$d = (3, 22) = 1$

$5^{\frac{22}{1}} \equiv 1 \ (23)$

$\Rightarrow$ 1 řešení

① (z DÚ) Řešte kongruenci $x^3 \equiv 5 \ (23)$

s využitím prim. kořenů

$\varphi(23) = 22 = 2 \cdot 11$

g je p.k. $\Leftrightarrow g^{\frac{22}{2}} \not\equiv 1 \ (23)$ $\wedge$ $g^{\frac{22}{11}} \not\equiv 1 \ (23)$

zkusme, co když by $g = 5$:

$5^2 = 25 \equiv 2 \not\equiv 1 \ (23)$

$5^{11} = (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 \equiv -1 \ (23)$

$\Rightarrow$ 5 je prim. kořen mod 23

POZN:

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

silnější:

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

Řešíme, substituce: $x \equiv 5^y \ (23)$

$5 \equiv 5^1 \ (23)$

$(5^y)^3 \equiv 5^1 \ (23)$

$5^{3y} \equiv 5^1 \ (23)$

$3y \equiv 1 \ (22)$

$3y \equiv -21 \ (22) \ | : 3$

$y \equiv -7 \ (22)$

$y \equiv 15 \ (22) \Leftrightarrow x \equiv 5^{15} \equiv 5^{11} \cdot 5^5 \equiv -2^2 \ (23)$

$x \equiv 19 \ (23)$

i) $x^3 \equiv 1 \ (23)$

víme, že $(3, 22) = 1 \Rightarrow$ má jediné řešení $x \equiv 1 \ (23)$

② Určete počet řešení kongruence $5x^{30} \equiv 34 \ (41^2)$

i) binomická kongruence: (V) $(30, \varphi(41^2)) = (30, 40 \cdot 41) = 10$

ii) Henselovo lemma má buď 0 nebo 10 řešení

ad i) 0 nebo 10 řešení

$41^2 = (40+1)^2 = 1681$

$5x^{30} \equiv 34 - 3362 \ (41^2)$

$5x^{30} \equiv -3325 \ (41^2) \ | : 5$

$x^{30} \equiv -665 \ (41^2)$

podmínka řešitelnosti je

$d=10$ $\quad (-665)^{\frac{40\cdot 41}{d}} = (-665)^{4\cdot 41} \equiv ? \pmod{41^2}$

$a \equiv b \pmod{m^n}$ ⇓ $a^m \equiv b^m \pmod{m^{n+1}}$

obtížný výpočet („na prapíle")

$(-665)^4 \overset{?}{\equiv} a \pmod{41} \Rightarrow \left((-665)^4\right)^{41} \equiv a^{41} \pmod{41^2}$

$a \equiv (-9)^4 = 9^3 = (9^2)^2 \equiv (-1)^2 \equiv 1 \pmod{41}$

$\Rightarrow ((-665)^4)^{41} \equiv a^{41} \equiv 1^{41} = 1 \pmod{41^2}$

$\Rightarrow$ kongruence má 10 řešení

ii) jinak, s využitím Henselova lematu:

$f(x) = 5x^{30} - 37 \Rightarrow f'(a) = 150x^{29}$

$\forall a \in \mathbb{Z},\ a \not\equiv 0 \pmod{41} \Rightarrow f'(a) \not\equiv 0 \pmod{41}$

$\Rightarrow$ každé řešení $f(x) \equiv 0 \pmod{41}$ dá jedno řešení mod 41^2

Otázka: počet řešení $5x^{30} \equiv 37 \pmod{41}$?

$5x^{30} \equiv 37 - 82 \pmod{41}$

$5x^{30} \equiv -45 \pmod{41} \quad / : 5$

$x^{30} \equiv -9 \pmod{41}$

Ta je řešitelná, právě když $(-9)^{\frac{\varphi(41)}{d'}} \equiv 1 \pmod{41}$ $\quad d' = (30, \varphi(41)) = 10$

$(-9)^{\frac{40}{10}} \equiv 1 \pmod{41}$

$(-9)^4 \equiv 1 \pmod{41}$

$3^8 \equiv (3^4)^2 \equiv (-1)^2 \equiv 1 \pmod{41}$ ✓

$\Rightarrow$ kongruence mod 41 má 10 řešení

$\Rightarrow$ kongruence mod 41^2 má 10 řešení

(3) Kvadratické kongruence

$ax^2 + bx + c \equiv 0 \pmod{m} \rightsquigarrow x^2 \equiv A \pmod{p}$

ta je řešitelná (pro $p \nmid A$), právě když $A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

DEFINICE. Nechť je p liché prvočíslo. *Legendreův symbol* definujeme předpisem

„a vzhledem k p" $\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a,\ a \text{ je kvadratický zbytek modulo } p, \\ 0 & p \mid a, \\ -1 & p \nmid a,\ a \text{ je kvadratický nezbytek modulo } p. \end{cases}$

tj. $x^2 \equiv a (p)$ je řešitelná

tj. $x^2 \equiv a (p)$ není řešitelná

dvě řešení, kongruence $x^2 \equiv a \pmod p$ má $1 + \left(\frac{a}{p}\right)$ řešení

$\left(\frac{1}{p}\right) = 1$ $(x^2 \equiv 1 \pmod p)$, $\left(\frac{-1}{5}\right) = 1$, $\left(\frac{-1}{3}\right) = -1$ $x^2 \not\equiv -1 (3)$ n. ř.

$x^2 \equiv -1 (5) \Leftrightarrow x \equiv \pm 2 (5)$

LEMMA. *Nechť p je liché prvočíslo, $a, b \in \mathbb{Z}$ libovolná. Pak platí:*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a \equiv b \pmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

ad 3. zřejmé: $x^2 \equiv a (p)$ je řešitelná $\Leftrightarrow x^2 \equiv b \pmod p$ je řešitelná

ad 1. souvislost s V o binomických kongruencích

pťa $x^2 \equiv a \pmod p$ je řeš. $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\left(\frac{a}{p}\right) = 1 \Rightarrow$ je řeš. $\Rightarrow a^{\frac{p-1}{2}} \equiv 1 (p) \Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$\left(\frac{a}{p}\right) = -1 \Rightarrow$ není řeš. $\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 (p)$

& $a^{\frac{p-1}{2}} \equiv \pm 1 (p)$; ii: $\left(\pm a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 (p)$

2 řeš. kongruence $x^2 \equiv 1 (p)$, kterými jsou ± 1

jinak ii) $p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$

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

$\Leftrightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$

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

pťa zřejmé

ad 2. chceme multiplikativitu (tj. Leg. symbol je homomorfismus $(\mathbb{Z}_p^\times, \cdot) \to (\{1, -1\}, \cdot) : [a]_p \mapsto \left(\frac{a}{p}\right)$)

$\left(\frac{ab}{p}\right) \overset{(1)}{\equiv} (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \overset{(1)}{\equiv} \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p$

2 kongruence dostaneme snadno rovnost, ovšem

$\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \in \{1, -1, 0\}$

ZÁKON KVADRATICKÉ RECIPROCITY

VĚTA 32. *Nechť p, q jsou lichá prvočísla. Pak*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (plyne z Lemmatu: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$ ⇓ rovnost)
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ RECIPROCITA

Dle vzor příkladů

ad 1. $\left(\frac{-1}{p}\right) = 1$ (tj. -1 je kvadr. zbytek mod p $\Leftrightarrow$) $\Leftrightarrow$ $\frac{p-1}{2}$ je sudé $\Leftrightarrow$ $4 \mid p-1 \Leftrightarrow p \equiv 1 \pmod 4$

ad 2. $\left(\frac{2}{p}\right) = 1 \Leftrightarrow \frac{p^2-1}{8}$ je sudé $\Leftrightarrow 16 \mid p^2-1 \Leftrightarrow p \equiv \pm 1 \pmod 8$

$p \equiv \pm 1 \pmod{2^3} \Rightarrow p^2 \equiv 1 \pmod{2^4}$

$p \equiv \pm 3 \pmod{2^3} \Rightarrow p^2 \equiv 9 \pmod{2^4}$

Snadnější:
$p = 8k \pm 1 \Rightarrow$
$p^2 = 64k^2 \pm 16k + 1$
$\Rightarrow 16 \mid p^2 - 1$
anal. $p = 8k \pm 3$

ad 3. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \Leftrightarrow$ $\frac{p-1}{2} \cdot \frac{q-1}{2}$ je sudé
$\Leftrightarrow 4 \mid p-1$ v $4 \mid q-1$
$\Leftrightarrow p \equiv 1 \pmod 4$ v $q \equiv 1 \pmod 4$

(4) Určete počet řešení kongruence $x^2 \equiv 433 \pmod{503}$, kde 503 je prvočíslo

Řeš: kongruence je řešitelná (a má 2 řešení), pokud:

$\left(\frac{433}{503}\right) = 1.$

$\left(\frac{433}{503}\right) \overset{\text{ZKR}}{=} \left(\frac{503}{433}\right) \cdot (-1)^{\frac{503-1}{2}\cdot\frac{433-1}{2}} = \left(\frac{503}{433}\right) \cdot (+1) \overset{L(3)}{=} \left(\frac{70}{433}\right) \overset{L(2)}{=}$

$503 \equiv 3 \pmod 4$, $433 \equiv 1 \pmod 4$

ověříme, že 433 je prvočíslo ✓

$= \left(\frac{2}{433}\right)\left(\frac{5}{433}\right)\cdot\left(\frac{7}{433}\right) \overset{\text{ZKR2}}{=} (+1) \cdot \left(\frac{433}{5}\right)(+1) \cdot \left(\frac{433}{7}\right)\cdot(+1) =$

$433 \equiv 1 \pmod 8$; $433 \equiv 1 \pmod 4$, $5 \equiv 1 \pmod 4$

$\overset{L(3)}{=} \left(\frac{3}{5}\right) \cdot \left(\frac{-1}{7}\right) \overset{\text{ZKR}}{=} \left(\frac{5}{3}\right)\cdot(+1)\cdot(-1) \overset{L(3)}{=} \left(\frac{-1}{3}\right)(-1) = (-1)(-1) = 1$

$5 \equiv 1 \pmod 4$, $7 \equiv 3 \pmod 4$, $3 \equiv 3 \pmod 4$

Kongruence $x^2 \equiv 433 \pmod{503}$ má 2 řešení. $\left(\frac{503+1}{4}\right)$
(pozn.: ± 433)

(5) Dokážeme, že existuje nekonečně mnoho prvočísel tvaru $4k+1$

Dk: sporem. Předpokládejme, že $p_1, p_2, \dots, p_e$ jsou všechna prvočísla tvaru $4k+1$.

Položme $N = (2p_1 \cdots p_e)^2 + 1$, to je opět tvaru $4k+1$.

a) N je prvočíslo, pak máme hned spor

b) N je složené, pak existuje prvočíslo $p \mid N$.

Určitě $p \notin \{2, p_1, \dots, p_e\}$

(pro $q \in \{2, \dots, p_e\}$ platí $q \mid N \Rightarrow q \mid (2p_1 \cdots p_e)^2$
$\Rightarrow q \mid N - (2p_1 \cdots p_e)^2 = 1$)

Protože ale $(2p_1 \cdots p_e)^2 \equiv -1 \pmod p$,
znamená to, že kongruence

$$x^2 \equiv -1 \pmod p$$

má řešení $2p_1 \cdots p_e$, tj. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$

To je hledané nové prvočíslo $p \equiv 1 \pmod 4$, $p \notin \{p_1, \dots, p_e\}$ □

Př: $p_1 = 5, p_2 = 13$

$N = (2 \cdot 5 \cdot 13)^2 + 1 = 16901 \dots$ to je prvočíslo