10. Troška z teórie čísiel

Faktorizácia faktoriálu

$$n! = \prod_{k=1}^{n} k, \quad \text{pre } n \geq 0.$$

S faktoriálmi sa stretávame v diskrétnej matematike často. Sú to veľmi veľké čísla, končiace kopou núl. Z kombinatoriky si pamätáme, že $n!$ je počet poradí, ktorými sa dá n rôznych objektov zoradiť do radu. Namiesto počítania faktoriálu, skúsme ho vyjadriť ako súčin prvočísiel, alebo inak povedané rozložiť ho na prvočinitele.

Pre dané prvočíslo p chceme určiť jeho maximálnu mocninu, ktorou je $n!$ deliteľný. Označme ho $\epsilon_p(n!)$. Ako vždy skúsme úlohu vyriešiť pre malé hodnoty neznámych. Napríklad pre $p = 2$ a $n = 10$ dostaneme

$n! =$	$1{\cdot}2{\cdot}3{\cdot}4{\cdot}5{\cdot}6{\cdot}7{\cdot}8{\cdot}9{\cdot}10$					
deliteľné 2	x	x	x	x	x	$5 = \lfloor \frac{10}{2} \rfloor$
deliteľné 4		x		x		$2 = \lfloor \frac{10}{4} \rfloor$
deliteľné 8				x		$1 = \lfloor \frac{10}{8} \rfloor$

Celkový exponent 2 v prvočíselnom rozklade dostaneme tak, že spočítame koľkými k nemu prispievajú mocniny 2. Keď si všimneme riadky v tabuľke vidíme, že k mocnine 2^1 v $10!$ prispeje každý druhý činiteľ, čo je $\lfloor \frac{10}{2} \rfloor$. K mocnine 2^2 prispeje každý štvrtý, teda $\lfloor \frac{10}{4} \rfloor$ a k 2^3 každý ôsmy. Preto je $\epsilon_2(10!) = 8$.

Inak zapísané, pre všeobecné n

$$\epsilon_2(n!) = \left\lfloor \frac{n}{2^1} \right\rfloor + \left\lfloor \frac{n}{2^2} \right\rfloor + \left\lfloor \frac{n}{2^3} \right\rfloor + \cdots = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor .$$

Suma je konečná lebo od nejakého k (keď $2^k > n$) už budú všetky sčítance rovné nule.

Po zovšobecnení na ľubovoľné prvočíslo p dostaneme rovnakou úvahou ako pred chvíľou

$$\epsilon_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Aké je $\epsilon_p(n!)$ veľké? Keď vynecháme dolné celé časti, pravú stranu zväčšíme, bude platiť

$$\epsilon_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) = \frac{n}{p-1}$$

Odhad $\epsilon_p(n!)$ nám umožní odhadnúť $p^{\epsilon_p(n!)}$,

$$p^{\epsilon_p(n!)} < p^{\frac{n}{p-1}}.$$

Keď uvážime, že $p \leq 2^{p-1}$, môžeme pravú stranu uvedenej nerovnosti odhadnúť zhora

$$p^{\frac{n}{p-1}} < \left(2^{p-1}\right)^{\frac{n}{p-1}} = 2^n.$$

Inými slovami, príspevok ľubovoľného prvočísla v $n!$ je menej než 2^n. Načo je to dobré? Napríklad keby existovalo iba k rôznych prvočísiel $2, 3, \ldots, p_k$, muselo by platiť pre všetky n, že $n! < (2^n)^k$. Čo očividne nie je pravda, keď si zvolíme dostatočne veľké n. Nech povedzme $n = 2^{2k}$, dostaneme

$$n! < (2^n)^k = \left(2^{2^{2k}}\right)^k = 2^{k2^{2k}} = 2^{2k\frac{2^{2k}}{2}} = n^{\frac{n}{2}}.$$

Dostali sme spor s tým, že $n! > n^{n/2}$ (8.6). Prvočísiel musí byť teda nekonečne veľa.

A to ešte nie je všetko! Rovnaký argument nám pomôže odhadnúť $\pi(n)$, počet prvočísiel neprevyšujúcich n. Každé také prvočíslo prispieva k $n!$ činiteľom menším než 2^n. Teda $n! < 2^{n\pi(n)}$. Keď nahradíme $n!$ Stirlingovým odhadom (8.7) a obe strany zlogaritmujeme dostaneme odhad $n\log(n/e) + \frac{1}{2}\log 2\pi n < n\pi(n)$ odkiaľ máme, že

$$\pi(n) > \log(n/e).$$

Odhad to nie je najlepší, ale ani sme sa veľmi nenamáhali pri jeho odvodení.

Legendreove sito

Keď poznáme prvočísla $\leq \sqrt{x}$, určíme počet prvočísiel $\leq x$, $\pi(x)$. Napríklad určime počet prvočísiel ≤ 28, keď poznáme prvočísla $\leq \sqrt{28}$, t.j. $p_1 = 3, p_2 = 5, p_3 = 7$. Označme A_i, množinu obsahujúcu násobky prvočísla p_i, $1 \leq i \leq 3$, z množiny $X = \{2, 3, \ldots, 28\}$. Zaujíma nás počet prvkov z množiny X, ktoré nepatria do žiadnej z množín A_i, to budú len tie, ktoré nie sú deliteľné číslom $\leq \sqrt{28}$, teda prvočísla. Ale to je predsa z kombinatoriky známy princíp inklúzie a exklúzie – chceme určiť $|X| - |A_1 \cup A_2 \cup A_3|$. Počet prvkov v množinách $|A_i \cap A_j|$, $1 \leq i < j \leq 3$, je počet čísiel z X deliteľných súčasne p_i a p_j, tých je $\lfloor 28/(p_i p_j)\rfloor$. Po dosadení dostaneme $\pi(28) - \pi(\sqrt{28}) = 6$, keďže prvočísla $\leq \sqrt{28}$ poznáme, vieme aj $\pi(\sqrt{28})$. Hľadaný výsledok $\pi(28) = 9$.

Vo všeobecnosti pre ľubovoľné x je $X = \{2, 3, \ldots, \lfloor x\rfloor\}$. Označme $p_1 < p_2 < \cdots < p_k \leq \sqrt{x}$, $A_i = \{a \in X \mid p_i | a\}$. $M(j_1, j_2, \ldots j_m) = |A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_m}|$ je počet prvkov X deliteľných súčasne p_{j_1} až p_{j_m} a rovná sa $\left\lfloor \frac{x}{p_{j_1} p_{j_2} \cdots p_{j_m}} \right\rfloor$. $M(0) = \lfloor x\rfloor - 1$. Využitím princípu inklúzie a exklúzie (8.5) spočítame $|A_1 \cup A_2 \cup \cdots \cup A_k|$ a dosadíme do $M(0) - |A_1 \cup A_2 \cup \cdots \cup A_k| = \pi(x) - \pi(\sqrt{x})$.

Adrien Marien Legendre (1752-1833) bol francúzsky matematik, ktorý okrem iných kníh vydal aj dvojzväzkovú Teóriu čísiel, kde sa zaoberal aj počtom prvočísiel.

Testovanie prvočíselnosti

Je n prvočíslo? Naivné testovanie, či je n prvočíslo postupným delením 2 a všetkými nepárnymi $2 \leq k \leq \sqrt{n}$ nie je prakticky možné. (Dôvody sú uvedené v časti rýchle umocňovanie.) Pokiaľ n nie je deliteľné žiadnym k, je prvočíslo, pokiaľ je niektorým deliteľné, máme dôkaz, že n je zložené. Teda sme sa dozvedeli viac ako sme sa pýtali. Je možné, že táto nevyžiadaná pridaná hodnota odpoveď tak predražila. Stále ostáva nádej, že odpoveď áno/nie bude lacnejšia – prakticky zistiteľná.

Rýchle umocňovanie

Základnou operáciou v takmer všetkých aplikáciách, ktoré spomíname v tejto časti je výpočet $x^y \bmod n$. Uvedomte si, že vypočítať najprv x^y a potom zistiť zvyšok po delení n nie je prakticky možné, lebo pracujeme s veľkými číslami – niekoľko desiatok cifier. Nepomohlo by ani keby sme počítali x^y postupným násobením x a po každom násobení by sme vykonali mod n, teda vlastne by sme počítali $x^y \bmod n = x \cdot (x^{y-1} \bmod n) \bmod n$.

Keď číslo zapíšeme v nejakej sústave po cifrách dostaneme $b_k b_{k-1} \dots b_1 b_0$. Ak zoberieme vykonanie aritmetickej operácie s dvoma ciframi za jednotku zložitosti, vynásobiť alebo vydeliť dve $k+1$ ciferné čísla si vyžaduje $O(k^2)$ aritmetických operácií. V druhom spôsobe výpočtu $x^y \bmod n$ by sme pracovali najviac s číslami n^2. Nech $n = b_k b_{k-1} \dots b_1 b_0$, potom $k+1 = \lfloor \log n \rfloor + 1$. Teda celkovo by sme potrebovali $O(k^y)$ operácií. Po dosadení za k máme $O\left((\lfloor \log n \rfloor)^y\right)$, čo je exponenciálne od počtu cifier n.

Aby sme dostali prakticky použiteľný algoritmus, t.j. taký ktorý nevyžaduje exponenciálne veľa operácii, musíme si nejako pomôcť. Skúsme si zapísať ešte raz definíciu x^y, predpokladajme, že $x \neq 0$:

$$x^y = \begin{cases} 1, & \text{keď } y = 0, \\ \left(x^2\right)^{\frac{y}{2}}, & \text{keď je } y \text{ párne}, \\ x x^{y-1}, & \text{keď je } y \text{ nepárne}. \end{cases}$$

Je to lepší spôsob než predchádzajúci. Nevšímajme si zatiaľ, že sme vynechali operácie mod n. Koľko násobení vyžaduje tento spôsob? Násobenie sa vyskytuje iba v druhom a treťom prípade. V druhom je jedno násobenie a rekurzívne sa počíta rovnaká funkcia, ale exponent sa zmenšil na polovicu. V treťom prípade je jedno násobenie a exponent sa zmenšil o 1. Všimnite si, že v najhoršom prípade budeme postupovať striedavo podľa tretieho a druhého prípadu, kým neprídeme k prvému prípadu. Ale druhý prípad môže nastať iba $\log y$ krát! Teraz si môžeme doplniť definíciu o operácie mod n. Treba ich vykonávať priebežne z rovnakého dôvodu ako predtým. Všimnite si, že tretí prípad sa dá upraviť dosadením, lebo vieme, že $y-1$ bude párne. Dostaneme:

$$x^y \bmod n = \begin{cases} 1, & \text{keď } y = 0, \\ \left(x^2 \bmod n\right)^{\frac{y}{2}} \bmod n, & \text{keď je } y \text{ párne}, \\ x \left(x^2 \bmod n\right)^{\frac{y-1}{2}} \bmod n, & \text{keď je } y \text{ nepárne}. \end{cases}$$

Teraz vidíme, prečo sa tomuto spôsobu hovorí *umocňovanie postupným umocňovaním na druhú*. Z praktického hľadiska ešte treba prepísať definíciu aby bola chvostovo rekurzívna, t.j. aby sme ju vedeli naprogramovať cyklom. Použijeme techniku akumulátora (po slovensky sumátora). Chvostovú rekurziu kazí tretí prípad. Aby sme odstránili túto prekážku, zadefinujme funkciu u takú, že zachováva invariant $u(a,b,s) = a^b \cdot s \bmod n$. Je zrejmé, že našu funkciu $x^y \bmod n$ získame ako $u(x,y,1)$. Aká ale bude definícia funkcie u?

$$u(a,b,s) = \begin{cases} v, & \text{keď } b = 0 \\ u(\left(a^2 \bmod n\right)^{\frac{b}{2}} \bmod n, v), & \text{keď je } b \text{ párne}, \\ u(\left(a^2 \bmod n\right)^{\frac{b-1}{2}} \bmod n, av \bmod n) & \text{keď je } b \text{ nepárne}. \end{cases}$$

Overte si, že definícia zachováva horeuvedený invariant. Na výpočet x^y pomocou funkcie u potrebujeme len $O\left((\lfloor \log n \rfloor)^{\log y}\right)$ operácií.

Millerov test prvočíselnosti

Pripomeňme si *malú Fermatovu vetu*. Piere Fermat (1601–1665) bol francúzsky právnik a matematik - samouk.

Veta. *Nech p je prvočíslo a a ľubovolné číslo, potom $a^p \equiv a \pmod p$. Keď $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod p$.*

Dôkaz. V prípade $p \nmid a$ je to dôsledok Eulerovej vety (). V prípade $p \mid a$, sú obe a^p aj $a \equiv 0 \pmod p$.

♠

Keď chceme overiť, či je p prvočíslo, nemôžeme využiť predchádzajúcu vetu, lebo opačná implikácia nanešťastie neplatí. Netreba sa vzdávať. Môžeme využiť, že ak nejaké n je prvočíslo, musí byť $a^{n-1} \equiv 1 \pmod n$. Teda ak $a^{n-1} \not\equiv 1 \pmod n$ isto vieme, aspoň to, že n zaručene nie je prvočíslo.

Keď začneme s nepárnym prvočíslom n, podľa Fermatovej vety musí platiť, že $a^{n-1} \equiv 1 \pmod n$, $n-1$ je párne, môžeme spočítať $x = a^{\frac{n-1}{2}}$. Pretože $x^2 \equiv 1 \pmod n$, musí byť $x \equiv \pm 1 \pmod n$. Ak $x = 1$ a $\frac{n-1}{2}$ je párne, môžeme pokračovať rovnakým spôsobom a zrátať $y = a^{\frac{n-1}{4}}$. Z rovnakých dôvodov ako predtým, pretože $y^2 \equiv 1 \pmod n$, musí byť $y \equiv \pm 1 \pmod n$. Takto môžeme pokračovať, pokým neskončíme s -1, alebo nepárnym exponentom (môžu nastať aj oba prípady súčasne). Intuitívne je idea zrejmá, zložené číslo sa len ťažko zamaskuje za prvočíslo. Dostali sme test, ktorý navrhol Gary Lee Miller v roku 1976.

Millerov test prvočíselnosti vzhľadom na bázu a

1. Nech n je nepárne prvočíslo > 1 a nech $(a, n) = 1$.
2. $k := n-1$; $r := a^k \pmod n$;
3. **while** $(r = 1) \wedge (k$ je párne$)$ **do begin**
   $k := k/2$;
   $r := a^k \pmod n$
   end;
   if $(r = 1) \vee (r = n-1)$ **then** Prešiel
   else Neprešiel

Zložené číslo, ktoré prejde testom rovnako, akoby ním prešlo aj prvočíslo, budeme nazývať *silné pseudoprvočíslo vzhľadom na bázu a*. Je zrejmé, že keď je n prvočíslo, nemôže neprejsť Millerovým testom (uvedomte si, že $x \equiv \pm 1 \pmod n$ je $x = 1$ alebo $x = n-1$), čo môžeme sformulovať do nasledujúcej vety.

Veta. *Ak n neprejde Millerovým testom je zložené.*

Pravdepodobnostné testovanie prvočíslenosti

Keď sa pokúsime nájsť najmenšie n, ktoré je súčasne silným pseudoprvočíslom vzhľadom na bázy $3, 5$ a 7, získame podozrenie, že výskyt čísiel, ktoré sú silnými pseudoprvočíslami súčasne vzhľadom na väčší počet báz je veľmi zriedkavý. Ozaj je pravda, že čím väčším počtom Millerových testov číslo prejde, tým je väčšia šanca, že je prvočíslom. Nasledujúcu vetu uvedieme bez dôkazu.

Veta. *Nech n je nepárne zložené číslo. Potom n spĺňa Millerov test najviac pre $(n-1)/4$ báz b, $1 \leq b \leq n-1$.*

Inak povedané, n nemôže byť silným pseudoprvočíslom vzhľadom na všetky bázy. Na to aby sme sa presvedčili, či je je číslo n zložené, by nebolo praktické skúšať všetkých $(n-1)/4$ báz. Keď n prejde Millerovým testom vzhľadom na bázu b, je pravdepodobnosť toho, že sme si zvolili bázu, pri ktorej sa to stane rovná $\frac{1}{4}$. Keď n prejde k Millerovými testami, vzhľadom na rôzne základy, pričom predpokladáme, že boli vybrané „nezávisle“, tak pravdepodobnosť, že je n zložené je $\frac{1}{4^k}$. Presvedčenie, že n je prvočíslo rastie s rastúcim k. Táto metóda sa nazýva *Rabinov pravdepodobnostný test*, lebo ho vymyslel Michael Oser Rabin. Miller ukázal, že za istých špeciálnych predpokladov (že platí rozšírená Riemanova hypotéza) zložené n neprejde testom pre niektorú z báz $< 2(\log n)^2$, čo je pomerne malé číslo aj pre veľmi veľké n.

Verejné prenášanie tajných kľúčov

V roku 1976 vymysleli Whitfield Bailey Diffie a Martin Edward Hellman ako posielať cez nechránený (mohol byť odpočúvaný) komunikačný kanál šifrovací kľúč. Začala sa tým nová éra kryptografie. Základná myšlienka tejto metódy je jednoduchá a využíva tzv. jednosmernú funkciu (t.j. takú, že ju vieme efektívne vypočítať, ale efektívne nevieme vypočítať jej inverznú funkciu.). Keď pomocou takejto funkcie zobrazíme tajnú správu, jej odpočutie nebude mať veľkú cenu, lebo bez dodatočných informácií nebude odpočúvateľ vedieť vypočítať inverznú funkciu.

Nie je zatiaľ dokázané, že jednosmerné funkcie (ne)existujú. Príkladom kandidáta na jednosmernú funkciu je umocňovanie mod n. Nie je (zatiaľ) známy spôsob na výpočet inverznej funkcie – určenie exponentu, tzv. diskrétny logaritmus. Zvolíme si veľké celé čísla $1 < g < n$. Môžu byť verejne známe. Používateľ A si zvolí tajné x_A a používateľ B tajné x_B. Keď sa chcú dohodnúť na tajnom kľúči, A pošle B číslo $g^{x_A} \bmod n$ a B pošle A číslo $g^{x_B} \bmod n$. Obaja môžu vypočítať $g^{x_A x_B} \bmod n$ a to bude ich tajný kľúč. (Je vhodné aby bolo n prvočíslo, potom $1 < g < n$ bude generátor $\mathbb{Z}_n$.)

Opísaný spôsob sa dal použiť priamo aj na šifrovanú komunikáciu, ale na prenesenie jednej správy vyžadoval niekoľko prenesení zašifrovaných správ. Nasledujúca metóda tento nedostaok odstraňuje a prakticky sa používa vo svete okolo nás, možno o tom iba nevieme.

Šifrovanie RSA

Túto metódu vymysleli Ronald Linn Rivest, Adi Shamir, Leonard Max Adleman v roku 1977 na MIT, kde pôsobili vo výskume, publikovaná bola v roku 1978. V roku 2002 získali za prínos k rozvoju šifrovania verejným kľúčom Turingovu cenu.

Zvolíme si veľké prvočísla (aspoň 512 bitov) p a q a vytvoríme ich súčin $n = pq$. Vypočítame $\phi(n) = (p-1)(q-1)$, kde ϕ je Eulerova funkcia. Zvolíme veľké d také, že $(\phi(n), d) = 1$ a dopočítame e, inverzný prvok k $d \pmod{\phi(n)}$, pre ktoré $de \equiv 1 \pmod{\phi(n)}$. Že taký prvok existuje a je určený jednoznačne ukážeme v časti o kongruenciách. Verejný kľúč tvorí dvojica n, e. Tajné sú p, q a d.

Ako prebieha šifrovanie správy? Textovú správu si predstavme ako veľké číslo. Každý znak správy môžeme nahradiť jeho kódom. Toto číslo rozdelíme na po sebe idúce bloky cifier tak, aby každý blok predstavoval číslo $< n$. Bloky sa šifrujú osobitne. V ďalšom budeme označovať W jeden blok pôvodnej správy.

Šifrovanie

Správu W zašifrujeme na základe vzťahu

$$C = W^e \pmod{n}.$$

Keď bude šifrovať človek X budeme to zapisovať ako $E_X(W)$ a bude to znamenať: $C = E_X(W) = W^{e_X} \bmod n_X$.

Dešifrovanie

Šifrovanú správu C dešifrujeme na základe vzťahu

$$W = C^d \pmod{n}.$$

Keď bude dešifrovať človek X budeme to zapisovať ako $D_X(C)$ a bude to znamenať: $W = D_X(C) = C^{d_X} \bmod n_X$.

Veta. *Nech $C = W^e$ (mod n) je šifrovaný text W, $ed \equiv 1$ (mod $\phi(n)$) a $(d, \phi(n)) = 1$, potom $W \equiv C^d$ (mod n). (V prípade jednoznačnosti platí =.)*

Dôkaz. Z $ed \equiv 1 \pmod{\phi(n)}$ vyplýva, že existuje $j \in \mathbb{N}$, pre ktoré platí, že $ed = j\phi(n) + 1$. Uvažujme niekoľko prípadov podľa toho, či p resp. q delí W.

i) Ani p, ani q nedelí W. Teda máme, že $(n, W) = 1$. Môžeme písať

$$C^d \equiv (W^e)^d \equiv W^{j\phi(n)+1} \equiv W \pmod{n}.$$

V poslednej kongruencii sme využili Eulerovu vetu, že pre $x \perp y$ platí $x^{\phi(y)} \equiv 1 \pmod{y}$.

ii) Práve jedno z p, q delí W. Bez straty všeobecnosti predpokladajme, že je to p. Očividne $W^{ed} \equiv W \pmod{p}$ (uvedomte si, že keď $p|W$, tak $W^{ed} \equiv 0 \pmod{p}$). Využitím malej Fermatovej vety máme $W^{q-1} \equiv 1 \pmod{q}$, teda aj $W^{\phi(n)} \equiv 1 \pmod{q}$ a aj $W^{j\phi(n)} \equiv 1 \pmod{q}$, odkiaľ vyplýva, že $W^{ed} \equiv W \pmod{q}$. Pretože platí aj $W^{ed} \equiv W \pmod{p}$ dostávame

$$C^d \equiv W^{ed} \equiv W \pmod{n}.$$

iii) Prípad, že by súčasne aj p aj q delili W nemôže nastať lebo predpokladáme, že $W < n$.

♠

V skutočnosti je prakticky dôležitý iba prípad i). V prípade ii) by nastali pri ozajstnom použití problémy, lebo na základe vedomosti, že $(n, W) = p$ vieme určiť aj q a všetko je odhalené. Našťastie šanca, že by nastala táto situácia je veľmi malá. Vieme zistiť, aká je? Za predpokladu, že všetky W sú rovnako pravdepodobné, môžeme uvažovať takto: všetkých správ je n. „Bezproblémových“ správ je $\phi(n)$ – toľko je nesúdeliteľných. Teda keď vyberieme náhodne jednu z n možných „problémových“ správ, dostaneme

$$\frac{n - \phi(n)}{n} = \frac{pq - (p-1)(q-1)}{pq} = \frac{1}{p} + \frac{1}{q} + \frac{1}{pq}.$$

Pretože p aj q sú veľmi veľké je zrejmé, že predchádzajúci výraz je veľmi malý.

Prvočísla p a q musíme zvoliť pozorne. Napríklad, keby bol výraz $|p-q|$ malý – teda p a q by boli približne rovnako veľké. Číslo n môžeme vyjadriť nasledovne

$$n = pq = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 = t^2 - s^2.$$

Pričom t bude trocha väčšie než $\sqrt{n}$ a s bude malé. Položme $t = \lfloor\sqrt{n}\rfloor + 1$, spočítajme $t^2 - n$ a zistíme, či je to štvorec, ak nie je, t zvýšime o 1 a opakujeme. Ak sme dostali štvorec, teda platí $t^2 - n = s^2$, máme číslo n rozložené. Dostali sme $n = (t-s)(t+s)$.

Digitálny podpis a posielanie správ

Predstavme si, že osoba A chce poslať správu W osobe B. Má niekoľko možností ako to urobiť.

1. Pošle $E_A(W)$. Všetci ju vedia podpísať. Lebo D_A je verejne známe. Autor správy môže byť len A, nik nemôže v jeho mene posielať správy, bez toho aby vedel jeho tajný kľúč E_A.
2. Pošle $D_B(W)$. Takúto správu vie čítať iba B, iba on pozná E_B. B nemá ale istotu, že správu poslal A, mohol ju poslať hocikto, lebo D_B je verejne známe.
3. Pošle $D_B(E_A(W))$. Iba B ju vie prečítať a iba A ju môže poslať. Z praktických dôvodov sa často posiela so správou W iba krátka správa $E_A(S)$, ktorou sa dá overiť pravosť W (B dostane $D_B(WE_A(S))$). $E_A(S)$ sa zvykne nazývať *podpis*.

Kongruencie

Definícia. *Kongruencia*, označenie $\equiv$. Pre $n \neq 0$

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad a \bmod n = b \bmod n \quad \Longleftrightarrow \quad n|(a-b).$$

Uvedieme iba tie vlastnosti relácie $\equiv$, ktoré v tejto časti využívame.

Veta.

i) *Keď* $a \equiv b \pmod{n}$ *a súčasne* $a \equiv b \pmod{m}$, *potom* $a \equiv b \pmod{(m,n)}$. *Keď* $(m,n) = 1$, *potom* $a \equiv b \pmod{mn}$.

ii) *Keď* $ac \equiv bc \pmod{m}$ *a* $(c,m) = d$, *potom* $a \equiv b \pmod{\frac{m}{d}}$. *Špeciálne keď* $(c,m) = 1$ *je* $a \equiv b \pmod{m}$.

Dôkaz.

i) $n|(a-b)$ a súčasne $m|(a-b)$ teda zrejme aj $(n,m)|(a-b)$. Keď $(n,m) = 1$, z toho, že $n|(a-b)$ a $m|(a-b)$ vyplýva, že $a - b = kn = jm$, teda $m|kn$ a $n|jm$, pre nejaké k a j. Z posledného máme, že $n|j$, inak zapísané $j = in$, pre nejaké i. Odkiaľ už vyplýva, že $a - b = imn$, čo sme chceli ukázať.

ii) Prepíšeme tvrdenie: $ac - bc = km$, pre nejaké k. Nech $c = c_1 d$ a $m = m_1 d$, potom po dosadení $m_1 d|(ac_1 d - bc_1 d)$, odkiaľ $m_1|(a-b)c_1$, ale keďže $(m_1, c_1) = 1$ máme $m_1|a-b$, čo sme chceli ukázať. (Keď $(c,m) = d$, potom $(\frac{c}{d}, \frac{m}{d}) = (c_1, m_1) = 1$, lebo inak by nebolo $(c,m) = d$.)

♠

Definícia. *Eulerova funkcia,* $\phi(n)$. Pre $n \geq 10$ označme $\phi(n)$ počet celých čísiel x, $1 \leq x \leq n$ takých, že $(x, n) = 1$.

Eulerova Veta (1760). *Pre* $n > 0$ *a celé číslo* a*, také, že* $(a, n) = 1$ *platí*

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \tag{10.1}$$

Dôkaz. Nech $r_1, r_2, \ldots, r_{\phi(n)}$ sú celé čísla nesúdeliteľné s n. Zoberme ar_1, ar_2, ..., $ar_{\phi(n)}$. Žiadne dve z nich nie sú kongruentné mod n. Keby $ar_i \equiv ar_j \pmod n$, podľa vlastnosti ii) kongruencií by sme mali $r_i \equiv r_j \pmod n$, lebo $(a, n) = 1$. Je ich $\phi(n)$, takže to musia byť opäť čísla $r_1, r_2, \ldots, r_{\phi(n)}$ v nejakom poradí. Teda musí platiť $r_1 r_2 \ldots r_{\phi(n)} \equiv ar_1 ar_2 \ldots ar_{\phi(n)} \pmod n$ Podľa vlastnosti ii) môžeme vykrátiť a dostaneme $a^{\phi(n)} \equiv 1 \pmod n$, čo sme chceli ukázať.

♠

Leonhard Euler (1707–1783) bol švajčiarsky matematik, fyzik, mechanik a astronóm. Pôsobil v Petrohrade a Berlíne.

Úloha: Existuje pre dané a také b, že platí $ab \equiv 1 \pmod m$? Keď také b existuje, vypočítame ho na základe a. Nazýva sa inverzný prvok vzhľadom na násobenie $\pmod m$.

Veta. *Pre dané* a *(*a m*), existuje* b *také, že* $ab \equiv 1 \ (mod\ m) \Leftrightarrow (a, m) = 1$*. Keď existuje také* b*, je tiež* $(b, m) = 1$ *a* b *je určené jednoznačne* $(mod\ m)$*, t.j. ak* $ab \equiv ab' \equiv 1 \ (mod\ m)$*, potom* $b \equiv b' \ (mod\ m)$.

Dôkaz.

$\Rightarrow$) Ak $ab \equiv 1 \pmod m$, potom je $ab = 1 + km$, takže spoločný deliteľ a a m musí deliť 1. Odkiaľ plynie $(a, m) = 1$ (a tiež $(b, m) = 1$).

$\Leftarrow$) Keď $(a, m) = 1$, Euklidov algoritmus na výpočet nsd určí celé čísla b a k také, že $ab + mk = 1$. Platí, že $ab \equiv 1 \pmod m$. $(ab - 1 = mk)$. Jednoznačnosť b vyplýva z vlastnosti i) kongruencií.

♠

Literatúra

Materiál tejto časti bol čerpaný z kníh: Graham, Knuth, Patashnik: Concrete Mathematics, : A Foundation for Computer Science, 2nd edition, Addison-Wesley, Reading, Massachusetts, 1994, 1989.; Peter Giblin: Primes and Programming, Introduction to Number theory with Computing, Cambridge University Press, 1993; Juraj Hromkovič: Algorithmics for Hard Problems, Introduction to Combinatorial Optimization, Randomization, Approximation and Heuristcs, Springer Verlag, 2001; Jozef Gruska: Foundation of Computing, International Thomson Press, 1997.