Cél:

<u>Tétel</u> $\mathbb{Q}_p^\times \simeq p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$, $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times \underset{\substack{\downarrow \\ \text{torzió}}}{(1+p\mathbb{Z}_p)}$

p ptlan $\Rightarrow$ $(1+p\mathbb{Z}_p, \cdot) \simeq (\mathbb{Z}_p, +)$ ↳ torziómentes

$\log \longrightarrow$

$\longleftarrow \exp$

$p=2$ $\quad 1+2\mathbb{Z}_2 \simeq C_2 \times (\mathbb{Z}_2, +)$ $\quad (\mathbb{F}_2^\times = \{1\})$

± 1

<u>Köv.:</u> $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \simeq \begin{cases} C_2 \times C_2 & (p \neq 2) \\ C_2 \times C_2 \times C_2 & (p=2). \end{cases}$ $\quad \mathbb{R}^\times / (\mathbb{R}^\times)^2 \simeq C_2$

<u>Lemma</u> $f_1, \dots, f_k \in \mathbb{Z}_p[x_1, \dots, x_m]$ polinomok.

Ekvivalensek:

(1) $f_1, \dots, f_k$-nak van közös gyöke $\mathbb{Z}_p^m$-ben.

(2) $f_1, \dots, f_k$-nak ——||—— $\left(\mathbb{Z}/(p^n)\right)^m$-ben $\forall n \geq 1$-re.

<u>Biz.:</u> (1) $\Rightarrow$ (2) $\quad \mathbb{Z}_p/(p^n) \cong \mathbb{Z}/(p^n)$.

$$\mathbb{Z}_p = \{a_0 + a_1 p + \dots \quad a_i \in \{0, \dots, p-1\}\}$$

$$(p^n) = \{p^n a_0 + p^{n+1} a_1 + \dots\}$$

közös gyököt mod p^n nézem.

$(2) \Rightarrow (1)$

$$X_n := \left\{ (\alpha_1, \dots, \alpha_m) \in \left(\mathbb{Z}/p^n\right)^m \;\middle|\; f_j(\alpha_1, \dots, \alpha_m) = 0 \quad j = 1, \dots, l \right\}.$$

$$X_n \to X_{n-1}$$

$$X_n \to \dots \to X_2 \to X_1$$

véges $\neq \emptyset$

König-lemma $\Rightarrow$ van ∞ út $\rightsquigarrow$ $\mathbb{Z}_p$-beli megoldás.

$\square$

Áll.: $f_1,\dots,f_k \in \mathbb{Z}_p[x_1,\dots,x_m]$ homogén polinomok.

Ekvivalensek:

(1) $f_1,\dots,f_k$-nak $\exists$ nem csupa 0 közös gyöke $\mathbb{Q}_p^m$

(2) — 〃 — / primitív közös gyöke $\mathbb{Z}_p^m$

(3) — 〃 — primitív közös gyöke $\left(\mathbb{Z}/(p^n)\right)^m$-ben $\forall\, n \geq 1$-re.

primitív $(\alpha_1,\dots,\alpha_m) \in \mathbb{Z}_p^m$, ha nem mind osztható p-vel.

Biz.: nem 0 skalárral be lehet szorozni a megoldásokat $\Rightarrow$ feltehető, hogy mindegyik $\mathbb{Z}_p$-ben van és nem osztható p-vel.

$(1) \Leftrightarrow (2)$. $(2) \Leftrightarrow (3)$ mint a Lemma. $\square$

Hensel-lemma $f(x) \in \mathbb{Z}_p[X]$, f': derivált, $n, k \in \mathbb{Z}^{\geq 0}$.

$0 \leq 2k < n$ $\quad f(\alpha) \equiv 0 \ (p^n)$ $\quad v_p(f'(\alpha)) = k$.

$\Rightarrow \exists\ \beta \in \mathbb{Z}_p$ $\quad f(\beta) = 0$, $\quad \beta \equiv \alpha \ (p^{n-k})$.

Biz.: Elég találni olyan $\beta \in \mathbb{Z}_p$-t, amire

$$f(\beta) \equiv 0 \quad (p^{n+1}), \quad \beta \equiv \alpha \quad (p^{n-r}), \quad v_p(f'(\beta)) = r.$$

$$\beta = \alpha + p^{n-r} z \qquad z \in \mathbb{Z}_p$$

$$f(\beta) = f(\alpha + p^{n-r} z) = \underbrace{f(\alpha) + p^{n-r} z f'(\alpha)}_{\equiv 0 \ (p^{n+1})} + p^{2n-2r}(\ldots\ldots)$$

$2r < n \Rightarrow 2n - 2r \geq n+1$

$$z := \frac{-f(\alpha)}{p^{n-r} f'(\alpha)} \in \mathbb{Z}_p \text{ jó}$$

$\square$

Tétel $f \in \mathbb{Z}_p[x_1, \dots, x_m]$, $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}_p^m$

$n, \ell \in \mathbb{Z}^{\geq 0}$, $0 \leq 2\ell < n$. Tfh. $\exists$ $j \in \{1, \dots, m\}$

$$f(\alpha) \equiv 0 \quad (p^n) \qquad\qquad v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = \ell$$

$$\Rightarrow \exists \ \beta \in \mathbb{Z}_p^m : f(\beta) = 0, \ \beta \equiv \alpha \quad (p^{n-\ell}).$$

Biz.: $\underset{\beta_1}{\alpha_1} , \dots, \underset{\beta_{j-1}}{\alpha_{j-1}}, \underset{\beta_{j+1}}{\alpha_{j+1}}, \dots, \underset{\beta_m}{\alpha_m}$. (csak x_j polinomjaként létezik.) $\square$

Köv.: $x^{p-1}-1$ kül. gyöktényezők szorzatára bomlik $\mathbb{Z}_p$ fölött.

Biz.: $\mathbb{F}_p$ fölött: $x^{p-1}-1 \equiv (x-1)\cdot\ldots\cdot(x-p+1)$ (p). (kis Fermat) □

$n=1$, $k=0$ előző tétel.

$\rightsquigarrow$ $(p-1)$-edrendű elem $\mathbb{Z}_p^\times$-ben

multiplikatív (Teichmüller) reprezentáns. $[\alpha]$

$$0 \longrightarrow 1+p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times \longrightarrow 0$$

$\beta \in \mathbb{Z}_p^\times$, $\alpha \in \mathbb{F}_p^\times$ (p)

$\beta^{p-1}=1$

$\beta\equiv\alpha\ (p)$

$\Longrightarrow \mathbb{Z}_p^\times$

$\gamma \longmapsto \alpha$

$\gamma \longmapsto \left(\alpha, \frac{\gamma}{[\alpha]}\right) \in \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$

<u>Áll.:</u> $1+p\mathbb{Z}_p$-ben $\forall$ elem négyzetszám, ha $p \neq 2$.

<u>Biz.:</u> $u \in \mathbb{Z}_p$ $\quad u \equiv 1 \quad (p) \Rightarrow x^2 = u$-nak $\exists$ mo.-a $\mathbb{Z}_p$-ben.

$x^2 \equiv 1 \quad (p) \qquad \pm 1$

$\Rightarrow$ Hensel miatt $x^2 = u$-nak $\exists$ mo.-a $\square$

<u>Áll.:</u> $1+8\mathbb{Z}_2$-ben $\forall$ elem négyzetszám.

$u \equiv 1 \quad (8) \qquad x^2 = u \quad (\mathbb{Z}_2\text{-ben}) \qquad u$

$x = 1 + 2y$

$1 + 4y + 4y^2 = u \Rightarrow y^2 + y = \frac{u-1}{4}$

$y^2 + y \equiv 0 \quad (2) \Rightarrow$ Hensel. $\square$

$y = 0, 1$

Köv.: $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = \begin{cases} C_2 \times C_2 & p \text{ ptlan} \\ C_2 \times C_2 \times C_2 & p = 2. \end{cases}$

Biz.: $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \simeq C_2 \times \left(\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \right)$$

$$\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \subseteq (\mathbb{Z}_p^\times)^2$$

$$\left(\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \simeq C_2 \right)$$

$$1 + 2\mathbb{Z}_2 / 1 + 8\mathbb{Z}_2 = (\mathbb{Z}/(8))^\times = C_2 \times C_2.$$

$\square$

Köv.: $A = A^T \in \mathbb{Z}_p^{m\times m}$ $p \neq 2$ $f(x) = x^T A x$ homogén 2-fokú pol.

$x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$

$a \in \mathbb{Z}_p$

$p \nmid \det A$

$f(x) \equiv a \mod p$ minden primitív megoldása

felemelhető $f(x) = a$ megoldásává $x \in \mathbb{Z}_p^m$-ben.

Biz.: $f(\alpha) \equiv a \pmod p$ $\exists j: \alpha_j \not\equiv 0 \ (p)$. $a_{ij} = a_{ji}$

$f(x) = \sum a_{ij} x_i x_j$

$\frac{\partial f}{\partial x_j} = 2 \sum_{i=1}^{m} a_{ij} x_i$

$i < j$ $2a_{ij}x_i x_j$

$a_{ii} x_i^2$

$\frac{\partial f}{\partial x_j}(\alpha) = 2A\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \not\equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \mod p.$

$\ell=0,\ n=1 \overset{\text{Hensel}}{\Longrightarrow} \square$

<u>Köv.:</u> $p=2$, $A=A^T\in\mathbb{Z}_2^{m\times m}$, $f(x)=x^TAx$ kv. alak.

$f(x)\equiv a \mod 8$ -nak $\exists$ primitív mo.-a, ahol nem minden parciális derivált osztható 4-gyel

$\Rightarrow$ A mod 8 megoldás felemelhető $\mathbb{Z}_2$-beli megoldássá.

Spec. $\det A\not\equiv 0\ (2)$ elég.

<u>Biz.:</u> ugyanígy $n>3$, $\ell=1$ $\square$

Hilbert szimbólum

$K = \mathbb{Q}_p$ vagy $\mathbb{R}$.

Def.: $a, b \in K^\times$ $\quad (a,b)_K := \begin{cases} 1 & z^2 - ax^2 - by^2 = 0 \text{ van nemtriviális megoldása } K\text{-ban} \\ -1 & \text{egyébként (ha nincs).} \end{cases}$

$(a,b)_p \quad (K = \mathbb{Q}_p)$

$(a,b)_\infty \quad (\mathbb{R})$

$K = \mathbb{R} \quad z^2 - ax^2 - by^2 = 0 \quad \exists$ nemtriviális mo. $\Leftrightarrow$ a, b közül min. egyik pozitív.

$(a,b)_\infty = \begin{cases} -1, & \text{ha } a, b < 0 \\ 1 & \text{egyébként.} \end{cases}$

Mj.: $(ac^2, b) = (a, b) = (a, bc^2)$ $\quad c \in K^\times$.

$(a, b) = (b, a)$

$$K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \longrightarrow \{\pm 1\}.$$

$\mathbb{F}_2$-vektortér

<u>Áll.:</u> $a, b \in K^\times$ $\quad (a, b) = 1 \iff$ "a" előáll egy $K(\sqrt{b})$-beli elem normájaként.

$\left[\, b = 1,\ (a, 1) = 1, \text{ mert } z^2 - ax^2 - y^2 = 0 \quad (0, 1, 1) \text{ mo.} \,\right]$

Biz.:

$\alpha \in K(\sqrt{b})$

$s_\alpha : K(\sqrt{b}) \longrightarrow K(\sqrt{b})$ K-lin. lekép.

$N(\alpha) := \det s_\alpha$.

$1, \sqrt{b}$ bázis

$\alpha = x + y\sqrt{b}$

$s_\alpha(\sqrt{b}) = (x + y\sqrt{b})\sqrt{b} = x\sqrt{b} + yb$

$s_\alpha(1) = x + y\sqrt{b} = \begin{pmatrix} x \\ y \end{pmatrix}$

$$\det \begin{pmatrix} x & yb \\ y & x \end{pmatrix} = x^2 - y^2 b = N(\alpha)$$

$$x^2 - y^2 b = (x + y\sqrt{b})(x - y\sqrt{b})$$

$a = x_0^2 - y_0^2 b$

$z^2 - a x^2 - b y^2$

$(1, y_0, x_0)$, az $(a, b) = 1$

Vissza: Tfh. $(a, b) = 1 \Rightarrow \exists\, x_0, y_0, z_0$: nem mind 0.

$z_0^2 - \cancel{a x_0^2} - b y_0^2 = 0$ $\quad / \, x_0^{-2}$

$x_0 = 0 \Leftrightarrow b \in (K^*)^2$ $\quad x_0 = 0$

$K(\sqrt{b}) = K$. $a \in N(a)$. $\square$

Áll.: (1) $(a,b)=(b,a)$, $(a,bc^2)=(a,b)$.

(2) $(a,-a)=1$, $(a,1-a)=1$.

(3) $(a,bc)=(a,b)(a,c)$, ha $(a,c)=1$. (Tetszőleges K testre)

Biz.: (1) ✓

(2) $z^2-ax^2+ay^2=0$ $(1,1,0)$ mo.

$z^2-ax^2-(1-a)y^2=0$ $(1,1,1)$ mo.

(3) Tfh. $(a,c)=1$ Ha $a\in(K^*)^2$ ✓

$\Vert$ $c=N(\gamma)$ $\gamma\in K(\sqrt{a})$

$b=N(\beta) \Rightarrow bc=N(\beta\gamma)$

$bc=N(\delta) \Rightarrow b=N\left(\frac{\delta}{\gamma}\right)$. □

$\boxed{p \neq 2}$

Lemma 1 Ha $a, b, c \in \mathbb{Z}_p^\times$, akkor az $ax^2+by^2+cz^2=0$ egyenletnek $\exists$ nemtriv. mo.-a $\mathbb{Z}_p^3$-ben. Speciálisan ha

$$p \nmid a, b \Rightarrow (a,b)_p = 1.$$

Biz.: $A = \begin{pmatrix} a & & \\ & b & \\ & & c \end{pmatrix}$ $\quad \det A = abc \not\equiv 0 \ (p).$

előző mátrixos $\Rightarrow$ elég $ax^2+by^2+cz^2 \equiv 0 \ (p)$-nek nemtriv. mo.

$$z=1 \quad \underbrace{\{c+ax^2\}_{x\in\mathbb{F}_p}}_{\frac{p+1}{2}} \cap \underbrace{\{-by^2\}}_{\frac{p+1}{2}}. \qquad \square$$

$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ reprezentánsa

„4-elemű"

$(a,b) = (a, b c^2)$

$1, u, p, up$

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

$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 = p^{\mathbb{Z}} / p^{2\mathbb{Z}} \times \left(\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2\right) \cancel{\left(\times\, 1+p\mathbb{Z}_p / 1+p\mathbb{Z}_p\right)}$

Kell: (u,p), (u,up), (p,up), (p,p), (up,up).