Kateřina Medková
katerina.medkova@gmail.com

Požadavky na zápočet

=> docházka - (max 3 absence)
- další - 2b.

=> vyřešení úlohy +2b.

=> zápočtový test + 10b.

na zápočet = 5b.

MASÁKOVÁ - ukázka testu na stránkách

Magická čísla

N
- pokud libovolné přirozené číslo, že v jeho desítkovém zápisu končí číslo n N, pak je magické
magická čísla: 1, 2, 10, 5.

$$M = \underline{P, N} = P \cdot 10^k + N$$

$N = n_i \dots n_k$

$N \mid P \cdot 10^k + N$

$\Rightarrow N \mid P \cdot 10^k \Rightarrow N \mid 10^k \Rightarrow N = 2^a \cdot 5^b, a, b \leq k$

N je magické $\Leftrightarrow N = 2^a \cdot 5^b, a, b \leq k$

① Najít lepší zápis

② Najděte všechna prvočísla $p \in \mathbb{P}$, že $2p^2 + 1 \in \mathbb{P}$
$\mathbb{P}$ - množina všech prvočísel

③ Dokažte, že pro žádné $n \in \mathbb{N}$ není $n^2 + n + 10$ dělitelné 169

④ Nechť $p, q \in \mathbb{P}$, že $p \mid q^3 - 1$ a $q \mid p - 1$, pak $p = 1 + q + q^2$

⑤ největší násobek 8, který nemá 2 stejné cifry a určí jeho zbytek po dělení 100

⑥ Jaké cifry je třeba přidat na místo a, b do 30a0b03, abychom dostali číslo dělitelné 13

Dělitelnost v $\mathbb{N}$;

$\mathbb{N} = \{0; 1; 2; 3 \dots\}$

$\mathbb{N}_0 = \{0; 1; 2 \dots\}$

pozorování: $a, b, c, d \in \mathbb{N}$

$a \mid b \Rightarrow a \leq b$

$a \mid b \wedge b \mid a \Rightarrow a = b$

$a \mid b \wedge b \mid c \Rightarrow a \mid c$

$a \mid b \wedge a \mid c \Rightarrow a \mid b \pm c$

$a \mid b \Rightarrow a \mid b \cdot c$

$a \mid c \wedge b \mid d \Rightarrow ab \mid cd$

Eukleidův algoritmus

$59 : 7 = 8$ zb. 3

(8 je vždy jednociferné)

↓

7
14
21
28
35
42
49
→ 56 : 7 = 8 zb. 59 − 56
63

Věta o zbytku

$\forall m; n \in \mathbb{N}$ existuje právě jedno $k \in \mathbb{N}$ a právě jedno $r \in \mathbb{N}_0$, takové že

$n = km + r$

Důkaz: $M = \{n - jm\}; j \in \mathbb{N}_0$, $n - km > 0$

$M = \{n; n-m; n-2m \dots\}$ $n - (k+1)m < 0$

$r = \min\{M \cap \mathbb{N}_0\}$ $r = n - km$

$r - (k-1)m < 0$

$r - km - m < 0$

$r - m < 0$

$r < m$

- dokázali jsme existenci

* Důkaz sporem

věta $*$: $A \Rightarrow B$

důkaz: $A \wedge \neg B \Rightarrow \dots \Rightarrow \dots$ SPOR

Důkaz jednoznačnosti

- důkaz sporem existují alespoň 2 k_1, r_1 $k_1 \neq k_2$ nebo $r_1 \neq r_2$
k_2, r_2

$r_1 = n - k_1 m$

$r_2 = n - k_2 m$

a) $r_1 = r_2 \Rightarrow k_1 = k_2$ - SPOR, mělo být různé

b) $r_1 \neq r_2$ $r_2 > r_1$ (bůno)

$r_2 - r_1 = (k_1 - k_2)m$

$r_1, r_2 \in \{0, \dots m-1\}$

$r_2 - r_1$ - není dělitelem m ⊥ SPOR
$\in \{1, \dots m-1\}$

$k_1 - k_2$ dělitelem

$\lfloor x \rfloor \in \mathbb{R}$
"nejmenší nebo nové přirozené číslo"
DOLNÍ CELÁ ČÁST $\mathbb{R}$

$\lceil x \rceil \in \mathbb{R}$
HORNÍ CELÁ ČÁST $\mathbb{R}$

Nechť $a, b \in \mathbb{N}_0$

$nsd(a,b)$ je $d \in \mathbb{N}$, že $d|a$, $d|b$ a přitom $\forall d' \in \mathbb{N}: d'|a \wedge d'|b \}$
platí $d'|d$
$d'|d \Rightarrow d' \leq d$

$nsd(18, 66) = 6$

$18 = 2 \cdot 3 \cdot 3$ $66 = 2 \cdot 3 \cdot 11$

E. alg.

~~$\forall a, b \in \mathbb{N}_0 \exists x_0, y_0 \in \mathbb{Z}$ tak, že $ax_0 + by_0 = nsd(a,b)$~~

V: $\forall a, b \in \mathbb{N} \exists x_0, y_0 \in \mathbb{Z}$ tak, že $ax_0 + by_0 = nsd(a,b)$

D $M = \{ax + by \mid x, y \in \mathbb{Z}\}$

uzavřená na násobení $z \in M \Rightarrow kz \in M$ $\forall k \in \mathbb{Z}$
uzavřená na sčítání $z, w \in M$ $z = ax_1 + by_1$
$w = ax_2 + by_2$
$z + w = a(x_1 + x_2) + b(y_1 + y_2)$
Mobsahuje a, b

$n = \min \{z \in M \mid z > 0\}$
$n = nsd(a,b)$

① $n = ax_0 + by_0$
$nsd(a,b) | n$

② $n | nsd(a,b)$
$\Rightarrow \boxed{n|a}$ - sporem
$n|b$
když $a = kn + r \neq 0$
$a < kn$
$r = a - kn \in M$
! SPOR !

spor s minimalitou n

Diofantické rovnice - řešením je pouze celočíselné řešení

$$x^2 + y^2 = z^2$$

$\boxed{ax + by = k}$ - tato rce má řešení právě když $k \mid nsd(a,b)$

Úloha na pěšte

① číslo 21982145917308330487013369 je 13 mocninou přirozeného čísla. Jakého?

② Dokažte, že existuje mocnina čísla 3, jejíž zápis v desítkové soustavě končí na 0001.

③ $n \in \mathbb{N}$
D| $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots + \frac{1}{n} \notin \mathbb{Z}$

④ Určete, které přirozené číslo mezi 1–1000 má největší počet dělitelů

⑤ Dokažte, že $n^4 + 4$ je složené číslo $\forall n > 1, n \in \mathbb{N}$

$a, b \in \mathbb{N}$ $\quad ax_0 + by_0 = nsd(a,b)$; $x_0, y_0 \in \mathbb{Z}$

$M_{ab} = \{ax + by \mid x, y \in \mathbb{Z}\} = \{ax - bx + bx + by \mid x, y \in \mathbb{Z}\} =$

$= \{(a-b)x + b(x+y) \mid x, y \in \mathbb{Z}\} = \{(a-b)x + bz \mid x, z \in \mathbb{Z}\} = M_{a-b,b}$ $\quad a > b$

$z \in \mathbb{Z}$

$= M_{a-2b,b}$

- $nsd(a,b) = \min(M_{ab} \cap \mathbb{N}) = \min(M_{a-b,b} \cap \mathbb{N})$ $\quad a > 2b$

$\Rightarrow nsd(a,b) = nsd(\underbrace{a-kb}_{>0}, b) = nsd(b-k'r, r) = nsd(a-b, b)$

$a = kb + r$

(Př.)

$nsd(13,21) = nsd(8,13) = nsd(8,5) = nsd(5,3) = nsd(2,3) = nsd(2,1)$

$\alpha \quad b \qquad r \quad a \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad *$

$21 = 1 \cdot 13 + 8 \qquad 13 = 1 \cdot 8 + 5$

$2 = 2 \cdot 1 + 0$

$r_{i+1} < r_i$

$* = nsd(1,0) = 1 \quad (r_i\ r_{i+1})$

$\boxed{nsd(0,b) = b}$

$\boxed{\begin{array}{l} nsd(a,b) = 1 \\ \text{nesoudělná } a \perp b \end{array}}$

(Př.) $nsd(432, 234) = nsd(198, 234) = nsd(36, 198) = nsd(36, 18) =$

$= nsd(18, 0) = 18$

$nsd(a,b)\ a \geq b = nsd(r_1, b) = nsd(r_2, r_1)$

$a = k_1 b + r_1$

$b = k_2 r_1 + r_2$

$\vdots$

$r_i = k_{i+2} r_{i+1} + 0$

$18 = 198 - 5 \cdot 36 =$

$= 198 - 5(234 - 198) = 6 \cdot 198 - 5 \cdot 234 =$

$= 6 \cdot (432 - 234) - 5 \cdot 234 = 6 \cdot 432 - 11 \cdot 234$

$x_0 = 6$

$y_0 = -11$

$nsd(21;13) = x_0 \cdot 21 + y_0 \cdot 13 = 1$

~~$1 = 13 - 2 \cdot 4 = 13 - 2(5-3) = 13 - 2 \cdot 5 + 6$~~

$1 = 1 \cdot 3 - 2 \cdot 1 = 1 \cdot 3 - 1 \cdot (5-3) = 2 \cdot 3 - 5 = 2(8-5) - 5 = 2 \cdot 8 - 3 \cdot 5 =$

$= 2 \cdot 8 - 3(13-8) = 5 \cdot 8 - 3 \cdot 13 = 5(21-13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$

$x_0 = 5$

$y_0 = -8$

$24x + 105y = 33, \quad x, y \in \mathbb{Z}$

$nsd(24;105) = nsd(24;9) = nsd(9;6) = nsd(6;3) = nsd(3;0) = 3$

$3 = 6 \cdot 1 - 1 \cdot 3 = 6 \cdot 1 - (9-6) = -9 + 2 \cdot 6 = 9 + (24 - 2 \cdot 9) = 24 + 3 \cdot 9 =$

$= -24 + 3(105 - 4 \cdot 24) = -13 \cdot 24 + 3 \cdot 105 \quad / \cdot 11$

$33 = -55 \cdot 24 + 33 \cdot 105$

~~$x \in \mathbb{Z}$~~ $x_0 = -13$ $\Rightarrow$ $x = -13 \cdot 11$ $\quad K = \{(-13 \cdot 11; 33)\}$

~~$y \in \mathbb{Z}$~~ $y_0 = 3$ $\quad y = 33$

V $a, b, c \in \mathbb{N}$ Rovnice $ax + by = c$ má řešení $x, y \in \mathbb{Z}$ *

$* \Leftrightarrow nsd(a,b) \nmid c$

D: $nsd(a,b) \mid a \atop \mid b \Big\} \Rightarrow nsd(a,b) \mid ax + by = c$, x, y řešení

① $\Rightarrow$

② $\Leftarrow (\exists c') : c = c' \cdot nsd(a,b) \atop nsd(a,b) = ax_0 + by_0 \Big\} \quad c = c'(ax_0 + by_0) = a(c'x_0) + b(c'y_0)$

$(c'x_0; c'y_0)$ je řešení

(Př) Největší číslo, které je dělitelné 8 a nemá 2 stejné cifry.

9 876 543 ---↗

1 2 0
1 0 2
2 0 1
2 1 0
0 1 2
0 2 1

Eukleidovo lemma

Nechť $a, b, c \in \mathbb{N}$, jestliže $a \mid bc$ a $a \perp b$, pak $a \mid c$

$\forall p \in \mathbb{N}, p > 1$, p je prvočíslo $\Leftrightarrow (\forall b, c \quad p \mid bc \Rightarrow p \mid b \vee p \mid c)$

Dk: $\Rightarrow$ $p \in \mathbb{P}$ ① $p \mid b \vee$
② $p \nmid b \Rightarrow p \perp b \overset{\text{E.L.}}{\Rightarrow} p \mid c$

$\Leftarrow$: $p = d_1 d_2$

$p \mid d_1 d_2 \Rightarrow p \mid d_1 \vee p \mid d_2$

$d_1 \leq p$ $\qquad$ $p \leq d_1$

$\sqrt{2}$ je iracionální

SPOREM $\sqrt{2} = \frac{p}{q}$, $p \perp q$

$2q^2 = p^2 \Rightarrow p^2$ je sudé $\Rightarrow p$ je sudé $\Rightarrow p = 2k, k \in \mathbb{N}$

$2q^2 = 4k^2$

$q^2 = 2k \Rightarrow q^2$ je sudé $\Rightarrow q$ je sudé

$\sqrt{17} \notin \mathbb{Q}$

$\sqrt{17} = \frac{a}{b}$

$17b^2 = a^2 \Rightarrow 17 \mid a^2 \Rightarrow 17 \mid a$ *

$\Rightarrow 17k = a$

$17b^2 = 17^2k^2$

$b^2 = 17k^2 \Rightarrow 17 \mid b^2 \Rightarrow 17 \mid b$

Základní věta aritmetiky

V: $n \in \mathbb{N}, n > 1, \exists p_1, \dots, p_k \in \mathbb{P}$ tak, že

$n = p_1 \dots p_k$ / Rozklad je jednoznačný (až na pořadí)

Dk) jednoznačnost

$n = p_1 \cdots p_k = q_1 \cdots q_s$ n nejmenší možné

$p_1 \mid q_1 \cdots q_s \Rightarrow \exists i \; p_1 \mid q_i \Rightarrow p_1 = q_1$

vydělíme $p_1 \Rightarrow n' = \frac{n}{p_1}, \; n' < n$

/ celé číslo a stále má jednoznačný rozklad

SPOR s minimalitou

Existence (indukcí)

① $n = p \in \mathbb{P}$

② $n = d_1 d_2 = p_1 \dots p_k \cdot q_1 \dots q_s$

a) nsd

b) nsn

$$\boxed{nsd(a,b) \cdot nsn(a,b) = a \cdot b}$$

$$nsn(a,b) = \frac{a \cdot b}{nsd(a,b)}$$

všechny dělitele čísla 108

$108 = 3^3 \cdot 2^2$

$d(1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108)$

2	3
0	0
1	1
2	2
	3

12 kombinací

libovolný dělitel je: $3^k \cdot 2^l$, $k = 0, 1, 2, 3$, $l = 0, 1, 2$

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$

počet dělitelů čísla $m = \alpha_1 \alpha_2$

$\alpha_1 + 1$ { p_1 | p_2 | ... | p_k
0 | 0 | | 0
α_1 | α_2 | | α_k

počet všech dělitelů $\tau(m) = \prod_{i=1}^{k} (\alpha_i + 1)$

$\tau(100) = 9$

$100 = 2^2 \cdot 5^2$

25 29 31

37+4 41 43 11 13 7+4

17 19 13+4 5 7 1+4

aritmetické funkce (funkce na $\mathbb{N}$)

Prvočísla

V: Prvočísel je nekonečně mnoho

Dk: SPOREM, konečně mnoho $p_1, p_2, \dots p_n$

$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

① N je prvočíslo — SPOR

② N není prvočíslo — „dělitel není v seznamu prvočísel" SPOR

Rozložení prvočísel

V: Existují libovolně dlouhé „mezery".

libovolně dlouhé posloupnosti přirozených čísel, které nebudou prvočísla

Dk: $(n+1)! + j$, $j \in \{2, \dots, n+1\}$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \dots \cdot (n+1) + 2 = 2(\dots + 1)$

$+3 = 3(\dots + 1)$

Prvočíselná dvojčata

3, 5,

29, 31

$\pi(n) = \{p \leq N \mid p \in \mathbb{P}\}$ $\lim_{n \to +\infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1$

$\pi(10) = 4$

$\pi(12) = 5$

$\pi(n) = \frac{n}{\ln(n)}$

$\pi(n) \approx \frac{n}{\ln(n)}$

Kongruence

– jiný způsob zápisu dělitelnosti

Def $a \equiv b \bmod m$

a, b dávají stejný zbytek po vydělení m

$\boxed{m \mid a-b}$

Vlastnosti $a+c \equiv b+c \bmod m$

$ac \equiv bc \bmod m$

$a \equiv b \bmod m$

$c \equiv d \bmod m$

$a+c \equiv b+d \bmod m$

$ac \equiv bd \bmod m$

$a^k \equiv b^k \bmod m$

Věta $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \; a_i \in \mathbb{Z}$

$x \equiv y \bmod m \iff f(x) \equiv f(y) \bmod m$

(Př) $f(x) = 14x^5 + 25x^4 + 35x^3 + 15x^2 - 19x + 4$

↙ můžeme menšit, aby byl se. stejný

nahradím zbytek po vydělení 4

$f(20)$ po zbytek po dělení 4

$f(20) \equiv \square \bmod 4$ ← hledané číslo (1; 2; 3; 4; 5; 6)

$\bar{f}(x) = 3x^4 + x^2 + 2x + 4$

$f(x) = \square \bmod 7$

$\hat{f}(x) = 0 \bmod 7$

$f(x) + \hat{f}(x) = \square \bmod 7$

$\hat{f}(x) = -14x^5 + 28x^4 - 35x^3 + 14x + 21x$

$20 \equiv 6 \bmod 7$

$20 \equiv -1 \bmod 4 \to f(20) \equiv f(-1)$

① D: $a \cdot nsd(a,b) + b \cdot nsd(a,b) \geq 2a \cdot b$, $\forall a,b \in \mathbb{N}$

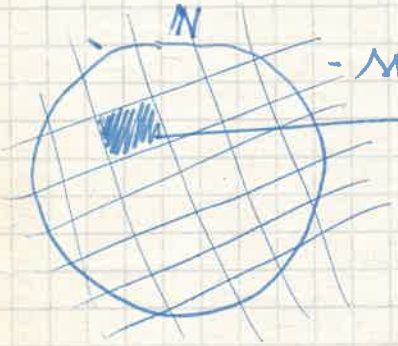
② D: Každé liché číslo, které není dělitelné pěti dělí některé z čísel 1, 11, 111, 1111, ...

③ D: Že desítkový rozvoj $1+2+3+\dots+n$ nekončí na cifry 2, 4, 7, 9, $\forall n \in \mathbb{N}$

④ Pro která t racionální je číslo $3t^3+10t^2-3t$ celé

⑤ Urči počet 10-ciferných čísel, ve kterých je možno dvě sousední cifry škrtnout a tím dostat číslo 99-krát menší.

Kongruence



- speciální relace ekvivalence
třída ekvivalence (zbytková třída)
- všechna čísla, která dávají zbytek j: $\{km-j \mid k \in \mathbb{Z}\}$

$m=2: \mathbb{Z} = \{2k-1 \mid k \in \mathbb{Z}\} \cup \{2k; k \in \mathbb{Z}\}$

$a+c \equiv b+c \bmod m \Rightarrow a \equiv b \bmod m$

$ac \equiv bc \bmod m \not\Rightarrow a \equiv b \bmod m$

$ac \equiv bc \bmod m \wedge m \perp c \Rightarrow a \equiv b \bmod m$

Kriterium dělitelnosti

Pozn. Poziční soustavy

q - základ

$\{0,1,2,\dots,q-1\}$ - abeceda

$12 \cdot 9 = 120 - 12 = 108 + 180 = 288$

V: $q \in \mathbb{N}, q > 1$, každé číslo lze jednoznačně vyjádřit ve tvaru

$$n = \sum_{i=0}^{k} a_i q^i, \quad a_i \in \{0,1,\dots,q-1\}$$

Dk | existence: indukcí

$n \equiv a_0 \mod q$

$n = \sum_{i=0}^{k} a_i q^i = a_0 + a_1 q + \ldots + a_{k-1} q^{k-1} + q^k \cdot a_k$

$\frac{n}{q} = 0 + \frac{a_0}{q}$ (zbytek)

$a_0 :=$ zb. po dělení n q, $a_0 \in \{0, 1, 2, \ldots q-1\}$

$n' = \frac{n - a_0}{q}$

$\hookrightarrow a_1$

⋮

25 v binární soustavě,

①

1	1	hladový algoritmus
2	0	
4	0	
8	1	9 − 8
16	1	25 − 16

$2^k \leq 25 < 2^{k+1}$

$a_k = \left\lfloor \frac{25}{q^k} \right\rfloor$

$25 = (11001)_2$

② $25 : 2 = 12 + ① — a_0$

$12 : 2 = 6 + ⓪ — a_1$

Př. 493 do 7 soustavy

1	3
7	0
49	3
343	1

$493 = (1303)_7$

$493 \equiv 3 \mod 7 \quad a_0 = 3$

$\frac{493 - 3}{7} = 70$

$70 \equiv 0 \mod 7 \quad a_1 = 0$

$\frac{70 - 0}{7} = 10$

$10 \equiv 3 \mod 7 \quad a_2 = 3$

$\frac{10 - 3}{7} = 1 \quad 1 \equiv 1 \mod 7 = 1 \quad a_3 = 1$

64 16 8 4 2 1
$(1\,0\,1\,1\,0\,1\,0)_2 = 90$

$(10100)_3$

Kriteria dělitelnosti

V: $n \in \mathbb{N}$ má po dělení 3 stejný zbytek jako jeho ciferný součet (v 10 soustavě)

$n = a_k \cdot 10^k + a_{k-1} 10^{k-1} + \dots + a_1 \cdot 10 + a_0$

$f(x) = a_k \cdot x^k + a_{k-1} x^{k-1} + \dots + a_1 \cdot x + a_0 \quad | f(10) = n, f(1) = \text{cif. s.}$

$\text{cif. s.} = a_k + a_{k-1} + \dots + a_1 + a_0$

$10 \equiv 1 \bmod 3$

$f(10) \equiv f(1) \bmod 3$

$a \equiv b \bmod m$

$f(a) \equiv f(b) \bmod m$

V: $n \in \mathbb{N}$ má po dělení 9 stejný zbytek jako jeho ciferný součet

$1 \equiv 10 \bmod 9 \Rightarrow f(1) \equiv f(10) \bmod 9$

V: 11

$1 \equiv 10 \bmod 11$ - není pravda

$-1 \equiv 10 \bmod 11$

$f(10) \equiv f(10) = f(-1) = (-1)^k \cdot a_k + \dots + a_1 + a_0$

① $\forall a,k \in \mathbb{N}$: $a \cdot nsd(a,b) + b \cdot nsd(a,b) \geq 2ab$

$a \geq b \geq nsd(a,b)$

$a \geq nsd(a,b)$ $\quad$ $b \geq nsd(a,b)$

$ba \geq nsd(a,b) \cdot b$ $\quad$ $ab \geq nsd(a,b) \cdot a$

$2ab \geq nsd(a,b) \cdot a + nsd(a,b) \cdot b$

② $\forall n \in \mathbb{N}$ $5 + 10n$

$5 + 2n - 1 \Rightarrow 2n-1 \mid 1 \;\vee\; 2n-1 \mid 11 \;\vee\; 2n-1 \mid 111 \;\vee \ldots$

$\Rightarrow (2n-1)k = 1 \;\vee\; (2n-1)k = 11 \;\vee \ldots$

③ Pro které $t \in \mathbb{Q}$ $V(t) = 3t^3 + 10t^2 - 3t \in \mathbb{Z}$

$V(t) = t(3t^2 + 10t - 3)$

$3t^2 + 10t - 3 = t$ $\quad$ $3t^2 + 10t - 3 = kt$

$3t^2 + 9t - 3 = 0$ $\quad$ $3t^2 + (10-k)t - 3 = 0$

$t^2 + 3t - 1 = 0$ $\quad$ $D = (10-k)^2 + 4(3 \cdot 3)$

$D = 100 - 20k + k^2 + 36$

$D = 136 - 20k + k^2$

k^2 $\quad$ $\frac{-10+}{6}$ $\quad$ $k = 10$ $\quad$ $12k = -120$

$-12k + 136 = 16$

$3t^2 + 10t - 3 - k = 0$ $\quad$ $\frac{-10}{6}$

$D = 10^2 + 4(3(3-k)) = 100 + 4(9-3k) = 100 + 36 - 12k = 136 - 12k$

$12k = 136 \Rightarrow k = \frac{136}{12} = \frac{68}{6} = \frac{34}{3} \in$ $12k - 136 = 16$

Naleznete všechna $t \in \mathbb{Q}$ taková, že $V(t) = 3t^3 + 10t^2 - 3t \in \mathbb{Z}$

Víme: • $t \in \mathbb{Q} \Rightarrow t = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}$

• triviálně platí pro všechna $t = \frac{a \cdot k}{a}, a \in \mathbb{N}, k \in \mathbb{Z}$

• hledaná t musejí nutně mít následující vlastnosti

① $3t^2 + 10t - 3 = 3\left(\frac{a}{b}\right)^2 + 10\left(\frac{a}{b}\right) - 3 = b \cdot k, k \in \mathbb{Z}$

~~$\frac{3a^2 + 10ab - 3b^2}{b^2} = b \cdot k$~~

~~[illegible]~~

② ~~$3t^2 + 10t - 3 = \frac{a}{t} k$~~

~~$3t^2 + 10t - 3$ [illegible]~~

~~$D = 100 + 4k$ [illegible]~~

① $3a^2 + 10ab - 3b^2 - b^2 \cdot k = 0$

~~$a_{1,2} = \frac{-10b \pm 2b\sqrt{28+bk}}{6} = \frac{-5 \pm b\sqrt{28+bk}}{3}$~~

~~$D = 100b^2 - 4(-3b^2 - b^3 k)$~~

~~$112b^2 + 4b^3 k$~~

~~$\sqrt{D} = 2b\sqrt{28 + bk}$~~

~~$\sqrt{28 + bk} \in \mathbb{Z}$~~

~~[illegible]~~

−28	1
−24	4
−19	6
−12	9
−3	11
+8	21

$$3a^2 + 10ak - 3k^2 - k^3k = 0$$

$$D = (10k)^2 - 4(3(-3k^2 - k^3k)) \cdot$$

$$D = 100k^2 + 36k^2 + 12k^3k = 136k^2 + 12k^3k$$

$$a_{1,2} = \frac{-5k \pm k\sqrt{34 + 3kk}}{3}$$

$x: 3 \mid x^2 - 34 > 0$

k

$\rightsquigarrow t = \frac{a}{k}, \quad a \geq k$

$V(t) = t \cdot (3t^2 + 10t - 3) \in \mathbb{Z}$

Dokažte, že $19 \cdot 8^n + 17$ je složené pro $\forall n \in \mathbb{N}$

$n \in \mathbb{N}$ D.: „mezi $n+1$ čísly lib. vybranými z $\{1, 2, \dots, 2n\}$ existují dvojice čísel a, b tak, že $a \mid b$"

6) Nechť $n \geq 2, n \in \mathbb{N}$, $n^2 + 2^n$ je prvočíslo $\Rightarrow n \equiv 3 \bmod 6$

7) $(\forall n \in \mathbb{N})(\exists x \in \mathbb{N})$ jehož desetinný rozvoj obsahuje jeden 1, 2, které je dělitelné 2^n

8) Kolika nulami končí desítkový rozvoj čísla $2017!$?

$n = a_0 + 10a_1 + \dots + 10^k a_k$

$f(x) = a_0 + a_1 x + \dots + a_k x^k$

$10 \equiv 1 \bmod 3 \Rightarrow f(10) \equiv f(1) \bmod 3$

(7) $10 \equiv 3 \bmod 7$

$f(10) \equiv f(3) \bmod 7$

↑ velké číslo

$10 \equiv 3 \bmod 7 \quad / \cdot 10$

$10^2 \equiv 30 \bmod 7$

$10^2 \equiv 2 \bmod 7 \quad / \cdot 10$

$10^3 \equiv 6 \bmod 7 \quad / \cdot 10$

$10^4 \equiv -3 \bmod 7$

$10^5 \equiv -2 \bmod 7$

$10^6 \equiv 1 \bmod 7$

$n = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \dots$

$\dots \bmod 7$

-17

$68 \nmid 102$

$34 \mid 85$

V: $n = (a_k a_{k-1} \dots a_1 a_0) \rightarrow m = (a_k a_{k-1} \dots a_1)$

n je dělitelné 7 $\Leftrightarrow$ $m - 2a_0$ je dělí 7

Dk: $n \equiv 0 \mod 7$

$n \equiv 10 \cdot m + a_0 \mod 7$

$10m + a_0 \equiv n \mod 7$

$\Rightarrow \begin{cases} 20m + 2a_0 \equiv n \mod 7 \\ 21m \equiv n \mod 7 \end{cases}$

$-m + 2a_0 \equiv \mod 7$

$m - 2a_0 \equiv \mod 7$

66951 dělí 7

6695 − 2 = 6693

6300	393
343	50

dělitelnost 9 v 16 soustavě

$n = a_k \cdot 16^k + a_{k-1} 16^{k-1} + \dots + a_1 \cdot 16 + a_0$

$m = a_k \cdot x^k + a_{k-1} x^{k-1} + \dots + a_1 \cdot x + a_0$

$16 \equiv 7 \mod 9$

$16^2 \equiv 4 \mod 9$

$16^3 \equiv 1 \mod 9$

$n \equiv a_0 + 7a_1 + 4a_2 + 1a_3 + 7a_4 + \dots \mod 9$

Malá Fermatova věta

V: Nechť $p \in P$, $a \in N$, $a \perp p$
potom $a^{p-1} \equiv 1 \mod p$

Dk: $a, 2a, 3a, \dots, (p-1)\cdot a$
$r_1 \quad r_2 \quad r_3 \quad \quad r_{p-1}$ zbytky po dělení p

$r_j \in \{1, 2, \dots, p-1\}$

$\{r_1, r_2, r_3, \dots, r_{p-1}\} = \{1, 2, 3, \dots, p-1\}$

$r_i = r_j \Rightarrow i = j$

$ia \equiv ja \mod p \;/\; a \perp p \Rightarrow /:a$

$i \equiv j \mod p$

$i, j \in \{1, \dots, p-1\}$

$\Rightarrow i = j$

$ia \equiv r_i \mod p$ } $(p-1)$ kongruencí ~~1, 2a, 3a, 4a ... (p-1)a~~

~~1, 2a, 3a, 4a, 5a ... (p-1)a ≡ (p-1)!~~

$1 \cdot 2a \cdot 3a \cdot 4a \cdot 5a \dots (p-1)a \equiv r_1 \cdot r_2 \cdot r_3 \dots r_{p-1} \mod p$

$(p-1)!\, a^{p-1} \equiv (p-1)! \mod p \quad 2 \perp p, 3 \perp p, \dots, p-1 \perp p$

$a^{p-1} \equiv 1 \mod p$

Kolik nejednobarevných náhrdelníků z „p" korálků lze vyrobit, mám-li korálky „a" barev

$$\frac{a^p - a}{p} \in \mathbb{Z}$$

$p \mid a^p - a$

$a^p - a \equiv \mod p$

$a^p \equiv a \mod p \Rightarrow a^{p-1} \equiv 1 \mod p$

① $(\forall k \in \mathbb{N})$ najděte $x \in \mathbb{N}$ tak, že $\underbrace{1\ldots1}_{x}$ je dělitelné $\underbrace{3\ldots3}_{k}$

② Najděte slyšek 100. mocniny číslem 125

③ Dokažte, že existují právě jedno $a, n \in \mathbb{N}$ tak, že $a^{n+1} - (a+1)^n = 2001$

④ $x, y \in \mathbb{N}$, $x + y < 100$:

člověk A pozná součin
člověk B — " — součet

A: nemám x a y
B: Já jsem to věděl
A: Tak já už taky
B: Tak já taky

Najdi x a y

Kongruence

- Řešení kongruencí

$ax + b \equiv cx + d \bmod m$

$(a-c)x \equiv d-b \bmod m$

$a' \quad x'$

$a'x \equiv b' \bmod m$

$\Leftrightarrow$

$m \mid a'x - b'$

$a'x - b' = km$

$a'x - km = b', \; x, k \in \mathbb{Z}$

$x \equiv 3 \bmod 5$

$x = \{3 + 5k \mid k \in \mathbb{Z}\}$

$x \equiv n \bmod m$ - lze řešit

Diofantická rovnice

$nsd(a', m) \mid b' \Leftrightarrow$ rovnice má řešení

$29x \equiv 1 \bmod 17$

[redacted]

$29x \equiv 1 \bmod 17$

$* \quad 17x \equiv 0 \bmod 17$

$12x \equiv 1 \bmod 17$

$* \quad 0 \equiv 17 \bmod 17$

$12x \equiv 18 \bmod 17 \quad / \cdot 6^{-1} \; (6 \perp 17)$

$2x \equiv 3 \bmod 17$

$* \quad 0 \equiv 17 \bmod 17$

$2x \equiv 20 \bmod 17 \quad / \cdot \frac{1}{2} \; (2 \perp 17)$

$x \equiv 10 \bmod 17 \quad x = \{10 + 17k \mid k \in \mathbb{Z}\}$

Soustavy

$$\left.\begin{array}{l} a_1 x \equiv r_1 \bmod m_1 \\ \vdots \\ a_k x \equiv r_k \bmod m_k \end{array}\right\} \begin{array}{l} \longrightarrow x \equiv r_1' \bmod m_1 \\ \\ \longrightarrow x \equiv r_k' \bmod m_k \end{array}$$

- pokud některá z rovnic nemá řešení, pak celá soustava nemá řešení
- pokud všechny lze vyřešit $\Rightarrow$ $x_1 \equiv r_1' \bmod m_1$, …, $x_k \equiv r_k' \bmod m_k$

① m_i jsou nesoudělná
- vždycky existuje řešení

V/ Čínská věta o zbytcích

$m_1, \dots, m_k$ nesoudělná

$r_1, \dots, r_k \in \mathbb{Z}^+$

Potom $x \in \mathbb{Z}$ je řešením

$$\Leftrightarrow x \equiv c_1 \cdot \frac{m}{m_1} r_1 + c_2 \cdot \frac{m}{m_2} r_2 + \dots + c_k \frac{m}{m_k} r_k \bmod m$$

$$m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$$

$$c_i \cdot \frac{m}{m_i} \equiv 1 \bmod m$$

(Př) 7 stupy 2 chybí

9 stupy 2 přebývají

děti < 100

$\Rightarrow$ $x \equiv -2 \bmod 7$ | $7 \perp 9 \Rightarrow$ má řešení

$x \equiv 2 \bmod 9$

$x = \{-2 + 7k \mid k \in \mathbb{Z}\}$ | $m = m_1 \cdot m_2 = 7 \cdot 9 = 63$

$x = \{2 + 9k \mid k \in \mathbb{Z}\}$ | $c_1 \cdot \frac{63}{7} \equiv 1 \bmod 7$

$9c_1 \equiv 1 \bmod 7$

$9c_1 \equiv 1 \mod 7$

$2c_1 \equiv 1 \mod 7$

$2c_1 \equiv 8 \mod 7$

$c_1 \equiv 4 \mod 7$

$7c_2 \equiv 1 \mod 9$

$-2c_2 \equiv 1 \mod 9$

$-2c_2 \equiv 10 \mod 9$

$c_2 \equiv -5 \mod 9$

$c_2 \equiv 4 \mod 9$

$X \equiv c_1 \cdot \frac{m}{m_1} r_1 + c_2 \cdot \frac{m}{m_2} r_2 \mod m$

$x \equiv 4 \cdot 9 \cdot (-2) + 4 \cdot 7 \cdot 2 \mod 63$

$x \equiv 47 \mod 63$

$X = \{47 + 63k \mid k \in \mathbb{Z}\}$

do 100 existuje pouze jedno řešení, dělí je 47

Dotaz na věk

$x \equiv 1 \mod 3 \quad c_1$

$x \equiv 3 \mod 4 \quad c_2$

$x \equiv 1 \mod 5 \quad c_3$

$m = 60$

$c_1 \; 20 \equiv 1 \mod 3$

$2c_2 \equiv 1 \mod 3$

$2c_2 \equiv 4 \mod 3$

$c_2 \equiv 2 \mod 3$

$c_2 \cdot 15 \equiv 1 \mod 4$

$-c_2 \equiv 1 \mod 4$

$c_2 \equiv -1 \mod 4$

$c_3 \cdot 12 \equiv 1 \mod 5$

$2c_3 \equiv 1 \mod 5$

$c_3 \equiv 3 \mod 5$

$x \equiv 1 \cdot 20 \cdot 1 + (-1) \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 1 \mod 60$

$x \equiv 11 \mod 60$

moduly jsou soudělné

$x \equiv r_1 \bmod m_1$
$x \equiv r_2 \bmod m_2$ má řešení v $\mathbb{Z} \Leftrightarrow r_1 \equiv r_2 \bmod \gcd(r_1, r_2)$

pokud má x řešení $y \equiv x \bmod \gcd(m_1, m_2)$

$x \equiv 5 \bmod 63$
$x \equiv 14 \bmod 36$

$\gcd(63,36) = \gcd(36,27) = \gcd(27,9) = 9$
$5 \equiv 14 \bmod 9$ ✓

$x = 63k + 5$

$63k + 5 \equiv 14 \bmod 36$
$63k \equiv 9 \bmod 36$
$-9k \equiv 9 \bmod 36$
$9k \equiv -9 \bmod 36 \quad / : 9$
~~$9k = 63 \bmod 36$~~
$k \equiv -1 \bmod 4$
$k = 4l - 1, \; l \in \mathbb{Z}$

$x = 63(4l-1) + 5 = 252l - 63 + 5 = 252l - 58 =$

$n \in \mathbb{N} \quad 90 \leq n \leq 100$

po dělení 2 zbyde 1

po dělení 5 zbyde 4

$n \equiv 1 \mod 2$ | $m = m_1 \cdot m_2 = 10$

$n \equiv 4 \mod 5$ |

I. Chci $\frac{m}{m_1} c_1 \equiv 1 \mod m_1$

$5c_1 \equiv 1 \mod 2$

$2c_2 \equiv 1 \mod 5$

$c_1 = 1$

$c_2 = 3$

$n \equiv c_1 \cdot \frac{m}{m_1} b_1 + c_2 \frac{m}{m_2} b_2 \mod m$

$n \equiv 5 \cdot 1 + 3 \cdot 4 \mod 10$

$n \equiv 29 \mod 10$

$n \equiv 9 \mod 10$

$\rightarrow n = 99$

II. Dosazování

$n \equiv 1 \mod 2$

$n \equiv 4 \mod 5$

$n = 1 + 2k$

$2k + 1 \equiv 4 \mod 5$

$2k \equiv 3 \mod 5$

$2k \equiv 8 \mod 5$

$k \equiv 4 + 5m$

$n = 2(4 + 5m) + 1 = 10m + 9$

Aritmetické funkce $n = p_1^{k_1} \cdots p_m^{k_m}$

$\tau(n)$ = počet dělitelů, $\tau(n) = \sum_{d|n} 1 = \prod_{i=1}^{m} (1+k_i)$

multiplikativní

$\tau(m \cdot n) = \tau(m) \cdot \tau(n)$ | $m \perp n$

$\tau(10) = \tau(5) \cdot \tau(2) = 4$

$\varphi(n)$ - Eulerova funkce

$\varphi(n)$ - počet čísel menších rovno n, která jsou nesoudělná s n

$\varphi(n) = \#\{k \in \mathbb{N} \mid k \perp n, k \leq n\} \quad \forall n \in \mathbb{N}$

$\varphi(1) = 0$

$\varphi(2) = 0$

$\varphi(3) = 1$

$\varphi(4) = 2$

$\varphi(5) = 4$

$\varphi(6) = 2$

$\varphi(7) = 6$

$a \perp b \Leftrightarrow nsd(a,b) = 1$

Lemma $p \in \mathbb{P}$

$\varphi(p) = p - 1$

$\varphi(p^k) = p^k - p^{k-1}$

$\{k\}$ — 1 — p^k

$p, 2p, 3p, \ldots, p^{k-1}$

$\varphi(p;q) = p \cdot q - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$

$p, 2p, 3p, \ldots, pq$ → q čísel

$q, 2q, 3q, \ldots, qp$ → p čísel

$\varphi(pq) = \varphi(p)\varphi(q)$

$\varphi(n)$ pro složená čísla

$n \in \mathbb{N}$ -

$$n = \sum_{d \mid n} \varphi(d) = \varphi(n) + \sum_{\substack{d \mid n \\ d < n}} \varphi(d)$$

$$\varphi(n) = n - \sum_{\substack{d \mid n \\ d < n}} \varphi(d)$$

$$\varphi(18) = 18 - \varphi(1) - \varphi(2) - \varphi(3) - \varphi(6) - \varphi(9) =$$
$$= 18 - 1 - 1 - 2 - 2 - 6 = 6$$

Dk $n = \sum_{d \mid n} \varphi(d)$

$(0;1\rangle$

počet zlomků tvaru, že n je ve jmenovateli

$\frac{1}{n}, \dots, \frac{n}{n}$ - počet je n

~~$\frac{d_1}{n} = \frac{d_2}{n}$~~

$\frac{d_2}{n} \cdot \frac{d_2}{d_2} = \frac{\cdot}{d_1}$ $\quad d_1 \mid n$

$d_1 \cdot d_2 = n$

$\square$

d_1 $\quad d_1 \mid n$ $\quad \varphi(d_1)$ $\quad \sum_{d \mid n} \varphi(d)$

zákl. tvar

Věta | $n \in \mathbb{N}$ $\quad n = p_1^{k_1} \cdots p_m^{k_m}$

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

* Princip sčítání a inkluse

$\left| \bigcup_{i=1}^{k} A_i \right|$ $\quad A_1, \dots, A_k$

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$\left| \bigcup_{i=1}^{k} A_i \right| = \sum_{j=1}^{k} (-1)^{j+1} \sum_{\{i_1, \dots, i_j\} \subseteq \{1, \dots, k\}} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_j}|$$

Dk | MI na $|\bigcup A_i|$

$k = 0$: $\left|\bigcup_{i=1}^{0} A_i\right| = 0$ ✓, ok

$\left| \bigcup_{i=1}^{k} A_i \right| \ni x$

$\swarrow$ obsahuje x — $A_i \setminus \{x\}$

$\searrow$ neobsahuje

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Dk! $\varphi(n) = n$ - soudělná

$$n = p_1^{k_1} \cdots p_m^{k_m}$$

$$p_1 \cdot 2p_1 \cdot 3p_1 \cdots \frac{n}{p_1} p_1 \cdots n$$
$$p_2 \cdot 2p_2 \cdot 3p_2 \cdots \frac{n}{p_2} \cdot p_2$$
$$\vdots$$
$$p_m \; 2p_m \; 3p_m \cdots \frac{n}{p_m} p_m$$

$$A_i^* = \{ \ell p_1 \mid \ell \leq \frac{n}{p_1} \}$$

$$|\bigcup A_i| = \sum_{j=1}^{k} (-1)^{j+1} \cdot \sum_{\{i_1, \dots, i_j\}} |A_1 \cap \dots \cap A_{ij}|$$

$$|A_1 \cap A_2| = \frac{n}{nsn(p_1, p_2)}$$

~~$|A_{i_1} \cap \dots \cap A_{ij}| =$~~

$$|A_{i_1} \cap \dots \cap A_{ij}| = \frac{n}{nsn(p_{i_1}, \dots p_{ij})} = \frac{n}{p_{i_1} \cdots p_{ij}}$$

$$\varphi(n) = n - \sum_{j=1}^{km} (-1)^{j+1} \sum_{\{i_1, \dots, i_j\}} \frac{n}{p_{i_1} \cdots p_{ij}} = *$$

$$* = n \left(1 - \sum_{i=1}^{km} (-1)^{j+1} \sum_{\{i_1 \cdots i_j\}} \left(\frac{1}{p_{i_1} \cdots p_{ij}}\right)\right) = n \left(\sum_{j=0}^{km} (-1)^j \sum \frac{1}{p_{i_1} p_{i_2} \cdots p_{ij}}\right) =$$

$$= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

Důsledky

$$\varphi(m\cdot n) = mn \prod_{i=1}^{l} \left(1-\frac{1}{\mu_i}\right) = m \prod \left(1-\frac{1}{p_i}\right) \cdot n \prod \left(1-\frac{1}{\mu_i}\right)$$

$m \perp n$

Eulerova rozšíření malé fermatovy věty

$$a^{\varphi(n)} \equiv 1 \bmod n, \quad n \perp a$$

4.12 - 101T

① Najděte všechna $n \in \mathbb{N}$, že $\varphi(n)$ liché

② Pro liché $m > 1$ najděte zbytek po dělení čísla $2^{\varphi(m)-1}$ číslem m

③ Najděte všechna $x, y \in \mathbb{Z}$, $x \cdot y = x + y$

④ Může se diskriminant $ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$ rovnat 23?

Šifrování s veřejným klíčem

A, B šachy po telefonu

do čísel

Tab 1032 ..... doplní na 100 místné prvočíslo

$q > p$ $\boxed{n = p \cdot q}$

Řeknu Bobovi n

pole prvočísel q

[A] ⟶ [B]

① příprava

→ zveřejní veřejný klíč

$p \cdot q$ - schová soukromý klíč

② šifrování VK

③ dešifrování SK

RSA

1977 ... Jména tvůrců

- příprava volí p, q velmi velké
- $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$
- $i \perp \varphi(n)$

↳ náhodně a vyzkoušet: $nsd(i, \varphi(n))$?

$$ij \equiv 1 \bmod \varphi(n)$$
$$\Leftrightarrow ij + k\varphi(n) = 1 = nsd(i, \varphi(n))$$
$$\Leftrightarrow$$

Veřejný klíč: n, i

Soukromý klíč: j
$(p, q, \varphi(n))$

- Šifrování

zpráva $\in \mathbb{N}$ ←

① $X < n$

② $X^i \equiv y \bmod n$

zašifrovaná zpráva

Dešifrování

y: $y^j \equiv X \bmod n$

původní zpráva

A: $p = 47$, $q = 67$

$n = 3149$

$\varphi(n) = 3036$

① $i = 13$

$13 \perp 3036$?

$nsd(3036, 13) = nsd(46, 13) = nsd(7, 13) = 1$ ✓

$nsd(1, 3) = nsd(1, 0)$

$13 j \equiv 1 \mod 3036$

~~13 = 2·7 + 1~~

13j =

~~...~~

$1 = -13 + 2·7 = -13 + 2(46 - 3·13) = \ldots$

$j = 2569$

AHOJ

ASCII: $A = 65 = (01000001)_2$

$H = 72 = (01001000)_2$

$O = 79 = (01001111)_2$

$J = 74 = (01001010)_2$

522 (11), 64 + 537 (11), 1685 (10)

0 1000001 0 10|01000 0100 1|111 0100 1010 1

blok délky m

doplníme: 100...

(1..000)

$2^m < n = 3149$

$m = 11$

1 0........ (m)

$522^{13} \equiv 1077 \mod 3149$

$*522 \equiv 522 \mod 3149$

$522^2 \equiv 1670 \mod 3149$

$(522^2)^2 \equiv (1670)^2 \mod 3149$

$\vdots$

$531^{13} \equiv 1901 \mod 3149$

$1685^{13} \equiv 1761 \mod 3149$

1077 1901 1761

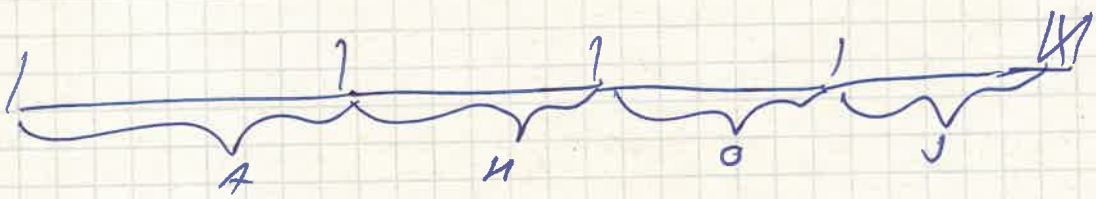
1 0000 1101 1011 0111 0101 1111 0001

Dešifrování

$1077^{2569} \equiv 522 \mod 3149$

$1901^{2569} \equiv 531 \mod 3149$

$1761^{2569} \equiv 1685 \mod 3149$



• poloměr

$n = p \cdot q$ $\qquad (p-1)(q-1) = \varphi(n)$

(n, i) $\qquad$ (j) $\leftarrow$ $ij \equiv 1 \bmod \varphi(n)$

V:

$ij \equiv 1 \bmod \varphi(n)$

$x^i \equiv y \bmod n$

$y^j \equiv x \bmod n$

$ij = k\varphi(n)+1$

Dkl $x^{ij} \equiv x \bmod n$

a) $x \perp n$ $\quad x^{\varphi(n)} \equiv x \bmod n$

$x^{k\cdot\varphi(n)} \equiv x \bmod n$

$x^{k\cdot\varphi(n)+1} \equiv x \bmod n$

b) x soud. n

$x = ap$, $bq = x$

① Najdi největšího dvojciferného prvočíselného dělitele $\binom{200}{100}$

② Popište všechna n taková, že $\sigma(n) = 2^k$, $k \in \mathbb{N}$, $\sigma(n) = \sum_{d|n} d$

③ Kolik existuje 4ciferných čísel x takových, že $x^2 \equiv x \bmod 10000$

④ Kniha má strany $1, 2, \ldots, N$. Je rozdělena na 2 části tak, že součet stran je roven součtu stran 2 částí.

⑤ Najděte $n \in \mathbb{N}$, pro které je zlomek $\frac{19n+7}{7n+11}$ celé číslo?

PŘ

Odhadněte počet 100 místných prvočísel

$\pi(n) = \#\{p \in \mathbb{P} \mid p \leq n\}$, $\pi(n) \sim \frac{n}{\ln n}$

Kolik 100 místných čísel: $10^{100} - 10^{99}$

Počet prvočísel: $\pi(10^{100}) - \pi(10^{99}) =$

$$= \frac{10^{100}}{100 \ln 10} - \frac{10^{99}}{99 \cdot \ln 10} = \frac{99 \cdot 10^{98} - 10^{99}}{99 \ln 10} =$$

$$= \frac{10^{98}(99)}{99 \cdot \ln 10} \sim 3{,}9 \cdot 10^{97}$$

Pravděpodobnost: $\frac{3{,}9 \cdot 10^{97}}{9 \cdot 10^{99}} = \frac{3{,}9}{9 \cdot 100} = \frac{1}{231}$

Fermatův test prvočíselnosti čísla n

a → $a^{n-1} \not\equiv 1 \bmod n$ - není prvočíslo

$a^{n-1} \equiv 1 \bmod n$ → n je prvočíslo

pseudoprvočíslo

a je Fermatův lhář

Carmichaelova čísla

- složená čísla
- první je 561

Millerův - Rabinův test

$a \in \{2, 3, \ldots, n-1\}$

$561 \mid a^{560} - 1$

a soudělné 560 $\Rightarrow 561 \mid a^{560} - 1 \Rightarrow n$ složené

a nesoudělné 560

a nesoudělné 561

$$a^{560} - 1 = (a^{280} - 1)(a^{280} + 1) = (a^{140} - 1)(a^{140} + 1)(a^{280} + 1) =$$

$$= (a^{70} - 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1) = \underline{(a^{35} - 1)(a^{35} + 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1)}$$

$560 = 2^k \cdot n = 2^4 \cdot 35$

Kdyby 561 prvočíslo, pak dělí, alespoň jeden ze závorek!

n dělí nějakou závorku $\Rightarrow$ „n se chová jako prvočíslo" vůči a

Když n nedělí žádnou závorku $\Rightarrow$ n je složené

$\Rightarrow$ n složené a ... $P(\text{chyby}) = \frac{1}{4}$

k - krát ... $P = \frac{1}{4^k}$

Dokonalá, Mersenova, Fermatova čísla

$\sigma(n) = \sum_{d|n} d$ součet dělitelů

Dokonalá

$\sigma(p) = p+1, \quad p \in \mathbb{P}$

$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1}-1}{p-1}$

Věta $n = p_1^{k_1} \cdots p_m^{k_m}$

$\sigma(n) = \sigma(p_1^{k_1}) \cdot \sigma(p_2^{k_2}) \cdots \sigma(p_m^{k_m})$

Dk.

$$\sigma(n) = \sum_{i_1=0}^{k_1} \cdot \sum_{i_2=0}^{k_2} \cdots \sum_{i_m=0}^{k_m} p_1^{i_1} \cdot p_2^{i_2} \cdots p_m^{i_m} =$$

$$= \left(\sum_{i_1=0}^{k_1} p_1^{k_1}\right)\left(\sum_{i_2=0}^{k_2} p_2^{k_2}\right) \cdots \left(\sum_{i_m=0}^{k_m} p_m^{k_m}\right) = \sigma(p_1^{k_1}) \cdots \sigma(p_m^{k_m})$$

Důsledek $n \perp m$

$\sigma(n)\,\sigma(m) = \sigma(n \cdot m)$ - multiplikativní

Dokonalá čísla

$\sigma(n) = 2n$

6, 28, 496, 8128

$6 = 2 \cdot 3 = 2(2^2 - 1)$

$28 = 4 \cdot 7 = 2^2(2^3 - 1)$

$496 = 2^4(2^5 - 1)$

$8128 =$

V (Euklides)

$n \in \mathbb{N}$ jestliže existuje $k \in \mathbb{N}$ tak, že $2^{k+1} - 1 \in \mathbb{P}$, pak $n = 2^k(2^{k+1} - 1)$ je dokonalé číslo

Dk| $\sigma(n) = \sigma(2^k)\cdot\sigma(2^{k+1}-1) = \frac{2^{k+1}-1}{2-1}\cdot(2^{k+1}-1+1) = 2n$

Mersenova čísla

$2^{k+1}-1 \in \mathbb{P}$

V (Euler)
Každé sudé dokonalé číslo n je tvaru $2^k(2^{k+1}-1)$, kde $2^{k+1}-1 \in \mathbb{P}$

$2^n - 1 \in \mathbb{P}$ - n-té Mersenovo číslo

$2^1 - 1 = 1$
$2^2 - 1 = 3$
$2^3 - 1 = 7$
$2^4 - 1 = 15$
$2^5 - 1 = 31$
$2^6 - 1 = 63$
$2^{11} - 1 = 2047$

$2047 = 23 \cdot 89$

Věta| Když je 2^n-1 prvočíslo, potom n je prvočíslo

Dk| $\Leftarrow$ když n je složené pak 2^{n-1} je složené

$n = a \cdot b$

[redacted]

$2^{a\cdot b} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \dots + 2^{(b-1)a})$

($a > 1$, $1 + 2^a + 2^{2a} + \dots + 2^{(b-1)a} > 1$)

по Ueno' n $\frac{19n+7}{7n+11} \in \mathbb{N}$

$19n+7 = k \cdot 7n + 11k$

$n(19-7k) = 11k - 7$

$n = \frac{11k-7}{19+7k} > 0$

Mersenova prvočísla

známe 48

$M_p = 57885161$

$2^{M_p} - 1 >$ 17 miliard cifer

$2^n + 1$

$A^n + B^n$ pro liché

Věta: je-li n složené ~~$n=0$~~ $= ak$, k liché > 1, $a \geq 1$, pak $2^n + 1$ složené

Dk: $\Leftarrow$ $2^n + 1$ prvočíslo $\Rightarrow n = 2^m \; \forall m \in \mathbb{N}$

$$2^{n \cdot k} + 1 = (2^a)^k + 1 = (2^a + 1)\underbrace{(1 + 2^{2a} + \dots + 2^{(k-1)a})}_{>1}$$

($2^a + 1 > 1$)

$\Rightarrow 2^{n+1}$ složené

$\Rightarrow 2^{2^m} + 1$ mohou být prvočíslo

m-té Fermatovo číslo

$2^{2^0} + 1 = 3$

$2^{2^1} + 1 = 5$

$2^{2^2} + 1 = 17$

$2^{2^3} + 1 = 257$ ✓

$2^{2^4} + 1 = 65537$ ✓

$2^{2^5} + 1 \; \cancel{\in} \; \mathbb{P}$, 641 je dělitelem

$f_{3329780}$ je složené, f_{23}, f_{20} je složené, ale nemůže se dělit

Každý dělitel Fermatova čísla $k 2^{n+2}+1$

je p^{2n}.

pravidelný n-úhelník

jde sestrojit $\Leftrightarrow n = 2^k \underbrace{f_{n_1} f_{n_2} \cdots f_{n_k}}_{\text{Fermatova čísla}}$

Každá 2 Fermatova čísla jsou nesoudělná

V $\text{nsd}(f_n, f_m) = 1$

Lemma

$$n \geq 1 \quad \prod_{k=0}^{n-1} f_k = f_n - 2$$

$n = 1$ ✓

$n \to n+1$

$$\prod_{k=1}^{n} f_k = \prod_{k=1}^{n-1} f_k \cdot f_n = (f_n - 2) f_n =$$

$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = f_{n+1}$$

dk V

$n < m$

$$f_n = \prod_{k=1}^{m-1} f_k = f_1 \cdot f_2 \cdots f_n \cdots f_{m-1}$$

$d \mid f_n \Rightarrow d \mid f_n - 2 \Rightarrow d = \pm 1$

jsou lichá

důkaz: nekonečně prvočísel

n - té prvočíslo $\leq f_{n-1} = 2^{2^{n-1}} + 1$

strašný prof. Nasákové - vzorový test

10 příkladů 1 za kod, 5 kodů poměr

10 příkladů pojmy a definice

① Najděte poslední cifru čísla 3^{17} v 10 soustavě

$3^2 \equiv 9 \bmod 10$

$3^3 \equiv 7 \bmod 10 \quad / \cdot 3$

$3^4 \equiv 1 \bmod 10 \quad / \cdot 3^4$

~~$3^8 \equiv 1 \bmod 10$~~

$3^8 \equiv 1 \bmod 10$

$3^{12} \equiv 1 \bmod 10$

$3^{16} \equiv 1 \bmod 10$

$3^{17} \equiv 3 \bmod 10$

$(17)_{10} = 10001_2$

② Kritérium dělitelnosti v libovolné soustavě pro 3

$f(2)\ n = a_k \cdot 2^k + a_{k-1} 2^{k-1} + \dots + a_1 \cdot 2 + a_0$

$f(1) = a_k + a_{k-1} + a_{k-2} + \dots + a_1 + a_0$

$f(2) \equiv f(1) \bmod 3$