RSA sistem in faktorizacija

- Probabilistično testiranje praštevilčnosti (ponovitev Monte Carlo algoritem, Solovay-Strassen algoritem in Miller-Rabinov test)
- Napadi na RSA (odšifrirni eksponent, Las Vegas algoritem)
- Rabinov kriptosistem
- Algoritmi za faktorizacijo (naivna metoda, metoda $p-1$, Dixonov algoritem in kvadratno rešeto)

Generiranje praštevil

Za inicializacijo RSA kriptosistema potrebujemo velika (npr. 80-mestna) naključna praštevila.

V praksi generiramo veliko naključno število in testiramo, ali je praštevilo z Monte Carlo algoritmom (npr. Solovay-Stassen ali Miller-Rabin).

Ti algoritmi so hitri, vendar pa so probabilistični in ne deterministični. Po izreku o gostoti praštevil je verjetnost, da je naključno 512-bitno liho število praštevilo, približno $2/\log p \approx 2/177$.

S praštevili, ki so "osnovni gradniki" matematike, so se ukvarjali učenjaki vse od antičnih časov dalje.

Odločitveni problem praštevilo
Za dano število n ugotovi ali je praštevilo.

Leta **240 pr. n. št.** se je grški matematik in filozof **Eratostenes**, bibliotekar aleksandrijske knjižnice, domislil prve neoporečne metode (čas. *zahtev.* $O(n)$). V primeru zelo dolgih števil bi za rešitev tega problema potrebovali več časa kot je staro vesolje.

Od tedaj so matematiki poskušali najti algoritem, ki bi dal odgovor v smiselnem času.

Karl Frederich Gauss (177-1855) je knjigi Disquisitiones Arithmeticae (1801) zapi

"Menim, da čast znanosti narekuje, da z vsemi sredstvi iščemo rešitev ta elegantnega in tako razvpitega proble

Od prihoda računalnikov dalje poudarek na iskanju matematične formule, ki bi praštevila, ampak na iskanju učinkovitega al za razpoznavanje praštevil.

Večji korak naprej je v 17. stoletju napravil F z že omenjenim **Fermatovim malim izrek**

$$a^{p-1} \equiv 1 \pmod p$$

za vsak $a \in \mathbb{N}$ in vsako praštevilo p, ki ne del

Po zaslugi kriptografije so postale raziskave problema praštevilo v zadnjih desetletjih še intenzejše:

- 1976 **Miller**: deterministični algoritem polinomske časovne zahtevnosti (temelji na Riemannovi hipotezi)
- 1977 **Solovay in Strassen**: verjetnostni algoritem časovne zahtevnosti $O(\log^3 n)$.
- 1980 **Rabin**: modifikacija Millerjevega testa v verjetnostni alg. (pravilnost dokazana)
- 1983 **Adleman, Pomerance in Rumely**: det. alg. čas. zathev. $O(\log n^{O(\log\log\log n)})$
- 1986 **Golwasser in Kilian**: polinomski verj. alg. za skoraj vse podatke z uporabo eliptičnih krivulj
- 2002 **Agrawal, Kayal in Saxena (AKS)**: det. alg. s časovno zahtevnostjo $O(\log^{12} n)$ v praksi $O(\log^6 n)$, tudi $O(\log^3 n)$ a brez dokaza.

Naj bo p liho praštevilo, $0 \leq x \leq p-1$.
Potem je x **kvadratni ostanek** po modulu p, tj. $x \in \mathrm{QR}(p)$, če ima kongruenca

$$y^2 \equiv x \pmod p$$

rešitev $y \in \mathbb{Z}_p$.

Eulerjev kriterij
Naj bo p liho praštevilo. Potem je

$$x \in \mathrm{QR}(p) \iff x^{(p-1)/2} \equiv 1 \pmod p.$$

Torej obstaja polinomski algoritem za odločitveni problem **kvadratnega ostanka**.

Naj bo p liho praštevilo in a nenegativno celo število.
Potem je **Legendrov simbol** definiran z

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{če } p \mid a, \\ 1, & \text{če je } a \in \mathrm{QR}(p), \\ -1, & \text{sicer.} \end{cases}$$

Po Eulerjevem kriteriju velja

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Legendrov simbol posplošimo v Jacobijev simbol. Število n naj bo celo liho število z naslednjo praštevilsko faktorizacijo $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

Za nenegativno celo število a definiramo **Jac simbol** z

$$\left(\frac{a}{n}\right) := \Pi_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Eulerjevo psevdopraštevilo: $91 = 7{\cdot}13$ pa obstaja tak $a = 10$, da je

$$\left(\frac{10}{91}\right) = -1 = 10^{45} \mod 91.$$

DN: Pokaži, da je za poljubno sestavljeno štev m Eulerjevo psevdopraštevilo glede na bazo a za največ polovico naravnih števil, ki so manj (glej nalogo 4.14).

DA-naklonjen Monte Carlo algoritem je probabilistični algoritem za odločitveni problem (tj. DA/NE-problem), pri katerem je “DA” odgovor (vedno) pravilen, “NE” odgovor pa je lahko nepravilen.

Verjetnost napake za **DA-naklonjen Monte Carlo** algoritem je ε, če za vsak odgovor “DA” algoritem odgovori z “NE” z verjetnostjo kvečjemu ε.

Solovay-Strassen algoritem

1. Izberi naključno celo število $a \in \mathbb{Z}_n$,

2. **if**
$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$$
then *n je praštevilo*
else *n je sestavljeno število.*

Verjetnost napake pri Solovay-Strassen algoritmu je kvečjemu $1/2$ (glej nalogo 4.14 v Stinsonu).

Monte Carlo verjetnostni algoritem za odločitveni problem, ali je število sestavljeno: test ponovimo m-krat z naključnimi vrednostmi a. Verjetnost, da bo odgovor napačen m-krat zapored napačen je ε^m, vendar pa iz tega še ne moremo zaključiti, da je verjetnost, da je n praštevilo, $1-\varepsilon^m$.

Dogodek A:

“naključen lih n določene velikosti je sestavljen”

in dogodek B:

“algoritem odgovori ‘n je praštevilo’ m-krat zapored.”

Potem očitno velja $P(B/A) \leq \varepsilon^m$, vendar p
resnici zanima $P(A/B)$, kar pa ni nujno isto.

Naj bo $N \leq n \leq 2N$ in uporabimo izrek o
praštevil
$$\frac{2N}{\log 2N} - \frac{N}{\log N} \approx \frac{N}{\log N} \approx \frac{n}{\log n}\ .$$
Sledi $P(A) \approx 1 - 2/\log n$. Bayesovo pravilo p
$$P(A/B) = \frac{P(B/A)P(A)}{P(B)}\ .$$
Imenovalec je enak $P(B/A)P(A) + P(B/\overline{A})$

Upoštevajmo še $P(B/\ \overline{A}) = 1$ in dobimo
$$P(A/B) = \frac{P(B/A)(\log n - 2)}{P(B/A)(\log n - 2) + 2} \leq$$
$$\leq \frac{2^{-m}(\log n - 2)}{2^{-m}(\log n - 2) + 2} = \frac{(\log n - 2)}{\log n - 2 + 2^{m+1}},$$
kar pomeni, da gre iskana verjetnost eksponentno proti 0.

Monte Carlo verjetnostni algoritem za odločitveni problem ali je število sestavljeno:

Test ponovimo k-krat z različnimi vrednostmi a. Verjetnost, da bo odgovor k-krat zapored napačen, je za nas ocenjena z ε^k.

DN: Iz naslednjega izreka izpeljite, da za izračun Jacobijevega simbola ne potrebujemo praštevilske faktorizacije števila n.

Gaussov izrek

Izrek o kvadratni recipročnosti (1796)

Če sta p in q različni lihi praštevili, potem velja
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$
ter za praštevilo 2
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Zakaj je ta izrek tako pomemben?

Pomaga nam, da odgovorimo, kdaj imajo kv
kongruence rešitev, saj velja multiplikativno p
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
Predstavlja pa tudi nepričakovano zvezo m
praštevil (pravilo, ki ureja praštevila).