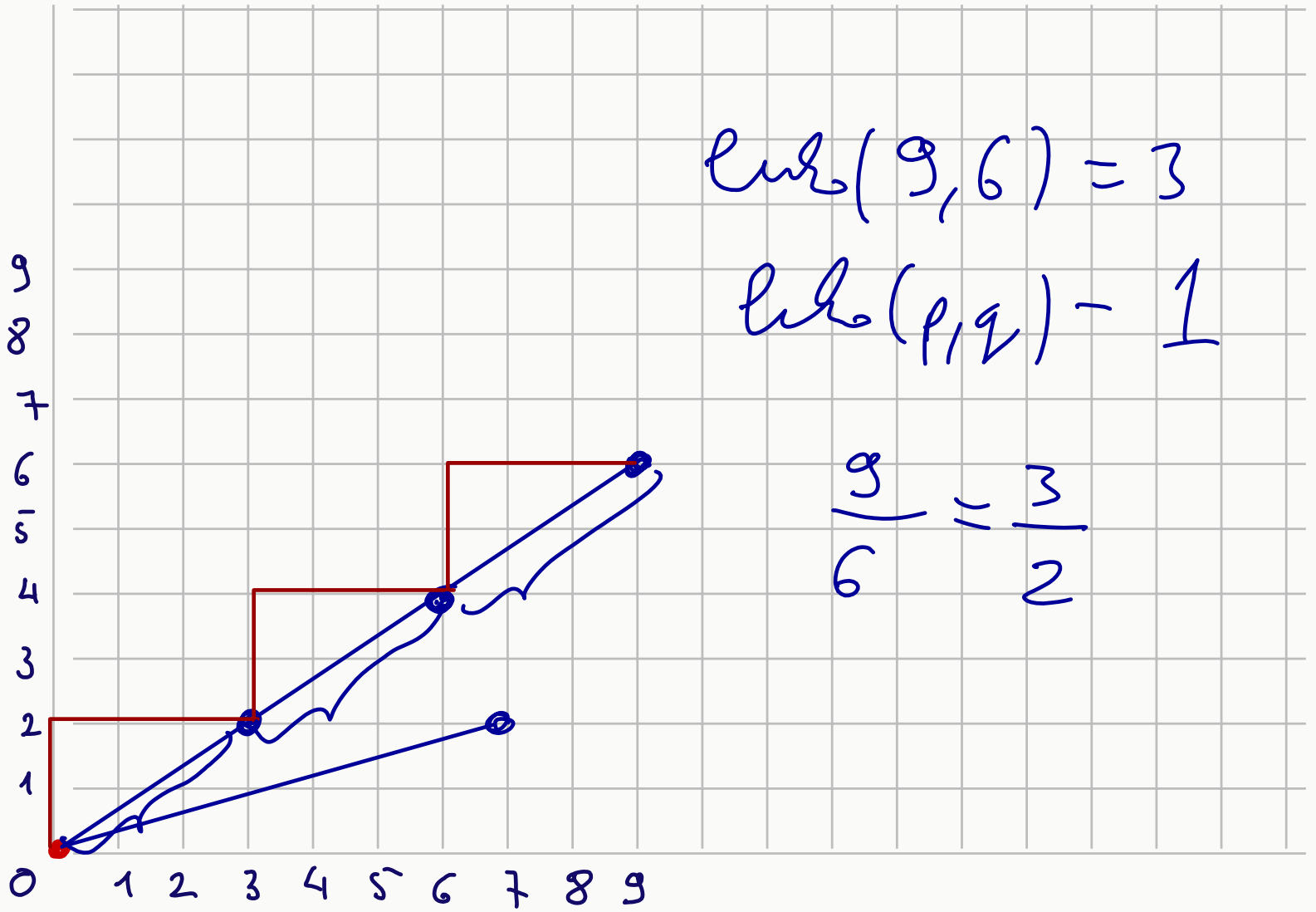
FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

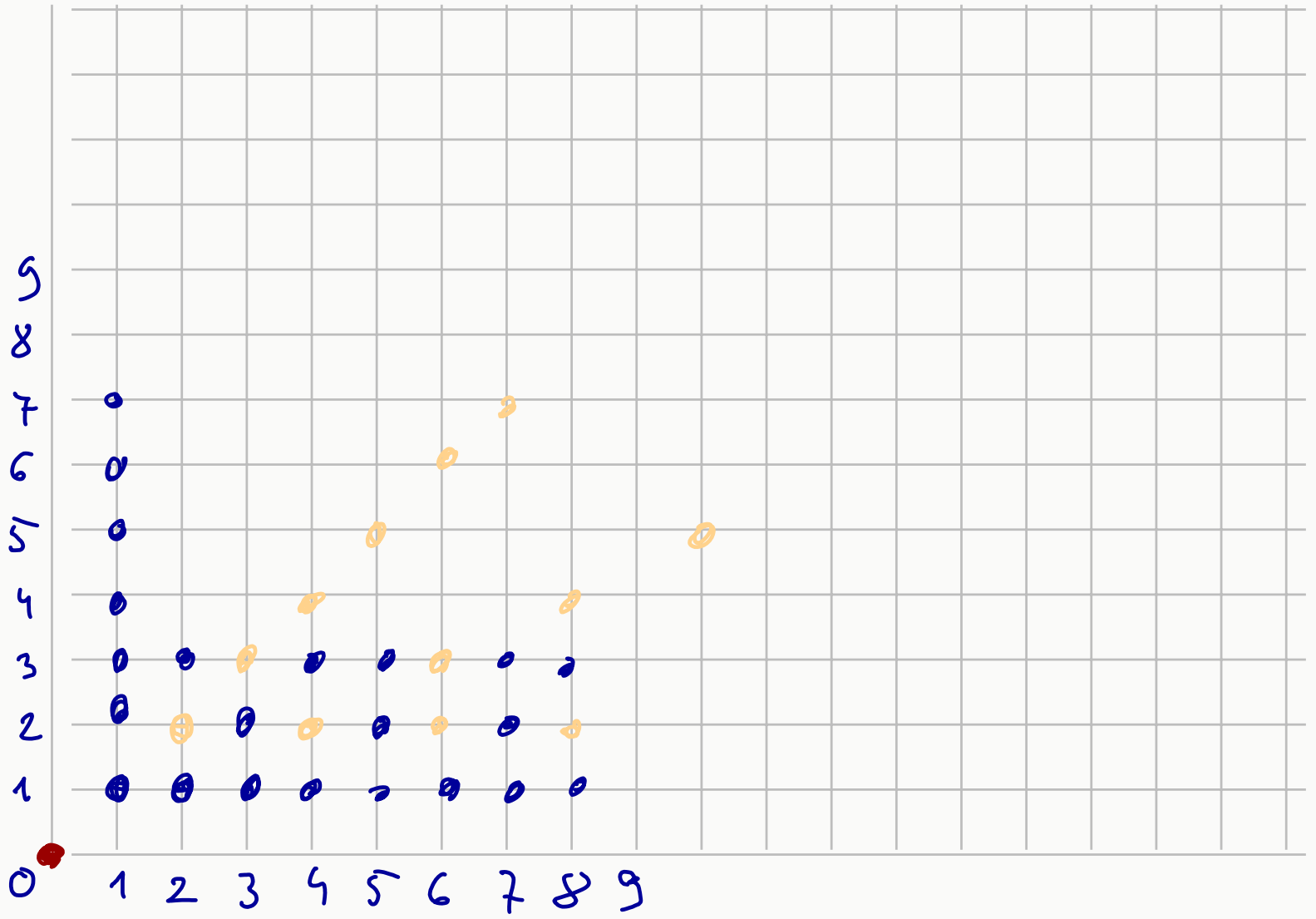
2021. február 23.

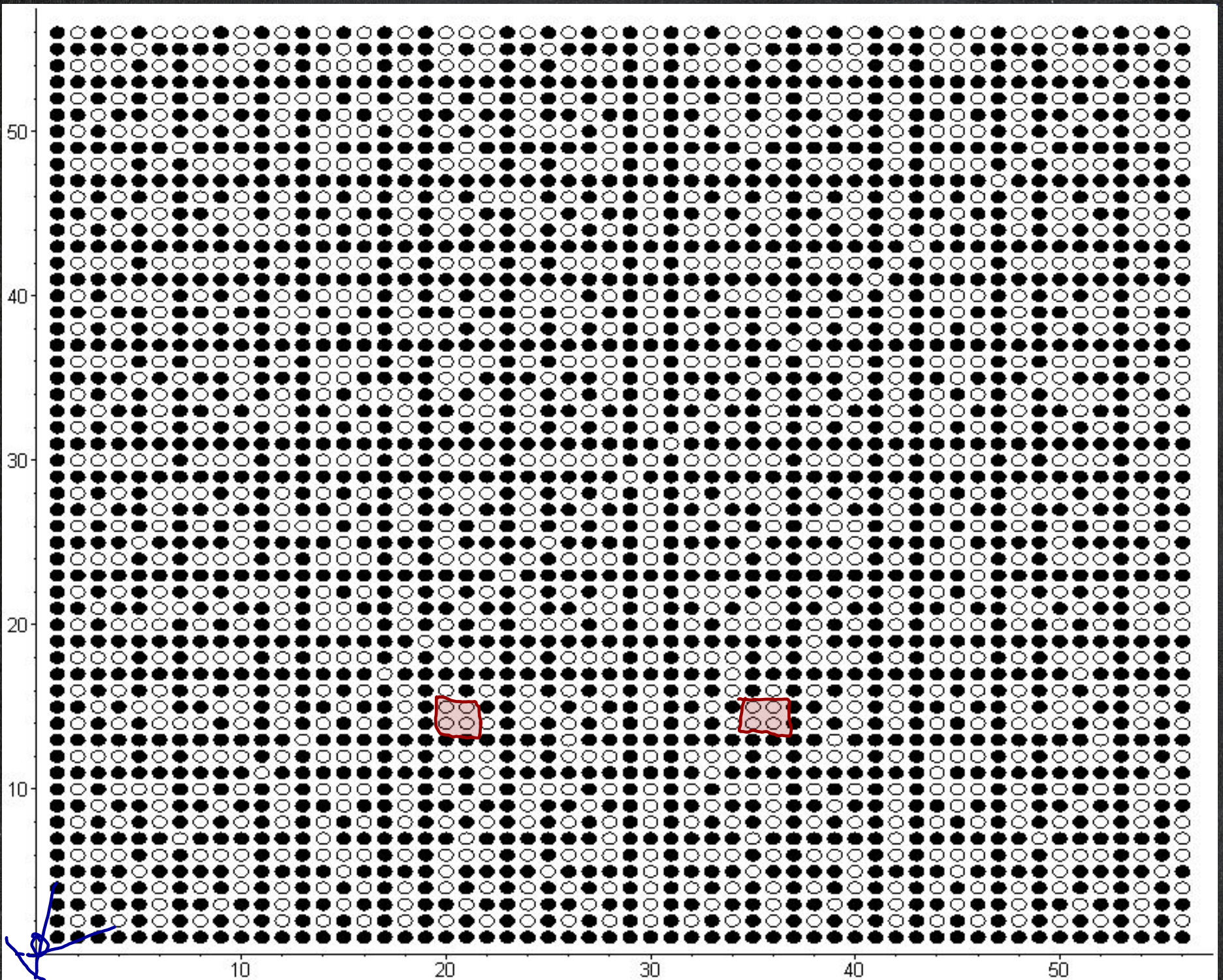


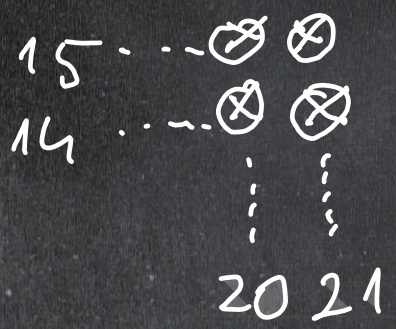
$$\text{lub}(9,6) = 3$$

$$\text{lub}(p,q) - 1$$

$$\frac{9}{6} = \frac{3}{2}$$


9
8
7
6
5
4
3
2
1
0
1 2 3 4 5 6 7 8 9


50
40
30
20
10
10
20
30
40
50



HF4.

$p = P(\ a \perp b\ ) = ?$

$P(\gcd(a,b)=2) = P(\underbrace{2 \mid a}_{\frac{1}{2}} \text{ és } \underbrace{2 \mid b}_{\frac{1}{2}} \text{ és } \underbrace{\tfrac{a}{2} \perp \tfrac{b}{2}}_{p}) = \frac{1}{4} \cdot p$

$P(\gcd(a,b)=3) = P(\underbrace{3 \mid a}_{\frac{1}{3}} \text{ és } \underbrace{3 \mid b}_{\frac{1}{3}} \text{ és } \underbrace{\tfrac{a}{3} \perp \tfrac{b}{3}}_{p}) = \frac{1}{9} p$

$\vdots$

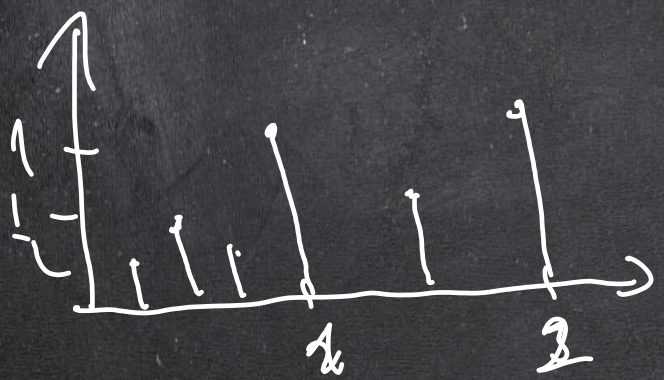
$P(\gcd(a,b)=n) = P(n \mid a \text{ és } n \mid b \text{ és } \tfrac{a}{n} \perp \tfrac{b}{n}) = \frac{1}{n^2} p$

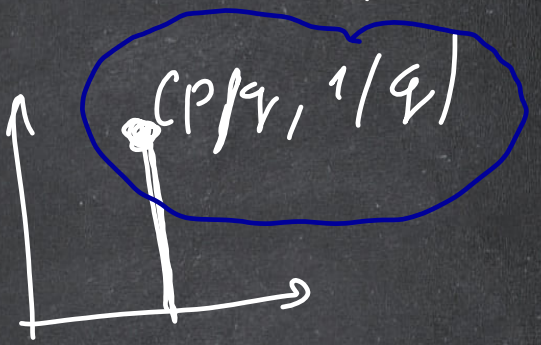
$$\sum_{n=1}^{\infty} P(\mathrm{ggT}(a,b)=n) = 1 = p \sum_{n=1}^{\infty} \frac{1}{n^2} = p \cdot \frac{\pi^2}{6}$$

$$\Rightarrow p = \frac{6}{\pi^2} = 0{,}6079\ldots \approx 60{,}8\%$$

$f: \mathbb{R} \to \mathbb{R}$ folgt. x_0-kan $\Leftrightarrow x_0 \notin \mathbb{Q}$

$$f(x) = \begin{cases} 0 & x \notin \mathbb{Q} \\ \frac{1}{q} & x = \frac{p}{q},\ p,q \in \mathbb{Z},\ q > 0,\ p \perp q \end{cases}$$





$$\left(\frac{3}{p}\right) \overset{QR}{=} \pm\left(\frac{p}{3}\right) = \pm\cdot(\pm 1) = \begin{cases} 1, \text{ če } p \equiv 1, 11 \pmod{12} \\ -1, \text{ če } p \equiv 5, 7 \pmod{12} \end{cases}$$

$p > 3$

$p \bmod 4$ $\qquad$ $p \bmod 3$

$p \bmod 4$	$p \bmod 3$	$p \bmod 12$	$\left(\frac{3}{p}\right)$
1	1	1	$+1\cdot(+1) = 1$
1	2	5	$+1\cdot(-1) = -1$
3	1	7	$-1\cdot(+1) = -1$
3	2	11	$-1\cdot(-1) = 1$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{la } p \equiv 1,7 \pmod 8 \\ -1, & \text{la } p \equiv 3,5 \pmod 8 \end{cases}$$

Biz: $\mathbb{Z}_p[x] \ni x^2 - 2$

Ha nincs gyöke, akkor $T := \mathbb{Z}_p[x]/(x^2-2)$ p^2-elemű test

$\cup|$

$\mathbb{Z}_p$

Ha van gyöke, akkor $T := \mathbb{Z}_p$

$\exists \alpha \in T : \alpha^2 = 2 \quad \alpha = \sqrt{2}$

$\exists K$ test: $\mathbb{Z}_p \leq K$ és $\sqrt{2}, i \in K$

$(\sqrt{2})^2 = 2 \in \mathbb{Z}_p \quad i^2 = -1 \in \mathbb{Z}_p$

$\operatorname{char} K = p$

EK $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p$

$\varepsilon = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i \quad \bar{\varepsilon} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i$

$2^{\frac{p-1}{2}} = \frac{1}{\sqrt{2}} 2^{p/2} = \frac{1}{\sqrt{2}} \sqrt{2}^p = \frac{1}{\sqrt{2}} \cdot (\varepsilon + \bar{\varepsilon})^p = \frac{1}{\sqrt{2}} \cdot (\varepsilon^p + \bar{\varepsilon}^p) =$

HF5 p prim, $0 < k < p$

$\Downarrow$

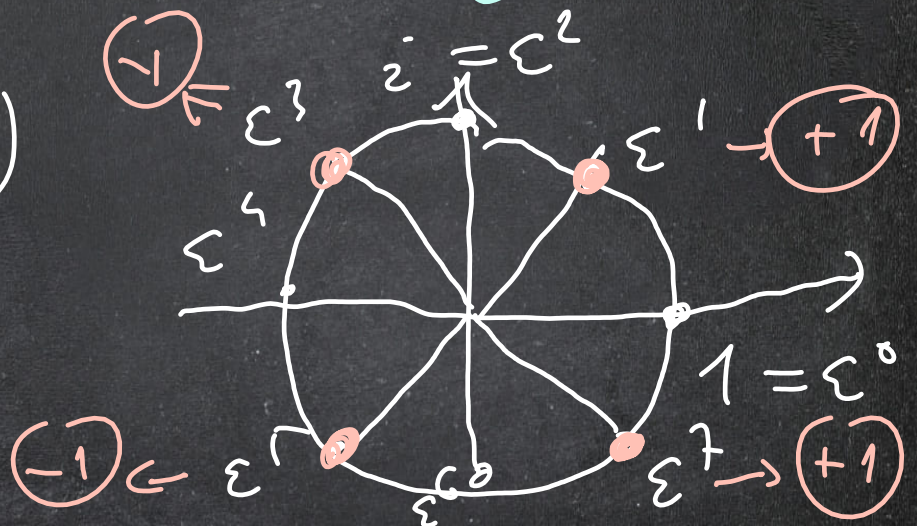
$p \mid \binom{p}{k}$

$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \cdot b^{p-k} =$

$= a^p + p a^{p-1} \cdot b + \dots + b^p$

$= \frac{1}{\sqrt{2}} (\varepsilon^p + \bar{\varepsilon}^p) = \frac{1}{\sqrt{2}} 2 \cdot \mathrm{Re}(\varepsilon^p)$

$= \sqrt{2} \cdot \mathrm{Re}(\varepsilon^p)$



JACOBI-SZIMBÓLUM

J $\quad$ $L=J$ $\quad$ $L=J$ $\quad$ $L=J$

DEF. $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)$

$m>1$, m pH., $a \perp m$

$m = p_1 \cdot p_2 \cdot \ldots \cdot p_r$

MEGJ. $\exists x\in\mathbb{Z}: x^2\equiv a \pmod m \Rightarrow \forall i: x^2\equiv a \pmod{p_i}$

$\Rightarrow \forall i: \left(\frac{a}{p_i}\right)=1 \quad \Rightarrow \left(\frac{a}{m}\right)=1$

$\left(\frac{a}{m}\right)=-1 \Rightarrow a$ [ ]-es reciprok mod. m.

$\left(\frac{a}{m}\right)=+1 \not\Rightarrow a$ [ ]-es reciprok mod. m pl. $\left(\frac{2}{9}\right)=+1$

Teil 4 ...

(1) $\left(\frac{a}{m \cdot n}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$

(2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right)$

(3) $a \equiv b \pmod{m} \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(4) $\left(\frac{-1}{m}\right) = \begin{cases} +1, & \text{falls } m \equiv +1 \pmod 4 \\ -1, & \text{falls } m \equiv -1 \pmod 4 \end{cases}$

Bsp: $m = p_1 \cdot \ldots \cdot p_u \cdot p_{u+1} \cdot \ldots \cdot p_r \equiv (-1)^u \pmod 4$

$p_1 \equiv -1$, $p_u \equiv -1$, $p_{u+1} \equiv +1$, $p_r \equiv +1 \pmod 4$

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \cdot \ldots \cdot \left(\frac{-1}{p_u}\right) \cdot \left(\frac{-1}{p_{u+1}}\right) \cdot \ldots \cdot \left(\frac{-1}{p_r}\right) = (-1)^u$$

$\left(\frac{-1}{p_1}\right) = -1$, $\left(\frac{-1}{p_u}\right) = -1$, $\left(\frac{-1}{p_{u+1}}\right) = +1$, $\left(\frac{-1}{p_r}\right) = +1$

(5) $\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right) = \begin{cases} +1, & \text{če } n \equiv 1 \vee m \equiv 1 \pmod 4 \\ -1, & \text{če } n \equiv -1 \wedge m \equiv -1 \pmod 4 \end{cases}$

Biz. $n = q_1 \cdot \ldots \cdot q_v \cdot q_{v+1} \cdot \ldots \cdot q_s \equiv (-1)^v \pmod 4$

$\quad\;\; \| \quad\quad \| \quad\quad \| \quad\quad \|$

$\quad -1 \quad\;\; -1 \quad\;\; +1 \quad\;\; +1 \pmod 4$

$m \perp n \Rightarrow \{p_1, \ldots, p_r\} \cap \{q_1, \ldots, q_s\} = \emptyset$

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i,j}\left(\frac{q_j}{p_i}\right)\cdot\prod_{i,j}\left(\frac{p_i}{q_j}\right) = \prod_{i,j}\underbrace{\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)}_{\| (QR)} = (-1)$$

-1, če $p_i \equiv q_j \equiv -1 \pmod 4$

urdbi (i,j) par

(6) $\left(\frac{2}{u}\right) = \begin{cases} +1, & \text{ha } u \equiv \pm 1 \pmod 8 \\ -1, & \text{ha } u \equiv \pm 3 \pmod 8 \end{cases}$

Biz: $u = p_1 \cdot \ldots \cdot p_u \cdot p_{u+1} \cdot \ldots \cdot p_r \equiv \pm 3^u = \begin{cases} \pm 1, \text{ha } u \text{ páros} \\ \pm 3, \text{ha } u \text{ páratlan} \end{cases}$

$\| \quad \| \quad \| \quad \| \qquad \pmod 8$

$\pm 3 \quad \pm 3 \quad \pm 1 \quad \pm 1$

$$\left(\frac{2}{u}\right) = \left(\frac{2}{p_1}\right) \cdot \ldots \cdot \left(\frac{2}{p_u}\right) \cdot \left(\frac{2}{p_{u+1}}\right) \cdot \ldots \cdot \left(\frac{2}{p_r}\right) = (-1)^u$$

$\| \quad \| \quad \| \qquad \|$

$-1 \quad -1 \quad +1 \qquad +1$ ∎

1. PÉLDA $\left(\frac{69}{83}\right) = \left(\frac{83}{69}\right) = \left(\frac{14}{69}\right) = \underbrace{\left(\frac{2}{69}\right)}_{-1} \cdot \left(\frac{7}{69}\right) = -\left(\frac{69}{7}\right) = -\left(\frac{-1}{7}\right) = \underline{\underline{+1}}$

HF6 $\left(\frac{77}{101}\right) = ?$ faktorizáció nélkül

$m = 2, q, p^\alpha, 2p^\alpha$