Zákon kvadratickej reciprocity

28. decembra 2020

Gaussova lema

Gaussova lema

Veta (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

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

Gaussova lema

Gaussova lema

Veta

Pre číslo m z Gaussovej lemy platí

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

Teda

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

Pre nepárne a platí

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

Gaussova lema

Gaussova lema

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

Lema

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

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

Zákon kvadratickej reciprocity

Zákon kvadratickej reciprocity

Veta (Gaussov zákon kvadratickej reciprocity)

Ak p a q sú rôzne nepárne prvočísla, tak

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

Dôsledok

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

Zákon kvadratickej reciprocity

Zákon kvadratickej reciprocity

Veta (Gaussov zákon kvadratickej reciprocity)

Ak p a q sú rôzne nepárne prvočísla, tak

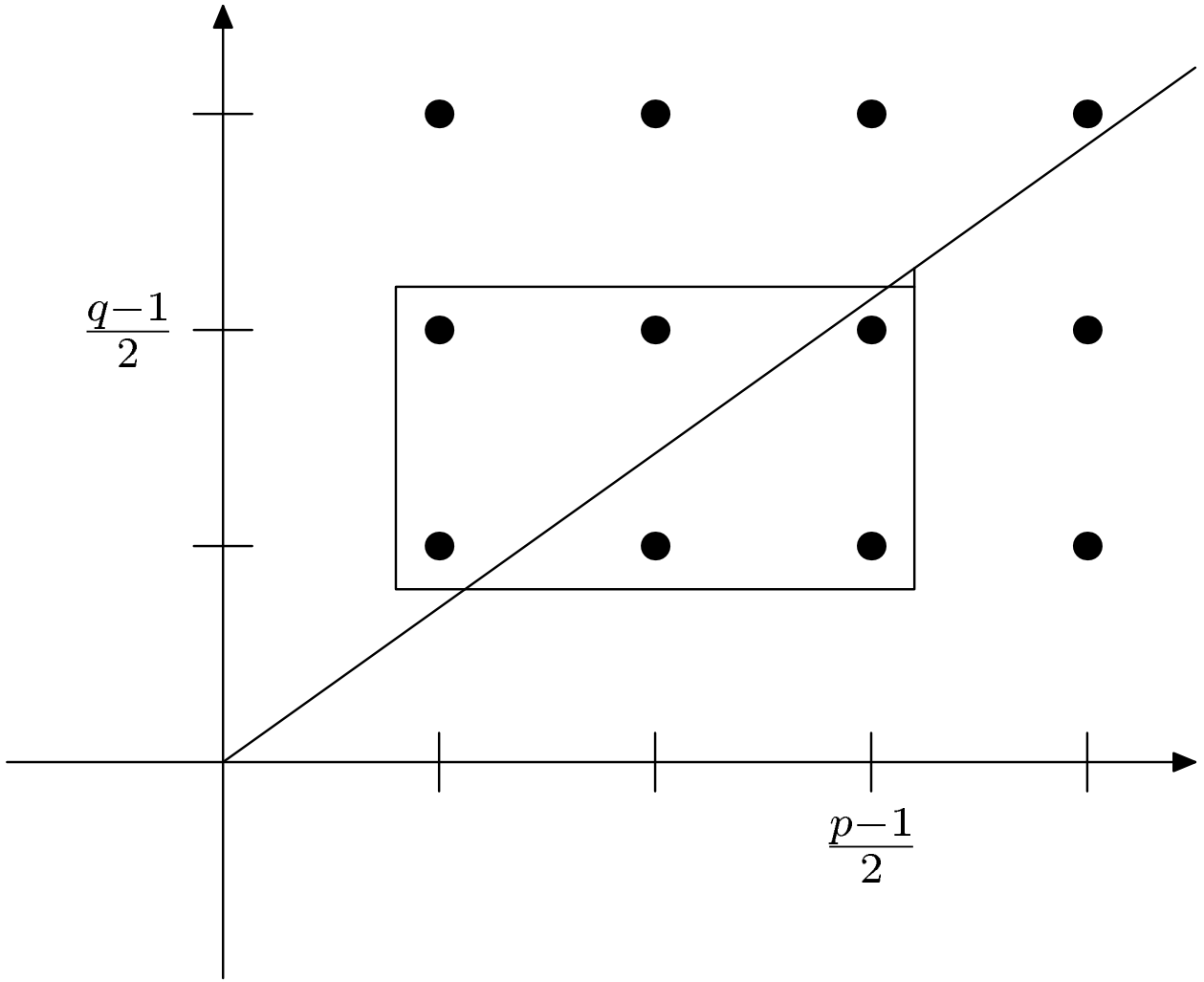
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

$$|S_1| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor,$$

$$|S_2| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Zákon kvadratickej reciprocity

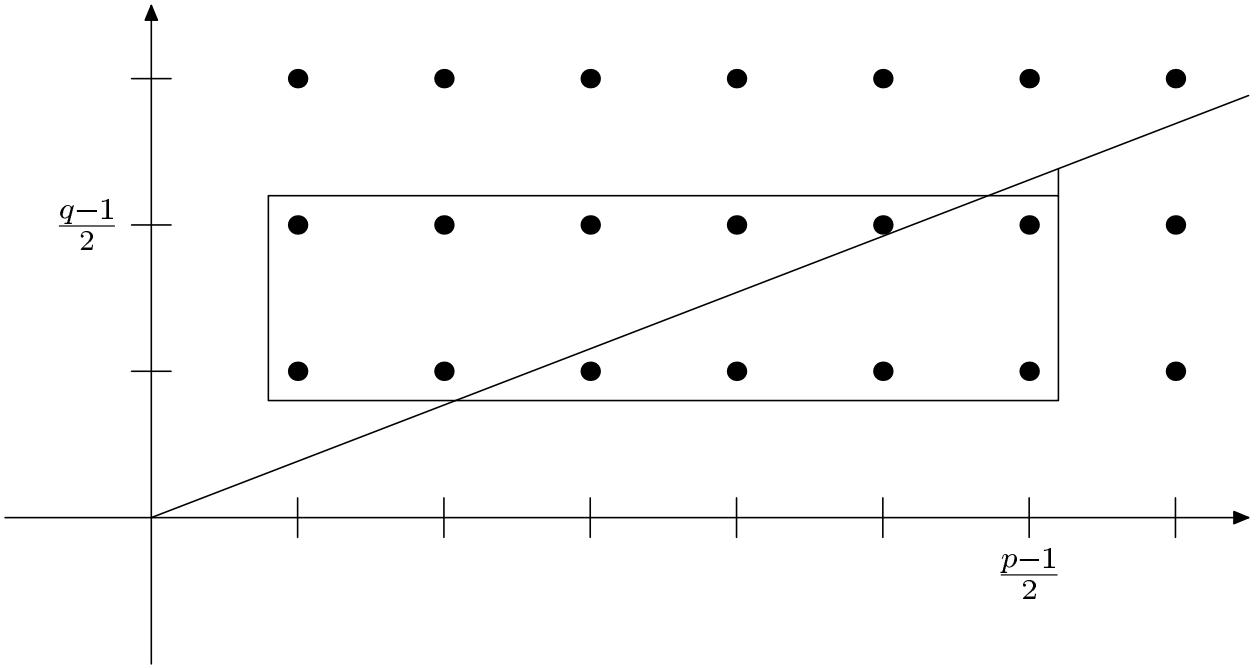
Zákon kvadratickej reciprocity



$$p = 7, q = 5$$

Zákon kvadratickej reciprocity

Zákon kvadratickej reciprocity

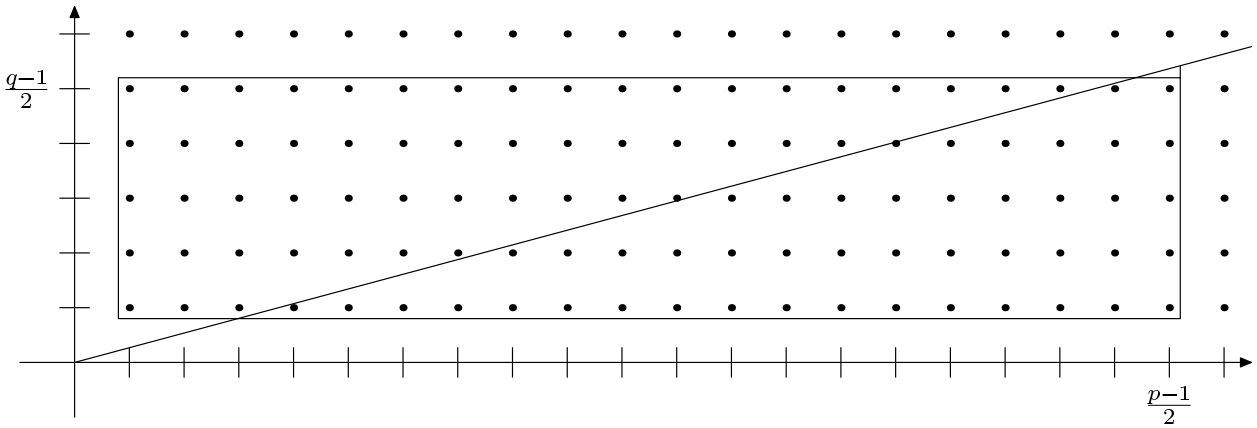


$p = 13, q = 5$

Obr. : Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 13$, $q = 5$

Zákon kvadratickej reciprocity

Zákon kvadratickej reciprocity



$p = 41, q = 7$

Obr. : Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 41$, $q = 7$

Zákon kvadratickej reciprocity

Zákon kvadratickej reciprocity

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

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{382\cdot 2/4} = \left(\frac{2}{3}\right)(-1)^{191} = 1$$

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)(-1)^{382\cdot 72/4} = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) \overset{(*)}{=} 1 \cdot 1 = 1$$