Algebra - zpracované otázky ke zkoušce

Karel Velička

16. ledna 2024

Doc. Mgr. et Mgr. Jan Žemlička Ph.D.

Obsah

1 Teorie čísel

1.1 Modulární aritmetika

1.1.1 Zformulujte a dokažte Základní větu aritmetiky.

Věta 1. *(Základní věta aritmetiky):* $\forall a \in \mathbb{N}$, kde $a \neq 1$, existují po dvou různá prvočísla $p_1, \ldots, p_n$ a $k_1, \ldots, k_n \in \mathbb{N}$ splňující:

$$a = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$

Důkaz: Dokážeme zvášť existenci a jednoznačnost:

(i) Existence: Nechť $a \in \mathbb{N}$ je nejmenší číslo, pro nějž neexistuje prvočíselný rozklad. To nemůže být prvočíslem, jinak bychom měli rozklad $a = a^1$, takže a je složené a můžeme ho pro nějaká $1 < b, c < a$ rozložit na $a = b \cdot c$. Podle indukčního předpokladu ale existuje prvočíselný rozklad jak pro b, tak pro c a jejich složením získáme rozklad a.

(ii) Jednoznačnost: Nechť $a \in \mathbb{N}$ je nejmenší číslo s nejednoznačným prvočíselným rozkladem. A nechť máme dva různé rozklady a:

$$a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}.$$

Jelikož $p_1 \mid a = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$, musí existovat i takové, že $p_1 \mid q_i$.

Protože je ale q_i prvočíslo, musí tak platit $p_1 = q_i$.

Nyní uvažme číslo $b = \frac{a}{p_1}$ opět s dvěma různými rozklady:

$$b = p_1^{k_1 - 1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_i^{l_i - 1} \cdot \ldots \cdot q_n^{l_n}.$$

Tím bychom ale dostali, že $b < a$, což je spor s minimalitou.

□

1.1.2 Co jsou Bézoutovy koeficienty? Napište Eukleidův algoritmus pro gcd a vysvětlete jak spočítat Bézoutovy koeficienty

Definice 1. *(Bézoutovy koeficienty u, v):* Pro každou dvojici čísel $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ splňující:

$$\gcd(a, b) = u \cdot a + v \cdot b.$$

Algoritmus 1. *(Eukleidův):*
`VSTUP`: $a, b \in \mathbb{N}, a \geq b$
`VÝSTUP`: $\gcd(a, b) \in \mathbb{Z}$ a Bézoutovy koeficienty $u, v \in \mathbb{Z}$

1. $i := 0, \quad (a_0, a_1) := (a, b); \quad (u_0, u_1) = (1, 0); \quad (v_0, v_1) = (0, 1)$
2. `while` $a_i > 0$ `do` {
3. $\quad a_{i+1} := a_{i-1} \mod a_i; \quad q_i := \frac{a_{i-1}}{a_i}; \quad u_{i+1} := u_{i-1} - u_i \cdot q_i; v_{i+1} := v_{i-1} - v_i \cdot q_i; \quad i := i + 1$
4. }
5. `return` $a_{i-1}, u_{i-1}, v_{i-1}$

1.1.3 Co je to konkgruence? Definujte Eulerovu funkci. Zformulujte a dokažte Eulerovu větu

Definice 2. *(Konkgruence):* Nechť $a, b, m \in \mathbb{Z}$ a $m \neq 0$, potom a je kongruentní s b modulo m, tedy

$$a \equiv b \pmod{m}, \quad \text{pokud } m \mid a - b.$$

Definice 3. *(Eulerova funkce):* Zobrazení $\varphi : \mathbb{N} \to \mathbb{N}$ značí pro $n \in \mathbb{N}$ počet čísel $k \in \{1, \ldots, n-1\}$ nesoudělných s číslem n. Tedy jinak $\varphi(n) = |\{k \in \{1, \ldots, n-1\} \mid \gcd(k, n) = 1\}|$.

Věta 2. *(Eulerova):* Nechť $\forall a, m \in \mathbb{N} : \gcd(a,m) = 1$, potom $a^{\varphi(m)} \equiv 1 \mod m$.

Lemma 1. Nechť $a, x, m \in \mathbb{N}$ a $\gcd(a,m) = 1 = \gcd(x,m) \iff \gcd(ax,m) = 1$, potom zobrazení

$$f_a : \Phi_m \to \Phi_m \quad \text{je bijekce a platí} \quad f_a(x) = ax \mod m.$$

Důkaz: Nejprve dokážeme platnost ekvivalence $\gcd(a,m) = 1 = \gcd(x,m) \iff \gcd(ax,m) = 1$:

$\implies$ Kdyby $\gcd(ax,m) \neq 1$, tak by podle Euklidova algoritmu $\exists p : p \mid ax, m$. Díky ZVA víme, že pokud $\exists p : p \mid ax, m$, pak $p \mid a \ \vee \ p \mid x$, což je spor s nesoudělností, protože by pak $\gcd(x,m) \neq 1$.

$\impliedby$ Kdyby $\gcd(a,m) \neq 1$ nebo $\gcd(x,m) \neq 1$, tak $\exists p : p \mid a$ nebo $p \mid x \implies p \mid ax, m \implies \gcd(ax,m) \neq 1$

Dále dokážeme, že zobrazení f_a je bijektivní.
Nejdříve nechť $x, y \in \Phi_m : f_a(x) = f_a(y)$, neboli $ax \equiv ay \mod m$. A protože $\gcd(a,m) = 1$, uvažme

$$x \equiv y \mod m \quad \implies \quad x < m \ \wedge \ y < m \implies x = y \implies f_a \textit{ je injektivní.}$$

A protože množiny jsou stejně velké a platí injektivita, dostaneme i potřebnou *surjektivitu* $\implies$ *bijekce* f_a. □

Důkaz:

$$\prod_{b \in \Phi_m} b \overset{\text{Lemma}}{\equiv} \prod_{b \in \Phi_m} f_a(b) = \prod_{b \in \Phi_m} ab \mod m \equiv \prod_{b \in \Phi_m} ab = a^{\varphi(m)} \cdot \prod_{b \in \Phi_m} b \mod m.$$

Rovnici můžeme přepsat jen jako $\prod_{b \in \Phi_m} b \equiv a^{\varphi(m)} \cdot \prod_{b \in \Phi_m} b \mod m$. A protože $\gcd\left(\prod_{b \in \Phi_m} b,\ m\right) = 1$, dostáváme potřebné:

$$1 \equiv a^{\varphi(m)} \mod m.$$

□

1.1.4 Zformulujte a dokažte Čínskou větu o zbytku.

Věta 3. *(Čínská o zbytcích):* Nechť $m_1, \dots, m_n \in \mathbb{N}$ jsou po dvou nesoudělná čísla, označme $M := \prod_{i=1}^{n} m_i$. Dále nechť $u_1, \dots, u_n \in \mathbb{Z}$. Potom $\exists! x \in \mathbb{Z}_m$ takové, že řeší soustavu $\forall i \in \{1, \dots, n-1\} : x \equiv u_i \mod m_i$.

Důkaz: Nejprve ukážeme jednoznačnost.
Pro spor předpokládejme, že má soustava dvě řešení $x, y \in \{0, \dots, n-1\}$, tedy platí:

$$\forall i : x \equiv y \equiv u_i \pmod{m_i} \implies m_i \mid x - y$$

a protože všechna m_i jsou navzájem nesoudělná, tak dostáváme $M = \prod_{i=1}^{n} \mid x - y$. Ovšem obě čísla x, y, a tedy i jejich rozdíl, jsou menší než M, takže nutně $x - y = 0 \implies x = y$.

Nyní ukážeme existenci. Uvažme zobrazení

$$f : \{0, \dots, n-1\} \to \{0, \dots, m_1 - 1\} \times \dots \times \{0, \dots, m_n - 1\}$$
$$x \to (x \mod m_1, \dots, x \mod m_n).$$

Ukázali jsme tak, že f je prostá. Přitom definiční obor i obor hodnot této funkce mají stejnou velikost M (velikost kartézského součinu je součin velikostí činitelů):

$$M = |\mathbb{Z}_m| = \left| \prod_{i=1}^{n} \mathbb{Z}_{m_i} \right| = \prod_{i=1}^{n} |\mathbb{Z}_{m_i}|$$

Takže zobrazení f musí být i na a je proto f bijekce, neboli $\forall i : x \equiv u_i \mod m_i \iff f(x) = u_1, \dots, u_n$.
Tedy $\exists! x$ ke každé n-tici $(u_1, \dots, u_n)$, které se na něj zobrazuje, a to je hledaným řešením soustavy. □

1.1.5 Popište jak spočítat hodnotu Eulerovy funke když známe faktorizaci prvočísla. Dokažte to.

Tvrzení 1. Nechť p je prvočíslo, kde $p_1 < \cdots < p_n$ a $k_1, \ldots, k_n \in \mathbb{N}$, potom $\varphi\left(\prod_i^n p_i^{k_i}\right) = \prod_i^n (p_i - 1)p_i^{k_i - 1}$.

Důkaz: Nechť $m_i = p_i^{k_i}$, použijeme zobrazení $f : \mathbb{Z}_n \to \prod \mathbb{Z}_{m_i}$ z Čínské věty o zbytku.

$$\begin{aligned} f(\Phi_m) = \overbrace{\prod_i \Phi_{m_i} \subseteq \prod \mathbb{Z}_{m_i}}^{\textit{Kartézský součin}}, \text{ proto : } \quad a \in \Phi_m &\iff \gcd(a, m) = 1 \\ &\overset{\text{Lemma}}{\iff} \gcd(a \mod m_i,\ m_i) = \gcd(a, m_i) = 1 \\ &\iff \forall i : a \mod m_i \in \Phi_{m_i} \\ &\iff f(a) \in \prod_{i=1}^n \Phi_{m_i}. \end{aligned}$$

Dostáváme tak $\varphi(m) = |\Phi_m| = |f(\Phi_m)| = \underbrace{\prod_{i=1}^n |\Phi_{m_i}|}_{= \textit{příklad } (p_i - 1)p_i^{k_i - 1}}$. □

2 Polynomy

2.1 Tělesa, okruhy, obory

2.1.1 Co je to obor integrity? Napiště alespoň dva příklady, kdy obor není těleso.

Definice 4. *(Ring/ okruh):* Pětice $\mathcal{R} = (R, +, -, \cdot, 0)$ se nazývá okruh, pokud R je množina s binárními operacemi $+, \cdot : R \times R \to R$, unární operací $- : R \to R$, prvkem $0 \in R$ a operacemi $\forall a, b, c \in R$:

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a, \qquad a + 0 = 0,$$
$$a + (-a) = 0, \qquad a \cdot 1 = 1 \cdot a = a \quad \textit{(okruh s jednotkou } 1 \in R\textit{)}$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \& \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Definice 5. *(Komutativní okruh $\mathcal{R}$):* $\equiv$ pokud je komutativní také operace násobení, tedy $\forall a, b \in R : a \cdot b = b \cdot a$.

Definice 6. *(Obor integrity):* $\equiv$ komutativní okruh s jendnotkou, pokud platí: $\forall a, b \in R \setminus \{0\} : \; a \cdot b \neq 0$.

Příklad 1. Příklady, kdy obor není tělesem.

(i) Obor celých čísel $\mathbb{Z}$ není těleso *(nemá inverzní prvek)*

(ii) Matice s nulovým determinantem, tedy pro těleso $\mathbb{F}$ a $M_n(\mathbb{F}) = \{$čtvercová matice $n \times n$ nad $\mathbb{F}\}$ definujeme $\left(M_n(\mathbb{F}), +, -, \circ, \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \right)$ je okruh s jednotkou I_n. Není ale tělesem *(nemá multiplikativní inverz)*.

(iii) Boolovský okruh $(\mathbb{Z}_2, \oplus, \wedge, 0, 1)$ není tělesem *(nemá aditivní inverz)*.

2.1.2 Pro která přirozená čísla je okruh 'Zn' oborem? Zdůvodněte svou odpověď.

Lemma 2. *Pro $\forall n > 1 \in \mathbb{N}$, je komutativní okruh $\mathbb{Z}_n = (\mathbb{Z}_n, +, -, \cdot, 0)$ s jednotkou 1 okruh $\iff$ n je prvočíslo.*

Důkaz: Z následující věty víme, že každé těleso je obor, dokážeme tedy, že $\mathbb{Z}_n$ je obor $\iff$ n je prvočíslo.
Kdyby $n = k \cdot l$ bylo složené číslo, kde $k, l > 1$, tak by v $\mathbb{Z}_n$ platilo $k \cdot l = n \pmod n = 0 \implies$ není obor.
A je-li n prvočíslo, pak je $a^{n-2} \pmod n$ inverzním prvkem pro $a \neq 0$, což plyne z malé Fermatovy věty. □

2.1.3 Popiště nosnou množinu a operace podílového tělesa oboru. Co je podílové těleso celých čísel? Co je podílové těleso tělesa R?

Definice 7. *(Podílové těleso):* Definujme nejprve relaci $\sim$ vztahem $(a, b) \sim (c, d) \iff ad = bc$ na množině $R \times M$, kde $M = R \setminus \{0\}$. Jedná se o relaci ekvivalence. Struktura $\mathcal{Q} = (Q, +, -, \cdot, 0)$ je tzv. *podílové těleso* oboru $\mathcal{R}$, kde Q je nosná množina všech zlomků $Q = \{\frac{a}{b} \mid (a, b) \in R \times M\}$, pro kterou platí operace:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}; \qquad -\frac{a}{b} = \frac{-a}{b}; \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad 0 = \frac{0}{1}, \qquad 1 = \frac{1}{1}.$$

Nejedná se konkrétně o dvojice (a, b), ale o třídy ekvivalence $\frac{a}{b} = [(a, b)]_\sim$. *(Aby platilo $\frac{a}{b} = \frac{ax}{bx}$).*

Příklad 2. *(Podílové těleso $\mathbb{Z}$):* $\{\frac{a}{b} \mid (a, b) \in \mathbb{Z}\}$ je těleso racionálních čísel $\mathbb{Q}$.

Příklad 3. *(Podílové těleso tělesa):* je opět původní těleso $\{\frac{a}{b} \mid (a, b) \in R \times M\}$.

2.1.4 Popiště nosnou množinu a operace komutativního okruhu R[x] nad okruhem R.

Definice 8. *(Komutativní okruh):* $\mathcal{R}$ je *komutativní okruh*, pokud je komutativní také operace násobení, tedy

$$\forall a, b \in R : a \cdot b = b \cdot a.$$

Definice 9. *(Polynom proměnné x):* nad komutativním okruhem $\mathcal{R}$ rozumíme výraz

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

kde $a_0, \ldots, a_n \in R$, $a_n \neq 0$.
Nosná množina všech polynomů na komutativním okruhu $R[x]$ je definována předpisy:

$$\sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i, \qquad -\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} (-a_i) x^i,$$

$$\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n} \left(\sum_{j+k=i} a_j b_k\right) x^i$$

2.1.5 Dokažte, že komutativní okruh R[x] nad oborem R je obor. Existuje těleso F takové, že F[x] je těleso?

Věta 4. Nechť $\mathcal{R} = (R[x], +, -, \cdot, 0)$ je komutativní okruh s jednotkou, potom

(i) $\mathcal{R}[x]$ je komutativní okruh,

(ii) pokud $\mathcal{R}$ je obor, potom $\mathcal{R}[x]$ je také obor a platí $\forall f, g \in R[x] \setminus \{0\}: \quad \deg(fg) = \deg(f) + \deg(g)$.

Důkaz: Označme $f = \sum_{i=0}^{m} a_i x^i,\ g = \sum_{i=0}^{n} b_i x^i,\ h = \sum_{i=0}^{p} c_i x^i$.

(i) Dokážeme postupně všechny axiomy.

- Sčítání triviálně. Sčítají se nezávisle koeficienty u jednotlivých mocnin, čili rovnosti pro polynomy ihned plynou z rovností v $\mathcal{R}$.
- Komutativita násobení plyne z toho, že vzorec je symetrický vzhledem k prohození písmen a a b.
- Jednotka z definice součinu: $f \cdot 1 = \left(\sum_{i=0}^{n} a_i x^i\right) \cdot (1 + 0 + 0 + \ldots) = \sum_{i=0}^{n} \left(\sum_{j+k=i} a_j b_k\right) x^i$
- Asociativita násobení: z jedné strany, $f \cdot (g \cdot h)$ je rovno:

$$\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\left(\sum_{i=0}^{n} b_i x^i\right) \cdot \left(\sum_{i=0}^{p} c_i x^i\right)\right) = \left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{i=0}^{n+p} \left(\sum_{k+l=i} b_k c_l\right) x^i\right)$$
$$= \sum_{i=0}^{m+n+p} \left(\sum_{j+k+l=i} a_j b_k c_l\right) x^i$$

- Distributivita analogicky

(ii) $\deg(fg)$, kde $f, g \geq 0 \implies \deg f \geq 0 \wedge \deg g \geq 0$ a zároveň $\deg(f) = m$ a $\deg(g) = n$.

Proto koeficient $f \cdot g : a_0 b_k + a_1 b_{k-1} + \cdots = \overbrace{a_0 \cdot 0 + \cdots + a_n \cdot 0}^{=0} + \overset{\neq 0}{a_m} \overset{\neq 0}{b_n} + \overbrace{a_{m-1} b_{n-1}}^{=0} = a_m b_n \neq 0.$

Vedoucím koeficientem $f \cdot g$ je $a_m b_n$, který je nenulový díky tomu, že $\mathcal{R}$ je obor

□

Těleso F takové, že $F[x]$ je tělesem neexistuje, protože nesplňuje existenci inverzního prvku vzhledem k násobení. Předpokládejme pro spor, že existuje. Vezměme $x \in F[x]$, kde zřejmě $x \neq 0$ (protože předpokládáme polynom). Pokud ale vynásobíme x jakýmkoliv polynomem$\neq 0$, tak výsledek bude vždy obsahovat x a jeho vyší mocniny, takže nemá inverz. □

2.1.6 Co je to kořen polynomu? Zformulujte a dokažte předpoklady o počtu kořenů polynomu nad oborem.

Definice 10. *(Kořen polynomu):* Nechť $R \leq S$ jsou obory, $f \in R[x]$ a $a \in S$. Řekneme, že a je kořen polynomu f, pokud $f(a) = 0$.

Věta 5. *(Počet kořenů):* Nechť $\mathcal{R}$ je obor, $f \in R[x]$, kde $\deg f = n \geq 0$, potom f má nejvýše n kořenů v $\mathcal{R}$.

Důkaz: (Indukcí podle n).

(i) Pro $n = 0 : f \in R \setminus \{0\}$, je nenulový konstantní polynom, nemá kořeny, tedy $\forall \alpha \in R : f(\alpha) \neq f \neq 0$

(ii) Pokud $\deg f = n + 1$, pak buď polynom f nemá žádný kořen, v tom případě tvrzení platí a nebo $\exists \alpha$ kořen:

$$\exists \alpha \in R : f(\alpha) = 0 \implies \exists g \in R[x] : f = (x - \alpha) \cdot g \implies \deg g = n$$

Pokud existuje nějaký druhý kořen $\beta \neq \alpha$, tak platí:

$$\exists \beta \in R : f(\beta) = 0 \implies 0 = f(\beta) = \underbrace{(\beta - \alpha)}_{0} \cdot g(\beta) \overset{\textit{je obor}}{\implies} \alpha = \beta \quad \vee \quad g(\beta) = 0$$

A protože má g nejvýše n polynomů, tak má f nejvýše $n + 1$ kořenů.

□

2.2 Dělitelnost, UFD

2.2.1 Definujte prvočíslo a ireducibilní prvek. Je každý prvek ireducibilní? Je každý ireducibilní prvek prvočíslo?

Definice 11. *(Prvočíslo):* Nechť $a, b, c \in R$, potom a je *prvočíslo*, pokud:

$$\forall b, c : \ a \mid b \cdot c \implies a \mid b \quad \vee \quad a \mid c \quad \& \quad a \notin R^* \cup \{0\}.$$

Definice 12. *(Triviální dělitel):* Nechť $a, b \in R$, potom a je *triviální dělitel* b, pokud $a \mid\mid b$ nebo $a \mid\mid 1$.

Definice 13. *(Ireducibilní prvek a):* Prvek $0 \neq a \in R$ je *ireducibilní*, pokud $a \not\parallel 1$ a a nemá triviální dělitele. Jinými slovy, pokud pro každý rozklad $a = bc$ platí $b \mid\mid 1$ nebo $c \mid\mid 1$.

Pozorování 1. *Všechna prvočísla jsou ireducibilní.*

Důkaz: Nechť rozklad $a = bc$ je prvočíselný prvek. Z toho můžeme odvodit, že $a \mid bc$, tedy $a \mid b$ nebo $a \mid c$, z čehož plyne $a \mid\mid b$ nebo $a \mid\mid c$, čili jde o triviální rozklad.

Opačná implikace obecně neplatí (jen pro některé obory, např. pro $\mathbb{Z}$, pro UFD). Konkrétně pro obor $\mathbb{Z}[\sqrt{5}]$ je prvek 2 ireducibilní, protože $2 \mid (\sqrt{5} - 1)(\sqrt{5} + 1)$, ale není prvočíslem, protože $2 \nmid (\sqrt{5} + 1)$ ani $2 \nmid (\sqrt{5} - 1)$. □

2.2.2 Co znamená, že dva prvky oboru jsou asociované? Popište tuto relaci na oboru pomocí inverzních prvků.

Definice 14. *(Asociovanost):* Nechť $a, b \in R$, kde R je obor. Potom a a b jsou navzájem *asociované*, tedy $a \mid\mid b$, pokud $a \mid b$ a $b \mid a$. Zároveň platí, že prvek a je invertibilní $\iff a \mid\mid 1$ a prvek b splňující $ab = 1$ značíme a^{-1}.

Pozorování 2. *Relace dělitelnosti je reflexivní i tranzitivní.* Pokud $a \mid b$ a $b \mid c$, tedy pokud $b = ax$ a $c = by$ pro nějaká x, y, pak $c = axy$, tedy $a \mid c$. Z toho ihned plyne, že relace $\mid\mid$ je ekvivalencí.

Tvrzení 2. *(Asociovanost vs. invertibilní prvky):* Nechť R je obor a $a, b \in R$. Pak $a \mid\mid b \iff$ existuje invertibilní prvek $q \in R$ takový, že $a = bq$.

Důkaz: Dokazujeme dvě implikace.

$\Longleftarrow$ Protože $a = bq$, tak platí $b \mid a$. Protože $b = aq^{-1}$, tak platí i $a \mid b$.

$\Longrightarrow$ Pokud $a = 0$, pak i $b = 0$ a tvrzení platí. Uvažujme proto, že $a \neq 0$. Protože $b \mid a$, tak $a = bu$, a protože $a \mid b$, tak $b = av$ pro nějaká u, v. Tedy $a = bu = avu$ a krácením dostáváme $uv = 1$, čili $u, v \mid\mid 1$.

□

2.2.3 Definujte největší společný dělitel dvou prvků na oboru. Co je gcd(a, 1) a gcd(a, 0) pro prvek na nějakém oboru?

Definice 15. *(Největší společný dělitel):* Nechť $a, b, c, d \in R$, potom c je $\gcd(a, b)$, pokud :

$$c \mid a \ \wedge \ c \mid b \quad \text{a} \quad d \mid a \ \wedge \ d \mid b \implies d \mid c.$$

Pro $\forall a \in R:\ \gcd(a, 1) = 1 \implies$ pouze $1 \mid a \wedge 1 \mid 1$. Pro $\forall a \in R:\ \gcd(a, 0) = \gcd(0, a) = |a| \implies$ pouze $a \mid a$.

2.2.4 Definujte ireducibilní rozklad. Definujte Gaussův obor (UFD). Dokažte, že existuje gcd(a, b) pro každou dvojici prvků a,b z UFD.

Definice 16. *(Ireducibilní rozklad):* prvku a je zápis $a \mid\mid p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, kde $p_1, \ldots, p_n$ jsou ireducibilní prvky, $p_i \not\parallel p_j$ pro $i \neq j$ a $k_1, \ldots, k_n \in \mathbb{N}$.

Definice 17. *(Gaussův obor (UFD)):* Obor R je UFD, pokud má každý nenulový neinvertibilní prvek unikátní rozklad na ireducibilní činitele.

Důsledek 1. *Nechť R je UFD, potom $\forall a, b \in R$ existuje* $\gcd(a, b)$.

Důkaz: Uvažujme ireducibilní prvky $p_1, \ldots, p_n$, $p_i \not\parallel p_j$, pro $i \neq j$, a $k_i, l_i \geq 0$ takové, že:

$$a \mid\mid p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}, \quad b \mid\mid p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$$

(Libovolné ireducibilní rozklady prvků a, b můžeme přepsat do této formy tak, že ze dvou asociovaných činitelů vybereme jeden a do rozkladu případně doplníme činitele v nulté mocnině.)
Nyní $c \mid a, b \iff c \mid\mid p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$, kde $0 \leq m_i \leq k_i$ a $0 \leq m_i \leq l_i$, čili $\iff 0 \leq m_i \leq \min(k_i, l_i)$, pro všechna i. Největším z těchto společných dělitelů tedy bude ten, kde $m_i = \min(k_i, l_i)$. □

2.2.5 Formulujte charakteristiku (nutnou a postačující podmínku) UFD za pomoci gcd a řetězce dělitelů. Dokažte to.

Věta 6. *(Zobecněná základní věta aritmetiky):*Nechť $\mathcal{R}$ je obor, potom $\mathcal{R}$ je UFD právě tehdy, když:

(i) existuje gcd všech dvojic prvků

(ii) neexistuje poslopunost $a_1, a_2, a_3, \dots \in R$ taková, že $a_{i+1} \mid a_i$ a $a_{i+1} \not\parallel a_i$.

Důkaz: Budeme dokazovat dvě implikace.

$\implies$ Dokázali jsme v Důsledku 5.3.

$\impliedby$ Nejprve dokážeme *existenci* rozkladů:

Pro spor uvažujme prvek a, který nemá ireducibilní rozklad, $0 \neq a \not\parallel 1$. Rekurzí zkonstruujeme spornou posloupnost s bodem (ii).

- Nechť $a_1 = 1$. Tedy $a_1 \not\parallel 1$ a nemá ireducibilní rozklad.
- Předpokládejme, že $a_i \not\parallel 1$ a nemá ireducibilní rozklad. Speciálně, prvek a_i není sám ireducibilní, a tedy $a_i = b \cdot c$ pro nějaká $b, c \not\parallel 1$. Kdyby b i c měly ireducibilní rozklad, pak by ho měl i a_i, takže aspoň jedno z nich ireducibilní rozklad nemá, označme jej a_{i+1}. Je tedy vlastní dělitel a_i a nemá ireducibilní rozklad. Tato posloupnost $a_1, a_2, \ldots$ je ve sporu s (ii)

Nyní dokážeme *jednoznačnost*: (Ve skriptech je, že se na to u zkoušky nebude ptát, takže nezbývá než doufat)

□

2.3 GCD a Modulo polynom

2.3.1 Definujte Eukleidovskou normu a obor. Napište dva příklady Eukleidovského oboru, které nejsou tělesa.

Definice 18. *(Eukleidovská norma):* je zobrazení $\mathcal{V} : R \to \mathbb{N}_0$ takové, že

(i) $\mathcal{V}(0) = 0$,

(ii) pokud $\forall a, b \in R,\ a \mid b \neq 0$, pak $\mathcal{V}(a) \leq \mathcal{V}(b)$,

(iii) $\forall a, b \in R,\ b \neq 0,\ \exists q, r \in R$ taková, že $\quad a = bq + r \quad$ a $\quad \mathcal{V}(r) < \mathcal{V}(b)$.

Definice 19. *(Eukleidovský obor):* Obor $\mathcal{R}$ se nazývá eukleidovský, pokud na něm existuje eukleidovská norma

Příklad 4. *(Eukleidovského oboru, které nená těleso)*

- Obor $\mathbb{Z}[x]$ není eukleidovský pro libovolné těleso $\mathbb{Z}$, protože nemá Eukleidovskou normu:

  Jeho normou je $\mathcal{V}(f) = 1 + \deg f$. Pro například polynomy $3x$ a $2x$ máme $3x = q \cdot 2x + r$ a $\deg r = 0 \implies r = 0 \implies 3x = 2qx \notin \mathbb{Z}[x]$.

- Obor $\mathbb{Z}[i]$ není eukleidovský. Jeho norma je $\mathcal{V}(a + bi) = a^2 + b^2$

2.3.2 Co znamená primitivní polynom? Zformulujte Gaussovo lemma a Gaussovu větu. Pokud R je UFD s podílovým tělesem Q, vysvětlete jak spočítat gcd v R[x] pomocí gcd v Q[x] a v R

Definice 20. *(Primitivní polynom f):* $\equiv$ jeho koeficienty jsou nesoudělné. *(c dělí všechny koeficienty $\implies c \mid\mid 1$).*

Lemma 3. *(Gaussovo):* Nechť $\mathcal{R}$ je UFD a f, g primitivní polynomy z $\mathcal{R}[x]$. Potom fg je také primitivní polynom.

Věta 7. *(Gaussova):* Pokud $\mathcal{R}$ je UFD, pak $\mathcal{R}[x]$ je také UFD.

Věta 8. (gcd *a UFD vs. podílové těleso)* Nechť $\mathcal{R}$ je UFD, $\mathcal{Q}$ jeho podílové těleso a f, g polynomy z $\mathbb{R}[x]$. Potom

(1) existuje $\gcd_{R[x]}(f, g) = c \cdot h$, kde $c = \gcd_{\mathcal{R}}(c_f, c_g)$ a kde $h = \gcd_{Q[x]}(\frac{f}{c_f}, \frac{g}{c_g})$ je primitivní polynom z $R[x]$. GCD koeficientů polynomu f značíme c_f a GCD koeficientů polynomu g značíme c_g.

(2) f je ireducibilní v $R[x] \iff \begin{cases} \deg f = 0 & f \text{ je ireducibilní v } \mathcal{R}, \\ \deg f > 0 & f \text{ je primitivní a ireducibilní v } Q[x]. \end{cases}$

Příklad 5. *Pro obor $\mathbb{Z}[x]$ a polynomy $f = 4x^2 + 8x + 4$ a $g = -6x^2 + 6$ počítáme:*
$c = \gcd_{\mathbb{Z}}(4, 6) = 2, \quad h = \gcd_{\mathbb{Q}[x]}(x^2 + 2x + 1, x^2 - 1) = x + 1$. A celkem tak máme $\gcd_{R[x]}(f, g) = 2 \cdot (x + 1)$

2.3.3 Napište zobecněný Eukleidův algoritmus pro Eukleidovský obor a Eukleidovskou normu

Algoritmus 2. *(Zobecněný Eukleidův):* Nechť $\mathcal{R}$ je eukleidovský obor:
`VSTUP:` $a, b \in R, \mathcal{V}(a) \geq \mathcal{V}(b)$
`VÝSTUP:` $\gcd(a, b) \in R$ a Bézoutovy koeficienty $u, v \in R$

1. $(a_0, a_1) := (a, b); \quad (u_0, u_1) = (1, 0); \quad (v_0, v_1) = (0, 1)$
2. `for` $i = 2, 3, \ldots$ `do` :
3. zvol q, r tak, aby $a_{i-1} = a_i q + r$ a $\mathcal{V}(r) < \mathcal{V}(a_i)$
4. definuj $a_{i+1} = r; \quad u_{i+1} := u_{i-1} - u_i q; \quad v_{i+1} := v_{i-1} - v_i q; \quad i := i + 1$
5. `if` $a_{i+1} = 0$:
6. `return` a_i, u_i, v_i

2.3.4 Dokažte, že každý Eukleidovský obor je UFD.

Věta 9. *Eukleidovské obory jsou UFD.*

Důkaz: Použijeme zobecněnou základní větu aritmetiky a ověříme body (1) a (2).

(1) $\forall a, b \in R : \exists \gcd(a, b) \in R$

(2) Za pomoci následujícího lemma. Taková posloupnost by totiž měla ostře klesající normu, což nelze.

Lemma 4. *Nechť $\mathcal{R}$ je Eukleidovský obor, $a, b \in R$, kde $a, b \neq 0$ a $\mathcal{V}$ je Eukleidovská norma. Potom:*

$$a \mid b \wedge a \not| \; b \implies \mathcal{V}(a) < \mathcal{V}(b).$$

Důkaz: Nechť $b = au$ pro nějaké $u \in R$ a nechť $a = bq + r$ pro nějaká $q, r \in R$, kde $\mathcal{V}(r) < \mathcal{V}(b)$.

Vzhledem k tomu, že $b \nmid a$, tak platí $r \neq 0$. Dosazením dostanem $r = a - bq = a - auq = a(1 - uq)$, z čehož plyne, že $a \mid r$.

A protože $r \neq 0$, tak dostáváme $\mathcal{V}(a) \leq \mathcal{V}(r) < \mathcal{V}(b)$. □

□

2.3.5 Zformulujte a dokažte Gaussovu větu.

Věta 10. *(Gaussova):* Pokud $\mathcal{R}$ je UFD, pak $\mathcal{R}[x]$ je také UFD.

Důkaz: Použijeme *"Zobecněnou základní větu aritmetiky"* a dokážeme oba body.

(1) $\forall a, b \in \mathcal{R}[x] : \; \exists \gcd(a, b)$. Platnost vychází z věty "gcd *a UFD vs. podílové těleso"*.

(2) Předpokládejme nekonečnou posloupnost vlastních dělitelů $\{a_i\}_{i \geq 1} \in \mathcal{R}[x] \setminus \{0\}$, tedy t.ž: $a_{i+1} \mid a_i$.
Potom $\forall i : -1 < \deg(a_{i+1}) \leq \deg(a_i)$ a musí tak $\exists n$ takové, že $\forall i > n$:

$$\deg(a_i) = \deg(a_n), \quad \text{tedy} \quad \deg(a_n) = \deg(a_{n+1}) = \dots.$$

Nakonec pokud si zadefinujeme u_i jakožto vedoucí koeficient a_i, tak $u_n, u_{n+1}, u_{n+2}, \dots$ tvoří nekonečnou posloupnost vlastních dělitelů v $\mathcal{R}$, což je spor.

□

2.3.6 Popište konstrukci faktorokruhu F[a]/m(a) modulo polynom m(a) nad tělesem F. Zformulujte a dokažte charakteristiku těchto polynomů m(a) tak, že faktor je těleso.

Definice 21. *(Faktorokruh):* Nechť $\mathbb{F}$ je těleso a nechť máme polynom $m \in F[\alpha]$, stupně $n = \deg(m) \geq 1$. Potom *Faktorokruh* $\mathbb{F}[\alpha]/(m)$ je množina všech polynomů stupně $< n$ se standardními oparacemi sčítání, odčítání a opercací násobení modulo m. Tedy:

$$\mathbb{F}[\alpha]/(m) = (\{f \in F[\alpha] \mid \deg(f) < n\}, +, -, \odot, 0, 1),$$

kde $f \odot g = f \cdot g \mod m$.

Platnost definice Je třeba dokázat, že se jedná o komutativní okruh. Axiomy pro $+, -$ jsou totožné s $\mathbb{F}[x]$, dokážeme proto jen axiomy s $\odot$.
Připomeňme si, že $f \equiv g \pmod{m} \iff f \mod m = g \mod m$ a že tak $f \equiv f \pmod{m \pmod{m}}$. Konkrétně využijeme vztahu $(f \cdot g \mod m) \cdot h \mod m = f \cdot (g \cdot h \mod m) \mod m$ a dokážeme za pomoci něj asociativitu:

$$\forall a, b, c \in F[\alpha]/(m) : \quad a \odot (b \odot c) \equiv a \odot (b \cdot c) \equiv a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \equiv (a \odot b) \odot c \pmod{m}$$

2.3.7 Pro prvočíslo p, přirozené k a ireducibilní celočíselný polynom m stupně k popište konstrukci konečného tělesa s p na n prvky. Jak můžeme počítat inverz prvků v tomto tělese?

Tvrzení 3. Nechť p je prvočíslo a $\mathbb{F}$ je konečné těleso, potom:

(1) pokud p je charakteristikou $\mathbb{F}$, pak $\exists k \in \mathbb{N} : |F| = p^k$

(2) pokud $k \in \mathbb{N}$ a $\mathbb{F}$ je rozkladové nadtěleso $x^{p^k} - x \in \mathbb{Z}_p[x]$, pak $|F| = p^k$

(3) $\forall k \in \mathbb{N}, \exists m \in \mathbb{Z}_p[x]$, kde m je ireducibilní se stupněm $\deg(m) = k$, pak $\mathbb{Z}_p[\alpha]/m(\alpha)$ je těleso p^k prvků.

Důkaz: (1): $\mathbb{F}$ je vektorový prostor nad $\mathbb{Z}_p$, takže $k = \dim_{\mathbb{Z}_p} \mathbb{F} \implies |F| = p^k$. □

Inverz $a^{-1}a \equiv 1 \pmod{b}$ se počítá za pomoci Bézoutovy rovnosti a Euklidova algoritmu, tedy

$$1 = \gcd(b, a) = ub + va \quad , \text{kde} \quad va \equiv 1 \pmod{b}.$$

2.3.8 Dokažte, že pro libovolný polynom f nad tělesem existuje těleso obsahující kořen f.

Věta 11. Nechť $\mathbb{F}$ je těleso, $f \in \mathbb{F}[x]$ je polynom a $n = \deg(f) \geq 1$. Potom existuje těleso $\mathcal{S} \geq \mathbb{F}$, kde f má kořen.

Důkaz: Pokud má f kořen v $\mathbb{F}$, vezmeme $\mathcal{S} = \mathbb{F}$.
V opačném případě má f nějaký ireducibilní dělitel $m = \sum_{i=0}^{n} a_i x^i$ stupně alespoň 2 a stačí najít nadtěleso, kde má kořen polynom m.
Uvažujme faktorokruh $\mathcal{S} = \mathbb{F}[\alpha]/(m(\alpha))$. Víme, že $\mathcal{S}$ je těleso. Vyhodnotíme-li v $\mathcal{S}$ polynom m na prvku α, dostaneme:

$$m(\alpha) = \sum_{i=0}^{n} a_i(\alpha^i \mod m(\alpha)) = \sum_{i=0}^{n-1} a_i \alpha^i + a_n(\alpha^n \mod m(\alpha)),$$

ovšem $a_n \alpha^n \mod m(\alpha) = -\sum_{i=0}^{n-1} a_i \alpha^i$, takže se to odečte na nulu.
Prvek α je tedy kořenem obou polynomů m, f v nadtělese $\mathcal{S}$. □

2.3.9 Zformulujte a dokažte Čínskou větu o zbytcích pro polynomy.

Věta 12. *(Čínská o zbytcích pro polynomy):* Nechť $\mathbb{F}$ je těleso a $k, n \in \mathbb{N}$. Nechť $m_1, m_2, \ldots, m_n \in F[x]$ jsou po dvou nesoudělné polynomy a nechť $d = \sum \deg(m_i)$. Dále nechť $u_1, \ldots, u_n \in F[x]$ jsou libovolné polynomy. Potom $\exists! f \in F[x]$ polynom stupně $\deg(f) < d$, který řeší soustavu kongruencí:

$$f \equiv u_1 \pmod{m_1}\ , \quad \ldots \quad , \ f \equiv u_n \pmod{m_n}.$$

Důkaz: Dokážeme zvlášť jednoznačnost a existenci.

- *Jednoznačnost*: Pro spor předpokládejme, že má soustava dvě řešení f, g stupně $< d$, tedy

  $$\forall i : f \equiv g \equiv u_i \pmod{m_i}.$$

  Z toho plyne, že $f - g \equiv 0 \pmod{m_i}$, tedy že $m_i \mid f - g$. Zároveň víme, že $\deg(f - g) < d$.

  A protože jsou všechny polynomy m_i navzájem nesoudělné, tak dostaneme:

  $$\underbrace{\prod_{i=1}^{n} m_i}_{\deg = d} \mid \underbrace{f - g}_{\deg < d}.$$

  Tedy polynom stupně d dělí polynom stupně $< d$, což je možné pouze v případě $f - g = 0 \implies f = g$.

- *Existence*: Nechť $m = \prod_{i=1}^{k} m_i$ a nechť $\Psi : F[x]/(m) \to \prod_{i=1}^{k} F[x]/(m_i)$, tedy:

  $$f \to (f \pmod{m_1}, f \pmod{m_2}, \ldots, f \pmod{m_n}).$$

  Jedná se o lineární zobrazení Ψ mezi vektorovými prostory. Zároveň víme díky jedinečnosti, že Ψ je injektivní. Určíme si dimenze, tedy:

  $$F[x]/(m) = \prod_{i=1}^{k} F[x]/(m_i)$$

  $$d = \dim_F \left(F[x]/(m)\right) = \dim_F \left(\prod_{i=1}^{k} F[x]/(m_i)\right) = \sum_{i}^{k} \deg(m_i) = d$$

  Mezi vektorovými prostory je stejná dimenze $\implies$ je i surjektivní $\implies$ je bijektivní $\implies$ má právě jedno řešení soustavy $f = \Psi^{-1}(u_1 \mod m_1, \ldots, u_n \mod m_n)$.

□

2.4 Aplikace

2.4.1 Popište (k, n)-schéma pro sdílení tajemství založený na CRT pro polynomy.

Máme (k, n)-schéma pro sdílení tajemství, kde n účastníků se dělí o tajemství t a k jich je potřeba k jeho odhalení. Obecně pracujeme v tělese $\mathbb{F}_2^m \sim \mathbb{F}_{2^m}$, kde $t \in \mathbb{F}_{2^m}$ je tajemství.

Zvolíme si polynom $f \in \mathbb{F}_{2^m}[x]$, kde $\deg(f) < k$ a kde $f(0) = t$. Dále vybereme n po dvou různých hodnot $a_1, \ldots, a_n \in \mathbb{F}_{2^m}$, tedy $\forall i \neq j : a_i \neq a_j$.
Následně každému účastníkovi přiřadíme právě jednu konkrétní hodnotu $f(a_1), \ldots, f(a_n)$.

- Pokud se sejde $\geq k$ účastníků, vezmou své hodnoty, provedou interpolaci ve svých bodech a spočtou ten jeden jediný polynom stupně $< k$ a vezmou jeho absolutní člen, což je výsledné tajemství
- Pokud se sejde $< k$ účastníků, také vezmou své hodnoty, také provedou interpolaci ve svých bodech, ale polynomů stupně $< k$ je mnoho a nezjistí tak nic o absolutním členu, který hledají. Museli by polynom uhádnout, což je proveditelné s pravděpodobností $\frac{1}{|\mathbb{F}|} = \frac{1}{2^m}$.

2.4.2 Popište protokol RSA s veřejným klíčem a vysvětlete proč dešifrování funguje.

Notace: Zadefinujeme si:

$p, q \in \mathbb{N}$	velká prvočísla, t.ž.: $p \neq q$
(N, e)	dvojice, veřejný klíč, kde $N = p \cdot q$
$\varphi(N) = (p-1)(q-1)$	Eulerova funkce
$e \in \mathbb{N},\ \ 0 < e < \varphi(N)$	šifrovací exponent
$d \in \mathbb{N}$	dešifrovací exponent

Zároveň musí plati platit $\gcd(e, \varphi(N)) = 1$ a dále se hodí k výpočtům následující vztahy:

$y = x^e \pmod N$	zašifrování plaintextu, výsledkem je ciphertext
$x = y^d \pmod N$	dešifrování ciphertextu, výsledkem je plaintext
$d \cdot e \equiv 1 \pmod{\varphi(N)}$	získání d (Euklidovým algoritmem)

Dešifrování se dá lehce odvodit: $y^d \equiv x^{e \cdot d} \equiv x^{1+u\varphi(N)} \equiv x(\overbrace{x^{\varphi(N)}}^{\equiv 1})^N \equiv x \pmod N$

Popis algoritmu: Bob si vygeneruje nahodná velká prvočísla $p, q \in \mathbb{N}, p \neq q$ a vypočítá z nich $N = p \cdot q$. Dále vypočítá Eulerovu funkci $\varphi(N) = (p-1)(q-1)$ a následně vygeneruje číslo $e \in N$, t.ž.: $0 < e < \varphi(N)$ a pro které platí, že $\varphi(N)$, tedy $\gcd(e, \varphi(N)) = 1$. Tímto číslem zašifruje plaintext x vztahem $y = x^e \pmod N$.
Pak už jen nalezne číslo $d \in \mathbb{N}$ euklidovým algoritmem $d \cdot e \equiv 1 \pmod{\varphi(N)}$.
Veřejný klíč, neboli dvojici (N, e) pošle Alici spolu s ciphertextem y.

Alice přijme veřejný klíč (N, e) - dvojici, i ciphertext y. Pouze Alici je znám soukromý klíč (N, d), využije ho k dešifrování y. To udělá vztahem $x = y^d \pmod N$.

Eva nemá možnost si zprávu přečíst, protože nezná dešifrovací exponent d. Musela by ho uhádnout, což není pravděpodobné, nebo by musela znát prvočísla p, q. Kdyby znala p, q mohla by si jednoduše dopočítat $\varphi(N)$ a následně d tak, jak jsme to udělali my.
Bezpečnost RSA tedy stojí na tom, že útočník není schopen rozložit $N = p \cdot q$ na p, q, proto je potřeba je volit dostatečně velká.

2.4.3 Popište schéma Reed-Solomonových kódů. Je zakódování F-lineární zobrazení? Dokažte.

Rood-Solomonovým (k, n)-kódem je zobrazení $\varphi : \mathbb{F}^k \to \mathbb{F}^n$, $f = \sum a_i x^i \to (f(\alpha_1), \ldots, f(\alpha_n))$.
Inverzním zobrazením je interpolace v daných bodech.
Různé polynomy f, g mají $< k$ stejných hodnot, čili $> n - k$ různých hodnot, takže jde o kód typu $(k, n; d)$ pro $d \geq n - k + 1$ a opravuje tak $\lfloor \frac{n-k}{2} \rfloor$ chyb.
Zakódování můžeme převést na lineární zobrazení následovně:

$$(a_0, \ldots, a_{k-1}) \to (f(\alpha_1), \ldots, f(\alpha_n)) = (a_0, \ldots, a_{k-1}) \cdot \begin{pmatrix} \alpha_1^0 & \ldots & \alpha_n^0 \\ \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}$$

Platí, že každé kódové slovo je lineární kombinací vstupních dat a že kódová slova lze zapsat ve formě lineárního zobrazení.

3 Grupy

3.1 Grupy a podgrupy

3.1.1 Definujte pojem grupy a její podgrupy. Co je to řád grupy a prvku? Uveďte příklad grupy řádu 99.

Definice 22. *(Grupa)* : *Grupa* je čtveřice $\mathcal{G} = (G, \cdot, ^{-1}, 1)$, kde G je množina, na které jsou definovány binární operace $\cdot : G \times G \to G$, unární operace $^{-1} : G \to G$ a konstanta $1 \in G$, splňující $\forall a, b, c \in G$:

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita),

(ii) $a \cdot 1 = 1 \cdot a = a$ (neutrální prvek),

(iii) $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (inverzní prvek).

Definice 23. *(Podgrupa)* : Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ a $\mathcal{H} = (H, \tilde{\cdot}, \tilde{^{-1}}, \tilde{1})$ jsou grupy, potom $\mathcal{H}$ je *podgrupa* grupy $\mathcal{G}$, značeno $\mathcal{H} \leq \mathcal{G}$, pokud:

$$1 = \tilde{1}, \qquad \forall a, b \in H : a \,\tilde{\cdot}\, b = a \cdot b, \qquad a^{\tilde{-1}} = a^{-1}.$$

Definice 24. *(Řád grupy $\mathcal{G}$):* je počet prvků její nosné množiny, značíme jej $|\mathcal{G}|$.

Definice 25. *(Řád prvku v grupě $\mathcal{G}$):* je nejmenší $n \in \mathbb{N}$ takové, že $a^n = 1$ pokud takové n existuje, resp. ∞ v opačném případě. Značíme jej $\mathrm{ord}(a)$.

Příklad 6. *(Grupa řádu 99.)* Musí mít 99 prvků. Třeba direktní součin grup $\mathcal{G}$ a $\mathcal{H}$, kde $|\mathcal{G}| = 3$ a $|\mathcal{H}| = 11$, dostaneme $3 \times 3 \times 9 = 99$, tedy $G_3 \times H_9 \to F_{99}$. (Bude Abelovská).

3.1.2 Definujte mocninu grupy. Mají všechny prvky konečné grupy konečný řád?

Definice 26. *(Mocnina):* Nechť $\mathcal{G}$ je grupa, $a \in G, n \in \mathbb{Z}$. Potom mocnina je $a^n = \begin{cases} 1 & n = 0 \\ \underbrace{a \cdot a \cdot \ldots \cdot a}_{n} & n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-n} & n < 0. \end{cases}$

Tvrzení 4. *(Mocniny):* Nechť $\mathcal{G}$ je grupa, $a, b \in G, k, l \in \mathbb{Z}$, potom: $a^{k+l} = a^k \cdot a^l, \qquad a^{kl} = (a^k)^l = (a^l)^k$.
A pokud je abelovská, tak ještě $(ab)^k = a^k b^k$.

Konečnost grupy a řádu: Všechny prvky konečné grupy mají konečný řád, protože v konečné grupě existuje pouze konečný počet různých mocnin prvku. Proto se v určitém okamžiku musí opakovat hodnota a^n a nejmenší takové kladné n je řád prvku.
Kdyby řád byl nekonečný, pak žádné $n \neq 0$ s vlastností $a^n = 1$ neexistuje, mocniny a jsou tak po dvou různé a podgrupa je nekonečná.

3.1.3 Jak spolu souvisí řád prvku a řád příslušné cyklické podgrupy?

Nechť $\mathcal{G}$ je konečná grupa a $g \in G$.
Z Lagrangeovy věty plyne, že řád prvku je dělitelem řádu grupy. Tedy $\mathrm{ord}(g) \mid |G|$.
Pokud je řád prvku roven řádu grupy, pak je tento prvek jejím generátorem, tedy $\mathrm{ord}(g) = |G| \implies G = \langle g \rangle$ a tato grupa $\mathcal{G}$ je tak cyklická.

3.1.4 Definujte, formulujte a dokažte ekvivalentní popis podgrupy generované množinou.

Definice 27. *(Generovaná množina):* Uvažujme podmnožinu $X \subseteq G$ grupy $\mathcal{G}$. Podgrupou generovanou množinou X rozumíme nejmenší podgrupu (vzhledem k inkluzi) grupy $\mathcal{G}$ obsahující podmnožinu X, značíme ji $\langle X \rangle_{\mathcal{G}}$.

Tvrzení 5. *(Podgrupa generovaná množinou):* Nechť $\mathcal{G}$ je grupa a $\emptyset \neq X \subseteq G$, potom:

$$\langle X \rangle_{\mathcal{G}} = \{a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \mid n \in \mathbb{N};\ a_1, \ldots, a_n \in X;\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Důkaz: Označme nejprve M mnořinu na pravé straně rovnosti. Musíme dokázat, že:

- *tvoří podgrupu.* Součin dvou prvků z M jistě $\in M$, jednotka $1 = a^0 \in M$, inverzy plynou ze vztahu $(a_1^{k_1} \cdot \ldots \cdot a_n^{k_n})^{-1} = a_1^{-k_1} \cdot \ldots \cdot a_n^{-k_n} \in M$.
- *obsahuje* X. Volbou $n = 1$, $k_1 = 1$ dostaneme libovolný prvek X.
- *je nejmenší podmnožinou grupy G splňující tyto podmínky.* Uvažujme libovolnou podgrupu $\mathcal{H}$ obsahující X. Tato podgrupa musí obsahovat všechny mocniny $a^i, a \in X$ i jejich libovolné násobky, tedy celé M.

, . $\square$

3.1.5 Zformulujte a dokažte Langrangeovu větu. Co je levá rozkladová třída podgrupy?

Věta 13. *(Langrangeova):* Pokud $\mathcal{H} \leq \mathcal{G}$, pak $|\mathcal{G}| = [\mathcal{G} : \mathcal{H}] \cdot |\mathcal{H}|$.

Důkaz: Zvolme transverzálu T z $\mathcal{H}$ a zapišme ji jako $G = \bigcup_{a \in T} aH$.

Z lemmatu "$aH \cap bH = \emptyset$ nebo $aH = bH$" víme, že se jedná o disjunktní sjednocení a platí $T = [\mathcal{G} : \mathcal{H}]$, takže počet prvků lze spočítat jako součet velikostí jednotlivých podmnožin:

$$|\mathcal{G}| = \sum_{a \in T} |aH| = \sum_{a \in T} |H| = |T| \cdot |H| = [\mathcal{G} : \mathcal{H}] \cdot |\mathcal{H}|$$

Rovnost $\sum_{a \in T} |aH| = \sum_{a \in T} |H|$ platí, protože platí lemma "$|aH| = |H|$". □

Definice 28. *(Levá rozkladová třída):* Nechť $\mathcal{G}$ je grupa a $\mathcal{H}$ její podgrupa, potom množiny $aH = \{ah \mid h \in H\}$, kde $a \in G$, se nazývají *levé rozkladové třídy* podgrupy $\mathcal{H}$.

3.2 Cyklické grupy a působení grup

3.2.1 Definujte působení grupy na množině X a relace tranzitivity na X. Co je stabilizátor prvku?

Definice 29. *(Působení grupy $\mathcal{G}$ na množině X):* je libovolné zobrazení $\pi : G \to S_X = \{f : x \to x \mid f \text{ bijektivní}\}$ splňující $\forall g, h \in G$:

$$\pi(gh) = \pi(g) \circ \pi(h), \quad \pi(g){-}1 = \pi(g)^{-1} \;\; a \;\; \pi(1) = id$$

Hodnotu permutace $\pi(g)$ na prvku $x \in X$ budeme značit $\pi(g)(x) = g(x)$.

Definice 30. *(Relace tranzitivity $\sim$ na množině X):* definujeme $x \sim y$, pokud $\exists g \in G$ takové, že $y = g(x)$.
($x \sim y$, pokud nějaká permutace přesouvá prvek x na prvek y.)

Definice 31. *(Stabilizátor prvku $x \in X$)* je množina $G_x = \{g \in G \mid g(x) = x\}$.

3.2.2 Zformulujte a dokažte tvrzení o velikosti orbity a indexu stabilizátoru.

Tvrzení 6. *(Velikost orbity VS index stabilizátoru):* Nechť grupa $\mathcal{G}$ působí na množině X, potom:

$$\forall x \in X: \; |[x]| = [\mathcal{G} : \mathcal{G}_x].$$

Důkaz: Index $[\mathcal{G} : \mathcal{G}_x]$ značí počet rozkladových tříd podgrupy $\mathcal{G}_x$, stačí tedy najít bijekci mezi prvky orbity a množinou rozkladových tříd. Uvažujme zobrazení

$$\varphi : \{gG_x \mid g \in G\} \to \{x\}, \quad gGx \to g(x).$$

Dokážeme, že to je bijekce.
Nejprve ověříme, že jsme dobře definovali zobrazení. Mohlo by se jinak stát, že tutéž rozkladovou třídu máme označenu dvěma různými způsoby, tj. že $gG_x = hG_x$, a přitom se jí snažíme přiřadit různé hodnoty $g(x) \neq g(x)$.
Z tvrzení o "rovnosti rozkladových třídách, tedy pro $aH = bH \iff a^{-1}b \in H$" víme, že platí

$$gG_x = hG_x \iff h^{-1}g \in G_x \iff h^{-1}g(x) = x \iff g(x) = h(x).$$

A tedy φ je dobře definováno a zároveň je i prosté. Navíc $\forall y \in [x], \exists g \in G : g(x) = y$, takže φ je i bijekce. □

3.2.3 Zformulujte a dokažte Burnsideovo lemma.

Věta 14. *(Burnsideova):* Nechť $\mathcal{G}$ je konečná grupa, která působí na konečnou množinu X.
Dále označme $X/\sim$ jako množinu všech orbit $\sim$ na $|X/\sim|$ jako počet orbit daného působení. Potom:

$$|X/\sim| = \frac{1}{|G|} \cdot \sum_{g\in G} |X_g| = |\{[x]_\sim \mid x \in X\}|.$$

(Můžeme interpretovat jako "počet orbit je roven průměrnému počtu pevných bodů").

Důkaz: Nechť $M = \{(g, x) \in G \times X \mid g(x) = x\}$ a počítáme prvky dvěma způsoby: buď ke každému x spočítáme počet g splňujících $(g, x) \in M$, nebo ke kadému g spočítáme počet x splňujících $(g, x) \in M$. Dostaneme rovnost:

$$|M| = \underbrace{\sum_{g\in G} |X_g|}_{\text{pevné body}} = \underbrace{\sum_{x\in X} |G_x|}_{\text{stabilizátor}}$$

$$\frac{1}{|G|} \cdot \sum_{g\in G} |X_g| = \frac{|M|}{|G|} = \frac{1}{|G|} \cdot \sum_{x\in X} |G_x| = \frac{1}{\cancel{|G|}} \cdot \sum_{x\in X} \frac{\cancel{|G|}}{|[x]|} = \sum_{x\in X} \frac{1}{|[x]|} =$$
$$= \sum_{O\in(X/\sim)} \sum_{x\in O} \frac{1}{|[x]|} = \sum_{O\in(X/\sim)} \sum_{x\in O} \frac{1}{|O|} = \sum_{O\in(X/\sim)} |O| \cdot \frac{1}{|O|} =$$
$$= \sum_{O\in(X/\sim)} 1 \implies \text{je rovno velikosti množiny } X/\sim.$$

□

3.2.4 Popište řády a počet prvků daného řádu v konečných cyklických grupách.

Tvrzení 7. *(Řády prvků cyklických grup):* Nechť $\mathcal{G} = \langle a \rangle$ je cyklická grupa konečného řádu $n = |G|$, potom pokud $\forall k \mid n$, tak $|\{b \in G \mid \mathrm{ord}(b) = k\}| = \varphi(k)$, neboli obsahuje právě $\varphi(n)$ prvků řádu k pro každé $k \mid n$.

Důkaz: Nechť $\mathcal{G} = \langle a \rangle$ je cyklická grupa konečného řádu $n = |G|$.
Každý prvek řádu $k \mid n$ je generátorem nějaké cyklické podgrupy řádu k. Taková podgrupa však v $\mathcal{G}$ existuje pouze jedna. Podle Lemmatu, které říká "$|G| = n \implies \langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$", jsou všechny podgrupy v $\mathcal{G}$ tvaru $\langle a^k \rangle,\ k \mid n$.
Přitom $|\langle a^k \rangle| = \frac{n}{k}$, tedy $\langle a^{\frac{n}{k}} \rangle$ je jediná podgrupa řádu d.
Tato podgrupa má podle Tvrzení říkající "konečná $|G| = n \implies$ generátorem jsou prvky a^k, kde $k \in \{1, \ldots, n-1\}$ nesoudělné s n", právě $|\{l \in \mathbb{Z}_k \mid \gcd(l, k)\}| = \varphi(k)$ generátorů. □

3.2.5 Je-li G = [a] konečná cyklická grupa řádu n, rozhodněte, které prvky a na n jsou generátory.

Tvrzení 8. *(Generátory cyklických grup):* Nechť $\mathcal{G} = \langle a \rangle$ je cyklická grupa, potom:

(1) pokud je $\mathcal{G}$ nekonečná, generátorem jsou pouze prvky a, a^{-1}

(2) pokud je $\mathcal{G}$ konečná řádu n, tak generátorem jsou takové prvky a^k, kde $k \in \{1, \ldots, n-1\}$ je nesoudeělné s n.

Důkaz: Dokážeme zvlášť oba body:

(1) Oba prvky a, a^{-1} grupu $\mathcal{G}$ generují, protože $\{a^k \mid k \in \mathbb{Z}\} = \{a^{-k} \mid k \in \mathbb{Z}\}$. Žádný jiný generátor $\mathcal{G}$ nemá:
Kdyby $\mathcal{G} = \langle a^n \rangle$ pro nějaké n, pak by $\exists m \in \mathbb{Z}$ takové, že $a = (a^n)^m$, a dostali bychom

$$1 = ({}^a n)^m \cdot a^{-1} = a^{mn-1}.$$

Řád a je ovšem nekonečný, a tedy $mn = 1$, čili $n = \pm 1$.

(2) Z Lemmatu o "podgrupách cyklických grup" víme, že platí $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$.
Uvažme dvě možnosti. Pokud $\begin{cases} \gcd(k, n) = 1 & \langle a^k \rangle = \langle a \rangle = \mathcal{G} \\ \gcd(k, n) = d \neq 1 & \langle a^k \rangle = \langle a^d \rangle = \{a^d, a^{2d}, \ldots, a^{\frac{n}{d}d}\} \text{ je vlastní podgrupa} \end{cases}$

□

3.2.6 Dokažte, že konečná podgrupa multiplikativní grupy tělesa je cyklická.

Věta 15. *Nechť $\mathbb{F}$ je těleso a $\mathcal{G}$ je konečná podgrupa grupy $\mathbb{F}^*$. Potom $\mathcal{G}$ je cyklická.*

Důkaz: Nechť $k \in \mathbb{N}$ a $n = |G|$. Definujme si počet ptvků k v grupě $\mathcal{G}$, tedy $u_k = \{a \in G \mid \text{ord}(a) = k\}$.
Uvažujme nějaký prvek a řádu k v $\mathcal{G}$, tedy $a \in u_k : \ k = \text{ord}(a)$.
Zároveň platí, že grupa $\langle a \rangle$ je cyklická řádu k a proto $\forall b \in \langle a \rangle : \quad b^k = 1$ a tedy $|\langle a \rangle| = k$.
Žádné jiné prvky s touto vlastností v $\mathcal{G}$ nejsou, takže $\langle a \rangle$ je jediná cyklická podgrupa řádu k v $\mathcal{G}$.
Dostáváme tak, že b je kořenem $x^k - 1$ a má proto $\leq k$ kořenů (v tělese $\mathbb{F}$). Takže $\langle a \rangle$ je množina všech kořenů $x^k - 1 \implies u_k \subseteq \langle a \rangle \implies u_k$ jsou všichni generátoři $\langle a \rangle \implies \forall k \mid n : \ |u_k| = \varphi(k) \implies u_k \leq k \implies$ je cyklická. □

(Aplikovali jsme lemma říkající, že "pokud $\forall k$ grupa obsajuje $\leq k$ prvků a splňujících $a^k = 1$, je potom cyklická").

3.2.7 Co je to diskrétní logaritmus? Popište Diffie-Hellmanův protokol pro výměnu klíčů.

Definice 32. *(Diskrétní logaritmus):* je inverzní zobrazení k tzv. diskrétní exponenciále, tedy k zobrazení

$$\exp : \mathbb{Z}_n \to \mathcal{G}, \quad k \to a^k,$$

kde $\mathcal{G} = \langle a \rangle$ je cyklická grupa řádu n,

Diffie-Hellmanův protokol Alice a Bob se potřebují dohodnout na nějakém společném klíči, přičemž k dispozici mají pouze veřejný kanál.
Nejprve se Alice a Bob dohodnou na nějaké cyklické grupě a generátoru $\mathcal{G} = \langle a \rangle$. Dále si Alice zvolí číslo m a Bob číslo n z intervalu $2, \dots, |G| - 1$, přičemž každý bude svoje číslo držet v tajnosti.

- Alice spočte $u = a^m$ a pošle u Bobovi.
- Bob spočte $v = a^n$ a pošle v Alici.

Poté Alice spočte $v^m = (a^n)^m = a^{mn}$ a Bob spočte $u^n = (a^m)^n = a^{mn}$. Oba tak získali stejný prvek a^{mn}, což je společný klíč.

Kdyby je poslouchala Eva, bude znát pouze grupu $\mathcal{G}$, generátor a a hodnoty u, v.
Prvek a^{mn} ale není schopná dopočítat, musela by provést diskrétní logaritmus, určit mn a dopočítat a^{mn}. Dodnes pro to ale není znám efektivní způsob.