KVADRATICKÉ ZVYŠKY

MINULE: $a \, R \, p \iff (\exists x \in \mathbb{Z}) \; x^2 \equiv a \pmod p$ $\quad (+ \; p \nmid a)$

p = nepárne prvočíslo

Legendrov symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } aRp, \\ -1 & \text{ak } a\overline{R}p, \\ 0 & \text{ak } p \mid a. \end{cases}$$

Veta 4.2.3 (Eulerovo kritérium). *Nech $p > 2$ je prvočíslo. Potom pre všetky n platí*

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

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad + \left(\frac{-1}{p}\right), \left(\frac{2}{p}\right)$$

Veta 4.2.12 (Gaussova lema). *Nech $p > 2$ je prvočíslo a $p \nmid a$. Nech m je počet tých čísel z množiny $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, ktorých zvyšok po delení p je väčší než $\frac{p}{2}$. Potom*

$$\left(\frac{a}{p}\right) = (-1)^m.$$

PR: $p = 11$ $\quad 1^2 \equiv 1 \quad 4^2 \equiv 5 \quad 1, 3, 4, 5, 9$

$2^2 \equiv 4 \quad 5^2 \equiv 3$

$3^2 \equiv 9$

$a = 5$ $\quad 5, 10, 15, 20, 25$

$5, 10, 4, 9, 3 \qquad m = 2 \Rightarrow \left(\frac{5}{11}\right) = (-1)^2 = 1$

$a = 6$ $\quad 6, 12, 18, 24, 30$

$6, 1, 7, 2, 8 \qquad m = 3 \Rightarrow \left(\frac{6}{11}\right) = (-1)^3 = -1$

Veta 4.2.13. *Pre číslo m z Gaussovej lemy platí*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor \pmod 2. \quad \checkmark$$

Teda

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor}. \quad \checkmark$$

Pre nepárne a platí

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}. \quad \checkmark$$

Veta 4.2.13. *Pre číslo m z Gaussovej lemy platí*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor \pmod 2.$$

$m = \#$ čísel ka, $k = 1, \dots, \frac{p-1}{2}$, ktorých zv. $\geq \frac{p}{2}$

Dk: $ka = qp + r$

$\frac{ka}{p} = q + \frac{r}{p}$

$\left\{\frac{ka}{p}\right\} = \left\{\frac{r}{p}\right\}$

$r < \frac{p}{2} \iff \left\{\frac{r}{p}\right\} = \left\{\frac{ka}{p}\right\} < \frac{1}{2}$

$r > \frac{p}{2} \iff \left\{\frac{r}{p}\right\} = \left\{\frac{ka}{p}\right\} > \frac{1}{2}$

Lema 1.3.3. *Pre ľubovoľné $x \in \mathbb{R}$ platí $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$. Presnejšie,*

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & \text{ak } 0 \leq \{x\} < \frac{1}{2}; \\ 1, & \text{ak } \frac{1}{2} \leq \{x\}. \end{cases}$$

$\left\{\frac{ka}{p}\right\} < \frac{1}{2}$

$\iff \left\lfloor 2\frac{ka}{p} \right\rfloor - 2\left\lfloor \frac{ka}{p} \right\rfloor = 0$

$\iff \left\lfloor \frac{2ka}{p} \right\rfloor$ párne

$> \frac{1}{2} \iff \left\lfloor \frac{2ka}{p} \right\rfloor - 2\left\lfloor \frac{ka}{p} \right\rfloor = 1$

$\iff \left\lfloor \frac{2ka}{p} \right\rfloor$ nepárne

párna m = párna $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ka}{p} \right\rfloor$

Pre kvadr. a:

Pre nepárne a platí

1. $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}$.

2. $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor}$ (*)

celé č.

$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2a + 2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right)$ ($\left(\frac{4}{p}\right) = 1$)

$= \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum \left\lfloor \frac{ak}{p} \right\rfloor} (-1)^{\frac{k^2-1}{8}}$

(*) $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2\frac{a+p}{2}k}{p} \right\rfloor = \sum \left\lfloor \frac{(a+p)k}{p} \right\rfloor = \sum \left\lfloor \frac{ak}{p} + k \right\rfloor =$

$= \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \frac{k^2-1}{8}$

$\left(\frac{2}{p}\right) = (-1)^{\frac{k^2-1}{8}} \Rightarrow$ ✓

$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}$ □

ZÁKON RECIPROCITY

$p \neq q$

Veta 4.3.1 (Gaussov zákon kvadratickej reciprocity). *Ak p a q sú rôzne nepárne prvočísla, tak*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

$\frac{(p-1)(q-1)}{4}$

Dôsledok 4.3.2. *Ak $p \neq q$ sú nepárne prvočísla, tak*

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

s výnimkou prípadu, že $p \equiv q \equiv 3 \pmod 4$. (V tomto prípade $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.)

$\frac{p-1}{4} \cdot (q-1)$

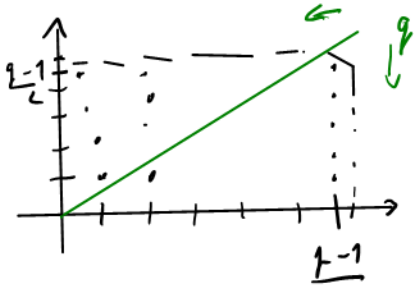
$\frac{p-1}{2} \cdot \frac{q-1}{2}$

D: (2.) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ (1.)

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

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

$S = \{(x,y) \in \mathbb{Z}^2;\ 1 \le x < \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2}\}$



$|S| = \frac{p-1}{2} \cdot \frac{q-1}{2}$

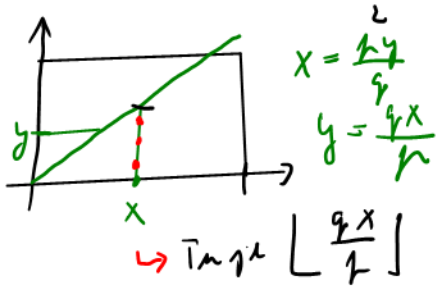
$S_1 = \{(x,y) \in S;\ qx < py\}$ → $S = S_1 \cup S_2$

$S_2 = \{(x,y) \in S;\ qx > py\}$ → $|S| = |S_1| + |S_2|$

Na priamke $qx = py$ neleží žiadny bod S

$\left[qx = py \Rightarrow q \mid py \Rightarrow q \mid y \right.$ SPOR

$\left. y \in \{1, 2, \dots, \frac{q-1}{2}\} \right]$



↳ $\mathrm{Im}\, \lfloor \frac{qx}{p} \rfloor$

$|S_1| = \sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$

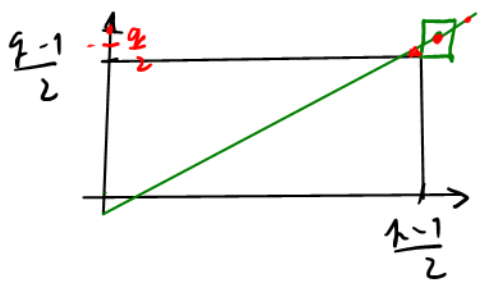
$|S_2| = \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$

$|S| = |S_1| + |S_2|$

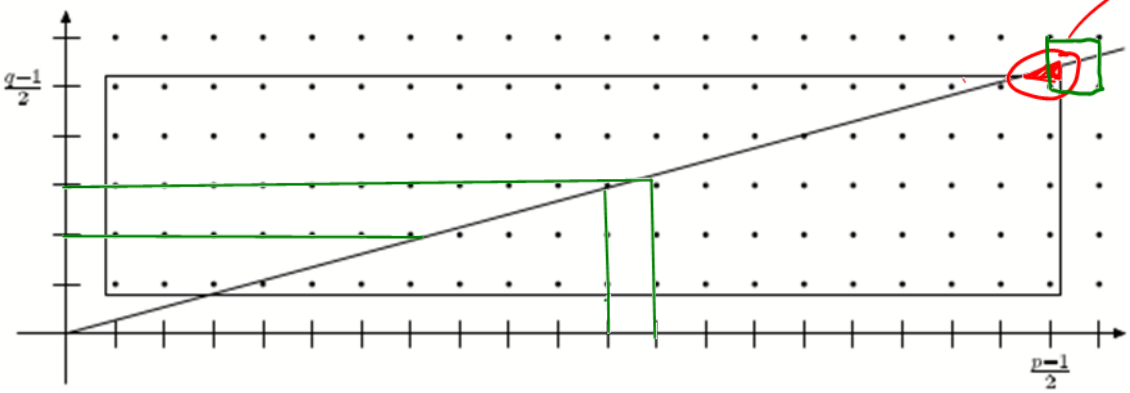
$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor + \sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$ + ~~0~~ o mriežnych bodoch

POZOR! Nerozlišili sme žiadnym spôsobom (2.) NIE

BÚNV: $p > q$



$qx = py$
↳ priamka obs. bod $\left(\frac{p}{2}, \frac{q}{2}\right)$



$p = 41, q = 7$

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

$$(-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{\xi}\cdot(-1)^{\xi} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \qquad \square$$

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}.$$

PR: $\left(\frac{219}{383}\right) = ?$ $\quad 383 \in \mathbb{P}$ $\quad 219 = 3\cdot 73$

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\cdot\left(\frac{73}{383}\right) = -\left(\frac{383}{3}\right)\cdot\left(\frac{383}{73}\right)$$

$-$ $\quad +$ $\quad 5\cdot 73 = 365$

$$= -\underbrace{\left(\frac{2}{3}\right)}_{=-1}\cdot\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right) = \underbrace{\left(\frac{2}{73}\right)}_{=1}\cdot\underbrace{\left(\frac{3^2}{73}\right)}_{=1} = 1$$

$73 = 8k+1$

Delenie so zyskom → OK

ROZKLAD NA PRVOCISLA → algoritmicky náročné

BUDE: Podobný postup bez rozkladu na prvočísla.

PR: už viem: $\left(\frac{-1}{p}\right) = ?$, $\left(\frac{2}{p}\right) = ?$

$\left(\frac{3}{p}\right) = ?$

$\frac{(p-1)(3-1)}{4}$

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

$$\left(\frac{p}{3}\right) \begin{cases} +1 & p = 3k+1 \\ -1 & p = 3k-1 \end{cases}$$

$$(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) \begin{cases} +1 & p = 4k+1 \\ -1 & p = 4k-1 \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & 12k \pm 1 \\ -1 & 12k \pm 5 \end{cases}$$

4.4 Jacobiho symbol

↗ P nemusí byť prvočíslo

Definícia 4.4.1. Nech P je nepárne číslo a $P = p_1 \cdot \ldots \cdot p_r$, kde $p_1, \ldots, p_r$ sú (nepárne) prvočísla. Potom *Jacobiho symbol* $\left(\frac{m}{P}\right)$ je definovaný ako

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_r}\right).$$

↖ Legendre

Ak $P \in \mathbb{P} \to \left(\frac{m}{P}\right)_J = \left(\frac{m}{P}\right)_L$ ... rozširuje Legendrov symbol.

Lema 4.4.3. *Nech P, Q sú nepárne prirodzené čísla a $a, b \in \mathbb{Z}$. Potom*

(i) $a \equiv b \pmod P \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$ ✓ ← $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$ $a \equiv b \pmod{p_i}$

(ii) $\left(\frac{1}{P}\right) = 1$ ✓

(iii) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$ ✓ ← $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$

(iv) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$ ✓ ← $P = p_1 \cdots p_n$ $Q = q_1 \cdots q_0$

$\left(\frac{a}{p_1}\right) \ldots \left(\frac{a}{p_n}\right)\left(\frac{a}{q_1}\right) \ldots \left(\frac{a}{q_0}\right)$

(v) *Ak $(b, P) = 1$, tak* $\left(\frac{b^2}{P}\right) = 1$. ✓ ↖

$\left(\frac{b^2}{p_1}\right) \ldots \left(\frac{b^2}{p_n}\right) = 1 \ldots 1 = 1$ ← ak $p_i \nmid b$

(vi) *Ak $(b, P) = 1$, tak* $\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)$. ✓

↑

$\left(\frac{a^2}{p}\right) = 1$ ← $p \nmid a$

BUDE: $\left(\frac{-1}{P}\right)$, $\left(\frac{2}{P}\right) = ?$

$\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = ?$