JACOBIHO SYMBOL

MINULE:

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

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

PLÁN: Viem pre Jacobiho symbol dokázať podobné veci ako pre Legendrov symbol - HLAVNE ZÁKON RECIPROCITY ?

Legendre: $\left(\frac{a}{p}\right) = 1 \Leftrightarrow a \; R \; p$ (p prvočíslo)

Jacobi: $\left(\frac{a}{P}\right)$ (P nepárne)

$a \; R \; P \Rightarrow \left(\frac{a}{P}\right) = 1$ $\not\Leftarrow$

$\left(\frac{a}{P}\right) = -1 \Rightarrow a \; \bar{R} \; P$

$\underbrace{\left(\frac{2}{5}\right)}_{-1}\underbrace{\left(\frac{2}{5}\right)}_{-1} = 1$ ale $(-1) \; \bar{R} \; 15$

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

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

(ii) $\left(\frac{1}{P}\right) = 1$

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

(iv) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

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

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

Tvrdenie 4.4.4. *Nech P je nepárne prirodzené číslo. Potom*

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2} \quad \checkmark$$

$$\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8} \quad \checkmark$$

D: VIEME: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

$P = p_1 p_2 \ldots p_n$

$$\left(\frac{-1}{P}\right) = \prod_{i=1}^{n}\left(\frac{-1}{p_i}\right) = \prod (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum \frac{p_i-1}{2}} \overset{?}{=} (-1)^{\frac{P-1}{2}}$$

$$P = \prod_{i=1}^{n} p_i = \prod_{i=1}^{n}(1 + (p_i - 1)) = 1 + \sum_{i=1}^{n}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \ldots$$

(súčin 4)

$$p-1 = \sum_{i=1}^{n} (p_i - 1) \pmod 4$$

$$\frac{p-1}{2} = \sum_{i=1}^{n} \frac{p_i - 1}{2} \pmod 2 \quad (*)$$

2. $\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}$ 2.

$$p^2 = \prod_{i=1}^{n} p_i^2 = \prod (1 + (p_i^2 - 1))$$

majú obe 4

$$(p_i^2 - 1)(p_j^2 - 1)$$

$$p^2 - 1 = \sum_{i=1}^{n} (p_i^2 - 1) \pmod{16}$$

$$\frac{p^2-1}{8} = \sum_{i=1}^{n} \frac{p_i^2 - 1}{8} \pmod 2$$

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\sum \frac{p_i^2-1}{8}} = \prod (-1)^{\frac{p_i^2-1}{8}} = \prod \left(\frac{2}{p_i}\right)$$

□

Veta 4.4.5 (Zákon reciprocity pre Jacobiho symbol). *Pre ľubovoľné nepárne prirodzené čísla $P \neq Q$ platí*

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

Dôsledok 4.4.6. *Ak $P \neq Q$ sú nepárne čísla, 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 $\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right)$.)

Veta 4.4.5 (Zákon reciprocity pre Jacobiho symbol). *Pre ľubovoľné nepárne prirodzené čísla $P \neq Q$ platí*

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

D: BÚNV $\boxed{(P,Q)=1}$ ($\not\leftarrow 0=0$)

(2.) $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) \overset{(2.)}{=} (-1)^{\frac{(P-1)(Q-1)}{4}}$ (2.) ✓

$P = p_1 \dots p_n \qquad Q = q_1 \dots q_0 \qquad p_i \neq q_j$

$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right) \dots \left(\frac{P}{q_0}\right) = \left(\frac{p_1}{q_1}\right) \dots \left(\frac{p_n}{q_1}\right) \dots \dots \dots$

$\left(\frac{P}{Q}\right) = \prod_{i=1}^{n} \prod_{j=1}^{n} \left(\frac{p_i}{q_j}\right) \qquad \left(\frac{Q}{P}\right) = \prod_{i=1}^{n} \prod_{j=1}^{n} \left(\frac{q_j}{p_i}\right)$

$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{n} \prod_{j=1}^{n} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \dots$ (2.)

ZR pre Legendrov symbol:

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{(p_i-1)(q_j-1)}{4}}$$

$\prod_{i=1}^{n} \prod_{j=1}^{n}$ -1|— $= (-1)^{\Sigma\Sigma -1|-}$

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \frac{(p_i-1)(q_j-1)}{4} = \sum_i \sum_j \frac{p_i-1}{2} \cdot \frac{q_j-1}{2}$$

$$= \left(\sum_i \frac{p_i-1}{2}\right)\left(\sum_j \frac{q_j-1}{2}\right) \overset{(*)}{\equiv} \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod 2$$

$\Downarrow \qquad \Downarrow$

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$ ✓ □

Dôsledok 4.4.6. *Ak $P \neq Q$ sú nepárne čísla, 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 $\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right)$.)

PR: $\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\underbrace{\left(\frac{4}{219}\right)}_{=1}\left(\frac{41}{219}\right) =$

$= -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) = -\underbrace{\left(\frac{2}{41}\right)}_{=(-1)^{\frac{41^2-1}{8}}=1}\left(\frac{7}{41}\right)$

$= -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{6}{7}\right) = -\underbrace{\left(\frac{-1}{7}\right)}_{=-1} = 1$

↳ nemuseli sme ROZKLADAŤ NA PRVOČÍSLA
↳ Máme veľmi efektívny alg.

Tvrdenie 4.4.8. *Nech a je celé číslo, ktoré nie je druhou mocninou celého čísla. Potom existuje nekonečne veľa prvočísel p, pre ktoré je a kvadratický nezvyšok.*

Dk: $a = (-1)^{\ell} q_1 \dots q_s$ $\quad \ell \in \{0,1\}$ $\quad q_1, \dots, q_s$ – rôzne nepárne prvočísla

$s > 1 \rightarrow a = 2 \dots$ NESKÔR

Nech $p_1, \dots, p_k$ sú prvočísla t.ž. $a \overline{R} p_i$, $i = 1, \dots, k$.

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 1 \pmod{p_i} \quad i = 1, \dots, k \\ x &\equiv 1 \pmod{q_j} \quad j = 1, \dots, s-1 \\ x &\equiv b \pmod{q_s} \qquad b \overline{R} q_s \end{aligned}$$

↓ ČÍV2 ↑

$\exists$ t.ž. m t.ž.

$$\left(\frac{a}{m}\right) = \underbrace{\left(\frac{2}{m}\right)^{\ell}}_{=1}\left(\frac{q_1}{m}\right) \dots \left(\frac{q_{s-1}}{m}\right)\left(\frac{q_s}{m}\right) \quad \leftarrow m \equiv 1 \pmod 4$$

$$= \left(\frac{m}{q_1}\right) \dots \left(\frac{m}{q_{s-1}}\right)\left(\frac{m}{q_s}\right)$$

$$= \left(\frac{1}{q_1}\right) \dots \left(\frac{1}{q_{s-1}}\right)\left(\frac{b}{q_s}\right) = \boxed{-1}$$

$\left(\frac{a}{n}\right) = -1 \Rightarrow \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_n}\right)$

$n = p_1 \dots p_n$

$\exists p \mid n \quad \boxed{\left(\frac{a}{p}\right) = -1}$

$a \not\equiv p$ $\qquad$ $p \neq p_1, \dots, p_k$

$[n \equiv 1 \pmod{p_i} \Rightarrow p_i \nmid n$

EULER $a = 2$ … $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p = 8k \pm 1$

$n = 8 p_1 \dots p_k + 3 \qquad 3 \notin \{p_1, \dots, p_k\}$

$(\exists p \in \mathbb{P})\ p \mid n \Rightarrow 2 \not\equiv p$

$+ p \neq p_1, \dots, p_k$ $\square$

4.5 Kvadratické kongruencie modulo zložené čísla

$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

Veta 4.5.1. *Nech p je nepárne prvočíslo, $p \nmid a$ a $n \geq 1$. Potom a je kvadratický zvyšok modulo p^n práve vtedy, keď $\left(\frac{a}{p}\right) = 1$.*

? $\Leftrightarrow$!

D: $\Rightarrow$ ✓

$\Leftarrow$ MI na n → p^n

1° $n = 1$ ✓

2° $a \not\equiv p^n \overset{2.}{\Rightarrow} a \not\equiv p^{n+1}$

$\exists x \in \mathbb{Z}$ $x^2 \equiv a \pmod{p^n}$ $\qquad (x, p) = 1$

$x^2 \equiv a + b p^n \pmod{p^{n+1}}$

$a + (b + 2xc) p^n \equiv a$

$(x + c p^n)^2 \equiv x^2 + 2xc p^n \equiv a + b p^n + 2xc p^n \pmod{p^{n+1}}$

$c = ?$ → zvolím c t. ž. $b + 2xc \equiv 0 \pmod{p}$

$2xc \equiv -b \pmod{p}$ ✓

Tvrdenie 4.5.2. *Modulo* 2, 4 *alebo* 8 *je jediným nepárnym kvadratickým zvyškom číslo* 1.
Ak $n \geq 3$, *tak existuje* 2^{n-3} *nepárnych kvadratických zvyškov modulo* 2^n *a sú to práve čísla tvaru* $8k+1$.

↑ D ... v škole

↓ ↓

VIEM: mod p^m $\Rightarrow$ ČV 2

$x^2 \equiv a \pmod{p_1^{a_1} \dots p_k^{a_k}}$ ⇐ N.D.V. (v škole - PR)

$x^2 \equiv a \pmod{p_1^{a_1}}$

$\vdots$

$x^2 \equiv a \pmod{p_k^{a_k}}$