Kvadratisk reciprocitet

pigeonhole principle p.f.a.

Lemma $\left(\frac{a}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$

Lemma • $J = \{1, 2, \dots, \frac{p-1}{2}\}$

• $aJ = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\} = \{a_j : j \in J\}$

• Vi har $c_1, \dots, c_{\frac{p-1}{2}}$ s.a $c_j \equiv a_j \mod p$, $0 \leq c_j < p$

• $S = \#\{i : \frac{p}{2} < c_i < p\}$

• Då: $\left(\frac{a}{p}\right) = (-1)^S$

Lemma Sätt $T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$

Då: $(-1)^{T(a,p)} = \left(\frac{a}{p}\right)$.

$p \nmid a$ udda

Bevis

- $J = \{1, 2, \ldots, \frac{p-1}{2}\}$
- $aJ = \{a_l p + u_l : 1 \le l \le s\}$

  $\cup$

  $\{e_k p + v_k : 1 \le k \le t\}$

  $0 \le u_l < \frac{p}{2}$

  $\frac{p}{2} < v_k < p$

  $0 \le u_l, v_k < p$

- $aj = \left\lfloor \frac{aj}{p} \right\rfloor p + \text{rest}$, rest $= u_l$ eller v_k
- $\sum_{j=1}^{\frac{p-1}{2}} aj = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor + \text{rest}$

  $= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$

Ex $p = 5$

$a = 3$

- $J = \{1, 2\}$
- $3J = \{3, 6\}$
- $= \{0 \cdot 5 + 3, 1 \cdot 5 + 1\}$
- $= \{0 \cdot 5 + 3\} \cup \{1 \cdot 5 + 1\}$

  $s = 1$ $t = 1$

- $3 + 6 = 5\left\lfloor \frac{3}{5} \right\rfloor + 3 + 5 \cdot \left\lfloor \frac{6}{5} \right\rfloor + 1$

  $= 5 \cdot \left\lfloor \frac{3}{5} \right\rfloor + 5 \cdot \left\lfloor \frac{6}{5} \right\rfloor + 3 + 1$

- $\{1, 2, \dots, \frac{p-1}{2}\} = \{p-u_1, \dots, p-u_s\} \dot\cup \{v_1, \dots, v_t\}$
- $\sum_{j=1}^{\frac{p-1}{2}} j = sp - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$
- $(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} aj - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor + \sum_{1}^{s} u_j + \sum_{1}^{t} v_j$

$$- sp + \sum_{1}^{s} u_j - \sum_{1}^{t} v_j$$

$$= \sum_{1}^{\frac{p-1}{2}} p\left\lfloor \frac{aj}{p} \right\rfloor - ps + 2\sum_{1}^{s} u_j$$

$$= p\sum_{1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor - ps + 2\sum_{1}^{s} u_j$$

$$= p\,T(a,p) - ps + 2\sum_{1}^{s} u_j$$

$$\equiv T(a,p) - s \pmod 2$$

Men $VL \equiv 0 \pmod 2$ by a udda.

Så: $T(a,p) \equiv s \pmod 2$.

Nu $\left(\frac{a}{p}\right) = (-1)^s = (-1)^{T(a,p)}$

- $\{1,2\} = \{5-3\} \dot\cup \{1\}$
- $1+2 = 1\cdot 5 - 3 + 1$

Satz Kv. reciprc.

p, q udda primtal.

Då: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Bl Visar att $\overline{T}(q,p) + \overline{T}(p,q) = \frac{p-1}{2}\cdot\frac{q-1}{2}$

Då: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\overline{T}(q,0)}\cdot(-1)^{\overline{T}(q,q)}$

$= (-1)^{\overline{T}(q,p)+\overline{T}(p,q)}$

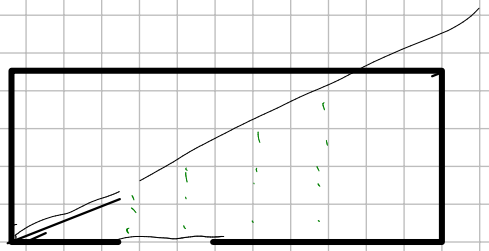
$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

- Rektangel $ABCD$ $A = (0,0)$

$B = \left(\frac{p-1}{2}, 0\right)$

$C = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$

$D = \left(0, \frac{q-1}{2}\right)$



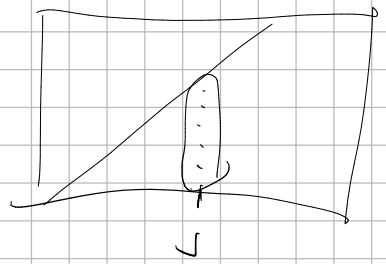
- Linje $y = \frac{q}{p}x$ går origo, ingår andra gitterpunkter; rekt.

- Gitterpunkter inre: (x,y), $1 \le x \le \frac{p-1}{2}$, $1 \le y \le \frac{q-1}{2}$

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ st

- Under linjen,

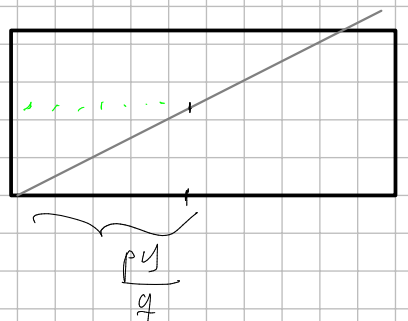
$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$$



$py = qx$

- Ovanför linjen

$$\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$$



- Inv: $\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$

$= T(q,p) + T(p,q).$