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

$\varphi(1) = 1$ 1

$\varphi(2) = 1$ 1, 2

Kako računamo Eulerjevo funkcijo

Trditev

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

Dokaz.

$\underline{1, 2, 3, \dots, p-1}, p$

Trditev

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

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

Dokaz.

delitelji p^n

$1, p, p^2, \dots, p^{n-1}, p^n$

$a \in [1 .. p^n]$

a ni tuje p^n ....

a deljivo s p

(a je večkratnik p)

Med $\underline{1 \dots p^n}$ je natanko

$p^{n-1} = p^n/p$ večkratnikov p.

toliko jih NI tujih p.

Trditev

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

φ je multiplikativna funkcija

(v teoriji števil)

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.

Dokaz

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_m^{k_m})$$

$$= p_1^{k_1-1}(p_1-1) \cdot p_2^{k_2-1} \cdot (p_2-1) \cdot \ldots \cdot p_m^{k_m-1}(p_m-1)$$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right) \cdot p_2^{k_2}\left(1-\frac{1}{p_2}\right) \cdot \ldots \cdot p_m^{k_m}\left(1-\frac{1}{p_m}\right)$$

$$= p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}\left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_m}\right)$$

Zgled

Naloga: izračunaj $\varphi(720)$.

$$720 = 8 \cdot 9 \cdot 10$$
$$= 8 \cdot 2 \cdot 9 \cdot 5 =$$
$$= 2^4 \cdot 3^2 \cdot 5^1$$

$$\varphi(720) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5)$$
$$= 2^3(2-1) \cdot 3^1(3-1) \cdot 5^0(5-1)$$
$$= 8 \cdot 3 \cdot 2 \cdot 4 = 192$$

Kongruence

$18 \bmod 4 = 3$

$17 \bmod 4 = 1$

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

$$a \pm c \equiv b \pm c \pmod{m}$$
$$a \cdot c \equiv b \cdot c \pmod{m}$$
$$a^n \equiv b^n \pmod{m}$$

3. Če $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$, potem

$$a \pm c \equiv b \pm d \pmod{m}$$
$$a \cdot c \equiv b \cdot d \pmod{m}$$

4. Če $a \cdot c \equiv b \cdot c \pmod{m}$ in $c \perp m$, potem $a \equiv b \pmod{m}$

$$a^n - b^n =$$
$$(a-b)(a^{n-1} + a^{n-2}b + \dots$$
$$\dots + ab^{n-2} + b^{n-1})$$

$$a \cdot c - b \cdot d =$$
$$a \cdot c - ad + ad - bd =$$
$$\underbrace{a(c-d) + (a-b)d}_{\text{večkratnik } m}$$

$$1 \cdot 4 \equiv 6 \cdot 4 \pmod{10}$$
$$1 \not\equiv 6 \pmod{10}$$

$$m \mid (a \cdot c - b \cdot c)$$
$$m \mid (a-b) \cdot c$$

ker je $m \perp c$, velja

$$m \mid a-b$$

Zgledi

Zgledi:

- Izračunaj ostanek pri deljenju števila 3^{120} s 13.
- Izračunaj zadnjo cifro števila $9^{8^{7^6}}$. $\longleftarrow$ ostanek pri deljenju z 10
- Izračunaj ostanek pri deljenju števila $9^{8^{7^6}}$ z 11.

Kakšne ostanke dajejo potence števila 3 pri deljenju s 13

$$3^0 \equiv 1 \pmod{13}$$
$$3^1 \equiv 3 \pmod{13}$$
$$3^2 \equiv 9 \pmod{13}$$
$$3^3 \equiv 27 \equiv 1 \pmod{13}$$
$$3^4 \equiv 3 \cdot 3^3 \equiv 3 \cdot 1 \equiv 3 \pmod{13}$$
$$3^5 \equiv 3^2 \cdot 3^3 \equiv 9 \cdot 1 \equiv 9 \pmod{13}$$
$$3^6 \equiv 3^3 \cdot 3^3 \equiv 1 \cdot 1 \equiv 1 \pmod{13}$$
$$3^{3k} \equiv 1 \pmod{13}$$
$$3^{120} \equiv 3^{3 \cdot 40} \equiv (3^3)^{40} \equiv 1^{40} \equiv 1 \pmod{13}$$

$$9^{8^{7^6}} = 9^{\left(8^{\left(7^6\right)}\right)} \neq \left(\left(9^8\right)^7\right)^6$$

$$9^0 \equiv 1 \pmod{10}$$
$$9^1 \equiv 9 \pmod{10}$$
$$9^2 \equiv 81 \equiv 1 \pmod{10}$$
$$9^{2k} \equiv 1 \pmod{10}$$

8^{7^6} je sodo število

$8^{7^6} = 2k$ (pri ustrezno izbranem k)

$$9^{8^{7^6}} \equiv 9^{2k} \equiv (9^2)^k \equiv 1^k \equiv 1 \pmod{10}$$

- Izračunaj ostanek pri deljenju števila $9^{8^{7^6}}$ z 11. $\leftarrow$ 3

kakšni so ostanki potenc 9 pri deljenju z 11.

$9^0 \equiv 1 \pmod{11}$
$9^1 \equiv 9 \pmod{11}$
$9^2 \equiv 4 \pmod{11}$
$9^3 \equiv 9 \cdot 4 \equiv 3 \pmod{11}$
$9^4 \equiv 4 \cdot 4 \equiv 5 \pmod{11}$
$9^5 \equiv 4 \cdot 3 \equiv 1 \pmod{11}$

$9^{5k} \equiv 1 \pmod{11}$

kakšen je ostanek 8^{7^6} po modulu 5

$9^{8^{7^6}} \equiv 9^{5k+3} \equiv (9^5)^k \cdot 9^3 \equiv$
$\equiv 1^k \cdot 9^3 \equiv 1 \cdot 3 \equiv 3 \pmod{11}$

$8^0 \equiv 1 \pmod 5$
$8^1 \equiv 3 \pmod 5$
$8^2 \equiv 4 \pmod 5$
$8^3 \equiv 2 \pmod 5$
$8^4 \equiv 1 \pmod 5$

kakšen je ostanek 7^6 po modulu 4

$8^{7^6} \equiv 8^{4l+1} \equiv$
$\equiv (8^4)^l \cdot 8 \equiv 1^l \cdot 8 \equiv$
$\equiv 1 \cdot 8 \equiv 3 \pmod 5$

$8^{7^6} = 5k + 3$ $\leftarrow$ pri nekem $k \in \mathbb{N}$

$7^0 \equiv 1 \pmod 4$
$7^1 \equiv 3 \pmod 4$
$7^2 \equiv 1 \pmod 4$

$7^6 \equiv 7^2 \cdot 7^2 \cdot 7^2 \equiv$
$\equiv 1 \cdot 1 \cdot 1 \equiv 1 \pmod 4$

$7^6 = 4 \cdot l + 1$ $\leftarrow$ pri nekem $l \in \mathbb{N}$

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

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

če $a \perp p$ ✓

če $p | a$ ✓

Zakaj $a \perp m$?

Če je $\gcd(a, m) = d > 1$

a^n ← deljivo z d

1 ← ni deljivo z d

$a^n - 1$ ← ni deljiva z d, niti z m

$\mathcal{T} = \{a_1, a_2, \dots, a_{\varphi(m)}\}$

množica ostankov pri deljenju z m, ki so tuji m.

$f: x \longmapsto a \cdot x \bmod m$

$f: \mathcal{T} \longrightarrow \mathcal{T}$

$\left.\begin{array}{l} x \text{ tuj } m \\ a \text{ tuj } m \end{array}\right\} a \cdot x$ tuj m

$a \cdot x \bmod m$ tuj m

Po Dirichletovem principu je f bijektivna.

$a_1 \longmapsto a \cdot a_1 \bmod m$

$a_2 \longmapsto a \cdot a_2 \bmod m$

$\vdots$

$a_{\varphi(m)} \longmapsto a \cdot a_{\varphi(m)} \bmod m$

$a^{\varphi(m)} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(m)} \equiv$

$a \cdot a_1 \cdot a \cdot a_2 \cdot \ldots \cdot a \cdot a_{\varphi(m)} \equiv$

$a_1 \cdot a_2 \cdot \ldots \cdot a_{\varphi(m)} \pmod m$

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

Trdimo: f je injektivna ✓

Če ne, obstajata $a_i, a_j \in \mathcal{T}$

$a_i < a_j$, $f(a_i) = f(a_j)$

$a \cdot a_i \bmod m = a \cdot a_j \bmod m$

$a a_j - a \cdot a_i$ je večkratnik m

$m | a(a_j - a_i)$, ker je $m \perp a$

$m | (a_j - a_i)$

$0 < a_j - a_i < m$ $\rightarrow\!\leftarrow$

Izračunaj ostanek pri deljenju števila $9^{8^{7^6}}$ z 11.

$9^0 \equiv 1 \pmod{11}$
$9^1 \equiv 9 \pmod{11}$
$9^2 \equiv 4 \pmod{11}$
$9^3 \equiv 9 \cdot 4 \equiv 3 \pmod{11}$
$9^4 \equiv 4 \cdot 4 \equiv 5 \pmod{11}$
$9^5 \equiv 4 \cdot 3 \equiv 1 \pmod{11}$

$9^{5k} \equiv 1 \pmod{11}$

Izrek (Eulerjev)

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

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

$a = 9$
$m = 11$

$9 \perp 11$

$$9^{10} = 9^{\varphi(11)} \equiv 1 \pmod{11}$$

$$9^{10 \cdot k} \equiv 1 \pmod{11}$$

RSA kriptosistem

Trditev

Naj bosta p in q različni praštevili. Potem je

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

natanko tedaj, ko je

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

$p \perp q$

Dokaz ($\Leftarrow$) $pq \mid a-b$

($\Rightarrow$) $p \mid a-b$ in $q \mid a-b$

$a-b = k \cdot p = l \cdot q$

$p \mid l \cdot q \Longrightarrow p \mid l$

Trditev

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

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

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

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

$$a^{p-1} \cdot \left\{ a^{p-1+1} \equiv a^p \equiv a \pmod{p} \right.$$

$$a^{2(p-1)+1} \equiv a^{p-1+1} \equiv a \pmod{p}$$

$$a^{k(p-1)+1} \equiv a \pmod{p} \longleftarrow \text{za vse } k \in \mathbb{N}$$

$$\left.\begin{array}{l} a^{k(q-1)(p-1)+1} \equiv a \pmod{p} \\ a^{k(p-1)(q-1)+1} \equiv a \pmod{q} \end{array}\right\} a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

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:

$x \xrightarrow{!} x$

- 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.

Trditev

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

n

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

Določimo naravno število e, ki reši diofansko enačbo: e *d = 1 + k phi*.

Ker sta *d* in *phi* tuji števili, je ta LDE rešljiva.

Z drugimi besedami, produkt e *d* je po modulu *phi* kongruenten *1*.

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.

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.)

NE
DA ... pravilen odgovor z verjetnostjo poljubno blizu 1

Izrek (mali Fermatov)

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

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

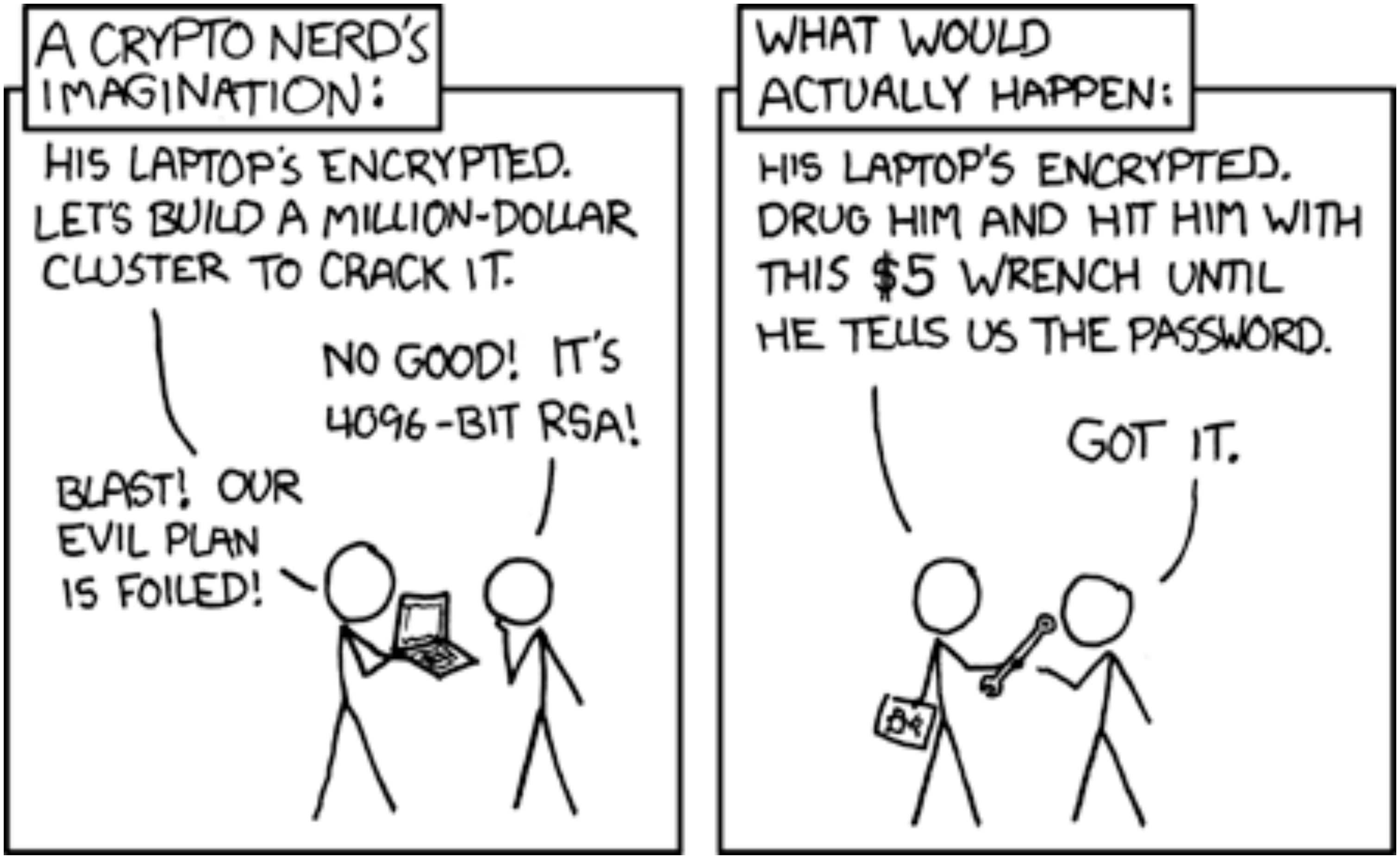
p veliko, veliko naravno število
ni očitno sestavljeno

$$a_1, a_2, a_3, \ldots, a_k \in [2, \ldots, p-2]$$

ali je $a_i^{p-1} \equiv 1 \pmod p$?

če pri kakem i odgovor NE, potem p NI praštevilo

če je za vse i odgovor DA, potem je p "verjetno" praštevilo xkcd.com/538/


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.