Teorija števil

1 Največji skupni delitelj in najmanjši skupni večkratnik

Definicija 1.1. Največji skupni delitelj števil a in b je največje število $\gcd(a, b)$, ki deli tako a kot b. Njun najmanjši skupni večkratnik je najmanjše število $\text{lcm}(a, b)$, ki ga delita oba.

Izrek 1.2. *Za poljubni števili $a, b \in \mathbb{N}$ velja $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.*

Povedano drugače, če najdemo največji skupni delitelj, lahko enostavno izračunamo tudi najmanjši skupni večkratnik.

Izrek 1.3 (Osnovni izrek o deljenju)**.** *Naj bosta $a, b \in \mathbb{N}$ poljubni. Potem obstajata enolično določeni števili $q \geq 0$ in $r < b$, da velja $a = bq + r$.*

Posledica 1.4. *Naj bo $a > b$ in d skupni delitelj teh števil. Potem d deli r, kjer je $a = bq + r$ razcep iz izreka.*

Posledica utemelji, da naslednji algoritem res najde največji skupni delitelj števil a in b:

Evklidov algoritem

Vhod: a, b
while $b > 0$ **do**
  $c = a\%b$ (ostanek pri deljenju)
  $a = b$
  $b = c$
end while
Odgovor: a

Izrek 1.5 (Bezoutova identiteta)**.** *Naj bosta $a, b \in \mathbb{N}$ poljubni in $d = \gcd(a, b)$. Potem obstajata $m, n \in \mathbb{Z}$, da je $d = ma + nb$.*

2 Praštevila

Definicija 2.1. Naravno število $p > 1$ je praštevilo, če sta njegova edina delitelja 1 in p.

Izrek 2.2 (Osnovni izrek aritmetike)**.** *Vsako število $n > 1$ je produkt končno mnogo praštevil. Ta praštevila so enolično določena z n.*

Za iskanje praštevil (do neke izbrane zgornje meje N) lahko uporabimo naslednji algoritem:

Eratostenovo rešeto

Ustvari seznam dolžine N, v katerem so same ničle.
Začni z $n = 2$.
while $n \leq N$ **do**
  if na n-tem mestu seznama je 0 **then**
    n je praštevilo.
    Nastavi $m = 2n$.
    while $m \leq N$ **do**
      Na m-to mesto v seznamu zapiši n.
      Povečaj m za n.
    end while
  end if
  Povečaj n za 1.
end while

S tem algoritmom smo našli praštevila, hkrati pa smo si v seznam zapisali pomembno informacijo. Na n-tem mestu seznama je shranjeno največje praštevilo, ki deli n. S tem lahko enostavno izračunamo praštevilski razcep:

Algoritem

Iščemo razcep števila n.
while $n > 1$ **do**
  Naj bo p praštevilo, zapisano na n-tem mestu seznama.
  p je eden od praštevilskih faktorjev začetnega n.
  Nastavi n na n/p.
end while

3 Modularna aritmetika

Vzemimo poljubno naravno število $n > 1$ in definiramo naslednjo relacijo:

$$x \equiv y \pmod{n} \iff n | x - y.$$

Pravimo, da sta x in y KONGRUENTNA po modulu n. To se zgodi natanko tedaj, ko imata x in y enak ostanek pri deljenju z n.

Izrek 3.1. *Naj bodo $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Če je $x_1 \equiv x_2 \pmod{n}$ in $y_1 \equiv y_2 \pmod{n}$, potem sta tudi $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$ in $x_1 y_1 = x_2 y_2 \pmod{n}$.*

Definicija 3.2. Število x je OBRNLJIVO po modulu n, če obstaja $y \in \mathbb{Z}$, da velja $xy \pmod{n} = 1$.

Izrek 3.3. *Število x je obrnljivo po modulu n če in samo če je $\gcd(x, n) = 1$.*

Za iskanje inverza lahko uporabimo Bezoutovo identiteto. Če je $1 = ax + bn$, je $ax \equiv 1 \pmod{n}$, torej je $a \mod n$ inverz x po modulu n.

4 Kriptosistem RSA

Definicija 4.1. EULERJEVA FUNKCIJA $\phi(n)$ predstavlja število števil $1 \leq m \leq n$, ki so tuja n (tj. da velja $\gcd(m, n) = 1$).

Izrek 4.2. *Če je y obrnljiv po modulu n, je $y^{\phi(n)} \equiv 1 \pmod{n}$.*

Primer. Če je p praštevilo, je $\phi(p) = p - 1$, iz česar dobimo Fermatov mali izrek: Za vsak $1 \leq x \leq p$ velja

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

Upoštevali smo tudi, da so vsa števila med 1 in $p - 1$ tuja p.

Zanimal nas bo specifično primer, v katerem je n produkt dveh različnih praštevil, $n = pq$.

Trditev 4.3. *Naj bosta p in q različni praštevili in $de \equiv 1 \mod (p-1)(q-1)$. Potem za poljuben $x \in \mathbb{Z}_{pq}$ velja $x^{de} \equiv x \pmod{pq}$.*

Trditev nam zagotavlja, da sta si naslednja algoritma obratna:

RSA kodiranje

Naj bodo p, q, d, e kot v trditvi in $n = pq$.
Naj bo $m \leq n$ neko število – sporočilo.
Kodirano sporočilo je $\mathfrak{m} = m^e \,\%n$.

RSA dekodiranje

Naj bodo p, q, d, e kot v trditvi in $n = pq$.
Naj bo $\mathfrak{m}$ RSA-kodirano sporočilo z e in n.
Originalno sporočilo je $m = \mathfrak{m}^d \,\%n$.

Podatki v RSA so potem naslednji:

- Javni ključ je sestavljen iz števil n in e.
- Privatni ključ je število d.
- Če oseba A pošlje sporočilo osebi B, ga kodira z javnim ključem osebe A po prvem postopku zgoraj.
- Če oseba A prejme sporočilo osebe B, ga dekodira s privatnim ključem osebe A po drugem postopku zgoraj.