FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. február 16.

$p \equiv 1 \pmod 4 \rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \,\vdots\, \frac{p+1}{2} \cdot \ldots \cdot (p-2)(p-1) \equiv -1 \pmod p$

$\equiv 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \,\vdots\, (-1) \cdot \frac{p-1}{2} \cdot \ldots \cdot (-1) \cdot 2 \cdot (-1) \cdot 1 \equiv$

$\equiv (-1)^{\frac{p-1}{2}} \cdot \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$\left(\frac{a}{p}\right)$ pph. pr. alp

$a\cdot 1, a\cdot 2, \dots, a\cdot\frac{p-1}{2}$ $\qquad k\in\{1,\dots,\frac{p-1}{2}\}=:M(p)$

$a\cdot k = q_k\cdot p + r_k \quad 0\le r_k<p \qquad q_k=\left\lfloor\frac{a\cdot k}{p}\right\rfloor$

$N:=\{k \mid r_k>\frac{p}{2}\}=\{k \mid g_k<0\}$

$P:=\{k \mid r_k<\frac{p}{2}\}=\{k \mid g_k>0\}$

$|N|=n \qquad \left(\frac{a}{p}\right)\overset{?}{=}(-1)^n$

$\left(\frac{10}{13}\right) = (-1)^4 = 1$, $p = 13$, $b = 10$, $k \in \{1, \dots, 6\}$

$b \cdot k$	10	20	30	40	50	60
r_k	10	7	4	1	11	8
s_k	-3	-6	4	1	-2	-5

$N = \{1, 2, 5, 6\}$
$n = |N| = 4$

$k \in N: \; b_k = (q_k + 1) \cdot p + \underbrace{(r_k - p)}_{s_k}$ $\qquad s_k = r_k - p < 0$

$k \in P: \; b_k = q_k \cdot p + \underbrace{r_k}_{s_k}$ $\qquad s_k = r_k > 0$

① $i \neq l \Rightarrow |s_i| \neq |s_l|$

Biz $s_i = s_l \Rightarrow b_i \equiv b_l \pmod p \overset{b \perp p}{\Longrightarrow} i \equiv l \pmod p \Rightarrow i = l$

$s_i = -s_l \Rightarrow b_i \equiv -b_l \pmod p \Rightarrow i \equiv -l \pmod p$

$\Downarrow$

$p \mid i + l$

$2 \leq i + l \leq p-1$ ↯

② $\{|s_1|, \dots, |s_{\frac{p-1}{2}}|\} = \{1, \dots, \frac{p-1}{2}\}$

Biz. $|s_i| < \frac{p}{2} \Rightarrow$ ⊂

① $\Rightarrow$ =

③ $\prod_{k} 2 \equiv \prod_{k}$  $\pmod p$

$$\prod_{k=1}^{\frac{p-1}{2}} (b \cdot k) \equiv \prod_{k=1}^{\frac{p-1}{2}} s_k \pmod p$$

$$b^{\frac{p-1}{2}} \cdot \left(\tfrac{p-1}{2}\right)! \equiv (-1)^u \cdot \prod_{k} |s_k| \overset{②}{\equiv} (-1)^u \cdot \left(\tfrac{p-1}{2}\right)! \pmod p$$

$$\left(\frac{b}{p}\right) \overset{\text{E.K.}}{\equiv} b^{\frac{p-1}{2}} \equiv (-1)^u \pmod p$$

GAUSS-LEMMA: $\left(\frac{b}{p}\right) = (-1)^u$

(4) $\sum_k$  $= \sum_k q_k \cdot p + \sum_k r_k \equiv \sum_k$  $\cdot p + \sum_k$  $+np$

$$\sum_{k=1}^{\frac{p-1}{2}} b_k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_{sk} \cdot \cancel{p} + \sum_{k=1}^{\frac{p-1}{2}} |s_k| + n \cdot \cancel{p} \pmod 2$$

$$b \cdot \underbrace{\left(1 + \dots + \frac{p-1}{2}\right)}_{\frac{p^2-1}{8}} \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{b_k}{p} \right\rfloor + \frac{p^2-1}{8} + n \pmod 2$$

$$n \equiv (b-1) \cdot \frac{p^2-1}{8} + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{b_k}{p} \right\rfloor \pmod 2$$

(5) $b=2$: $n \equiv \frac{p^2-1}{8} + 0 \pmod 2$

$0 < \frac{2}{p} \leq \frac{2\varepsilon}{p} \leq \frac{p-1}{p} < 1$

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

II. ERGÄNZUNGSSATZ

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ falls } p \equiv 1 \pmod 4 \\ -1, \text{ falls } p \equiv 3 \pmod 4 \end{cases}$$

I. ERGÄNZUNGSSATZ

⑥ b pk. $n = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{bk}{p} \right\rfloor \pmod 2$

$$\left(\frac{b}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{bk}{p} \right\rfloor}$$

⑦ $p \neq q$ pk. pk.

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor} \overset{?}{=} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

(8)

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{e=1}^{\frac{q-1}{2}} \left\lfloor \frac{pe}{q} \right\rfloor \overset{?}{=} \frac{p-1}{2} \cdot \frac{q-1}{2}$$

classic

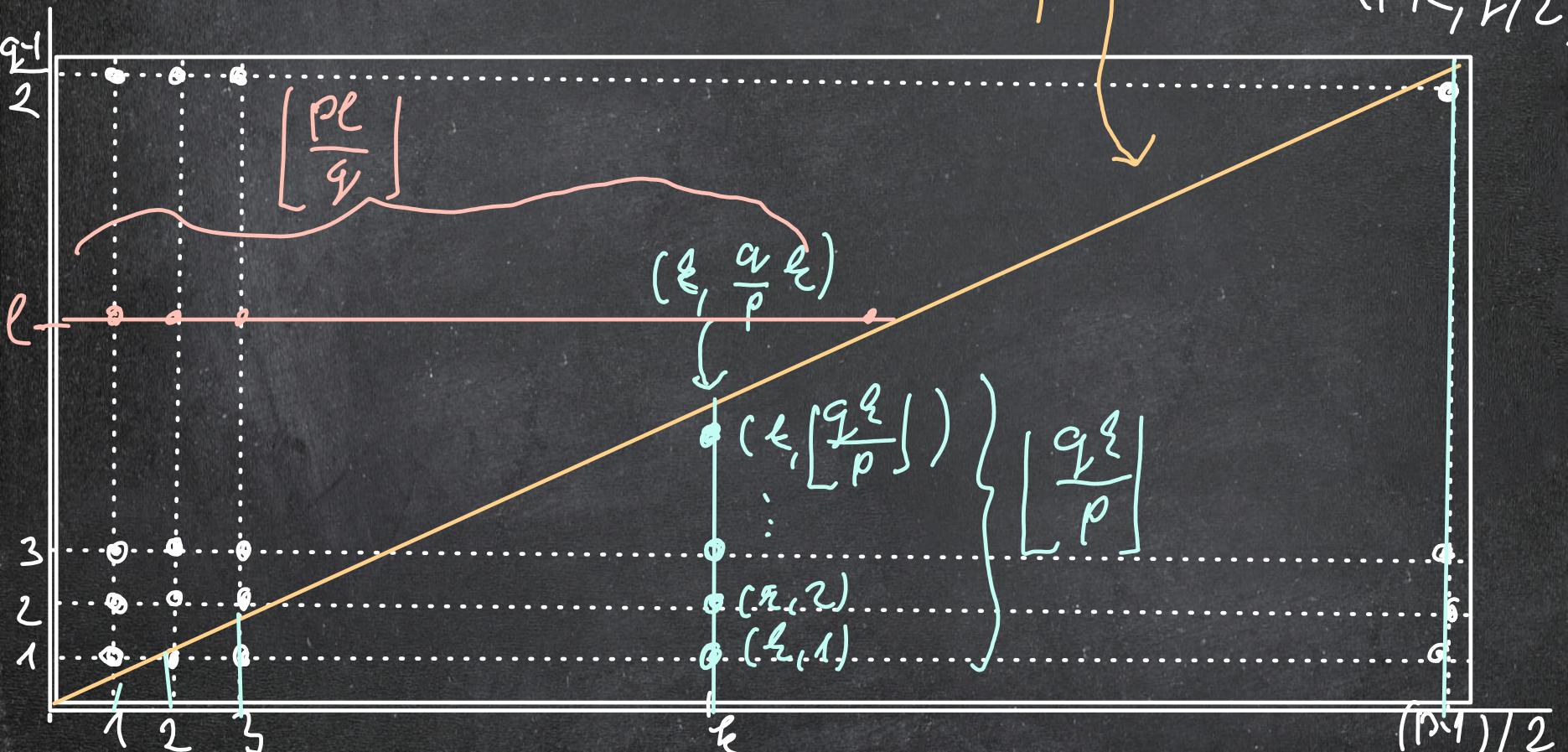
finite

+0 alle

EISENSTEIN

$y = \frac{q}{p} x$

$(p/2, q/2)$



Exponent von $\frac{p-1}{2} \cdot \frac{q-1}{2}$

Da $(x,y) \in \mathbb{Z}^2$ auf der Linie, dann $y = \frac{q}{p} x$

$yp = qx$

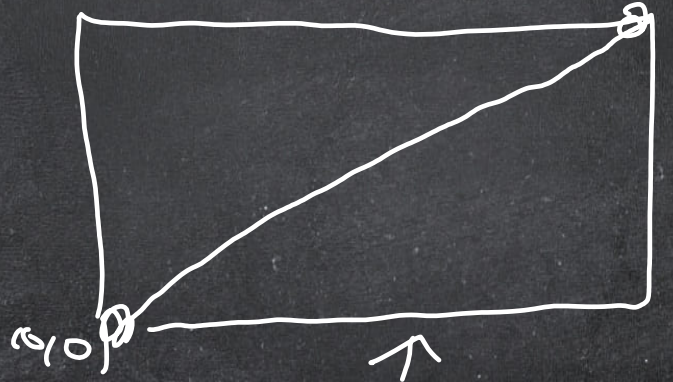
$p \mid qx \Rightarrow p \mid x$

$x \in \{1, \dots, p-1\} \Rightarrow$ es nen Punkt

Anzahl: Odd

Anz. Punkte: $\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor$ odd

Anz. Punkte: $\sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor$ odd



HF1 $p,q \in \mathbb{N}$ Hány rácspont van az átlón, a téglalap belsejében?

QR $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, \text{ ha } p \equiv 1 \lor q \equiv 1 \pmod 4 \\ -1, \text{ ha } p \equiv 3 \land q \equiv 3 \pmod 4 \end{cases}$

PÉLDA

$$\left(\frac{10}{13}\right) = \underbrace{\left(\frac{2}{13}\right)}_{-1} \cdot \left(\frac{5}{13}\right) = (-1)\left(\frac{5}{13}\right) = (-1)\cdot\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) =$$

$$= -\left(\frac{2}{3}\right) = (-1)\cdot(-1) = \underline{\underline{+1}}$$

HF2 $\left(\frac{77}{101}\right) = ?$

HF3 $\left(\frac{3}{p}\right) = \begin{cases} +1, \text{ ha } p \equiv & (\text{mod }) \\ -1, \text{ ha } p \equiv & (\text{mod }) \end{cases}$

PÉLDA

$$\left(\frac{69}{83}\right) = \left(\frac{3}{83}\right)\cdot\left(\frac{23}{83}\right) \overset{\uparrow}{=}_{QR} -\left(\frac{83}{3}\right)\cdot\left[-\left(\frac{83}{23}\right)\right] = \underbrace{\left(\frac{2}{3}\right)}_{-1 \,(\text{II.Ö.S.})}\cdot\left(\frac{14}{23}\right) =$$

$$= -\underbrace{\left(\frac{2}{23}\right)}_{+1 \,(\text{II. Ö.S.})}\cdot\left(\frac{7}{23}\right) \overset{\uparrow}{=}_{QR} -(+1)\cdot(-1)\left(\frac{23}{7}\right) = \left(\frac{2}{7}\right) \overset{\uparrow}{=} 1$$

II. Ö.S. $22^2 \equiv 69 \pmod{83}$