1. Čínska veta o zvyškoch

Uvažujme dvojicu lineárnych kongruencií

$$3x \equiv 2 \pmod 5,$$
$$x \equiv 2 \pmod 3.$$

Nech $x \in \mathbb{Z}$ je číslo vyhovujúce prvej kongruencii napríklad $x = 4$. Ohľadne riešenia tejto lineárnej kongruencie vieme, že riešením je presne zvyšková trieda $[4]_5$. Teraz budeme chvíľu sledovať aj jednotlivé celé čísla, nielen celú zvyškovú triedu. Vidíme, že síce

$$3 \cdot 4 \equiv 2 \pmod 5,$$

ale druhej kongruencii toto číslo už nevyhovuje:

$$4 \not\equiv 2 \pmod 3.$$

Avšak niektoré z čísel zvyškovej triedy $[4]_5$ sú aj riešením druhej kongruencie, napríklad $x = 14$.

Toto pozorovanie o chvíľu zovšeobecníme. No bude výhodné ho trochu preformulovať. Kongruencia

$$3x \equiv 2 \pmod 5$$

je ekvivalentná kongruencii

$$x \equiv 4 \pmod 5.$$

Hľadáme teda také celé číslo x, pre ktoré platí

$$x \equiv 4 \pmod 5,$$
$$x \equiv 2 \pmod 3.$$

Už vieme, že $x = 14$ je riešením. Lahko sa tiež presvedčíme, že každé číslo zo zvyškovej triedy $[14]_{15}$ je riešením oboch kongruencií; takže znovu ako riešenie dostávame celú zvyškovú triedu modulo $15 = 5 \cdot 3$.

Existenciou takýchto čísel vo všeobecnosti sa zaoberá nasledujúce tvrdenie.

Veta 1.1 (Čínska veta o zvyškoch). Nech $n_1, n_2, \ldots, n_k$ sú po dvoch navzájom nesúdeliteľné prirodzené čísla, t.j. $(n_i, n_j) = 1 \ \forall i \neq j$. Nech ďalej $b_1, b_2, \ldots, b_n$ sú ľubovoľné celé čísla. Potom existuje také $x \in \mathbb{Z}$, že

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \\ &\ldots \\ x &\equiv b_k \pmod{n_k}. \end{aligned} \tag{1}$$

Navyše, ak $\tilde{x}$ ďalším celým číslom, ktoré vyhovuje všetkým kongruenciám, potom

$$\tilde{x} \equiv x \pmod N,$$

kde $N = n_1 n_2 \ldots n_k$,

Stručnejšie možno túto vetu sformulovať aj tak, že sústava kongruencií (1) má jediné riešenie modulo N.

Dôkaz. Prvé rýchle pozorovanie hneď odhalí, že ak $x \in \mathbb{Z}$ je riešením všetkých kongruencií, potom aj každé ďalšie $\tilde{x}$ také, že $\tilde{x} \equiv x \pmod N$ je riešením: $\tilde{x} \equiv x \pmod N$ znamená, že $N \mid (\tilde{x} - x)$. Potom pre všetky $i = 1, \ldots, k$ spolu s $n_i \mid N$ dostávame $n_i \mid (\tilde{x} - x)$, čo znamená $\tilde{x} \equiv x \pmod{n_i}$. Odtiaľ $\tilde{x} \equiv b_i \pmod{n_i}$.

Nech teraz x a $\tilde{x}$ sú dve riešenia sústavy kongruencií (1). Máme tak, že $\tilde{x} \equiv b_i \pmod{n_i}$, t.j.

$$\begin{aligned} n_1 \mid x - \tilde{x}, \\ n_2 \mid x - \tilde{x}, \\ \dots \\ n_k \mid x - \tilde{x}. \end{aligned}$$

Keďže n_i sú po dvoch nesúdeliteľné, z vlastností deliteľnosti indukciou dostávame, že

$$N \mid x - \tilde{x}$$

a teda x a $\tilde{x}$ patria tej istej zvyškovej triede modulo N.

Potrebujeme ešte overiť, že riešenie sústavy (1) naozaj existuje. To ukážeme indukciou na k.

Nech najprv $k = 2$, teda máme dve kongruencie

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \end{aligned}$$

kde $(n_1, n_2) = 1$. Existujú preto také celé u, v, že

$$un_1 + vn_2 = 1.$$

Potom

$$c = un_1b_2 + vn_2b_1$$

je hľadané riešeie:

$$c = un_1b_2 + (1 - un_1)b_1 = b_1 + un_1(b_2 - b_1),$$

t.j. $c \equiv b_1 \pmod{n_1}$. Druhú kongruenciu overíme analogicky.

Ak $k > 2$, nech c je riešením prvých dvoch kongruencií

$$\begin{aligned} x &\equiv b_1 \pmod{n_1}, \\ x &\equiv b_2 \pmod{n_2}, \end{aligned}$$

Pôvodné kongruencie (1) nahradíme $k - 1$ kongruenciami

$$\begin{aligned} x &\equiv c \pmod{n_1n_2}, \\ x &\equiv b_3 \pmod{n_3}, \\ &\dots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

Zjavne ich riešenie je aj riešením (1) a naopak. Z indukčného predpokladu tak plynie dokazované tvrdenie. □

Príklad 1.2. Nájdime spoločné riešnie kongruencií

$$\begin{aligned} 2x &\equiv 1 \pmod{3}, \\ 3x &\equiv 1 \pmod{4}, \\ x &\equiv 0 \pmod{5}. \end{aligned}$$

Každá z týchto kongruencií je riešiteľná a má jediné riešenie v príslušnej zvyškovej triede. Sústavu si po vyriešení jednotlivých kongruencií preto vieme následne prepísať na ekvivalentnú sústavu:

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{4}, \\ x &\equiv 0 \pmod{5}. \end{aligned}$$

Pre nájdenie riešenia postupujeme ako v dôkaze vety. Uvažujeme najprv prvé dve kongruencie

$$x \equiv 2 \pmod 3),$$
$$x \equiv 3 \pmod 4).$$

Vyjadríme 1 ako kombináciu 3 a 4

$$1 = (-1) \cdot 3 + 1 \cdot 4$$

a toto vyjadrenie použijeme na konštrukciu spoločného riešenia týchto dvoch kongruencií:

$$c_1 = (-1) \cdot 3 \cdot 3 + 1 \cdot 4 \cdot 2 = -1 \equiv 11 \pmod{12}.$$

Pôvodnú trojicu teraz nahradíme dvojicou kongruencií

$$x \equiv 11 \pmod{12},$$
$$x \equiv 0 \pmod 5)$$

a tým istým postupom pokračujeme v riešení:

$$1 = (-2) \cdot 12 + 5 \cdot 5$$
$$c_2 = (-2) \cdot 12 \cdot 0 + 5 \cdot 5 \cdot 11 = 275 \equiv 35 \pmod{60}.$$

Riešením trojice kongruencií je zvyšková trieda $[35]_{60}$.

2. Algoritmus RSA (Rivest–Shamir–Adleman)

Ide o tzv. asymetrickú šifrovaniu schému, keď sa na odšifrovanie správ používa iný kľúč ako na ich zašifrovanie. Kľúč na zašifrovanie správ sa tak môže zverejniť, keďže jeho znalosť umožňuje správy iba zašifrovať, no nie už odšifrovať.

Vysvetlíme si tento algoritmus v dvoch krokoch: najprv si ukážeme princíp využitia Eulerovej vety pri dôkaze fungovania tejto šifrovacej schémy. Potom si ukážeme, ako sa algoritmus reálne používa, aby išlo naozaj o asymetrické kľúče, a znovu overíme jeho fungovanie.

2.1. Ako RSA využíva Eulerovu vetu.

Verejný kľúč, kľúč na zašifrovanie (zvolíme):

p: prvočíslo (tzv. *modulus*)
e: $e \in \{1, 2, \ldots, p-2\}$, $(e, p-1) = 1$

Súkromný kľúč, kľúč na odšifrovanie (dopočítame):

d: $de \equiv 1 \pmod{p-1}$

Keďže e a $p-1$ sú nesúdeliteľné, diofantická rovnica

$$ex + (p-1)y = 1$$

má jediné riešenie také, že $x \in \{1, 2, \ldots, p-2\}$. Toto x v riešení je hľadané d.

Šifrovanie:

m: $m \in \{0, 1, \ldots, p-1\}$ – správa,
c: $c \equiv m^e \pmod p$ – zašifrovaná správa.

Potom

$$m \equiv c^d \pmod p$$

je odšifrovaná správa.

Dôkaz. Ak $c \neq 0$, potom $(c, p) = 1$ a podľa Eulerovej vety

$$c^{p-1} \equiv 1 \pmod p.$$

Preto

$$c^d = (m^e)^d = m^{ed} = m^{1+z\cdot(p-1)} = m \cdot m^{(p-1)^z} \equiv m \cdot 1 \pmod{p} = m.$$

Prípad $c = 0$ nastáva, len ak pôvodná správa $m = 0$, a vtedy triviálne $c^d = 0 = m$. □

Problém: ak poznáme verejný kľúč, t.j. dvojicu (p, e), ľahko si Euklidovým algoritmom dopočítame súkromný kľúč (d) na odšifrovanie správ. Táto schéma teda v skutočnosti nie je asymetrická: znalosť verejného kľúča nám umožňuje dopočítať súkromný. Inak: ak správu vieme zašifrovať, vieme ju dostupnými výpočtovými prostriedkami aj odšifrovať.

2.2. RSA as it is.
Voľba a výpočet kľúčov:

p, q: prvočísla – zvolíme
n: $n = pq$ (modulus) – vypočítame; pre n tiež platí $\varphi(n) = (p-1)(q-1)$
e: $e \in \{1, 2, \ldots, \varphi(n) - 1\}$, $(e, \varphi(n)) = 1$ – zvolíme
d: $de \equiv 1 \pmod{\varphi(n)}$, $0 < d < \varphi(n)$ – vypočítame

Aj v tomto prípade d dopočítame Euklidovým algoritmom a vďaka podmienke $(e, \varphi(n)) = 1$ bude existovať jediné také, že $0 < d < \varphi(n)$. Čiže máme

- verejný kľúč, kľúč na zašifrovanie: (e, n) (zverejníme),
- súkromný kľúč, kľúč na odšifrovanie: d (držíme v tajnosti).

Šifrovanie:

m: $m \in \{0, 1, \ldots, n-1\}$ – správa,
c: $c \equiv m^e \pmod{n}$ – zašifrovaná správa.

Potom

$$m \equiv c^d \pmod{n}$$

je odšifrovaná správa.

Dôkaz. Tvrdenie je triviálne ak $m = 0$. Vtedy aj $c = 0$ a naopak. Inak (m a c sú nenulové) rozlíšime dva prípady.

(1) Ak $(m, n) = 1$, pri dôkaze postupujeme presne ako v prvom náčrte algoritmu: znovu máme

$$c^d = (m^e)^d = m^{ed} = m^{1+z\varphi(n)} = m \cdot m^{\varphi(n)^z} \equiv m \pmod{n},$$

kde posledná kongruencia vyplýva z (Eulerova veta)

$$m^{\varphi(n)} \equiv 1 \pmod{n}.$$

(2) Ak $(m, n) \neq 1$, potom buď $p \mid m$ alebo $q \mid m$. Oboma prvočíslami správa m určite nie je deliteľná: znamenalo by to, že $m = 0$, no tento prípad sme už vylúčili. Nech napríklad $p \mid m$. Z

$$m \equiv 0 \pmod{p}$$
$$m^{ed} \equiv 0 \pmod{p}$$

usúdime

$$m^{ed} \equiv m \pmod{p}.$$

Teraz sa pozrime na $c^d = m^{ed}$ modulo q:

$$m^{ed} = m^{1+z\varphi(n)} = m \cdot m^{\varphi(n)^z} = m \cdot m^{z(p-1)(q-1)} = m \cdot (m^{q-1})^{z(p-1)} \equiv m \pmod{q},$$

lebo $(m, q) = 1$ (znovu sme použili Eulerovu vetu). Platí teda, že

$$m \equiv m^{ed} \pmod{p}$$
$$m \equiv m^{ed} \pmod{q}$$

Podľa Čínskej vety o zvyškoch existuje jediné také $x \in \mathbb{N}$, $x < n$, pre ktoré platí

$$x \equiv m \pmod{p}$$
$$x \equiv m \pmod{q}$$

a zjavne $x = m$ je hľadaným riešením. To znamená, že

$$m^{ed} \equiv m \pmod{n}.$$

□