

$\Phi_n \in \mathbb{Z}[x]$, χ צימודים ζ , $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)}$ (d,n)=1

$\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$, $\Phi_p(x) = x^{p-1} - 1$ כי $\Phi_p(x) = x^{p-1} - 1$ כי $\Phi_p(x) = x^{p-1} - 1$

$Q(\zeta_n) = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n)$

בסדר: $2 < q = p^n$ יהי $\zeta = \zeta_q$ $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_2, \zeta_p)$ כי $\zeta = \zeta_2 \zeta_p$ $L = \mathbb{Q}(\zeta)$ $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_2, \zeta_p)$

$\Gamma: \mathbb{Q} \rightarrow \mathbb{Q}$ (1)

ζ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ (2)

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ (3)

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ (4)

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ כי $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$

-1) , 0) ל מרחב 3, 4) ל מרחב 2

$$\Delta(0/\mathbb{Z}) | \Delta(\mathbb{Z})$$

$\Delta(0/\mathbb{Z}) = \mathbb{Z}$ פז יס' $\Delta(\mathbb{Z}) = \mathbb{Z}$ זנת ילול ע' אל, פז
 , ומד2 ודלול - 0) ל, פז

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(\zeta) = \prod_{i=1}^{p-1} \zeta^i = \zeta^{\sum_{i=1}^{p-1} i} = \zeta^{\frac{p-1}{2}(p-1)}$$

$$p \text{ זנת } \mathbb{Z} \text{ זנת } \mathbb{Z} \text{ זנת } \mathbb{Z} = \zeta^{\frac{p-1}{2}(p-1)}$$

$$(1-x) \bar{\Phi}_p(x) = x^p - 1$$

-1) (זבול) רעל

$$(1-y) \bar{\Phi}'_p(y) = p y^{p-1}$$

$$\bar{\Phi}'_p(y) = \frac{p y^{p-1}}{1-y}$$

$$\bar{\Phi}'_q(x) = \bar{\Phi}'_p(x^{p^{a-1}})$$

$$\bar{\Phi}'_q(x) = \bar{\Phi}'_p(x^{p^{a-1}}) \cdot p^{a-1} \cdot x^{p^{a-1}-1}$$

$$\bar{\Phi}'_p(\zeta) = \frac{p y^{p-1}}{1-y} \cdot p^{a-1} \cdot x^{p^{a-1}-1} =$$

$$= \frac{p^a y^{p-1}}{1-y} \cdot y^j = \boxed{\frac{p^a \cdot \zeta^{-1}}{1-\zeta}}$$

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{p^a}) = p^{a \cdot \varphi(p)} \cdot (-1)^{\varphi(p)}$$

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{p^a}) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta)^{p^a} = p^{a \cdot (p-1)}$$

$$\varphi(p^a) = \varphi(p) = p-1$$

$$\Delta(\mathbb{Z}) = (-1)^{\varphi(p)(\varphi(p)-1)/2} \cdot p^{a \cdot (p-1)}$$

! 215 וזה $\varphi(q) = m \cdot p$ כי

$\Leftrightarrow \varphi(q) = 0, 1 \pmod{4} \Leftrightarrow 4 \mid \varphi(q) - 1 \parallel 4 \mid \varphi(q) \Leftrightarrow q \equiv 1 \pmod{4}$
 $p \mid 0 \Rightarrow \dots$ $p = 2^a, a \geq 1, p \equiv 1 \pmod{4}$
 $\dots \cdot r = p^{a-1} (ap - a - 1)$

$p^r \mathbb{O} \subseteq \mathbb{Z}[\zeta]$

$\cdot p^r, f(\beta) = 1 \leftarrow$ \dots p

$\mathbb{O}/\alpha \mathbb{O} = \mathbb{Z}/p\mathbb{Z}$
 $= \mathbb{F}_p$

בגודל $\mathbb{Z}[\zeta] = p^r$ \dots $\mathbb{Z}[\zeta] \rightarrow$

$\mathbb{O} = \mathbb{Z}[\zeta] + \alpha \mathbb{O}$

$\alpha = 2 \dots$

$\alpha \mathbb{O} \subseteq \mathbb{Z}[\zeta] + \alpha^2 \mathbb{O}$

p^d

$\mathbb{O} \subseteq \mathbb{Z}[\zeta] + \alpha^2 \mathbb{O} \subseteq \mathbb{O}$

\dots

$\mathbb{O} \subseteq \mathbb{Z}[\zeta] + \alpha^{2^k} \mathbb{O} \subseteq \mathbb{O}$

\dots

$\mathbb{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathbb{O} \Rightarrow \mathbb{Z}[\zeta] = \mathbb{O}$

\square

\dots

\dots

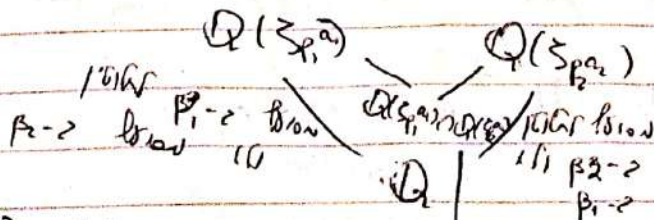
$m = p^{a_1} \dots p^{a_r}$

\dots

$\mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_{p^{a_1}} \dots \zeta_{p^{a_r}}] =$

$= \mathbb{Q}[\zeta_{p^{a_1}}] \dots \mathbb{Q}[\zeta_{p^{a_r}}]$

\dots



\dots

צ'ב'נ'ל \Rightarrow \mathbb{Q} \mathbb{R} \mathbb{C} \mathbb{Q} \mathbb{R} \mathbb{C} \mathbb{Q} \mathbb{R} \mathbb{C} \mathbb{Q} \mathbb{R} \mathbb{C}

$$[\mathbb{Q}(\zeta_{p_1 a_1} - \zeta_{p_1^{a_1}}) : \mathbb{Q}] = \varphi(p_1^{a_1}) \cdot \frac{\varphi(p_2^{a_2})}{\varphi(p_1^{a_1})} = \varphi(p_1^{a_1} p_2^{a_2})$$

$$\Delta_{p_1 p_2^{a_2}} = \Delta_{p_1} \Delta_{p_2^{a_2}}$$

$$\Rightarrow \mathbb{O} = \sum [\zeta_{p_1 a_1} \zeta_{p_2 a_2}] = \sum [\zeta_{p_1 p_2^{a_2}}]$$

- $\mathbb{Q}(\zeta_m) : \mathbb{Q} = \varphi(m)$

$$\mathbb{O} = \sum [\zeta_m]$$

$p \mid m \Leftrightarrow$ ζ_m^p

$$\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$$

$\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

$$\sigma \Big| : \begin{matrix} \mu_m & \rightarrow & \mu_m \\ \mu_m & \mapsto & \mu_m \end{matrix}$$

$$(\mathbb{Z}/m\mathbb{Z})^* \quad (\mathbb{Z}/m\mathbb{Z})^*$$

$\mathbb{Z}/m\mathbb{Z}$ $\mathbb{Z}/m\mathbb{Z}$ $\sigma \in \text{Aut}(\mathbb{Z}/m\mathbb{Z})$

$p > 2$ $(\mathbb{Z}/p\mathbb{Z})^*$ $p > 2$ $(\mathbb{Z}/p\mathbb{Z})^*$

$$1 \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\pm 1} 1$$

$(a, p) = 1$ $a \in \mathbb{Z}$ $\mathbb{Z}/p\mathbb{Z}$ $\mathbb{Z}/p\mathbb{Z}$ $\mathbb{Z}/p\mathbb{Z}$

$$\left(\frac{a}{p}\right) = (a)^{\frac{p-1}{2}} \pmod{p} \in \{\pm 1\}$$

$\left(\frac{a}{p}\right) = 0$ if $p \mid a$.
 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Legendre symbol $\left(\frac{a}{p}\right)$ for $p=3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Galois group of L/\mathbb{Q} is cyclic of order $p-1$.
 $\sigma \in \text{Gal}(L/\mathbb{Q})$

$$\sigma(x) = x^2$$

$$\left(\frac{x \mapsto x^2}{\text{Gal}(L(\sqrt{x})/\mathbb{Q})}\right)$$

Frobenius automorphism $\sigma = \text{Frob}_{q, L}$

$$E(p) = (-1)^{\frac{p-1}{2}}$$

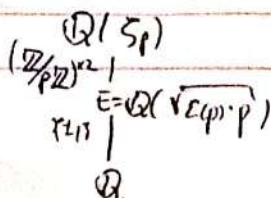
$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{Z}/p\mathbb{Z}$$

$$\text{Frob}_{q, \mathbb{Q}(\zeta_p)} = q$$

$$\sum \text{Frob}_q = \sum \zeta^2 \pmod{p}$$

$$\sum \zeta^q = \sum \zeta^2 \pmod{p}$$

$$\text{Frob}_q = q$$



$E = \mathbb{Q}(\sqrt[p]{\Delta})$: נורמל
 יש $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ (כמה פעמים Δ נכנס ל $\mathbb{Q}(\zeta_p)$) -> Δ אינו
 . $\text{Frob}_{q, \mathbb{Q}(\zeta_p)/E} = \left(\frac{\Delta}{q}\right)$

הוכחה : $\Delta \in \mathbb{Q}(\zeta_p)$, $\Delta = \sqrt[p]{\Delta} \in \mathbb{Q}(\zeta_p)$
 $\mathbb{Q}(\sqrt[p]{\Delta}) \subseteq \mathbb{Q}(\zeta_p)$
 כ"כ : $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ -> Δ אינו נכנס ל $\mathbb{Q}(\zeta_p)$

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\text{res}} \text{Gal}(E/\mathbb{Q})$$

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/p\mathbb{Z}$$

$\left(\frac{\Delta}{q}\right) = 1 \Leftrightarrow \Delta \in \mathbb{Q}(\zeta_p) \Leftrightarrow \text{Frob}_{q, \mathbb{Q}(\zeta_p)/E} = 1$, $p \nmid \Delta$
 הוכחה : $\Delta \in \mathbb{Q}(\zeta_p) \Leftrightarrow \Delta = \sum_{i=1}^p a_i \zeta_p^i$, $\Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$

$$\Delta \in \mathbb{Q}(\zeta_p) \Leftrightarrow \Delta = \sum_{i=1}^p a_i \zeta_p^i$$

$$\text{Frob}_{q, E} = \text{Frob}_{q, \mathbb{Q}(\zeta_p)/E}$$

נניח $\Delta \in \mathbb{Q}$, $\Delta \neq 0$, $\Delta \in \mathbb{Q}(\zeta_p)$, $\Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$
 $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$, $\Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$
 $\text{Frob}_{q, \mathbb{Q}(\zeta_p)/E} = \left(\frac{\Delta}{q}\right)$

הוכחה : $\Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$, $\Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$
 $\left(\frac{\Delta}{q}\right) = 1 \Leftrightarrow \Delta \in \mathbb{Q} \Leftrightarrow \sum_{i=1}^p a_i = 0$
 $\text{Frob}_{q, E} = 1 \Leftrightarrow \text{Frob}_{q, \mathbb{Q}(\zeta_p)/E} = 1$

אנחנו רוצים להראות ש $d = \mathcal{E}(p) = 2$ כאשר p ראשוני.

$$\left(\frac{\mathcal{E}(p)}{p}\right) \cdot \left(\frac{p}{\mathcal{E}(p)}\right) = \left(\frac{\mathcal{E}(p)}{p}\right) = \text{Frob}_{2, \mathbb{Q}(\sqrt{p})} = \left(\frac{2}{p}\right)$$

↓
ערך של

□

$$\left(\frac{2}{p}\right) \cdot \left(\frac{p}{2}\right) = \left(\frac{\mathcal{E}(p)}{2}\right) = \left(\frac{-1}{2}\right)^{p/2} = (-1)^{\frac{p-1}{2} \cdot \frac{p-1}{2}}$$

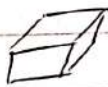
כעת נראה ש $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}$ עבור p ראשוני.

הצגת המרחב הריבועי

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ - נבחר בסיס $\{u_1, \dots, u_n\}$ עבור \mathbb{C} מעל \mathbb{R} .

המרחב \mathbb{C} הוא מרחב וקטורי ממד $2n$ מעל \mathbb{R} .

$$C = \left\{ \sum_{i=1}^n a_i u_i \mid 0 \leq a_i \leq r_i \right\}, \text{Vol}(C) = r_1 \cdots r_n$$



$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

$$C' = \left\{ \sum_{i=1}^n r_i v_i \mid 0 \leq r_i \leq a_i \right\}$$



$$\text{Vol}(C') = |\det(A)| \cdot a_1 \cdots a_n$$

הצגת הבעיה

נניח $L \subseteq \mathbb{Z}^n$ היא רשת סגורה.

$$L = v_1 \mathbb{Z} + \dots + v_n \mathbb{Z}$$

אם $k = n$ אז L היא רשת סגורה במרחב \mathbb{R}^n .

אם $k < n$ אז L היא רשת סגורה במרחב \mathbb{R}^k .

אם L היא רשת סגורה במרחב \mathbb{R}^n אז L היא רשת סגורה במרחב \mathbb{R}^k .

אם L היא רשת סגורה במרחב \mathbb{R}^n אז L היא רשת סגורה במרחב \mathbb{R}^k .

אם L היא רשת סגורה במרחב \mathbb{R}^n אז L היא רשת סגורה במרחב \mathbb{R}^k .

אם L היא רשת סגורה במרחב \mathbb{R}^n אז L היא רשת סגורה במרחב \mathbb{R}^k .

אם L היא רשת סגורה במרחב \mathbb{R}^n אז L היא רשת סגורה במרחב \mathbb{R}^k .

$$T = \left\{ \sum_{i=1}^n r_i v_i \mid 0 \leq r_i < 1 \right\}$$

$$\text{Vol}(T) = \text{Vol}(L) - \text{...}$$

$V = \sum_{i=1}^n r_i v_i$
 $\sum_{i=1}^n r_i v_i = \sum_{i=1}^n (r_i + t_i) v_i - \sum_{i=1}^n t_i v_i$

... $0 \leq r_i < 1$, ... $a = n+1$... $a \in \mathbb{Z}$... $a \in V$...

$$U = \sum_{i=1}^n a_i v_i = \sum_{i=1}^n m_i v_i + \sum_{i=1}^n r_i v_i$$

$U(m) = \left\{ \sum_{i=1}^n r_i v_i \mid \sum_{i=1}^n r_i^2 = m^2, r_i \in \mathbb{Z} \right\}$

\exists ... \Leftrightarrow ... V ... L ...

... n ... L ...

$$|U(m) \cap L| = \left| \sum_{i=1}^n r_i v_i \mid \sum_{i=1}^n r_i^2 = m^2, r_i \in \mathbb{Z} \right| \leq (2m+1)^n < \infty$$

$V = \mathbb{R}v_1$... $L=0$... $n=1$...

$$L \cap U(m) \neq \emptyset \iff \exists \sum_{i=1}^n r_i v_i \in L \text{ s.t. } \sum_{i=1}^n r_i^2 = m^2$$

$\forall u \in L, u = \alpha v, \alpha \in \mathbb{R}$

$\forall u \in L, \alpha u \in L$

$$x = u + y, u \in L, y \in (0,1)$$

$$L \ni \omega - uu = yu \Rightarrow y = 0$$

סדרת וקטורים $v_1, \dots, v_n \in L$

$$L_0 = L \cap V_0, V_0 = \mathbb{R}v_1 + \dots + \mathbb{R}v_n$$

$$L_0 = \sum \mathbb{R}u_i + \dots + \sum \mathbb{R}u_{n-1}$$

$\lambda = \sum_{i=1}^{n-1} r_i u_i + r_n u_n \in L$

L

12

V

$x, y \in X$

$\frac{x+y}{2} \in X$

$\tau \subseteq V$

$\phi \neq \lambda + \tau$