

17.5.2010

10 יולי

$a, b, c \in k^*$ מה יהיה: Cent

$$(a, c^2) = 1 \quad (1)$$

$$(a, b) = (b, a) \quad (2)$$

$$(cac, b) = (c, b) \quad \text{כל } (a, b) = 1 \quad \text{כל } (3)$$

$$(a \neq 0, 1) \quad (a, -a) = 1 = (a, 1-a) \quad (4)$$

$$(a, -ab) = (a, b) = (a, (1-a)b) \quad (5)$$

$$(a, b) = 1 \Leftrightarrow a \in N(k(\sqrt{b})^*) \quad (3) \text{ הוכחה:}$$

k^* - $\sqrt{b}$ נקרא

$$\text{כל } a \in N(k(\sqrt{b})^*) \quad \text{כל } \sqrt{b}$$

$$c \in N(k(\sqrt{b})^*) \Leftrightarrow ac \in N(k(\sqrt{b})^*)$$

$$(c, b) = 1 \Leftrightarrow (ac, b) = 1 \quad \text{כל } b$$

$$\Rightarrow (c, b) = (ac, b)$$

$$(a, -a) = 1 \quad \text{כל } (0, 1, 1), \quad z^2 - ax^2 + ay^2 = 0 \quad (4)$$

$$(1, 1, 1), \quad z^2 - ax^2 + (a-1)y^2 = 0 \quad (5)$$

$$4, 3 \sim 1 \quad (5)$$

הוכחה:

נניח: $\exists$ p ראשוני. נניח $\forall v \in Z_p^*$ יש x, y כאלה ש-

$$z^2 - px^2 - vy^2 = 0 \quad \text{כל } z \in Z_p^*, x, y \in Z_p$$

הוכחה: נניח $\exists$ p ראשוני. נניח $\forall v \in Z_p^*$ יש x, y כאלה ש-

$$(Z_p^*)^3 \ni (x, y, z) \quad \text{כל } (x, y, z) \in (Z_p^*)^3$$

$$z, y \in Z_p^* \quad \text{כל } z, y \in Z_p^*$$

$$z \in pZ_p \quad \text{כל } z \in pZ_p$$

$$vy^2 = z^2 - px^2 \in pZ_p$$

$$\text{כל } y \in Z_p^* \quad \text{כל } y^2 \in pZ_p, \quad \forall v \in Z_p^*$$

$$\text{כל } y \in pZ_p \quad \text{כל } y \in pZ_p$$

$$z \in pZ_p \quad \text{כל } z^2 = px^2 + vy^2 \in pZ_p$$

נסתחבר: $z^2, y^2 \in p^2 Z_p$ ולכן $z, y \in p Z_p$ מכאן

$$\Rightarrow p x^2 = z^2 - v y^2 \in p^2 Z_p$$

$$\Rightarrow x^2 \in p Z_p \Rightarrow x \in p Z_p$$

לכן סתירה לפי הנחה $x, y, z \in p Z_p$

נניח: $a, b \in \mathbb{Q}_p^*$ ונניח $p \neq 2$
 $\alpha, \beta \in \mathbb{Z}$, $u, v \in Z_p^*$ כש $a = p^\alpha u$, $b = p^\beta v$

$$(a, b) = (-1)^{\alpha\beta \cdot \frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \left(\left(\frac{u}{p}\right) = \left(\frac{\varepsilon_2(u)}{p}\right)\right)$$

הוכחה: כיוון ש ε_2 הוא חצי-הוויסטה
 $\alpha, \beta \in \{0, 1\}$ די לקרוא

$$\text{! הוכחה } \forall u, v \in Z_p^* \quad (u, v) = 1 \quad ; \text{ "3 } \alpha = \beta = 0 \quad \underline{1.}$$

$$(pu, v) = \left(\frac{v}{p}\right) \quad ; \text{ "3 } \alpha = 1, \beta = 0 \quad \underline{2.}$$

$$(p, v) = \left(\frac{v}{p}\right) ; \text{ "3 } (pu, v) = (p, v) \quad \text{כיון ש } (u, v) = 1 \quad \text{נובע}$$

$$Z_p^* = (1 + p Z_p) \times V \quad \text{כיון ש}$$

$$V = \{x \in Z_p^* \mid x^{p-1} = 1\} \xrightarrow{\varepsilon_2} (Z/pZ)^*$$

$$v = v_2 \cdot a \quad a \in V, \quad v_2 \in 1 + p Z_p, \quad \text{לכן}$$

$$\mathbb{Q}_p^* \text{ הולך ב- } 1 + p Z_p \text{ הם בעלי סדר } p-1 \text{ ונבחר } c \in \mathbb{Q}_p^* \text{ כש } V_2 = c^2$$

$$(p, v) = (p, v_2 a) = (p, a c^2) = (p, a)$$

$$\left(\frac{v}{p}\right) = \left(\frac{\varepsilon_2(v)}{p}\right) = \left(\frac{\varepsilon_2(v_2) \varepsilon_2(a)}{p}\right) = \left(\frac{\varepsilon_2(a)}{p}\right) = \left(\frac{a}{p}\right)$$

$$\mathbb{Q}_p^* \text{ הולך ב- } a \text{ כש } \left(\frac{a}{p}\right) = 1$$

$$(p, a) = 1 \quad \text{כש } a \text{ הוא ריבוע מוד } p, \quad \left(\frac{a}{p}\right) = 1$$

$$\text{כש } (p, a) = -1 \quad \text{אז } \left(\frac{a}{p}\right) = -1 \quad \text{לכן } (p, a) = -1$$

$$z^2 - p x^2 - a y^2 = 0 \quad \text{לפי הנחה יש פתרון } z, y \in Z_p^*, x \in Z_p$$

$$z^2 - a y^2 \equiv 0 \pmod{p} : p \text{ חלקי } z^2 - a y^2$$

$$a \equiv \frac{z^2}{y^2} \pmod{p} \quad \text{כיון ש } \varepsilon_2(a) \text{ הוא ריבוע מוד } p \quad (Z/pZ)^*$$

$$(pu, pv) = (-1)^{\frac{p-1}{2}} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right) \quad ; \text{ "3 } \alpha = \beta = 1 \quad \underline{3.}$$

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

$$\begin{aligned}
 (u, v) &\in \mathbb{Z}_p^* & (pu, pv) &= \left(-\frac{uv}{p}\right) & : \text{3} \\
 (pu, pv) &= (pu, pu^2v) = \left(\frac{a}{pu}, \frac{a}{-pu}\right) (-uv) = \\
 &= (pu, -uv) = (p, -uv) = \left(-\frac{uv}{p}\right) \\
 &\uparrow & & & \\
 (u, -uv) &= 1 \Rightarrow (pu, -uv) = (p, -uv) \quad (2)
 \end{aligned}$$

הוכחה: בנוסחה שבה, כי $\mathbb{Z}_p$ הוא ביקר, גם משנה אותו.

$$(a_1 a_2, b) = (a_1, b)(a_2, b)$$

$(\mathbb{Z}_p)$ הולדת הוא תבנית בי-טורית בסימטרית

$$\begin{aligned}
 \mathbb{Z}_2 = \{0, 1\} &\text{ הוא שדה וקטורי שבו } \frac{k^*}{(k^*)^2} \quad k = \mathbb{Q}_p \\
 \left((h+2\mathbb{Z}) \cdot (a(k^*)^2) = a^n (k^*)^2 \right)
 \end{aligned}$$

$$(p \neq 2) \quad k = \mathbb{Q}_p \quad : \text{Cohen}$$

$\mathbb{Z}_p$ הולדת הוא ביקר, כל שדה

$$b \in (\mathbb{Q}_p^*)^2 \Leftrightarrow \forall a \in \mathbb{Q}_p^* \quad (a, b) = 1$$

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^*$$

$$\Rightarrow (\mathbb{Q}_p^*)^2 \cong 2\mathbb{Z} \times \mathbb{Z}_p \times ((\mathbb{Z}/p\mathbb{Z})^*)^2$$

$\mathbb{Q}_p^* / (\mathbb{Q}_p^*)^2$ - שדה $\neq$ שדה $\neq$ שדה

$(1, 0, 1), (1, 0, -1), (0, 0, -1)$ - שדה $\neq$ שדה $\neq$ שדה

$$p, v_0, pv_0 \quad \therefore \left(\frac{v_0}{p}\right) = -1 \quad \forall v_0 \in V$$

$$(p, v_0) = \left(\frac{v_0}{p}\right) = -1 \quad \text{כל } v_0 = v_0$$

$$(u, p) = \left(\frac{u}{p}\right) \leftarrow \text{שדה } u \in \mathbb{Z}_p^* \quad \text{כל } u = p$$

$$(u, pv_0) = (u, p) = \left(\frac{u}{p}\right) \leftarrow \text{שדה } v_0 = pv_0$$

$$a = 2^\alpha u, b = 2^\beta v \quad : \text{שדה} \quad a, b \in \mathbb{Q}_p^*, p = 2 \quad : \text{Cohen}$$

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

$$u \in \mathbb{Z}_p^* \rightarrow \omega(u) = \varepsilon_2\left(\frac{u-1}{2}\right), \quad \varepsilon(u) = \varepsilon_2\left(\frac{u-1}{2}\right)$$

תכונות של חבורת הבר

$$V = \{ \text{מספרים } p \} \cup \{ \infty \} \quad \text{שמו}$$

$$v \in V \rightarrow Q_v = \begin{cases} Q_v & \text{מספר } v = p \\ R & v = \infty \end{cases}$$

אם $a, b \in Q^*$ שמו, $(a, b)_v$ הוא חבורת הבר של Q_v .
 Q_v^* הוא חבורת הבר של Q_v .
 (הצגה של $Q^* \times Q^*$ על $Q_v^* \times Q_v^*$ היא חבורת הבר של Q_v).

למה $(a, b)_v = 1$, $a, b \in Q^*$, $v \in V$, $v \neq p$, $v \neq \infty$:

$$\prod_{v \in V} (a, b)_v = 1$$

הוכחה
 $a = \pm p_1^{r_1} \dots p_n^{r_n}$, p_i מספרים ראשוניים שונים , $r_i \in \mathbb{Z}$
 נניח $a = \pm p_1^{r_1} \dots p_n^{r_n}$, $b = \pm p_1^{s_1} \dots p_n^{s_n}$.
 נניח $a = \pm p_1^{r_1} \dots p_n^{r_n}$, $b = \pm p_1^{s_1} \dots p_n^{s_n}$.
 נניח $a = \pm p_1^{r_1} \dots p_n^{r_n}$, $b = \pm p_1^{s_1} \dots p_n^{s_n}$.

$$(-1, -1)_\infty = -1 \quad a = b = -1, \underline{\underline{1}}$$

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

$$p = 2 \quad (-1, -1)_2 = (-1)^{\varepsilon(-1)\varepsilon(-1)} = -1$$

$$(-1, p)_\infty = 1 \quad a = -1, b = p \neq 2 \Rightarrow$$

$$3 \leq q \neq p \quad (-1, p)_q = 1$$

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

$$(-1, p)_2 = (-1)^{\varepsilon(-1)\varepsilon(p)} = (-1)^{-\varepsilon(p)} = (-1)^{\varepsilon(p)}$$

$$(-1, 2)_\infty = 1 \quad a = -1, b = 2 \Rightarrow$$

$$3 \leq p \quad (-1, 2)_p = 1$$

$$(-1, 2)_2 = (-1)^{\omega(-2)} = 1$$

$$a = b = p \Rightarrow$$

$$(p, p)_v = (p, (p)^{-1})_v = (p, -1)_v \leftarrow \text{לפי } 1$$

$$b=2 \quad a=\rho^{2,3} \quad \underline{\underline{2}}$$

$$(p, 2)_q = 1$$

$$(p, 2) = (-1)^{\omega(p)}$$

2. - nur wenn $a = p$, $b = q$!

$$(p, q)_\infty = 1$$

also $l \neq p, q, 2$ $(p, q) \neq 1$

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

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

$$(p, q)_2 = (-1)^{E(p)E(q)} = (-1)$$

(Weak Approximation) $2.17 p \geq \text{Coen}$

15.02 mit Δ_S^{-2} muss, nicht abh. von $S \subseteq V$ sein

$$\prod_{v \in S} \mathbb{Q}_v \rightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$$

$$\Delta_f(x) = (x, x, \dots, x)$$

$$x \in \mathbb{Q} \quad \circlearrowleft x \in \mathbb{Q}_{V_1} \quad \searrow x \in \mathbb{Q}_{V_2} \quad \dots$$

$x \in \mathbb{Q}$ $\forall \epsilon > 0$ $\exists \delta > 0$ $\forall x \in \mathbb{Q}$ $|x - x| < \delta$ $\Rightarrow$ $|x - x| < \epsilon$

דוגמה: $S = \{0, 1\}$ → ∞ מילים, $\infty \in S$ → $S' = S \cup \{\infty\}$ → ∞ מילים

$$1 \leq i \leq n \quad x_i \in \mathcal{Q}_{p_i}, x_\infty \in \mathbb{R} \quad \text{and} \quad S = \{\infty, p_1, p_2, \dots, p_n\} \quad \text{w/o } \infty$$

2.1.2. $|x_i|_{P_i} > 1 \Rightarrow \exists i_1, i_2, \dots, i_r \in n$ s.t.

мы получим B и наоборот. $(u_i \in \mathbb{Z}_p^* \text{ и } k_{ij}) \quad x_i = p_i^{-k_{ij}} u_i$

$$m = p_{i_1}^{k_{i_1}} \cdots p_{i_r}^{k_{i_r}} \quad \gamma \geq 0, \quad \gamma \geq 0$$
$$1 \leq i \leq n \quad \text{sof} \quad m x_i \in \mathbb{Z}_{p_i} \quad ! \quad \text{sof}$$

$$|x_i - \frac{x}{m}| \leq \frac{\varepsilon}{m} \Leftrightarrow |mx_i - x| \leq \varepsilon \quad \forall x \in \mathbb{Q}$$

$$|x_\infty - \frac{x}{m}|_\infty < \frac{\varepsilon'}{1/m} < \varepsilon \Rightarrow |mx_\infty - x|_\infty < \varepsilon'$$

$p \equiv a \pmod{m}$ ו p איז ראשי a, m זייט. (ממש). זייט B איז ראשי a, m זייט. $p \in S \cup T$ נאכט, $x = ap$ איז ראשי a, m זייט. (ממש).

איין $i \in I$ נאכט $\varepsilon_{i,v} = 1$, $v \in T$ ווייל $v \in S$ איז ראשי a, m זייט. $(a_i, ap)_v = 1$ נאכט a_i, ap איז ראשי a, m זייט.

$(v \in S \text{ נאכט}) \quad Q_v^* \rightarrow x = ap \equiv a^2 \pmod{m}$

$(x, a) \in Q_2 \rightarrow x \equiv a^2 \pmod{8}$ נאכט

$$x = a^2(1+8z), z \in \mathbb{Z}_2$$

$l \neq 2$ איז ראשי x, a $Q_l \rightarrow x \equiv a^2 \pmod{l}$ נאכט m איז ראשי a, m זייט. $(Z_p^* \rightarrow \text{נאכט})$

$$x = a^2(1+lz), z \in \mathbb{Z}_l$$

$R \rightarrow x = ap > 0$ איז ראשי a, m זייט.

$x = ap \in \mathbb{Z}_l^*$ ווי $a_i \in \mathbb{Z}_l^*$ נאכט, $v = l \notin T \cup \{p\}$ נאכט, $v \in S$ איז ראשי a, m זייט.

$\varepsilon_{i,l} = 1$, $l \notin T$ ווייל $(a_i, ap)_l = 1$ נאכט a_i, ap איז ראשי a, m זייט.

$$(a_i, ap)_l = \left(\frac{a_i}{l}\right)^{v_l(ap)=1} = \left(\frac{a_i}{l}\right) = \varepsilon_{i,l} \text{ נאכט, } l \in T$$

$$\forall i \in I \quad (a_i, x)_l = \varepsilon_{i,l} \text{ ווי } x \in \mathbb{Q}_l^* \text{ ווי (3) נאכט}$$

$$\left(\frac{a_i}{l}\right)^{v_l(x)}$$

$$v_l(x) = v_l(a^2(1+lz)) = 2v_l(a) = 2 \text{ נאכט } \varepsilon_{i,l} = -1 \text{ ווי } i \in I \text{ ווי}$$

$$\left(\frac{a_i}{l}\right)^{v_l(x)} = \left(\frac{a_i}{l}\right) \text{ נאכט}$$

$$(a_i, ap)_l = \left(\frac{a_i}{l}\right) = \left(\frac{a_i}{l}\right)^{v_l(x)} = \varepsilon_{i,l} \quad \forall i \leq n$$

$l = p$ נאכט a, m זייט.

$$\forall i \quad \prod_{v \in V} (a_i, x)_v = 1$$

$$\forall i \quad \prod_{v \in V} \varepsilon_{i,v} = 1$$

$$(i \text{ נאכט}) \quad v \neq p \text{ נאכט } (a_i, x)_v = \varepsilon_{i,v}$$

$$(a_i, x)_p = \varepsilon_{i,p} \text{ נאכט}$$