Kapitola 6

Šifrování, diofantické rovnice

6.1 Opakování z přednášky

Připomeneme si šifrovací systémy pro asymetrickou kryptografii, které jsme na cvičení používali.

protokol na výměnu klíčů DH Obě strany komunikace se dohodnou na prvočísle p a primitivním kořenu g modulo p pak každý z účastníků vybere a, respektive b, a pošle druhé straně g^a, resp. g^b modulo p. Společným klíčem pro komunikaci (pro symetrickou kryptografii) je pak $g^{a\,b} = (g^a)^b = (g^b)^a$, což mohou oba účastníci spočítat bez toho, aby jej mohl zjistit kdokoli jiný.

ElGamal Systém je odvozen z protokolu DH. Účastník zvolí prvočíslo p, primitivní kořen g modulo p, náhodné a a spočítá $h \equiv g^a \pmod{p}$. Veřejným klíčem pak je $V = (p, g, h)$ a soukromým klíčem je pak $S = a$. Při šifrování zprávy M zvolíme náhodné b a spočítáme $C_1 \equiv g^b \pmod{p}$ a $C_2 \equiv M \cdot h^b \pmod{p}$; následně pošleme $C = (C_1, C_2)$. Pro dešifrování pak účastník spočítá $M \equiv C_2 / C_1^a \pmod{p}$.

Rabinův kryptosystém Pro generování klíčů zvolí účastník dvě *podobně velká* prvočísla $p \equiv q \equiv 3 \pmod{4}$ a spočítá $n = p \cdot q$. Veřejným klíčem je $V = n$, soukromým klíčem je $S = (p, q)$. Při šifrování zprávy M spočítáme $C \equiv M^2 \pmod{n}$. Pro dešifrování účastník spočítá (čtyři) modulární odmocniny z C a následně zjistí, která byla původní zprávou (například dohodou na kódu). Pro počítání odmocnin z C se spočítají $r \cong \pm C^{\frac{p+1}{4}} \pmod{p}$ a $s \cong \pm C^{\frac{q+1}{4}} \pmod{q}$, následně se určí kandidáti na M řešením soustavy lineárních kongruencí.

6.2 Příklady řešení na cvičení

Poznámka. Nejprve jsme řešili příklady 5.6 a 5.7, které jsou v souboru 5.

Příklad 6.1. V Rabinově kryptosystému zvolila Alice svůj soukromý klíč $p = 19$, $q = 23$, veřejným klíčem je pak $n = p \cdot q = 437$. Zašifrujte pro Alici zprávu $m \equiv 327 \pmod{437}$ a ukažte, jak bude Alice tuto zprávu dešifrovat.

Řešení. Šifrou je $C \equiv M^2 \pmod{n}$, tedy v našem případě je

$$M^2 = 327^2 = 106\,929 \equiv 301 =: C \pmod{437}.$$

Pro dešifrování spočítáme odmocniny modulo p a modulo q. Hledáme r a s tak, že

$$r^2 \equiv 301 \pmod{19} \qquad\qquad s^2 \equiv 301 \pmod{23}.$$

Z řešení kvadratických kongruencí (viz příklady 4.6 a 4.7) máme

$$r \equiv \pm 301^{\frac{19+1}{4}} \pmod{19} \qquad\qquad s \equiv \pm 301^{\frac{23+1}{4}} \pmod{23}.$$

Zbývá tedy spočítat mocniny 301^5 modulo 19 a 301^6 modulo 23. Máme

$$301 \equiv -3 \pmod{19} \qquad\qquad 301 \equiv 2 \pmod{23},$$

tudíž díky $\pm$ u odmocnin vidíme, že

$$r \equiv \pm 3^5 = \pm 9 \cdot 27 \equiv \pm 9 \cdot 8 = \pm 72 \equiv \mp 4 \pmod{19}$$

a

$$s \equiv \pm 2^6 = 64 \equiv \mp 5 \pmod{23}.$$

Pak pro každou dvojici (ze čtyř) r a s hledáme M takové, že $M \equiv r \pmod{19}$ a $M \equiv s \pmod{23}$. Tedy řešíme čtyři soustavy kongruencí

$$\begin{aligned} M &\equiv \pm 4 \pmod{19}, \\ M &\equiv \pm 5 \pmod{23}. \end{aligned}$$

Například pro $r = 4$ a $s = 5$ máme z první kongruence $M = 19\,k + 4$, dosazením do druhé kongruence dostaneme

$$\begin{aligned} 19\,k + 4 &\equiv 5 \pmod{23} \\ 19\,k &\equiv 1 \pmod{23} \\ -4\,k &\equiv 1 \pmod{23} \\ 4\,k &\equiv -1 \pmod{23} \end{aligned}$$

odkud vynásobením 6 dostaneme

$$24\,k \equiv k \equiv -6 \pmod{23}$$

tedy $k = 23\,l - 6$ a $M = 437\,l - 110$, tedy $M \equiv -110 \equiv 327 \pmod{437}$. Je jasné, že pro dvojici $r = -4$ a $s = -5$ bychom dostali $M \equiv 110 \pmod{437}$. (Mohli jsme si z první

kongruence vyjádřit $M = -19\,k - 4$, dosazením do druhé by se opět řešení jen vynásobilo -1.) Pro dvojici $r = 4$, $s = -5$ bychom dostali z první kongruence opět $M = 19\,k + 4$, následně bychom řešili kongruenci

$$\begin{aligned} 19\,k + 4 &\equiv -5 \pmod{23} \\ 19\,k &\equiv -9 \pmod{23} \\ -4\,k &\equiv -9 \pmod{23} \\ 4\,k &\equiv 9 \pmod{23} \end{aligned}$$

a opět vynásobením 6 dostaneme

$$24\,k \equiv k \equiv 54 \equiv 8 \pmod{23}$$

tedy $k = 23\,\ell + 8$ a $M = 437\,\ell + 156$, tedy $M \equiv 156 \pmod{437}$. Opět volbou $r = -4$, $s = 5$ bychom jednoduše dostali $M \equiv -156 \equiv 281 \pmod{437}$. Tedy máme 4 kandidáty pro původní zprávu, $M \equiv 110$ nebo 156 nebo 281 nebo 327 $\pmod{437}$. Například domluvou (nebo kódem) bychom pak zjistili, že $M \equiv 327 \pmod{437}$. △

Příklad 6.2. Vyřešte diofantickou rovnici $21\,x + 34\,y = 1\,597$, prvně nad $\mathbb{Z}$, pak nad $\mathbb{N}_0$.

Řešení. Nejprve si vyjádříme x. Máme

$$21\,x = 1\,597 - 34\,y.$$

Vidíme, že rovnice má nad $\mathbb{Z}$ řešení, pokud bude pravá strana dělitelná 21, neboli platí-li kongruence $34\,y \equiv 1\,597 \pmod{21}$. Tuto si můžeme zjednodušit a dále řešit

$$13\,y \equiv 1 \pmod{21}$$

vynásobením 5 dostaneme

$$2\,y \equiv 5 \pmod{21}$$

neboť $65 \equiv 2 \pmod{21}$, z čehož následně vynásobením 11 máme

$$y \equiv 13 \pmod{21}$$

protože $22 \equiv 1$ a $55 \equiv 13 \pmod{21}$. Tedy $y = 21\,k + 13$. Dosazením do původní rovnice řešíme vzhledem k x.

$$\begin{aligned} 21\,x + 34\,(21\,k + 13) &= 1\,597 \\ 21\,(x + 34\,k) &= 1\,155 \\ x + 34\,k &= 55 \\ x &= 55 - 34\,k \end{aligned}$$

Vidíme tedy, že řešeními jsou všechny dvojice

$$(x, y) = (55 - 34\,k, 13 + 21\,k), \quad k \in \mathbb{Z}.$$

Chceme-li řešit rovnici nad $\mathbb{N}_0$, uvažujeme ještě omezující podmínky $x \geq 0$, $y \geq 0$. Podmínka pro x je tvaru

$$55 - 34\,k \geq 0,$$

neboli

$$k \leq \frac{55}{34} < \frac{68}{34} = 2.$$

Podmínka pro y dává

$$13 + 21\,k \geq 0,$$

neboli

$$k \geq -\frac{13}{21} > -\frac{21}{21} = -1.$$

Tedy k může být jedině 0 nebo 1. Dostáváme tedy jediná dvě řešení nad $\mathbb{N}_0$ (i nad $\mathbb{N}$), dvojice $(55, 13)$ nebo $(21, 34)$. △

Příklad 6.3. Vyřešte diofantickou rovnici $50\,x + 70\,y + 57\,z = 1\,234$, nejprve nad $\mathbb{Z}$, pak nad $\mathbb{N}_0$.

Řešení. Můžeme si rovnici psát jako

$$10\,(5\,x + 7\,y) = 1\,234 - 57\,z,$$

odkud vidíme, že pravá strana rovnice musí být dělitelná 10, neboli musí být $57\,z \equiv 1\,234 \pmod{10}$. Po zjednodušení řešíme kongruenci $7\,z \equiv 4 \pmod{10}$. Vynásobením 3 dostaneme $z \equiv 2 \pmod{10}$ ($3 \cdot 7 = 21 \equiv 1$ a $3 \cdot 4 = 12 \equiv 2 \pmod{10}$), neboli $z = 10\,k + 2$. Dosazením do původní rovnice dostaneme rovnici

$$\begin{aligned} 50\,x + 70\,y + 570\,k + 114 &= 1\,234 \\ 50\,x + 70\,y + 570\,k &= 1\,120 \end{aligned}$$

což můžeme vydělit 10

$$5\,x + 7\,y + 57\,k = 112 \tag{6.1}$$

přičemž nyní můžeme rovnou počítat modulo 5 (opět $112 - 57\,k - 7\,y$ musí být dělitelné 5). Dostaneme kongruenci

$$2\,y + 2\,k \equiv 2 \pmod{5}$$

kterou můžeme vydělit 2 (protože $(2, 5) = 1$) a získat vyjádření $y \equiv 1 - k \pmod{5}$, neboli $y = 1 - k + 5\,l$. Dosazením do (6.1) vyřešíme pro x.

$$5\,x + 7 - 7\,k + 35\,l + 57\,k = 112$$

$$5\,(x + 10\,k + 7\,l) = 105$$

což můžeme vydělit 5

$$\begin{aligned} x + 10\,k + 7\,l &= 21 \\ x &= 21 - 10\,k - 7\,l. \end{aligned}$$

Nad $\mathbb{Z}$ jsou tedy řešeními všechny trojice tvaru

$$(x, y, z) = (21 - 10\,k - 7\,l, 1 - k + 5\,l, 2 + 10\,k), \quad k,\, l \in \mathbb{Z}.$$

Nad $\mathbb{N}_0$ musíme opět važovat omezení $x \geq 0$, $y \geq 0$, $z \geq 0$. Vzhledem k tomu, že z je parametricky vyjádřeno jen pomocí k, máme ihned omezení $10\,k + 2 \geq 0$, neboli

$$k \geq -\frac{1}{5} > -1,$$

tedy $k \geq 0$. Poté z omezení pro y dostaneme

$$1 \geq k - 5\,l \geq,$$

neboli

$$l \geq \frac{k-1}{5} \geq -\frac{1}{5} > -1$$

kde poslední nerovnost platí, protože je $k \geq 0$. Vidíme, že musí být $l \geq 0$. Jedná se však o dolní odhad pro l, nicméně vždy musí být $l \geq \left\lceil \frac{k-1}{5} \right\rceil$. Musíme tedy kontrolovat, jestli je v daném řešení skutečně $y \geq 0$.

Omezení pro x je ekvivalentní nerovnosti $10\,k + 7\,l \leq 21$. Vidíme, že pro $k \geq 3$ nebo $l \geq 4$ jistě neplatí, jelikož k i l jsou nezáporná. Můžeme postupně procházet například všechny možnosti k a dívat se na omezení pro l.

- $k = 0$: Zde dostaneme $7\,l \leq 21$, neboli $l \leq 3$. Máme tak dvojice parametrů $(0, 0)$, $(0, 1)$, $(0, 2)$ nebo $(0, 3)$, odpovídající trojicím $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$, $(0, 16, 2)$, přičemž všechna tato řešení jsou nad $\mathbb{N}_0$.

- $k = 1$: Máme omezení $7\,l \leq 11 < 14$, neboli $l < 2$. Máme možné parametrické dvojice $(1, 0)$ a $(1, 1)$, které odpovídají trojicím řešení $(10, 0, 12)$ a $(4, 5, 12)$, obě nad $\mathbb{N}_0$.

- $k = 2$: Dostaneme omezení $7\,l \leq 1$, tedy může být jedině $l = 0$. Dosteneme trojici řešení $(1, -1, 22)$, přičemž toto řešení již není nad $\mathbb{N}_0$. To je proto, že není splněna podmínka pro y, jelikož zde $5\,l = 0$ a $k = 2$, tedy $y = 1 - 2 = -1 < 0$.

Nad $\mathbb{N}_0$ tedy máme jen 6 řešení, jsou to trojice (x, y, z) tvaru $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$, $(0, 16, 2)$, $(10, 0, 12)$ nebo $(4, 5, 12)$. (Nad $\mathbb{N}$ bychom dostali 4 řešení – $(21, 1, 2)$, $(14, 6, 2)$, $(7, 11, 2)$ a $(4, 5, 12)$.) $\triangle$