

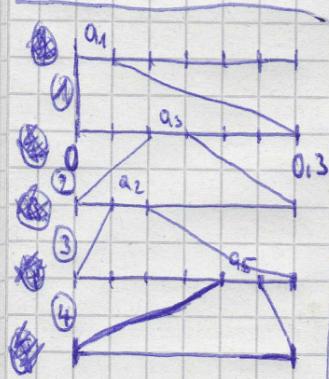
22.1.18; 9:30-11:00; G-G313

1. Uvažujte zdrojovou abecedu

znak	a_1	a_2	a_3	a_4	a_5	a_6
pst.	0,3	0,2	0,15	0,15	0,15	0,05

. Pomocí metody DFWLD zakódujte slovo $a_1a_3a_2a_5$.
2. Určete, kolika nulami končí číslo $700!$ Svůj postup řádně zdůvodněte!
3. a) Určete počet generátorů grupy $(Z_{14 \cdot 141 \cdot 875}, +)$. b) Vypište všechny podgrupy (včetně nevlastních) grupy $(Z_{10}, +)$ a všechny jejich generátory.
4. Vyřešte soustavu kongruencí $22x \equiv 84 \pmod{15}$, $16x \equiv 42 \pmod{9}$, $17x \equiv 49 \pmod{10}$, $15x \equiv 21 \pmod{8}$. Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.
5. Nechť $f(x), g(x) \in Z_7[x]$, kde $f(x) = 6x^5 + 6x^3 + 3x^2 + 6x + 1$, $g(x) = 4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2$. Pomocí Eukleidova algoritmu spočtěte $NSD(f(x), g(x))$. Výsledek zapište jako monický polynom s koeficienty ze soustavy nejmenších nezáporných zbytků.

1. Uvažujte rozložení abecedy $\{a_1, a_2, a_3, a_4, a_5, a_6\}$. Pomocí metody DFWLD zápisujte slovo $a_1 a_3 a_2 a_5$.



$$\langle \Delta_1, \Delta + l \rangle$$

$$\langle \Delta_1, \epsilon \rangle \quad l = e - s$$

start end length (délka)

Začínáme s intervalenem $\langle 0, 1 \rangle$ a ten postupně shrávajeme podle pravděpodobnosti jednotlivých slov, co hledáme.

První, které hledáme.

$$\Delta_i = \Delta_{i-1} + l_{i-1} \left(\sum_{j=0}^{i-1} a_j \right) - \text{kde } k \text{ je index rnačky od } 0 \quad (a_1 \Rightarrow k=1)$$

Nedopodložíme, že $a_0 = 0$

Hledané a_1 : ① $\Delta_1 = 0 + 1 \cdot 0 \quad l_1 = 1 \cdot 0,3$
 $a_1 = 0 \quad l_1 = 0,3 \quad \langle 0; 0,3 \rangle$

$$l_i = l_{i-1} \cdot a_i$$

Hledané a_3 : ② $\Delta_2 = 0 + 0,3 \cdot (0,3 + 0,2) \quad l_2 = 0,3 \cdot 0,15 \quad \langle 0; 0,15 \rangle$
 $a_2 = 0,15 \quad l_2 = 0,045$

Hledané a_2 : ③ $\Delta_3 = 0,15 + 0,045 \cdot (0,3) \quad l_3 = 0,045 \cdot 0,2 \quad \langle 0,1635; 0,1635 \rangle$
 $a_3 = 0,1635 \quad l_3 = 0,009$

Hledané a_5 : ④ $\Delta_4 = 0,1635 + 0,009 \cdot (0,3 + 0,2 + 0,15 + 0,15) \quad l_4 = 0,009 \cdot 0,15$
 $a_4 = 0,1707 \quad l_4 = 0,00135$

interval $\langle 0,1707, 0,1707 + 0,00135 \rangle$ neboli $\langle 0,1707; 0,17205 \rangle$

Výpočet reprezentanta (DFWLD)

dyadický slounek - slounek, kde jinovatelská možností jsou 2 neboli $\frac{a}{2^k}, a \in \mathbb{Z}$

$$R = \frac{\bar{x}}{2^k} \quad \text{všechny } R \in \langle 0,1707; 0,17205 \rangle$$

Nejmenší možné k : $\frac{1}{2^k} < \ln \frac{1}{2^{k-1}}$

$$\frac{1}{2^k} \leq 0,00135 < \frac{1}{2^{k-1}}$$

délka výplňky
intervalu

$$\frac{1}{2^k} \leq 0,00135 < \frac{1}{2^{k-1}} \quad (\log_2)$$

$$-1 \log_2 2 \leq \log(0,00135) < (-k+1) \log_2 2$$

$$-1 \leq \log(0,00135) < -k+1$$

$$1 \leq -9,53 < -1+1$$

$$1 \geq 9,53 \quad 1-1 < 9,5328$$

$$\boxed{L=10}$$

Umiření \bar{x} : $\Delta \leq \frac{\bar{x}}{2^k} \leq \epsilon$ - například $R \in \langle \Delta, \epsilon \rangle$

$$0,1707 \leq \frac{\bar{x}}{2^{10}} < 0,17205 / \cdot 2^{10}$$

$$174,797 \leq \bar{x} < 176,1792$$

hledané přesné číslo: 175 176

přesné součet čísla $\boxed{\bar{x}/2^k}$

$$\boxed{\bar{x} = 176}$$

$$R = \frac{176}{2^{10}} = \frac{2^4 \cdot 11}{2^{10}} = \frac{11}{2^6}$$

$$\frac{11}{2^6} = \frac{1011_2}{1000000_2} = 0,00\overline{1011}$$

exponent může počítat množství zadání čísel

2. Vrčete, kolika nulami končí číslo 700! (najděte řádky)

Faktoriál stačí vydělit možnými čísly 5 a zůstává se 1.

$$700 : 5 = 140$$

$$700 : 25 = 28$$

$$700 : 125 = 5,6 \rightarrow \text{zbytek nás nezajímá (doplň celou číslo)}$$

$$700 : 625 = 1,12$$

$$\underline{174} \rightarrow \text{Číslo } 700! \text{ končí } 174 \text{ nulami.}$$

Jak určit, kolik má číslo na konci nul?

Tolik faktoriál je násobek 10. $1000 = 10^3 = 3$ nuly

Císlo 10 lze rozložit na dva díly 5 a 2. Z toho plyne, že kardí číslo 5. Kde má v rozložení čísla 2 a 5 je násobek 10. $1000 = 2^3 \cdot 5^3 = 3$ nuly

Jak ale rychle počít nul u faktoriálu, když nemáme jeho rozložení?

$$700! = 700 \cdot 699 \cdot 698 \cdot 697 \dots$$

Stojí se na faktoriál dílčí jako na postupnost násobků. Kardí 5.

Císlo je dělitelné 5, když má v rozložení číslo 5. A co ta drojka?

V rozložení faktoriálu bude mít víc Čísel dvě než pět (protože sudých čísel je v rozmezí 1 až 700 více než čísel dělitelných pěti). Proto stačí rychle počít kolik má faktoriál v rozložení pěti.

Pozor na to, že kardí 25. číslo nemá v rozložení jednu, ale dvě pětky a když to samozřejmě platí i pro další množiny čísla 5.

$$700 : 5 = 140 \dots \text{kardí 5. číslo}$$

$$700 : 25 = 28 \dots \text{kardí 25. číslo - číslo 25 má sice rozložod } 5^2 \\ \text{ale započítáváme ho jen jednou, protože už jsme ho jednou zahrnuli (kardí 5. číslo v předchozím kroku)}$$

$$700 : 125 = 5$$

$$700 : 625 = 1$$

$$\underline{174} - \text{číslo } 700! \text{ má v rozložení } 5^{174} \rightarrow \text{má 174 nul}$$

2. 3. a) Počet generátorů grupy $(\mathbb{Z}_{141875}, +)$

úplná soustava rytmů
modulo m = 141875

aditivní operace
(sčítání modulo m)

Generátor grupy $\langle G, \ast \rangle$ - generátor je počet z množiny G , na který když aplikujeme operaci \ast nejdříve generuje celou množinu G .

- pro sčítání $(+)$ - $a+a+a\dots$
- pro nasobení (\cdot) - $a.a.a\dots$

Jak určíme počet generátorů pro také někou množinu?

Počet generátorů grupy $(\mathbb{Z}_m, +)$ je počet nesoudělných prvků z \mathbb{Z}_m s moduluem m.

Příklad: $(\mathbb{Z}_4, +)$ $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

pro 0: $0+0=0$ - není generátor
pro 1: $1+1=2$ $2+1=3$ $3+1=0$ $0+1=1\dots$

$\angle 1 \rangle$ je generátor

pro 2: $2+2=0$ $0+2=2$ - není generátor

pro 3: $3+3=2$ $2+3=1$ $1+3=0$ $0+3=3$

$\angle 3 \rangle$ je generátor

$\varphi(4) = (2^2 - 2^1) = 2$ - počet generátorů
pro $(\mathbb{Z}_m, +)$

Počet nesoudělných prvků zjistíme pomocí Eulerovy věty.

$$\text{pro } m = 141875 \text{ když } \varphi(m) = (5^4 - 5^3) \cdot (11^3 - 11^2) \cdot (17^1 - 17^0) = \underline{\underline{9680000}}$$
$$141875 = 5^4 \cdot 11^3 \cdot 17$$

Grupa $\langle \mathbb{Z}_{141875}, + \rangle$ má 9 680 000 generátorů.

b) Výpis všech podgrup (všechny nevlasních) grupy $(\mathbb{Z}_{10}, +)$ a všechny její generátory.

Obecně pro podgrupy grupy \ast musí platit: a) $H \subseteq G$ - H je podmnožina G
(H, \ast) (G, \ast)

b) $\ast = \ast - (H, \ast) \cap (G, \ast)$ musí mít stejnou operaci

(POZOR NATO že sčítání modulo 5 JE

JINÁ OPERACE NEŽ SČÍTÁNÍ MODULO 6!)

c) (H, \ast) je uspořádání méně operací grupy (G, \ast)

(neboli H je kote' grupa)

Vlastní podgrupy

$(\{0, 2, 4, 6, 8\}, +) - \langle 2 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 8 \rangle$

$(\{0, 5\}, +) - \langle 5 \rangle$

$\boxed{+}$ - zde představuje operaci
sčítání modulo 10

$(\mathbb{Z}_5, +)$ nem' podgrupy $(\mathbb{Z}_{10}, +)$
protože tyto grupy nemají stejnou operaci!

4. Vyřešte soustavu Kongruencí $22x \equiv 84(15), 16x \equiv 42(9), 17x \equiv 49(10), 15x \equiv 21(8)$.

Výsledek rapsite v soustavě nejmenších pozitivních reálných odpovídajících modulu.

$$22x \equiv 84(15) \quad | :15 \quad 16x \equiv 42(9) \quad | :9 \quad 17x \equiv 49(10) \quad | :10 \quad 15x \equiv 21(8) \quad | :8$$

$$7x \equiv 9(15)$$

$$7x \equiv 6(9)$$

$$7x \equiv 9(10)$$

$$7x \equiv 5(8)$$

Riešení kongruencie 1. skupiny
NSD(m₁, a)

$$15 = 7 \cdot 2 + 1$$

$$7 = 1 \cdot 7 + 0$$

$$\begin{array}{r|rr} 1 & -1 & 0 & 1 \\ \hline 9 & 1 & 2 & 7 \\ \hline 1 & 1 & 2 & \equiv \end{array}$$

$$x \equiv (-1)^1 \cdot 2 \cdot 9(15) \equiv -18(15)$$

$$\underline{x_1 \equiv 12(15)}$$

$$\underline{x_2 \equiv 6(9)}$$

$$\underline{x_3 \equiv 7(10)}$$

$$\underline{x_4 \equiv 3(8)}$$

①. převod kongruencí $a_i x_i \equiv b_i(m_i)$

na $x_i \equiv b_i(m_i)$

②. Výsledný modul $M = \text{NSN}(b_1, b_2, b_3, b_4) \Rightarrow M = \text{NSN}(15, 9, 10, 8) = 360$

③. jednotlivé moduly M_i : platí $M = M_1 \cdot M_2 \cdots M_n$

$$\prod M_i \mid m_i$$

$\forall i \neq j \quad \text{NSD}(M_i, M_j) = 1$ - násobky moduly jsou mezi sebou nezávislé

Náhodná souprava:

5	9	1	8
M_1	M_2	M_3	M_4

$$\begin{aligned} 15 &= 3 \cdot 5 \\ 9 &= 3^2 \\ 10 &= 2 \cdot 5 \\ 8 &= 2^3 \end{aligned}$$

④. Určení $c_i \equiv g_i$

$$\frac{M}{M_i} c_i \equiv 1(M_i)$$

$$1 \bmod 1 = 0$$

$$\frac{M}{M_1} c_1 \equiv 1(M_1)$$

$$40c_1 \equiv 1(9)$$

$$360c_3 \equiv 1(1)$$

$$45c_4 \equiv 1(8)$$

$$\frac{360}{5}c_1 \equiv 1(5)$$

$$4c_2 \equiv 1(9)$$

$$\underline{c_3 \equiv 0(1)}$$

$$5c_4 \equiv 1(8)$$

$$72c_1 \equiv 1(5)$$

$$\underline{\underline{c_2 \equiv 7(9)}}$$

$$2c_1 \equiv 1(5)$$

$$c_1 \equiv 3(5)$$

$$\underline{\underline{c_1 \equiv 3(5)}}$$

- b_i - jsou z upraveného kongruence

m 1. složka

⑤. Dosazení

$$x = \frac{M}{M_1 \cdot g_1 \cdot b_1} + \frac{M}{M_2 \cdot g_2 \cdot b_2} + \dots + \frac{M}{M_n \cdot g_n \cdot b_n}$$

$$x \equiv \frac{360}{5} \cdot 3 \cdot 12 + \frac{360}{9} \cdot 7 \cdot 6 + \frac{360}{1} \cdot 0 \cdot 7 + \frac{360}{8} \cdot 5 \cdot 3 (360)$$

$$x \equiv 4947 (360)$$

$$\underline{\underline{x \equiv 267(360)}}$$

$$5. \text{ Nechť } f(x), g(x) \in \mathbb{Z}_7[x], \text{ kde } f(x) = 6x^5 + 6x^3 + 3x^2 + 6x + 1, g(x) = 4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2$$

Pomocí Euklidova algoritmu spočítáte NSD($f(x), g(x)$). Výsledek zapíšte jako monický polynom

→ koeficienty re soustavy nějmenších nezajímajících řežek.

(pořizujeme stejně jako u celých čísel.)

$$\boxed{f(x) = q(x) \cdot g(x) + r(x)}$$

$$\begin{aligned} 1.) (6x^5 + 6x^3 + 3x^2 + 6x + 1) : (4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2) &= 5 + (5x^4 + 4x^3 + 5x + 5) \\ - (6x^5 + 2x^4 + 2x^3 + 3x^2 + x + 3) \end{aligned}$$

$$\underline{5x^4 + 4x^3 + 5x + 5} = q(x) \cdot g(x) + r(x)$$

$$\text{, když } (6x^5 + 6x^3 + 3x^2 + 6x + 1) = 5 \cdot (4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2) + 5x^4 + 4x^3 + 5x + 5$$

2. dělání problém je:

$$\boxed{q(x) = q_1(x) \cdot r(x) + r_1(x)}$$

$$\begin{aligned} (4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2) : (5x^4 + 4x^3 + 5x + 5) &= 5x + (6x^2 + 5x^2 + 6x + 2) \\ - (4x^5 + 6x^4 + 4x^3 + 4x) \end{aligned}$$

$$\underline{6x^2 + 5x^2 + 6x + 2} = q_1(x) \cdot r(x) + r_2(x)$$

$$\text{, když } (4x^5 + 6x^4 + 6x^3 + 2x^2 + 3x + 2) = 5x \cdot (5x^4 + 4x^3 + 5x + 5) + (6x^2 + 5x^2 + 6x + 2)$$

3. dělání problém je:

$$\boxed{r(x) = q_2(x) \cdot r_2(x) + r_3(x)}$$

$$(5x^4 + 4x^3 + 5x + 5) : (6x^2 + 5x^2 + 6x + 2) = 2x + 6 \quad \text{nb} = 0$$

$$-(5x^4 + 3x^3 + 5x^2 + 4x)$$

$$\underline{x^3 + 2x^2 + x + 5}$$

$$-(\underline{x^3 + 2x^2 + x + 5})$$

$$0$$

$$\text{Když } 5x^4 + 4x^3 + 5x + 5 = 2x \cdot (6x^2 + 5x^2 + 6x + 2) + 0$$

NSD - poslední nenulový slounek - $6x^2 + 5x^2 + 6x + 2$

Převod na monický polynom - největšího řádu je roven 1.

$$(6x^2 + 5x^2 + 6x + 2) \cdot 6 = \underline{\underline{x^3 + 2x^2 + x + 5}}$$