1. PŘ

- max. 2 neomluvené neúčasti na cvičeních
- ~~2 písemky~~
- písemná + ústní + vnitrosemestrální písemka — test — 20.11. — po soustavy lin. kongruencí (písemky bez kalkulačky — nutnost mentální arit.)
- bonusové domácí úlohy
- literatura: elektronická skripta: Elementární teorie čísel: Bulant; 10. kapitola Matematika drsně a svižně

PARI-GP, SAGE   sage.math.muni.cz

- důkaz věty o dělení, ...   všude to vybezoutit

$a \mid b \iff 2^a - 1 \mid 2^b - 1$ $a = qb + r$

- eukleidův algoritmus (alternativní tvar) $(a,b) = (r,b)$ $\ldots$

1. CV

$3n+4$

- najít všechna $n \in \mathbb{Z}$: $3n+4 \mid 7n+1$

$3n+4 \mid 3(7n+1) - 7(3n+4)$

- $\forall n \in \mathbb{N}: 9 \mid 4^n + 15n - 1$ indukce nebo binomická věta

- $\forall a,b \in \mathbb{Z}: 17 \mid 2a+3b \iff 17 \mid 9a+5b$

~~např. $9a + 5b \equiv 26a + 5b \pmod{17}$~~

$2a + 3b \equiv 0 \ (17)$ $9a + 5b \equiv 0 \ (17)$

$a \equiv 7b \ (17)$ $a \equiv 7b \ (17)$

- $(2673, 7221) = 3$

$7221 = 2673 \cdot 2 + 1875$

$2673 = 1875 + 798$

$\vdots$

$240 = 39 \cdot 6 + 6$

$39 = 6 \cdot 6 + 3$

$6 = 3 \cdot 2 + 0$

$3 = 39 - 6 \cdot 6 = 39 - 6(240 - 39 \cdot 6) = 1 \cdot 39 \ldots 240 \ldots 37$

$= -6 \cdot 240 + 37 \cdot 39 = \ldots = 412 \cdot 7221 - 1113 \cdot 2673$

$n \in \mathbb{N}$ $d = (2n-1, 9n+4) = (2n-1, n+8) = (-17, n+8)$ $\quad d \in \{1, 17\}$

$9n+4 = (2n-1)\cdot 4 + n + 8$

$2n-1 = (n+8)\cdot 2 - 17$

$17 \mid n+8 \iff d = 17$

$17 \nmid n+8 \iff d = 1$

$n \in \mathbb{N}$ $d = (2n+3, n+7) = (-11, n+7)$

$11 \mid n+7 \iff d = 11$

$11 \nmid n+7 \iff d = 1$

$m, n \in \mathbb{N}$, $(m,n) = 1 \implies (m^2+mn+n^2, m^2-mn+n^2) = 1$

(m^2+mn+n^2, mn)

$((m+n)^2, mn)$

$p \mid m^2 - mn + n^2$

$p \mid m^2 + mn + n^2$

$p \mid 2mn$

$p \mid 2 \vee p \mid m \vee p \mid n$

$\vdots$

$x + y = 150$
$(x,y) = 30$

$x = 30x_1$
$y = 30y_1$
$(x_1, y_1) = 1$

$x_1 + y_1 = 5$ . . . 1,4 ; 2,3 ; 3,2 ; 4,1

$x \cdot y = 20$
$[x,y] = 10$

$(x,y) = 2$

$x = 2x_1$
$y = 2y_1$
$(x_1, y_1) = 1$

$x_1 y_1 = 5$ . .

2. PŘ

2. CV

– $\forall n \in \mathbb{N}$: nelze $6n+5$ rozpadnout jako součet dvou prvočísel

$6n+5 = q + q$

mod 2 dlyne $n = 2$

$6n+3 = q \cdot$ spor

- Najděte všechna $n \in \mathbb{N}$, pro která je n, $n+10$ a $n+14$ jsou prvočísla

mod 3 a je to $n \in \{3\}$

- Najděte všechna $p \in \mathbb{P}$ pro která je $4p^2+1$ a $6p^2+1$ jsou prvočísla

mod 5 a je to $p = 5$

- Dokažte, že $5^{20} + 2^{30}$ je složené.

~~mod 7 a je to~~ ~~(lze také použít $(a+b)^2 = 2ab$)~~

$5^2 + 2^{30} = (5^{10} + 2^{15})^2 - (5^5 \cdot 2^8)^2 = (5^{10} + 2^{15} - 5^5 \cdot 2^8) \cdot (5^{10} \cdot 2^{15} + 5^5 \cdot 2^8)$

nebo $(5^4)^5 + (2^6)^5$ rozložíme

- Určete $(a+b, ab)$, kde $(a,b) = 1$, $a, b \in \mathbb{N}$

~~$[a,b] = ab$~~

Předpoklad: $(a+b, ab) = 1$ spor: $p \mid a+b$

$p \mid ab$

~~$p \mid (a+b)^2 - 2ab = a^2 + b^2$~~

Euklid. věta: $p \mid a \vee p \mid b$

WLOG: $p \mid a$

$p \mid a+b$ $\Big\}$ $p \mid b$ ... spor s $(a,b) = 1$

- Určete $(a+b, [a,b])$ pro $a, b \in \mathbb{N}$

1) ~~Pokud~~ $(a,b) = 1$, pak z předchozí úlohy $(a+b, [a,b])$

2) $(a,b) \neq 1$ $a = dx$ $d = (a,b)$

$b = dy$ $(x,y) = 1$

$(a+b, [a,b]) = (d(x+y), d[x,y]) = d(x+y, [x,y]) = d = (a,b)$

Závěr $(a+b, [a,b]) = (a,b)$ (nebo z min. úlohy

~~$(dx+dy, xy) = 1$~~

$\left(\frac{a}{d} + \frac{b}{d}, \frac{a}{d} \cdot \frac{b}{d}\right) = 1$

$\left(a+b, \frac{ab}{d}\right) = d$

$(a+b, [a,b]) = d$

- Nechť $n \in \mathbb{N}$, p je prvočíslo $\quad v_p(n) = \max\{k \in \mathbb{N}_0 ; p^k \mid n\}$

$v_p(ab) = v_p(a) + v_p(b)$

$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

(rovnost $v_p(a) \neq v_p(b)$, jinak $v_p(a+b) = \min\{v_p(a), v_p(b)\}$

$v_p(\gcd(a,b)) = \min(v_p(a), v_p(b))$

$v_p([a,b]) = \max(v_p(a), v_p(b))$

- rozbor předchozí úlohy

$v_p(a) \leq v_p(b)$

~~$v_p((a,b)) = v_p$~~ obě strany mají stejné v_p

3 PŘ

$5^{20} \equiv 25^{10} \equiv (-1)^{10} \equiv 1 \pmod{26}$

$37^{n+2} + 16^{n+1} + 23^n \equiv 2^{n+2} + 2^{n+1} + 2^n \equiv 2^n(4+2+1) \equiv 0 \pmod 7$

$(835^5+6)^{18} - 1$

$112 \mid (835^5+6)^{18} - 1$

$112 = 16 \cdot 7$

$(835^5+6)^{18} - 1 \equiv (2^5+6)^{18} - 1 \equiv 3^{18} - 1 \equiv 27^6 - 1 \equiv (-1)^6 - 1 \equiv 0 \pmod 7$

$(835^5+6)^{18} - 1 \equiv (3^5+6)^{18} - 1 \equiv (3+6)^{18} - 1 \equiv 9^{18} - 1 \equiv 1^9 - 1 \equiv 0 \pmod{16}$

- Lemma: $a \equiv b \pmod{m^n} \Rightarrow a^m \equiv b^m \pmod{m^{n+1}}$

$1001 = 7 \cdot 11 \cdot 13$

$1000A + B \equiv B - A \pmod{\substack{7 \\ 11 \\ 13}}$

př. $5014410024 \equiv 24 - 5014410 \equiv 24 - (910 - 5014) \equiv 24 - 910 + 14 - 5 \equiv 5 \pmod 7$

3. CV.

* Dokažte, že $([a,b]\,|\,[a,c],[b,c]) = [(a,b),(a,c),(b,c)]$

WLOG $v_p(a) \le v_p(b) \le v_p(c)$

$v_p(L) = \min(v_p(b), v_p(c), v_p(c)) = v_p(b)$

$v_p(P) = \max(v_p(a), v_p(a), v_p(b)) = v_p(b)$ □

* Dokažte, že $[a,b,c]\cdot(ab,bc,ca) = abc$

WLOG $v_p(a) \le v_p(b) \le v_p(c)$

$\max(v_p(a), v_p(b), v_p(c)) + \min(v_p(a)+v_p(b), v_p(b)+v_p(c), v_p(c)+v_p(a)) = v_p(abc)$

$v_p(c) + v_p(ab) = v_p(abc)$

$v_p(c) + v_p(a) + v_p(b) = v_p(abc)$ □

* Dokažte, že pro $a,b,c \in \mathbb{N}$ a $(a,b)=1$ platí $(ab,c) = (a,c)\cdot(b,c)$

WLOG $v_p(a) \le v_p(b)$ $\quad v_p(a) = 0$

$v_p(L) = \min(v_p(c), v_p(c)) = \min(v_p(b), v_p(c))$

$v_p(P) = \min(v_p(a), v_p(c)) + \min(v_p(b), v_p(c)) = \min(v_p(b)+v_p(c))$

□

* Dokažte, že pro $a,n \in \mathbb{N}$ platí

$$\sqrt[n]{a} \in \mathbb{Q} \Rightarrow \sqrt[n]{a} \in \mathbb{Z}$$

$\exists p,q \in \mathbb{N}$ $\quad \sqrt[n]{a} = \frac{p}{q}$ $\quad (p,q)=1$ $\quad (p^n, q^n)=1$

$a = \frac{p^n}{q^n}$

$q^n a = p^n$

$q^n \mid p^n$

$\forall r \in \mathbb{P}$

$n\, v_r(q) + v_r(a) = n\, v_r(p)$

$v_r(q) = v_r(p) - v_r(a)$

Pokud $q \neq 1$, pak $\exists r \in \mathbb{P}: r \mid q$, pak i $r \mid p$, spor s $(p,q)=1$

Jedy $q=1$

□

* Nechť $a, b \in \mathbb{Q}^+$: $\sqrt{a} + \sqrt{b} \in \mathbb{Q} \Rightarrow \sqrt{a} \in \mathbb{Q} \wedge \sqrt{b} \in \mathbb{Q}$

$\sqrt{a} + \sqrt{b} = x$

$a + 2\sqrt{a}\sqrt{b} + b = x^2$

$2\sqrt{a}\sqrt{b} = x^2 - a - b \in \mathbb{Q}$

$\sqrt{a}\sqrt{b} \in \mathbb{Q}$

$y^2 - (\sqrt{a} + \sqrt{b})y + \sqrt{a}\sqrt{b} = 0$

$\frac{1}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}$

$\frac{\sqrt{a} - \sqrt{b}}{a - b} \in \mathbb{Q}$

$\sqrt{a} - \sqrt{b} \in \mathbb{Q}$

$\sqrt{a} + \sqrt{b} \in \mathbb{Q}$

$\Big\} \; 2\sqrt{a} \in \mathbb{Q}$

$\sqrt{a} \in \mathbb{Q}$

analogicky $\sqrt{b} \in \mathbb{Q}$

$\frac{\sqrt{a} + \sqrt{b}}{\sqrt{ab}} = \frac{1}{\sqrt{a}} + \frac{1}{\sqrt{b}} \in \mathbb{Q}$

$\left(\frac{1}{\sqrt{a}} + \frac{1}{\sqrt{b}}\right)(\sqrt{a} + \sqrt{b}) = 2 + 2\sqrt{ab}$

$\sqrt{a} - \sqrt{b}$

$y^2 - py + q = 0$

$a - (\sqrt{a} + \sqrt{b})\sqrt{a} + \sqrt{a}\sqrt{b} = 0$

$\sqrt{a} = \frac{a + \sqrt{a}\sqrt{b}}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}$

* Dokažte, že $a \in \mathbb{N}, a > 4$: a je složené $\Rightarrow a \mid (a-1)!$

$\exists d \in \mathbb{N}: 1 < d < a \wedge d \mid a$, tedy $\frac{a}{d}$

$a = d \cdot \frac{a}{d}$

nechť $d \neq \frac{a}{d}$, tak jsme hotovi

nechť $d^2 = a$:

$2d < a = d^2$

$2 < d$

$4 < a$

$a = d^2 \mid d \cdot 2d \mid (a-1)!$

* Dokaž $13 \mid 2^{60} + 7^{30}$

$2^{60} + 7^{30} \equiv 1 + 7^6 \equiv 1 + (-3)^3 \equiv 1 - 27 \equiv 0 \pmod{13}$

* Dokaž $25 \mid 72^{2n+2} - 47^{2n} + 28^{2n-1}$

$72^{2n+2} - 47^{2n} + 28^{2n-1} \equiv (-3)^{2n+2} - (-3)^{2n} + 3^{2n-1} \equiv 3^{2n-1}(27 - 3 + 1) \equiv 0 \pmod{25}$

* $15^{2015} \equiv 15^5 \equiv 30 \pmod{31}$

* $15^{2015} \equiv 3^{2015} \cdot 5^{2015} \equiv 9 \cdot (5^3)^{1007} \cdot 5 \cdot (3^3)^{671} \equiv 1 + 45 \equiv 7 \pmod{26}$

* $11 \mid 5^{5k+1} + 4^{5m+2} + 3^{5n}$

$5^{5k+1} \equiv 5 \cdot (5^5)^k \equiv 5 \pmod{11}$

$4^{5m+2} \equiv 16 \cdot (4^5)^m \equiv 16 \equiv 5 \pmod{11}$

$3^{5n} \equiv (3^5)^n \equiv 1 \pmod{11}$ □

4. PŘ.

- aritmetická funkce – zobrazení $\mathbb{N} \to \mathbb{C}$.
- Möbiova funkce μ. Definujme $\mu(1) = 1$. $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

$$\mu(n) = \begin{cases} 0 & \text{je dělitelné čtvercem} \\ (-1)^k & \text{je bezčtvercové, } k \text{ počet prvočísel} \end{cases}$$

$\mu(1) = 1$

- Lemma. $n \in \mathbb{N}$ $n > 1$

$$\sum_{d \mid n} \mu(d) = 0$$

- Dirichletův součin arit. funkcí $f \circ g$ (není to skládání) (tvoří komutativní pologrupu)

$$(f \circ g)(n) = \sum_{d \mid n} f(d) \cdot g\left(\frac{n}{d}\right)$$

je komutativní a asociativní

$$\mathbb{I}(n) = \begin{cases} 1 & n = 1 \\ 0 & n = 0 \end{cases}$$ neutrální prvek je $\mathbb{I}$

$\mathbb{I}(n) = 1$

$$(f \circ \mathbb{I})(n) = \sum_{d \mid n} f(n)$$

$\mu \circ \mathbb{I} = \mathbb{II}$

- Möbiova inverzní formule: $F(n) = \sum_{d \mid n} f(d)$

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot F(d)$$

dk. $F \circ \mu = (f \circ \mathbb{I}) \circ \mu = f \circ \mathbb{II} = f$

- multiplikativní arit. funkce.

$(a,b)=1 \Rightarrow f(ab)=f(a)\cdot f(b)$

- např.: I, II, μ

- dirichletův součin 2 multiplikativních funkcí je multiplikativní

- Eulerova funkce

- Lemma $\sum_{d|n} \varphi(d)=n$

pozn. $F=\varphi \circ I$ #, kdy $F(n)=n$

dle Möb. inv. $\varphi = F\circ\mu$, kdy φ je multiplikativní

kdy $\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\cdot d = n - \frac{n}{p_1}-\frac{n}{p_2}-\dots+\frac{n}{p_1p_2}+\frac{n}{p_1p_3}+\dots$

$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

Q

$\varphi(n)$ počet prvků grupy $\mathbb{Z}_n^\times=\{[a]_n, a\in\mathbb{Z}, (a,n)=1\}$

RSZ - rozš. soustava zbytků

- Eulerova věta
- Malá Fermatova věta
- Tvrzení 3.1. $p\equiv 3 \pmod 4$

$p\mid a^2+b^2 \Rightarrow p\mid a \wedge p\mid b$

- věta 17
- ## - Wilsonova věta

4. CV.

* pro $a,b\in\mathbb{Z}$: $a^2+b^2\equiv 0 \pmod 7 \Rightarrow a\equiv b \pmod 7$ $a\equiv b\equiv 0 \pmod 7$

$a^2, b^2 \in \{1,2,4\}$ □

* pro mod 5 to neplatí

* $p\equiv 3 \pmod 4 \Rightarrow p\mid a^2+b^2 \Rightarrow p\mid a \wedge p\mid b$

$a^2 \equiv -b^2 \pmod p$ lze psát $a+a\,1\,p+b$

$(a^3)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \pmod p$

$1 \equiv -1 \pmod p$ spor

* pro $a,b,c \in \mathbb{Z}$: $a^3+b^3+c^3 \equiv 0 \pmod 9 \Rightarrow a \equiv b \equiv c \pmod 3$ nebo $\equiv 0 \pmod 3$

$1^3 \equiv 1 \pmod 9$
$2^3 \equiv -1 \pmod 9$
$3^3 \equiv 0 \pmod 9$
$4^3 \equiv 1 \pmod 9$
$5^3 \equiv -1 \pmod 9$
$6^3 \equiv 0 \pmod 9$ obměnou
$7^3 \equiv 1 \pmod 9$
$8^3 \equiv -1 \pmod 9$ □
$0^3 \equiv 0 \pmod 9$

lze zobecnit na liché čísla

platí to i pro 5, 7 čísel

pozn: lze zavřít $a \equiv b \pmod{m^n} \Rightarrow a^m \equiv b^m \pmod{m^{n+1}}$

* Nalezněte všechna $n \in \mathbb{N}$: $3 \mid n \cdot 2^n + 1$

$n \cdot 2^n + 1 \equiv n \cdot (-1)^n + 1 \pmod 3$

$n \equiv 0 \pmod 6$: ✗
$n \equiv 1 \pmod 6$: ✓
$n \equiv 2 \pmod 6$: ✓
$n \equiv 3 \pmod 6$: ✗
$n \equiv 4 \pmod 6$: ✗
$n \equiv 5 \pmod 6$: ✗ □

* $\varphi(1000) = \varphi(2^3) \cdot \varphi(5^3) = 2^2 \cdot 5^2 \cdot 4 = 400$

$1000 - 500 - 200 + 100$ PIE

$\varphi(1001) = \varphi(7) \cdot \varphi(11) \cdot \varphi(13) = 6 \cdot 10 \cdot 12 = 720$

* pro $n \in \mathbb{N}$: $\varphi(5n) = 5\varphi(n)$ ∨ $\varphi(5n) = 4\varphi(n)$

$5 \mid n$ $5 \nmid n$

$n = 5^k \cdot m$

$\varphi(5^{k+1}) \cdot \varphi(m) = 5\varphi(5^k) \cdot \varphi(m)$ □

* $\varphi(3^x \cdot 5^y) = 600$, kde $x, y \in \mathbb{N}_0$

$2 \cdot 3^{x-1} \cdot 4 \cdot 5^{y-1} = 600$ pro $x, y > 0$

$3^{x-1} \cdot 5^{y-1} = 75 = 3 \cdot 5^2$

$(x, y) = (2, 3)$

$x = 0$: $\varphi(5^y) = 4 \cdot 5^{y-1}$ ... spor s dělitelností ($y \neq 0$)

$y = 0$: $\varphi(3^x) = 2 \cdot 3^{x-1}$ ... spor s dělitelností ($x \neq 0$)

$x = 0, y = 0$: spor

* $\varphi(n) = \frac{n}{3}$ $n \in \mathbb{N}$

$3\varphi(n) = n$

$n = 3^c k$

$2\varphi(k) = k$

$k = 2^d \ell$

$2 \cdot \varphi(\ell) = \ell$

$\varphi(\ell) = \frac{\ell}{2}$ $\ell = 1$

$n = 2^d \cdot 3^c$ $c, d \in \mathbb{N}$

* najděte $n \in \mathbb{N}$: $24 \mid \varphi(n)$

$\varphi(n) = \prod_{i=1}^{n} p_i^{\alpha_i - 1}(p_i - 1)$

z toho plyne $n \in \{1, 2, 3\}$

5. PŘ.

- věta 18: řešení kongruence
- Lemma: Buď $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$, je-li a různé od b různé $\pmod m$ ...
- řešení kongruencí o jedné neznámé
- Def.: Buď $m \in \mathbb{N}$, $f(x), g(x) \in \mathbb{Z}[x]$

  Zápis $f(x) \equiv g(x) \pmod m$ nazýváme polynomiální kongruencí o jedné neznámé
- kongruence nazveme ekvivalentními, mají-li stejnou množinu řešení
- Def.: počet řešení kongruence mod m je počet vzájemně různých čísel mod m obsahujících řešení
- lin. kong.: $ax \equiv 1$, $ax + b \equiv 0$ (rozšíření)

  $ax \equiv b \pmod m$.
- řešení pomocí Eukleidovy věty nebo Eukleida a Bezoutův nebo ekvivalentními úpravami
- Wilsonova věta

5. CV.

D

* $\varphi(n) = 14 = 2 \cdot 7 = \prod p_i^{\alpha_i - 1}(p_i - 1)$

~~$p_i = 7$~~ $3 \mid n$ $p_i - 1 = 14$ $p_i - 1 = 7$

~~$p_i - 1 = 6$~~ spor, když $n \in \emptyset$ $p_i = 15$ spor $p_i = 15$ spor

$\forall p_i : p_i \mid n \Rightarrow p_i - 1 \mid \varphi(n)$

$\forall p_i : p_i^{\alpha_i} \mid n \Rightarrow p_i^{\alpha_i - 1} \mid \varphi(n)$

alternativně $p_i - 1 \in \{1, 2, 7, 14\}$

$p_i \in \{2, 3, 8, 15\}$

$n = 2^\alpha \cdot 3^\beta$ $\alpha - 1 \leq 1, \beta - 1 \leq 0$ $\alpha \in \{0, 1, 2\}$, $\beta \in \{0, 1\}$

* $\varphi(n) = 30 = 2 \cdot 3 \cdot 5$

$p_i - 1 \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

$p_i \in \{2, 3, 7, 11, 31\}$

$n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 7^{\alpha_3} \cdot 11^{\alpha_4} \cdot 31^{\alpha_5}$

$\alpha_1 \in \{0, 1, 2\}$

$\alpha_2 \in \{0, 1, 2\}$

$\alpha_3, \alpha_4, \alpha_5 \in \{0, 1\}$

$5 \mid n$: $\alpha_5 = 1 \vee \alpha_4 = 1$

$\alpha_5 = 1$: ~~$n = 31$~~ $\varphi(n) = 30$ $\varphi(n_1) = 30$ $n_1 \in \{1, 2\}$ $n \in \{31, 62\}$

$\alpha_4 = 1$: $n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 11$

$\varphi(n) = 10 \cdot \varphi(n_2) = 30$

$\varphi(n_2) = 3$, což nelze (protože je n_2 liché)

* $\varphi(n) = 34 = 2 \cdot 17$

$p_i - 1 \in \{1, 2, 17, 34\}$

$p_i \in \{2, 3, 18\}$

$n = 2^\alpha \cdot 3^\beta$

$\alpha \in \{0, 1, 2\}$

$\beta \in \{0, 1\}$ 17 Asi nejde dostat $n \in \emptyset$

* určete n: $9 \mid \varphi(n)$ a $n \leq 100$

(i) $9 \mid p_i^{\alpha_i - 1}$ $p_i = 3$, $\alpha_i \geq 3$

(ii) $3 = p_i^{\alpha_i - 1} \wedge 3 \mid p_j - 1$

(iii) $9 \mid p_i - 1$

(iv) $3 \mid p_i - 1 \wedge 3 \mid p_j - 1$

ad (i): $n \in \{27, 54, 81\}$

ad (ii): $n = 9 \cdot m$ $n \in \{63\}$
$m = 7$

ad (iii): $n_i \in \{14, 37, 73, \dots\}$ $n_i \equiv 1 \pmod 9$
$n \in \{14, 37, 38, 57, 73, 76, \dots, 74\}$

ad (iv): $n_i \equiv 1 \pmod 3$
$n_j \equiv 1 \pmod 3$
$n_i, n_j \in \{7, 13, \dots\}$ další jsou moc velký
$n = 7 \cdot 13 = 91$

Závěr: $n \in \{14, 27, 37, 38, 54, 57, 73, 74, 76, 81, 91, 95\}$

*
$2^{181} + 3^{181} + 5^{181} \equiv x \pmod{37}$

$2^{181} \equiv 2 \pmod{37}$
$3^{181} \equiv 3 \pmod{37}$
$5^{181} \equiv 5 \pmod{37}$
$x \equiv 10 \pmod{37}$

* $\frac{73-1}{37-1} = 2$

* $7^{6^{5^{4^3}}} \equiv 7^{\varphi(10)} \equiv 1 \pmod{10}$

$6^{5^{4^3}} \equiv 0 \pmod{4}$

$5^{4^3} \equiv 1 \pmod{2}$

*
$12^{13^{14}} \equiv 2^{13^{14}} \equiv 2 \pmod{10}$

$2^{13^{14}} \equiv 0 \pmod{2}$
$2^{13^{14}} \equiv 2 \pmod{5}$
$13^{14} \equiv 1 \pmod{4}$
$14 \equiv 0 \pmod{2}$

$2^{13^{14}} = 2^{5k+2} = 2^{10l+2}$
$5k + 2 \equiv 0 \pmod 2$
$k \equiv 0 \pmod 2$

* $3^{5^{7^9}} \equiv 3 \pmod{10}$
$5^{7^9} \equiv 1 \pmod 4$

6.CV.

* $14x \equiv 23 \pmod{31}$
a) $28x \equiv 15 \pmod{31}$
$-3x \equiv 15 \pmod{31}$
$-x \equiv 5 \pmod{31}$
$x \equiv 26 \pmod{31}$

zkouška, úprava

$14x \equiv 23 \pmod{31}$
$14x \equiv -8 \pmod{31}$
$7x \equiv -4 \pmod{31}$
$7x \equiv -35 \pmod{31}$
$x \equiv 26 \pmod{31}$

7 b) eukleid. algoritmus

$d = (14, 31) = 1$

$31 = 2 \cdot 14 + 3$

$14 = 4 \cdot 3 + 2$

$3 = 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 2 = 3 - (14 - 4 \cdot 3) = 5 \cdot 3 - 14 = 5(31 - 2 \cdot 14) - 14 = 5 \cdot 31 - 11 \cdot 14$

$5 \cdot 31 - 11 \cdot 14 = 1$

$14^{-1} \equiv -11 \pmod{31}$

$x \equiv 23 \cdot (-11) \equiv -253 \equiv -5 \equiv 26 \pmod{31}$

c) Eulerova věta

$x \equiv 23 \cdot 14^{29} \equiv 23 \cdot 10^{14} \equiv 13 \cdot 7^7 \equiv 13 \cdot (-12) \cdot (-12)^3 \equiv$

$\equiv 13^3 \equiv 13 \cdot 14 \equiv 13 \cdot 10$

$x \equiv 23 \cdot 14^{29} \equiv 23 \cdot 2^{29} \cdot 7^{29} \equiv -2^{32} \cdot 7^{29} \equiv -2^2 \cdot 7^{29} \equiv -2^2 \cdot (7^3)^9 \cdot 7^2 \equiv -2^{11} \cdot 7^2 \equiv -2 \cdot 49 \equiv$

$\equiv -5 \equiv 26 \pmod{31}$

*

$673x \equiv 542 \pmod{347}$

a) $-21x \equiv 195^{203} \pmod{347}$ $\varphi(7) = 2(7)$ odečteme

$-10x \equiv 195 \cdot 12 \pmod{347}$

$10x$

$x \equiv 39 \cdot 6 \pmod{347}$

$x \equiv 39 \cdot 6 \equiv -234 \pmod{347}$

$x \equiv 113 \pmod{347}$

$-7x \equiv 69 \pmod{347}$ $347 \cdot 3$

$\varphi(7) = 2(7)$ $\varphi(7) = 4(7)$

$-7x \equiv 1106 \pmod{347}$

$-x \equiv 158 \pmod{347}$

$x \equiv -158 \pmod{347}$

b) $673 = 347 \cdot 1 + 326$

$347 = 326 \cdot 1 + 21$

$326 = 21 \cdot 15 + 11$

$21 = 11 \cdot 1 + 10$

$11 = 10 \cdot 1 + 1$

$1 = 11 - 10 = 2 \cdot 11 - 21 = 2 \cdot 326 - 31 \cdot 21 = \dots =$

$= 33 \cdot 673 - 64 \cdot 347$

$33 \cdot 673 \equiv 1 \pmod{347}$

$x \equiv 33 \cdot 542 \equiv -158 \pmod{347}$

*

a) $3446x \equiv 8642 \pmod{208}$

$118x \equiv 114 \pmod{208}$

$59x \equiv 57 \pmod{104}$ $x \equiv -29 \pmod{104}$

2 řešení

$14x \equiv 57 \cdot 2 \equiv 6 \pmod{104}$

$7x \equiv 3 \pmod{52}$

$7x \equiv 3 + 3 \cdot 52 \equiv 161 \pmod{52}$

$x \equiv 23 \pmod{52}$

b) CRT $208 = 16 \cdot 13$

$118x \equiv 114 \pmod{13} \iff x \equiv -3 \pmod{13}$
$118x \equiv 114 \pmod{16} \iff x \equiv 3 \pmod{8}$
$\Big\} \; x \equiv 75 \pmod{208}$

* $11 \mid 5^n - 4^n - 3^n$ nalezněte n.

n	1	2	3	4	5	6	7	8	9	10
5^n	5	3	4	9	1	5	3	4	9	1
4^n	4	5	9	3	1	4	5	9	3	1
3^n	3	9	5	4	1	3	9	5	4	1
$5^n - 4^n - 3^n$	-2	0	1	2	-1	...				

$n \equiv 2 \pmod 5$

* Nalezněte $n \in \mathbb{N}$: $7 \mid 2^{2^n} - 2^{n^2}$

$2^{2^n} \equiv 2^{n^2} \pmod 7$

$\operatorname{ord}_7(2) = 3$

1) $2^n \equiv n^2 \pmod 3$
$(-1)^n \equiv n^2 \pmod 3$

$n \equiv 0 \; (6)$: X
$n \equiv 1 \; (6)$: X
$n \equiv 2 \; (6)$: ✓
$n \equiv 3 \; (6)$: X
$n \equiv 4 \; (6)$: ✓
$n \equiv 5 \; (6)$: X

$n \equiv 2 \; (6) \vee n \equiv 4 \; (6)$

6. PŘ.

- CRT, součiny, Vandermondova matice

7. CV

* Nalezněte $n \in \mathbb{N}$: $43 \mid 2^{2^n} - 2^{n^2}$

$42 = 2 \cdot 3 \cdot 7$

$2^{2^n} \equiv 2^{n^2} \pmod{43}$

$2^n \equiv n^2 \pmod{14}$

$2^2 \equiv 4 \pmod{43}$
$2^3 \equiv 8 \pmod{43}$
$2^6 \equiv 21 \pmod{43}$
$2^7 \equiv -1 \pmod{43}$
$2^{14} \equiv 1 \pmod{43}$
$\operatorname{ord}_{43}(2) = 14$

$2^n \equiv n^2 \pmod{2}$

$n \equiv 0 \pmod{2}$

~~$2^n \equiv n^2 \pmod{7}$~~ ~~$n = 2k,\ k \in \mathbb{Z}$~~

n	1	2	3	4	5	6
2^n	2	4	1	2	4	1
n^2	1	4	2	2	4	1

~~$n \equiv 2, 4, 5 \pmod{7}$~~

$2^n \equiv n^2 \pmod{7}$

n	1	2	3	4	5	6	7
n^2 (7)	1	4	2	2	4	1	0

1) $n \equiv 0 \pmod{3}$

$1 \equiv n^2 \pmod{7}$

$n \equiv \pm 1 \pmod{7}$

} $n \equiv 6 \pmod{21}$, $n \equiv 15 \pmod{21}$

2) $n \equiv 1 \pmod{3}$

$2 \equiv n^2 \pmod{7}$

$n \equiv \pm 3 \pmod{7}$

} $n \equiv 4 \pmod{21}$, $n \equiv 10 \pmod{21}$

3) $n \equiv 2 \pmod{3}$

$4 \equiv n^2 \pmod{7}$

$n \equiv \pm 2 \pmod{7}$

} $n \equiv 2 \pmod{21}$, $n \equiv 5 \pmod{21}$

~~$n \equiv 2, 4, 6, 26, 36$~~

$\boxed{n \equiv 2, 4, 6, 10, 26, 36 \pmod{42}}$

* Piráti uloupili n zlaťáků, 13 pirátů, piráti rozdělí zlaťáky na 13 hromádek a zbylo jim 10 zlaťáků, jednoho zabili...

$n \equiv 10 \pmod{13} \Rightarrow$ 12 pirátů

$n \equiv 3 \pmod{12} \Rightarrow$ 11 pirátů

$n \equiv 0 \pmod{11}$

$n = 13a + 10 = 156b + 75 = 1716c + 231$

$a + 10 \equiv 3 \pmod{12}$

$a \equiv 5 \pmod{12}$

$a = 12b + 5$

~~$b + 5 \equiv 0 \pmod{11}$~~

$2b + 75 \equiv 5 \pmod{11}$

$b \equiv 1 \pmod{11}$ $\qquad b = 11c + 1$

$n \equiv 231 \pmod{1716}$

$$\begin{array}{r} 156 \\ \times 11 \\ \hline 312 \\ 156 \\ \hline 1872 \end{array}$$

* $x \equiv 7 \pmod{33}$
$x \equiv 3 \pmod{63}$

$x \equiv 1 \equiv 0 \pmod{3}$, spor

□

* $17x \equiv 5 \pmod{6}$
$11x \equiv 35 \pmod{36}$

$x \equiv 1 \pmod{6}$
$-3x \equiv -3 \pmod{36}$
$x \equiv 13 \pmod{36}$

$x \equiv 13 \pmod{36}$

$x \equiv 1 \pmod{4}$
$x \equiv 4 \pmod{9}$

$x = 9a + 1 = 36b + 1$
$9a + 1 \equiv 1 \pmod{4}$
$a \equiv 4b$

* $a \in \mathbb{Z}$ libovolné

$2 \mid a$ $a = 2b$ $2 \mid b$ $a = 4c$

$2x \equiv a \pmod{4}$
$3x \equiv 4 \pmod{10}$

$x \equiv b \pmod{2}$
$3x \equiv 24 \pmod{10}$
$x \equiv 8 \pmod{10}$

$x \equiv b \equiv 0 \pmod{2}$
$x \equiv 3 \pmod{5}$

$x \equiv 8 \pmod{10}$, pokud $4 \mid a$
pokud $4 \nmid a$, pak $x \in \emptyset$

* $a \in \mathbb{Z}$ libovolné

$a = 2b$

$2x \equiv a \pmod{4}$
$3x \equiv 4 \pmod{7}$

$x \equiv b \pmod{2}$
$3x \equiv 6 \pmod{7}$

$x = 7b + 6 = 14k + \frac{7a}{2} + 6$
$b \equiv b \pmod{2}$
$b = 2k + b$

$x \equiv \frac{7a}{2} + 6 \pmod{14}$ pro $2 \mid a$
$x \in \emptyset$ pro $2 \nmid a$

* Máme spravit vojáky

Čtverec 5×5, zbyde 9
Čtverec 7×7, zbyde 45
Čtverec 12×12, zbyde 9
Kolik je vojáků

$x \equiv 9 \pmod{25}$
$x \equiv 45 \pmod{49}$
$x \equiv 9 \pmod{144}$

$x = 144a + 9$
$144a + 9 \equiv 45 \pmod{49}$
$3a + 9 \equiv$

$x \equiv 9 \pmod{25 \cdot 144}$
$x = 25 \cdot 144a + 9$
$-3 \cdot 25a \equiv 36 \pmod{49}$
$25a \equiv -12 \pmod{49}$
$a \equiv 25 \pmod{49}$

$x = 25 \cdot 144 (49k + 25) + 9 = \dots = 176400k + 90009$

* dokažte $2^{2^{6n+2}} + 13$ je složené pro $\forall n \in \mathbb{N}$.

$n = 0: \quad 2^4 + 13 = 29$

$2^{2^{6n+2}} \equiv 16 \pmod{29}$

$2^{2^{6n+2}} \equiv 2^4 \pmod{29}$

$2^{6n+2} \equiv 4 \pmod{28}$ (mod)

$2^{6n+2} \equiv 2^2 \pmod{28}$

$2^{6n} \equiv 1 \pmod{7}$

$6n \equiv 3 \pmod{3}$

$0 \equiv 0 \pmod{3}$, sedí

$29 \mid 2^{2^{6n+2}} + 13$

1, 2, 4, 7, 14, 28

n	1	2	4	7	14	28
$2^n \pmod{29}$	1	2	16	12	-1	1

$\varphi(28) = 6 \cdot 2 = 12$

7. PŘ.

- kongruence s neznámým modulem
- sad po soustavy lin. rovnic
- binomické kongruence $x^n \equiv a \pmod{m}$

n - tý mocninný zbytek (musí být nesoudělný s modulem)

řády mod. zbytek je 1 (mod p).

zbytek 3, 5, 7 (mod 8)

*

- prvočíselní kořen, diskrétní logaritmus (DLP)

8. PŘ.

- věty 26, 27, 29

9. PŘ.

- Rubin's conjecture
- hledání prim. kořenů
- kvadratické kongruence
- Legendrův symbol $\left(\frac{a}{p}\right)$ (a relativně k p)

8. CV.

chybět jsem

9. CV.

test

10. CV.

* určete všechny prim. kořeny mod 11.

$2^2 \equiv 4 \ (11)$

$2^5 \equiv -1 \ (11)$

Tedy 2 je prim. kořen.

všechny prim. kořeny jsou $2, 2^3, 2^7, 2^9$.

$2^3 \equiv 8 \ (11)$

$2^7 \equiv 7 \ (11)$

$2^9 \equiv 6 \ (11)$

* najděte všechny prim. kořeny $23; 23^2; 2 \cdot 23^2$

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

m	2	4	8	11
$2^m \ (23)$	4	-7	3	1
$3^m \ (23)$	9	-11	6	1
$5^m \ (23)$	2	4	16	22

Z toho je vidět, že 5 je prim. kořen!

$5; 5^3; 5^5; 5^7; 5^9; 5^{13}; 5^{15}; 5^{17}; 5^{19}; 5^{21}$ jsou prim. kořeny

$5^{22} \equiv (5^2)^{11} \equiv (23+2)^{11} \equiv 2^{11} + 11 \cdot 2^{10} \cdot 23 \equiv$

$\equiv 2048 + 11 \cdot 1024 \cdot 23 \equiv -68 + 11 \cdot (-34) \cdot 23 \equiv -68 - 6 \cdot 23 \not\equiv$

5 je prim kořen mod. $23^2; 2 \cdot 23^2$

* řešte $x^3 \equiv 1 \ (23)$

$d = (3, \varphi(23)) = 1$, má to 1 řešení $x \equiv 1 \ (23)$

* řešte $x^3 \equiv 5 \ (23)$

$d = (3, \varphi(23)) = 1 \quad 5^{\frac{\varphi(23)}{d}} \equiv 1 \ (23)$

5 je prim. kořen, $x = 5^y$

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

$3y \equiv 1 \ (22)$

$y \equiv -7 \ (22)$

$y \equiv 15 \ (22)$ ##

$x \equiv 5^{15} \equiv \dots \equiv 2^7 \cdot 5 \equiv 13 \cdot 5 \equiv 19 \ (23)$

* řešte $x^8 \equiv 8 \ (23)$

$d = (8, \varphi(23)) = 2$ 2 řešení $\quad 8^{\frac{\varphi(23)}{2}} \equiv 8^{11} \equiv 2^{33} \equiv 2^{11} \equiv 1 \ (23)$

$x \equiv 5^y \qquad 8 \equiv 5^6 \ (23)$

$5^{8y} \equiv 5^6 \ (23)$

$8y \equiv 6 \ (22)$

$4y \equiv 3 \ (11)$

$4y \equiv 36 \ (11)$

$y \equiv 9 \ (11)$

$x \equiv 5^9 \equiv 16 \cdot 5 \equiv 11 \ (23)$

$x \equiv 5^{20} \equiv -11 \equiv 12 \ (23)$

* $x^8 \equiv 5 \ (23)$ nemá řešení

* řešte $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \ (29)$

$x \not\equiv 1 \ (29)$

$x^7 \equiv 1 \ (29)$ $\qquad \varphi(29) = 4 \cdot 7$

$d = (7, 28) = 7 \qquad 1^{\frac{28}{7}} \equiv 1 \ (29)$ $\qquad 4, 14$

má 7 řešení

k	2	4	10	14
$2^k \ (29)$	4	16	9	-1

2 je prim. kořen

$x = 2^y \qquad 1 = 2^0$

$7y \equiv 0 \ (28)$

$x \equiv 0, 7, 14, 21 \ (28)$

$x \equiv 7, 14, 21 \ (29)$

$y \equiv 0 \ (4)$

$x = 2^{4k} = 16^k$ 6 řešení

$k \in \{1, 2, 3, 4, 5, 6\}$

* určete počet řešení $5x^{30} \equiv 37 \ (41^2)$

$5x^{30} \equiv 37 \ (41)$

$x^{30} \equiv 32 \ (41)$ $\qquad d = (30, 40) = 10 = 2 \cdot 5$ $\qquad 32^{\frac{40}{10}} \equiv 1 \ (41)$

→ 10 řešení, z Henselova lemmatu má x původní rovnice 10 řešení

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

10. PŘ.

– zákon kvadratické reciprocity $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ $p \neq q$ $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right)$

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

F1:IV119 – seminář z diskrétních matematických metod goo.gl/QLVArS

– prvočísel $4k+1$ je ∞

$S = \left\{-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}\right\}$

$\mu_p(a)$ ... počet záporných nejmenších zbytků v abs. hodnotě (tedy prvků S) čísel

$1\cdot a, 2\cdot a, \dots, \frac{p-1}{2}\cdot a$

– Gaussovo lemma $\left(\frac{a}{p}\right) = (-1)^{\mu_p(a)}$

11. CV.

* $x^7 \equiv 12 \ (29^2)$

$x^7 \equiv 12 \ (29)$

$d = (7, \varphi(29)) = 7$ $12^4 \equiv 1 \ (29)$

7 řešení mod 29

$f(x) = x^7 - 12$

$f'(x) = 7x^6 \not\equiv 0 \ (29)$

Dle Henselova lemmatu máme 7 řešení mod 29^2

* $6x^2+5x+1 \equiv 0 \ (13)$

$(3x+1)(2x+1) \equiv 0 \ (13)$

$2x \equiv -1 \ (13)$
$x \equiv 6 \ (13)$

$3x \equiv -1 \ (13)$
$x \equiv 4 \ (13)$

2. způsob

$6^{-1} \equiv 11 \equiv -2 \ (13)$

$x^2 - 10x - 2 \equiv 0 \ (13)$

$x^2 + 3x - 2 \equiv 0 \ (13)$

$x^2 - 10x - 2 \equiv 0 \ (13)$

$(x-5)^2 - 1 \equiv 0 \ (13)$

$(x-5)^2 \equiv 1 \ (13)$

$x-5 \equiv 1 \ (13)$
$x \equiv 6 \ (13)$

$x-5 \equiv -1 \ (13)$
$x \equiv 4 \ (13)$

* $6x^2+5x+1 \equiv 0 \ (m)$

Dokažte, že je řešitelná pro libovolné m

pozn. rovnost $6x^2+5x+1 = 0$ nemá řešení v $\mathbb{Z}$

$(3x+1)(2x+1) \equiv 0 \ (2^k \cdot l)$

$2 \nmid l$ $k \in \mathbb{N}_0$

$3x+1 \equiv 0 \ (2^k) \wedge (2x+1 \equiv 0 \ (l))$

$3x \equiv -1 \pmod{2^k}$

$d = (3, 2^k) = 1$, je lichý přirozená

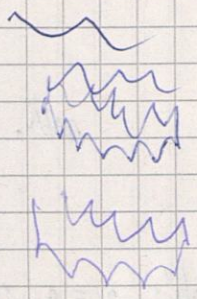
$2x \equiv -1 \pmod{l}$

$d = (2, l) = 1$, je lichý přirozená

Z těchto dvou faktů a ČRT plyne úloha.

* Vypočtěte $\left(\frac{5}{17}\right)$ pomocí Gaussova lemmatu

$S = \{-8, -7, -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6, 7, 8\}$



$5 \cdot 1 \equiv 5$

$5 \cdot 2 \equiv -7$

$5 \cdot 3 \equiv -2$

$5 \cdot 4 \equiv 3$

$5 \cdot 5 \equiv 8$

$5 \cdot 6 \equiv -4$

$5 \cdot 7 \equiv 1$

$5 \cdot 8 \equiv 6$

$\left(\frac{5}{17}\right) = (-1)^3 = -1$

* Vypočtěte pomocí Gaussova lemmatu $\left(\frac{-1}{n}\right)$

$(-1) \cdot 1 < 0$

$(-1) \cdot 2 < 0$

$\vdots$

$(-1) \cdot \frac{n-1}{2} < 0$

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

* Určete počet řešení kongruence

$x^2 \equiv 433 \pmod{503}$, 503 je prvočíslo

Obecně, zda je 433 prvočíslo.

$2 \nmid 433 \quad 3 \nmid 433 \quad 5 \nmid 433 \quad 7 \nmid 433 \quad 11 \nmid 433 \quad 13 \nmid 433 \quad 17 \nmid 433 \quad 19 \nmid 433$

Tedy 433 je prvočíslo

$$\left(\frac{433}{503}\right) = \left(\frac{503}{433}\right) = \left(\frac{70}{433}\right) = \underbrace{\left(\frac{2}{433}\right)}_{433 \equiv 1 \pmod 8} \cdot \left(\frac{5}{433}\right) \cdot \left(\frac{7}{433}\right) = \left(\frac{5}{433}\right) \cdot \left(\frac{7}{433}\right) = \left(\frac{433}{5}\right) \cdot \left(\frac{433}{7}\right) =$$

$$= \left(\frac{3}{5}\right) \cdot \left(\frac{-1}{7}\right) = (-1) \cdot (-1)^3 = 1$$

Tedy kongruence je řešitelná a má právě 2 řešení

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

- Jacobiho symbol $\left(\frac{a}{b}\right)$ $a \in \mathbb{Z}, b \in \mathbb{N}, 2 \nmid b$

$b = \underbrace{q_1 \cdot q_2 \cdots q_e}_{\text{mohou se opakovat}} \quad (q_i \neq 2)$

$\left(\frac{a}{b}\right) = \left(\frac{a}{q_1}\right) \cdot \left(\frac{a}{q_2}\right) \cdots \left(\frac{a}{q_e}\right)$

- platí $x^2 \equiv a \pmod b$ je řešitelná $\Rightarrow \left(\frac{a}{b}\right) = 1$

neplatí ekvivalence

např. $x^2 \equiv 2 \ (15) \iff x^2 \equiv 2 \ (3) \wedge x^2 \equiv 2 \ (5)$

$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$

- platí: $a_1 \equiv a_2 \ (b) \Rightarrow \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$

$\left(\frac{a_1 \cdot a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right)$

$\left(\frac{a}{b_1 \cdot b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right)$

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

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

a, b liché, > 0: $\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}} \cdot \left(\frac{b}{a}\right)$

* určete počet řešení $x^2 \equiv 3766 \ (5987)$ 5987 je prvočíslo

$\left(\frac{3766}{5987}\right) = \left(\frac{2}{5987}\right) \cdot \left(\frac{1883}{5987}\right) = (-1) \cdot \left(\frac{1883}{5987}\right) = \left(\frac{5987}{1883}\right) = \left(\frac{338}{1883}\right) =$

$5987 \equiv 3 \pmod 8$
$1883 \equiv 3 \pmod 8$

$= \left(\frac{2}{1883}\right) \cdot \left(\frac{169}{1883}\right) = (-1) \cdot \left(\frac{169}{1883}\right) = (-1) \cdot \left(\frac{1883}{169}\right) = (-1) \cdot \left(\frac{74}{169}\right) =$

$= (-1) \cdot \left(\frac{13}{1883}\right)^2 = -1$

tedy

nemá řešení

* určete počet řešení kongruence $x^2 \equiv 280 \ (459)$

$459 = 3^3 \cdot 17$

$x^2 \equiv 280 \ (459) \iff \begin{matrix} x^2 \equiv 280 \ (27) \\ x^2 \equiv 280 \ (17) \end{matrix}$

$\left(\frac{280}{27}\right) = \left(\frac{10}{27}\right) = \left(\frac{2}{27}\right)\cdot\left(\frac{5}{27}\right) = (-1)\cdot(-1) = 1$

$27 \equiv 3 \pmod 8$

$\left(\frac{280}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{2}{17}\right)^3 = 1$ 2 řešení

$x^2 \equiv 280 \pmod 3$

$x^2 \equiv 1 \pmod 3$

$x \in \{0,1,2\} \pmod 3$

$x \equiv 1, 2 \pmod 3$

Sudy kongruence $x^2 \equiv 280 \pmod{27}$ má 2 řešení dle Henselova lemmatu

Soustava kongruence má $2 \cdot 2 = 4$ řešení

11. PŘ.

- diofantické rovnice
- lineární diofantická rovnice
- diofantické rovnice lineárním rozkladem na jednu neznámou

12. PŘ.

* Určete prvočísla p taková, že $\left(\frac{13}{p}\right) = 1$, 13 je kvadr. zbytek mod p.

pro $p = 2$ to je $p = 13$ to není

$p \neq 3$

$p \neq 2$: $\left(\frac{13}{p}\right) = (-1)^{\frac{p-1}{2}\cdot 6}\cdot\left(\frac{1}{13}\right) = \left(\frac{p}{13}\right) = 1$

p	± 1	± 2	± 3	± 4	± 5	± 6
$p^2 \pmod{13}$	1	4	9	3	−1	−3

$p = 2 \vee p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$

* -11- -3 je kvadr. zbytek mod p.

$p = 2$ to je $p = 3$ to není

$p \neq 3$: $\left(\frac{-3}{p}\right)$ $p \notin \{2,3\}$: $\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot(-2)}\cdot\left(\frac{p}{-3}\right) = \left(\frac{p}{-3}\right) = 1$

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

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

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

$p \equiv 1 \pmod 3$

$p = 2 \vee p \equiv 1 \pmod 3$

$p = 2 \vee p \equiv 1 \pmod 3$

$p = 2 \vee p \equiv 1 \pmod 3$

lze to taky rozdělit na dva případy $1 \cdot 1 = 1$ v $(-1)\cdot(-1) = 1$

* řešte $x^2 \equiv 7 \ (83)$

$$\left(\frac{7}{83}\right) = -\left(\frac{83}{7}\right) = -\left(\frac{-1}{7}\right) = (-1)\cdot(-1)^3 = 1$$

$p \equiv 3 \ (4)$

$$x \equiv \pm a^{\frac{p+1}{4}} \ (p)$$

$83 \equiv 3 \ (4)$

$$x \equiv \pm 7^{21} \equiv \pm 343^7 \equiv \pm 11^7 \equiv \pm 11 \cdot 38^3 \equiv \pm 11 \cdot 33 \cdot 38 \equiv \pm 3 \cdot 38 \equiv \pm 16 \ (83)$$

* dokažte, že prvočísel kořen modulo liché prvočíslo je nutně kvůli nezbytek modulo sudé prvočíslo

$x^2 \equiv a \ (p)$ — obměna — $a \equiv x^2 \ (p)$

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

tedy a není prim. kořen.

nebo takto $\left(\frac{a}{p}\right) = 1$, tedy $a^{\frac{p-1}{2}} \equiv 1 \ (p)$

* Řešte v $\mathbb{Z}$ $379x + 314y + 183y^2 = 210$

$$314y + 183y^2 \equiv 210 \ (\mathrm{mod}\ 379)$$

379 je prvočíslo

$$183y^2 + 314y - 210 \equiv 0 \ (\mathrm{mod}\ 379)$$

$$379 = 2 \cdot 183 + 13$$
$$183 = 14 \cdot 13 + 1$$

$$1 = 183 - 14 \cdot 13 = 183 - 14(379 - 2 \cdot 183) = 29 \cdot 183 - 14 \cdot 379$$

$$29 \cdot 183 \equiv 1 \ (\mathrm{mod}\ 379)$$

$$y^2 + 10y - 26 \equiv 0 \ (379)$$
$$(y+5)^2 \equiv 51 \ (379)$$
$$y + 5 = z$$
$$z^2 \equiv 51 \ (379)$$

$$\left(\frac{51}{379}\right) = \left(\frac{3}{379}\right)\cdot\left(\frac{17}{379}\right) = (-1)\cdot\left(\frac{379}{3}\right)\cdot 1\cdot\left(\frac{379}{17}\right) = -\left(\frac{1}{3}\right)\cdot\left(\frac{5}{17}\right) = (-1)\cdot 1\cdot(-1) = 1$$

$x \equiv \pm 51^{95} \pmod{379}$

$y = \pm 51^{95} - 5 + 379 k$

× dostaneme dosazením

12. PŘ.

- řešení diofantických rovnic – modulární přístup
  - řešení pomocí nerovností
  - metoda rozkladu
  - důkaz nemožnosti
- řešte v $\mathbb{Z}$ $6x^2 + 5y^2 = 74$
- řešte v $\mathbb{Z}$ $2^x = 1 + 3^y$

  nějaké řešíme v $\mathbb{N}_0$, pokud $y < 0 \Rightarrow 0 < 1 + 3^y < 1 \Rightarrow 0 < 2^x < 1$

  mod 8 dostaneme pro $x \geq 3$ spor.
- řešte v $\mathbb{Z}$ $\underbrace{x(x+1)(x+7)(x+8)} = y^2$

  $(x^2+8x)(x^2+8x+7) = y^2$

  $z(z+7) = y^2$

  $z^2 + 7z = y^2$

  je to ve skriptech

13. CV.

* Řešte diof. rovnici

$x^2 + 4y^2 + 6x + 7y + 8z = 1$

$x^2 + 4z^2 + 6x + 8z \equiv 1 \pmod 7$

$(x+3)^2 + 4(z+1)^2 \equiv 0 \pmod 7$

~~a dále podobně, protože~~ všechny druhých mocnin mod 7 jsou 0, 1, 2, 4

tedy $x+3 \equiv z+1 \equiv 0 \pmod 7$

$x \equiv 4 \pmod 7$

$z \equiv 6 \pmod 7$

$x = 7a + 4$

$z = 7b + 6$ $\quad a, b \in \mathbb{Z}$

a y dopočítáme

* Řešte v $\mathbb{Z}$ $5^x + 3^y = 8^n - 2$

$x < 0: \ 0 < 5^x < \frac{1}{2}$
$y < 0: \ 0 < 3^y < \frac{1}{2}$
$\Rightarrow x, y \in \mathbb{N}_0$

x	1	2
$5^x \ (8)$	5	1

y	1	2
$3^y \ (8)$	3	1

$5+3 \equiv 0 \pmod 8$
$5+1 \equiv 6 \pmod 8$
$3+1 \equiv 4 \pmod 8$
$1+1 \equiv 2 \pmod 8$

$x = 2n+1$
$y = 2m \qquad n, m \in \mathbb{N}_0$
$n = \frac{5^{2n+1} + 3^{2m} + 2}{8}$

* Řešte v $\mathbb{N}$ $6(x-y) = xy$

$6x > 6x - 6y = xy$
$6 > y$

dopočítáním získáme řešení (x,y) takováto $(3,2), (6,3), (12,4), (30,5)$

jde to i rozkladem $(6+x)(6-y) = 36$

* Řešte v $\mathbb{N}$

$\frac{1}{x} + \frac{1}{y} + \frac{1}{n} = 1$

BÚNO $x \le y \le n$
$\frac{1}{x} \ge \frac{1}{y} \ge \frac{1}{n}$

$\frac{3}{n} \le 1 \le \frac{3}{x}$
$x \le 3$

$x = 1$: $y = -n$, spor
$x = 2$: $\frac{1}{y} + \frac{1}{n} = \frac{1}{2}$

$\frac{1}{2} \le \frac{2}{y} \qquad y \le 4$

$y = 1$: spor
$y = 2$: ~~$n = 0$~~ spor
$y = 3$: $\frac{1}{n} = \frac{1}{2} - \frac{1}{3} = \frac{1}{6} \qquad n = 6$

$y = 4$: $\frac{1}{n} = \frac{1}{2} - \frac{1}{4} = \frac{1}{4}$
$n = 4$

$x=3$: $\frac{1}{y}+\frac{1}{z}=\frac{2}{3}$ $1-\frac{1}{3}=\frac{2}{3}$

$\frac{1}{2}\leq\frac{2}{3}\leq\frac{2}{y}$

$y\leq 3$

$y=1$: spor

$y=2$: $\frac{1}{z}=\frac{2}{3}-\frac{1}{2}=\frac{4-3}{6}=\frac{1}{6}$ $z=6$

$y=3$: $\frac{1}{z}=\frac{2}{3}-\frac{1}{3}=\frac{1}{3}$ $z=3$

Všechna řešení (x,y,z) jsou $(2,3,6),(2,4,4),(3,3,3)$ a všechny jejich permutace

* řešte v $\mathbb{N}$

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}=3$$

je to případ rovnosti v AG.

$x=y=z$

* řešte v $\mathbb{Z}$ $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$ kde n je nenulový parametr.

xyn

$xn+yn=xy$

$x(y-n)-yn=0$

$x(y-n)-n(y-n)=n^2$

$(x-n)(y-n)=n^2=1\cdot n^2=(-1)\cdot(-n^2)=n\cdot n=(-n)\cdot(-n)$

$x-n=1$, $y-n=n^2$ $\Leftrightarrow$ $x=n+1$, $y=n^2+n$

$x-n=-1$, $y-n=-n^2$ $\Leftrightarrow$ $x=n-1$, $y=-n^2+n$

$x-n=n$, $y-n=n$ $\Leftrightarrow$ $x=2n$, $y=2n$

$x-n=n$, $y-n=-n$ $\Leftrightarrow$ $x=0$, $y=0$ spor

Všechna řešení (x,y) jsou $(n+1,n^2+n),(n^2+n,n+1),(n-1,-n^2+n),(-n^2+n,n-1),(2n,2n)$

* Řešte v $\mathbb{N}$ $2x^2+5xy-12y^2=28$

$$2\cdot\left(\frac{x}{y}\right)^2+5\left(\frac{x}{y}\right)-12=\frac{28}{y^2}$$

$$\left(2\cdot\frac{x}{y}-3\right)\left(\frac{x}{y}+4\right)=\frac{28}{y^2}$$

~~$(2x-3y)(x+4y)=28$~~

$(2x-3y)(x+4y)=28=4\cdot7=2\cdot14=1\cdot28$

$x+4y\geq 5$

$(x,y)\in\{(8,5)\}$ jediné řešení

* Řešte v $\mathbb{Z}$

$$x_1^4+x_2^4+\cdots+x_{14}^4=1599$$

~~Čtverce mocniny mod 8 jsou 0,1 což je úplně mod 8~~

Čtverce mocniny mod 16 jsou 0,1, což je úplně mod 16.

* Řešte v $\mathbb{N}$

$$1!+2!+3!+\cdots+x!=y^2$$

~~$1!+2!+3!+4!+5!=9+24+120\equiv -1+1$~~

~~$x\geq 5: y^2\equiv 2$~~

$1!+2!+3!+4!+5!\equiv 3 \pmod 5$

Tedy $x\leq 4$, protože 3 není kvadr. zbytek mod 5.

Tedy jediné řešení je $(x,y)=$

Tedy $(x,y)=\{(1,1),(3,2)\}$