Úvod

Právě se díváte na moje řešení příkladů z X01AVT z roku 2007/2008. Zajisté obsahují spousty chyb a nedokáže je pochopit nikdo včetně autora, ale aspoň můžou posloužit jako menší návod k tomu, jak počítat příklady u zkoušky. **Důrazně** doporučuji ty příklady si vypočítat sám a teprve potom, co vyjde nějaký výsledek jinak, než jak má podle dr. Gollové vyjít, se podívat sem. Když si budete ty příklady jen tupě pročítat, tak se naučíte lim $\to 0$. Pokud máte pocit, že tu něco chybí, či snad přebývá, máte naprosto volnou ruku k úpravám, za předpokladu, že své úpravy zveřejníte, a to včetně zdrojového kódu v .tex a obrázků. Odkazy na použitou literaturu jsou na konci. Obrázky nakresleny pomocí maker XY-pic.

Tímto bych také chtěl poděkovat dr. Aleně Gollové za její pečlivou kontrolu mých výpočtů a množství cenných připomínek a oprav.

Hodně štěstí u zkoušek a co nejméně trápení s algebrou,

Štěpán Rezek

Obsah

1 Konečné grupy a počítání v $\mathbb{Z}_n$

1.1 Příklad 1

V $\mathbb{Z}_{267}$ najděte všechna x, pro která platí $114x = 15$.

Počítá se pomocí rozšířeného eukleidova algoritmu.

$$
\begin{aligned}
114x + 267y &= 15 \\
267 &= 2 \cdot 114 + 39 & 39 &= 367 - 2 \cdot 114 \\
114 &= 2 \cdot 39 + 36 & 36 &= 114 - 2 \cdot 39 = 114 + 4 \cdot 114 - 267 \cdot 2 \\
39 &= 1 \cdot 36 + \underline{3} & 3 &= 39 - 36 = 3 \cdot 267 - 7 \cdot 114
\end{aligned}
$$

Na levé straně vyšla trojka, což znamená, že nejmenší společný dělitel 114 a 267 (gcd) je 3. Na pravé straně (Bezoutova nerovnost) pak mám tu trojku vyjádřenou pomocí násobků 114 a 267.

Jelikož $c = gcd(114, 267)$ dělí $d = 15$, pak rovnice má tolik řešení, kolik je c. V tomto případě tedy 3. Dále musím vyjádřit d pomocí násobků 114 a 267. Vydělím tedy d/c a získám číslo 5, kterým vynásobím Bezoutovu nerovnost. Tedy

$$15 = 5 \cdot 3 = 5 \cdot (3 \cdot 267 - 7 \cdot 114) = 15 \cdot 267 - 35 \cdot 114$$

Tím jsem získal partikulární řešení rovnice: $(x_p, y_p) = (-35, 15)$ (protože 267 je u y a 114 u x). Nyní hledám nesoudělné řešení homogenní rovnice. To najdu tak, že vezmu zadanou rovnici a na levou stranu napíšu 0. Pak ji vyřeším a dostanu nějaké koeficienty u x a y:

$$
\begin{aligned}
114x + 267y &= 0 & &\cdot 3^{-1} \\
38x + 89y &= 0
\end{aligned}
$$

Z této rovnice snadno vyčtu, že aby se pravá strana rovnala nule, na levé straně musí $x = 89$ a $y = -38$. Z toho tedy $(x_0, y_0) = (89, -38)$. Celkové řešení v $\mathbb{Z}$ je tedy

$$(x, y) = (x_p, y_p) + k \cdot (x_0, y_0), k \in \mathbb{Z}$$

V tomto případě

$$(x, y) = (-35, 15) + k \cdot (89, -38), k \in \mathbb{Z}$$

A pro $\mathbb{Z}_{267}$ má x tři řešení:

$$
\begin{aligned}
x_1 &= -35 + 1 \cdot 89 = \underline{54} \\
x_2 &= -35 + 2 \cdot 89 = \underline{143} \\
x_3 &= -35 + 3 \cdot 89 = \underline{232}
\end{aligned}
$$

1.2 Příklad 2

Spočtěte 18^{-1} a 19^{-1} v $\mathbb{Z}_{26}$, pokud existují.

Aby k nějakému prvku existoval inverz, musí být největší společný dělitel toho prvku a základu soustavy 1. Jinými slovy, prvek a v $\mathbb{Z}_m$ má inverzi právě tehdy, když platí

$$\gcd(a, m) = 1. \tag{1}$$

Jelikož $\gcd(18, 26) = 2$, 18 nemá v $\mathbb{Z}_{26}$ inverzi. 19 inverzi má, spočítat se dá pomocí eukleidova algoritmu:

$19x + 26y = 15$ v $\mathbb{Z}$

$$\begin{aligned} 26 &= 1 \cdot 19 + 7 & 7 &= 26 - 19 \\ 19 &= 2 \cdot 7 + 5 & 5 &= 19 - 2 \cdot 7 = 3 \cdot 19 - 2 \cdot 26 \\ 7 &= 1 \cdot 5 + 2 & 2 &= 7 - 5 = 3 \cdot 26 - 4 \cdot 19 \\ 5 &= 2 \cdot 2 + 1 & 1 &= 5 - 2 \cdot 2 = \underline{11} \cdot 19 + (-8) \cdot 26 \end{aligned}$$

Jelikož $1 = 11 \cdot 19$ v $\mathbb{Z}_{26}$, $19^{-1} = 11$ v $\mathbb{Z}_{26}$.

1.3 Příklad 3

Spočtěte zbytky po dělení čísel 49^{107} a 6^{22} číslem 40.

Tady se dá s úspěhem použít Euler-Fermatova věta[1]: Je-li $\gcd(a, m) = 1$, potom platí

$$a^{\varphi(m)} = 1 \text{ v } \mathbb{Z}_m \tag{2}$$

Dál si musím uvědomit, že 49^{107} se dá napsat jako

$$\underbrace{49 \cdot 49 \cdots}_{107\times} = (49 \bmod 40)^{107} = 9^{107} \text{ v } \mathbb{Z}_{40}.$$

Dál umím vypočítat $\varphi(40) = \varphi(2^3 \cdot 5) = (8 - 4) \cdot 4 = 16$. Teď tedy můžu použít E-F (Euler-Fermat):

$$9^{107} = 9^{6 \cdot 16 + 11} \overset{E-F}{\to} 9^{11} = 9 \cdot (9^2)^5 = 9 \cdot 81^5 = 9 \cdot 1^5 = \underline{9}$$

Podobně ovšem nemůžu postupovat v tomhle případě, jelikož základ 6 je soudělný s tím, kolik modulo se počítá (tj. 40), neboli $\gcd(6, 40) \neq 1$. Proto mi nezbývá nic jiného, než použít rovnou opakované čtverce, $22 = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1$:

1		0		1		1		0
X	S		S	X	S	X	S	

Jinými slovy, rozepsal jsem si 22 do binární podoby, mezi každou číslici jsem vepsal S a tam, kde je jednička, jsem napsal X. Teď to napíšu pod sebe (nejlevější X je nahoře, nejpravější dole) a dostanu:

X	$6^1 = 6$
S	$6^2 = -4$
S	$6^4 = 16$
X	$6^5 = 16$
S	$6^{10} = 16$
X	$6^{11} = 16$
S	$6^{22} = \underline{16}$

1.4 Příklad 4

Najděte přirozené číslo x takové, že platí:

$$x \equiv 2 \pmod 8, x \equiv 5 \pmod{11}, x \equiv 7 \pmod{15}$$

Tady přichází na řadu Čínská věta o zbytcích. Pokud si to nahoře napíšu jako $x \equiv a_1 \pmod{m_1}$, pak postup je následující:

1. Najdu číslo M, $M = m_1 \cdot m_2 \cdots m_k$.
2. Pro každé m_i si najdu číslo $q_i = s \cdot \prod_{j \neq i} m_j$, kde $s = \left(\prod_{j \neq i} m_j \right)^{-1}$ v $\mathbb{Z}_{m_i}$

[1] Velebil to ve skriptech nazývá jen Eulerova věta, na wikipedii se to nazývá zase jen Malá Fermatova věta - malá Fermatova věta je vyslovena jen pro počítání modulo prvočíslo, Euler ji zobecnil pro libovolné n

3. Celkový výsledek bude $a_1 \cdot q_1 + a_2 \cdot q_2 \cdots a_k \cdot q_k$ v $\mathbb{Z}_M$

V tomhle případě tedy $M = 8 \cdot 11 \cdot 15 = 1320$ a

$$\begin{aligned} q_1 &= s_1 \cdot 11 \cdot 15 = s_1 \cdot 168 = s_1 \cdot 5 & [5]_8^{-1} = 5 \\ &= 5 \cdot 11 \cdot 15 = 825 \\ q_2 &= 8 \cdot s_2 \cdot 15 = s_2 \cdot 120 = s_2 \cdot 10 & [10]_{11}^{-1} = 10 \\ &= 8 \cdot 10 \cdot 15 = 1200 = -120 \\ q_3 &= 8 \cdot 11 \cdot s_3 = s_3 \cdot 88 = s_3 \cdot 13 & [13]_{15}^{-1} = 7 \\ &= 8 \cdot 11 \cdot 7 = 616 \end{aligned}$$

Mimochodem, je lepší si psát místo třeba q_1, q_2 atd. spíš q_8, q_{11} atd., protože člověk pak přesně ví, v kterém $\mathbb{Z}$ počítá ty inverzy.

Po vynásobení to dá $2 \cdot 825 - 5 \cdot 120 + 7 \cdot 616 = 5362 = 82$ v $\mathbb{Z}_{1320}$, což se dá napsat jako

$$\underline{x = 82 + 1320k, k \in \mathbb{Z}}$$

1.5 Příklad 5

Určete řád prvku 11 v aditivní grupě $(\mathbb{Z}_{26}, +)$ a řád prvku 11 v multiplikativní grupě $(\mathbb{Z}_{26}^*, \cdot)$ všech invertibilních prvků v $\mathbb{Z}_{26}$.

V obou případech hledám prvek, který dokáže vygenerovat všechny ostatní, a to tak, že na něj aplikuju operaci $\oplus$ tolikrát, kolik je prvků v grupě. Pokud mi po n opakováních té operace dá neutrální prvek vzhledem k operaci $\oplus$, tak n je jeho řád. Aditivní grupa je taková, kde se ty prvky sčítají, a počet prvků je tedy 26. Multiplikativní grupa je taková, kdy prvky umocňuji, a prvků takové množiny (invertibilních) je $\varphi(26) = \varphi(2 \cdot 13) = 12$ (protože eulerova funkce mi dává počet prvků nesoudělných s daným číslem, a prvek a je invertibilní, pokud má $gcd(a, m) = 1$ v $\mathbb{Z}_m$) Zkusím tedy na 11 (zadaná) aplikovat operaci $\cdot$ (v $\mathbb{Z}_{26}$):

$$\begin{aligned} 11^1 &= 11 \\ 11^2 &= 121 = 17 \\ 11^3 &= 17 \cdot 11 = 187 = 5 \\ 11^4 &= 5 \cdot 11 = 55 = 3 \\ 11^5 &= 3 \cdot 11 = 33 = 7 \\ 11^6 &= 7 \cdot 11 = 77 = 25 \\ 11^7 &= 25 \cdot 11 = 275 = 15 \\ 11^8 &= 15 \cdot 11 = 165 = 9 \\ 11^9 &= 9 \cdot 11 = 99 = 21 \\ 11^{10} &= 21 \cdot 11 = 231 = 23 \\ 11^{11} &= 23 \cdot 11 = 253 = 19 \\ 11^{12} &= 19 \cdot 11 = 209 = 1 \end{aligned}$$

Vidím, že mi vygenerovala 12 prvků, její řád je tedy $\underline{r(a) = 12}$. Vzhledem k tomu, že její řád je roven počtu prvků množiny, je i její generátor.

Výpočet se dá výrazně zjednodušit, když si uvědomím, že řád prvku musí být dělitelem počtu prvků grupy, v tomto případě tedy stačí ověřit jen řády 1, 2, 3, 4, 6 (a 12 už ani nemusím, protože to jsou to zbylé).

Co se týče aditivní grupy, výpočet by vypadal podobně, jen by tam bylo $11 \cdot 1, 11 \cdot 2, \cdots, 11 \cdot 26$, kde $11 \cdot 26 = 0$. Takže 11 je i její generátor, protože dokázala vygenerovat 26 prvků; $\underline{r(a) = 26}$. Stejně tak i tady stačí vyzkoušet řády 1,2 a 13.

1.6 Příklad 6

Najděte všechny generátory grupy $(\mathbb{Z}_{13}^*, \cdot)$. Kolik různých generátorů má tato grupa?

Cyklická grupa má $\varphi(r)$ generátorů řádu r (kde r je soudělné s velikostí grupy), takže generátorů řádu $|M|$ je $\varphi(|M|)$, což je $\varphi(\varphi(13)) = \varphi(12) = \underline{4}$ (ta hvězdička nad $\mathbb{Z}$ znamená, že je to grupa invertibilních prvků). Abych našel prvky zadaného řádu, tak musím najít generátor grupy. To se bohužel dá dělat pouze postupným zkoušením, přičemž pravděpodobnost, že se trefím, je $\frac{\text{počet generátorů grupy}}{\text{počet prvků grupy}} = \frac{4}{12} = 1/3$.

Takže začnu postupně zkoušet všechny prvky grupy. Jednička generátor evidentně nebude, protože $1^{\text{cokoliv}} = 1$. Její řád je tedy 1. Zkusím dvojku (v $\mathbb{Z}_{13}$):

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 3 \\ 2^5 &= 6 \\ 2^6 &= 12 \\ 2^7 &= 11 \\ 2^8 &= 9 \\ 2^9 &= 5 \\ 2^{10} &= 10 \\ 2^{11} &= 7 \\ 2^{12} &= 1 \end{aligned}$$

Stejně jako minule se to dá výrazně zjednodušit, když budu zkoušet jen řády soudělné s počtem prvků grupy.

Dostal jsem celou množinu čísel, jejichž $\gcd(a, 13) = 1$. 2 je tedy generátor. Mimo dvojky ještě ovšem musí existovat další generátory, protože jsem si nahoře spočítal, že jsou celkem čtyři. Ty další můžu najít buď zase systémem BruteForce$^{\text{TM}}$, což je poněkud zdlouhavé, nebo pomocí vzorce

$$r(a^k) = \frac{r(a)}{\gcd(r(a), k)} \tag{3}$$

V tomto případě, mám prvek 2^1, $r(2^1) = 12$, a hledám další prvky, jejichž řád je taky 12. Jinými slovy, řeším rovnici pro k:

$$r(2^1) = \frac{12}{\gcd(12, k)} = 12$$

Z toho vyplývá, že k budou všechna čísla nesoudělná s 12. Tedy $k \in \{1, 5, 7, 11\}$ a ty generátory jsou $\{2^1, 2^5, 2^7, 2^{11}\} =$ (podle tabulky, co jsem si vytvořil nahoře) $\underline{\{2, 6, 11, 7\}}$.

1.7 Příklad 7

Najděte všechny generátory grupy $(\mathbb{Z}_{13}, +)$. Kolik různých generátorů má tato cyklická grupa?

Příklad v zásadě stejný jako 1.5. Pro každou cyklickou grupu platí, že cyklická grupa řádu n má právě $\varphi(n)$ různých generátorů, zde tedy cyklická grupa řádu 13 má $\underline{12}$ různých generátorů (a jsou to $\underline{\text{všechny její prvky kromě nuly}}$).

1.8 Příklad 8

Vypište všechny podgrupy multiplikativní grupy $(\mathbb{Z}_{13}^*, \cdot)$. Nejdříve si uvědomte, kolik prvků tyto podgrupy mohou mít.

Řád pogrupy d musí dělit řád grupy, tedy $d|\varphi(13) = 12$. Řády podgrup tedy mohou být $1, 2, 3, 4, 6, 12$ (pogrupa řádu r je generována prvky řádu r). Podgrupa řádu 12 je tedy celá grupa, pogrupa řádu 1 bude generována prvkem 1. U těch ostatních musím najít generátory daného řádu, v příkladu 1.6 už jsem našel generátor řádu 12, což je dvojka. Z toho už se dají dost jednoduše najít generátory požadovaného řádu: použitím vzorce 3 dopočítám ostatní:

- **Řád 2:** $\frac{12}{\gcd(12,k)} = 2$: $k \in \{6\}, a = 2^6 = 64 = 12 \Rightarrow M_2 = \{1, 12\}$
- **Řád 3:** $\frac{12}{\gcd(12,k)} = 3$: $k \in \{4, 8\}, a = 2^4 \wedge 2^8, 2^4 = 16 = 3 \Rightarrow M_3 = \{1, 3, 9\}$
- **Řád 4:** $\frac{12}{\gcd(12,k)} = 4$: $k \in \{3, 9\}, a = 2^3 \wedge 2^9, 2^3 = 8 \Rightarrow M_4 = \{1, 5, 8, 12\}$
- **Řád 6:** $\frac{12}{\gcd(12,k)} = 6$: $k \in \{2, 10\}, a = 2^2 \wedge 2^{10}, 2^2 = 4 \Rightarrow M_6 = \{1, 3, 4, 9, 10, 12\}$

1.9 Příklad 9

Vypište všechny podgrupy aditivní grupy $(\mathbb{Z}_{12}, +)$. Nejdříve si uvědomte, kolik prvků tyto podgrupy mohou mít.

Příklad podobný (dokonce izomorfní :-)) s 1.8. Řád pogrupy d musí dělit řád grupy, tedy $d|12$ (protože prvků v grupě je 12). Řády podgrup tedy mohou být $1, 2, 3, 4, 6, 12$ (pogrupa řádu r je generována prvky řádu r). Podgrupa řádu 12 je tedy celá grupa generovaná prvkem 1 (a grupa $(\mathbb{Z}_{12}, +)$ tudíž je i cyklická, protože má generátor). Podgrupa řádu 1 je zase generována prvkem 0 (to jsou tzv. *triviální podgrupy*, tedy celá grupa a podgrupa generovaná jednotkovým prvkem). U těch ostatních musím najít generátory daného řádu. Znám však generátor řádu 12, což je jednička. Z toho už se dají dost jednoduše najít generátory požadovaného řádu: použitím vzorce 3 dopočítám ostatní:

- **Řád 2:** $\frac{12}{\gcd(12,k)} = 2$: $k \in \{6\}, a = 1 \cdot 6 \Rightarrow M_2 = \{0, 6\}$
- **Řád 3:** $\frac{12}{\gcd(12,k)} = 3$: $k \in \{4, 8\}, a = 1 \cdot 4 \wedge 1 \cdot 8 \Rightarrow M_3 = \{0, 4, 8\}$
- **Řád 4:** $\frac{12}{\gcd(12,k)} = 4$: $k \in \{3, 9\}, a = 1 \cdot 3 \wedge 1 \cdot 9 \Rightarrow M_4 = \{0, 3, 6, 9\}$
- **Řád 6:** $\frac{12}{\gcd(12,k)} = 6$: $k \in \{2, 10\}, a = 1 \cdot 2 \wedge 1 \cdot 10 \Rightarrow M_6 = \{0, 2, 4, 6, 8, 10\}$

Zadání pokračuje: "Grupy $(\mathbb{Z}_{13}^*, \cdot)$ a $(\mathbb{Z}_{12}, +)$ jsou izomorfní. Najděte nějaký izomorfismus mezi nimi."

Co to je vlastně ten *izomorfismus*? Izomorfismus je *bijektivní homomorfismus*. Super. Takže další otázka: Co to je homomorfismus?

Definice 1.1. *Homomorfismus je zobrazení $\phi : A \to B$ mezi dvěma algebraickými strukturami stejného typu takové, že pro každou definovanou operaci f a pro všechna x_i v A platí*

$$\phi(f_A(x_1, \ldots, x_n)) = f_B(\phi(x_1), \ldots, \phi(x_n))$$

Přeloženo do češtiny, je homomorfismus jakési mapování (zobrazení) mezi dvěma algebraickými strukturami, které zachovává strukturu. Například množina přirozených čísel s operací sčítání. Funkce, která zachovává sčítání musí splňovat: $f(a + b) = f(a) + f(b)$. Takže třeba $f(x) = 3x$ je jeden takový homomorfismus, jelikož $f(a + b) = 3(a+b) = 3a+3b = f(a)+f(b)$. Další příklad může být pro grupoid reálných čísel s operací sčítání a grupoid kladných reálných čísel s operací násobení. Funkce, která bude zachovávat operace musí tedy splňovat $f(a+b) = f(a) \cdot f(b)$, jelikož sčítání je operace v prvním grupoidu a násobení ve druhém. Tuto vlastnost splňuje např. $f(x) = e^x$: $2 + 3 = 5$ se zobrazí na $e^2 \cdot e^3 = e^5$.

U homomorfismů platí, že jestliže existuje neutrální prvek, musí být zachován. Takže pro první příklad, $f(0) = 0$, a 0 je netrální prvek vůči sčítání. V druhém případě, $f(0) = 1$, jelikož 0 je neutrální vůči sčítání a 1 vůči násobení.

Další příklad, z Velebilových skript [3], je pro pro grupoid $(\mathbb{Z}, \cdot)$ a $(\mathbb{Z}_4, \odot_4)$ (násobení modulo 4). Zobrazení

$$[-]_4 : \mathbb{Z} \to \mathbb{Z}4,$$

kde $[-]_4$ přiřazuje každému číslu ($[-]$) ze $\mathbb{Z}$ zbytek po dělení 4, je homomorfismus. Pokud si totiž zkusím dosadit pár čísel, pak pro $[x \cdot y]_4 = [x]_4 \odot_4 [y]_4$ dostanu

$$\begin{aligned} [0 \cdot 1]_4 &= [0]_4 \odot_4 [1]_4 && \Rightarrow 1 = 1 \\ \underbrace{[50 \cdot 20]_4}_{0} &= \underbrace{\underbrace{[50]_4}_{2} \odot_4 \underbrace{[20]_4}_{2}}_{0} && \Rightarrow 0 = 0 \end{aligned}$$

(Postup: snažím se najít zobrazení z, které splňuje $z(u \oplus_1 v) = z(u) \oplus_2 z(v)$)

Když se vrátím k izomorfismu, tak to je tzv. *oboustranný* homomorfismus. Tudíž, je to podmnožina homomorfismů. Definice (jen pro pologrupy, monoidy a grupy!) tedy bude podobná jako u homomorfismu, jen musí existovat k zobrazení $A \to B$ i inverzní zobrazení $B \to A$.

Jako příklad izomorfismu se dá (úplně mimo od matematiky) označit hraní kartami. Dejme tomu, že mám 52 hracích karet, jejichž 4 barvy (nebo jak se tomu nadává) jsou $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$. Kdybych si ty 4 barvy označil místo toho jako $\{\alpha, \beta, \gamma, \epsilon\}$, tak můžu hrát úplně stejně, jen si musím zapamatovat, že

$$\begin{aligned} k(\alpha) &= \heartsuit \\ k(\beta) &= \diamondsuit \\ k(\gamma) &= \spadesuit \\ k(\epsilon) &= \clubsuit \end{aligned}$$

Zobrazení k je tedy izomorfismus (neboli struktury se až na označení prvků sobě rovnají).

Další příklad izomorfismu jsou třeba logaritmy. Jak do nás hustili už v EO1 a naposledy PARech, násobení se dá pomocí logaritmu převést na sčítání. Takže mám dvě grupy. Jedna pro násobení (kladných čísel): $G_1 = (\mathbb{R}^+, \cdot, 1, ^{-1})$[2] a druhá pro sčítání: $G_2 = (\mathbb{R}, +, 0, -)$. Homomorfismus je zobrazení $\exp : \mathbb{R} \to \mathbb{R}^+$, zadáno předpisem $x \mapsto e^x$ (protože splňuje definici homomorfismu, tedy pro $\forall(x, y) : \exp(x + y) = e^{x+y} = e^x \cdot e^y = (\exp x) \cdot (\exp y)$). A je zároveň i izomorfní, protože

$$\ln : (\mathbb{R}^+, \cdot, 1, ^{-1}) \to (\mathbb{R}, +, 0, -)$$

a inverzní zobrazení je $\ln^{-1} = \exp$:

$$\exp : (\mathbb{R}, +, 0, -) \to (\mathbb{R}^+, \cdot, 1, ^{-1}).$$

Teď už je konečně jasné, co se po mně v poznámce k zadání příkladu vlastně chce. Mám najít takové zobrazení, které převede $(\mathbb{Z}_{13}^*, \cdot)$ na $(\mathbb{Z}_{12}, +)$. Prvků mají obě stejně 12, takže to asi nějak půjde.

$(\mathbb{Z}_{13}^*, \cdot)$ je generována prvkem 2, tedy $(\mathbb{Z}_{13}^*, \cdot) = <2> = \{2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 8, \ldots, 2^{12} = 1\}$. To si můžu představit jako zobrazení, které každému prvku přiřadí "jakou je mocninou generátoru 2", tedy $f(a) = f(2^k) = k$. To je zřejmě bijekce (jednoznačné zobrazení, každý prvek má jednoznačný obraz a naopak) do $\mathbb{Z}_{12}$. Teď musím ověřit, že se skutečně jedná o homomorfismus. To znamená, že respektuje binární operace, neutrály a inverzy se pak podle věty z přednášky respektují automaticky:

Dejme tomu, že $a = 2^k, b = 2^l$ jsou prvky ze $\mathbb{Z}_{13}^*$.

$$f(a \cdot b) = f(2^k \cdot 2^l) = k + l = f(2^k) + f(2^l) = f(a) + f(b)$$

Jinými slovy, násobení mezi vzory (operace v grupě, z níž zobrazuji), se převede na sčítání mezi obrazy (což je operace v grupě, do níž zobrazuji). Dostal jsem tedy homomorfismus.

Podrobněji viz kapitola 4.

1.10 Příklad 10

Nejděte řády všech prvků v $(\mathbb{Z}_{11}^*, \cdot)$.

Příklad podobný asi třem minulým, v zásadě spočívá pouze v nalezení generátoru a pak dopočítání řádů prvků podle 3. Vím, že $r(1) = 1$. Standardně zkouším dvojku, která zatím vždycky vyšla jako generátor a mocním do $\varphi(11) = 10$:

[2] Tohle označení zmamená, že grupa je definovaná na množině $\mathbb{R}^+$, s operací násobení, neutrální prvek je 1 a inverzi k prvku x vytvořím aplikací x^{-1}

$$
\begin{aligned}
2^1 &= 2 \\
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 5 \\
2^5 &= 10 \\
2^6 &= 9 \\
2^7 &= 7 \\
2^8 &= 3 \\
2^9 &= 6 \\
2^{10} &= 1
\end{aligned}
$$

Dvojka je generátor (překvapivě), $r(2) = 10$. Další generátory budou 2^k, kde $\gcd(k, \varphi(11)) = 1$, což jsou $\{6, 7, 8\}$. $\gcd(k = 5, 10) = 2$, takže $r(10) = 5$. Zbylé prvky budou mít řád 5, protože možné řády jsou jen ty, co dělí 10.

1.11 Příklad 11

V $\mathbb{Z}_{21}$ najděte všechna řešení rovnice $x^2 = x$.

Příklady tohoto typu je asi nejrychlejší řešit Čínskou větou o zbytcích. $\mathbb{Z}_{21}$ si rozdělím na $\mathbb{Z}_3 \times \mathbb{Z}_7$ a řeším pro tyto dvě grupy:

- $\mathbb{Z}_3$: $x^2 = x \Rightarrow x \in 0, 1$
- $\mathbb{Z}_7$: $x^2 = x \Rightarrow x \in 0, 1$

Teď si vypočítám koeficenty pro větu:

$$
\begin{aligned}
q_3 &= s \cdot 7 = s \cdot 1 & [1]_3^{-1} &= 1 \\
&= 1 \cdot 7 = 7 & & \\
q_7 &= 3 \cdot s & [3]_7^{-1} &= 15 \\
&= 3 \cdot 5 = 15 & &
\end{aligned}
$$

Všechna řešení pak už jen budou všechny kombinace: $\{0, 1\} \cdot 7 + \{0, 1\} \cdot 15 = \{0, 1, 7, 15\}$.

1.12 Příklad 12

V $\mathbb{Z}_{39}$ najděte všechna řešení rovnice $x^4 = 1$.

Podobný příklad jako 1.4 a 1.11. Zase rozložím 39 na součin prvočísel, takže $\mathbb{Z}_{39} = \mathbb{Z}_3 \times \mathbb{Z}_{13}$ a řeším pro obě zvlášť. Obecně, rovnice $x^k = 1$ v $\mathbb{Z}_n^*$ má $\gcd(k, \varphi(n)) = d$ řešení a jsou to prvky řádů r, kde $r|d$.

v $\mathbb{Z}_3$ $r(x)$ dělí $\varphi(3)$: $x = 1 \wedge x = -1$

v $\mathbb{Z}_{13}$ Rovnice má $gcd(4, 12) = 4$ řešení a jsou to prvky řádů $1, 2, 4$. Prvek řádu jedna je jeden, $x = 1$. Prvek řádu dva je taky jeden, a je to $(-1) = 12$. Prvky řádu 4 jsou dva $(= \varphi(4))$, a najdu je nejlépe přes generátor (tipnu si dvojku):

$$
\begin{aligned}
2^1 &= 2 \\
2^2 &= 4 \\
2^3 &= 8 \\
2^4 &= 3 \\
2^5 &= 6 \\
2^6 &= 12 \\
2^7 &= 11 \\
2^8 &= 9 \\
2^9 &= 5 \\
2^{10} &= 10 \\
2^{11} &= 7 \\
2^{12} &= 1
\end{aligned}
$$

$$r(2^k) = \frac{12}{\gcd(12,k)} = 4 \Rightarrow k = \{3,9\}$$

Z toho vyplývá, že hledaná x jsou 8 a 5.

Teď výpočet koeficientů:

$$
\begin{aligned}
q_3 &= s \cdot 13 = s \cdot 1 \\
&= 1 \cdot 13 = 13 \\
q_1 3 &= 3 \cdot s \\
&= 3 \cdot 9 = 27 = -12
\end{aligned}
\qquad
\begin{aligned}
[1]_3^{-1} &= 1 \\
\\
[3]_7^{-1} &= 9
\end{aligned}
$$

Všechna řešení jsou tedy $x = \{1,-1\} \cdot 13 + \{1,5,8,12\} \cdot (-12) = \{1,5,8,14,25,31,34,38\}$.

1.13 Příklad 13

1. Najděte generátor grupy $(\mathbb{Z}_{37}^*, \cdot)$. Kolik různých prvků poslouží jako generátor v této cyklické grupě?
2. Najděte všechny prvky řádu 6 v grupě $(\mathbb{Z}_{37}^*, \cdot)$.
3. Řešte rovnici $x^{30} = 1$ v $\mathbb{Z}_{37}$.

Možností, jak zvolit generátor je přesně tolik, kolik je generátorů všech prvků nesoudělných s 37. Takových prvků je $\varphi(37) = 36$ a jejich generátorů je $\varphi(36) = 12$. Zkusím tedy najít generátor řádu 36, což je například 2 (tabulku vypisovat nebudu a doufám, že to po mně nikdo nikdy nebude chtít). Dále postupuji podle profláknutého vzorce 3:

$$r(2^k) = \frac{36}{\gcd(36,k)} = 6 \Rightarrow k = \{6,30\}$$

Tudíž $(\mathbb{Z}_{37}^*, \cdot)$ má prvky 11 a 27 řádu 6.

Rovnici $x^{30} = 1$ v můžu řešit rovnou v $\mathbb{Z}_{37}$, protože 37 je prvočíslo. Rovnice má $\gcd(30,36) = 6$ řešení a jsou prvky řádů dělících 6, tedy $r(a) = \{1,2,3,6\}$ a to jsou $a = \{1,10,11,26,27,36\}$ (zase podle generátoru a vzorce 3).

1.14 Příklad 14

Pro RSA šifrování je dáno $N = 247$ a veřejný klíč $t = 11$. Spočtěte soukromý klíč a dešifrujte zprávu $b = 147$. Pro dešifrování použijte Čínskou větu o zbytcích.

V těchto typech příkladů je zapotřebí si zapamatovat pár vzorců. Je-li t veřejný klíč, s soukromý, a dešifrovaná zpráva a b zašifrovaná zpráva, pak

$$a = b^s \text{ v } \mathbb{Z}_N. \tag{4}$$

$$b = a^t \text{ v } \mathbb{Z}_N. \tag{5}$$

$$t \cdot s = 1 \text{ v } \mathbb{Z}_{\varphi(N)}. \tag{6}$$

První, co musím udělat, je vypočítat rozklad N na prvočísla. To udělám hrubou silou, testováním všech čísel od 3. Tím získám $N = 13 \cdot 19$. Z toho jednoduše vypočtu $\varphi(N) = 216$ a vyřeším rovnici 6:

$$\begin{aligned} 11s + 216y &= 1 \\ 216 &= 19 \cdot 11 + 7 & 7 &= 216 - 19 \cdot 11 \\ 11 &= 1 \cdot 7 + 4 & 4 &= 11 - 1 \cdot 7 = 20 \cdot 11 - 216 \\ 7 &= 1 \cdot 4 + 3 & 3 &= 7 - 4 = 2 \cdot 216 - 39 \cdot 11 \\ 4 &= 3 \cdot 1 + 1 & 1 &= 4 - 3 = \underline{59} \cdot 11 - 3 \cdot 216 \end{aligned}$$

Získal jsem $s = 59$. Teď musím odšifrovat b, neboli dosadit a vypočítat rovnici 4:

$$a = 147^{59} \text{ v } \mathbb{Z}_{247}$$

Tohle vypočítám tak, že si rozložím $\mathbb{Z}_{247} = \mathbb{Z}_{13} \times \mathbb{Z}_{19}$ a počítám pro každé zvlášť:

Pro $\mathbb{Z}_{13}$: $147^{59} = 4^{59} = 4^{4\cdot 12+11} \overset{E-F(2)}{\to} 4^{11} = 2^{22} = 2^{1\cdot 12+10} \overset{E-F}{\to} 2^{10} = 1024 = 10$

Pro $\mathbb{Z}_{19}$: $147^{59} = 14^{59} = 14^{3\cdot 18+5} \overset{E-F}{\to} 14^5$. Tohle číslo už bych sice asi nacpal do kalkulačky, ale ve zkoušce se stejně píše ještě "spočítejte pomocí reziduálního umocňování". Takže tady jsou opakované čtverce, $5 = 1\cdot 4 + 0\cdot 2 + 1\cdot 1$:

1		0		1
X	S		S	X

Jinými slovy, rozepsal jsem si 5 do binární podoby, mezi každou číslici jsem vepsal S a tam, kde je jednička, jsem napsal X. Teď to napíšu pod sebe (nejlevější X je nahoře, nejpravější dole) a dostanu:

X	$14^1 = 14$
S	$14^2 = 6$
S	$14^4 = 17$
X	$14^5 = 10$

Výsledek je tedy $147^{59} = 10$ v $\mathbb{Z}_{19}$. Teď vypočítám koeficenty pro Čínskou větu o zbytcích:

$$\begin{aligned} q_{13} &= s \cdot 19 = s \cdot 6 & [6]_{13}^{-1} &= 11 \\ &= 11 \cdot 19 = 209 = -38 \\ q_{19} &= 13 \cdot s & [13]_{19}^{-1} &= 3 \\ &= 13 \cdot 3 = 39 \end{aligned}$$

A výsledek $\underline{a} = -38 \cdot 10 + 39 \cdot 10 = \underline{10}$.

1.15 Příklad 15

Pro RSA šifrování je dáno $N = 247$ a veřejný klíč $t = 11$. Najděte všechny zprávy x, které se po zašifrování nezmění, tj. platí $x^t = x$ v $\mathbb{Z}_N$, pro dané t a N.

Příklad podobný příkladu 1.12. V zásadě jenom řeším $x^{11} = x$ v $\mathbb{Z}_{13}$ a $\mathbb{Z}_{19}$ a pomocí Čínské věty o zbytcích tato řešení nakombinuji.

Pro $\mathbb{Z}_{13}$: Nejdřív vydělím rovnici x a zapíšu si řešení $x = 0$. Dostanu $x^{10} = 1$, přičemž rovnice má $\gcd(10, 12) = 2 = d$ řešení, a jsou to prvky řádu 1 a 2. Prvek řádu 1 je $x = 1$, prvek řádu 2 je jen jeden, jelikož grupa ma za základ prvočíslo a je tudíž cyklická (prvků řádu r, kde r dělí mohutnost grupy, je právě $\varphi(r)$. Takový prvek je -1. Hledaná řešení jsou tedy $x_{13} = \{0, 1, -1\}$

Pro $\mathbb{Z}_{19}$: Totéž jako v předchozím, rovnice má $\gcd(10, 18) = 2 = d$ řešení, řádu 1 a 2. Hledaná řešení jsou tedy $x_{19} = \{0, 1, -1\}$

Z minulého příkladu 1.14 znám $q_{13} = -38$ a $q_{19} = 39$, všechna řešení budou jen kombinace $-38 \cdot \{0, 1, -1\} + 39 \cdot \{0, 1, -1\} = \{0, 1, 38, 39, 77, 170, 208, 209, 246\}$.

1.16 Příklad 16

Pro RSA šifrování Vám byla přidělena prvočísla $p = 23$, $q = 59$ a veřejný klíč $t = 181$.

1. Spočtěte svůj soukromý klíč
2. Písmena anglické abecedy kódujte dvojčíslími $A = 01$, $B = 02$, $\dots Z = 26$, $mezera = 00$. Posíláte zprávu HARD DAY a chcete ji digitálně podepsat. Domluvená hašovací funkce vybere ze zprávy každou pátou číslici (počítáno zleva). Spočtěte tento podpis a použijte k tomu Čínskou větu o zbytcích.

Ze zadání vyplývá, že $N = 23 \cdot 59 = 1357$. Spočtení soukromého klíče se řeší stejným způsobem jako v 1.14, zde v $\mathbb{Z}_{\varphi(N)} = \mathbb{Z}_{22 \cdot 58} = \mathbb{Z}_{1276}$. Po výpočtu eukleida vyjde

$$1 = \underline{141} \cdot 181 - 20 \cdot 1276,$$

tudíž $s = 141$.

Teď musím zakódovat HARD DAY do čísel:

H	A	R	D		D	A	Y
08	01	$\underline{1}8$	04	$0\underline{0}$	04	01	$\underline{2}5$

Hašovací funkce je tedy $f(a) = 102$. Teď tenhle podpis musím zašifrovat, což znamená vypočítat

$$f(a)^s \text{ v } \mathbb{Z}_N = 102^{141} \text{ v } \mathbb{Z}_{1357}.$$

To se udělá nejlépe Čínskou větou o zbytcích, pro $\mathbb{Z}_{23}$ a $\mathbb{Z}_{59}$. Nejdřív to umocním pomocí reziduálního umocňování:

Pro $\mathbb{Z}_{23}$: $102^{141} = 10^{141} = 10^{6 \cdot 22 + 9} \overset{E-F}{\to} 10^9$.

$9 = 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$:

1		0		0		1
X	S		S		S	X

X	$10^1 = 10$
S	$10^2 = 8$
S	$10^4 = 18$
S	$10^8 = 2$
X	$10^9 = \underline{20}$

Pro $\mathbb{Z}_{59}$: $102^{141} = 43^{141} = 43^{2 \cdot 58 + 25} \overset{E-F}{\to} 43^{25}$.

$25 = 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$:

1		1		0		0		1
X	S	X	S		S		S	X

X	$43^1 = 43$
S	$43^2 = 20$
X	$43^3 = -25$
S	$43^6 = -24$
S	$43^{12} = -14$
S	$43^{24} = 19$
X	$43^{25} = \underline{50}$

Koeficienty (pro jejich výpočet je ještě zapotřebí 2× e-euklid, ale šetřím místem):

$$\begin{aligned} q_{23} &= s \cdot 59 = s \cdot 13 & [13]_{23}^{-1} &= -7 \\ &= -7 \cdot 59 = -413 \\ q_{59} &= 23 \cdot s & [23]_{59}^{-1} &= 18 \\ &= 23 \cdot 18 = 414 \end{aligned}$$

Podpis pak bude $-413 \cdot 20 + 414 \cdot 50 = 12440 = \underline{227}$ (v $\mathbb{Z}_{1357}$).

2 Polynomy nad $\mathbb{Z}_n$ a konečná tělesa

2.1 Příklad 1

V $\mathbb{Z}_2[x]$ najděte největší společný dělitel $d(x)$ polynomů $p(x) = x^7 + x^6 + x^5 + x$ a $q(x) = x^3 + 1$. Polynom $d(x)$ napište jako kombinaci polynomů $p(x)$ a $q(x)$.

Postup je takový, že dělím polynomy, dokud to jde (tzn., dokud nedostanu nulový zbytek) a toto si píšu do tabulky podobné euklidově algoritmu. Nejdřív tedy ty dva polynomy vydělím a uvidím, co vznikne:

$$\begin{array}{rrrrrrrr|l}
x^7 & +x^6 & +x^5 & +x^4 & & & +x & & : (x^3+1) \quad = x^4 + x^3 + x^2 + 1 \\
-x^7 & & & -x^4 & & & & & \\
\hline
 & x^6 & +x^5 & & & & +x & & \\
 & -x^6 & & & +x^3 & & & & \\
\hline
 & & x^5 & & +x^3 & & +x & & \\
 & & -x^5 & & & +x^2 & & & \\
\hline
 & & & & x^3 & +x^2 & +x & & \\
 & & & & -x^3 & & & +1 & \\
\hline
 & & & & & x^2 & +x & +1 &
\end{array}$$

Vidím, že mi vznikl nějaký podíl a nějaký zbytek po dělení. Pokračuji dál:

$$\overbrace{x^7 + x^6 + x^5 + x^4 + x}^{p(x)} = \overbrace{(x^3+1)}^{q(x)}(x^4 + x^3 + x^2) + (x^2 + x + 1)$$
$$q(x) = (x+1)\underline{(x^2 + x + 1)} + 0$$

Zde $(x+1)$ vzniklo jako podíl $(x^3+1) : (x^2+x+1)$.

Z toho je jasně viditelné, že gcd je $d(x) = (x^2 + x + 1)$ a $d(x) = p(x) - (x^4 + x^3 + x^2) \cdot q(x)$ (v dané soustavě je $+$ totéž co $-$, takže zároveň $d(x) = p(x) + (x^4 + x^3 + x^2) \cdot q(x)$).

2.2 Příklad 2

Najděte všechny ireducibilní polynomy pátého stupně v $\mathbb{Z}_2[x]$ a dokažte, že jsou ireducibilní.

Polynomy pátého stupně v $\mathbb{Z}_2[x]$ budou vždy tvaru

$$a \cdot x^5 + b \cdot x^4 + c \cdot x^3 + d \cdot x^2 + e \cdot x + f \cdot 1$$

Jelikož polynom s nulovým absolutním členem má kořen 0, pak absolutní člen musí být roven 1. Dál vím, že musí mít lichý počet nenulových členů, jelikož kdyby měl sudý, tak by řešením byla jednička (protože $(1+1) = 0$).

Tím jsem vyčerpal všechny možnosti, jak řešení osekat a nastává čas na BruteForce™. K ireducibilním polynomům se můžu chovat podobně jako k prvočíslům. Třeba na to, abych dokázal, že 5 je prvočíslo, mi stačí vyzkoušet jen čísla do $\lfloor\sqrt{5}\rfloor$. Stejně tak na to, abych zjistil zda-li je polynom řádu n ireducibilní, mi stačí vyskoušet ho dělit polynomu do stupně $\lfloor n/2 \rfloor$. Tudíž musím najít ireducibilní polynomy stupně 1 a 2 (to jsou $(x+1)$ a (x^2+x+1)) a zkusit jimi vydělit polynom řádu 5 (protože polynom řádu 5 může vzniknout jen jako násobek $1 \cdot 4, 2 \cdot 3, 3 \cdot 2, 4 \cdot 1$). Polynomy si pro zkrácení napíšu jako n-tici (a, b, c, d, e, f), hned vyřadím ty se sudým počtem členů a zkusím dělit (když to dělitelné daným polynomem není, škrtnu ho):

- $(1,0,0,0,1,1)$: ~~$(x+1)$~~, $(x^2+x+1) \cdot (x^3+x^2+1)$
- $\underline{(1,0,0,1,0,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~
- $\underline{(1,0,1,0,0,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~
- $\underline{(1,0,1,1,1,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~
- $(1,1,0,0,0,1)$: ~~$(x+1)$~~, $(x^2+x+1) \cdot (x^3+x+1)$
- $\underline{(1,1,0,1,1,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~
- $\underline{(1,1,1,0,1,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~

- $\underline{(1,1,1,1,0,1)}$: ~~$(x+1)$~~, ~~$(x^2+x+1)$~~

Výpočet se zase dá poněkud zkrátit, když si uvědomím, že pokud polynom nemá kořen, pak zaručeně není ani dělitelný lineárním polynomem (čímž mi v tomto případě vypadne dělení $(x+1)$).

Ireducibilní polynomy pátého stupně v $\mathbb{Z}_2[x]$ jsou: $x^5+x^2+1, x^5+x^3+1, x^5+x^3+x^2+x+1, x^5+x^4+x^2+x+1, x^5+x^4+x^3+x+1, x^5+x^4+x^3+x^2+1$.

2.3 Příklad 3

Rozložte polynom $p(x)=x^7-x$ na součin ireducibilních polynomů v okruzích $\mathbb{Z}_2[x]$ a $\mathbb{Z}_7[x]$.

V okruhu $\mathbb{Z}_7[x]$ je to jednoduché, jelikož

$$\text{v } \mathbb{Z}_p[x] \text{ platí: } x^p-x=x(x-1)\cdots(x-(p-1))$$

a polynom x^7-x se dá rozložit na $x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)=x(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)$.

V $\mathbb{Z}_2[x]$ je to o něco horší, protože takový krásný vzoreček nemám. Takže musím postupně dělit, nejdřív $x$kem a pak postupně ireducibilními polynomy:

$$\begin{aligned}x^7+x &= x\cdot(x^6+1)\\ &= x\cdot(x+1)(x^5+x^4+x^3+x^2+x+1)\\ &= x\cdot(x+1)(x+1)(x^4+x^2+1)\\ &= x\cdot(x+1)(x+1)(x^2+x+1)(x^2+x+1)\end{aligned}$$

Ten součin je tedy $x\cdot(x+1)^2(x^2+x+1)^2$.

2.4 Příklad 4

V $\mathbb{Z}_3[x]$ rozložte na součin ireducibilních polynomů polynom $p(x)=x^7+2x^6+x+2$.

---

x^7+2x^6+x+2 si napíšu jako $x^6(x+2)+x+2=(x^6+1)(x+2)$. Teď si vzpomenu na další krásný vzoreček:

Věta 2.1.

$$(a+b)^p=a^p+b^p \textit{ nad každým tělesem charakteristiky } p,$$

tedy $(x^6+1)=((x^2)^3+1)=(x^2+1)^3$ a konečný výsledek je $p(x)=(x^2+1)^3(x+2)$.

2.5 Příklad 5

Najděte všechny prvky, které jsou invertibilní v $\mathbb{Z}_3[x]/(x^2+2)$. Spočtěte k nim inverzní prvky.

Především je nutné si uvědomit, které všechny prvky může obsahovat okruh:

$$\mathbb{Z}_p[x]/q(x)=\{[a(x)]|st(a)<st(q)\}$$

Jinými slovy, okruh je množina polynomů (+ operace sčítání a násobení), které mají stupeň nižší než $q(x)$. Počet jejích prvků je $p^{st(q(x))}$. Ještě jinak se dá říct, že je to okruh zbytkových tříd modulo $q(x)$, což je něco jako grupa v $\mathbb{Z}_p$, jen prvky nejsou čísla, nýbrž polynomy.

První, co musím udělat, je zjistit, jestli ten okruh je taky těleso. Pokud je, tak to znamená, že všechny prvky (mimo 0) mají inverz. Takže musím udělat `std::deleni` ireducibilními polynomy. Zkusím $(x+1)$, dostanu $p(x)=(x+1)(x+2)$. Takže to není těleso, a inverzy budou mít jen polynomy nesoudělné s $(x+1)(x+2)$ (obdoba toho, co se dělalo u grup, pokud by gcd bylo >1, pak neumím najít inverz). Prvky okruhu jsou $0,1,2,x,x+1,x+2,2x,2x+1,2x+2$:

- 0 inverz je asi $-\infty$, zkrátka ho nemá :-)
- $1\to 1^{-1}=1$

- $2 \to 2^{-1} = 2$ (počítám to jakoby v $\mathbb{Z}_p$)
- $x \to x^{-1} = x$ (protože používám přepisovací pravidlo $x^2 = -2 \Rightarrow x^2 = 1$)
- $x + 1$ - soudělné s $q(x)$, nemá inverz
- $x + 2$ - soudělné s $q(x)$, nemá inverz
- $2x \to 2x^{-1} = 2x$ $(2x \cdot 2x = 4x^2 = 1)$
- $2x + 1$ - soudělné s $q(x)$, protože $x^2 + 2 = (2x + 1) \cdot (2x + 2)$, nemá inverz
- $2x + 2 = 2(x + 1)$ - soudělné s $q(x)$, nemá inverz

2.6 Příklad 6

Zjistěte, zda okruh $A = \mathbb{Z}_3[x]/P(x)$, kde $P(x) = x^3 + x^2 + x + 2$, tvoří těleso. Kolik má okruh A prvků?

Nechť je α kořen polynomu $P(x)$ v okruhu A. Vypište všechny prvky okruhu A ve tvaru polynomů v proměnné α a odvoďte pravidla pro přepisování vyšších mocnin při násobení.

Ověřte, zda je α také kořenem polynomu $Q(x) = 2x^4 + x^3 + x^2 + 1$ v okruhu A.

Najděte inverzní prvek k $(2\alpha^2 + \alpha + 2)$ v okruhu A, pokud existuje.

Okruh tvoří těleso, protože $P(x)$ je ireducibilní, protože je stupně 3 a nemá kořen:

Věta 2.2. *Polynom stupně 2 nebo 3 je ireducibilní právě tehdy, když nemá kořen.*

Má $p^{st(P)} = 3^3 = 27$ prvků (viz příklad 2.5).

Pro imaginární kořen α platí: $\alpha^3 + \alpha^2 + \alpha + 2 = 0$. Z toho se dají odvodit přepisovací pravidla pro násobení:

$$\alpha^3 = 2\alpha^2 + 2\alpha + 1$$

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

To, jestli je α kořenem něčeho, zjistím snadno - za x dosadím α a pokud se to zredukuje na 0, je α kořen.

$$2\alpha^4 + \alpha^3 + \alpha^2 + 1 = 4\alpha + 4 + 2\alpha^2 + 2\alpha + 1 + \alpha^2 + 1 = 6\alpha + 3\alpha^2 + 6 = \underline{0}$$

Nalezení inverzního prvku k $(2\alpha^2 + \alpha + 2)$ se dá udělat dvěma způsoby:

1. Vyřešení rovnice $(2\alpha^2 + \alpha + 2) \cdot (a \cdot \alpha^2 + b \cdot \alpha + c) = 1$ pro nalezení a, b, c

$$2a\alpha^4 + 2b\alpha^3 + 2c\alpha^2 + a\alpha^3 + b\alpha^2 + c\alpha + 2a\alpha^2 + 2b\alpha + 2c =$$

$$\ldots \text{ následuje asi 7 řádků upravování a dosazování } \ldots$$

$$= a(\alpha^2 + 1) + b(2\alpha^2) + c(2\alpha^2 + \alpha + 2)$$

$$\begin{array}{r|llll} \alpha^2: & a & +2b & +2c & = 0 \\ \alpha^1: & & & +c & = 0 \\ 1: & a & & +c & = 1 \end{array}$$

Z toho vyplývá jednak to, že inverz je $(\alpha^2 + \alpha)$ a také to, že je to způsob extrémně náchylný na chyby

2. Vyřešení rozšířeného euklida $A(x)\overbrace{(2x^2 + x + 2)}^{P(x)} + B(x)\overbrace{(x^3 + x^2 + x + 2)}^{R(x)} = 1$

$$R(x) = P(x) \cdot (2x + 1) + 2x \qquad 2x = R(x) - P(x)(2x + 1)$$
$$P(x) = 2x \cdot (x + 2) + 2 \qquad 2 = P(x) - 2x \cdot (x + 2)$$

Jako gcd mi vyšla dvojka, když vynásobím obě strany inverzem k 2 dostanu (něco) +1. V Bezoutově rovnosti tedy na začátku nechám na pravé straně 2, aby se mi to lépe vyjadřovalo, a nakonec to vynásobím 2^{-1}, abych dostal na pravé straně 1:

$$
\begin{aligned}
2 &= P(x) - 2x(x+2) \\
2 &= P(x) - (R(x) - P(x)(2x+1))(x+2) \\
2 &= P(x) - R(x)(x+2) + P(x)(2x^2+4x+x+2) \\
2 &= P(x)(1+2x^2+4x+x+2) - R(x)(x+2) \\
2 &= P(x)(2x^2+2x) - R(x)(x+2) \\
1 &= P(x)\underline{(x^2+x)} - R(x)(2x+1)
\end{aligned}
$$

Výsledek stejný, postup taky pracný :-)

2.7 Příklad 7

Zjistěte, zda okruh $B = \mathbb{Z}_3[x]/Q(x)$, kde $Q(x) = x^3 + x + 2$, tvoří těleso. Kolik má okruh B prvků?
Vypište všechny prvky okruhu B ve tvaru polynomů v proměnné x.
Najděte inverzní prvek k (x^2+1) a k (x^2+2x+1) v okruhu B, pokud existují (řešte polynomiální rovnice).

Aby okruh tvořil těleso, musí být $Q(x)$ ireducibilní. Jelikož polynom je stupně 3 a nemá kořen, pak je ireducibilní; v opačném případě ireducibilní není (je reducibilní :-)). Kořen má, a to 2, takže je je dělitelný polynonem $(x-2) = (x+1)$:

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

Ireducibilní není, a B není těleso. Okruh B má $p^{st(P)} = 3^3 = 27$ prvků. Všechny prvky jsou všechny polynomy stupně nejvýše 2 v $\mathbb{Z}_3[x]$.

Inverzní prvek k (x^2+1) najdu vyřešením $A(x)\overbrace{(x^2+1)}^{P(x)} + B(x)\overbrace{(x^3+x+2)}^{R(x)} = 1$:

$$R(x) = x \cdot P(x) + 2 \qquad\qquad 2 = R(x) - x \cdot P(x) \Rightarrow 1 = 2R(x) + \underline{x} \cdot P(x)$$

Z toho plyne, že $(x^2+1)^{-1} = x$.

Inverzní prvek k (x^2+2x+1) najdu podobně: $A(x)\overbrace{(x^2+2x+1)}^{P(x)} + B(x)\overbrace{(x^3+x+2)}^{R(x)} = 1$

$$
\begin{aligned}
R(x) &= (x+1) \cdot P(x) + (x+1) \\
P(x) &= (x+1)(x+1) + 0
\end{aligned}
$$

Jak je vidno, k (x^2+2x+1) inverz najít nedokážu, protože je soudělný s $Q(x)$.

2.8 Příklad 8

Zdůvodněte, proč je okruh $\mathbb{Z}_2[x]/(x^5+x^2+1)$ tvoří těleso. Kolik má prvků?
Najděte v tomto tělese inverzní prvek k x^2+1 (řešte polynomiální rovnici).
Kolik primitivních prvků má toto těleso? Nalezněte nějaký primitivní prvek.

Polynom $x^5 + x^2 + 1$ je v $\mathbb{Z}_2$ ireducibilní (viz příklad 2.2), okruh je tedy i tělesem. Má $p^{st(P)} = 2^5 = 32$ prvků.

Pro nalezení inverzu k (x^2+1) musím řešit rovnici $A(x)\overbrace{(x^2+1)}^{P(x)} + B(x)\overbrace{(x^5+x^2+2)}^{R(x)} = 1$

$$
\begin{aligned}
R(x) &= P(x) \cdot (x^3+x+1) + x & \qquad x &= R(x) - P(x)(x^3+x+1) \\
P(x) &= x \cdot x + 1 & \qquad 1 &= P(x) - x \cdot x
\end{aligned}
$$

Podle Bezoutovy věty dopočítám inverz:

$$1 = P(x) - (R(x) - (P(x)(x^3 + x + 1))) \cdot x = x \cdot R(x) + P(x)\underline{(x^4 + x^2 + x + 1)}$$

Primitivní prvek tělesa $(F, +, \cdot, 0, 1)$ je generátor grupy $(F \setminus \{0\}, \cdot, 1)$, přičemž takových primitivních prvků je $\varphi(m-1)$, kde m je počet prvků tělesa. Jinými slovy, primitivní prvek tělesa je prvek, jež mi postupným umocňováním dokáže vytvořit všechny nenulové prvky tělesa. Prvek řádu 1 je 1, a jelikož primitivních prvků tělesa je $\varphi(m-1) = \varphi(31) = 30$, tak všechny ostatní (vyjma 0 a 1) musí být primitivní. Obecně jsou v grupě prvky takových řádů, které dělí mohutnost grupy - v tomto případě tedy 1 a 31.

2.9 Příklad 9

Zkonstruujte těleso $GF(16)$, popište jeho konstruování a odvoďte přepisovací pravidla pro násobení.

Nalezněte ve vašem tělese všechny primitivní prvky.

Věta 2.3. *Konečné těleso s n prvky existuje právě tehdy, když n je mocnina prvočísla. Pak existuje právě jedno (až na isomorfismus, tedy ‚přeznačení prvků').*

Toto těleso se nazývá **Galoisovo** a značí se $GF(p^k)$, kde p^k je počet jeho prvků, k je stupeň generujícího (ireducibilního) polynomu a n je základ soustavy grupy $\mathbb{Z}_n$.

V tomto případě tedy mám těleso $GF(2^4)$ a musím najít ireducibilní polynom stupně 4 v $\mathbb{Z}_2$. Vyzkouším tedy postupně polynomy nemající kořen a nemající nulový absolutní člen (rozepíšu si je podobně jako v příkladě 2.2 a jedu):

- $\underline{(1,0,0,1,1)}$: ~~$(x+1)$~~, ~~(x^2+x+1)~~

Hned první pokus byl úspěšný, polynom $x^4 + x + 1$ je ireducubilní a můžu ho použít jako generující. Přepisovací pravidla budou:

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

Co se týče primitivního prvku, platí pravidla z příkladu 2.8, tedy primitivních prvků je $\varphi(16-1) = 8$. Tyto prvky budou evidentně řádu 15. Způsob, jak takový prvek najít je obdobný tomu, co jsem dělal v první části, např. příkladu 1.6. Zkusím třeba kořen α:

$$\begin{aligned}
\triangle\alpha^1 &= \alpha^1 \\
\alpha^2 &= \alpha^2 \\
\triangle\alpha^3 &= \alpha^3 \\
\alpha^4 &= \alpha + 1 \\
\triangle\alpha^5 &= \alpha^2 + \alpha \\
\alpha^6 &= \alpha^3 + \alpha^2 \\
\alpha^7 &= \alpha^4 + \alpha^3 \\
\alpha^8 &= \alpha^2 + 1 \\
\alpha^9 &= \alpha^3 + \alpha \\
\alpha^{10} &= \alpha^2 + \alpha + 1 \\
\alpha^{11} &= \alpha^3 + \alpha^2 + \alpha \\
\alpha^{12} &= \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^{13} &= \alpha^3 + \alpha^2 + 1 \\
\alpha^{14} &= \alpha^3 + 1 \\
\triangle\alpha^{15} &= 1
\end{aligned}$$

Počet prvků grupy je $T \setminus \{0\} = 15$, a jak vím, tak řády prvků musí dělit řád grupy - v tomto případě tedy ty řády mohou být $1, 3, 5$ a 15. Z toho vyplývá, že jen pro rozhodnotí, zda-li je daný prvek generátor, mi ho stačí umocnit na tyhle řády (označeny $\triangle$). Ty ostatní se mi pak ale taky budou hodit. Evidentně α je hledaný generátor, další najdu pomocí vzorce 3:

$$r(a^k) = \frac{r(a)}{\gcd(r(a), k)} \Rightarrow \frac{15}{\gcd(15, k)} = 15 \Rightarrow \gcd(15, k) = 1$$

Hledané primitivní prvky jsou tedy $\{\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}\} = \{\alpha, \alpha^2, \alpha+1, \alpha^4+\alpha^3, \alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+1, \alpha^3+1\}$.

2.10 Příklad 10

Okruh komplexních čísel nad $\mathbb{Z}_p$ je množina $K_p = \{a + b\imath, \text{ kde } a, b \in \mathbb{Z}_p\}$ s operacemi sčítání a násobení jako u komplexních čísel, tj. $\imath^2 = -1$. Dokažte, že okruh komplexních čísel nad $\mathbb{Z}_7$ tvoří těleso, zatímco okruh komplexních čísel nad $\mathbb{Z}_5$ těleso netvoří. (Návod: Najděte izomorfismus na nějaký faktorový okruh okruhu polynomů nad $\mathbb{Z}_p$.)

Najděte řády prvků $\imath, \imath+1$ a $\imath+2$ v multiplikativní grupě tělesa K_7. Je některý z nich primitivním prvkem v tělese K_7?

Návod směřuje na použití následující věty:

Věta 2.4. *Faktorový okruh $\mathbb{Z}_p[x]/q(x)$ je tělesem právě tehdy, když polynom $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$.*

Jinými slovy, pokud dokážu najít izomorfismus na faktorový okruh polynomů, tak k rozhodnutí, jestli je daná věc těleso či nikoliv mi pak jen stačí otestovat, zda-li je $q(x)$ ireducibilní v $\mathbb{Z}_5$ a $\mathbb{Z}_7$.

Podle zadání je sčítání definováno následovně:

$$(a\imath + b) + (c\imath + d) = (a+c)\imath + (b+d)$$

a násobení jako

$$(a\imath + b) \cdot (c\imath + d) = ac\underbrace{\imath^2}_{=-1} + (ad+bc)\imath + bd = (ad+bc)\imath + (bd-ac)$$

Když se na násobení podívám pořádně, tak mě může napadnout, že to, co dělám, je vlastně násobení modulo x^2+1 (na to by se asi dalo přijít tak, že si řeknu, že $x = \imath$ a $x^2+1=0$):

$$(ax+b)\cdot(cx+d) = (acx^2 + (ad+bc)\imath + bd) \bmod (x^2+1) = (ad+bc)x + (bd-ac)$$

Hledaný izomorfismus je tedy $\mathbb{Z}_p[x]/x^2+1$ (ovšem jak se tohle dá dokázat podle definice od Demlové fakt netuším).

Další, v zásadě triviální záležitost, je zjistit, jestli je x^2+1 ireducibilní v $\mathbb{Z}_5$. Má kořen 2 a 3, takže

$$(x^2+1) = (x+2)(x+3) \text{ v } \mathbb{Z}_5.$$

V $\mathbb{Z}_5$ tedy ireducibilní není, zatímco v $\mathbb{Z}_7$ už kořen nemá - tady ireducibilní je.

Co se týče řádů prvků v grupě, tak ty dělí počet prvků v grupě. Počet prvků v grupě $K_7 - \{0\}$ (neboli všechny kombinace $ax+b$, kde pro a mám 7 možností a pro b taky 7 možností) je $7^2 - 1 = 48$ prvků, řády mohou být $1, 2, 3, 4, 6, 8, 12, 16, 24, 48$. V $\mathbb{Z}_7$:

$$\begin{aligned}
\imath^1 &= \imath \\
\imath^2 &= -1 \\
\imath^3 &= -\imath \\
\imath^4 &= 1
\end{aligned}
\qquad
\begin{aligned}
(\imath+1)^1 &= \imath+1 \\
(\imath+1)^2 &= 2\imath \\
(\imath+1)^3 &= 2\imath+5 \\
(\imath+1)^4 &= 3 \\
(\imath+1)^6 &= 6\imath \\
(\imath+1)^8 &= 2 \\
(\imath+1)^{12} &= 6 \\
(\imath+1)^{16} &= 4 \\
(\imath+1)^{24} &= 1
\end{aligned}
\qquad
\begin{aligned}
(\imath+2)^1 &= \imath+2 \\
(\imath+2)^2 &= 4\imath+3 \\
(\imath+2)^3 &= 4\imath+2 \\
(\imath+2)^4 &= 3\imath \\
(\imath+2)^6 &= 2\imath+2 \\
(\imath+2)^8 &= 5 \\
(\imath+2)^{12} &= \imath \\
(\imath+2)^{16} &= 4 \\
(\imath+2)^{24} &= 6 \\
(\imath+2)^{48} &= 1
\end{aligned}$$

Z toho vyplývá, že $(\imath+2)$ je primitivní prvek; $r(\imath+2) = 48, r(\imath+1) = 24$ a $r(\imath) = 4$.

2.11 Příklad 11

Rozložte polynom $f(x) = x^4 + 2x^2 + x + 1$ na součin ireducibilních polynomů nad $\mathbb{Z}_3$ a potom na tělesem $GF(27)$, které si pro tento účel vhodně zkonstruujte.

Nejdřív zkusím vydělit polynom $f(x)$ ireducibilními polynomy nižších stupňů, začnu polynomem $(x + 1)$:

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

A právě jsem dostal rozklad $f(x)$, jelikož polynom $(x^3 + 2x + 1)$ nemá kořen, a pokud polynom stupně 2 či 3 nemá kořen, tak je ireducibilní.

Tím jsem získal takový pěkný ireducibilní polynom, vhodný jako základ tělesa $GF(27)$: $GF(27) = GF(3^3) = \mathbb{Z}_3[x]/x^3 + 2x + 1$.

Věta 2.5. *Prvek $a \in K$ je kořen polynomu $p(x)$, pokud platí rovnost $p(a) = 0$.*

Takže můžu zkoušet kořeny $1, 2, \alpha \ldots$ a pokud to po dosazení dá jako výsledek 0, je to kořen, vydělím jím $f(x)$ a jedu dál.

FIXME: Nesedí s výsledky dr. Gollové!

3 Lineární a cyklické kódy

3.1 Příklad 1

Lineární kód K nad $\mathbb{Z}_3$ délky 5 má generující matici $\mathbf{G} = \begin{pmatrix} 2 & 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 \end{pmatrix}$.

a) Zakódujte informaci $\bar{a} = (102)$ pomocí matice $\mathbf{G}$. Spočtěte systematickou generující matici $\mathbf{G}_S$ kódu K a opět zakódujte informaci $\bar{a} = (102)$ pomocí systematické matice $\mathbf{G}_S$.

b) Spočtěte kontrolní matici $\mathbf{H}$ kódu K a zkontrolujte, zda je slovo $\bar{v} = (12201)$ kódové.

c) Dekódujte $\bar{v}$ za předpokladu, že bylo použito systematické kódování, a potom za předpokladu, že bylo použito kódování pomocí matice $\mathbf{G}$.

---

a) Kódování se provádí pomocí vzorce

$$\bar{w} = \bar{a} \cdot \mathbf{G} \tag{7}$$

Zde tedy $\bar{w} = (102) \cdot \begin{pmatrix} 2 & 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 \end{pmatrix} = (1 \cdot 2 + 0 \cdot 2 + 2 \cdot 0, 1 \cdot 2 + 0 \cdot 0 + 2 \cdot 2, 1 \cdot 0 + 0 \cdot 2 + 2 \cdot 2, 1 \cdot 1 + 0 \cdot 2 + 0 \cdot 0, 1 \cdot 2 + 0 \cdot 2 + 2 \cdot 0) = (2, 6, 4, 1, 2) = (2, 0, 1, 1, 2)$

Převést matici na systematickou matici znamená udělat z ní Gaussovou eliminací matici typu $\mathbf{G} = (\ \mathbf{E}\ \mathbf{B}\ )$, kde $\mathbf{E}$ je jednotková matice. Takže hurá do toho:

$$\begin{pmatrix} 2 & 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 \end{pmatrix} \begin{matrix} \\ \mid \cdot 2 \\ \mid \cdot 2 \\ \mid \cdot 2 \end{matrix} \sim \begin{pmatrix} 1 & 1 & 0 & 2 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow + \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} 2 \sim \begin{pmatrix} 1 & 1 & 0 & 2 & 1 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \leftarrow + \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} 2$$

$$\sim \begin{pmatrix} 1 & 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow + \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} 2 \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} 2 \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad (= \mathbf{G}_S)$$

Systematické zakódování znamená vypočítat $\bar{w}_S = \bar{a} \cdot \mathbf{G}_S = (10221)$ (první tři číslice můžu opsat, díky jednotkové matici).

b) Kontrolní matici vypočítám podle následující věty:

Věta 3.1. *Je-li generující matice $\mathbf{G}_S$ systematická tvaru*

$$\mathbf{G}_S = (\ \mathbf{E}\ \mathbf{B}\ ),$$

pak kontrolní matice $\mathbf{H}$ je rovna

$$\mathbf{H} = (\ -\mathbf{B}^T\ \mathbf{E}\ ),$$

kde $\mathbf{E}$ je jednotková matice řádu $n - k$.

Kód K má k informačních znaků a $n - k$ kontrolních - např. tenhle kód má 3 informační znaky a 2 kontrolní (n je délka kódu, ze $\mathbb{Z}_p^n$, v tomhle případě $\mathbb{Z}_3^5$).

$$\mathbf{H} = (\ -\mathbf{B}^T\ \mathbf{E}\ ) = \left(- \begin{pmatrix} 0 & 1 \\ 2 & 0 \\ 1 & 0 \end{pmatrix}^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Kontrola správnosti slova se provádí pomocí výpočtu syndromu

$$\bar{s}^T = \mathbf{H} \cdot \bar{v}^T \tag{8}$$

Pokud je syndrom nulový, pak je $\bar{v}$ kódové slovo. V tomhle příkladu to vychází

$$\bar{s}^T = \mathbf{H} \cdot \bar{v}^T = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 2 \\ 0 \\ 1 \end{pmatrix} = (6,3) = (0,0) = \bar{o}.$$

Slovo je kódové.

c) Dekódování je v případě systematického kódování jednoduché, jednoduše vezmu informační znaky: $\bar{v} = (\boxed{122}01)$, slovo je $\bar{a}_S = (122)$.

Obecně je to trošku složitější, musím najít souřadnice kódového slova $\bar{v}$ vůči bázi v $\mathbf{G}$. To znamená vyřešit soustavu n rovnic o k neznámých, $(12201) = a_1 \cdot (22012) + a_2 \cdot (20222) + a_3(02200)$.

$$\begin{array}{cccc} 2a_1 & +2a_2 & & = 1 \\ 2a_1 & & +2a_3 & = 2 \\ & 2a_2 & +2a_3 & = 2 \\ a_1 & +2a_2 & & = 0 \\ 2a_1 & +2a_2 & & = 1 \end{array}$$

Od posledního řádku můžu odečíst předposlední, vyjde mi $a_1 = 1$. Pak už stačí jen dosazovat, $a_2 = 1, a_3 = 0$. Tedy slovo $\bar{a} = (110)$.

Trochu větší problém by nastal, kdyby základ soustavy nebylo prvočíslo, protože bych pak nemohl použít Gaussovu eliminaci, ale musel bych to počítat přes inverzní matici a matici doplňků.

3.2 Příklad 2

Je dána kontrolní matice lineárního kódu K nad $\mathbb{Z}_7$, $\mathbf{H} = \begin{pmatrix} 1 & 2 & 2 & 0 & 4 \\ 0 & 2 & 3 & 6 & 1 \end{pmatrix}$.

a) Kolik informačních a kolik kontrolních znaků má kód K? Kolik je kódových slov v K?

b) Spočtěte systematickou generující matici a zakódujte pomocí ní informaci $\bar{a} = (a_1 \dots a_k)$, kde $a_i = 2$ pro všechna $i = 1, \dots, k$.

c) Slovo $\bar{v} = (13360)$ bylo zakódováno systematicky. Ověřte, zda je bez chyby, případnou chybu opravte a dekódujte (Předpokládáme, že chyba je nejvýše jedna).

---

a) Kontrolní matice není určena jednoznačně, a proto ani generující matice nemůže být určena jednoznačně. Nicméně vždy platí, že má vždy n sloupců a její hodnost je $n - k$. Takže zadaný kód má 5 znaků, 2 kontrolní a 3 informační.

Dejme tomu, že mám bázi $(\beta_1 \dots \beta_k)$ kódu K. Potom libovolné kódové slovo lze právě jedním způsobem vyjádřit jako lineární kombinaci $a_1\beta_1 + a_2\beta_2 + \dots + a_k\beta_k$, přičemž koeficienty a_i volím nezávisle p (v $\mathbb{Z}_p$) způsoby. Takže existuje celkem $p \cdot p \cdot p \dots ... = p^k$ různých lineárních kombinací. Neboli počet slov je 7^3.

b) Spočítání systematické generující matice z $\mathbf{H}$ je obrácená aplikace věty 3.1, lépe řečeno vzorce $\mathbf{H} = (\ -\mathbf{B}^T\ \mathbf{E}\ )$. Postup je takový, že si tu kontrolní matici převedu do tvaru, kdy na konci bude jednotková matice a pak pomocí tohohle vzorce získám $\mathbf{B}$. To stačí už jen dosadit do $\mathbf{G}_S = (\ \mathbf{E}\ \mathbf{B}\ )$ a mám generující matici.

$$\mathbf{H} = \begin{pmatrix} 1 & 2 & 2 & 0 & 4 \\ 0 & 2 & 3 & 6 & 1 \end{pmatrix} \overset{\leftarrow +}{\underset{\rightarrow 3}{\sim}} \begin{pmatrix} 1 & 1 & 4 & 4 & 0 \\ 0 & 2 & 3 & 6 & 1 \end{pmatrix} \overset{\rightarrow 2}{\underset{\leftarrow +}{\sim}} \begin{matrix} \\ \cdot 2 \end{matrix} \begin{pmatrix} 2 & 2 & 1 & 1 & 0 \\ 2 & 4 & 4 & 0 & 1 \end{pmatrix}$$

$$\mathbf{B} = -\begin{pmatrix} 2 & 2 & 1 \\ 2 & 4 & 4 \end{pmatrix}^T = \begin{pmatrix} 5 & 5 \\ 5 & 3 \\ 6 & 3 \end{pmatrix}$$

$$\mathbf{G}_S = \begin{pmatrix} 1 & 0 & 0 & 5 & 5 \\ 0 & 1 & 0 & 5 & 3 \\ 0 & 0 & 1 & 6 & 3 \end{pmatrix}.$$

Zakódování slova se řídí vzorcem 7, takže $\bar{a} = (222)$ se zakóduje na $\bar{w} = (22241)$.

c) Ověření správnosti slova se řídí stejnými pravidly jako v příkladu 3.1; musím spočítat syndrom, a pokud nebude nulový, tak opravit chybu.

$$\bar{s}^T = \mathbf{H} \cdot \bar{v}^T = \begin{pmatrix} 1 & 2 & 2 & 0 & 4 \\ 0 & 2 & 3 & 6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \\ 3 \\ 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \end{pmatrix}$$

Syndrom vyšel nenulový, takže slovo obsahuje chybu. Pro její nalezení musím najít, se kterým sloupcem $\mathbf{H}$ je syndrom lineární kombinací. Takový sloupec je sloupec třetí, jelikož $3 \cdot 2 = 6$ a $3 \cdot 3 = 2$. Další takový sloupec není, slovo obsahuje jednu chybu (a víc stejně neumím opravit). Chybové slovo $\bar{e}$ vytvořím tak, že si označím koeficient, kterým jsem vynásobil syndrom tak, abych dostal l-tý sloupec v $\mathbf{H}$ a tento koeficient napíšu na l-té místo v $\bar{e}$, ostatní koeficienty budou nulové: $\bar{e} = (00300)$. Teď tenhle vektor odečtu od přijatého slova a dostanu opravené slovo $\bar{w}$: $\bar{w} = \bar{v} - \bar{e} = (13360) - (00300) = (13060)$.

3.3 Příklad 3

Lineární kód nad $\mathbb{Z}_3$ má generující matici $\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}$. Najděte jeho kontrolní matici.

a) Opravte slovo $\bar{v} = (1020)$ za předpokladu, že obsahuje nejvýše jednu chybu.

b) Jak by se dalo slovo $\bar{v} = (1020)$ opravit, kdyby v něm byly právě dvě chyby? Najděte všechna kódová slova, jejichž Hammingova vzdálenost od $\bar{v}$ je 2.

c) Dokažte, že kód (vždy) opravuje jednu chybu.

Kontrolní matici najdu jediným krokem GEM

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix} \begin{matrix} \\ \leftarrow +^1 \end{matrix} \sim \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

a dosazením do $\mathbf{H} = (\ -\mathbf{B}^T\ \mathbf{E}\ )$:

$$\mathbf{H} = \left(-\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^T \mathbf{E} \right) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

a) Totéž co v příkladu 3.2. Nejdřív si vypočítám syndrom

$$\bar{s}^T = \mathbf{H} \cdot \bar{v}^T = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Vidím, že lineárně závislý je s 2. sloupcem, koeficient je 2. $\bar{e} = (0200), \bar{w} = \bar{v} - \bar{e} = (1020) - (0200) = (1120)$.

b) Opravit by se s jistotou nedalo, jediné, co o něm vím, že by se lišilo přesně ve dvou bitech. To znamená, že jsou to všechna slova s Hammingovou vzdáleností 2. Což jsou $\{(0000), (2021), (1012)\}$.

c) Důkaz spočívá v tom, že žádný sloupec $\mathbf{H}$ není násobkem jiného sloupce v $\mathbf{H}$.

3.4 Příklad 4

ISBN (International Standard Book Number) je lineární délky 10 nad $\mathbb{Z}_{11}$, jehož kódová slova splňují rovnici $\sum_{i=1}^{10} i \cdot v_i = 0$ v $\mathbb{Z}_{11}$. (Pozn. Číslo 10 se v tomto kódu značí X, tedy jako římská desítka.)

a) Opravte slovo $\bar{v} = (1020)$ za předpokladu, že obsahuje nejvýše jednu chybu.

b) Jak by se dalo slovo $\bar{v} = (1020)$ opravit, kdyby v něm byly právě dvě chyby? Najděte všechna kódová slova, jejichž Hammingova vzdálenost od $\bar{v}$ je 2.

c) Dokažte, že kód (vždy) opravuje jednu chybu.

Podrobně vysvětleno ve Velebilových skriptech [3], str. 80-82. Stačil by copy/paste, tak radši nebudu zaplácávat místo. Mimochodem, dokonce je tu Easter Egg - to ISBN mají "Malé dějiny filozofie".

3.5 Příklad 5

Ověřte, zda množina slov tvoří binární lineární kód. Pokud ano, nalezněte jeho generující matici

a) $A = \{(11111), (11110), (11101), (11100), (00011), (00010), (00001), (00000)\}$

b) $B = \{(1111), (1110), (1101), (0011), (0010), (0001), (0000)\}$

Kód je binární, tzn. základ soustavy je 2 a musí mít 2^k slov - tím okamžitě vypadává možnost B), jelikož má jen 7 slov (a třeba $(0010) + (0011) = (0101)$ není kódové slovo). Co se týče 1. možnosti, tak další test musí být ten, zda-li libovolná lineární kombinace kódových slov je zase kódové slovo. Evidentně je, protože protože nenajdu slovo, které bych nedostal lineární kombinací jiných dvou. Zkusím tedy najít bázi prostoru, tzn. 3 takové vektory (protože 2^3), které mi dají libovolné slovo $u = a_1 \cdot g_1 + a_2 \cdot g_2 + a_3 \cdot g_3$, kde a_n je 0 nebo 1. Nejlepší bude najít takové, které mi dají součtem nulový vektor, ale z nichž ani jeden nebude nulový. Taková kombinace je jen jedna:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Na tuhle matici se dá přijít třeba tak, že si vezmu všechna kódová slova, napíšu si je do matice a nad ní provedu GEM. Vypadne mi matice o 3 řádcích, což je hledaná $\mathbf{G}$ (A je podprostor s bází $\mathbf{G}$).

3.6 Příklad 6

Lineární kód délky 4 nad $\mathbb{Z}_3$ má generující matici $\mathbf{G} = \begin{pmatrix} 2 & 2 & 1 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}$.

a) Vypište všechna kódová slova a ověřte, že se jedná o cyklický kód.

b) Najděte generující polynom a pomocí něj zakódujte informaci $\bar{a} = (12)$.

c) Najděte generující matici, která určuje stejné kódování jako generující polynom. Ověřte to zakódováním informace $\bar{a} = (12)$ pomocí této matice.

---

a) Kódová slova budou všechny kombinace báze, tedy $K = \{a_1\beta_1 + a_2\beta_2, a_i \in \mathbb{Z}_3\}$. Kódových slov bude $p^k = 3^2$ (viz příklad 3.2). Ta slova jsou $(2211), (2112), (1122), (1221), (0000), (2010), (0102), (1020), (0201)$. Jak je vidno, pro každé slovo existuje v K i jeho cyklický posun $\Rightarrow$ kód je cyklický.

b) Generující polynom je nenulový polynom nejnižšího stupně ($= n - k$). Takový polynom je tady stupně 2 a z těch kódových slov, co jsem si nahoře vypsal, jsou takoví adepti 2. Já si vyberu (0102), pak $g(z) = z^2 + 2$ je monický. Zakódování (12) znamená vynásobit polynom $g(z)$ polynomem $u(z) = 1 + 2z$ (v $\mathbb{Z}_3^{(4)}$, což je jiné označení pro okruh $\mathbb{Z}_3[x]/(x^4 - 1)$). Takže zakódovaně $v(z) = 2 + z + z^2 + 2z^3$.

c) Generující matice kódu je rovna

$$\mathbf{G} = \begin{pmatrix} g(z) \\ z \cdot g(z) \\ \vdots \\ z^{k-1}g(z) \end{pmatrix} = \begin{pmatrix} 2 + z^2 \\ 2z + z^3 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$$

Zkusím zakódovat (12) a uvidíme, jestli mi vyjde (2112):

$$\bar{w} = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = (2112)$$

Vyšlo, matice určuje stejné kódování.

3.7 Příklad 7

Cyklický kód délky 6 nad $\mathbb{Z}_3$ má generující polynom $g(z) = z^2 + z + 1$.

a) Kolik informačních znaků a kolik kontrolních znaků má kód K? Kolik je kódových slov v K?

b) Zakódujte pomocí $g(z)$ informaci ze samých 1, tj. $\bar{a} = (a_1 \dots a_k)$, kde $a_i = 1$ pro všechna $i = 1, \dots, k$.

c) Najděte kontrolní polynom a ověřte pomocí něj, zda je slovo $\bar{v} = (100200)$ bez chyb. Pokud ano, dekódujte.

---

a) Generující polynom má stupeň $n - k = 2$ (k je počet info-znaků a n délka kódu), a tedy kontrolní znaky jsou 2 a informační znaky jsou 4. Kódových slov je $p^k = 3^4$.

b) Zakódování $\bar{a} = (1111)$:

$$w(z) = g(z) \cdot a(z) = (z^2 + z + 1)(1 + z + z^2 + z^3) = 1 + 2z + 2z^4 + z^5$$

c) Kontrolní polynom $h(z)$ získám jako podíl $(z^n - 1) : g(z)$, tedy $h(z) = (z^6 - 1) : (z^2 + z + 1) = z^4 + 2z^3 + z + 2$. Ověření znamená vynásobit $h(z) \cdot v(z)$ v $\mathbb{Z}_3$ podle pravidla $z^6 = 1$ a jako výsledek dostat 0: $(z^4 + 2z^3 + z + 2) \cdot (1 + 2z^3) = 3z^4 + 6z^3 + 3z + 6 = 0 \Rightarrow$ je bez chyb. Dekódování $\bar{v} = (100200)$ znamená vydělit kódové slovo generujícím polynomem:

$$\bar{w} = (2z^3 + 1) : (z^2 + z + 1) = 2z + 1 \equiv \bar{a} = (1200).$$

3.8 Příklad 8

Ověřte, že polynom $g(z) = 1 + 2z + 2z^2 + z^3$ může generovat cyklický kód délky 6 nad $\mathbb{Z}_3$.

a) Zakódujte systematicky zprávu $\bar{a} = (122)$ pomocí $g(z)$.

b) Najděte kontrolní polynom $h(z)$ a ověřte, že váš polynom je kódový.

c) Nalezněte systematickou generující matici daného kódu a pomocí ní opět systematicky zakódujte zprávu $\bar{a} = (122)$.

Aby polynom mohl generovat lineární kód délky 6 nad $\mathbb{Z}_3$, musí dělit generující polynom $(z^6 - 1)$ v $\mathbb{Z}_3$ beze zbytku. Jelikož

$$(z^6 - 1) : (z^3 + 2z^2 + 2z + 1) = z^3 + z^2 + 2z + 2 \,(= h(z)),$$

tak $g(x)$ je generující polynom.

a) Systematické zakódování zprávy znamená udělat z ní polynom takový, který bude na začátku stejný jako kódové slovo a na konci bude mít nějaké kontrolní znaky (podobně to bylo v lineárních kódech, viz. třeba příklad 3.1). Aby se prohloubila schizofrenie studenta algebry, tak teď už slova nebudou kódovat jako $(a_1 a_2 a_3) \sim (a_1 \cdot z^0 + a_2 \cdot z^1 + a_3 \cdot z^2)$, jak tomu bylo v případě cyklických nesystematických kódů, ale pro změnu jako $(a_1 a_2 a_3) \sim (a_1 \cdot z^2 + a_2 \cdot z^1 + a_3 \cdot z^0)$.

   Zakódovanou zprávu vytvořím tak, že si vytvořím polynom s nejvššími koeficienty na začátku, tedy v tomto případě (122) jako $(z^5 + 2z^4 + 2z^3)$ a tenhle polynom vydělím polynomem generujícím. Tím získám nějaký zbytek po dělení, který odečtu od posílaného polynomu. Takže:

$$(z^5 + 2z^4 + 2z^3) : (z^3 + 2z^2 + 2z + 1) = z^2, \text{ zbytek } r(z) = 2z^2$$
$$w(z) = v(z) - r(z) = z^5 + 2z^4 + 2z^3 + z^2$$

b) Kontrolní polynom $h(z)$ už jsem našel na začátku, ověření znamená vynásobit $h(z) \cdot w(z) = (z^3 + z^2 + 2z + 2) \cdot (z^5 + 2z^4 + 2z^3 + z^2) = 0$, můj polynom je kódový.

c) Systematickou generující matici daného kódu najdu úplně stejným postupem jako v příkladu 3.6. Nejdřív si musím uvědomit, jak získám k. Dr. Gollová používá nějaký sofistikovaný výpočet, já postupuji systémem KOUKNU A VIDIM^{TM}: generující polynom je nejnižšího stupně, jaký se v tom kódu vyskytuje, a ten stupeň je roven $n-k=3$. Evidentně $n-(n-k)=k$, takže $n-3=k \Rightarrow n=6, k=3$ (ono je to úplně jasné, pokud si člověk uvědomí, že pokud se využívají jen znaky od 3 a výš, protože nejmenší polynom je $z^3 \ldots$ tak ty kódově nevyužité znaky řádu $0,1,2$ se použijí na kontrolní znaky).

$$\mathbf{G} = \begin{pmatrix} g(z) \\ z \cdot g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} = \begin{pmatrix} z^3 + 2z^2 + 2z + 1 \\ z^4 + 2z^3 + 2z^2 + z \\ z^5 + 2z^4 + 2z^3 + z^2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$$

Tahle matice zrovna moc systematicky nevypadá, takže ji ještě proženu GEM, abych takovou získal:

$$\begin{pmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix} \overset{\leftarrow +}{\underset{\leftarrow +}{\underset{\longrightarrow 1}{}}} \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix} \overset{\leftarrow +}{\underset{\longrightarrow 2}{}} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix} \quad (= \mathbf{G}_S)$$

Následuje zakódování $\bar{a} = (122)$, což už jsem dělal minimálně ve třech předchozích příkladech, a to podle vzorce 7.

$$\bar{w} = \bar{a} \cdot \mathbf{G}_S = (122) \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix} = (122100)$$

3.9 Příklad 9

Najděte generující polynomy všech cyklických kódů délky 5 nad $\mathbb{Z}_5$.

a) Vyberte nějaký generující polynom cyklického kódu délky 5 nad $\mathbb{Z}_5$ se 3 informačními znaky. Najděte některou jeho generující matici a některou jeho kontrolní matici.

b) Zjistěte, zda je $\bar{v} = (12221)$ kódové slovo vámi vybraného kódu. Pokud ne, opravte chybu, je-li to možné.

Generující polynom musí dělit polynom $(x^5 - 1)$ v $\mathbb{Z}_5[x]$. Jelikož 5 je prvočíslo, a tedy to, nad čím počítám je těleso, tak platí následující vzorec:

$$(a+b)^p = a^p + b^p$$

(x^5-1) si tedy můžu napsat jako $(x^5+(-1)^5)$, což se podle vzorce rovná $(x-1)^5$. Teď už je poměrně jednoduché najít všechny generující polynomy: jsou to polynomy $(x-1)^i$, kde $i \in < 0; 5 >$. Jelikož však polynom $(x-1)^0$ nemá kontrolní znaky, a $(x-1)^5$ zase nemá žádné informační, tak netriviální generující polynomy jsou jen tvaru $(x-1)^i$, kde $i \in \{1,2,3,4\}$.

a) Generující polynom se 3 informačními znaky je $g(z) = (z-1)^2 = z^2 - 2z + 1 = z^2 + 3z + 1$ $(k=3)$. Generující matici najdu stejně jako minule:

$$\mathbf{G} = \begin{pmatrix} g(z) \\ z \cdot g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} = \begin{pmatrix} z^2 + 3z + 1 \\ z^3 + 3z^2 + z \\ z^4 + 3z^3 + z^2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}$$

Pro vytvoření kontrolní matice musím nejdřív najít kontrolní polynom. Ten najdu vydělením: $h(z) = (z-1)^5 : (z-1)^2 = (z-1)^3 = z^3 + 2z^2 + 3z + 4$. Kontrolní matici pak vytvořím tak, že vezmu postupně koeficienty od nejvyššího do nejnižšího řádu a píšu je do řádků matice, začnu vlevo a na každém řádku posunu koeficienty o 1 doprava. Zbylé budou 0. Počet řádků je tolik, kolik je kontrolních znaků = 2.

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}$$

b) Zjištění, zda je $\bar{v} = (12221)$ kódové slovo se provádí stejným způsobem jako v příkladu 3.2. Nejdřív si vypočítám syndrom:

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

Syndrom je nenulový, a je lineární kombinací sloupce 3, s koeficientem $e = 2$. Tedy $\bar{e} = (00200)$ a $\bar{w} = \bar{v} - \bar{e} = (12221) - (00200) = (12021)$.

3.10 Příklad 10

Najděte generující polynomy všech binárních cyklických kódů délky 5 a napište jejich systematické generující matice.

Stejný postup jako minule, generující polynom musí dělit polynom $(x^5 - 1)$ v $\mathbb{Z}_2[x]$. Bohužel už tady nemůžu použít ten zupa vzorec, protože polynom má jiný řád než je základ soustavy. Takže zkusím dělit ireudicibilními polynomy:

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

Takže jsem našel jeden $g_1(x) = (x + 1)$. Teď je otázka, jestli je $(x^4 + x^3 + x^2 + x + 1)$ ireducibilní. Nemá kořen, takže zřejmě už nepůjde vydělit $(x + 1)$. Mohl by jít tedy vydělit $(x^2 + x + 1)$, což je ireducibilní polynom stupně 2. To ovšem taky nejde $\Rightarrow g_2(x) = (x^4 + x^3 + x^2 + x + 1)$.

$(z + 1)$:

$$\mathbf{G}_1 = \begin{pmatrix} g(z) \\ z \cdot g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} = \begin{pmatrix} z + 1 \\ z^2 + z \\ z^3 + z^2 \\ z^4 + z^3 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Když se na to člověk podívá, tak se jedná o slova délky 5 se sudým počtem jedniček - takže jde o paritní kód.

$(x^4 + x^3 + x^2 + x + 1)$:

$$\mathbf{G}_2 = \begin{pmatrix} g(z) \\ z \cdot g(z) \\ \vdots \\ z^{k-1} g(z) \end{pmatrix} = \begin{pmatrix} z^4 + z^3 + z^2 + z + 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Možná slova jsou jen $\{(00000), (11111)\}$, tudíž se jedná o opakovací kód.

3.11 Příklad 11

Najděte cyklický kód nad $\mathbb{Z}_3$, jehož kontrolní matice má ve sloupcích všechna nenulová slova délky 2 nad $\mathbb{Z}_3$. Najděte generující polynom tohoto kódu. Návod: využijte těleso GF(9) a jeho primitivní prvek.

To těleso $GF(9) = GF(3^2), \mathbb{Z}_3,\ \mathrm{st}(g(x)) = 2$, generující polynom třeba $P(x) = x^2 + x + 2$ má primitivní prvek např. $\alpha = i + 1$. Ten mi dokáže vygenerovat všechny nenulové prvky, které chci (přepisovací pravidlo $i^2 = 2i + 1$):

$$\alpha^1 = i + 1$$
$$\alpha^2 = i + 2$$
$$\alpha^3 = 2i$$
$$\alpha^4 = 2$$
$$\alpha^5 = 2i + 2$$
$$\alpha^6 = 2i + 1$$
$$\alpha^7 = i$$
$$\alpha^8 = 1$$

Přepsáno do matice **H**:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Protože sloupce **H** jsou uspořádány podle mocnin, tak $\mathbf{H} \cdot v^T = o^T$ iff $v(\alpha) = 0$, aneb kódová jsou právě ta slova, která mají kořen α ve vytvořeném tělese $GF(9)$. Polynom $p(x)$ použitý k vytváření tělesa má kořen α a žádný polynom nižšího stupně nemá v tělese kořen α (neboť pomocí toho α se zapisují prvky tělesa a jsou to všechny polynomy nižšího stupně než st(p), a nejsou to nuly). Takže $p(z)$ je nenulový kódový polynom nejnižšího stupně, tedy generující polynom.

4 Homomorfismy a podgrupy

You asked me once, what was in Room 101. I told you that you knew the answer already. Everyone knows it. The thing that is in Room 101 is the worst thing in the world.

–George Orwell, 1984

4.1 Příklad 1

Popište obraz libovolného binárního slova u v homomorfismu $\varphi : (\{0,1\}^*, \circ) \to (\mathbb{Z}_{12}, +)$, je-li dáno $\phi(0) = 3, \phi(1) = 7$. (Pozn.: $\{0,1\}^*$ je množina všech binárních slov včetně prázdného a $\circ$ je zřetězení binárních slov.

Co říká to zadání je, že chci nějaké mapování, nějaké zobrazení, funkci, které mi řekne, jakou hodnotu bude mít zřetězení dvou binárních slov v zadaném homomorfismu.

Jinak řečeno, tupě si opíšu definici 1.1:

$$\phi(f_A(x_1, \ldots, x_n)) = f_B(\phi(x_1), \ldots, \phi(x_n))$$

Nejdřív zkusím, co mi to udělá po dosazení dvou prvků:

$$\begin{aligned}\phi(f_A(x_1, x_2)) &= f_B(\phi(x_1), \phi(x_2)) \\ \phi(x_1 \circ x_2) &= \phi(x_1) + \phi(x_2) \\ \phi(0 \circ 1) &= \underbrace{\phi(0)}_{3} + \underbrace{\phi(1)}_{7}\end{aligned}$$

Jak vidím, $\phi(0 \circ 1)$ musí mít hodnotu 10. Zkusím to teda pro více hodnot:

$$\begin{aligned}\underbrace{\phi(0 \circ 0 \circ 1)}_{13} &= \underbrace{\phi(0)}_{3} + \underbrace{\phi(0)}_{3} + \underbrace{\phi(1)}_{7} \\ \underbrace{\phi(0 \circ 1 \circ 1)}_{17} &= \underbrace{\phi(0)}_{3} + \underbrace{\phi(1)}_{7} + \underbrace{\phi(1)}_{7}\end{aligned}$$

Takhle to budu zkoušet do zblbnutí, nebo do té doby, než mi dojde, že ta hodnota na levé straně je 3x počet nul + 7x počet jedniček. Takže obraz binárního slova u je $\varphi(u) = 3n + 7j$, kde n je počet jeho nul a j je počet jedniček.

4.2 Příklad 2

Najděte všechny grupové homomorfismy $f : (\mathbb{Z}_6, +) \to (\mathbb{Z}_{15}, +)$ a $g : (\mathbb{Z}_6, +) \to (\mathbb{Z}_{15}^*, \cdot)$.

Nejdříve je nutné si uvědomit, co to vlastně hledám:

Definice 4.1. *Nechť $(G, \cdot)$ a $(H, \circ)$ jsou grupy. Zobrazení $f : G \to H$ je grupový homomorfismus, pokud pro každé $a, b \in G$ platí*

$$f(a \cdot b) = f(a) \circ f(b),$$

zároveň

$$f(e_G) = e_H$$

a pro každé a platí

$$f(a^{-1}) = (f(a))^{-1}.$$

V podstatě se jedná o přepsání definice 1.1. Jinými slovy, hledám takovou funkci, zobrazení, která mi dá stejnou hodnotu na pravé i levé straně rovnice pro libovolné a, b. Co vím je, že generátor první grupy je <1>, takže libovolné x si můžu vyjádřit jako $n \cdot 1$. Co dál vím je, že $\varphi(0) = 0$, podle druhého bodu definice. Označím si tedy obraz jedničky jako a, neboli $\varphi(a) = 1$. Teď si tyhle informace dosadím do definice:

$$\varphi(x) = \varphi(\underbrace{1 + \ldots + 1}_{n}) = \underbrace{\varphi(1) + \ldots + \varphi(1)}_{n} = a \cdot n.$$

Neboli jsem dostal $\varphi(x) = a \cdot n$. Pokud bych měl jako zadání najít homomorfismus $\mathbb{Z} \to \mathbb{Z}$, tak to můžu označit za výsledek pro libovolné x a a, a končím. Nicméně to nemůžu, protože grupy mají pouze omezený počet prvků. Zkusím si to rozepsat:

$$\begin{aligned}\varphi(1) &= 1a\\ \varphi(2) &= 2a\\ \varphi(3) &= 3a\\ \varphi(4) &= 4a\\ \varphi(5) &= 5a\\ \varphi(6) &= 6a\end{aligned}$$

Problém je, že 6 je totéž co 0 v $\mathbb{Z}_6$, neboli $\varphi(6) = 6a = \varphi(0) = 0$. Nyní tedy musím vyřešit tuto rovnici:

$$6a = 0 \text{ v } \mathbb{Z}_{15}.$$

Tato rovnice má přesně 3 řešení, jelikož $\gcd(6, 15) = 3$, a jsou to $a_1 = 0, a_2 = 5, a_3 = 10$. Teď už mám konečně hotové řešení, a to $\varphi_1(x) = 0 \cdot x, \varphi_2(x) = 5 \cdot x, \varphi_3(x) = 10 \cdot x$. Jiná řešení nejsou, kdybych si napsal třeba $\varphi_s(x) = 4x$, tak $\varphi_s(6) = 4 \cdot 6 = 24 = 9 \neq f(0) = 0$ v $\mathbb{Z}_{15}$.

Pro druhý homomorfismus budu postupovat podobně, nejdřív vyřeším neutrální prvky. Tím dostanu rovnici $\varphi(0) = 1$. Dál postupuji jako minule, generátor v první grupě je opět $<1>$, $\varphi(1) = a$:

$$\varphi(x) = \varphi(\underbrace{1 + \ldots + 1}_{n}) = \underbrace{\varphi(1) \cdot \ldots \cdot \varphi(1)}_{n} = a^n.$$

Dostávám tvar $\varphi(x) = a^n$. Zbývá dořešit $\varphi(6) : \varphi(6) = a^6 = \varphi(0) = 1$. Dostávám rocnici

$$a^6 = 1 \text{ v } \mathbb{Z}_{15},$$

jejíž vyřešení v praxi znamená vyřešit příklad podobný příkladu 1.12:

Rozložím 15 na součin prvočísel, takže $\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$ a řeším pro obě zvlášť. Obecně, rovnice $x^k = 1$ v $\mathbb{Z}_n^*$ má $\gcd(k, \varphi(n)) = d$ řešení a jsou to prvky řádů r, kde $r|d$.

v $\mathbb{Z}_3$ Má $\gcd(6, \varphi(3)) = 2$ řešení, a jsou to prvky řádů 1 a 2 $\Rightarrow x = 1 \wedge x = -1$

v $\mathbb{Z}_3$ Má $\gcd(6, \varphi(5)) = 2$ řešení, a jsou to prvky řádů 1 a 2 $\Rightarrow x = 1 \wedge x = -1$

Teď výpočet koeficientů čínské věty:

$$\begin{aligned} q_3 &= s \cdot 5 = s \cdot 2 & [2]_3^{-1} &= 2\\ &= 2 \cdot 5 = 10 & &\\ q_5 &= 3 \cdot s & [3]_5^{-1} &= 2\\ &= 3 \cdot 2 = 6 & &\end{aligned}$$

Všechna řešení jsou tedy $a = \{1, -1\} \cdot 10 + \{1, -1\} \cdot 6 = \{1, 4, 11, 14\}$.

Isomorfismy tedy budou 4, a to $g_1(x) = 1, g_2(x) = 4^x, g_3(x) = 11^x, g_4(x) = 14^x, x \in \mathbb{Z}_6$.

4.3 Příklad 3

Najděte všechny grupové homomorfismy $f : (\mathbb{Z}_9^*, \cdot) \to (\mathbb{Z}_{21}, +)$ a $g : (\mathbb{Z}_9^*, \cdot) \to (\mathbb{Z}_{21}^*, \cdot)$.

Použiju stejný postup co minule - nejprve vyřeším neutrály, čímž dostanu $f(1) = 0$. Jelikož $<2>$ je generátor 1. grupy, můžu vyjádřit libovolný prvek x v ní jako $x = 2^n$. Homomorfismus tohoto generátoru si tedy napíšu jako $\varphi(2) = a$, a jedu jako motorová myš:

$$\varphi(x) = \varphi(2^n) = \varphi(\underbrace{2 \cdot \ldots \cdot 2}_{n}) = \underbrace{\varphi(2) + \ldots + \varphi(2)}_{n} = a \cdot n.$$

Neboli tvar homomorfismu je $\varphi(x) = \varphi(2^n) = a \cdot n$, zbývá najít, pro která a to platí:

$$\varphi(2^9) = 9a = \varphi(2^0) = \varphi(1) = 0,$$

neboli

$$9a = 0 \text{ v } \mathbb{Z}_{21}.$$

Řešení jsou $gcd(9, 21) = 3$, a to $a_1 = 0, a_2 = 7, a_3 = 14$, výsledek $\varphi_1(x) = 0 \cdot n, \varphi_2(x) = 5 \cdot n, \varphi_3(x) = 10 \cdot n$. kde $x = 2^n$.

Druhý příklad je poněkud zapeklitější, ale jeho řešení podobné, jako minule. Dejme tomu, že mám homomorfismus φ. Protože $(\mathbb{Z}_9^*, \cdot) = < 2 >$, z hodnoty v bodě 2 můžu dopočítat hodnoty všech bodech: je-li $\varphi(2) = a$, a $\varphi(1) = 1$, pak

$$\varphi(x) = \varphi(2^n) = \varphi(\underbrace{2 \cdot \ldots \cdot 2}_{n}) = \underbrace{\varphi(2) \cdot \ldots \cdot \varphi(2)}_{n} = a^n.$$

Zbývá vyřešit

$$\varphi(2^6) = a^6 = \varphi(2^0) = 1,$$

neboli

$$a^6 = 1 \text{ v } \mathbb{Z}_{21}^*.$$

To splňují všechny prvky v (necyklické) $\mathbb{Z}_{21}^*$, takže řešení je $g_i(x) = a^n$, kde $a \in \mathbb{Z}_{21}^*$, pro $x = 2^k \in \mathbb{Z}_9^*$.

4.4 Příklad 4

Najděte podgrupu v grupě $\mathbb{Z}_{19}^*$, která je izomorfní s grupou $\mathbb{Z}_9^*$. Najděte předpis nějakého izomorfismu mezi nimi.

Pro začátek musím najít podgrupu $\mathbb{Z}_{19}^*$ mající stejný počet prvků jako $\mathbb{Z}_9^*$. Cyklická grupa má $\varphi(n)$ prvků, takže $\mathbb{Z}_9^*$ má $\varphi(9) = 3^2 - 3 = 6$ prvků. V $\mathbb{Z}_{19}^*$ hledám takové prvky, které mají řád 6 - k tomu musím nejprve najít generátor, zkusím 2:

$$\begin{aligned}
2^1 &= 2 & 2^{10} &= 7\\
2^2 &= 4 & 2^{11} &= 5\\
2^3 &= 8 & 2^{12} &= 1\\
2^4 &= 7 & 2^{13} &= 2\\
2^5 &= 5 & 2^{14} &= 4\\
2^6 &= 1 & 2^{15} &= 8\\
2^7 &= 2 & 2^{16} &= 7\\
2^8 &= 4 & 2^{17} &= 5\\
2^9 &= 8 & 2^{18} &= 1
\end{aligned}$$

Dvojka je, jako obvykle, generátor $\mathbb{Z}_{19}^*$. Nalezení generátoru řádu 6 je už je jednoduché, $\gcd(18, k) = 18/3 \Rightarrow k = 3 \wedge k = 12 \Rightarrow g_1 = 8 \wedge g_2 = 12$. Podgrupa izomorfní s $\mathbb{Z}_9^*$ je $<8> = <12> = \{1, 7, 8, 11, 12, 18\}$.

Nalezení izomorfismu znamená nalezení jakéhosi mapování 1:1 mezi nosnými množinami (viz číslování karet v příkladu 1.9). Takové mapování najdu zřejmě snadno - na levé straně mám 6 prvků generovaných $2^a, a = \langle 1, 6\rangle$, na pravé straně mám 6 prvků generovaných $8^a, a = \langle 1, 6\rangle$ (nebo 12^a). Izomorfismus tedy bude $2^a \cong 8^a$, neboli $\varphi(x = 2^a) = 8^a$ (nebo $\varphi(x = 2^a) = 12^a$), $a \in \mathbb{Z}_9^*$.

4.5 Příklad 5

Nechť T je těleso o devíti prvcích. Najděte $n \in \mathbb{N}$ tak, aby multiplikativní grupa $(T^*, \cdot)$ byla izomorfní s grupou $(\mathbb{Z}_n, +)$. Zkonstruujte nějaké GF(9) na napište předpis hledaného izomorfismu.

Věta 4.1. *Cyklická grupa řádu n je izomorfní s $(\mathbb{Z}_n, +)$.*

Řád grupy je 8, jelikož je cyklická a obsahuje všechny prvky tělesa vyjma nuly - což je osm prvků. Proto je izomorfní se $(\mathbb{Z}_8, +)$, přičemž $n = 8$.

Těleso GF(9) jsem už zkonstruoval v příkladu 3.11.

T^* je cyklická grupa, dvě cyklické grupy o stejném počtu prvku jsou izomorfní, pričemž izomorfismus zobrazí generátor na generátor (a pak stejné mocniny na stejné mocniny). Zbýva u zkonstruovaného tělesa najít primitivní prvek (generator T^*) - tedy (i+1) (viz 3.11) a napsat předpis homomorfismu

$$f : \mathbb{Z}_8 \to T^* : f(k) = (i+1)^k.$$

4.6 Příklad 6

Nechť $T = \mathbb{Z}_5[x]/x^2 + x + 1$. Kolik prvků mohou mít podgrupy multiplikativní grupy $(T^*, \cdot)$? Vypište tabulku pro násobení v nějaké tříprvkové podgrupě a v nějaké čtyřprvkové podgrupě.

První, co musím zjistit je, jestli je $x^2 + x + 1$ ireducibilní polynom. Zřejmě je, jelikož nemá kořen, a polynomy stupně 2 a 3 jsou ireducibilní, když nemají kořen. T je tedy těleso, a to dokonce $GF(25) = GF(5^2)$. Jak jsem popsal v předchozím příkladu, tak jeho grupa má $25 - 1 = 24$ prvků, a jelikož je i cyklická, tak obsahuje podgrupy řádů d, kde d dělí 24 (viz. třeba příklad 1.8). Řády jsou tedy $1, 2, 3, 4, 6, 8, 12, 24$. Proto, abych našel nějakou tříprvkovou a čtyřprvkovou grupu, musím najít nejlépe primitivní prvek tělesa grupy, nebo alespoň prvky řádu 3 a 4.

Zkusím $\alpha \Rightarrow r(\alpha) = 3$, prvek dokáže vygenerovat podgrupu o 3 prvcích, $P_3 = \{1, \alpha, 4\alpha + 4, \}$. Dál zkusím $(\alpha + 1) \Rightarrow r(\alpha + 1) = 6$. Tak zkouším $(\alpha + 2) \Rightarrow r(\alpha + 2) = 24$, konečně úspěch. Teď už mi jen stačí najít nějaký prvek řádu 4, tzn. $gcd(24, k) = 24/4 \Rightarrow k = 6$ (třeba). $(\alpha + 2)^6 = 3$, $P_4 = \{1, 2, 3, 4\}$.

$\cdot$	1	α	$4\alpha + 4$
1	1	α	$4\alpha + 4$
α	α	$4\alpha + 4$	1
$4\alpha + 4$	α	α	α

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

4.7 Příklad 7

Které z následujících zobrazení $f_i : K \to K$, kde K je těleso komplexních čísel nad $\mathbb{Z}_3$, je homomorfismus těles?

a) $f_1(a\imath + b) = (a\imath + b)^3$,

b) $f_2(a\imath + b) = (a\imath + b)^6$,

c) $f_2(a\imath + b) = (a\imath + b)^9$.

Tady je nutné ověřit, že se jedná tělesový homomorfismus, tedy že respektuje sčítání, násobení, $\underline{0}$ a $\underline{1}$. Tedy např. zda platí $f(a + b) = f(a) + f(b)$ pro libovolné $a, b \in K$ atd.

Důležitou roli hraje vzorec $(a + b)^p = a^p + b^p$ v tělese charakteristiky p (**nedopočítáno**).

a) $(\imath + \imath)^3 = (2\imath)^3 = -2\imath = (\imath)^3 + (\imath)^3 = -\imath - \imath$,

b) $(\imath + \imath)^6 = (2\imath)^6 = -1 \neq (\imath)^6 + (\imath)^6 = \imath^2 + \imath^2 = -2$,

c) $(\imath + \imath)^9 = (2\imath)^9 = 2\imath = (\imath)^9 + (\imath)^9 = 2\imath$.

5 Svazy a Booleovy algebry

And now for something completely different.

5.1 Příklad 1

Je dána množina A^* všech slov nad abecedou A. Na množině A^* je definovaná operace předpisem

$$u \sqsubseteq v \text{ iff } v = wu \text{ pro nějaké slovo } w \in A^*.$$

Rozhodněte, zda se jedná o uspořádání a zda existují suprema a infima všech dvojic prvků z A^*, případně jak se suprema a infima najdou.

Co to znamená, když se řekne, že relace je uspořádání? To znamená, že relace je *reflexivní*, *antisymetrická* a *tranzitivní* (ve zkratce RAT):

Relace $\sqsubseteq$ na množině A se nazývá

- *reflexivní*, jestliže pro $\forall a \in A$ platí $a \sqsubseteq a$
- *antisymetrická*, jestliže pro $\forall a, b \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq a$, pak $a = b$
- *tranzitivní*, jestliže pro $\forall a, b, c \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq c$, pak $a \sqsubseteq c$

Teď zpátky k zadání. Co se tu říká je, že slovo u je "menší"než v, pokud v má na svém konci část u (u je suffixem u). Neboli, ještě lépe, pokud třeba $u = 4$ a $v = 1234$, pak $u \sqsubseteq v$. Teď vyřeším podmínky pro uspořádání:

- *reflexivní*: pro $\forall a \in A$ platí $a \sqsubseteq a$, tzn. třeba $1234 \sqsubseteq 1234 \Rightarrow$ to je splněno, jelikož pokud $w = \emptyset$, pak $u = v$.
- *antisymetrická*: pro $\forall a, b \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq a$, pak $a = b \Rightarrow$ to je splněno také. Nedokážu totiž najít dvě rozdílná slova, pro něž by platily obě nerovnosti.
- *tranzitivní*: pro $\forall a, b, c \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq c$, pak $a \sqsubseteq c \Rightarrow$ to platí také, znamená to, že a je suffixem jak b, tak i c.

Relace je tedy uspořádání. Teď co je to závora:

Definice 5.1. *Pokud je množina A uspořádána relací $\sqsubseteq$ a B je podmnožina A, pak prvek $a \in A$ je **horní závorou** B, právě když pro $\forall b \in B$ platí $b \sqsubseteq a$.*

Není to tedy nutně prvek množiny, v níž hledám horní závoru, a dokonce nemusí být jen jeden, ale může jich být více - třeba pro množinu reálných čísel $(0, 1)$ jsou horní závory např. čísla $1, 5, \pi$ ad. Dolní závora má definici podobnou, pro tu množinu jsou dolní závory třeba čísla $0, -1, -\pi$.

Definice 5.2. ***Supremum množiny** B je nejmenší ze společných horních závor všech prvků množiny B, podobně **infimem množiny** B je nejvetší ze společných dolních závor všech prvků množiny B.*

Pro ten příklad $(0, 1)$ je tedy supremum $= 1$, infimum $= 0$, a stejné supremum/infimum má i $\langle 0, 1 \rangle$.

Zpět k zadání. Mám zjistit, jestli existují suprema a infima všech *dvojic* prvků. To slovo dvojic je důležité, jelikož jinak bych hledal supremum nekonečné množiny. Podstatná věc, kterou můžu vyčíst ze zadání je, že dva prvky nemusí být vůbec porovnatelné - dejme tomu slovo $a = 12$ a slovo $b = 34$ - ani jedno není suffixem druhého, takže nemůžu rozhodnout, které je menší a které větší. Pozor však na to, že ač jsou prvky neporovnatelné, ještě to neznamená, že nemají infimum nebo supremum.

Dejme tomu, že mám dva neporovnatelné prvky, třeba 234 a 567. Nejsem schopen najít jejich společnou horní závoru, jelikož pro 234 (který je menší[3] než $1234 < 11234$ atd.) už nikdy nenajdu stejný prvek, který by byl zároveň větší než 567 ($< 1567 < 11567$ atd.). Supremum nemohu najít. V případě, že jsou prvky porovnatelné, třeba 1 a 21, tak nejmenší horní závora je prvek 21, neboli ten větší z nich. V případě infima, pokud jsou prvky neporovnatelné, jsem ale stále schopen najít největší dolní závoru - prázdný řetězec. Pokud porovnatelné jsou, pak infimum je jejich nejdelší společný suffix (třeba pro 1 a 21 je dolní závora 1).

[3] Pozor na značení, v písemce je vždy nutné používat „$\sqsubseteq$" namísto názornějšího „$\leq$"

5.2 Příklad 2

Označme $\mathcal{F}$ množinu všech posloupností $\{a_n\}_{n=0}^{\infty}$ přirozených čísel a definujme relaci $\sqsubseteq$ takto:

$$\{a_n\}_{n=0}^{\infty} \sqsubseteq \{b_n\}_{n=0}^{\infty} \text{ právě tehdy, když 1) } a_0 = b_0, \text{ 2) } a_n \geq b_n$$

Ukažte, že $(\mathcal{F}, \sqsubseteq)$ je uspořádaná množina. Pro které dvojice posloupností existuje supremum a pro které infimum a jak se utvoří? Je $(\mathcal{F}, \sqsubseteq)$ svaz?

Nejdřív je zase nutné pochopit zadání - jedná se o posloupnosti nekonečně mnoha čísel, přičemž posloupnost je třeba $\{1, 2, 1, 2, \ldots\}$, nebo třeba $\{10, 20, 30, \ldots\}$. Důležité je, že mají stejný počet prvků ($= \infty$). Nastává otázka, jestli se jedná o uspořádání:

- *reflexivita*: pro $\forall a \in A$ platí $a \sqsubseteq a$, tzn. třeba $\{2, 3, 2, \ldots\} \sqsubseteq \{2, 3, 2, \ldots\} \Rightarrow$ to je splněno, $a_0 = a_0$ a libovolné $a_n \geq a_n$.
- *antisymetričnost*: pro $a, b \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq a$, pak $a = b \Rightarrow$ to taky platí, $a_0 = b_0$ a pro každé a_n platí, že je-li $a_n \leq b_n$ a zároveň $a_n \geq b_n$, pak $a_n = b_n$.
- *tranzitivita*: pro $\forall a, b, c \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq c$, pak $a \sqsubseteq c \Rightarrow$ to platí také, znamená to, že $a_0 = b_0 = c_0$ a je-li $a_n \geq b_n$ a $b_n \geq c_n$, pak $a_n \geq c_n$.

$(\mathcal{F}, \sqsubseteq)$ je uspořádaná množina. Podle definice je menší ta posloupnost, kde každé $a_n \geq b_n$. Tzn. číslo, které bude určitě menší než obě posloupnosti, musí mít číslo na pozici n větší, než jaká jsou a_n i b_n (a pokud to má být největší dolní závora, pak toto číslo $c_n = \max(a_n, b_n)$, což je hledané infimum; u suprema $c_n = \min(a_n, b_n)$). Problém nastává, pokud číslo na první pozici bude jiné v obou posloupnostech - pak totiž nemohu nikdy rozhodnout, jestli je některá posloupnost menší nebo větší, a nemůžu ani najít dolní, nebo horní závoru těch prvních čísel (mám jenom informaci o tom, co se děje, když $a_0 = b_0$, ale už ne o tom, co se děje, když $a_0 \neq b_0$).

Otázka svazu se vyřeší rychle:

Definice 5.3. *Svaz je uspořádaná množina* $(A, \sqsubseteq)$*, kde pro každé* $a, b \in A$ *existuje* $\sup(\{a, b\})$ *a* $\inf(\{a, b\})$.

Evidentně $(\mathcal{F}, \sqsubseteq)$ není svaz.

5.3 Příklad 3

Na množině M všech binárních slov délky nejvýše tři je dána relace předpisem

$$u \sqsubseteq v \text{ iff } |u| < |v|, \text{ anebo } |u| = |v| \text{ a } u_i \leq v_i \text{ pro všechna } i$$

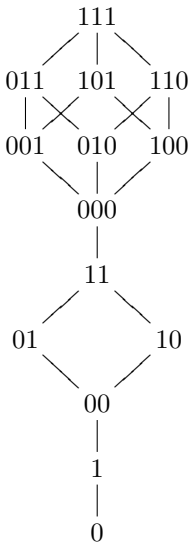
a) Dokažte, že daná relace je uspořádání a nakreslete Hasseho diagram.

b) Ověřte, že $(M, \sqsubseteq)$ tvoří svaz (napište, jak najít supremum a infimum pro libovolnou dvojici prvků).

c) Vyšetřete vlastnosti daného svazu (tj. zda má největší a nejmenší prvek, zda je distributivní, komplementární či dokonce Booleova algebra).

Zde předpokládám, že zavisí na počtu znaků ve slově, tedy např. že $001 \neq 01$

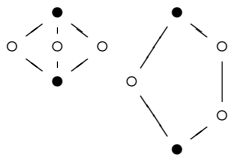
a) Hasseho diagram je následující:



- *reflexivita*: pro $\forall a \in A$ platí $a \sqsubseteq a$, tzn. třeba $010 \sqsubseteq 010 \Rightarrow$ to je splněno, každý znak je stejný a délka slova se nemění.
- *antisymetričnost*: pro $a, b \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq a$, pak $a = b \Rightarrow$ to také platí. Dvě slova, aby se nerovnala, musí mít buď jinou délku, nebo rozdílné znaky na alespoň jednom místě - pokud toto není splněno, pak se nutně musí rovnat.
- *tranzitivita*: pro $\forall a, b, c \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq c$, pak $a \sqsubseteq c \Rightarrow$ to platí také, znamená to, že se slova buď rovnají, nebo že má menší slovo alespoň na jednom místě menší znak a na žádném místě nemá větší. To platí pro všechna slova, tedy tato relace je tranzitivní.

b) Pro každou dvojici prvků existuje supremum a infimum, což je viditelné z Hasseho diagramu. Pokud jsou jejich délky rozdílné, pak jejich supremum je ten menší prvek z nich, supremum ten větší z nich. Pokud jsou jejich délky shodné, pak supremum je slovo složené z maxim odpovídajících dvojic znaků (třeba $\sup(101, 110) = 111$) a infimum z jejich minim ($\sup(101, 110) = 100$). Uspořádaná množina tvoří svaz.

c) Svaz má nejmenší prvek $\underline{0}$ a největší $\underline{111}$, což vyplývá z Hasseho diagramu. Aby byl svaz distributivní, nesmí obsahovat ani jeden z následujících svazů jako podsvaz (první se nazývá trojlampiónek, $\mathcal{L}_3$, druhý pentagon, $\mathcal{P}_5$):



Evidentně neobsahuje ani jeden z nich jako podsvaz, tudíž je distributivní. Komplementární už však nikoliv, třeba 000 nemá komplement.

Definice 5.4. *Každý distributivní a komplementární svaz nazveme* Booleova algebra*.*

Svaz není komplementární, nejedná se o Booleovu algebru.

5.4 Příklad 4

Na množině slov délky dva nad $\mathbb{Z}_3$ je definováno uspořádání vztahem

$$u \sqsubseteq v \text{ iff } u_i \leq v_i \text{ pro všechna } i$$

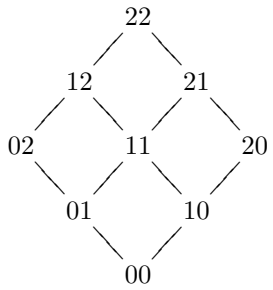
Nakreslete Hasseho diagram a rozhodněte podle něj, zda se jedná o distributivní nebo komplementární svaz. Pokud svaz není distributivní, nalezněte trojici prvků, na které není splněn distributivní zákon. Pokud svaz není komplementární, nalezněte prvek, který nemá doplněk

---

Nejdřív si napíšu, o která slova se vlastně jedná:

$$\begin{array}{ccc} 00 & 10 & 20 \\ 01 & 11 & 21 \\ 02 & 12 & 22 \end{array}$$

Z toho na Hasseho diagram přijdu snadno a rychle:



Distributivní evidentně je, neobsahuje $\mathcal{L}_3$ ani $\mathcal{P}_5$. Teď k problému komplementárnosti.

Definice 5.5. *Svaz $(A, \vee, \wedge, \sqsubseteq)$ s nejmenším prvkem $\underline{0}$ a největším prvkem $\underline{1}$ se nazývá* komplementární*, jestliže každý prvek $a \in A$ má doplněk.*

Co to znamená, že má prvek doplněk? To znamená, že prvek $b \in A$ je doplňkem prvku $a \in A$ právě tehdy, když

$$b \vee a = \underline{1} \text{ a } b \wedge a = \underline{0}.$$

Pomůcka může být taková, že to $\vee$ jakoby ohraničuje prvky zeshora, zatímco $\wedge$ je ohraničuje zespoda.

Z téhle pomůcky se dá vyjít i při určování výsledků $a \vee b = \sup(\{a, b\})$ a $a \wedge b = \sup(\{a, b\})$: $\vee$ je to "větší"(supremum), $\wedge$ je to "menší"(infimum). Pro ty dvě operace dál platí ve svazu $(A, \sqsubseteq)$ následující:

(1) *idempotence*: pro $\forall a \in A$ platí
$$a \vee a = a \text{ a } a \wedge a = a$$

(2) *komutativita*: pro každé dva prvky $a, b \in A$ platí
$$a \vee b = b \vee a \text{ a } a \wedge b = b \wedge a$$

(3) *asociativita* (nebo taky přezávorkování): pro každé tři prvky $a, b, c \in A$ platí
$$a \vee (b \vee c) = (a \vee b) \vee c \text{ a } a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

(4) *absorbce*: pro každé dva prvky $a, b \in A$ platí
$$a \vee (b \wedge a) = a \text{ a } a \wedge (b \vee a) = a$$

Pokud nějaká množina, nad níž jsou definovány operace $\vee$ a $\wedge$ splňující předchozí podmínky, pak relace $\sqsubseteq$ je uspořádání na množině A pokud platí

$$a \sqsubseteq b \text{ právě tehdy, když } a \wedge b = b \text{ (tj. } a \vee b = a).$$

Zpátky k problému komplementárnosti - aby byl svaz komplementární, tak musím pro každý jeho prvek a nalézt doplněk, tzn. prvek b takový, že $b \vee a = \underline{1} = 22$ a $b \wedge a = \underline{0} = 00$, neboli, v řeči uspořádaných množin:

$$\text{komplement k } a \text{ je } b \text{ iff } \sup(a, b) = \text{nejvetší prvek, } \inf(a, b) = \text{nejmenší prvek}$$

Teď tedy musím najít způsob, jak vytvořit supremum a infimum ke každému prvku. To bude stejné jak minule, tedy $\sup(a, b) = (\forall i)(max(a_i, b_i))$ a $\inf(a, b) = (\forall i)(min(a_i, b_i))$, kde a_i, b_i jsou jednotlivé znaky slov.

Co se týče komplementárnosti, tak řeba pro prvek 11 doplněk nenajdu, svaz tedy není komplementární, a podle definice 5.4 se tedy nejedná ani o Booleovu algebru.

5.5 Příklad 5

$(D_{60}, |)$ je množina všech kladných dělitelů čísla 60 uspořádaná podle relace dělitelnosti.

a) Ověřte, že se jedná o svaz a nakreslete jeho Hasseho diagram.

b) Vyšetřete vlastnosti daného svazu (tj. zda má největší a nejmenší prvek, zda je distributivní, komplementární či dokonce Booleova algebra).

c) Která z následujících podmnožin uspořádaných podle dělitelnosti je podsvaz v $(D_{60}, |)$?
$A = \{2, 4, 6, 12\}$, $B = \{2, 4, 6, 10, 60\}$.

---

a) Nejdříve jak ověřit, že se jedná o svaz - tady použiju druhou definici svazu, nicméně podle té první by se to dalo dokázat taky (ten vztah $x \sqsubseteq y$, neboli uspořádání, je dělitelnost. $x \sqsubseteq y$ iff x dělí y beze zbytku. Jelikož sup=lcm a inf=gcd a jelikož gcd i lcm dvou čísel, která dělá 60, je opět dělitelem 60, tak existují suprema a infima pro každou dvojici a je to tedy svaz).

Nejdřív ale musím vyřešit problém suprema a infima pro dva prvky. To je nejjednodušší určit až pohledem do Hasseho diagramu (HD), který se vyskytuje o pár odstavců níže - nicméně by to šlo i bez toho (i když složitěji). Vidím, že pro dva prvky je supremum ten prvek, který je "nahoře"v diagramu, a infimum ten, co je "dole". Ten, co je nahoře, je nejmenší společný násobek (tedy $a \vee b = \text{lcm}(a, b)$), ten, co je dole, je největší společný dělitel ($a \wedge b = \gcd(a, b)$).

(a) *idempotence*: pro $\forall a \in A$ platí

$$a \vee a = a \quad \text{a} \quad a \wedge a = a$$

$\gcd(a, a) = a, \text{lcm}(a, a) = a \Rightarrow$ platí

(b) *komutativita*: pro každé dva prvky $a, b \in A$ platí

$$a \vee b = b \vee a \quad \text{a} \quad a \wedge b = b \wedge a$$

u *gcd* i *lcm* je jedno, jestli je prvek na 1. nebo 2. místě $\Rightarrow$ platí

(c) *asociativita* (nebo taky přezávorkování): pro každé tři prvky $a, b, c \in A$ platí

$$a \vee (b \vee c) = (a \vee b) \vee c \quad \text{a} \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

Neboli $\text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(\text{lcm}(a, b), c)$. Důkaz tohohle je trochu složitější, protože si člověk musí uvědomit, jak se to *lcm* vlastně počítá. Počítá se tak, že si rozložím číslo na součin prvočísel (třeba $60 = 2^2 \cdot 3 \cdot 5$ a pro druhé číslo udělám totéž (třeba $4 = 2^2$). Pak si napíšu tyhlety rozklady pod sebe a lcm(a,b) bude součin prvočísel s max. umocněním, takže dostanu

$$\begin{array}{rl} 60 = & 2^2 \cdot 3^1 \cdot 5^1 \\ 4 = & 2^2 \cdot 3^0 \cdot 5^0 \\ \text{lcm}(60, 4) = & 2^2 \cdot 3^1 \cdot 5^1 = 60 \end{array}$$

Co dělám je, že hledám maximální koeficienty u prvočísel - a je úplně jedno, jestli to udělám nejdřív pro 1. a 2. číslo, a pak k tomu najdu 3., nebo v jiném pořadí. Je to i úplně stejný postup, jako bych dělal lcm(a,b,c). Pro *gcd* to udělám *Hard-Way*©:

Věta 5.1. *Binární operace* gcd *je asociativní, tj. pro libovolná přirozená čísla* a, b, c *platí*

$$\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)).$$

Důkaz. Položím $d = gcd(gcd(a, b), c)$. Co to znamená? To znamená, že (1) d dělí $\gcd(a, b)$ a c a (2) jestliže d' je nějaké jiné přirozené číslo, $d' \neq d$, které dělí beze zbytku $\gcd(a, b)$ a c, pak nutně $d > d'$. K tomu, abych dokázal asociativitu gcd, musím dokázat, že (1) d dělí a a $\gcd(b, c)$ a (2) jestliže d' je nějaké jiné přirozené číslo, které dělí a a $\gcd(b, c)$, potom $d > d'$.

(1) Jelikož d dělí $\gcd(a, b)$, d musí dělit a a b. Vím, že d dělí c, tedy d musí dělit i $\gcd(b, c)$.

(2) Předpokládám, že d' dělí a a $\gcd(b, c)$. Potom d' dělí b a c, takže d' musí dělit i $\gcd(a, b)$. Tedy, podle předpokladu, $d > d'$.

□

(d) *absorbce*: pro každé dva prvky $a, b \in A$ platí

$$a \vee (b \wedge a) = a \quad \text{a} \quad a \wedge (b \vee a) = a$$

Neboli $\text{lcm}(a, \gcd(b, a)) = a$. Označím si $d = gcd(b, a)$. Toto číslo $d \leq \min(a, b)$, a číslo a bude násobkem čísla d. Pokud si dosadím d, tak dostanu $\text{lcm}(a, d) = a$. To je vždy splněno, jelikož a je násobkem d. Ten druhý tvar by se dokazoval dost podobně.

Všechny čtyři podmínky splněny, jedná se o svaz.

Jak nakreslit HD? Jedno z možných řešení (a překvapivě použitelných) spočívá ve čtyřech krocích:

(a) Vypsání všech prvků svazu

(b) Pro každý prvek nakreslení jeho jednoúrovňového Hasseova diagramu přímých dělitelů, vpravo největší, vlevo nejmenší. Toto dělat rekurzivně pro každý HD každého prvku, dokud se nedostanu na prvočíslo. Tzn. třeba pro prvek 20 to budou prvky 10 a 4, ale už ne třeba 10,5,4, protože 5 dělí 10. Pak znovu nakreslit HD pro 10 a 4.

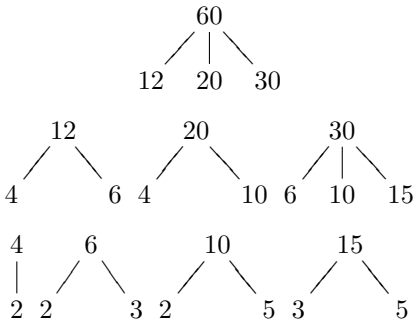
(c) Pospojování těchto prvků do Hasseova diagramu, zase do úrovní řadit prvky zprava doleva.

(d) (Překreslení diagramu do nějaké rozumější podoby, která se objeví v předchozím bodě.)

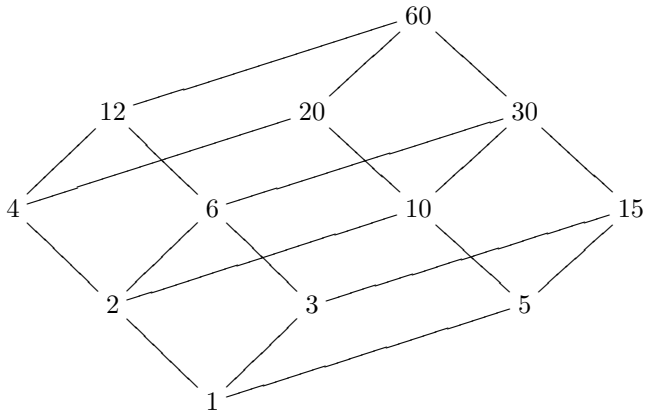
Pro tento příklad tedy

(a) $(D_{60}, |) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

(b) MiniHD:



(c) MeziHD:



Poslední krok tady nebyl nutný, ale když to člověk kreslí na papíře, tak se obvykle hned netrefí do takové krásné podoby.

b) Nejmenší prvek svazu je z HD $\underline{0} = 1$, největší $\underline{1} = 60$. Distributivita se dá dokázat buď tak, že v HD nenajdu $\mathcal{L}_3$ ani $\mathcal{P}_5$ jako podsvaz (což tady opravdu nenajdu). Co je to vlastně podsvaz[4]:

Definice 5.6. *Mějme dán svaz $L = (A, \vee, \wedge, \sqsubseteq)$. Množinu $B \subseteq A$ nazveme* podsvaz *svazu L, jestliže platí*

$$\textit{je-li } b, c \in B, \ \textit{pak } b \vee c, b \wedge c \in B.$$

[4]Dr. Gollová má na cvičení 12/2 napsáno, že podsvaz je podmmožina, kde operace $\vee, \wedge$ dávají stejné výsledky. To si myslím nemůže fungovat, protože svaz jako celek je i svým podsvazem a $\sup(a, \bar{a})$ nemůže být stejné jako $\inf(a, \bar{a})$.

Alternativně, můžu se problém distributivity dívat i takhle:

Definice 5.7. *Svaz* $(A, \vee, \wedge, \sqsubseteq)$ *se nazývá* distributivní *svaz, jestliže pro každé tři prvky* $a, b, c \in A$ *platí*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Přičemž stačí ověřovat jen jednu z podmínek.

Takže hurá do toho:

Věta 5.2. *Svaz* $(\mathbb{N}, lcm, \gcd, |)$ *je distributivní, neboli pro každé* $a, b, c \in N$ *platí*

$$\gcd(a, lcm(b, c)) = lcm(\gcd(a, b), \gcd(a, c))$$

Důkaz. Každému z čísel a, b, c přiřadím celočíselný rozklad, tzn. třeba $a = 2^3 \cdot 3^1 \cdot 7^1, b = 2^2 \cdot 3^2 \cdot 7^0$. Pak operace $\cup$ (sjednocení) prvočísel odpovídá lcm, operace $\cap$ (průnik) odpovídá gcd. Např.

$$\begin{array}{ll} \text{lcm} = & 2^3 \cdot 3^2 \cdot 7^1 \quad \leftrightarrow A \cup B \\ \gcd = & 2^2 \cdot 3^1 \cdot 7^0 \quad \leftrightarrow A \cap B \end{array}$$

Jelikož operace $\cup$ a $\cap$ jsou distributivní, pak i gcd a lcm jsou distributivní. □

Svaz není komplementární, protože třeba k prvku 2 nejsem schopen najít doplněk. Není to tedy ani Booleova algebra.

c) Při ověřování, zda je něco podsvazem, postupuji podle definice 5.6, musím tedy zjistit, zda je pro každou dvojici prvků výsledek operace $\vee$ a $\wedge$ zase prvkem svazu. U svazu A to je, ale u svazu B nikoliv - třeba $4 \vee 6 = \text{lcm}(4, 6) = 2^2 \cdot 3 = 12 \notin B$.

5.6 Příklad 6

Dokažte, že $(D_n, |)$ je Booleova algebra právě, když n je square free. $(D_n, |)$ je množina všech kladných dělitelů čísla n uspořádaná podle relace dělitelnosti. Přirozené číslo je square free, pokud není dělitelné druhou mocninou žádného prvočísla.

Nejdřív si musím uvědomit, jak funguje lcm a gcd: lcm vezme sjednocení prvočísel, gcd vezme jejich průnik. Když chci, abych dostal prvek maximální, tak musím těmi prvky obsadit všechna místa, tzn. třeba pokud mám $(D_{30}, |)$, a hledám doplněk pro $a = 15 = 3 \cdot 5$, tak musím najít takové číslo, které mi obsadí ještě to poslední místo do $30 = 2 \cdot 3 \cdot 5$, což je supremum svazu - což je evidentně $\bar{a} = 2$. Podobně infimum, tam zase nesmím žádným prvočíslem (vyjma 1) obsadit místa pod sebou - takže pro $a = 15 = 3 \cdot 5$ je to zase $\bar{a} = 2$. Kdybych ovšem měl třeba $(D_{60}, |)$, tak mám problém s tím, že v prvočíselném rozkladu můžu mít i mocniny. Třeba pro $60 = 2^2 \cdot 3 \cdot 5$, kdybych hledal doplněk k $2 = 2^1$ a snažil se použít podobný způsob jako u $(D_{30}, |)$, tak mám problém, protože 1. místo už bude vždy obsazené 2, a tudíž nikdy nedocílím toho, aby průnik těch prvočíselných rozkladů byl prázdný. Proto musím zabránit tomu, aby šlo libovolné číslo vyjádřit jako $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, kde libovolné k_n je vyšší než 1 - a toho docílím pouze tehdy, je-li supremum square free.

5.7 Příklad 7

Ukažte, že v každé Booleově algebře $(B, \wedge, \vee, 0, 1, \bar{})$ platí:

$$a \sqsubseteq b \text{ iff } a \wedge \bar{b} = 0.$$

Důkaz. Jelikož mám zadanou ekvivalenci, tak musím dokázat obě implikace (tedy $\Rightarrow$ a $\Leftarrow$):

$\Rightarrow$ Za základ si položím, že $a \sqsubseteq b$ iff $a \vee b = b$ (věta 4.1.11 z přednášky 10 od Demlové [1]). Pokud obě strany rozšířím o $(\wedge \bar{b})$, pak upraveně dostanu

$$(a \vee b) \wedge \bar{b} = b \wedge \bar{b} = 0.$$

To můžu dál rozvíjet:

$$0 = b \wedge \bar{b} = (a \vee b) \wedge \bar{b} = (a \wedge \bar{b}) \vee \underbrace{(b \wedge \bar{b})}_{0} = (a \wedge \bar{b}) \vee 0 = a \wedge \bar{b}$$

Neboli jsem dokázal, že $a \vee b = b$ je totéž, co $a \wedge \bar{b} = 0$.

$\Leftarrow$ Tady si za základ položím, že $a \wedge \bar{b} = 0$ a snažím se z toho dokázat, že nutně $a \sqsubseteq b$. K tomu mi stačí dokázat, že $a \wedge b = a$ (z $a \sqsubseteq b$ iff $a \wedge b = a$). Označím si levou stranu rovnice jako $L = a \wedge b$ a pravou jako $P = a$ a jedu:

$$P = a = a \wedge 1 = a \wedge (b \vee \bar{b}) = (a \wedge \bar{b}) = \underbrace{(a \wedge \bar{b})}_{a \wedge \bar{b} = 0} \vee (a \wedge b) = 0 \vee (a \wedge b) = a \wedge b = L$$

□

5.8 Příklad 8

Ukažte, že v distributivním svazu může mít daný prvek nejvýše jeden doplněk.

Důkaz. Předpokládám, že b a c jsou doplňky a. Pak $b = \underbrace{b \wedge \underline{1}}_{a \wedge \underline{1} = a} = b \wedge (\underbrace{a \vee c}_{a \vee \bar{a} = \underline{1}}) = \underbrace{(b \wedge a) \vee (b \wedge c)}_{\text{distributivita}} = b \vee (\underbrace{a \wedge b}_{a \wedge \bar{a} = \underline{1}}) \vee c =$ $(b \wedge \underline{1}) \wedge c = b \wedge c$. Tudíž $b \sqsupseteq c$, a obdobně, pokud bych začal s c, bych dostal $b \sqsubseteq c$, a tedy $b = c$ (podle antisymetrie). □

Reference

[1] *Marie Demlová:* **Algebra pro VT.**
http://math.feld.cvut.cz/demlova/teaching/avt/predn-avt.html

[2] *Alena Gollová:* **Algebra pro výpočetní techniku.**
http://math.feld.cvut.cz/gollova/algebra_pro_vt.html

[3] *Jiří Velebil:* **Diskrétní matematika.**
http://math.feld.cvut.cz/velebil/teaching/y01dma.html