

Alena Gollová
gollova@fel.wut.cz

<http://pitbul.pcland.cz>

konzultace: St 14-15 hod

katedra mat, dveře $\in$ 6 proti dveřím

+ domluvit jinak

sápočet: docházka (max 4 řádné oml. absence)

literatura: math. feld - Velebil - skripta DML
paráta o počítání v $\mathbb{Z}_n$ + dodatek o polynomech

math.feld.wut.cz/gollova - poznámky ze cvičení

①

Počítání v $\mathbb{Z}_m$

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ - klyšové třídy modulo m

přesněji: $\mathbb{Z}_m = \mathbb{Z}/\equiv(\text{mod } m)$ - celá čísla rozbita na třídy dle kongruence modulo m

$$a \equiv b (\text{mod } m) \text{ iff } a - b = k \cdot m \text{ pro } k \in \mathbb{Z}$$

$$\text{iff } a = b + k \cdot m$$

iff a, b mají stejný zb. po dělení m

$$0 = [0]_m = \{0, m, 2m, 3m, \dots, -m, -2m, \dots\} = \{k \cdot m; k \in \mathbb{Z}\}$$

$\text{Relace } \equiv (\text{mod } m)$ je zachována při sčítání a násobení tudíž lze sčítání a násobení definovat po třídách

$$[a] + [b] = [a + b]$$

$\Rightarrow$ při $+$, $\cdot$ lze čísla nahradit zb. modulo m (počítáme-li v $\mathbb{Z}_m$)

Př. $\mathbb{Z}_7$ $2 \cdot 6 + 4 = 8 \cdot 6 + 4 = 1 \cdot 6 + 4 = 10 = 3$

Lineární rovnice v $\mathbb{Z}_m$

$$a \cdot x = b \text{ v } \mathbb{Z}_m$$

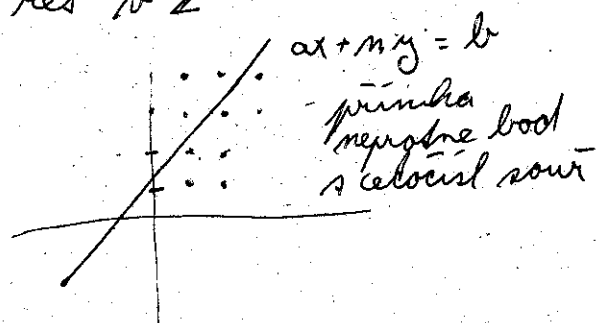
$$a \equiv b (\text{mod } m)$$

$$\hookrightarrow \boxed{ax + my = b} \text{ v } \mathbb{Z}$$

pro $a, b \in \mathbb{Z}_m$ hledáme mex. $x \in \mathbb{Z}_m$

Diophantická rovnice
(hledání řeš. v $\mathbb{Z}$)

pokud $\gcd(a, m)$ nedělí pravou stranu b , pak rovnice
(greatest common divider)
nemá řeš v $\mathbb{Z}$



pokud $\gcd(a, m)$ dělí číslo b , pak je nekonečně mnoho řeš. v $\mathbb{Z}$
které lze psát $(x, y) = (x_p, y_p) + k(x_0, y_0) \rightarrow$ je $\gcd(a, m)$

part. řeš.
(rozšířený Eukl. alg.)

nesouditelné řeš.
přidružen. homog. rov.

pak stačí brát $k \in \mathbb{Z}$

(Kdyby např. 2 dělila x_0, y_0 , tak pro
 $k = \frac{1}{2}$ vyjde $x, y \in \mathbb{Z}$)

Př. $9x = 6 \quad \text{v } \mathbb{Z}_{12}$

$9x + 12y = 6 \quad \text{v } \mathbb{Z}$

$\gcd(9, 12) = 3$ dělí 6 $\rightarrow$ exist. řeš. (budou 3)

$3x + 4y = 2$

Part. řeš. - uhradíme

$x_p = 2, y_p = -1$

Nesouditelné řeš. homog. rov.

$3x + 4y = 0$

$x_0 = 4, y_0 = -3$

Obsah v $\mathbb{Z}$

$x = 2 + k \cdot 4$

$y = -1 - k \cdot 3$ pro $k \in \mathbb{Z}$

$$\text{V } \mathbb{Z}_{12} \quad x_1 = 2 \quad (k=0)$$

$$x_2 = \cancel{6} 6 \quad (k=1)$$

$$x_3 = 10 \quad (k=2)$$

$$x_4 = 14 = 2 \quad (\text{pro } k=3 \text{ vyjde totéž v } \mathbb{Z}_{12} \text{ jako pro } k=0)$$

$$\underline{\text{Pr}} \quad 9x = 5 \quad \text{v } \mathbb{Z}_{12}$$

$$9x + 12y = 5$$

$$\text{gcd}(9, 12) = 3 \text{ nedělí } 5 \rightarrow \text{neexist. řešení v } \mathbb{Z}$$

$$\underline{\text{Pr}} \quad \text{Úloha Diofantova: najdi } 90x + 126y = 54$$

Eukleidov algoritmus na nalezení $\text{gcd}(90, 126)$

$$(1) \quad 126 = 90 + 36$$

$$(2) \quad 90 = 2 \cdot 36 + \boxed{18}$$

$$(3) \quad 36 = 2 \cdot 18 + 0$$

$$\text{gcd}(90, 126) = 18$$

$$54 = 3 \cdot 18 \rightarrow \text{exist. řeš. v } \mathbb{Z}$$

Bézantova věta: $\text{gcd}(a, b) = k \cdot a + l \cdot b$ pro $k, l \in \mathbb{Z}$
celočís. kombinace

$$\begin{aligned} 18 &= 90 - 2 \cdot 36 = 90 - 2 \cdot (126 - 90) = (-2) \cdot 126 + 3 \cdot 90 \\ (2) \quad & \quad (1) \end{aligned}$$

$$\begin{aligned} 54 &= 3 \cdot 18 = 3 \left((-2) \cdot 126 + 3 \cdot 90 \right) = (-6) \cdot 126 + 9 \cdot 90 \\ & \quad \uparrow \quad \quad \quad \uparrow \\ & \quad y \quad \quad \quad x \end{aligned}$$

$$(x_p, y_p) = (9, -6)$$

Nesouditel. řes. hom. rov

$$90x + 126y = 0$$

$$| : \text{gcd} = 18$$

$$5x + 7y = 0$$

$$x_0 = 7, y_0 = -5$$

Obecné řes. v $\mathbb{Z}$:

$$x = 9 + 7k$$

$$y = -6 - 5k$$

pro $k \in \mathbb{Z}$

PA

$$\vee \mathbb{Z}_{204} \text{ řes. } 150x = 6$$

$$\hookrightarrow 150x + 204y = 6$$

$$\text{gcd}(150, 204)$$

Rekurzivní Eukleidův algoritmus
při hledání společného dělitele pomocí kombinací
relativních čísel (zde 204, 150)

$$(1) \quad 204 = 150 + 54$$

$$(1) \quad 54 = \underline{204} - \underline{150}$$

$$(2) \quad 150 = 2 \cdot 54 + 42$$

$$(2) \quad 42 = \underline{150} - 2 \cdot 54 = 150 - 2(204 - 150) = -2 \cdot 204 + 3 \cdot 150$$

$$(3) \quad 54 = 42 + 12$$

$$(3) \quad 12 = 54 - 42 = 204 - 150 + 2 \cdot 204 - 3 \cdot 150 = 3 \cdot 204 - 4 \cdot 150$$

$$(4) \quad 42 = 3 \cdot 12 + \boxed{6} \text{ gcd}$$

$$(4) \quad 6 = 42 - 3 \cdot 12 = -2 \cdot 204 + 3 \cdot 150 - 9 \cdot 204 + 12 \cdot 150 =$$

$$(5) \quad 12 = 2 \cdot 6 + 0$$

$$= \underline{15 \cdot 150} - \underline{11 \cdot 204}$$

x_p

y_p

Nesouditel. řes. hom. rov

$$150x + 204y = 0 \quad | : \text{gcd} = 6$$

$$25x + 34y = 0$$

$$x_0 = 34, y_0 = -25$$

Obecné v $\mathbb{Z}$:

$$x = 15 + 34k$$

$$y = -11 - 25k$$

pro $k \in \mathbb{Z}$

V $\mathbb{Z}_{204}$: $\text{gcd} = 6$ různých řeš ($k=0,1,\dots,5$)

$$x_1 = 15 ; \quad x_2 = 49 ; \quad \text{~~183~~ } x_3 = 83 ;$$

$$x_4 = 117 ; \quad x_5 = 151 ; \quad x_6 = 185$$

Inverzní prvek k a v $\mathbb{Z}_m$

je a^{-1} takové, že $a \cdot a^{-1} = 1$ v $\mathbb{Z}_m$.

$\rightarrow a^{-1}$ je řešením rovnice $ax = 1$ v $\mathbb{Z}_m$

Tedy a^{-1} existuje jen pro a nesoudělné s m
(neboť rov. má řeš., pokud $\text{gcd}(a,m)$ dělí 1)

PH Najít 13^{-1} v $\mathbb{Z}_{44}$

$\text{gcd}(13,44) = 1 \rightarrow$ existuje 13^{-1} v $\mathbb{Z}_{44}$

$$13^{-1} = x, \text{ kde } 13x = 1 \text{ v } \mathbb{Z}_{44}$$

$$13x + 44y = 1$$

$$44 = 3 \cdot 13 + 5$$

$$5 = 44 - 3 \cdot 13$$

$$13 = 2 \cdot 5 + 3$$

$$3 = 13 - 2 \cdot 44 + 6 \cdot 13 = 7 \cdot 13 - 2 \cdot 44$$

$$5 = 3 + 2$$

$$2 = 44 - 3 \cdot 13 + 2 \cdot 44 - 7 \cdot 13 = 3 \cdot 44 - 10 \cdot 13$$

$$3 = 2 + 1$$

$$1 = 17 \cdot 13 - 5 \cdot 44$$

$$2 = 2 \cdot 1 + 0$$

$$\begin{array}{ccc} \parallel & & \parallel \\ x_p & & y_p \end{array}$$

$$x_0 = 44, y_0 = -13$$

$$x_1 = 17 + 1 \cdot 44$$

$$\underline{\underline{13^{-1} = 17}}$$

$$\hookrightarrow \text{v } \mathbb{Z}_{44} \quad x = 17$$

01 Kolik prvků má inverz. v $\mathbb{Z}_n$?

v $\mathbb{Z}_p$ vs. prvky kromě 0 (tj $p-1$ prvků)
prvočíslo

v $\mathbb{Z}_n$ vs. nesoudělné s n (mezi 0 a $n-1$)

Eulerova fce $\varphi(n)$ = počet čísel mezi 0 a $n-1$,
která jsou nesoudělná s n

$$\text{Platí: } \varphi(p) = p-1$$

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

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \text{ jen pro } m, n \text{ nesoudělné}$$

→ Známe-li prvočísl. rozklad pro $n = p_1^{k_1} \dots p_m^{k_m}$,
pak spočteme $\varphi(n) = \varphi(p_1^{k_1}) \cdot \dots \cdot \varphi(p_m^{k_m})$

Pr Kolik prvků má inverz v $\mathbb{Z}_{44}$?

$$= \varphi(44) = \varphi(2^2 \cdot 11) = \varphi(2^2) \cdot \varphi(11) = (4-2) \cdot 10 = \underline{\underline{20}}$$

Umocňování v $\mathbb{Z}_n$

Euler-Fermatova věta: Pro a nesoudělné s n je

$$a^{\varphi(n)} = 1 \text{ v } \mathbb{Z}_n$$

→ Exponent se dá snížit modulo $\varphi(n)$

$$a^k = a^{k_2 \cdot \varphi(n) + k_1} = (a^{\varphi(n)})^{k_2} \cdot a^{k_1} = 1^{k_2} a^{k_1} = a^{k_1} \text{ v } \mathbb{Z}_n$$

(2)

Umocňování v $\mathbb{Z}_m$

Pr $5^{64} \text{ v } \mathbb{Z}_{18}$

$\gcd(5, 18) = 1$ --- lze užit E-Friedm

$5^{\varphi(18)} = 1 \text{ v } \mathbb{Z}_{18}$

$\varphi(18) = \varphi(2 \cdot 3^2) =$

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

$5^{64} = 5^{6 \cdot 10 + 4} = (5^6)^{10} \cdot 5^4 =$

$= 1 \cdot 5^4 = 25^2 = 7^2 = 49 = 2 \cdot 18 + 13 =$

$= \underline{\underline{13}}$

$\rightarrow 5^6 = 1 \text{ v } \mathbb{Z}_{18}$

Pr Zbytek po dělení 26 k 115^{131}

$115^{131} = 11^{131} \text{ v } \mathbb{Z}_{26}$

$\gcd(11, 26) = 1$

$11^{\varphi(26)} = 1 \text{ v } \mathbb{Z}_{26}$

$\varphi(26) = \varphi(2 \cdot 13) =$

$= \varphi(2) \cdot \varphi(13) = 1 \cdot 12$

$= 12$

$11^{131} = 11^{12 \cdot 10 + 11} = 11^{11} =$

$= 11 \cdot (11^2)^5 = 11 \cdot 121^5 = 11 \cdot 17^5 = 11 \cdot 17 \cdot (17^2)^2 =$

$= 11 \cdot 17 \cdot 289^2 = 11 \cdot 17 \cdot 3^2 = 11 \cdot 17 \cdot 9 =$

$11 \cdot 153 = 11 \cdot 23$

Metoda opakovaných čtverců

pocítání a^b v $\mathbb{Z}_n$

jediná možnost v případě $b < \varphi(n)$

nebo pro a součet $a \equiv 1$ (nelze E-F)

Př 17^{339} v $\mathbb{Z}_{312}$

$$\text{gcd}(17, 312) = 1$$

$\rightarrow$ E-F

$$17^{\varphi(312)} = 1 \text{ v } \mathbb{Z}_{312}$$

$$\varphi(312) = ?$$

$$312 = 2 \cdot 156 = 2^2 \cdot 78 = 2^3 \cdot 39 = 2^3 \cdot 3 \cdot 13$$

$$\begin{aligned} \varphi(2^3) \cdot \varphi(3) \cdot \varphi(13) &= (2^3 - 2^2) \cdot 2 \cdot 12 = \\ &= 4 \cdot 2 \cdot 12 = 96 \end{aligned}$$

$$17^{339} = 17^{96 \cdot 3 + 51} = 17^{51} \text{ v } \mathbb{Z}_{312}$$

Metoda opak. čtverců

- postupně umocňujeme na druhou a nahrazujeme
výsl. zb. mod n

$\rightarrow$ počet umocňování $\log_2 b$

$\rightarrow$ vel. čísel $< n^2$

Algoritmus

1) napsat exponent binárně

$$b = 51 = 1 + 2^5 \cdot 2 = 1 + 2(1 + 2 \cdot 12) = 1 + 2 + 2^2 \cdot (12) =$$

$$= 1 + 2 \cdot 2^4 \cdot (2+1) = 1 + 2 + 2^4 + 2^5$$

$$b = 110011$$

2) → počet umocňování na druhou bude 5

→ napsat posloupnost pěti 5 (=square)

$$\begin{array}{cccccc} 5 & 5 & 5 & 5 & 5 & \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 5 & 4 & 3 & 2 & 1 & 0\text{-tá moc} \end{array}$$

→ do té posl. se vloží X (=times)
na místa těch mocnin dvojky, pokud se vyskytní
v bin. rozvoji exponentu

$$\begin{array}{ccccccc} X & 5 & X & 5 & 5 & 5 & X & 5 & X \\ \uparrow & & & & & & \uparrow & & \uparrow \\ 2^5 & & & & & & 2^1 & & 2^0 \end{array}$$

3) napsat posl. místo $L \rightarrow P$ khora dolů a provádět
násobení základem a (kde je X) a umocnění nadruhou
(kde je 5) + počítat v $\mathbb{Z}_n$

$\text{v } \mathbb{Z}_{312}$

$$X \quad 17^2 = \underline{17^1} = 17$$

$$S \quad (17^1)^2 = \underline{17^2} = 289 = (-23)$$

$$X \quad 17^2 \cdot 17 = \underline{17^3} = (-23) \cdot 17 = -391 = -79$$

$$S \quad (17^3)^2 = \underline{17^6} = (-79)^2 = 6241 = 1$$

$$S \quad \underline{17^{12}} = 1^2 = 1$$

$$S \quad \underline{17^{24}} = 1^2 = 1$$

$$X \quad \underline{17^{25}} = 1 \cdot 17 = 17$$

$$S \quad \underline{17^{50}} = 17^2 = -23$$

$$X \quad \underline{17^{51}} = (-23) \cdot 17 = -391 = \underline{233} \rightarrow 17^{51} = 233 \text{ v } \mathbb{Z}_{312}$$

RSA šifrování

$N = p \cdot q$ kde p, q jsou velká prvočísla (obecně 15 místná)

$$\varphi(N) = (p-1)(q-1) \quad \leftarrow \text{le spočítat jen když známe } p, q$$

volíme t nesoudělné s $\varphi(N)$ $\rightarrow t$ má inverz v $\mathbb{Z}_{\varphi(N)}$
($\in \mathbb{Z}_{\varphi(N)}$)

$$\text{spočtem si } s = t^{-1} \text{ v } \mathbb{Z}_{\varphi(N)}$$

Zveřejníme (N, t) - tzv. veřejný klíč

Kdo mi pošle správu, tak ji šifruje

$$a \rightsquigarrow b = a^t \text{ v } \mathbb{Z}_N$$

(Pokud p správa $> N$, tak ji rozložíme na k-tice

$$\text{tak aby } \underbrace{9 \cdot 10^k}_{10^{k+1}} < N$$

Souborný klíč (N, s)

Dešifruje: $b \rightarrow b^s \text{ v } \mathbb{Z}_N$

platí: $b^s = a$

$$\begin{aligned} \text{Dk: } b^s &= (a^t)^s = a^{t \cdot s} = & \left| \begin{array}{l} s = t^{-1} \rightarrow t \cdot s = 1 \text{ v } \mathbb{Z}_{\varphi(N)} \\ t \cdot s = 1 + k \cdot \varphi(N) \end{array} \right. \\ &= a^{1+k \cdot \varphi(N)} = a^1 \end{aligned}$$

pro a nesoud s N : E-F

pro a soud s N

- aby funguje, $b^s = a$, dk k Čínské v.o. sb.

Pří Znáte veřejný klíč $(N=1469, t=5)$

Zachytili jste 2 zprávy $b_1=108, b_2=83$

Pokuste se rozbit N na prvočísla, dopočítejte soukromý klíč a dešifrujte,

1) $N = p \cdot q$

$$1469 = 13 \cdot 113$$

pro soukromé prvočís $< \sqrt{N} \approx 38$

2, 3, 5, 7, 11, 13

2) $\varphi(N) = \varphi(13 \cdot 113) = 12 \cdot 112 = 1344$

$$s = t^{-1} \text{ v } \mathbb{Z}_{\varphi(N)}$$

$$s = 5^{-1} \text{ v } \mathbb{Z}_{1344}$$

$$a_2 = 83^{269} \text{ v } \mathbb{Z}_{1469}$$

$s=269$ - stejná posl. X a S

výjde $a_2 = 424$

Zpráva $a = a_1 a_2 = \overbrace{010}^D \overbrace{424}^{EY}$

potřebuji $a_i < 1469 \rightarrow$ rozložit zprávu po 3 cifrách

Angl. abeceda - 26 písmen

A	B	C	...	Y	Z
↓	↓			↓	↓
00	01			24	25

(3)

Řád prvků v grupě, cyklická grupa

grupa $(G, *)$ = množ. G , na které je def binární operace

$$* : G * G \rightarrow G$$

s vlastnostmi

$*$ je asociativní $(a * b) * c = a * (b * c)$

$*$ má neutrální prvek e $\forall a \in G$ je $e * a = a = a * e$

$*$ má všechny inverzy

Plati: pro lib $a \in G$, G grupa

výjde $a^{|G|} = e = 1$

Def: nejmenší $k \in \mathbb{N} + \bar{\mathbb{Z}}$ $a^k = e$ se nazývá
řád prvku a v grupě G . Značí se $\kappa(a) = k$

Def: $|G| =$ řád grupy

Platí: Řád podgrupy P v grupě G dělí řád grupy G

$$|P| \cdot e = |G| \quad \text{pro } e \in \mathbb{N}$$

Def: Grupa G je cyklická, pokud exist. $a \in G$ $\neq e$.
Každý $g \in G$ je tvaru $g = a^k$ pro vhodné $k \in \mathbb{N}$

$$G = \langle a \rangle = \{a, a^2, a^3, \dots, a^{\kappa(a)}\} \rightarrow a = \text{generator}$$

$$\rightarrow |G| = \kappa(a)$$

Důsledek: $\kappa(a)$ dělí $|G|$, protože $\kappa(a) = |\langle a \rangle| = \text{dělitel } |G|$

$(\mathbb{Z}_m, \cdot)$ je to grupa? např. 0^{-1} nebylo

$$(\mathbb{Z}_p \setminus \{0\}, \cdot) \quad \text{ANO}$$

$$(\mathbb{Z}_m \setminus \{a \text{ soudělná s } m\}, \cdot) \quad \text{ANO}$$

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}, \text{ exist } a^{-1}\} = \{a \in \mathbb{Z}_m, \text{ gcd}(a, m) = 1\}$$

$$(\mathbb{Z}_m^*, \cdot) \quad \text{je grupa}$$

ověření: • funkce invert. $\mathbb{Z}_m^*$

- když $a, b \in \mathbb{Z}_m^*$ (tj. a^{-1}, b^{-1} exist.) $\rightarrow c = a \cdot b \in \mathbb{Z}_m^*$, tj.

$$\text{exist } c^{-1} = a^{-1} \cdot b^{-1} \quad (ab) \cdot (a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \cdot 1 = 1$$

Pozn: pro obecný monoid (množ s bin. relací - asoc. a má neutrální) $(M, *)$ je $M^* = \{a \in M, \text{ exist } a^{-1}\}$ grupa jen $(a.b)^{-1} = b^{-1}a^{-1}$ neboť nemusí platit $ab = ba$.
 $(a.b)(b^{-1}a^{-1}) = a(b.b^{-1})a^{-1} = a.1.a^{-1} = a.a^{-1} = 1$

- je asoc

má neutrální $1 \in \mathbb{Z}_n^*$

vs $a \in \mathbb{Z}_n^*$ mají inverze v $\mathbb{Z}_n^*$

Víme $a^{-1} \in \mathbb{Z}_n$ - je $a^{-1} \in \mathbb{Z}_n^*$? ANO, neboť

má inverze $(a^{-1})^{-1} = a$

$$|\mathbb{Z}_n^*| = \varphi(n)$$

$\Rightarrow \kappa(a)$ je dělitel $\varphi(n)$

Pr $(\mathbb{Z}_9, \cdot)$ monoid

grupa $(\mathbb{Z}_9^*, \cdot)$ najít řády všech prvků v $\mathbb{Z}_9^*$

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$$

← nesoudělná s 9

$$\varphi(9) = 3^2 - 3 = 6$$

$\kappa(a)$ je nejmenší číslo z $\mathbb{N}$, že $a^{\kappa(a)} = 1$ v $\mathbb{Z}_9$

$$a = 1 \quad \kappa(1) = 1$$

$$a = 2 \quad \kappa(2) = 6$$

$$2^1, 2^2=4, 2^3=8, 2^4=16=7, 2^5=32=5$$

$$2^6=64=1$$

$$\Rightarrow \kappa(2) = 6$$

$$a = 4 \quad \kappa(4) = 3$$

$$3^1, 3^2=9, 3^3=27=3 \quad 4^1, 4^2=16=7, 4^3=64=1$$

$$a=8 \quad n(p)=2 \quad p^1, p^2=64=1$$

$$a=5$$

$$a=7$$

Platí: $n(a)=k = e \cdot d \xrightarrow{\text{pak}} n(a^d) = e$

obecně
$$n(a^d) = \frac{n(a)}{\gcd(d, n(a))}$$
 $(a^d)^e = a^{d \cdot e} = a^k = 1$

najdeme-li generátor a grupy (když grupa je cyklická) pak můžeme dopočítat řád každého $b = a^d$

$$a=5 = 2^5 \rightarrow n(5) = n(2^5) = \frac{n(2)}{\gcd(5, n(2))} = \frac{6}{\gcd(5, 6)} = 6$$

$$a=6 = 2^4 \rightarrow n(6) = n(2^4) = \frac{6}{\gcd(4, 6)} = 3$$

Platí: a je generátor v $\mathbb{Z}_n^*$, když řád a $n(a) = \varphi(n) = |\mathbb{Z}_n^*|$
 Každý a^k pro $\gcd(k, \varphi(n)) = 1$ je $n(a^k) = \frac{n(a)}{1} = n(a) = \varphi(n)$

$\rightarrow a^k$ je opět generátor

Pakud je $\mathbb{Z}_n^*$ cyklická (má aspoň 1 generátor), pak má $\varphi(\varphi(n))$ různých generátorů

$$\mathbb{Z}_n^* = \langle a \rangle = \langle a^k \rangle, \quad \gcd(k, \varphi(n)) = 1$$

Pro $\mathbb{Z}_9^*$ $\varphi(9) = 6$

Víme, že $\mathbb{Z}_9^* = \langle 2 \rangle$ $\mu(2) = 6$

$\hookrightarrow$ celkem $\varphi(\varphi(9)) = \varphi(6) = \varphi(2 \cdot 3) = 1 \cdot 2 = 2$

druhým generátorem je 5, $\mathbb{Z}_9^* = \langle 5 \rangle$

Podgrupy v $\mathbb{Z}_9^*$

P	$ P $	generátory	
$\{1\}$ $\begin{array}{c c} & 1 \\ \hline 1 & 1 \end{array}$	1	1	
$\{1, 8\}$ $\begin{array}{c cc} & 1 & 8 \\ \hline 1 & 1 & 8 \\ 8 & 8 & 1 \end{array}$	2	8	$x^2 = 1$ $x_1 = 1, x_2 = 8 = -1$
$\{1, 4, 7\}$ $\begin{array}{c ccc} & 1 & 4 & 7 \\ \hline 1 & 1 & 4 & 7 \\ 4 & 4 & 1 & 7 \\ 7 & 7 & 7 & 1 \end{array}$	3	4, 7	$x^3 = 1$ má 3 řeš
$\{1, 2, 4, 5, 7, 8\}$	6	2, 5	$x^6 = 1$ má 6 řeš

Platí: Cyklická grupa o $\varphi(n)$ prvcích má podgrupy
 opět cyklické a pro každý dělitel m čísla $\varphi(n)$
 je v grupě právě 1 podgrupa o m prvcích
 (generovaná $a^{\frac{\varphi(n)}{m}}$)
 např. pro $Z_n^* = \langle a \rangle$
 (která má $\varphi(n)$ generátorů jako podgr.)

Pozn ($Z_{12}^*, \cdot$) nemusí být cyklická

• $\text{Pr}(Z_{12}^*, \cdot)$

$\pi(a) < \varphi(12) \Rightarrow a$ není generátor

počet prvků $\varphi(12) = \varphi(3 \cdot 2^2) = 2 \cdot (2^2 - 2) = 4$

$$Z_{12}^* = \{1, 5, 7, 11\}$$

$$1 \quad \pi(1) = 1$$

$$5 \quad 5^2 = 25 = 1 \quad \pi(5) = 2$$

$$7 \quad 7^2 = 49 = 1 \quad \pi(7) = 2$$

$$11 \quad 11^2 = 121 = 1 \quad \pi(11) = 2$$

žádný prvek řádu $\varphi(12) = 4 \rightarrow$ není generátor

$\Rightarrow Z_{12}^*$ není cyklická

Pozn: V Z_{12}^* má rovnici $x^2 = 1$ 4 řešení

$$(x_1 = 1, x_2 = 5, x_3 = 7, x_4 = 11)$$

generátor a by musel mít $\pi(a) = 4$, tj. řešit $x^4 = 1$
 a přitom $x^2 \neq 1$ ALE nebyl žádný

Platí: $(\mathbb{Z}_p^*, \cdot)$ je vždy cyklická pro p prvočíslo

[důvod $x^k - 1 = 0$ má v $\mathbb{Z}_p$ právě k různých řešení = k různých k -tých odmocnin z 1]

Pr V $\mathbb{Z}_{23}^*$ najděte vs. generátory

Postup: Pochopně najdeme jeden generátor a a víme, že ostatní jsou tvaru $b = a^k$ pro k nesoudělné s $\varphi(23)$

$$\varphi(23) = 22$$

$$\mathbb{Z}_{23}^* = \mathbb{Z}_{23} \setminus \{0\}$$

Hledáme $a \in \mathbb{Z}_{23}^*$ s.t. $\chi(a) = 22 \rightarrow a^{22} = 1$, ale

$$a^k \neq 1 \text{ pro } k < 22$$

Pro hledání můžeme vyjít $a^k = 1$ v $\mathbb{Z}_{23}^*$

$$k \text{ dělí } |\mathbb{Z}_{23}^*| = \varphi(23) = 22$$

$$\Rightarrow k = \{1, 2, 11, 22\}$$

$$|\langle a \rangle| \text{ dělí } |\mathbb{Z}_{23}^*|$$

$$\text{Chci } a^1 \neq 1 \rightarrow a \neq 1$$

$$a^2 \neq 1$$

Víme $x^2 = 1$ má v $\mathbb{Z}_p$ 2 řeš: 1, -1

$$\rightarrow a \neq 1, a \neq 22$$

$$b = a^{11} \neq 1$$

$$1 = a^{22} = (a^{11})^2 = b^2$$

$$\rightarrow \text{buď } b = a^{11} = -1$$

$$\text{Počet generátorů} = \varphi(\varphi(n)) = \varphi(22) = \varphi(2 \cdot 11) = 1 \cdot 10 = 10$$

→ V $\mathbb{Z}_{23}^*$ je 22 prvků, ± 1 nevypdají,
 zbývá 20 prvků, z nich je 10 generátorů
 → pravděp. $\frac{1}{2}$, to je krásné

Opak čísel $a^{11} \in \mathbb{Z}_{23}$

$$11 = 8 + 2 + 1$$

$$\begin{array}{cccc} 1 & 0 & 1 & 1 \\ X & S & S & X & S & X \end{array}$$

$$a=3$$

$$\begin{array}{ll} X & 3^1 \\ S & 3^2 = 9 \\ S & 3^4 = 81 = 12 \\ X & 3^5 = 36 = 13 \\ S & 3^{10} = 13^2 = (-10)^2 = 100 = 8 \\ X & 3^{11} = 24 = 1 \end{array}$$

$$a=5$$

$$\begin{array}{ll} X & 5^1 \\ S & 5^2 = 25 = 2 \\ S & 5^4 = 4 \\ X & 5^5 = 20 \\ S & 5^{10} = (-3)^2 = 9 \\ X & 5^{11} = -1 \\ & \underline{\quad\quad\quad} \\ & 5^{22} = 1 \end{array}$$

Převodní tabulka

$\mathbb{Z}_{23}^*$	1	2	3	4	5	6
$a=5^k$	5^{22}	5^2	5^{16}	5^4	5^1	5^{11}

$$3 = (-3)(-1) = 5^5 \cdot 5^{11} = 5^{16}$$

Další generátory

5^k pro k nesoudělné

$$\Rightarrow \varphi(23) = 22$$

$$5^1 = 5, \quad 5^3 = \quad, \quad 5^5 = 20$$

$$5^7 = \quad, \quad 5^9 = \quad, \quad 5^{13} = \quad$$

$$5^{15} = \quad, \quad 5^{17} = \quad, \quad 5^{19} = \quad$$

$$5^{21} = \quad$$

(4)

Rád prvku v $\mathbb{Z}_p^*$

$\mathbb{Z}_p^* = \langle a \rangle$ a^k vytvoří vs. prvky z $\mathbb{Z}_p^*$, tj. $\varphi(p) = p-1$ prvků

Př. Řešte $x^k = 1$ v $\mathbb{Z}_{19}$

~~X~~ $x \in \mathbb{Z}_p^*$ protože pro x nesouditel s $n=19$ je $x^k \neq 1$
(jinak by $x^{k-1} = \text{inverze } k \cdot x$)

$x^9 = 1$? jakého řádu bude řešení $x=a$ této rovnice?

$$\underline{\kappa(a)=9} \rightarrow a^9 = 1$$

$$\underline{\kappa(a)=1} \quad a = 1$$

? $\kappa(a)=2$ NE $a^2=1$ $a^9 = (a^2)^4 \cdot a = 1 \cdot a \neq 1$ (jinak by $\kappa(1)=1$)

$$\underline{\kappa(a)=3} \rightarrow a^3=1 \rightarrow a^9 = (a^3)^3 = 1^3 = 1$$

$x^k = 1$ řešení $x=a$ je prvek řádu d , kde $d|k$

? jak najít prvky řádu 9 a řádu 3?

$$\kappa(a^k) = \frac{\kappa(a)}{\gcd(k, \kappa(a))}$$

Bad Když najdu jeden prvek a řádu 9, tak ostatní
dopocítám $b = a^k$, kde $\gcd(k, 9) = 1$

$$\rightarrow \kappa(b) = \kappa(a^k) = \frac{9}{1} = 9$$

$\rightarrow$ je funkce $\varphi(9) = 6$

nebo $\rightarrow$ Když najdu generátor $\mathbb{Z}_{19}^* = \langle a \rangle$, $\kappa(a) = \varphi(19) = 18$

pak $b = a^k$ (pro vs. $b \in \mathbb{Z}_{19}^*$)

$$\kappa(b) = \frac{18}{\gcd(k, 18)} = 9 \text{ pro } k \text{ taková, že } \gcd(k, 18)$$

Hledáme generátor v $\mathbb{Z}_{19}^*$

$$|\mathbb{Z}_{19}^*| = \varphi(19) = 18 \rightarrow \text{hledáme prvek řádu 18}$$

$$a^{18} = a^{\varphi(19)} = 1 \text{ v } \mathbb{Z}_{19}^* \text{ Euler-Fermat}$$

$\kappa(a) \nmid 18$ $\kappa(a)$ může být 1, 2, 3, 6, 9, 18 (dělitelé $|G| = 18$)

- musím ověřit, že $a^2 \neq 1, a^3 \neq 1, a^6 \neq 1, a^9 \neq 1$

[Zjednodušení: $x^2 = \pm 1$ v $\mathbb{Z}_p$

$$(a^3)^2 = a^6 \neq 1 \leftrightarrow a^3 \neq \pm 1 \quad]$$

$\mathbb{Z}_{19}^*$

$$a = 2$$

$$a^2 = 4 \neq 1$$

$$a^3 = 8 \neq \pm 1 \rightarrow a^6 \neq 1$$

$$a^9 = 2^9 = 512$$

$$= 2 \cdot (2^2)^4 = 2 \cdot (4^2)^2 = 2 \cdot 16^2 = 2 \cdot (-3)^2 = 2 \cdot 9 = 18 = -1 \neq 1$$

$$\rightarrow \kappa(2) = 18 \rightarrow \langle 2 \rangle = \mathbb{Z}_{19}^*$$

2. jaká je pravděp., že při náhodném výběru prvku ze $\mathbb{Z}_{19}^*$ vybereme generátor

$$\text{počet generátorů } \varphi(18) = \varphi(2 \cdot 3^2) = 1 \cdot (9-3) = 6$$

$$p = \frac{\varphi(18)}{|\mathbb{Z}_{19}^*|} = \frac{6}{18} = \frac{1}{3}$$

při výběru $x \in \mathbb{Z}_{19}^* \setminus \{1, 18\}$

$$p = \frac{6}{16}$$

-1

$$x^9 = 1$$

$$x_1 = 1$$

$$\mu(1) = 1$$

$$\mu(x) = 3 \quad x = 2^k \quad \text{kde } k: \mu(x) = \frac{18}{\gcd(k, 18)} = 3$$

$$\rightarrow \gcd(k, 18) = 6; \quad k < 18$$

$$k = 6; \quad k = 12$$

$$x_2 = 2^6 = 4^3 = 4 \cdot 16 = 4 \cdot (-3) = -12 = 7$$

$$x_3 = 2^{12} = (2^6)^2 = 7^2 = 49 = 11$$

$$\mu(x) = 9 \quad x = 2^k \quad \text{kde } k: \mu(x) = \frac{18}{\gcd(k, 18)} = 9$$

$$\gcd(k, 18) = 2, \quad k < 18$$

$$k \in \{2, 4, 6, 8, 10, 12, 14, 16\}$$

$$x_4 = 2^2 = 4$$

$$x_5 = 2^4 = (2^2)^2 = 16$$

$$x_6 = 2^6 = (2^4)^2 = (-3)^2 = 9$$

$$x_7 = 2^{10} = 4 \cdot 2^6 = 4 \cdot 9 = 36 = 17$$

$$x_8 = 2^{14} = 2^{10} \cdot 2^4 = (-3) \cdot (-2) = 6$$

$$x_9 = 2^{16} = 2^{14} \cdot 2^2 = 6 \cdot 4 = 24 = 5$$

Platí: Rovnice $x^k = 1$ má v $\mathbb{Z}_p$

převě $d = \gcd(k, \varphi(p))$ různých řešení
 jsou to prvky řádu d (těk je $\varphi(d)$)
 a prvky řádu l , kde $l | d$
 (těk je $\varphi(l)$) $\Rightarrow \sum_{l|d} \varphi(l) = d$

Pozn:

$$\mathbb{Z}_{19}: x^{10} = 1$$

řešení $x = a$ je prvek
 řádu $\mu(a) = 10; 5; 2; 1$

$$\forall \mathbb{Z}_{19}^*, |\mathbb{Z}_{19}^*| = 18, \mu(a) | 18$$

$\rightarrow$ nejprve řádu 5, 10

$\rightarrow$ jediná řeš $x_1 = 1, x_2 = -1 \equiv 18$

Podobně to bude pro $\mathbb{Z}_m^* = \langle a \rangle$ cyklické

Ale pro $\mathbb{Z}_m^*$ necyklické to neplatí $\mathbb{Z}_{12}^*$ $x^2=1$ má 4 řešení

Čínská věta o zbytcích

Věta: Nechtě $m_1, \dots, m_k$ jsou po dvou nesoudělná čísla z $\mathbb{N}$

Pak soustava zbytkových rovnic:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$\vdots$

$$x \equiv a_k \pmod{m_k}$$

má jediné řešení v $\mathbb{Z}_M$, kde $M = \prod_{i=1}^k m_i = m_1 \dots m_k$

Postup č. 1

– řešit $k-1$ Diofant. rovnice

Př. Řešte v $\mathbb{Z}_{105}$ zbytkovou soustavu

$$x \equiv 1 \pmod{3}$$

$$x \equiv 0 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

$$M = 105 = 3 \cdot 5 \cdot 7 = m_1 \cdot m_2 \cdot m_3$$

relativní úvahy

$$x = \underbrace{3k+1 = 5l = 7r+4}$$

$$3k - 5l = -1$$

$$\text{part. řes. } k = -2, l = -1$$

$$\text{hom. rov. } 3k - 5l = 0$$

$$k_0 = 5, l_0 = 3$$

$$\text{obecně } k = -2 + 5s$$

$$l = -1 + 3s$$

$$\rightarrow x = 3 \underbrace{(-2 + 5s)}_{-2} + 1 = -5 + 15s \quad \text{řeší první 2 kb. rov.}$$

$$\text{cht. } x = \underbrace{-5 + 15s}_{-5 + 15s} = 7x + 4$$

$$15s - 7x = 9$$

$$n_p = 3 \quad s_f = 2$$

$$\text{hom. rov.} \quad n_p n_0 = 15 \quad s_0 = 7$$

$$\text{obecně} \quad s = 2 + 7m$$

$$n =$$

$$\hookrightarrow x = -5 + 15(2 + 7m) = 25 + 105m$$

$$\vee \mathbb{Z}_{105} \quad \underline{\underline{x = 25}}$$

Výhoda - použitelné i když $m_1, \dots, m_k$ současně

Ale - nemusí tam být řešení $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{4} \end{cases}$
nemá řeš.]

- má-li řeš., tak je jediné v $\mathbb{Z}_N$, kde

$N = \text{nejmen. spol. nás. } m_1, \dots, m_k$

Postup č. 2

Najdeme univerzální $q_1, \dots, q_k$ - řešení soustav

s pr. str. = 0 kromě i -té (= 1)

q_i řeší $x \equiv 0 \pmod{m_j} \quad j \neq i$

$x \equiv 1 \pmod{m_i}$

Pak řešení obecně soustavy $x_i \equiv a_i \pmod{m_i}$

má tvar $x = a_1 q_1 + \dots + a_k q_k \pmod{\mathbb{Z}_M}$

$$(\text{Dk.: } \forall \mathbb{Z}_{m_i} \quad x \equiv a_1 \cdot 0 + \dots + a_i \cdot 1 + \dots + a_k \cdot 0 \equiv a_i)$$

jak najít $q_i, i=1, \dots, k$?

$$q_i = \prod_{j \neq i} m_j \cdot s$$

↓

$$q_i \equiv 0 \pmod{m_j}$$

$$\text{kde } s \cdot (\prod_{j \neq i} m_j) \equiv 1 \pmod{m_i}$$

$$\hookrightarrow s = \left(\prod_{j \neq i} m_j \right)^{-1}$$

existuje inverze, neboť $\left(\prod_{j \neq i} m_j \right)$
nesoudělné s m_i

(předpoklad čísel v.o.s.b.)

$$\text{Př.: } m_1 = 3, m_2 = 5, m_3 = 7$$

$$x \equiv 1 \pmod{3}$$

$$x \equiv 0 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

Najdi q_i

$$q_1 = 5 \cdot 7 \cdot s = 35 \cdot s, \text{ kde } s = 35^{-1} \pmod{3}$$

$$s = 2^{-1} = 2$$

$$\rightarrow \underline{q_1 = 35 \cdot 2 = 70}$$

$$q_2 = 3 \cdot 7 \cdot t = 21t, \text{ kde } t = 21^{-1} \pmod{5}$$

$$t = 1^{-1} = 1$$

$$\underline{q_2 = 21}$$

$$q_3 = 3 \cdot 5 \cdot r = 15r, \text{ kde } r = 15^{-1} \pmod{7}$$

$$r = 1^{-1} = 1$$

$$\underline{q_3 = 15}$$

Res:

$$x_4 = 1 \cdot q_1 + 0 \cdot q_2 + 4 \cdot q_3 \in \mathbb{Z}_{105}$$

$$= 1 \cdot 70 + 0 + 4 \cdot 15 = 130 = \underline{\underline{25}}$$

Pr:

$$m_1 = 4, m_2 = 5, m_3 = 9, m_4 = 11 \rightarrow M = 4 \cdot 5 \cdot 9 \cdot 11 = 1980$$

$\in \mathbb{Z}_{1980}$ Teste

$$x \equiv 2 \pmod{4}$$

$$x \equiv 0 \pmod{5}$$

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

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

Nagel'sche univers q_i

$$q_1 = 5 \cdot 9 \cdot 11 \cdot s = 495s, \text{ hole } s = (495)^{-1} \in \mathbb{Z}_{1980} \\ = (-1)^{-1} = -1 = 3$$

$$q_1 = 495 \cdot 3 = 1485$$

$$(\text{nebo } q_1 = 495 \cdot (-1) = -495)$$

$$q_2 = 4 \cdot 9 \cdot 11 \cdot t = 396t$$

$$q_2 = 396$$

$$\text{hole } \in \mathbb{Z}_5 \quad t = (396)^{-1} = 1^{-1} = 1$$

$$q_3 = 4 \cdot 5 \cdot 11 \cdot r = 220r$$

$$\in \mathbb{Z}_9 \quad r = (220)^{-1} = (4)^{-1} = 7$$

$$q_3 = 220 \cdot 7 = \cancel{1540} 1540$$

$$q_4 = 4 \cdot 5 \cdot 9 \cdot k = 180k$$

$$\in \mathbb{Z}_{11} \quad k = (180)^{-1} = 4^{-1} = 3$$

$$q_4 = 180 \cdot 3 = 540$$

$$x = 2q_1 + 0q_2 + 1q_3 + 2q_4 = 2 \cdot (-495) + 0 + 1540 + 540 = (-990) + 1540 +$$

$$+ 1080 = 550 + 1080 = 1630$$

$$\in \mathbb{Z}_{1980}$$

5

Residuální aritmetika

$$M = m_1 \dots m_n \quad - m_i, m_j \text{ nesoud.}$$

$$\begin{array}{cc} \parallel & \parallel \\ p_1^{k_1} & p_n^{k_n} \end{array}$$

Čin. věta o zb. $A \in \mathbb{Z}_M \xleftrightarrow[\text{jednozn}]{\text{vzaj}} (a_1, \dots, a_n) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$

$$A \cdot B \in \mathbb{Z}_M \leftrightarrow ([a_1 b_1]_{m_1}, \dots, [a_n b_n]_{m_n})$$

$$A^k \in \mathbb{Z}_M \leftrightarrow ([a_1^k]_{m_1}, \dots, [a_n^k]_{m_n})$$

Residuální aritmetika - mohou násobit (umocňovat)
sčítat v $\mathbb{Z}_{m_i}$ a k čin. v.o.zb. spočítat
součin (mocniny) v $\mathbb{Z}_M$ (máme spočtena $q_1, \dots, q_n$)

Pr Spočítejte residuálně součin $AB = 3576 \cdot 212155$ v $\mathbb{Z}_{1980}$.

Víme od minule $1980 = 4 \cdot 5 \cdot 9 \cdot 11$

$$q_4 = 1485, q_5 = 396, q_9 = 1540, q_{11} = 540$$

$$3576 = A \leftrightarrow ([0]_4, [1]_5, [3]_9, [1]_{11})$$

$$\text{v } \mathbb{Z}_4: A = 3 + 5 + 7 + 6 = 21 = 2 + 1 = 3$$

$$\text{v } \mathbb{Z}_{11}: A = 6 - 7 + 5 - 3 = 1$$

$$212155 \leftrightarrow ([3]_4, [0]_5, [7]_9, [-2]_{11})$$

Kvůbra: Věty o dělitelnosti

$$3, 9 \quad a \equiv \text{ciferný součet} \pmod{3, 9}$$

$$a = \sum_0^k c_i \cdot 10^i \equiv \sum_0^k c_i \cdot 1^i \pmod{3, 9}$$

$c_k \dots c_1 c_0$ - cifry

$$\begin{aligned} 11 \quad a &= \sum c_i \cdot 10^i \equiv \sum c_i (-1)^i \pmod{11} \\ &= c_0 - c_1 + c_2 - \dots + (-1)^k c_k \end{aligned}$$

$$7, 13, (11) \quad 7 \cdot 11 \cdot 13 = 1001$$

$$1000 \equiv -1 \pmod{7, 11, 13}$$

$$a = \sum t_i \cdot 1000^i \equiv \sum t_i (-1)^i \pmod{7, 11, 13}$$

$\uparrow$ hojnésti -390 $+65$

$$\mathbb{Z}_{13} \quad 1234/567 = 567 - 234 + 1 = 334 = -56 = 9$$

Pokrač. př.

$$\begin{aligned} A \cdot B &\leftrightarrow ([0 \cdot 3]_4, [1 \cdot 0]_5, [3 \cdot 7]_9, [1 \cdot (-2)]_{11}) \\ &= ([0]_4, [0]_5, [3]_9, [-2]_{11}) \end{aligned}$$

$$\begin{aligned} A \cdot B &= 0 \cdot q_4 + 0 \cdot q_5 + 3 \cdot q_9 - 2 \cdot q_{11} = 3 \cdot 1540 - 2 \cdot 540 = \\ &= 4620 - 1080 = 3540 = \underline{\underline{1560}} \end{aligned}$$

$\text{in } \mathbb{Z}_{1980}$

V praxi se použív. $m_1, \dots, m_8 = 5, 7, 11, 13, 17, 19, 23, 29$

posloup. nich se zpracovávají součiny v rozsahu
 $0 \dots 2^{30}$ nebo $-2^{29} \dots 2^{29}$

Použ. : Dešifrování v RSA

Soukromý klíč (N, s) ... dešifruje $a = b^s$ v $\mathbb{Z}_N$

Já znám $N = p \cdot q$

$\rightarrow$ mohu spočítat $a_p = b^s$ v $\mathbb{Z}_p$, $a_q = b^s$ v $\mathbb{Z}_q$
a použít čin. v. o. sb.

Př. Soukromý klíč $(N = 1469, s = 269)$

Klíče $N = \underset{p}{13} \cdot \underset{q}{113}$

Dešifruje $b = 571$

Nejprve spočteme q_p, q_q pro čin. v. o. sb.

$$q_p = 113 \cdot s \stackrel{\text{dci}}{=} 1 \text{ v } \mathbb{Z}_{13}$$

$$\rightarrow 9 \cdot s = 1 \rightarrow s = 9^{-1} \text{ v } \mathbb{Z}_{13}$$

$$\rightarrow s = 3 \text{ odhadem}$$

$$q_{13} = q_p = 113 \cdot 3 = 339$$

$$9/9 = 13 \cdot 5 \stackrel{\text{div}}{=} 1 \text{ v } \mathbb{Z}_{113}$$

$$\rightarrow 13 \cdot 5 + 113k = 1$$

Eukleid

$$113 = 8 \cdot 13 + 9$$

$$13 = 1 \cdot 9 + 4$$

$$9 = 2 \cdot 4 + 1$$

$$1 = 9 - 2 \cdot 4 = 9 - 2(13 - 9) =$$

$$= (-2) \cdot 13 + 3 \cdot (113 - 8 \cdot 13) =$$

$$= 3 \cdot 113 - 26 \cdot 13$$

$\underbrace{\quad}_{=5}$

$$9/9 = 9_{113} = 13 \cdot (-26) = \underline{\underline{-338}}$$

Děufrování

$$a = 571^{269} \text{ v } \mathbb{Z}_{1469}$$

$$\leftrightarrow (a_1, a_2) \text{ kde } a_1 = 571^{269} \text{ v } \mathbb{Z}_{13}$$

$$a_1 = 12^{269} = (-1)^{269} = -1$$

$$a_2 = 571^{269} \text{ v } \mathbb{Z}_{113}$$

$$a_2 = 6^{269} = 6^{112 \cdot 2 + 45} = 6^{45}$$

Euler-Formal

$$\boxed{6^{\varphi(113)} = 1 \text{ v } \mathbb{Z}_{113}}$$

= opak. čísel

$$45 = \begin{array}{c} 101100 \\ \uparrow \uparrow \uparrow \uparrow \uparrow \\ x5 \quad sx \quad x5 \quad s \quad x \end{array}$$

$$\mathbb{Z}_{113} \quad 6^{45}$$

$$X \quad 6^1$$

$$S \quad 6^2 = 36$$

$$S \quad 6^4 = 36^2 = 1296 = 53$$

$$X \quad 6^5 = 6 \cdot 53 = 318 = 92$$

$$S \quad 6^{10} = 92^2 = 8464 = 102$$

$$X \quad 6^{11} = 6 \cdot 102 = 47$$

$$S \quad 6^{22} = 47^2 = 62$$

$$S \quad 6^{44} = 62^2 = 2$$

$$X \quad 6^{45} = 6 \cdot 2 = \underline{\underline{12}}$$

$$a \leftrightarrow \left(\underset{\substack{\parallel \\ 12}}{[-1]_{13}}, [12]_{113} \right)$$

$$a = 12 \cdot q_{13} + 12 \cdot q_{113} = 12 \cdot 339 - 12 \cdot 338 = \underline{\underline{12}}$$

Rěšení rovnice $x^k = 1$ v $\mathbb{Z}_n$

Víme - pro $\mathbb{Z}_n = \langle a \rangle$ cyklickou má rovnice $x^k = 1$

celkem $d = \gcd(k, \varphi(n))$ různých řešení.

jeou to prvky řádu ℓ , kde ℓ dělí d .

(Najdeme je např. tak, že najdeme generátor
 $\rightarrow$ patřičné mocniny generátoru mají řád ℓ)

Cín. v. o. sb.: Každému řes. rov. $x^k = 1$ v $\mathbb{Z}_N$

odpovídá jednozn. $(x_1, \dots, x_n) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$

$$(N = p_1^{k_1} \dots p_n^{k_n} = m_1 \dots m_n)$$

kde $x_i^{k_i} = 1$ v $\mathbb{Z}_{m_i}$

Speciálně pro $N = p_1 \dots p_n$ (square free - není dělit p^2)

pro $\mathbb{Z}_p^*$ cyklické $\rightarrow x_i^k = 1$ má $d = \gcd(k, \varphi(p))$

řešení v $\mathbb{Z}_p$

$\rightarrow$ v $\mathbb{Z}_N$ je $d_1 \dots d_n$ řešení rov. $x^k = 1$

Př.: $\mathbb{Z}_{105} : x^2 = 1$

$$N = 105 = 3 \cdot 5 \cdot 7$$

známe z minule $q_3 = 70$, $q_5 = 21$, $q_7 = 15$

$$x \leftrightarrow (x_1, x_2, x_3)$$

$$\mathbb{Z}_3 : x_1^2 = 1$$

$\rightarrow \gcd(2, \varphi(3)) = 2$ právě 2 řes. $\rightarrow \underline{x_1 = 1}, \underline{x_1 = -1 = 2}$

[pozn: v $\mathbb{Z}_p$ $x^2 = 1$ má 2 řes. $x = \pm 1$]

$$\mathbb{Z}_5 : x_2^2 = 1 \rightarrow \underline{x_2 = 1}$$
$$\underline{x_2 = -1 = 4}$$

$$\mathbb{Z}_7 : x_3^2 = 1 \rightarrow \underline{x_3 = 1}$$
$$\underline{x_3 = -1 = 6}$$

$$\mathbb{Z}_{105} \quad 2 \cdot 2 \cdot 2 = 8 \quad \text{řešení}$$

$$(1, 1, 1) \rightarrow x = 1 \cdot q_3 + 1 \cdot q_5 + 1 \cdot q_7 = 70 + 21 + 15 = 106 = 1$$

$$(1, 1, -1) \rightarrow x = q_3 + q_5 - q_7 = 70 + 21 - 15 = 76$$

$$(1, -1, 1) \quad x = 70 - 21 + 15 = 64$$

$$(1, -1, -1) \quad 70 - 21 - 15 = 34$$

$$(-1, 1, 1) \quad -70 + 21 + 15 = -34 = 71$$

$$(-1, 1, -1) \quad -70 + 21 - 15 = -64 = 41$$

$$(-1, -1, 1) \quad -76 = 29$$

$$(-1, -1, -1) \quad -1 = 104$$

$\rightarrow \mathbb{Z}_{105}$ není cyklická ($x^2 = 1$ má více než 2 řeš.)

Pr 2 $\mathbb{Z}_{105} : x^4 = x$

$$\mathbb{Z}_{105} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

$$\mathbb{Z}_3 : x^4 = x \quad \begin{cases} \text{bud } x = 0 \\ \text{pro } x \neq 0 \rightarrow x \in \mathbb{Z}_3^* \rightarrow \text{že náleží } x^{-1} \end{cases}$$

($\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$)

$$\rightarrow x^3 = 1$$

$$\gcd(3, \varphi(3)) = 1 \quad \text{řešení}$$

$$\rightarrow x = 1 \quad (\text{prvek řádu 1})$$

$$\mathbb{Z}_5: x^4 = x \begin{cases} x=0 \\ \text{nebo } x^3=0 \end{cases} \quad \text{jinak naprosto úvaha}$$

$$\rightarrow \kappa(a) \text{ v } \mathbb{Z}_5^* \text{ dělí } \varphi(5)=4$$

$$\rightarrow \kappa(a) \in \{1, 2, 4\}$$

$$\rightarrow \text{res } x^3 = 1 \text{ je jen prv. řádu 1}$$

$$\rightarrow \underline{x=1}$$

$$\mathbb{Z}_7: x^4 = x \begin{cases} x=0 \\ x^3=1 \end{cases}$$

$$\kappa(a) \text{ v } \mathbb{Z}_7^* \text{ dělí } \varphi(7)=6$$

$$\rightarrow \kappa(a) \in \{1, 2, 3, 6\}$$

$$\rightarrow x^3=1 \text{ res prv. řádu 1} \rightarrow x=1$$

řád 3 $\rightarrow$

$$\text{Např. } x=2 \quad \kappa(2)=3 \quad \text{vhodně}$$

$$2 \neq 1, 2^2 \neq 1, 2^3 = 1 \text{ v } \mathbb{Z}_7$$

$$\text{další prv. řádu 3 jsou } b=2^k,$$

$$\text{kde } k \text{ nesouděl s } 3$$

$$\kappa(2^k) = \frac{\kappa(2)}{\gcd(k, \kappa(2))} = \frac{3}{1}$$

$$x = b_1 = 2^1, \quad x = b_2 = 2^2 = 4$$

$$\vee \mathbb{Z}_{105} \text{ je } 2 \times 2 \times 4 \text{ res} = 16 \text{ res.}$$

$$(0, 0, 0) \rightarrow x = 0$$

$$(0, 0, 1) \rightarrow x = 1q_7 = 15$$

$$(0, 0, 2) \rightarrow x = 30$$

$$(0, 0, 4) \rightarrow x = 60$$

můžeme si dohledat sami

Dur. RSA s veřejným klíčem ($N=1469$, $t=5$)

Které správy a se kófováním nesmění?

$$a^t = a \text{ v } \mathbb{Z}_N$$

(6)

Polynomy nad $\mathbb{Z}_p$

$\mathbb{Z}_p[x]$ = m. pol. s koef. v $\mathbb{Z}_p$ a proměnná x

- polynom je určen stupněm a koeficienty

$\rightarrow$ Počet pol. st. $\leq n$ je p^{n+1} $| a_n x^n + \dots + a_1 x + a_0$; $a_i \in \mathbb{Z}_p$

$\rightarrow$ Všechny pol. nekonečně mnoho (společně $\approx |N|$)

=

Pro $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$

- f je určena def. oborem a výsledky v každém bodě (nikoli předpisem)

$$p \left\{ \begin{matrix} \vdots \\ \vdots \\ \vdots \end{matrix} \right\}_p \quad f \leftrightarrow (f(0), f(1), \dots, f(p-1)), \text{ kde } f(h) \in \mathbb{Z}_p$$

všechny

teh je p^p

Platí nad $\mathbb{Z}_p$: Výsledky v p bodech je jednoznačně určen
 jediný pol. st. $\leq p-1$

$\Rightarrow$ Na každou funkci $\overset{\text{z } \mathbb{Z}_p \text{ do } \mathbb{Z}_p}{\text{se lze dívat jako na pol. st. } \leq p-1}$

Jak pro pol. $P(x)$ najít pol. st. $\leq p-1$, který určuje stejnou
 fci (dává stejné výsl.)

pro vs. $a \in \mathbb{Z}_p$ platí $a^p = a$

$a=0$

$a \neq 0 \rightarrow \text{ex. } a^{-1}$

$$a^{p-1} = 1$$

do násí vs. $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

E-F věta

$\Downarrow$

$$x^p \sim x^1$$

dávají všude stejné výsl.

$\Downarrow$

$$x^{2p+k} \sim x^{2 \cdot 1 + k}$$

$\mathbb{P}_A: \mathbb{Z}_3[x]$

$$P(x) = x^5 + x + 1$$

$$0 \rightarrow 1$$

$$1 \rightarrow 0$$

$$2 \rightarrow 2$$

Hledám pol. st. ≤ 2 , který dává
 st. výsl.

$$\underline{x^5 + x + 1 = x^{3+2} + x + 1}$$

$$= x^{1+2} + x + 1 = x^1 + x + 1 = \underline{2x + 1}$$

$\uparrow$
 jeho fci

$$0 \rightarrow 1$$

$$1 \rightarrow 0$$

$$2 \rightarrow 2$$

Dělení polynomů, gcd, polynomiální rovnice

Př. $(2x^5 + 2x^2 + x + 3) : (3x^2 + x) = 4x^3 + 2x^2 + x + 2$ pol v $\mathbb{Z}_5[x]$

$$\begin{array}{r} -2x^5 - 4x^4 \\ \hline \end{array} \quad \cdot 3^{-1} = \cdot 2$$

$$-4x^4 = x^4$$

$$-x^4 - 2x^3$$

$$\hline (-2x^3) 3x^3 + 2x^2 + x + 3$$

$$-3x^3 - x^2$$

$$\hline x^2 + x + 3$$

$$-x^2 - 2x$$

$$\hline 4x + 3$$

$$P(x)$$

$$Q(x)$$

$$(1) \quad (2x^5 + 2x^2 + x + 3) = (4x^3 + 2x^2 + x + 2) \cdot (3x^2 + x) + (4x + 3)$$

Najít gcd $(P(x), Q(x))$

- je lich $(\neq 1)$

Když $D(x)$ dělí P i Q a je všemi spol. děliteli sdílený,
pak $a \cdot D(x) = a \cdot D(x)$ to také splňuje
($a \neq 0$)

$$[D(x) | P(x) \rightarrow P(x) = D(x) \cdot R(x) \rightarrow P(x) = (a \cdot D(x)) \cdot (a^{-1} \cdot R(x))]$$

- funguje Eukleidův alg.

$$(3x^2 + x) = (2x) \cdot (4x + 3) + 0$$

$$(3x^2 + x) : (4x + 3) = 2x$$

$$\cdot 4^{-1} = \cdot 4$$

$$\begin{array}{r} -3x^2 - x \\ \hline 0 \end{array}$$

$$\text{gcd} = D(x) = 4x + 3$$

Berousova věta: $\gcd(P(x), Q(x)) = A(x) \cdot P(x) + B(x) \cdot Q(x)$

je "polynomiální" kombinací

Najít $A(x), B(x)$ - spěšným použit. rovnice Eukleid. alg.

$$4x+3 \stackrel{(1)}{=} P(x) - (4x^3+2x^5+x+2) \cdot Q(x) =$$

$$= 1 \cdot P(x) + \underbrace{(1x^3+3x^2+4x+3)}_{B(x)} \cdot Q(x)$$

"
 $A(x)$

"
 $B(x)$

(dopočítáno v $\mathbb{Z}_5$)

→ Dají se řešit polynomiální rovnice

$$A(x) \cdot P(x) + B(x) \cdot Q(x) = C(x)$$

kde $P, Q, C \in \mathbb{Z}_p[x]$ zadané

Hledáme $A, B \in \mathbb{Z}_p[x]$

má řeš, jen když $\gcd(P, Q)$ dělí pr. str. $C(x)$

part. řeš. - Eukleid. alg., Berousova věta

obecně = part. řeš. + polynom násobky nesouditel řeš. hom. rov.

Př. $A(x) \cdot (2x+1) + B(x)(x^2+1) = 1$ nad $\mathbb{Z}_3$ ($\in \mathbb{Z}_3[x]$)

part. řeš. - Eukleid

$$(x^2+1) = (2x+2) \cdot (2x+1) + 2$$

$$(2x+2) = (x+2) \cdot 2 + 0$$

$$\begin{array}{r} (x^2+1) : (2x+1) = 2x+2 \\ \underline{-(x^2-2x)} \\ x+1 \\ \underline{-(x-2)} \\ 2 \end{array}$$

$$(2x+2) : 2 = \dots$$

$$2 = (x^2+1) - (2x+2)(2x+1) \quad | \cdot 2^{-1}$$

$$1 = 2 \cdot 2 = 2(x^2+1) - 2(2x+2)(2x+1)$$

$$1 = 2 \cdot (x^2+1) + \underbrace{(2x+2)}_{-x-1} (2x+1)$$

"
 $B_P(x)$

"
 $A_P(x)$

$$A(x) = x^2 + 1, \quad B(x) = -(2x+1)$$

← jsou nesoudělné
gcd = 1

Obecné řešení

$$A(x) = (2x+2) + K(x) \cdot (x^2+1)$$

$$B(x) = 2 + K(x) \cdot (-2x-1) \\ (x+2)$$

$$K(x) \in \mathbb{Z}_3[x]$$

$$[\text{ Pozn: } (2x+1)^{-1} = 2x+2 \text{ v } \mathbb{Z}_3[x] / \equiv \text{ mod } (x^2+1)]$$

Kongruence modulo $P(x)$

$$A(x) \equiv B(x) \pmod{P(x)} \text{ iff } A(x) - B(x) = R(x) \cdot P(x) \\ \text{pro } R(x) \in \mathbb{Z}_p[x]$$

$\equiv \pmod{P(x)}$ je relace ekvivalence
je zachována při $+$, $\cdot$

Lze faktorisovat $\mathbb{Z}_p[x] / \equiv \pmod{P}$ = dyshkové třídy modulo $P(x)$
= všechny polynomy st. $< \text{st } P$

$$\text{Např. } \mathbb{Z}_3[x], \quad P(x) = x^2+1$$

$$\mathbb{Z}_3[x] / \equiv \pmod{(x^2+1)} = \{ [0], [1], [2], [x], [x+1], [x+2], \\ [2x], [2x+1], [2x+2] \}$$

$$q = 3^2 \text{ pol. st. } \leq 1 \text{ nad } \mathbb{Z}_3$$

$$(2x+1) \cdot (2x+2) = x^2 + 0x + 2 = x^2 + 1 + 1 \equiv 1 \pmod{x^2+1}$$

$$\text{Od: } \mathbb{Z}_p[x] / \cong (\text{mod } P(x)) = W$$

Kdy mají nš. pol. $Q(x) \in W$, $Q(x)$ nenulový, inverz?

$$Q(x) \cdot Q(x)^{-1} + B(x) \cdot P(x) = 1$$

↑
Kdy mají řešení?

- Když $Q(x), P(x)$ nesoudělné

- nš. $Q(x)$ sd $Q < \text{sd } P$ jsou nesoud. s $P(x)$, když P je ireducibilní

Def: $P(x)$ je ireducibilní, když nelze rozložit na součin polynomů nižšího stupně než. sd. P

$$P(x) = a \cdot (a^{-1} \cdot P(x))$$

↑
nš. pol. sd. sd. P

Tyto rozklady se dají udělat vždy → nezajímají nás

Platí: $P(x)$ ireducib. $\Leftrightarrow$ není dělitelný žádným ireducib. pol. sd. $\leq \frac{\text{sd } P}{2}$

$P(x)$ sd. 2, sd. 3 je ireducib. $\Leftrightarrow$ nemá kořen

(neboť v rozkladu by byl pol. sd. 1 a ten má vždy kořen)

Př. $\mathbb{Z}_3[x]$ najít ireducib. pol. sd. 2 a sd. 3

sd. 2: $x^2 + 1$

$$\begin{array}{l} 0 \rightarrow 1 \\ 1 \rightarrow 2 \\ 2 \rightarrow 2 \end{array}$$

$$P(x) \neq 0$$

nemá kořen a je sd. 2

→ je ireducib.

sd. 3: $x^3 + 1$

$$\begin{array}{l} 0 \rightarrow 1 \\ 1 \rightarrow 2 \\ 2 \rightarrow 0 \end{array}$$

Kořen → rozkladný $P(x)$

$$P(x) = (x-2)^3 = x^3 - \underbrace{3x^2(-2)}_0 + \underbrace{3(2^2)x}_0 - 1 = x^3 - 2 = x^3 + 1$$

$$\boxed{x^3 + 2x + 1}$$

nemá koř. a sd. 3
→ ireducib.

$$\begin{array}{l} 0 \rightarrow 1 \\ 1 \rightarrow 1 \\ 2 \rightarrow 1 \end{array}$$

Př $\mathbb{Z}_2[x]$ ireducib. pol. st. 2, st 3

st 2: $x^2 + 1$ $\begin{matrix} 0 \rightarrow 1 \\ 1 \rightarrow 0 \end{matrix}$ $P(x) = (x+1)^2$

st 3: $\frac{x^2+x+1}{\text{ireducib.}}$ $\begin{matrix} 0 \rightarrow 1 \\ 1 \rightarrow 1 \end{matrix}$

st 3.

0 není kořen $\Leftrightarrow$ abs. člen = 1
1 není kořen $\Leftrightarrow$ lichý počet sčítanců

st 3 $x^3 + x^2 + 1$

$x^3 + x + 1$

st 4. - nemá kořen

- není součinem ireduc. pol. st 2 $\neq (x^2+x+1)^2$

Závěr: $\mathbb{Z}_3[x]/\equiv (\text{mod } x^2+1)$ je těleso

$\mathbb{Z}_2[x]/\equiv (\text{mod } x^3+1)$ není těleso

8

Konečná tělesa

Galoisova tělesa $GF(p^n)$

- kon. tělesa exist. p^n a p^n prvočísl

Konstrukce

1) Pol. nad $\mathbb{Z}_p \dots \mathbb{Z}_p[x]$

ireducibilní pol. $P(x)$ stupně n

$$T = \mathbb{Z}_p[x]/\equiv (\text{mod } P(x)) = \{ [Q(x)], \text{ ať } Q < \text{st } P = n \}$$

rel. trž

+ modulo $P(x)$

$$\mathbb{Z}_3[x] / (\text{mod } x^2 + 1) = GF(9)$$

2) Druhý pohled na násobení v $GF(p^n)$

odvození: v $GF(9)$ $x^2 + 1 = 0$

ANEB $x \in GF(9)$ je kořen pol. $x^2 + 1 = 0$
 $x^2 = -1$

Zavedeme imaginární kořen i ireducibilního pol. $P(x)$

Norm. množ. $T = \{Q(i) \in \mathbb{Z}_p[i], \text{ s } Q < \text{s } P\}$

+ jako pol. $T = \{0, 1, 2, i, i+1, i+2, 2i, 2i+1, 2i+2\}$

• vyjád. jako pol. a přepisu vyšší mocniny
 dle prav. $P(i) = 0$

v $GF(9)$ $i^2 + 1 = 0$

$$\underline{i^2 = -1}$$

Např. (nad $\mathbb{Z}_3$)

$$2i \cdot (2i+2) = i^2 + i = -1 + i = i+2$$

Inverze $(2i+1)^{-1} = ai+b, a, b \in \mathbb{Z}_3$

$$\text{tj. } (2i+1)(ai+b) = 1$$

$$2a(-1) + 2bi + ai + b = 1$$

$$(2b+a)i + (b-2a) = 1$$

Stejně pol. st ≤ 1

$\rightarrow$ stejné koef. ust. mocnin

$\mathbb{Z}_3$

$$\hookrightarrow i: 2b + a = 0 \quad \rightarrow a = -2b = b$$

$$1: b - 2a = 1 \quad b - 2b = 1$$

$$-b = 1$$

$$b = 2$$

$$\Rightarrow (2i+1)^{-1} = 2i+2$$

$$P_A: GF(p) = GF(2^3)$$

nad $\mathbb{Z}_2$

ireducibil pol. st. 3

$$P(x) = x^3 + x + 1$$

(nemá kořen a je st 3 $\rightarrow$ irred)

Zavedeme imaginární kořen $\alpha: P(\alpha) = \alpha^3 + \alpha + 1 = 0$

$$T = \{ Q(\alpha) \in \mathbb{Z}_2[\alpha], \text{ st } Q \leq 2 < \text{st } P \}$$

$$= \{ 0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1 \}$$

+ jako polynomy $(\alpha^2 + (\alpha^2+1) = 2\alpha^2 + 1 = 1)$

• dle prav.

(vynásobíme-li jako pol. prvky z T vznikne až α^4)

$$\rightarrow \text{přepis prav. pro } \alpha^3 = -\alpha - 1 = \alpha + 1 \quad P(\alpha) = 0$$

$$\alpha^4 = \alpha^2 + \alpha$$

$$(\alpha \cdot P(\alpha) = 0)$$

Pozn: Pro $GF(p^n)$ je ? přesírovacích pravidel

pro $\alpha^0, \dots, \alpha^{2(n-1)}$ neboť v nosné množ. jsou pol st $\leq n-1$

$\rightarrow$ je $(n-1)$

$$\text{Např.: } (x^2+1) \cdot (x^2+x) = x^4 + x^2 + x^3 + x = \\ = x^2 + x + x + 1 + x^2 + x = 2x^2 + 3x + 1 = \underline{x+1}$$

$$\text{Inverz } (x^2+1)^{-1}$$

$$\text{chci } (x^2+1)(ax^2+bx+c) = 1$$

$$a(x^2+x) + b(x+1) + cx^2 + ax^2 + bx + c = 1$$

↳ soustava

$$\# \text{ at } x^2: a + c + a = 0 \rightarrow c = 0$$

$$x^1: a + b + b = 0 \rightarrow a = 0$$

$$x^0: b + c = 1 \rightarrow b = 1$$

$$(x^2+1)^{-1} = x$$

$$\text{Zk.: } (x^2+1)x = 1$$

$$x^3 + x = 1$$

$$x^3 + 1 + x = 1 \quad \checkmark$$

Inverzy v $GF(p^n)$

- soust. m rovnic o m neznámých

(každ. obecně sapraného inverzu jako prvku
množ. = pol. st. $\leq m-1$)

Pro velká m se vyplatí řešit polynom. rovnici (add 1)
to jako minule

$$\mathbb{Z}_2[x]/\equiv \text{mod } (x^3+x+1)$$

$$(x^2+1)^{-1} = A(x)$$

$$\text{kde } A(x)(x^2+1) + B(x)(x^3+x+1) = 1$$

↳ Eukleid

$$(1) \quad (x^3 + x + 1) = (x) (x^2 + 1) + (1)$$

$$\mathbb{Z}_2[x] \quad (x^3 + x + 1) : (x^2 + 1) = x$$

$$\frac{-x^3 - x}{1}$$

$$\text{Berout} \quad 1 = P(x) - x \cdot (x^2 + 1) = P(x) + \underbrace{x(x^2 + 1)}_{A(x) = (x^2 + 1)^{-1}}$$

3) Třetí pohled na násobení v $GF(p^m)$

- multiplikativní grupa nenulových prvků $(T \setminus \{0\}, \cdot)$
je cyklická

→ mohl vs. nenulové prvky napsat jako mocniny generátoru a při násobení počítat modulo $|T \setminus \{0\}| = p^m - 1$ v exponentu

$$(a^{|G|}) = 1 \Rightarrow (a^k)^{-1} = a^{|G| - k}$$

$$GF(p) \dots |T \setminus \{0\}| = 7$$

generátor = prvek řádu 7

řád prvků dle mohutnosti grupy → jsou tam prvky řádu 1 ($a=1$), 7 ($a = \text{vs. ostatní}$)

→ jakýkoliv $a \in T \setminus \{0\}$ lze použít jako generátor

Tabulka (pro generátor α)

α^k	α	α^2	α^3	α^4	α^5	α^6	α^7
prvek z GF(8)	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^3+1	1

$$\Phi(\alpha) = 0$$

$$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha^2 + \alpha) \cdot \alpha = \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2$$

$$\alpha^6 = \alpha^5 \cdot \alpha = \alpha \cdot (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + 1 = \alpha^2 + 1$$

(V tab. bude $p^n - 1$ přepisovacích prav.)

Např: $(\alpha^2 + 1) \cdot (\alpha^2 + \alpha) \stackrel{\text{tab}}{=} \alpha^6 \cdot \alpha^4 = \alpha^{10} \stackrel{\text{v exp počítám mod 7}}{=} \alpha^3 = \alpha + 1$

$$(\alpha^2 + 1)^{-1} \stackrel{\text{tab}}{=} (\alpha^6)^{-1} = \alpha^{7-6} = \alpha$$

+ jako pol. $\alpha^i < \alpha^j$

• jako mocniny generátoru (mod $p^n - 1$ v exp)

Pozn: Je-li $p^n - 1$ = prvočíslo,
pak každý prvek kromě 0 a 1 lze použít jako generátor
v multiplikativní grupě $T \setminus \{0\}$

$$(GF(32) = GF(2^5)) - |T \setminus \{0\}| = 31 - \text{prvočíslo}$$

$$GF(9) \quad T = \{Q(i), \text{ kde } Q \leq 1 \in \mathbb{Z}_3[i]\}$$

$$\text{prav } i^2 = -1 = 2$$

Najít generátor $(T \setminus \{0\}, \cdot)$

$$i, i^2 = -1, i^3 = -i, i^4 = 1$$

→ není generátor ($\bar{n}(i) = 4$)

$|T \setminus \{0\}| = 4$ generátor má řád 4

$$\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 2 \text{ možnosti}$$

Nebude to $i, -i, 1, -1$

→ zbylé 4 prvky jsou použitelné

Např. $i+1$

$$\left. \begin{aligned} (i+1)^2 &= i^2 + 2i + 1 = -1 + 2i + 1 = 2i \\ (i+1)^4 &= (2i)^2 = 4i^2 = -4 = 0 \end{aligned} \right\} \begin{aligned} \bar{n}(i+1) &\neq 1 \\ &\neq 2 \\ &\neq 4 \end{aligned}$$

$$\rightarrow \bar{n}(i+1) = 4$$

je to generátor

DÚ: 1) $GF(4)$ - konstruujte a vysvětlíte násobení 3 způsoby

$$2) GF(25) = GF(5^2)$$

v $\mathbb{Z}_5[x]$ ireducibil pol. st. 2 $P(x) = x^2 + x + 1$ (ne má koř.,
st. 2 → ireducibil)

$$\begin{aligned} 0 &\rightarrow 1, 1 \rightarrow 3, 2 \rightarrow 2, \\ 3 &\rightarrow 3, 4 \rightarrow 1 \end{aligned}$$

$$\text{Imaginární kořen } \alpha \quad P(\alpha) = \alpha^2 + \alpha + 1 = 0$$

$$T = \{Q(\alpha) \in \mathbb{Z}_5[\alpha], \text{st } Q \leq 1\} = \{a\alpha + b, a, b \in \mathbb{Z}_5\}$$

$$\bullet \text{ dle prav. } \alpha^2 = -\alpha - 1 = 4\alpha + 4$$

Najít generátor v $T \setminus \{0\}$ $|T \setminus \{0\}| = 24$, hledáme pr.
řádu 24 (nikoliv 2, 3, 4, 6, 8, 12)

$$3) \text{GF}(32) = \text{GF}(2^5)$$

mod $\mathbb{Z}_2$ ireducib. pol. st. 5 $P(x) = x^5 + 1$
 lichý počet

$R \cdot Q \neq P$ nemá kořen

st. 1 st. 4

P ireducib.

+ Zkusit, že $P(x)$ nemá dělit ireducib. pol. st. 2 (ten je jediný $x^2 + x + 1$)

Najít $(x^2 + 1)^{-1}$
 $(x^2 + 1)^{-1}$

$\rightarrow P \neq Q \cdot R$
 st. 2 st. 3

9

Isomorfismus konečných těles

Platí: Konečná tělesa o stejném počtu prvků jsou
 isomorfní (liší se jen v pojmenování prvků)

Isomorfismus = vzájemně jednozn. zobr. mezi nosnými
 množ. $\varphi: T_1 \rightarrow T_2$ které zachovává operace $+$, $\cdot$

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$\text{GF}(p^m)$... v $\mathbb{Z}_p[x]$ vezmeme ireducib. pol. st. m ... $P(x)$

$$T = \mathbb{Z}_p[x] / \equiv \text{mod } P(x)$$

$$GF(8) = GF(2^3)$$

$\in \mathbb{Z}_2[x]$ ireducibil pol. st 3 $P_1(x) = x^3 + x + 1$

$$P_2(x) = x^3 + x^2 + 1$$

$$T_1 = \mathbb{Z}_2[x] / \equiv \text{mod } P_1$$

2. zp.
nás.

imaginární kořen $\alpha \dots P(\alpha) = \alpha^3 + \alpha + 1 = 0$

$$T_1 = \{a\alpha^2 + b\alpha + c; a, b, c \in \mathbb{Z}_2\}$$

+ jako pol

- dle prav. $\alpha^3 = \alpha + 1$
 $\alpha^4 = \alpha^2 + \alpha$

$$T_2 = \mathbb{Z}_2[x] / \equiv \text{mod } P_2$$

2. zp.

imaginární kořen β pol. P_2 $P_2(\beta) = \beta^3 + \beta^2 + 1 = 0$

$$T_2 = \{a\beta^2 + b\beta + c, a, b, c \in \mathbb{Z}_2\}$$

+ jako pol

- dle prav $\beta^3 = \beta^2 + 1$
 $\beta^4 = \beta^3 + \beta = (\beta^2 + 1) + \beta$

Budeme hledat vřej. jednozn. zobr. $\varphi: T_1 \rightarrow T_2$
které zachová + i.

$\rightarrow$ zachová neutrály $\varphi(0) = 0, \varphi(1) = 1$

Když budm znát $\varphi(\alpha)$, pak (kvůli +):

$$(*) \quad \varphi(a\alpha^2 + b\alpha + c) = a\varphi(\alpha)^2 + b\varphi(\alpha) + c$$

[Pak je zachováno + : $\varphi((a_1\alpha^2 + b_1\alpha + c) + (a_2\alpha^2 + b_2\alpha + c)) =$
 $= \varphi(a_1 + a_2, b_1 + b_2, c_1 + c_2)$

✓

$$= \left((a_1 + a_2)x^2 + ()x + () \right) = (a_1 + a_2)\varphi(x)^2 + (b_1 + b_2)\varphi(x) + (c_1 + c_2)$$

$$\varphi() + \varphi() = (a_1\varphi(x)^2 + b_1\varphi(x) + c_1) + (a_2\varphi(x)^2 + b_2\varphi(x) + c_2)$$

Aby bylo zachováno násobení, tak musí $\varphi(x)$ splňovat
stejná pravidla jako x

stačí 1. prav. $x^3 = x + 1 \rightarrow \varphi(x)^3 = \varphi(x) + 1$ předch. str.

[Součin pol. problém stejně v T_1 i T_2 díky (*) a pak
stejně přepíšeme výš mocniny]

Hledám řeš. rov. $\varphi(x)^3 = \varphi(x) + 1$ (tj. $x^3 = x + 1$ tj. hledám
kořen $P_1(x) = x^3 + x + 1$ v tělese T_2)

$$\varphi(x) \neq \beta \text{ neboť } \beta^3 = \beta^2 + 1$$

$$\varphi(x) = \beta^2 + 1$$

$\text{nad } \mathbb{Z}_2$ $\vee T_2: (\beta^2 + 1)^3 = (\beta^2 + 1)(\beta^4 + 2\beta^2 + 1) =$

$$= (\beta^2 + 1)(\beta^2 + \beta + 1 + 1) = \beta^4 + \beta^2 + \beta^3 + \beta =$$

$$= \beta^2 + \beta + 1 + \beta^2 + 1 + \beta^2 + \beta = \underline{\beta^2}$$

$$(\beta^2 + 1) + 1 = \underline{\beta^2}$$

ANO, $(\beta^2 + 1)$ je kořenem $P_1(x)$

$$T_1 \xrightarrow{\varphi} T_2$$

$$A \quad 0 \longrightarrow 0$$

$$B \quad 1 \longrightarrow 1$$

$$C \quad \alpha \longrightarrow \beta^2 + 1$$

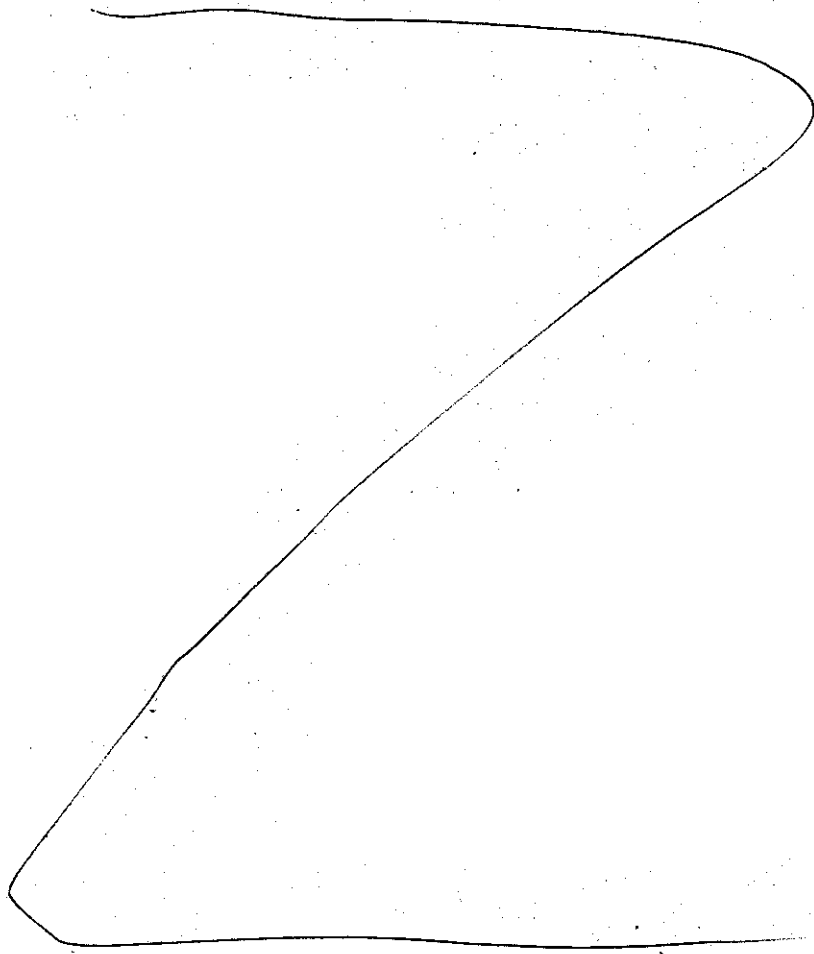
$$D \quad \alpha + 1 \longrightarrow \varphi(\alpha) + \varphi(1) = \beta^2 + 1 + 1 = \beta^2$$

$$E \quad \alpha^2 \longrightarrow \varphi(\alpha)^2 = (\beta^2 + 1)^2 = \beta^4 + 1 = (\beta^2 + \beta + 1) + 1 = \beta^2 + \beta$$

$$F \quad \alpha^2 + 1 \longrightarrow \varphi(\alpha)^2 + 1 = \beta^2 + \beta + 1$$

$$G \quad \alpha^2 + \alpha \longrightarrow \varphi(\alpha)^2 + \varphi(\alpha) = (\beta^2 + \beta) + (\beta^2 + 1) = \beta + 1$$

$$H \quad \alpha^2 + \alpha + 1 \longrightarrow \varphi(\alpha)^2 + \varphi(\alpha) + \varphi(1) = (\beta + 1) + 1 = \beta$$



Lineární kódy

Def: Lineární kód K délky n dimenze k je podprostor $\mathbb{Z}_p^n$ dimenze $K = k$.

(T^n , kde T konečné těleso)

→ tento kód má k - info znaků
 $n-k$ - kontrolních znaků

prvek podprostoru = kódové slovo

Generující matice $G =$ n řádků jsou báze vektorů prost. K
 $\begin{pmatrix} \\ \\ \end{pmatrix}$
 $k \times n$

Zahodování $(a_1, \dots, a_k) \cdot G = \bar{w}$ ($\bar{w}$.. kódové slovo)

Systematický kód $G = (E | B) \rightarrow (a_1, \dots, a_k) \cdot G = (\underbrace{a_1, \dots, a_k}_{\text{info}}, \underbrace{b_{k+1}, \dots, b_n}_{\text{kontrol. zn.}})$

Na podprostor K se lze dívat jako na prostor všech řeš.

homog. soust. $H \cdot \bar{x}^T = \bar{0}^T$

Kontrolní matice = matice té homog. soust.

Výpočet: $H \cdot \bar{w} = \bar{0}$ matice samých nul

$$H \cdot G^T = \mathbf{0} \quad \begin{pmatrix} \\ \end{pmatrix}^T$$

$$G \cdot H^T = \mathbf{0}$$

→ V řádcích matice H jsou báze vektorů prostoru vs. řeš.

hom. soust. $G \cdot \bar{x}^T = \bar{0}^T$

A NAOPAK

Pro syst. kód $G = (E_m | B)$ vyjde $H = (-B^T | E_n)$

$$\underline{P\bar{r}}: \mathbb{Z}_2$$

Kód délky 4, dim 3

Kontrola parity $(1, 1, 0, 0)$ $\nwarrow$ kontrol

$$\bar{w} = (a_1, a_2, a_3, b)$$

b přidáme tak, aby $a_1 + a_2 + a_3 + b = 0$ $\text{nad } \mathbb{Z}_2$

$$K = \{ \bar{w}, \bar{w} \}$$

báze: $\bar{b}_1 = (1, 0, 0, 1)$ $\begin{matrix} \text{info} \\ \downarrow \end{matrix}$

$\bar{b}_2 = (0, 1, 0, 1)$

$\bar{b}_3 = (0, 0, 1, 1)$

lin.
nezáv.

$$\bar{w} = (a_1, a_2, a_3, b) =$$

$$= a_1(1, 0, 0, 1) + a_2(0, 1, 0, 1) + a_3(0, 0, 1, 1)$$

$$= (a_1, a_2, a_3, (a_1 + a_2 + a_3))$$

OK, neboť $a_1 + a_2 + a_3 + b = 0$

$$\rightarrow b = -a_1 - a_2 - a_3$$

$$= a_1 + a_2 + a_3 \text{ nad } \mathbb{Z}_2$$

$|K| = 8$ neboť $a_1, a_2, a_3 \in \mathbb{Z}_2$ lib. (souř. vůči bázi)

$$K = \{ (1, 0, 0, 1), (0, 1, 0, 1), (0, 0, 1, 1), (1, 1, 0, 0), (1, 0, 1, 0), (0, 1, 1, 0), (1, 1, 1, 1), (0, 0, 0, 0) \}$$

= vš. slova nad $\mathbb{Z}_2$ délky 4, která mají sudý počet 1

$$G = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array} \right) = (E_3, B)$$

$$H = (-B^T, E) = (-1, -1, -1 | 1) = (1111)$$

$$H \cdot \bar{w} = \bar{0} \quad 1 \cdot a_1 + 1 \cdot a_2 + 1 \cdot a_3 + 1 \cdot b = 0$$

Posílá $\bar{w} \xrightarrow{\text{přenos}} \text{Přijmeme } \bar{v}$

za předp. ≤ 1 chyby

$$H \cdot \bar{v}^T = \bar{0}^T \rightarrow \text{bez chyby}$$

$$H \cdot \bar{v}^T \neq \bar{0}^T \rightarrow \text{chyba}$$

Pokud umíme určit $H \cdot \bar{v} = e \cdot s_i$
 $\hookrightarrow i$ -tý sl. v H

$$\text{pak } \bar{w} = \bar{v} - (0, \dots, 0, e, 0, \dots, 0)$$

 $\hookrightarrow i$ -tá

chybové slovo

Platí: Pokud n je každých k sloupců $\leq n$, pak pro $\leq k$ chyb
 ≥ 1

vychází $H \cdot \bar{v} \neq \bar{0}$ (objevuje k chyb) a umíme opravit $\lceil \frac{k}{2} \rceil$ chyb

$\underline{PA}: \mathbb{Z}_5$ generující matice $G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

Kód délky 5, 3-info znaky, 2 kontrolní

spočítejte kontrolní matici H

Zjistěte, zda přijaté slovo je bez chyb (je-li možno;
opravte chyby)

$$\bar{v}_1 = (4, 0, 1, 1, 4)$$

$$\bar{v}_2 = (4, 0, 0, 3, 0)$$

$$G = (E | B) \rightarrow H = (-B^T, E)$$

$$= \left(\begin{array}{ccc|cc} -2 & 0 & -2 & 1 & 0 \\ -2 & -2 & -4 & 0 & 1 \end{array} \right) =$$

$$= \left(\begin{array}{ccccc} 3 & 0 & 3 & 1 & 0 \\ 3 & 3 & 1 & 0 & 1 \end{array} \right)$$

$$H \cdot \bar{v}_1^T = \begin{pmatrix} 3 & 0 & 3 & 1 & 0 \\ 3 & 3 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 0 \\ 1 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$\rightarrow$ $\bar{v}$ není kódové slovo
 $\rightarrow$ je tam chyba

$$\text{syndrom} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$= 2 \cdot S_3$$

jiný sloupec nejde

$$\bar{v}_2 = \bar{w} + (0, 0, 2, 0, 0)$$

$$H \cdot (\bar{v}_2^T) = H \cdot \bar{w} + H \cdot \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + 2S_3$$

$$\bar{w}_2 = \bar{v}_2 - \bar{e} = (4, 0, 1-2, 1, 4) = \underline{\underline{(4, 0, 4, 1, 4)}}$$

$$\bar{v}_2 : H \cdot \bar{v}_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 4S_2$$

$$\text{syndrom} = 2S_5$$

$\rightarrow$ nemůžeme opravit

10

Cyklické kódy

Def: Lineární kód je cyklický, když cyklické posunutí kódového slova je kódové slovo, tj.

$$\bar{v} = (v_0, v_1, \dots, v_{n-1}) \in K \rightarrow c(\bar{v}) = (v_{n-1}, v_0, \dots, v_{n-2}) \in K$$

Můžeme si zde na kódová slova délky n dívat jako na pol. st. $\leq n-1$

$$\bar{v} \rightarrow v(x) = v_0 + v_1 x + v_2 x^2 + \dots + v_{n-1} x^{n-1}$$

Počítáme-li modulo $(x^m - 1)$, pak cykl. posun odpovídá násobení x

$$c(\bar{v}) \rightarrow x \cdot v(x) = v_0 x + v_1 x^2 + \dots + v_{m-1} x^m$$

$$\equiv 1 \pmod{x^m - 1}$$

$\rightarrow$ používáme faktorový okruh

$$\rightarrow \bar{v} \in \mathbb{Z}_p^m \rightarrow v(x) \in \mathbb{Z}_p[x] / \equiv \pmod{x^m - 1}$$

$\rightarrow$ cykl. kód K je podprostor $\mathbb{Z}_p^{(m)}$

$$\text{hde } v(z) \in K \rightarrow z \cdot v(z) \in K$$

$$\text{Tudíž } v(z) \in K \rightarrow z^k \cdot v(z) \in K$$

$$\Rightarrow f(z) \cdot v(z) \in K$$

$$(K \text{ je ideál v okruhu } \mathbb{Z}_p^{(m)})$$

generující polynom $g(z) \in K$

cykl. kód délky n a dim k

$$v(z) \in K \iff v(z) = f(z) \cdot g(z)$$

kódové
sl.

pro nějaký pol. $f(z) \in \mathbb{Z}_p^{(m)}$

$$\text{sd } g = n - k$$

$g(z)$ = nenulový kódový pol. min. stupně

(ex. jediný až na konst. násobky)

$\uparrow$ 2. pohled na faktor. okruh

- zavedeme imag. kořen α
polynomu $x^m - 1$ ($\alpha^m - 1 = 0$)

norma množ

$$\{P(z) \in \mathbb{Z}_p[z], \text{ st } P \leq m-1\}$$

$$= \{v_0 + v_1 z + \dots + v_{m-1} z^{m-1},$$

$$v_i \in \mathbb{Z}_p\}$$

+ jako pol.

• jako pol + pravidla

$$z^m = 1$$

$$z^{m+1} = z$$

$$z^{2m-2} = z^{m-2}$$

$\uparrow$ kračí se $\mathbb{Z}_p^{(m)}$

Platí $g(z), z g(z), \dots, z^{k-1} g(z)$ tvoří bázi v K

→ generující matice $\begin{pmatrix} g(z) \\ z g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} \leftarrow \text{koef. od nejvyššího}$

Kódování: info $\bar{a} = (a_0 \dots a_{k-1})$

$$\bar{v} = \bar{a} \cdot G = (a_0 \dots a_{k-1}) \begin{pmatrix} g(z) \\ z g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix}$$

$$= \underbrace{(a_0 + z a_1 + \dots + a_{k-1} z^{k-1})}_{a(z)} \cdot g(z)$$

$$\Rightarrow v(z) = a(z) \cdot g(z)$$

Kontrolní polynom

Platí: $g(x)$ dělí $(x^n - 1)$ beze zbytku. $\rightarrow h(x) = (x^n - 1) : g(x)$

$h(z)$ je kontrol. pol. $v(z) \in K \leftrightarrow h(z) \cdot v(z) = 0$ v $\mathbb{Z}_p^{(n)}$
 $= \mathbb{Z}_p[x] / \equiv \text{mod } x^n - 1$

Dekodování: $v(z) : g(z) = a(z)$ - info. pol.

PA: $\mathbb{Z}_2 \quad G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \leftarrow b_1$
 $\leftarrow b_2$

Kód délky 4 dim 2 $\rightarrow$ 2 info zn.

Vypíšte kódová slova a ověřte, že K je cyklický

$$K = \{ a_1 \cdot \bar{b}_1 + a_2 \cdot \bar{b}_2, a_i \in \mathbb{Z}_2 \} = \left\{ \begin{matrix} (1111), (0101), \\ \bar{b}_1 & \bar{b}_2 \\ (1010), (0000) \end{matrix} \right\}$$

$$|K| = 4$$

$$\bar{b}_1 + \bar{b}_2 \quad 0 \cdot \bar{b}_1 + 0 \cdot \bar{b}_2$$

$$c(\bar{b}_1) = \bar{b}_1 \in K, c(\bar{b}_2) = \bar{b}_1 + \bar{b}_2 \in K, \text{ATD} \rightarrow \text{je cykl}$$

$\rightarrow$ lze K chápat jako podpr. $\mathbb{Z}_2^{(4)} \rightarrow$ pol. st ≤ 3
 $\mathbb{Z}^4 = 1$

$$K = \{ 1 + \mathbb{Z} + \mathbb{Z}^2 + \mathbb{Z}^3, \mathbb{Z} + \mathbb{Z}^3, 1 + \mathbb{Z}^2, 0 \}$$

$$\text{gener. pol. } g(\mathbb{Z}) = 1 + \mathbb{Z}^2 \quad (\text{nenulový min st.})$$

$$\text{ověření} \quad 0 = 0 \cdot (1 + \mathbb{Z}^2)$$

$$1 + \mathbb{Z}^2 = 1 \cdot (1 + \mathbb{Z}^2)$$

$$\mathbb{Z} + \mathbb{Z}^3 = \mathbb{Z} \cdot (1 + \mathbb{Z}^2)$$

$$1 + \mathbb{Z} + \mathbb{Z}^2 + \mathbb{Z}^3 = (1 + \mathbb{Z}) \cdot (1 + \mathbb{Z}^2)$$

$$\text{Kódování info } (a_0 a_1) \rightarrow a_0 + a_1 \mathbb{Z}$$

$$v(\mathbb{Z}) = (a_0 + a_1 \mathbb{Z}) \cdot g(\mathbb{Z})$$

což je vlastně
tato tabulka

Toto kódování odpovídá násobení gen. mat.

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \leftarrow g(\mathbb{Z}) = 1 + \mathbb{Z}^2$$

$$\leftarrow \mathbb{Z} \cdot g(\mathbb{Z}) = \mathbb{Z} + \mathbb{Z}^3$$

$$\begin{pmatrix} 1 & 1 \end{pmatrix} \cdot G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\bar{a}$$

G, G_1 - Gauss. eliminací vyrobím $G, \mathbb{Z} G$

$\rightarrow$ řádky generují stejný prostor (kód K)

$$\text{zakódování } (a_0 a_1) \cdot G = \bar{v}$$

$$(a_0 a_1) \cdot G_1 = \bar{w}$$

$\uparrow$ stejné info se zakóduje na jiné kódové slovo
(stejný kód)

Zakódování jinak pospojíte do dvojic info a kódová slova.

Pr $\mathbb{Z}_3$ kód cyklu délky $n=6$

$\hookrightarrow$ gener. pol. $g(z) = z^2 + 2$

? - Info znaků je 4 $n=6$, $\text{ne } g$ 2. mocnina, nemůžeme
kacykčit $\rightarrow$ info slovo max 2^3
 $\rightarrow 4$ znaky

? - odpovídající gener. matice $G =$

$$G = \begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow g(z) \\ \leftarrow zg(z) \\ \leftarrow z^2g(z) \\ \leftarrow z^3g(z) \end{matrix}$$

Zakódujte $\bar{a} = (2 \ 2 \ 1 \ 0)$

$$\rightarrow a(z) = 2 + 2z + z^2$$

$$\rightarrow v(z) = a(z) \cdot g(z) = (2 + 2z + z^2) (2 + z^2) =$$

$$= 1 + z + 2z^2 + 2z^2 + 2z^3 + z^4 = 1 + z + z^2 + 2z^3 + z^4$$

$$\rightarrow \bar{v} = (1 \ 1 \ 2 \ 2 \ 0)$$

Spočítejte hromadní polynom

$$h(x) = (x^6 - 1) : g(x)$$

$$\text{v } \mathbb{Z}_3[x] \quad (x^6 - 1) : (x^2 + 2) = x^4 + x^2 + 1$$

$$\begin{array}{r} \text{míteliv v } \mathbb{Z}_3^{(6)} \quad \underline{-x^6 - 2x^4} \\ 1x^4 \\ \underline{-x^4 - 2x^2} \\ x^2 - 1 \\ \underline{-x^2 - 2} \\ 0 \end{array}$$

$$\rightarrow h(z) = z^4 + z^2 + 1$$

$\hookrightarrow x^2 + 2$ je dělitel $(x^6 - 1)$ nad $\mathbb{Z}_3$

$\Rightarrow g(z) = z^2 + 2$ lze použít

jako gener. polynom. cyklu
délky 6 nad $\mathbb{Z}_3$

- Overle, zda $u(x) = 2x + 2x^3 + 2x^5$ je bez chyby

$$u(x) \cdot h(x) = 0 \quad \text{v } \mathbb{Z}_3^{(6)}$$

$$x^6 = 1$$

$$x^7 = x$$

$$\vdots$$

$$(2x + 2x^3 + 2x^5) \cdot (x^4 + x^2 + 1) =$$

$$= \cancel{2x^5} + \cancel{2x^7} + \cancel{2x^9} + \cancel{2x^5} + \cancel{2x^7} + \cancel{2x^9} + \cancel{2x} + \cancel{2x^3} + \cancel{2x^5} =$$

$$= \underset{0}{6x} + \underset{0}{6x^3} + \underset{0}{6x^5} = 0$$

$$(2x^5 + 2x^3 + 2x) : g(x) = a(x) = x + 2x^3$$

$$\rightarrow \bar{a} = (0102)$$

Systematické kódování

$$\bar{a} = (a_0 \dots a_{k-1}) \rightarrow \bar{u} = (\underbrace{a_0, \dots, a_{k-1}}_{\text{info na zač. kód. slova}}, b_1, \dots, b_{n-k})$$

• Generátor matice

$$G \sim (E | B)$$

↑ úpravy Gauss. elim. + změna pořadí sloupců

• Polynomy u cykl. kódů

- bude třeba příst mocniny od nejvyšší

info $\bar{a} = (a_0, \dots, a_{k-1}) \rightarrow v(z) = a_0 z^{n-1} + \dots + a_{k-1} z^{n-k} + b_1 z^{n-k-1} + \dots + b_{n-k}$

kódový pol = násobek gener. pol.

Víme $\deg g = n-k$

$\rightarrow$ Vezmeme $(a_0 z^{n-1} + \dots + a_{k-1} z^{n-k}) : g(z)$

$\swarrow$ $rb = r(z)$ $\text{st } r \leq n-k-1$
 $v(z) = \tilde{a}(z) - r(z)$ $\text{je dělitelné pol } g(z)$

$= a_0 z^{n-1} + \dots + a_{k-1} z^{n-k} + \underbrace{b_1 z^{n-k-1} + \dots + b_{n-k}}_{-r(z)}$

Viz předchozí pří.

$\bar{a} = (2 \ 2 \ 1 \ 0) \rightarrow \tilde{a}(z) \cdot g(z) = (2z^5 + 2z^4 + z^3 + 0z^2) : (z^2 + 2) =$
 $\text{postup dělení} \quad \vdots \quad = 2z^3 + 2z^2 + 2$
 $r(z) = 2 = -1$

$\rightarrow v(z) = 2z^5 + 2z^4 + z^3 + 0z^2 + 0z + 1$
 $(-r(z))$

$\bar{v} = (\underbrace{2 \ 2 \ 1 \ 0 \ 0 \ 1}_{\text{info}})$

Kontrola $h(z) \cdot v(z) = 0$

Dekodování - první k znaků je info

PA : $\mathbb{Z}_2$ Najít všechny cyklické kódy délky 5 nad $\mathbb{Z}_2$

$\rightarrow g(x)$ musí dělit $(x^5 - 1)$ v $\mathbb{Z}_2[x]$
gener. pol.

Rozložit $(x^5 - 1)$ na irred. pol.

$$(x^5 - 1) = (x - 1) \cdot (x^4 + x^3 + x^2 + x + 1)$$

(kořen 1)

z 2
mohou být
gener. polynomy

je
irreducibilní

není kořen $\rightarrow$ nelze P. Q
st 1 st 3

- není dělitelný ani irred. pol. st. 2

(ten je jeden $x^2 + x + 1$)

$\rightarrow$ nelze rozložit P. Q
st 2

Exist 2 cykl. kódy

1) $g(z) = z - 1$

2) $g(z) = z^4 + z^3 + z^2 + z + 1$

(napíšte gen. matice

$\rightarrow$ 1) je kód parity

$\rightarrow$ 2) je opakov. kód

(11)

viz na kopie

cv. 11 poskytl Karlosak

(11)

Použití konečných těles

1) Imaginární kořeny cyklických kódů

Př.: Hammingův kód délky 7 - ve sloupcích kontrol. matice H binár. rozvoji 1-7

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$\begin{matrix} 1 & 2 & 3 & \dots & 7 \end{matrix}$

kód není cyklický

$$\bar{v} = (1101001) \in K$$

$$\text{ale } c(\bar{v}) = (1110100) \notin K$$

$$H \cdot \bar{v}^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \bar{v} \in K$$

je kódové slovo

$$H \cdot c(\bar{v})^T = \begin{pmatrix} - & - & - \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow c(\bar{v}) \notin K$$

Cíl: pokusíme se změnit pořadí sloupců mat. H , aby vzniklý kód byl cyklický

Sloupce matice H budeme chápat jako koef. polynomů st. ≤ 2

$\rightarrow$ tedy jako prvky $\mathbb{GF}(8) = \mathbb{Z}_2[x] / \equiv \text{mod } (x^3 + x + 1)$

$$T = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_2\}$$

α irrac. kořen $P(x)$

$\rightarrow$ dle pravidla $\alpha^3 = \alpha + 1$

Platí: α je generátor multiplikační grupy $(T \setminus \{0\}, \cdot)$, tj. řád α je 7

$\alpha^1, \alpha^2, \dots, \alpha^7 = 1 \Rightarrow$ různé mocniny, které vytvoří všechny nenulové prvky $\mathbb{GF}(8)$ $\rightarrow \alpha$ je tzv. primitivní prvek $\mathbb{GF}(8)$

α^1	α^2	α^3	α^4	α^5	α^6	α^7
α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

Kontrolní matice: Hamming. kód

$$H = (1 \alpha \alpha^2 \alpha^3 \dots \alpha^6)$$

$$\alpha^5 = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$$

$$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$$

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \leftarrow \alpha^2 \\ \leftarrow \alpha \\ \leftarrow 1 \end{matrix}$$

Tato H je kontrolní matice cykl. kódu, neboť: $H \cdot \bar{v}^T = \bar{0}^T$ pro $\bar{v} \in K$

$$(1 \alpha \alpha^2 \dots \alpha^6) \cdot \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{m-1} \end{pmatrix} = v_0 + v_1 \alpha + v_2 \alpha^2 + \dots + v_6 \alpha^6 = 0$$

aneb α je kořen kódového pol. $v(\alpha) = v_0 + v_1 \alpha + \dots + v_{m-1} \alpha^{m-1}$

$v(\alpha) \in K$, iff $v(\alpha) = 0 \rightarrow$ potom $v(\alpha)$ nemá žádný kořen...

$$\alpha := \alpha$$

$$\alpha \cdot v(\alpha) = \alpha \cdot 0 = 0 \quad \text{cykl. poslocení} \quad (\alpha^7 = 1)$$

$$\rightarrow \alpha \cdot v(\alpha) \in K \quad \text{tedy kód je cyklický}$$

Generující polynom $g(\alpha) = \alpha^3 + \alpha + 1$ je pol. min. sd., který má kořen α

$$(\forall j. j \in K)$$

$$\leftarrow \text{Kontrolní polynom } h(\alpha) \dots (x^7 - 1) = g(x) = h(x)$$

$\leftarrow$ Kontrola - dosadím α do příslušného pol. $u(\alpha)$

$$\left\{ \begin{array}{l} \text{když } u(\alpha) = 0 \rightarrow u(\alpha) \text{ kódový} \\ \text{když } u(\alpha) = \alpha^k \quad (k \in \{0, 1, \dots, 6\}) \rightarrow 1 \text{ chyba na } k\text{-té pozici} \end{array} \right.$$

$$u(\alpha) = u_0 + u_1\alpha + \dots + u_{m-1}\alpha^{m-1}$$

$$\xrightarrow{\text{opravím na}} v(\alpha) = u_0 + \dots + (u_{k-1})\alpha^k + \dots + u_{m-1}\alpha^{m-1}$$

2) Latinské čtverce

Def. = Latinský čtverec vel. n je čtvercové schéma $n \times n$, kde v každém řádku i sloupci jsou všechna čísla od 1 do n .
(tedy čísla v řádku či sloupci se neopakuji)

Př. = Lat. čtverec vel. 3 s 1. řádkem 1 2 3

$$L_1 = \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 3 & 3 & 1 & 2 \end{array} \quad L_2 = \begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 3 & 1 & 2 \\ 3 & 2 & 3 & 1 \end{array}$$

Další čtverce by měly jiné pořadí sloupců
 $\rightarrow$ celkem je jich $(3!) \cdot 2 = 12$

Pozorování = Grupa o n prvcích nřcuje latinský čtverec $n \times n$.

Důkaz = Tabulka pro operaci na grupě $(G, *)$:

$$\begin{array}{c|cccc} * & a_1 & a_2 & \dots & a_n \\ \hline & & & & \\ \hline i\text{-tý} \rightarrow a_i & & a_s & & a_s \end{array}$$

$\Rightarrow$ v každém řádku (sloupci) je každý prvek právě jednou

$$\text{kdyby } a_{i0} = a_i * a_j = a_s = a_i * a_k$$

a_i má inverz v grupě $\rightarrow$ vynásob. rovnici a_i^{-1}

$$a_i = a_k \quad \left\{ \begin{array}{l} (a_i^{-1} * a_i) * a_j = (a_i^{-1} * a_i) * a_k \end{array} \right.$$

Opacná implikace: když $a_j \neq a_k$ (jiný sloupec) pak $a_i * a_j \neq a_i * a_k$ (jiné výsledky)

$*$	a_i

$\xrightarrow{\text{přejmenování}} \boxed{\text{latin. čtverec}}$
 $a_i \rightarrow i$

Poznámka: Ne každý latin. čtverec vznikl z grupy.

$$L_1 =$$

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

$\xrightarrow{\text{přejmenování}}$
 $1 \rightarrow 0$
 $2 \rightarrow 1$
 $3 \rightarrow 2$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$(\mathbb{Z}_3, +)$

* má neutrála 1

* má inverzy (1 v každém ř.-i sl.)

* je asociativní

$(L_1, *)$ je izomorfna $(\mathbb{Z}_3, +)$

$\rightarrow$ * stejné vlastnosti jako + na $\mathbb{Z}_3$

$\rightarrow$ * je asoc.

$\cup L_2$ nelze najít neutrála
 $\rightarrow$ nevznikla z grupy

Položíme L_1^1, L_1^2 na sebe a prohledáme uspořádané dvojice (L_{ij}^1, L_{ij}^2)

1	2	3
2	3	1
3	1	2

} obsahuje všechny uspořádané dvojice $(a, b) \in \{1, 2, 3\} \times \{1, 2, 3\}$
 a každá právě jednou
 $\Rightarrow$ takové čtverce nazýváme na sebe kolmé (ortogonální)

Def.: Latinské čtverce L^1, L^2 jsou na sebe kolmé / ortogonální, když pro každou dvojici (a, b) lze najít pozici (i, j) tak, že:

$$(i, j) \in \{1, \dots, n\}^2$$

$$(L_{ij}^1, L_{ij}^2) = (a, b).$$

aneb: dvojice se v přebýhání čtverců neopakuje.

Věta = 1) Nelze najít více než $(n-1)$ po dvou ortogonálních latin. čtverců $n \times n$

2) Je-li $n = p^m$, pak skutečně existuje $(n-1)$ po dvou ortogonál. lat. čtverců $n \times n$.

[Pozn. pro $n=6$ neexist. ani dvojice ortog. čtverců 6×6]

Důkaz 2): Zkonstruujeme $L^1, \dots, L^{n-1}$ pro dvou ortogonál.

Vezmeme $GF(p^m) = GF(n)$ kon. těleso (existuje pro mocniny prvočíslo)

Vezmeme α = primitivní prvek v tělese T (tj. generátor $(T, \{0\}, +, \cdot)$)

$\alpha^1, \alpha^2, \dots, \alpha^{n-1} = 1$ jsou všechny (různé) prvky z $T \setminus \{0\}$

Uděláme tabulku pro $+$ na T :

L^k	$+$	α	α^2	$\dots$	α^{n-1}	0
0		α	α^2			
α^k		α^{k+1}	α^{k+2}			
α^{k+i}						
$\vdots$						
$1 = \alpha^{n-1}$						
α						
α^{k-1}						

$\alpha^k = \alpha^j$

přejmenování

$\alpha^t \rightarrow t$
 $t \in \{1, \dots, n-1\}$
 $0 \rightarrow n$

1	2	$\dots$	$(n-1)$	n
t				

L^k

1) L^k je lat. čtverec, neboť vznikl z grupy $(T, +)$

2) L^k, L^l jsou ortogonální pro $k \neq l$

Latinské čtverce 5×5

Nejprve ukážu kolmost dvou takto složených čtverců 5×5

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

primitivní prvek α je řádu 4

$\alpha = 2 \quad \alpha^2 = 4 \quad \alpha^3 = 3 \quad \alpha^4 = 1$

$\rightarrow \alpha = 2$ je prim. prvek

$a \in \mathbb{Z}_5$	1	2	3	4	0
$\downarrow$					
$\alpha^k = 2^k$	2^4	2^1	2^3	2^2	
přejmenování	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	4	1	3	2	5

L^1	$+$	2^1	2^2	2^3	2^4	0
0		2^1	2^2	2^3	2^4	0
$2 = 2^1$		2^2	2^3	2^4	0	2^1
$4 = 2^2$		2^3	2^4	0	2^1	2^2
$3 = 2^3$		2^4	0	2^1	2^2	
$1 = 2^4$		0	2^1	2^2		

$\rightarrow$

1	2	3	4	5
2	4	5	3	1
4	3	1	5	2
5	1	4	2	3
3	5	2	1	4

$= L^1$

L^2

0
 $4 = 2^2$
 2^3
 2^4
 2^1

$\rightarrow$

R_1
R_3
R_4
R_5
R_2

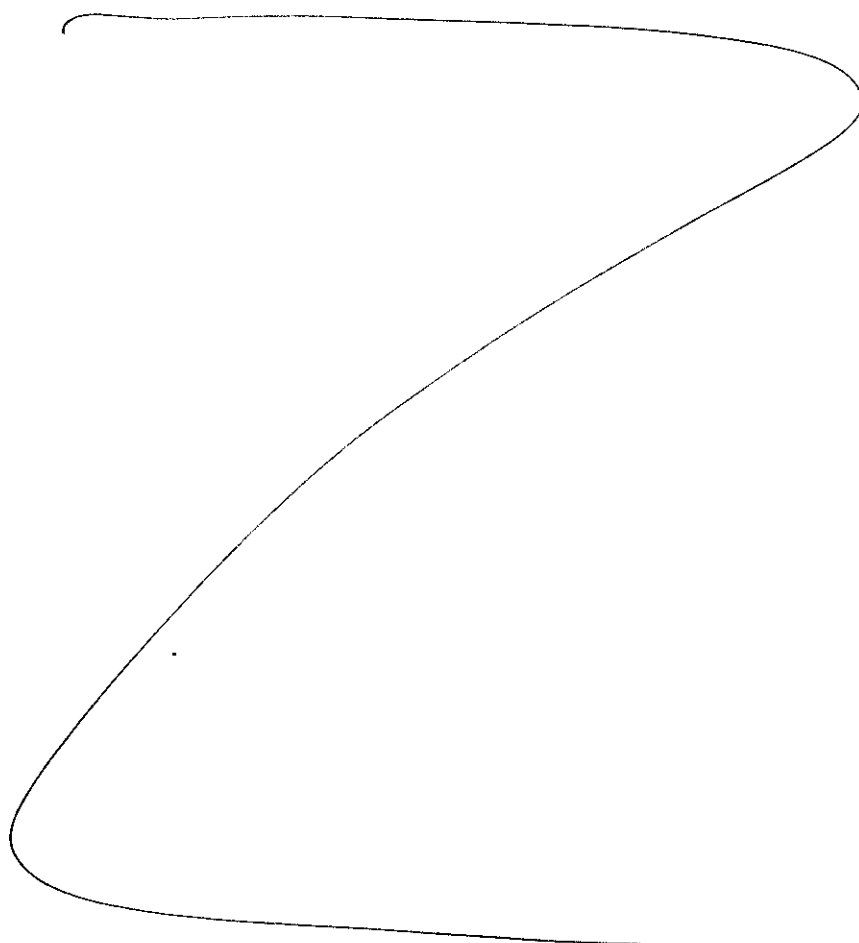
//

①	2	3	4	5
4	3	1	5	②
5	1	④	2	3
3	⑤	2	1	4
2	4	5	③	1

$= L^2$

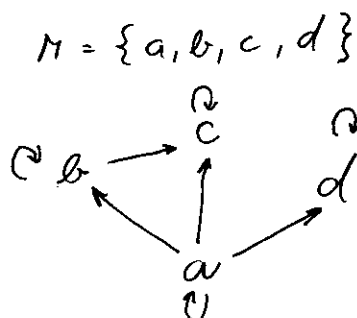
orthogonal.

)



Uspořádané množiny a svazy

$(M, \leq)$ uspoř. množ. = množ., na níž je def. relace
uspořádání (tj. reflex., antisym., tranzit. relace)



$$U = \{ (a,b), (a,a), (b,b), (c,c), (d,d), (b,c), (a,c), (a,d) \}$$

" $\leq$ "

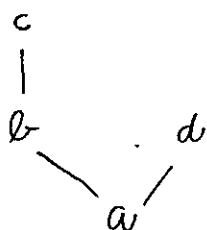
U je refl

antisym

- nikdy mezi různými prvky
nejvýše jedním směrem

tranz

Hasseho diagram (jenom pro relace uspořádání)



nejmenší prvek a
největší prvek neex.
minimální a
maximální c, d

Pojmy - největší prvek $a \in M : x \leq a$ pro vš. $x \in M$
(větší (roven) než vš. prvky)

nejmenší prvek ...

maximální prvek $b \in M : \text{neexist. } x \in M \text{ tak, že } b \leq x$
(neex. nic většího, ale mohou exist.)

neporovnatelné prvky

minimální

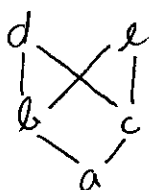
Značení : největší pr. $\frac{1}{0}$
 nejmenší 0

Pojmy - supremum ... $\sup \{a, b\} = s \in M$, kde
 množ $\{a, b\}$

1) $a \leq s, b \leq s$

2) když $a \in K, b \in K$, pak $s \in K$
 „nejmenší horní mez pro dvojici a, b “

PA



$\inf(d, e) = \text{neex}$

1) dolní meze b, c, a

2) neex - největší z dolních mezí

$\inf(b, c) = a$

$\sup(b, d) = d$

Pozorování když $a \leq b$, pak $\sup(a, b) = b$
 $\inf(a, b) = a$

PA $(N, \leq)$

3
2
1
0

0 - nejmenší

největ. neex

max. neex (nad každým $m \in N$ je $(m+1)$)

$\sup(m, m) = m$ pro $m \in m$

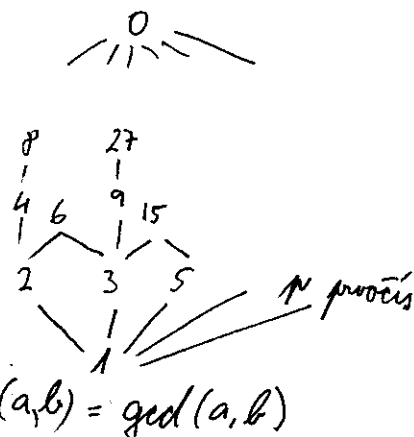
PA $(N, |)$ $a|b$ iff $b = k \cdot a, k \in N$

1 je uspořádání

nejmenší .. 1

největší .. 0 ($a|0 \dots 0|0$)

$\sup(a, b) = \text{nejmen. spol. násobek} = \text{lcm}(a, b)$, $\inf(a, b) = \text{gcd}(a, b)$



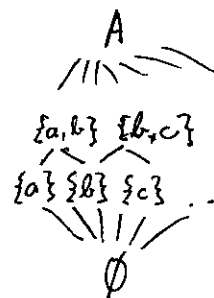
Pr : $(P(A), \subseteq)$ potenční množ. s inkluzí
 $\{B, B \subseteq A\}$

nejmen. $\emptyset$

největ. A

$$\sup(B, C) = B \cup C$$

$$\inf(B, C) = B \cap C$$



dvoupřískové
jednopřískové
podmnož

Pr $\Sigma = \text{abeceda}$

Σ^* = vs. konečná slova (včetně prázdného) vytvoř. z písmen v Σ

$(\Sigma^*, \preceq)$

$u \preceq v$ iff $v = uz$

u je prefixem slova v

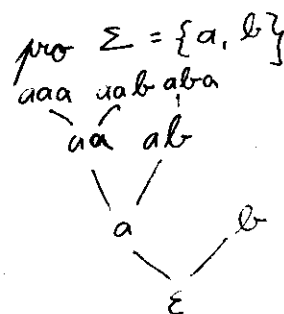
$\preceq$ je uspořádání

nejmen. pr. ε

největší. max

$\sup(a, b) = s$ pak 1) $u \preceq s, v \preceq s$

když $s = uz$
 $s = vt$



což plyne jenom když u je prefix v
(nebo naopak)

$\Rightarrow \sup$ existuje jen když $u \preceq v$ (nebo $v \preceq u$)
 $\sup$ je to větší

$\inf(u, v) = i$ největší spol. začátek / prefix dvou slov
 $\Rightarrow$ exist. vs. infima, ale ne vs. sup.

Def: Svoz je uspořádaná množ. $(M, \sqsubseteq)$, kde existují
sup. i inf. pro každou dvojici $a, b \in M$

→ Na M se dají korektně definovat binární operace

spojení $a \vee b = \sup(a, b)$

průsečík $a \wedge b = \inf(a, b)$

(Korektně def. - def. pro každou dvojici a výsledek je $\in M$)

Operace splňují:

1) Komutativní $a \vee b = b \vee a$
 $\wedge \quad \wedge$

2) Asociativní $a \vee (b \vee c) = (a \vee b) \vee c$ $(= \sup(a, b, c))$
 $\wedge \quad \wedge \quad \wedge \quad \wedge$

3) absorbece $a \vee (b \wedge a) = a$

$$\begin{array}{c} b \quad a \\ \backslash \quad / \\ b \wedge a \\ \sup(b \wedge a, a) = a \end{array}$$

4) idempotence $a \vee a = a$
 $\wedge$

Například:

Druhý pohled na svaz

$(M, \vee, \wedge)$ množ. se dvěma binár. operacemi,
které splňují kom., asoc., absorb., idempot.

→ pak lze na M def. relaci $\sqsubseteq$

předpisem $x \sqsubseteq y$ iff $x \vee y = y$
(iff $x \wedge y = x$)

Ukážeme, že $\sqsubseteq$ je uspořádaní

1) reflex. $x \sqsubseteq x$ 

iff $x \vee x = x$ Ato platí (idempotence)

2) antisym.

Chceme: $x \in y \wedge y \in x$, pak $x = y$

Přepíšeme dle def $\in$

$$x \vee y = y \text{ a také } y \vee x = x$$

$$\text{pak } \underline{y} = x \vee y \underset{\text{kom.}}{=} y \vee x = \underline{x}$$

3) transitivita

Chceme dok.: když $x \in y$, $y \in z$, pak $x \in z$

tj. předpokládáme $x \vee y \stackrel{(1)}{=} y$, $y \vee z \stackrel{(2)}{=} z$

$$\text{pak } z \stackrel{(2)}{=} y \vee z \stackrel{(1)}{=} (x \vee y) \vee z \underset{\text{asoc}}{=} x \vee (y \vee z) \stackrel{(2)}{=} \underline{\underline{x \vee z}}$$

$$\text{at } \frac{x \vee z = z}{x \in z}$$

Na $(M, \in)$ jsou nš. sup a inf

$$\sup(a, b) = s = a \vee b$$

(výsledek operace $a \vee b$ má vlastnosti supremu)

$$1) a \in s, b \in s$$

$$a \in a \vee b, b \in a \vee b$$

tj (dle def $\in$)

$$\text{musím. dok. } a \vee (a \vee b) \stackrel{?}{=} a \vee b$$

asoc //

$$(a \vee a) \vee b$$

idempot //

$$a \vee b = a \vee b$$

$$\text{! } b \vee (a \vee b) = a \vee b$$

kom //

$$b \vee (b \vee a)$$

asoc //

$$(b \vee b) \vee a$$

idemp //

$$b \vee a = a \vee b$$

kom

2) s je nejmenší horní mez

Nechť: $a \in \kappa, b \in \kappa \dots$ chci dok. $s \in \kappa$

tj. $a \vee \kappa = \kappa, b \vee \kappa = \kappa \dots$ chci dok. $s \vee \kappa = \kappa$
 $\underbrace{(a \vee b) \vee \kappa = \kappa}_{\text{dok}}$

$$L = (a \vee b) \vee \kappa = a \vee (b \vee \kappa) = a \vee \kappa = \kappa = \mathcal{P}$$

↑
asoc

A podařilo se.

(13)

Distributivní svaz, Booleovy algebry

Svaz = $(M, \leq)$ kde exist. sup. a inf. pro $\{a, b\} \in M$

= $(M, \vee, \wedge)$ kde bin. operace splňují kom, asoc, absorpci,
 idempotenci

Distributivní svaz = svaz, kde $\vee, \wedge$ splňují dva distrib. zákony

$$\begin{matrix} a & \vee & (b & \wedge & c) \\ & & \wedge & \vee & \wedge \end{matrix} = (a \vee b) \wedge (a \vee c)$$

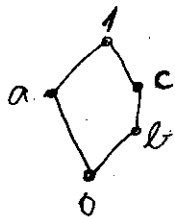
Komplementární svaz = svaz s nejmenším (0) a největším (1)
 prvkem, kde každý prvek má komplement

(tj. pro každý $a \in M$ exist. $\bar{a} \in M$ tak, že

$$\begin{matrix} a \vee \bar{a} = 1 \\ a \wedge \bar{a} = 0 \end{matrix})$$

Booleova algebra = distrib. a komplement svaz

Pr: Svaz je dán Hass. diag.



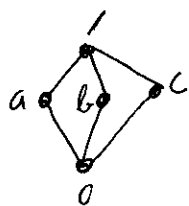
$$(a \wedge c) \vee b \stackrel{?}{=} (a \vee b) \wedge (c \vee b)$$

$$L = 0 \vee b = b$$

$$P = 1 \wedge c = c$$

$$L \neq P$$

neplatí distributivita



$$a \vee (b \wedge c) \stackrel{?}{=} (a \vee b) \wedge (a \vee c)$$

$$L = a \vee 0 = a$$

$$P = 1 \wedge 1 = 1$$

$$L \neq P$$

Platí: Svaz není distributivní. právě když obsahuje pětiúhelník nebo trojlampiónek jako podsvaz.

Podsvaz = podmnož., kde operace spojení „ $\vee$ “ a průsečík „ $\wedge$ “ dávají stejné výsledky jako ve svazu (aneb sup., inf. běhají stejně)
potvrzení množ

Pr: $(P(A), \subseteq)$ je Booleova algebra
sup = „ $\cup$ “, inf = „ $\cap$ “

sjednoc. a-průnik splňují distrib. zákony

Komplementy $\bar{B} = A \setminus B$

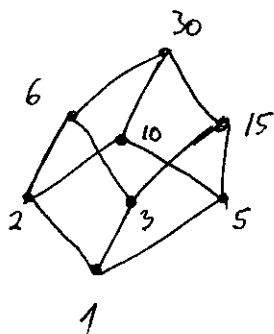
Platí: Každá Booleova algebra je izomorfni s $(P(A), \subseteq)$

Izomorf = vzájem. jednozn. zobr. f (přejmenování objektů, které zachovávají operace $\wedge, \vee$ (aneb zobrazí sup(a, b) na sup(f(a), f(b)) a inf. na inf.))

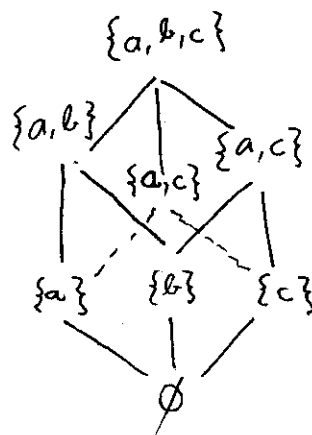
PA $(D_{30}, 1)$ $D_{30} = \{a \in \mathbb{N}, a | 30\} = \text{deliteli } 30$

Nakreslit Hass. diag. Zjistit vlastnosti tohoto svazu

1, 2, 3, 5, 6, 10, 15, 30



$\longleftrightarrow$



$P(\{a, b, c\}, \subseteq)$

Bool. alg.

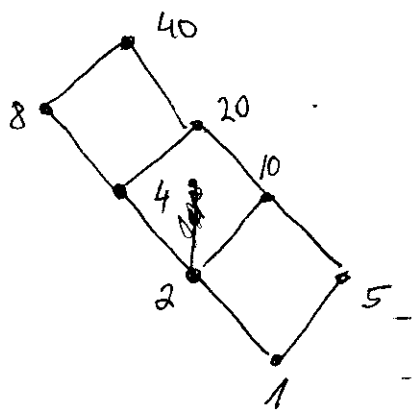
$(D_{30}, 1)$ je iso

a Bool alg,

tedy je to take Bool. alg

PA $(D_{40}, 1)$

1, 2, 4, 5, 8, 10, 20, 40



Kompl. $\bar{5} = 8$

$\bar{10} = \text{neexist.}$

$\bar{1} = 40$

$\text{sup} = \text{scm}$

$\text{inf} = \text{gcd}$

$\text{scm}(5, 8) = 40$ $\text{gcd}(5, 8) = 1$

→ svaz není komplementární

Distributivita

Dk, že obecně $(N, 1)$ je distribut. svaz

Převádíme čísla z $\mathbb{N}$ na multimnož.

např. $a = 2^3 \cdot 3 \cdot 7^2 \leftrightarrow A = \{2_1, 2_2, 2_3, 3_1, 7_1, 7_2\}$
vzájemně si odpovídají

$$b = 2^2 \cdot 3^2 \cdot 5 \leftrightarrow B = \{2_1, 2_2, 3_1, 3_2, 5_1\}$$

$$\gcd(a, b) = 2^2 \cdot 3 \leftrightarrow A \cap B$$

$$\text{sem}(a, b) = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \leftrightarrow A \cup B$$

Tedy distrib. zák.

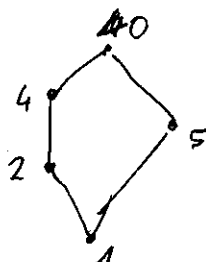
$$\gcd(a, \text{sem}(b, c)) = \text{sem}(\gcd(a, b), \gcd(a, c))$$

odpovídá rovnosti

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ a to platí}$$

Důl.: $(D_{40}, 1)$ je distrib. svaz.

otázka: A co podobrůžek



to tedy nemůže být podsvaz (jinak by neplat. distrib. z.)

$$\text{sup}(2, 5) = 40 \quad \neq \quad \text{sup}(2, 5) = 10$$

vše ve svazu

DŮ: Kdy je $(D_m, 1)$ Booleova alg?

Pr $(\text{Rel}(A), \subseteq) = (\mathcal{P}(A \times A), \subseteq) \rightarrow$ je to Bool. alg.

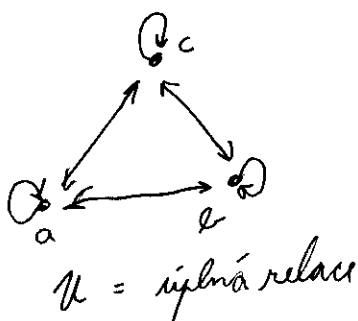
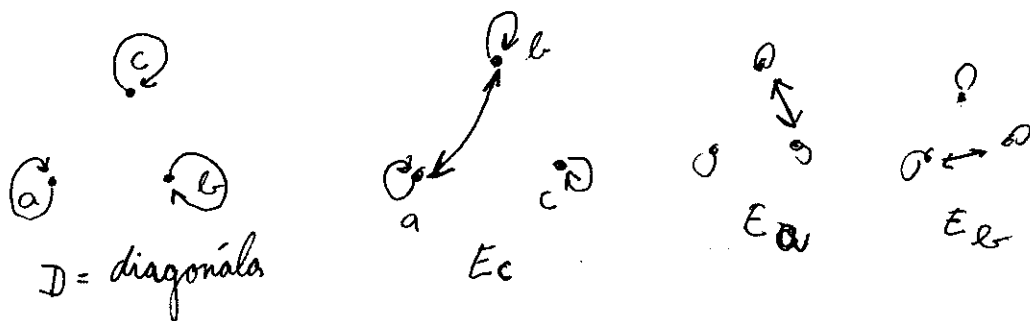
"mnoz. vř. relací (binárních) na množ. A

$(\text{Ekv}(A), \subseteq)$

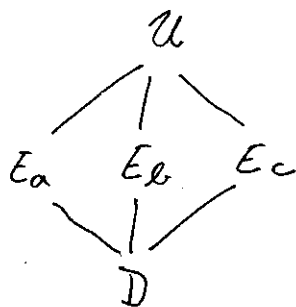
"
vřechy rel. ekvivalence na A (tj. ref, sym, tranz.)

Např. $A = \{a, b, c\}$

$\text{Ekv}(A) = \{D, E_a, E_b, E_c, U\}$



Uspoř. přes. inkluzi $\subseteq$
 $(R_1 \subseteq R_2 \text{ iff } a R_1 b \rightarrow a R_2 b)$



$\Rightarrow$ Vlastnosti svazů

- není distrib (trojlampiónek)

- komplementární

$\bar{E}_a = E_b$ nebo $\bar{E}_a = E_c$

$\bar{D} = U, \bar{U} = D$

prostor prvky vždy 2 kompl.
 může se stát jen o nedistrib. svazu

obecně $(E_{\text{kw}}(A), \subseteq)$

nejmen. prvek $0 = D = \text{diagonála}$
 $1 = U = \text{úplná rel.}$

je to svaz?

$\inf(E_1, E_2) = E_1 \cap E_2$ (průnik je ekvivalence)
 $\sup(E_1, E_2) = \text{trans. uzavěr}(E_1 \cup E_2)$
 $\rightarrow$ nemusí být ekv. rel.

ANO, ale není to podsvaz $(\text{Rel}(A), \subseteq)$,
sup. funguje jinak

P4 Svaz konceptů daného kontextu

kontext = trojice (G, M, I) , kde

G = množ. objektů

M = množ. ~~relací~~ atributů

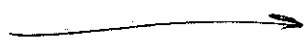
$I \subseteq G \times M$ relace z G do M

($g I m$ objekt g má atribut m)

P4 $G = \{1, 2, 3, 4\}$

$M = \{a, b, c, d\}$

I



	a	b	c	d
1	x		x	
2	x	x	x	
3				x
4	x	x	x	

Označme : Pro $A \subseteq G$ je $A^\uparrow = \{ m \in M, g I m \text{ pro vš. } g \in A \}$
atributy společně všem obj. z A

Pro $B \subseteq G$ je $B^\downarrow = \{ g \in G, g I m \text{ pro vš. } m \in B \}$
objekty, které mají vš. atrib. z B

Pr. $\{1, 2\}^\uparrow = \{a, c\}$

$\{a, c\}^\downarrow = \{1, 2, 4\}$

Nuže se stáá $A^{\uparrow\downarrow} \supseteq A$
 $= A_1$

$\{1, 2, 4\}^\uparrow = \{a, c\}$

Dále už se to neměňuje $A_1^{\uparrow\downarrow} = A_1$

Koncept daného kontextu je pářda dvojice (A, B) ,
kde $A^\uparrow = B$, $B^\downarrow = A$.

("množ. vyřikují jedna druhou")

Pr. $(A, B) = (\{1, 2, 4\}, \{a, c\}) \quad K_1$

posm: koncepty posm $(A^{\uparrow\downarrow}, A^\uparrow)$

$(A, B) = (\{2, 4\}, \{a, b, c\}) \quad K_2$

$= (\{3\}, \{d\}) \quad K_3$

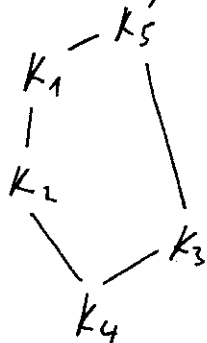
$= (\emptyset, \{a, b, c, d\}) \quad K_4$

$= (\{1, 2, 3, 4\}, \emptyset) \quad K_5$

Na konceptech je definováno uspořádání

$$(A_1, B_1) \leq (A_2, B_2) \text{ iff } A_1 \subseteq A_2 \\ (\text{iff } B_1 \supseteq B_2)$$

Koncepty s tímto uspoř. tvoří svaz.



plastnosti

není distrib.

je komplementární

$$\bar{K}_2 = K_3, \bar{K}_1 = K_3, \bar{K}_3 = \begin{matrix} K_1 \\ K_2 \end{matrix}$$

DŮ: vlastnosti svazu konceptů

1)

	a	b
1	x	
2		x

2)

	a	b	c
1	x	x	
2	x		
3			

3)

	a	b	c	d
1	x	x		
2	x		x	
3				x

satz nejak treba pr. v premenne

Homomorfismy algeber

Algebra typu Ω ($\Omega = \{ \text{symboly pro operace + jejich aridy} \}$)

je $X = (X, \text{operace})$ $X = \text{mnohá množina}$

operace - pro každý symbol $\omega \in \Omega$ aridy n

je dána n -ární operace ω_x na množ X

$$\text{tj } \omega_x : X^n \rightarrow X$$

Např. Prologrupa je algebra typu $\Omega = \{ *, \text{aridy } 2 \}$

navíc - platí asociat. $x * (y * z) = (x * y) * z$

Algebra typu Ω splňující rovnice E

($E = \text{mnohá formál. rovnice, které musí}$
 platit pro libovolné dosazení prvků x
 za neznámé)

Např. Grupa - algebra typu $\Omega = \{ *, \text{aridy } 2, e \text{ aridy } 0, ()^{-1} \text{ aridy } 1 \}$

splňující 5 rovnic - asoc. *

e pravý a levý neutrální

$()^{-1}$ pravý a levý inverz

Např. Slaz - algebra typu $\Omega = \{ \wedge, \vee \text{ aridy } 2 \}$

splňující 8 rovnic - kom., asoc., absorpce,
 idempotence pro obě operace

Podalgebra typu Ω = podmnožina uzavřená na výsledky všech operací $\kappa \in \Omega$

Homomorfismus typu Ω = zobrazení mezi dvěma algebry

X, Y typu Ω , které zachovávají všechny operace $\kappa \in \Omega$

$$\text{tj. } f(w_x) = w_y \text{ pro } w \text{ arit. } 0$$

$$f(w_x(x_1, \dots, x_n)) = w_y(f(x_1), \dots, f(x_n)) \text{ pro } w \text{ arit. } n$$

ANEB
komutuje
diagram:

$$\begin{array}{ccc} (x_1, \dots, x_n) \in X^n & \xrightarrow{f^n} & Y^n \ni (f(x_1), \dots, f(x_n)) \\ \omega_x \downarrow & & \downarrow \omega_y \\ \omega_x(x_1, \dots, x_n) \in X & \xrightarrow{f} & Y \end{array}$$

Algebry X, Y typu Ω jsou izomorfní, jestliže existuje homomorfismus typu Ω $f: X \rightarrow Y$, který je bijekcí (vzáj. jednoznač. zobr.) mezi nosnými množinami.

Pozn.: Platí-li v $X = (X, \text{operace } \omega_x)$ rovnice $\kappa \in E$ a máme $f: X \rightarrow Y$ homomorf. typu Ω , pak stejné rovnice budou platit v $f(X)$ (co splňují vzory, to splňují výsledky)

Př.: (když dáme) $GF(p^n)$ - konstrukce přes křivé
ireducib. pol $P(x), Q(x)$ dá izomorf. konečná tělesa

izomorf. byl určen obrátem kořene α pol. $P(x): f(x)$
byl prvek druhého tělesa splňující stejnou rovnici

Pr. S čím je izomorfní cyklická grupa G řádu n ?
 $(G = \langle a \rangle, G = |n|)$

$$f: G \rightarrow ? \mathbb{Z}_n$$

$$f(g) = f(a^k) = k$$

to bude bijekce, neboť $g \in \langle a \rangle$ je
 jednozn. určen exponentem $k \in \{0, \dots, n-1\}$
 $a^n = e = a^0$

$$f(g \cdot h) = f(a^k \cdot a^l) = f(a^{k+l}) = f(g) + f(h) = k + l$$

Pozn.: Pokud zobrazení mezi grupami zachová binární
 operace, automaticky zachová neutrála a inverzy

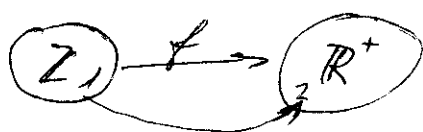
Pozn.: Svazky jsou izomorfní iff mají stejný Hasseho diagram.

Pr.: Dodefinujte zobr. $f: (\mathbb{Z}, +) \rightarrow (\mathbb{R}^+, \cdot)$ tak, aby
 byl grupový homomorf, vědě-li, že $f(1) = 2$

$(\mathbb{Z}, +, e=0, \text{inv}(k) = -k)$ grupa

$(\mathbb{R}^+, \cdot, e=1, \text{inv}(x) = \frac{1}{x})$ grupa

$x=0$, platí v $\mathbb{R}^+$



Všech zobrazení $\kappa: \mathbb{Z} \rightarrow \mathbb{R}^+$
 splňujících $f(1) = 2$ je
 nekonečně mnoho

Kolik z nich zachová grupové operace?

$$f(0) = 1 \quad (\text{neutrály})$$

$$f(-1) = \frac{1}{2} \quad (\text{inverzy})$$

$$f(2) = f(1+1) = 2 \cdot 2 = 2^2 \quad (\text{binární oper.})$$

$$\begin{cases} f(k) = f(\underbrace{1+\dots+1}_k) = 2 \cdot \dots \cdot 2 = 2^k \\ f(-k) = \frac{1}{2^k} \end{cases} \quad k \geq 0$$

= jediná možnost dodef. na grupový homomorf

Důvod: 1 je generátor komut. grupy $(\mathbb{Z}, +)$

Pozn: $f(1) = a \in \mathbb{R}^+$

vždy lze rozšířit na grupový homomorf.

$(\mathbb{Z}, +)$ volná kom. grupa

Př. Najděte všechny grupové homomorfismy $f: (\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_6, +)$

$\mathbb{Z}_4$ $\mathbb{Z}_6$

0 $\longrightarrow$ 0

1 1

2 2

3 3

4

5

$$f(0) = 0$$

$$f(1) = a \quad \text{pak jednoznačně}$$

$$f(2) = a + a$$

$$f(3) = a + a + a$$

1 splňuje v $(\mathbb{Z}_4, +)$ rovnici $1+1+1+1=0$

$$\text{tudíž } f(1+1+1+1) = f(0)$$

$$\xrightarrow{\quad \parallel \quad} a+a+a+a = 0 \quad \text{v } (\mathbb{Z}_6, +)$$

tato rovnice musí platit

$$\text{pro } f(1)=a \quad \text{v } (\mathbb{Z}_6, +)$$

aby byl
homomorf

$$\rightarrow \text{v } \mathbb{Z}_6$$

$$4a = 0$$

$$\text{v } \mathbb{Z}$$

$$4a + 6 \cdot n = 0 \quad |:2$$

$$2a + 3n = 0$$

$$a = 3k \quad n = -2k \quad k \in \mathbb{Z}$$

$$\text{v } \mathbb{Z}_6 \quad \underline{a_1 = 3}$$

$$\underline{a_2 = 6 = 0}$$

pro $k=1$

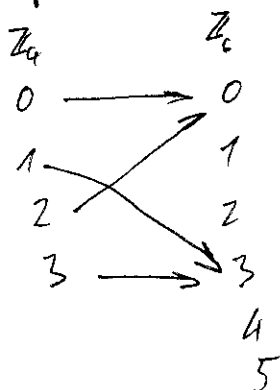
pro $k=0$

1) f pro $f(1)=0$
 $f(2)=0+0=0$
 $f(3)=0$



tedy $f(k) = 0, k \in \mathbb{Z}_4$
nulový homomorf.

2) pro $f(1) = 3$



$f(2) = 3+3=0$

$f(3) = 3+3+3=3$

$f(0) = 0$

obraz $f(\mathbb{Z}_4) = \{0, 3\}$

$(\{0, 3\}, +)$ je podgrupa v $(\mathbb{Z}_6, +)$

+	0	3
0	0	3
3	3	0

Pozn.: $(\mathbb{Z}_4, +)$ není volná komut. grupa,
neboť $f(1) = a$ se dalo rozšířit na grupový
hom. jen pro $a=0, a=3$,
ne vždy

Def.: Algebra typu Ω splňující rovnice E je volná nad
množ. generátorů V , jestliže
každé zobrazení generátorů do libovolné algebry Y typu Ω
s rovnicemi E lze jednoznačně rozšířit na homomorf.
typu Ω

$$\begin{array}{ccc} V & \xrightarrow{f} & Y \\ \uparrow & \dashrightarrow & \uparrow \\ X & \xrightarrow{\varphi} & Y \end{array}$$

 φ homomorf.

$\mathbb{Z}$ $(\mathbb{Z}, +)$ je volná kom. grupa
 $(\mathbb{Z}_m, +)$ není ——— " ———

Konstrukční pokles

Volná algebra typu Ω splňující rovnice E s generátory $x \in V$
je saková, kde generátory splňují jenom rovnice
 $x \in E$ a nic víc.

$$(\mathbb{Z}_m, +) \quad \text{neutrál}$$

$$\underbrace{1 + \dots + 1}_m = 0$$

tato rovnice neplatí ve všech kom. grupách!

Konstrukce volných algeber typu Ω s rovnicemi $x \in E$
- možná množ. - z termů, které vybíráme z generátorů
pomocí operací $x \in \Omega$, přitom musíme sledit
dohromady ty termy, které se musí rovnat
kvůli rovnicím $x \in E$

Např.: Volná pologrupa s 2 generátory a, b

$$X = \{ a, b, a * b, a * a, \dots \}$$

$$\dots (a * b) * b = a * (b * b) \dots \}$$

musím sledit

stepence mohou nazvat ab^2b

$$\Rightarrow X = \{ \text{slova z písmen } a, b \}$$

* ... křesření slov

Volný monoid - přidám prázdné slovo ε

Volná grupa -

$$X = \{ \varepsilon, a, b, \bar{a}, \bar{b} \dots$$

$$a\bar{a} = \varepsilon$$

$\Rightarrow$ operace „redukující zkrácení“ - $a\bar{a}$ se zruší

$\Rightarrow$ normální množ. = pouze zredukovaná slova

Volná komut. grupa

$$\{ a^k b^l, k, l, \in \mathbb{Z} \}$$

$$\xrightarrow[\text{izo}]{} (\mathbb{Z} \times \mathbb{Z}, +)$$