Algebra - zpracované příklady 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 Najděte $u, v \in \mathbb{Z}$, pro která $103u + 77v = 1$.

Hledáme Bézoutovy koeficienty pro $\gcd(77, 103) = 1$ podle vzorce $(u_{i+1}, v_{i+1}) = (u_{i-1}, v_{i-1}) + q_i(u_i, v_i)$.
Pro $i \in \{0, \ldots, 4\}$: $a_i = (103, 77, 26, 25, 1)$, $u_i = (1, 0, 1, -2, 3)$, $v_i = (0, 1, -1, 3, -4)$, takže:

$$103 \cdot 3 - 77 \cdot 4 = 1.$$

1.1.2 Vypočítejte poslední číslici 33^{999}.

Počítáme poslední cifru, tedy $33^{999} \pmod{10}$. Použijeme Eulerovu větu: $\varphi(10) = 4$ a $\gcd(33, 10) = 1$ platí. A také využijeme faktu, že $33 \pmod{10} = 3$.

$$33^{999} \equiv 33^{1000} \cdot 3^{-1} \equiv \underbrace{33^{4 \cdot 250}}_{(33^4)^{250} = 1^{250}} \cdot 3^{-1} = 1 \cdot 3^{-1} \equiv 7$$

1.1.3 Vypočítejte $2023^{2022^{2021}} \pmod{101}$.

Nejprve zmodulíme $2023 \pmod{101} = 3$ a dosadíme do původní rovnice: $3^{2022^{2021}} \pmod{101}$.
Dále si můžeme uvědomit, díky Eulerově větě, že: $3^{2022^{2021}} \bmod n \pmod{101}$, kde $n = \varphi(101) = 100$ (protože 101 je prvočíslo). Tedy spočítáme $a := 2022^{2021} \pmod{100}$ a dosadíme do $3^a \pmod{101}$.

$$2022^{2021} \pmod{100} \equiv 22^{2021} \pmod{100}, \textit{ spočítáme Eulerovu funkci pro } \varphi(100):$$
$$\varphi(100) = \varphi(4 \cdot 25) = 2 \cdot 4 \cdot 5 = 40, \textit{ dostaneme tak: } 22^{40} \equiv 1 \pmod{40} \textit{ a upravíme původní výraz:}$$
$$(22^{40})^{50} \cdot 22^{21} \pmod{100} \equiv 1^{50} \cdot 22^{21} \pmod{100} = 22^{21} \pmod{100}$$

Nyní tedy hledáme řešení pro $22^{21} \pmod{100}$, a protože 100 můžeme rozepsat jako $100 = 25 \cdot 4 \implies \gcd(25, 4) = 1$, můžeme k tomu použít Čínskou zbytkovou větu:

$$x = 22^{21} \pmod{25} = 22$$
$$x = 22^{21} \pmod{4} = 22^{20} \cdot 22^1 \pmod{4} \equiv 0 \cdot 22 \pmod{4} = 0$$

Víme, že výsledek by měl být ve formátu $22^{21} \pmod{100} = (a_1 \cdot b_1 \cdot m_1) + (a_2 \cdot b_2 \cdot m_2) \bmod 100$, kde už tedy máme $a_1 = 22$ a $a_2 = 0$. Ostatní členy s indexem 1 dopočítáme, s indexem 2 nemusíme díky $a_2 = 0$:
$b_1 = 4$ a $m_1 = b_1^{-1} \pmod{25} = 4^{-1} \pmod{25} = 19$
A dostáváme tak:

$$22^{21} \pmod{100} = 22 \cdot 4 \cdot 19 \pmod{100} = 1672 \pmod{100} \equiv 72$$

Nyní dosadíme do původní rovnice $3^{72} \pmod{101}$ a podle tabulky už určíme mocninu:

3^n	úprava	mod 101
3^1	3	3
3^2	$3 \cdot 3$	9
3^3	$3 \cdot 9$	27
3^6	$(3^3)^2 = 27^2 = 729$	22

Dostáváme $3^{72} = (3^6)^{12} = 22^{12} \pmod{101}$ a opět podle tabulky:

22^n	úprava	mod 101
22^1	22	22
22^2	$22 \cdot 22 = 484$	80
22^3	$22 \cdot 80 = 1760$	43
22^4	$22 \cdot 43 = 946$	37
22^5	$22 \cdot 37 = 814$	6
22^6	$22 \cdot 6 = 132$	31
22^{12}	$(22^6)^2 = 31^2 = 961$	52

Takže $2023^{2022^{2021}} \pmod{101} \equiv 3^{72} \equiv 22^{12} \equiv 52$.

Vyřešte systém kongruencí:

$$\begin{aligned}
x &\equiv 1 \pmod 3 \\
x &\equiv 2 \pmod 5 \quad \rightsquigarrow \quad x = 5k + 2 \\
x &\equiv 1 \pmod 7 \\
&- - - - - - - - - - - - - - - - - - - \\
5k + 2 &\equiv 1 \pmod 7, \quad (k \in \mathbb{Z}) \\
5k &\equiv -1 \equiv 6 \pmod 7 \\
k &= 4 \implies \\
\implies x &= 5 \cdot 4 + 2 = 22 \in \mathbb{Z}_{35} \\
&- \\
22 + 35l &\equiv 1 \pmod 3, \quad (l \in \mathbb{Z}) \\
35l &\equiv -21 \equiv 0 \pmod 3 \\
35l &\equiv 0 \pmod 3 \\
l &= 0 \implies \\
\implies x &= 22 + 35 \cdot 0 = 22 \in \mathbb{Z}_{105}
\end{aligned}$$

Celkově je řešením množina $\{x = 22 + 35l \mid x < 105, l \in \mathbb{Z}\}$, tedy $x \in \{22, 57, 92\}$.

2 Polynomy

2.1 Tělesa, okruhy, obory

2.1.1 Vypočítejte 33^{-1} v tělese $(\mathbb{Z}_{37}, +, \cdot -, 0)$.

Máme těleso $\mathbb{Z}_{37}$ a hceme vypočítat inverz 33^{-1}. Ověříme nejprve, že $\gcd(33, 37) = 1$. Dále hledáme Bézoutovy koeficienty u a v takové, že $33u + 37v = 1$:

$$\text{Pro } i \in \{0, \dots 3\} : \; a_i = (37, 33, 4, 1), \quad u_i = (1, 0, 1, 8), \quad v_i = (0, 1, 1, 9)$$
$$\implies 33 \cdot 9 - 37 \cdot 8 = 1$$

Takže 33^{-1} v tělese $\mathbb{Z}_{37}$ je 9.

2.1.2 Zkostruujte těleso o 125 prvcích.

Potřebujeme najít prvočíslo p a $k \in \mathbb{N}$ tak, aby platil vztah $p^k = 125$.
Jednou možností je vzít $p = 5$ a $k = 3$, protože $5^3 = 125$. Tímto způsobem získáme těleso se 125 prvky.

2.2 Dělitelnost, UFD

2.2.1 Dokažte, že $4x^3 - 15x^2 + 60x + 180$ je ireducibilní v $\mathbb{Q}[x]$ (Eisensteinovo kritérium)

Pokud $\exists p \in Q$ ireducibilní prvek splňující $p \mid a_0$, $p|a_1, \dots, p|a_{n-1}$ a $p^2 \nmid a_0$, pak je polynom ireducibilní v $\mathbb{Q}[x]$.
Hledáme proto p, které dělí první až předposlední koeficient. V našem případě je to $p = 5$.
Platí, že 5 je ireducibilní, zároveň platí $5 \mid 180,\ 5 \mid 60,\ 5 \mid 15$ a dokonce i $5^2 \nmid 180 \equiv 25 \nmid 180$.
Eisensteinovým kritériem jsme určili, že polynom $4x^3 - 15x^2 + 60x + 180$ je ireducibilní.

2.2.2 V $\mathbb{Z}_2[x]$ najděte všechny ireducibilní polynomy stupně nejvýše 4.

Budeme postupně zkoušet všechny možnosti s tím, že předem nějaké vyloučíme.
Například vyloučíme možnosti bez x^0 - například: $x^2 + x = x(x + 1)$, protože pak bychom mohli vytknout x.
Ze stejného důvodu vyřadíme všechny x^i a $x^i + 1$ pro $i = 2, 3, 4$. Obecně řečeno odstraníme všechny polynomy, které jsou nějakým násobkem našeho polynomu.

deg 0: Nic.

deg 1: Pouze x a $x + 1$ jsou ireducibilní.

deg 2: Pouze $x^2 + x + 1$ je ireducibilní.

deg 3: Pouze $x^3 + x^2 + 1$ a $x^3 + x + 1$ jsou ireducibilní.

deg 4: Pouze $x^4 + x^3 + x^2 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x + 1$

2.2.3 Napiště $2x^2 - 6$ jako násobek ireducibilních polynomů v (a) $\mathbb{Z}[x]$, (b) $\mathbb{Q}[x]$, (c) $\mathbb{C}[x]$

(a) $\mathbb{Z}[x]$: Vytkneme 2 a dostaneme výsledný polynom $f(x) = 2(x^2 - 3)$, musíme ověřit ireducibilu.
Číslo 2 je ireducibilní, protože je prvočíslo. Polynom $(x^2 - 3)$ je také ireducibilní, protože může být rozloženo pouze na $(x + \sqrt{3})(x - \sqrt{3})$, což ovšem nemá celočíselný kořen $\sqrt{3} \notin \mathbb{Z}[x]$.

(b) $\mathbb{Q}[x]$: 2 jako polynom stupně nula nad tělesem je invertibilní, jinak také $\sqrt{3} \notin \mathbb{Q}[x]$, takže $2x^2 - 6$

(c) $\mathbb{C}[x]$: Podobně jako v $\mathbb{Q}[x]$, akorát $\sqrt{3} \in \mathbb{C}[x] \implies f(x) = (2x + 2\sqrt{3})(x - \sqrt{3})$.
Stačí určit ireducibilitu $(x \pm \sqrt{3})$. Jsou ireducibilní, protože jsou stupně 1.

2.3 GCD a Modulo polynom

2.3.1 Show that $m(\alpha) = \alpha^3 + \alpha + 1$ is irreducible in the domain $\mathbb{Z}_7[\alpha]$. Solve the equation $(\alpha^2 + 3)x + \alpha + 4 = \alpha^2$ in the feld $\mathbb{Z}_7[\alpha]/(m(\alpha))$.

2.3.2 Vypočítejte $\gcd(x^5 + x^2 + x + 1, \quad x^3 + x + 1 \in \mathbb{Z}_2[x])$ a určete Bézoutovy koeficienty.

2.3.3 Vypočítejte $\gcd(5 - 3i, 7 + i)$ v oboru $\mathbb{Z}[i]$

Budeme řešit za pomoci Eukleidova algoritmu v oboru $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Abychom věděli, co čím dělit, musíme určit normy: $\mathcal{V}(a) = ||7+i|| = 50 > 34 = ||5-3i|| = \mathcal{V}(b)$. Dělíme:

$$\frac{7+i}{5-3i} = \frac{(7+i)(5+3i)}{(5-3i)(5+3i)} = \frac{35+21i+5i-3}{25+9} = \frac{16}{17} + \frac{13}{17}i$$

Nyní zvolím vhodné q, r takové, aby $\mathcal{V}(r) < \mathcal{V}(5-3i)$. Protože $\frac{16}{17} + \frac{13}{17}i = \frac{1}{17}(16+13i) = \frac{13}{17}(\approx 1+i)$, zvolíme jako $q = 1+i$ a dopočítáme r.

$$(7+i) - (5-3i)(1+i) = 7+i-5-5i+3i-3 = -1-i = r$$

Vidíme, že zjevně platí $\mathcal{V}(-1-i) = ||-1-i|| = 2 < 34 = \mathcal{V}(5-3i)$. Budeme proto pokračovat v algoritmu:

$$\frac{5-3i}{-1-i} = \frac{-5+3i}{1+i} = \frac{(-5+3i)(1-i)}{(1-i)(1+i)} = \frac{-5+5i+3i+3}{2} = \frac{-2+8i}{2} = -1+4i$$

Vidíme, že zbytek po dělení je 0, proto $\gcd(5-3i, 7+i) = -1-i$.

2.4 Aplikace

2.4.1 Reed-Solomonovy kódy

Mějme těleso $T := \mathbb{F}_8 = \mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ a Reed-Solomonův $(2,4)-$kód nad abecedou T pro

$$u_1 = 1, \quad u_2 = \alpha, \quad u_3 = \alpha^2 \quad \text{a} \quad u_4 = \alpha + 1.$$

Tento kód může opravit jednu chybu.

(a) Zakóduj $(0, \alpha)$.

(b) Obdrželi jsme kód $(\alpha, \alpha^2, \alpha+1, \alpha^2)$. Co bylo původní slovo?

(c) Obdrželi jsme slovo $w = (0,0,1,1)$, ale kanál byl nespolehlivý.
Ukažte, že toto slovo nelze dekódovat. Explicitně se po vás chce, abyste:
- ukázali, že neexistuje kód c s Hammingovou vzdáleností $\delta(c,w) \leq 1$.
- nalezli dva kódy c_1, c_2 takové, že $\delta(c_1, w) = \delta(c_2, w) = 2$.

(a) Zprávu $(0, \alpha)$ rozepíšeme jako polynom $f(x) = \sum \alpha_i x^i \implies f(x) = 0x^0 + \alpha x^1 \implies f(x) = \alpha x$.
A dopočítáme kód $(f(u_1), f(u_2), f(u_3), f(u_4))$:

- $f(u_1) = \alpha \cdot u_1 = 1 \cdot \alpha = \alpha$
- $f(u_2) = \alpha \cdot u_2 = \alpha \cdot \alpha = \alpha^2$
- $f(u_3) = \alpha \cdot u_3 = \alpha^2 \cdot \alpha = \alpha^3 = -\alpha - 1 = \alpha + 1$
- $f(u_4) = \alpha \cdot u_4 = (\alpha+1) \cdot \alpha = \alpha^2 + \alpha$

Takže po zakódování dostaneme výsledný kód: $(\alpha, \alpha^2, \alpha+1, \alpha^2+\alpha)$.

(b) Máme kód $c = (c_1, c_2, c_3, c_4) = (\alpha, \alpha^2, \alpha+1, \alpha^2)$ s maximálně jednou chybou a víme, že $c_i = f(u_i)$, pro $i \in \{1,2,3,4\}$. Potřebujeme určit polynom, z kterého odvodíme původní zprávu, což je zjevně opět $f(x) = \alpha x$.

Naše obdržená zpráva splňuje podmínku jedné chyby se zprávou z (a), protože nesedí pouze c_4.

Původní slovo tak je opět $(0, \alpha)$.

(c) Slovo nejde dekódovat, protože Hammingova vzdálenost pro w je nejméně 2. Víme, že lze opravit nejvýše $\lfloor \frac{d-1}{2} \rfloor$ chyb $\implies d \geq n-k+1 \implies d \geq 4-2+1 \implies d \geq 3$.

Celkem proto platí, že můžeme opravit nejvýše $\lfloor \frac{3-1}{2} \rfloor = 1$ chybu, takže 3 výstupy musí být správné:

- Buď dvě 0 a jedna 1 $\implies f(x) = 0 \implies (0,0,0,0)$, takže $\delta(c,w) > 1$, protože u_3, u_4 neodpovídá
- Nebo dvě 1 a jedna 0 $\implies f(x) = 1 \implies (1,1,1,1)$, takže $\delta(c,w) > 1$, protože u_1, u_2 neodpovídá

Slovo proto nelze dekódovat, protože v něm máme více než 2 chyby, tedy $\delta(c,w) \geq 2$

Dva kódy c_1, c_2 s $\delta(c_1, w) = \delta(c_2, w) = 2$:

- $(0,0) \rightsquigarrow f(x) = 0 \rightsquigarrow c_1 = (0,0,0,0)$ a tedy $\delta((0,0,0,0),(0,0,1,1)) = 2$.
- $(1,0) \rightsquigarrow f(x) = 1 \rightsquigarrow c_2 = (1,1,1,1)$ a tedy $\delta((1,1,1,1),(0,0,1,1)) = 2$.

2.4.2 Sdílení klíčů

Navrhněte schéma sdílení tajemství pro sedm účastníků - dva králové a pět eforů tak, že tajemství mohou rekonstruovat buď oba králové, nebo jeden král a všech pět eforů.

(a) Tajemstvím je konkrétní prvek tělesa T. Volba tělesa je na vás a výběr tajemství je na vás.

(b) Pravděpodobnost, že někdo náhodně uhodne tajemství, je menší než 2%.

---

1. Inspiroval jsem se učebnicovým příkladem, konkrétně Shamirovým protokolem a zvolil jsem těleso $T = \mathbb{Z}_{2^m}$ s pravděpodobností $\frac{1}{|T|} = (\frac{1}{2})^m$. Aby pravděpodobnost byla $< 2\%$, musíme volit $m \geq 6$. Já jsem se rozhodl pro $\mathbb{Z}_{2^{256}}$. Tajemství je schováno v absolutním členu polynomu, $t = f(0)$.

2. Počet klíčů pro 2 krále musí být stejný jako počet klíčů pro 1 krále a 5 eforů.

$$2k = k + 5 \implies k = 5$$

   Což by znamenalo 5 klíčů pro krále a 1 klíč pro každého z 5 eforů, tedy celkem 10/15 klíčů pro odhalení tajemství. Vytváříme proto $(10, 15)-$schéma a volíme tak polynom stupně < 10:

$$f(x) = t + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^5 + a_7x^7 + a_8x^8 + a_9x^9$$

3. Vygenerujeme 15 náhodných hodnot $\alpha_1 \dots \alpha_{15} \in \mathbb{Z}_{2^8}$ a ty rozdáme po 5 králům a po 1 eforům.

   - První král dostane vygenerované klíče $f(\alpha_i)$, kde $i \in \{1, \dots, 5\}$
   - Druhý král dostane vygenerované klíče $f(\alpha_i)$, kde $i \in \{6, \dots, 10\}$
   - Každý efor e_j dostane vygenerované klíče: $f(\alpha_i)$, kde $j \in \{1, \dots, 5\}$ a $i = 10 + j$

   Jakmile se sejdou 2 králové, nebo 1 král a 5 eforů, interpolují dokud jim nevyjde polynom < 10. Ve chvíli kdy se tak stane, vezmou absolutní člen, což je tajemství.

   Pokud se sejdou v jiném počtu a dají dohromady < 10 klíčů, vyjde jim polynomů stupně < 10 mnoho a pravděpodobnost, že klíč uhodnou bude $\frac{1}{2^8} = 0.4\%$.

2.4.3 RSA

Mějme systém RSA s veřejným klíčem $(N, e) = (91,\ 5)$.

(a) Zašifrujte zprávu $x = 4$ za pomoci klíče $(91,\ 5)$.

(b) Protože jsme si vybrali malé N, je možné dešifrovat zprávu bez veřejného klíče. Dešifrujte zprávu $y = 61$. Co bylo původní zprávou?

(c) Mějme jiný veřejný klíč $(N, e) = (169,\ 5)$. Najděte d a číslo $0 < x < 169$ takové, že po dešifrování veřejným klíčem $(169,\ 5)$ vrátí RSA hodnotu různou od x.

(a) Zašifrování probíhá způsobem $y = (x^e) \mod N$. V našem případě pro $x = 4,\ e = 5,\ N = 91$:

$$\begin{aligned} y &= (4^5) \mod 91 \\ y &= 1024 \pmod{91} \\ y &= 23 \pmod{91} \end{aligned}$$

(b) Pokud chceme zprávu dešifrovat, musíme použít $x = y^d \pmod N$, kde d je tajný klíč.

Ten sice neznáme, můžeme ho ale získat vztahem $de \equiv 1 \pmod{\varphi(N)}$, kde $\varphi(N) = (p-1)(q-1)$.

Máme $N = 91$, tedy jediná varianta pro prvočísla jsou $p = 7, q = 13$ (a naopak). Proto $\varphi(N) = 12 \cdot 6 = 72$

Dosadíme do $de \equiv 1 \pmod{\varphi(N)}$ a dostáváme $5d \equiv 1 \pmod{72}$. A protože $\gcd(5, 72) = 1$, můžeme d určit za pomoci euklidova algoritmu:

$$\begin{aligned} 5d &\equiv 1 \pmod{72} \quad // \quad 5 \cdot 29 = 145 \equiv 1 \\ 145d &\equiv 29 \pmod{72} \\ d &\equiv 29 \pmod{72} \implies d = 29 + 72k\ (\forall k \in \mathbb{Z}) \end{aligned}$$

Stačí nám už jen dopočítat x, to uděláme za pomoci $x = (y^d) \mod N$:

$$\begin{aligned} x &= (y^d) \mod N \quad // \quad y = 61,\ N = 91,\ d = 29 \\ x &= (61^{29}) \mod 91 \\ x &= 3 \end{aligned}$$

(c) Máme zadáno $N = 169$ a $e = 5$. A lehce si odvodíme $p = q = 13 \implies \varphi(N) = (p-1)^2 = 12^2 = 144$.
Hledáme d a číslo $x \in (0, 169)$ takové, že po dešifrování dostaneme hodnotu různou od x.

Nejprve si určíme d a to opět za pomoci $d \cdot e \equiv 1 \pmod{\varphi(N)}$, kde $e = 5$ a $\varphi(N) = 144$:

$$\begin{aligned} 5d &\equiv 1 \pmod{144} \quad // \quad 5 \cdot 29 = 145 \equiv 1 \\ 145d &\equiv 29 \pmod{144} \\ d &\equiv 29 \pmod{144} \implies d = 29 + 144k\ (\forall k \in \mathbb{Z}) \end{aligned}$$

Nyní už stačí jen najít $x \in (0, 169)$ takové, že $x \neq \mathrm{dec}(\mathrm{enc}(x))$:

$$\begin{aligned} y &= (x^e) \mod N \quad // \quad x = 2,\ e = 5,\ N = 169 \\ y &= (2^5) \mod 169 \\ y &= 32 \pmod{169} \end{aligned}$$

$$\begin{aligned} x &= (y^d) \mod N \quad // \quad y = 32,\ N = 169,\ d = 29 \\ x &= (32^{29}) \mod 169 \\ x &= 93 \pmod{169} \neq 2 \end{aligned}$$

Takových čísel najdeme hodně, protože RSA nefunguje - kvůli špatně vypočítanému $\varphi(N)$:
Z Eulerovy funkce $\varphi(pq)$ pro prvočísla $p \neq q$ se dá jednoduše odvodit, že $\varphi(pq) = (p-1)(q-1)$.
Pokud ale $p = q$, tak určujeme $\varphi(p^2)$, což není $(p-1)^2$, ale $\varphi(p^2) = p(p-1)$.
Aby RSA fungovalo pro $p = q$, museli bychom přepočítat $\varphi(N) = 13 \cdot 12 = 156$ a tím pádem i přepočítat d.

3 Grupy

3.1 Grupy a podgrupy

3.1.1 .

3.1.2 .

3.2 Cyklické grupy a

3.2.1 .

3.2.2 .