-2} \sum_a \chi(a)\, \omega_h^{-i}(a)\right) \lambda^i$$

$$= \begin{cases} \lambda^i & \text{si } \chi = \omega_h^i \\ 0 & \text{sinon} \end{cases}$$

thus:

$$e_\chi \frac{1}{\xi_h - 1} \equiv \frac{B_{n+1}}{n+1} \frac{\lambda^n}{n!} \quad (m^{h-2})$$

But $$e_\chi \frac{1}{\xi_h - 1} = \frac{1}{h-1} \sum_{a=1}^{h-1} \frac{\overline{\chi}(a)}{\xi_h^a - 1}$$

$$= \frac{1}{h-1} B_{1,\chi}\, \tau(\chi^{-1})$$

$$\equiv B_{1,\chi} \frac{\lambda^n}{n!} \quad (m^{h-2})$$

thus: $$B_{1,\chi} \equiv \frac{B_{n+1}}{n+1} \quad (m) \quad \text{si } n < h-2$$

Therefore $$B_{1,\chi} \equiv \frac{B_{n+1}}{n+1} \quad (h)$$

Let H_p be the p-Sylow ~~group~~ subgroup of $Cl(K)$ where $K = \mathbb{Q}(\zeta_p)$.
Then H is a finite abelian p-group thus a $\mathbb{Z}_p$-module.
Note that Δ acts on H and therefore H is a $\mathbb{Z}_p[\Delta]$-module.

Therefore we have a direct sum of (finite) $\mathbb{Z}_p$-modules:

$$H_p = \bigoplus_{\chi \in \hat{\Delta}} H_p(\chi),$$

where $H_p(\chi) = \{ h \in H_p \mid \forall s \in \Delta,\ s.h = \chi(s) h \}$.

<u>Theorem</u> (Herbrand - Ribet 1976-) p: an odd prime
Let $\chi = \omega_p^{n}$, $3 \leq n \leq p-2$, $n \equiv 1 (2)$.
We have:

$$H(\chi) \neq \{0\} \iff B_{p-n} \equiv 0 (p)$$

We will only prove $\Rightarrow$ called Herbrand's Theorem:

By Stickelberger's Theorem, $\forall \beta \in \mathbb{Z}[\Delta]$, $\beta\theta \in \mathbb{Z}[\Delta]$, we have:

$$\beta\theta \ H(\chi) = \{0\}.$$

Let $c \in \mathbb{Z} \setminus p\mathbb{Z}$, then:

$$(c - \sigma_c) \sum_{a=2}^{p-2} a \sigma_a^{-1}$$

$$\equiv \sum_a ac \ \sigma_a^{-1} - \sigma_c \sum_a a \ \sigma_a^{-1} \quad (p)$$

$$\equiv \sum ac \ \sigma_{ac}^{-1} \sigma_c - \sigma_c \sum a \ \sigma_a^{-1} \quad (p)$$

$$\equiv 0 \quad (p).$$

thus $(c - \sigma_c)\theta \in \mathbb{Z}[\Delta]$.

T.S.V.P. →

let $c \in \mathbb{Z}$ such that $c^{n-2} \not\equiv 1 \ (n)$.

$$(c-\sigma_c)\theta \ H_n(\chi)$$

$$= (c-\sigma_c)\theta \ e_\chi H_n$$

$$= (c-\chi(c)) \ B_{1,\chi} \ e_\chi H_n$$

But $c-\chi(c) \equiv c-c^n \ (n)$. thus $c-\chi(c) \in \mathbb{Z}_n^\times$.

Therefore $B_{1,\chi^{-1}} H_n(\chi) = \{0\}$. since $H_n(\chi) \neq \{0\}$, this implies:

$$B_{1,\chi^{-1}} \equiv 0 \ (n).$$

But $B_{1,\chi^{-1}} = B_{1,\omega_n^{n-2}}$

$$\equiv \frac{B_{n-n}}{n-n} \ (n)$$

Therefore $B_{n-n} \equiv 0 \ (n)$. $\square$

<u>Theorem</u> (B. Mazur – A. Wiles 1980–)

Let $\chi = \omega_p^n$, $3 \leq n \leq p-2$, $n \equiv 1 (2)$.

$$\mathrm{Fitt}_{\mathbb{Z}_p} H_p(\chi) = B_{1,\chi} \mathbb{Z}_p$$

<u>Conjecture</u> (Iwasawa – Leopoldt)

For any odd prime number p, for any odd number n, $3 \leq n \leq p-2$, we have:

$$H_p(\omega_p^n) \simeq \mathbb{Z}_p / B_{1,\chi} \mathbb{Z}_p$$

<u>Conjecture</u> (Kummer – Vandiver)

The odd class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is prime to p.

We have:

$$H_p = \bigoplus_{\chi \in \hat{\Delta}} H_p(\chi)$$

<u>Theorem</u> (Spiegelungssatz – Leopoldt)

Let $1 \leq n \leq p-2$, $n \equiv 1 (2)$. Then:

$$\dim_{\mathbb{F}_p} \frac{H_p(\omega_p \chi^{-1})}{p H_p(\omega_p \chi^{-1})} \leq \dim_{\mathbb{F}_p} \frac{H_p(\chi)}{p H_p(\chi)} \leq \dim_{\mathbb{F}_p} \frac{H_p(\omega_p \chi^{-1})}{p H_p(\omega_p \chi^{-1})} + 1$$

where $\chi = \omega_p^n$.

Now the Kummer – Vandiver conjecture for the prime p is equivalent to:

$$\forall \chi \in X, \ \chi(-1) = 1, \quad H_p(\chi) = \{0\}.$$

Therefore, in this case, $\forall \chi \in X_{od}$, $H_p(\chi)$ is a cyclic group.

By the analytic class number formula, we get:

$$H_p(\chi) \simeq \mathbb{Z}_p / B_{1,\chi} \mathbb{Z}_p.$$
