Teorija števil, praznična epizoda

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

25. december 2023

Eulerjeva funkcija φ

Eulerjeva funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ je definirana takole:

$$\varphi(n) = |\{k \in \mathbb{N} \,;\, 1 \leq k \leq n \text{ in } k \perp n\}|$$

$\varphi(n)$ je število števil med 1 in n, ki so tuja n.

Zgled:

$\varphi(4) = 2$	1,2,3,4
$\varphi(5) = 4$	1,2,3,4,5
$\varphi(6) = 2$	1,2,3,4,5,6

Kako računamo Eulerjevo funkcijo

Trditev

Če je p praštevilo, je $\varphi(p) = p - 1$.

Trditev

Če je p praštevilo, je $\varphi(p^n) = p^n - p^{n-1}$.

Trditev

Če $a, b \in \mathbb{N}$ in $a \perp b$, potem je $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Kako računamo Eulerjevo funkcijo

Izrek

Naj bo $n = {p_1}^{k_1} {p_2}^{k_2} \cdots {p_m}^{k_m}$*, kjer so* $p_1, p_2, \ldots, p_m$ *različna praštevila. Potem je*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

Če želimo izračunati Eulerjevo funkcijo števila n, je nujno poznati praštevilski razcep števila n.

Zgled

Naloga: izračunaj $\varphi(720)$.

Kongruence

Naj bo $a \in \mathbb{Z}$ in $m \in \mathbb{N}$, $m \geq 2$.

$$a \bmod m$$

je ostanek a-ja pri deljenju z m.
(ki je naravno število med 0 in $m - 1$)

Definirajmo relacijo, *kongruenco po modulu m*, z naslednjim opisom:

$$a \equiv b \pmod{m} \quad \textit{ntk.} \quad m|(a-b) \quad \textit{ntk.} \quad a \bmod m = b \bmod m$$

Lastnosti kongruenc

1. *kongruenca po modulu m* je ekvivalenčna relacija v $\mathbb{Z}$
2. Če $a \equiv b \pmod{m}$, potem
$$\begin{aligned} &a \pm c \equiv b \pm c \pmod{m} \\ &a \cdot c \equiv b \cdot c \pmod{m} \\ &a^n \equiv b^n \pmod{m} \end{aligned}$$
3. Če $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$, potem
$$\begin{aligned} &a \pm c \equiv b \pm d \pmod{m} \\ &a \cdot c \equiv b \cdot d \pmod{m} \end{aligned}$$
4. Če $a \cdot c \equiv b \cdot c \pmod{m}$ in $c \perp m$, potem $a \equiv b \pmod{m}$

Zgledi

Zgledi:

- Izračunaj ostanek pri deljenju števila 3^{120} s 13.
- Izračunaj zadnjo cifro števila $9^{8^{7^6}}$.
- Izračunaj ostanek pri deljenju števila $9^{8^{7^6}}$ z 11.

Rezultati

Izrek (Eulerjev)

Naj bo $a \in \mathbb{Z}$, $m \geq 2 \in \mathbb{N}$ *in* $a \perp m$. *Potem je*

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

Izrek (mali Fermatov)

Če je p *praštevilo in* $a \perp p$, *potem je*

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Za vse $a \in \mathbb{Z}$ *pa velja*

$$a^{p} \equiv a \pmod{p}.$$

RSA kriptosistem

Trditev

Naj bosta p in q različni praštevili. Potem je

$$a \equiv b \pmod{p} \quad \textit{in} \quad a \equiv b \pmod{q}$$

natanko tedaj, ko je

$$a \equiv b \pmod{pq}.$$

Trditev

Naj bosta p in q različni praštevili. Potem za poljubni naravni števili a in k velja

$$a^{k \cdot \varphi(pq)+1} \equiv a^{k \cdot (p-1)(q-1)+1} \equiv a \pmod{pq}$$

RSA kriptosistem

RSA kriptosistem deluje na principu *javnih* in *privatnih ključev*.

Pogovarjajmo se o dveh uporabnikih *Ančki* in *Borutu*. Vsak izmed njiju ima svoj *privatni ključ* P_A, P_B, ki ga hrani na skrivnem mestu, svoj *javni ključ* J_A, J_B da na vpogled vsem.

RSA kriptosistem

Komunikacija med Ančko in Borutom:

- Ančka bi rada Borutu posredovala sporočilo x:

  $x,\ J_B(x) \quad \xrightarrow{!} \quad J_B(x),\ P_B(J_B(x)) = x$

- Ančka bi rada Borutu posredovala sporočilo x in Borut bi rad bil prepričan, da mu je sporočilo res posredovala Ančka:

  $x,\ P_A(x),\ J_B(P_A(x)) \quad \xrightarrow{!}$

  $\xrightarrow{!} \quad J_B(P_A(x)),\ P_B(J_B(P_A(x))) = P_A(x),\ J_A(P_A(x)) = x$

Veljati mora:

1. P_A in J_A kot tudi P_B in J_B sta *inverzni preslikavi*.
2. Če poznamo J_A iz tega ne moremo (vsaj ne enostavno) izračunati P_A.

Kako poiskati praštevila?

- *Težko* odločiti, ali je $n \in \mathbb{N}$ praštevilo.
- *Lahko* odločiti, ali je $n \in \mathbb{N}$ zelo verjetno praštevilo.
- *Fermatov test* (Obstajajo tudi naprednejši testi.)

RSA kriptosistem

Sloni na dejstvu, da je *težko* razcepiti naravno število na prafaktorje.

Trenutno se zdi dovolj, da je n 2048 bitno število. Najbolj bi bilo, da bi bili praštevili p in q primerljivi po velikosti, torej 1024 bitni. V desetiškem sestavu to pomeni, da gre za približno 300-mestni števili.

Čez prst je (v povprečju) pri 300 mestnih številih vsako 700-to število tudi praštevilo.