KVADRATICKÉ KONGRUENCIE

$$x^2 \equiv a \pmod p$$

DANÉ: $a, p \in \mathbb{P}$ → OTÁZKA: je. riešiteľné?

↳ ~~skúšanie v možnostiach~~

$x^2 \equiv 5 \pmod{11}$

$4^2 \equiv 5 \pmod{11}$ ↖ SR 11

4.1 Kvadratické zvyšky

Definícia 4.1.1. Nech $n \nmid q$. Potom sa číslo q sa nazýva *kvadratický zvyšok* modulo n, ak existuje také $x \in \mathbb{Z}$, že

$$x^2 \equiv q \pmod n.$$

V opačnom prípade hovoríme, že q je *kvadratický nezvyšok* modulo n.

Budeme používať aj stručnejší zápis: qRn znamená, že q je kvadratický zvyšok modulo n a $q\overline{R}n$ znamená, že q je kvadratický nezvyšok modulo n.

PR: $n = 7$:

$1^2 \equiv 6^2 \equiv 1 \pmod 7$ $\quad 6^2 \equiv (-1)^2 \equiv 1^2 \pmod 7$

$2^2 \equiv 5^2 \equiv 4 \pmod 7$

$3^2 \equiv 4^2 \equiv 2 \pmod 7$

1, 2, 4 ... zvyšky

3, 5, 6 ... nezvyšky

Veta 4.1.4. *Nech $p > 2$ prvočíslo. Ľubovoľný redukovaný zvyškový systém $\{a_1, \ldots, a_{p-1}\}$ modulo p obsahuje $\frac{p-1}{2}$ kvadratických zvyškov a $\frac{p-1}{2}$ kvadratických nezvyškov modulo p.*

Kvadratické zvyšky sú práve tie čísla, ktoré sú kongruentné s číslami $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

1, 2, ..., p-1

D1: $x^2 \equiv a \pmod p$

$x^2 = a$ v $\mathbb{Z}_p$

$x^2 = y^2 \Leftrightarrow x^2 - y^2 = 0 \Leftrightarrow (x+y)(x-y) = 0 \Leftrightarrow x = \pm y$ $\quad$ (v $\mathbb{Z}_p$)

Každé z nich 2 rôzne. → $\frac{p-1}{2}$ možností. □

D2: $G(\mathbb{Z}_p^*, \cdot)$

$\varphi: x \longmapsto x^2$ hom.

$|\operatorname{Im}\varphi| = 2$

$\operatorname{Im}\varphi \cong \mathbb{Z}_p^* / \operatorname{Ker}\varphi$

$|\operatorname{Im}\varphi| = \frac{p-1}{2}$

$|\operatorname{Ker}\varphi| = 2$ ... $x^2 = 1 \Leftrightarrow x = \pm 1$ □

4.2 Legendrov symbol

Definícia 4.2.1. Ak p je prvočíslo a a je celé číslo, tak *Legendrov symbol* $\left(\frac{a}{p}\right)$ definujeme nasledovne:

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

Niekedy sa používa aj označenie $(a|p)$.

PR: $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$

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

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

D: $p \mid n$ ✓

$p \nmid n \Rightarrow n^{p-1} \equiv 1 \pmod{p}$

$p \mid n^{p-1} - 1 = \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$

$\Rightarrow p \mid n^{\frac{p-1}{2}} - 1 \quad \vee \quad p \mid n^{\frac{p-1}{2}} + 1$

$\Rightarrow n^{\frac{p-1}{2}} \equiv 1 \pmod{p} \vee n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

L'S, PS $\equiv \pm 1 \pmod{p}$

$n R p \Rightarrow n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

[$n \equiv x^2 \pmod{p} \Rightarrow n^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$

+ VIEME: $\frac{p-1}{2}$ kr. nejako → INÉ n TO NESPĹŇAJÚ

[Lagrange: $\leq \frac{p-1}{2}$ riešení

nerovnosť: ~~$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$~~ $\vee$ $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

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

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

Lema 4.2.5. *Nech p je nepárne prvočíslo a $a, b \in \mathbb{Z}$. Potom*

(i) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ✓ $\quad x^2 \equiv a \equiv b \pmod p$

(ii) $\left(\frac{1}{p}\right) = 1$ ✓

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

(iv) $\left(\frac{a^2}{p}\right) = 1$ ✓

(v) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

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

$\left(\frac{ab}{p}\right) \overset{?}{=} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p$

LS: ± 1 $\quad \pm 1 \equiv \pm 1 \pmod p \quad p > 2$

↳ ROVNOSŤ □

$\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ ← $Z \cdot Z = Z$, $N \cdot Z = Z \cdot N = N$, $N \cdot N = Z$ } N.D.Ú. bez Eulera

Tvrdenie 4.2.6. *Pre každé nepárne prvočíslo platí*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \quad ✓$$

Teda -1 je kvadratický zvyšok modulo p ak $p = 4k+1$ a kvadratický nezvyšok modulo p ak $p = 4k+3$.

D: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$ $\quad L/P: \pm 1$, $p > 2$

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

$\frac{p-1}{2}$ < párne: $\frac{p-1}{2} = 2k \Rightarrow p-1 = 4k$; nepárne: $\frac{p-1}{2} = 2k+1 \Rightarrow p-1 = 4k$, $p = 4k+3$ □

PR: $p=5 \quad 2^2 \equiv -1 \pmod 5$

$p=7 \quad (-1) \not\equiv 7$

Tvrdenie 4.2.7. *Existuje nekonečne veľa prvočísel tvaru $4k+1$.*

D: $q_1, \dots, q_n \in \mathbb{P} \cap (4\mathbb{N}+1)$ $\quad N = (2q_1 \dots q_n)^2 + 1$

$p \mid N = x^2 + 1$ $\quad x^2 \equiv -1 \pmod p$

$p \neq q_1, \dots, q_n$ $\quad (-1) R\, p \Rightarrow p = 4k+1$ □

Prvočísla v AP: DIRICHLET

$(a,d)=1$ $dm+a$ $\rightarrow \infty$ veľa $\mathbb{P}$

Tvrdenie 4.2.8. *Nech $p>2$ je prvočíslo. Potom*

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

Teda 2 je kvadratický zvyšok pre prvočísla tvaru $8k\pm1$ a kvadratický nezvyšok pre prvočísla tvaru $8k\pm3$.

D: $2, 4, \dots, p-1$ $\pm 1, 2, \dots, \frac{p-1}{2}$

$p-1 \equiv -1 \pmod p$

$2 \equiv (-1)^2 2 \pmod p$

$p-3 \equiv (-1)^3 3$ — || —

$4 \equiv (-1)^4 4$ — || —

$\vdots$

$\frac{p\pm1}{2} \equiv (-1)^{\frac{p-1}{2}} \frac{p-1}{2}$

VYNÁSOBME

PS: $(-1)^{\frac{p-1}{2}} 1\cdot 2\cdot 3\cdot 4 \cdots \left(\frac{p-1}{2}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \pmod p$

$1+2+3+\dots+\frac{p-1}{2} = \frac{\frac{p-1}{2}\cdot\frac{p+1}{2}}{2} = \frac{p^2-1}{8}$

LS: súčin V párnych:

$2\cdot 4\cdot \dots \cdot (p-1) \equiv$

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

$(-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \equiv 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$

$(-1)^{\frac{p^2-1}{8}} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod p$

L/P: ± 1 $(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)$

$\frac{p^2-1}{8}$ < párne / nepárne

$p=8k\pm1$: $\frac{p^2-1}{8} = \frac{(64k^2\pm16k+1)-1}{8} = 8k^2\pm2k$

$p=8k\pm3$: $\frac{q-1}{8} = 2(\ )+1$

PR: $p=7$ $3^2 \equiv 2 \pmod 7$ ✓

$p=5$ $1^2\equiv 4^2\equiv -1 \pmod 5$, $2^2\equiv 3^2\equiv 4 \pmod 5$ $\left(\frac{2}{5}\right)=-1$ ✓

∎

Tvrdenie 4.2.10. *Existuje nekonečne veľa prvočísel tvaru $8k+7$.*

D: $q_1, \dots, q_n \dots$ prvočísla tvaru $8k+7$

$$N = (4q_1 \dots q_n)^2 - 2 = 2 \cdot (8q_1^2 \dots q_n^2 - 1)$$

$p \neq 2 \quad p \mid N \quad p \neq q_1, \dots, q_n$

$p \mid x^2 - 2 \qquad x^2 \equiv 2 \pmod p$

$2 R p \Rightarrow p = \begin{cases} 8k+1 \\ 8k+7 \end{cases}$

Musí byť aspoň 1 z $8k+7$ ($k-1$) ... chceme $\equiv -1 \pmod 8$

$p = 8k+7 \qquad p \neq q_1, \dots, q_n$ □

Veta 4.2.11. *Ak $p = 4k+3$ je prvočíslo, $k > 1$, tak $q = 2p+1$ je prvočíslo práve vtedy, keď $2p+1 \mid M_p = 2^p - 1$.*

D: ⇒ $q = 2p+1 = 8k+7 \Rightarrow 2 R q \Rightarrow x^2 \equiv 2 \pmod q$

$$\left.\begin{aligned} x^{2p} &\equiv 2^p \pmod q \\ x^{2p} = x^{q-1} &\equiv 1 \pmod q \end{aligned}\right\} \Rightarrow \quad 2^p \equiv 1 \pmod q$$

$q \mid 2^p - 1$

⇐ $d \mid 2p+1 \Rightarrow d \mid M_p \overset{3.1.15}{\Rightarrow} d = kp+1$

$1, \cancel{p+1}, 2p+1$

$\leftarrow \begin{cases} p+1 \mid 2p+1 \\ p+1 \mid 2p+2 \end{cases} \Rightarrow p+1 \mid 1$

$q = 2p+1$ nemá nt. deliteľa □

PR: $p = 11, \ q = 23 \qquad 23 \mid 2^{11} - 1 = 2047 = 23 \cdot 89$

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*

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

PRÍ: $\left(\frac{2}{7}\right) = 1$ $\quad a=2,\ p=7$

$\left(\frac{5}{7}\right) = -1$ $\quad a=5,\ p=7$

$k \cdot a,\ k = 1, \ldots, \frac{p-1}{2} = 3$

$2, 4, 6$ $\quad \frac{7}{2}$ $\quad m=2$

$2, -3, -1$

$5, 10, 15$

$5, 3, 1$ $\quad m=1$

$-2, 3, 1$

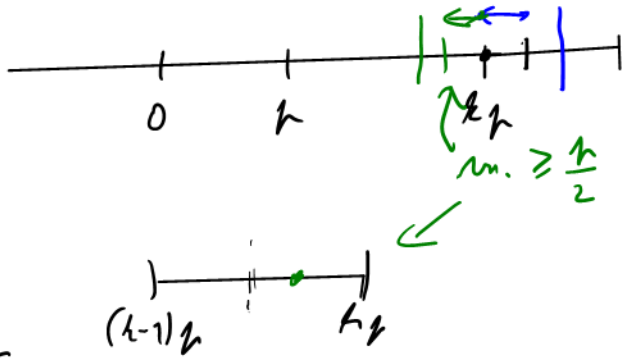
Veta 4.2.12 (Gaussova lema). *Nech $p > 2$ je prvočíslo a $p \nmid a$. Nech m je počet tých čísel z množiny $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, ktorých zvyšok po delení p je väčší než $\frac{p}{2}$. Potom*

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

D: $a, 2a, \ldots, \frac{p-1}{2}a$

$k \cdot a,\ k = 1, \ldots, \frac{p-1}{2}$

$ka \equiv \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$



SÚČIN: $a \cdot 2a \cdot \ldots \cdot \left(\frac{p-1}{2}\right)a \equiv$

$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$

$\pm 1 \cdot \pm 2 \cdot \ldots \cdot \pm\frac{p-1}{2}$

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

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

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

UKÁŽEME: 2. každý dvojice práve 1

$ka \equiv la \pmod p \Rightarrow k \equiv l \pmod p$

$\Rightarrow k = l$

$ka \equiv -la \pmod p \Rightarrow$

$\Rightarrow (k+l)a \equiv 0 \pmod p \Rightarrow p \mid k+l$

$k, l \in \{1, 2, \ldots, \frac{p-1}{2}\}$

$2 \le k+l \le p-1$

žiadna dvojica nám nie je duplicitná

$\Rightarrow$ každá z nich sa vyskytuje práve raz