Lemma 2 $\quad p \neq 2 : \left(\frac{u}{p}\right) = -1 \Rightarrow (u, p)_p = -1$

(avagy $ux^2 + py^2 = z^2$ -nek $\nexists$ nemtriviális mo.-a $\mathbb{Q}_p$-ben).

Biz.: $\quad \underline{z^2 - ux^2} - py^2 = 0$. $\quad \mathbb{Z}_p$-ben.

$$z^2 \equiv ux^2 \quad (p).$$

$$p \nmid x \Rightarrow \left(\frac{z}{x}\right)^2 \equiv u \quad (p) \text{ ↯ } \left(\frac{u}{p}\right) = -1.$$

$$\Rightarrow p \mid x,\ p \mid z \Rightarrow p^2 \mid py^2 \Rightarrow p \mid y. \Rightarrow \frac{x}{p}, \frac{y}{p}, \frac{z}{p} \text{ is mo. ↯} \quad \square$$

$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ $\quad 1, u, p, up \quad$ $(1,a)=1$, $(u,u)=1$

$(u,p)=-1$. $\quad (p,-p)=1$

2 eset: $p\equiv 3\ (4) \Rightarrow \left(\frac{-1}{p}\right)=-1$. $\quad u=-1$ választható.

$(up,p)=(p,up)=1 \qquad -1=(u,p)=(p,u)=(p,-up)=(p,p)$

$(a,bc)=(a,b)(a,c)$, ha $(a,c)=1$

$(u,up)=(u,u)(u,p)=(u,p)=-1 \qquad (p,-p)=1$

$p=a,\ b=u,\ c=-p$

$(u,u)=1$

$(up,up)=(up,u)\cancel{(u,p)}=-1$.

Ila $p \equiv 1 \ (4) \Rightarrow \left(\frac{-1}{p}\right) = 1.$

$$\left.\begin{array}{l} 1 = (p, -p) = (p, p) \\ -1 = (u, p) = (p, u) \end{array}\right\} \Rightarrow (p, up) = -1$$

$$(p, up) = (p,u)(p,p)$$

$$(u, up) = (u,u)(u,p) = -1.$$

$$(u,u) = 1$$

$$(up, up) = (up, -up) = 1$$

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

$$-1 \in (\mathbb{Q}_p^\times)^2$$

u

Tétel $(p \neq 2)$ $a = p^\alpha v$, $b = p^\beta w$ $v, w \in \mathbb{Z}_p^\times$.

$$(a,b)_p = (-1)^{\alpha \cdot \beta \cdot \frac{p-1}{2}} \cdot \left(\frac{v}{p}\right)^\beta \cdot \left(\frac{w}{p}\right)^\alpha.$$

Speciálisan $(a, bc)_p = (a,b)_p (a,c)_p$ és nemelfajuló.

Biz.: Meg kell nézni $a, b \in \{1, u, up, p\}$-re. $\square$

$$(a,b): \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \longrightarrow \{\pm\}$$

bilin.
és nemelfajuló.

Tétel $(p=2)$ $a = 2^{\alpha} \cdot v$, $b = 2^{\beta} w$ $v, w \in \mathbb{Z}_2^{\times}$.

$$(a, b)_2 = (-1)^{\varepsilon(v)\varepsilon(w) + \alpha\omega(w) + \beta\omega(v)}$$

$$\varepsilon(v) \equiv \frac{v-1}{2} \ (2), \qquad \omega(v) \equiv \frac{v^2-1}{8} \ (2).$$

Speciálisan $(a, b)_2$ is bilineáris és nemelfajuló.

$$\mathbb{Q}_2^{\times} / (\mathbb{Q}_2^{\times})^2 = \{\pm 1, \pm 5, \pm 2, \pm 10\}$$

Hilbert szimbólum globális tulajdonságai

Tétel (Hilbert reciprocitás) $a, b \in \mathbb{Q}^\times$. Ekkor

$(a, b)_v = 1$ véges sok $v \in \{\infty\} \cup \underbrace{P}_{\text{prímek}} =: V$

kivételével. Továbbá

$$\prod_{v \in V} (a, b)_v = 1. \quad (\text{tehát ps sok kivétel})$$

Biz.: Tfh. $v_p(a) = v_p(b) = 0 \underset{\text{Lemma}}{\Longrightarrow} (a, b)_p = 1 \Rightarrow$ véges sok kivétel.

bilinearitás miatt elég $a, b \in \{-1\} \cup P$ esetén ellenőrizni.
prímek

1) $a = -1 = b$, $(-1,-1)_\infty = -1$.

$p \neq 2 \Rightarrow (-1,-1)_p = 1$.

$(-1,-1)_2 = -1$: $z^2 - (-x^2) - (-y^2) = x^2 + y^2 + z^2 = 0$

mod 8

$x^2 \equiv 0, 1, 4 \ (8)$ $\mathbb{Z}_2$-ben.

2) $a = -1$, $b = \ell$ prím.

$\ell = 2$ $z^2 + x^2 - 2y^2 = 0$

$(-1,2)_v = 1$ tv-re.

$\ell > 2$ prím. $p \neq 2$, $p \neq \ell$

$(-1, \ell)_p = 1$. $(-1, \ell)_\infty = 1$.

$(-1, \ell)_\ell = (-1)^{\frac{\ell-1}{2}} = (-1)^{\varepsilon(\ell)} = (-1, \ell)_2$

$z^2 + x^2 - \ell y^2$

$\ell \equiv 3 \ (4) \Rightarrow$ nincs m.o.

$\ell \equiv 1 \ (4) \Rightarrow$ van, mert

$y = 1$, $x = 0$ v. 2 jó lesz

3) $a = \ell$, $b = \ell'$ $\quad \ell = \ell' \Rightarrow$

$(\ell, \ell) = (\ell, -\ell^2) = (\ell, -1)$ már láttuk.

$(a, bc) = (a, b)(a, c)$

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

$\ell \neq \ell' \Rightarrow (\ell, \ell')_\infty = 1.$ $(\ell, \ell')_p = 1$ $p \neq \ell, p \neq \ell'$
$p \neq 2.$

$\ell' = 2$ $(\ell, 2)_2 = (-1)^{w(\ell)} = (\ell, 2)_\ell$
$y = 1$

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

$x^2 - \ell y^2 - 2z^2$

$\ell \equiv 1 \ (8) \Rightarrow z = 0$ jó!
$\ell \equiv -1 \ (8) \Rightarrow z = 1$ jó!

$\ell \equiv 3, 5 \ (8) \Rightarrow$ mod 8 nincs mo. $y = 1$

$\ell = p$, $\ell' = q \neq p$.

$$(p,q)_p = \left(\frac{q}{p}\right) \qquad (p,q)_q = \left(\frac{p}{q}\right).$$

$$(p,q)_2 = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$\underset{\text{kv. recip.}}{\Longrightarrow} \qquad \prod_v (p,q)_v = 1. \qquad \square$$

Tétel $(a_i)_{i\in I} \subseteq \mathbb{Q}^\times$, I véges halmaz és $\varepsilon_{i,v} \in \{\pm 1\}$, $i \in I$, $v \in V$.
Akkor és csak akkor $\exists\, x \in \mathbb{Q}^\times$ úgy, hogy $(a_i, x)_v = \varepsilon_{i,v}$ $\forall i \in I$ és $v \in V$-re, ha az alábbi 3 feltétel teljesül:

(1) Véges sok kivétellel $\varepsilon_{i,v} = 1$

(2) $\forall i \in I \quad \prod_{v \in V} \varepsilon_{i,v} = 1.$

(3) $\forall v \in V$-re $\exists\ x_v \in \mathbb{Q}_v^\times$ $\quad (\mathbb{Q}_\infty = \mathbb{R})$

úgy, hogy $(a_i, x_v) = \varepsilon_{i,v}$.

Biz.: (1), (2), (3) szükséges az előző tétel miatt.

Tfh. $a_i \in \mathbb{Q}^\times$, $\varepsilon_{i,v} \in \{\pm 1\}$ teljesítik (1), (2), (3)-at.

Lemma (approximáció) Legyen $S \subset V$ véges halmaz

$\Rightarrow \quad \mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$ képe sűrű.

Biz.: S-et növeljük $S = \{\infty, p_1, \ldots, p_n\}$.

$$(x_\infty, x_1, \ldots, \underset{\in \mathbb{Z}}{,} x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$$

és $\varepsilon > 0$ $N > 0$ kell: $x \in \mathbb{Q}$ úgy, hogy

$$|x - x_\infty|_\infty \leq \varepsilon. \quad v_{p_i}(x - x_i) \geq N. \quad i = 1, \ldots, n.$$

$x_1, \dots, x_n$ közös nevezőjével beszorozva feltehető,

hogy $x_i \in \mathbb{Z}_{p_i}$

$x_0 \equiv x_i \quad (p_i^N)$ kínai maradéktétel miatt $\exists\, x_0 \in \mathbb{Z}$.

$x_0 + \dfrac{\ell \cdot p_1^N \cdots p_n^N}{q}$ $\quad q \neq p_i$ prím

$q >> 0$

$\dfrac{p_1^N \cdots p_n^N}{q} < \varepsilon \Rightarrow \exists\, \ell \in \mathbb{Z} : \left| x_0 + \dfrac{\ell \cdot p_1^N \cdots p_n^N}{q} - x_\infty \right|_\infty < \varepsilon$

tételbiz.: feltehetjük, hogy $a_i \in \mathbb{Z}$.

$$S := \{\infty, 2\} \cup \{a_i\text{-k prímosztói}\}.$$

$$T := \{v \in V \mid \exists i \in I \;\; \varepsilon_{i,v} = -1\}. \rightarrow \text{véges.}$$

1) eset: $S \cap T = \emptyset$.

$$a := \prod_{\substack{\ell \in T \\ \ell \neq \infty}} \ell \quad , \quad m = 8 \cdot \prod_{\substack{\ell \in S \\ \ell \neq 2, \infty}} \ell \qquad (a, m) = 1.$$

Dirichlet $\Longrightarrow$ $\exists\, p$ prím: $p \equiv a \ (m)$.

Áll.: $x = ap$ jó, azaz $(a_i, ap)_v = \varepsilon_{i,v}$.

$v \in S \qquad (p \notin S \cup T)$

$\varepsilon_{i,v} = 1$, mert $v \notin T$.

$v = \infty \qquad ap > 0 \Rightarrow (a_i, ap)_\infty = 1$ ✓

$v = \ell$ prím $\Rightarrow \ell \mid m \Rightarrow p \equiv a \ (\ell)$

$\Rightarrow$ pa négyzet mod ℓ

$\Rightarrow (a_i, pa)_\ell = 1 \quad (\ell \neq 2)$

$\ell = 2 \qquad p \equiv a \ (8) \qquad 8 \mid m$.

$\Rightarrow (a_i, pa)_2 = 1 \qquad pa \equiv 1 \ (8)$.

$\ell \in T \Rightarrow \ell \notin S \Rightarrow a_i \in \mathbb{Z}_\ell^\times$.

$$(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(b)}$$

$\varepsilon_{i,\ell} = -1 \Rightarrow \ell \mid x_\ell$ ((3) miatt $\exists x_\ell$)

$v_\ell(x) = 1 \Rightarrow (a_i, x)_\ell = -1$.

$\Rightarrow \forall i \in I \; \varepsilon_{i,\ell} = \left(\frac{a_i}{\ell}\right) \Rightarrow v_\ell(ap) = 1$ miatt

$x = a\ell$ jó.

$\ell \notin T \cup S \quad \varepsilon_{i,\ell} = 1, \quad v_\ell(a_i) = 0 \qquad (a_i, ap)_\ell = 1$, kivéve

esetleg $\ell = p$-t.

pontosan 1 db sívéből nem lehet a Hilbert nép. miatt.

2. eset $S \cap T \neq \emptyset$: approximációs tétel (jövő órán.)