Izrek 1 (Kitajski izrek o ostankih) *Naj bodo* $m_1, m_2, ..., m_r$ *paroma tuji* ($gcd(m_i, m_j) = 1$ *za* $i \neq j$), $a_1, a_2, ..., a_r \in Z$. *Sistem kongruenc*

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ &\vdots \\ x &= a_r \pmod{m_r} \end{aligned}$$

ima enolično rešitev po modulu $M = m_1 \cdot m_2 \cdots m_r$,

$$x = \sum_{i=1}^{r} a_i \cdot M_i \cdot y_i \pmod{M},$$

kjer je $m_i = M/m_i$, $y_i = M_i^{-1} \bmod m_i$, $i = 1, ..., r$.

Izrek 2 (Fermatov izrek) *p praštevilo,* $b \in Z_p$ *potem velja:* $b^p \equiv b \pmod{p}$.

Izrek 3 $P(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \not\equiv 0 \pmod{p}$, *p praštevilo. Potem ima kongruenca* $P(x) \equiv 0 \pmod{p}$ *kvečjemu n različnih rešitev po modulu p.*

Kvadratni ostanek

p liho praštevilo, $0 \leq x \leq p-1$. Potem je x *kvadratni ostanek* po modulu p, če ima kongruenca $y^2 \equiv x \pmod{p}$ rešitev $y \in Z_p$.

Izrek 4 (Eulerjev kriterij) *Naj bo p praštevilo. Potem je x kvadratni ostanek* $\pmod{p} \Longleftrightarrow x^{(p-1)/2} \equiv 1 \pmod{p}$.

Kvadratni koreni

- n praštevilo, $x^2 \equiv 1 \pmod n$

$$n|x^2 - 1, \qquad n|(x-1)(x+1) \quad \Longrightarrow$$

$$x \equiv 1 \pmod n \quad \text{ali} \quad \mathrm{x} \equiv -1 \pmod{\mathrm{n}}$$

- $n = p \cdot q, \quad p, q$ praštevili $\quad x^2 \equiv 1 \pmod n$

$$p \cdot q|(x-1)(x+1)$$

Štiri rešitve: $x \equiv 1$ ali $x \equiv -1 \pmod n$ (trivialni rešitvi)

$$\left.\begin{array}{l} x \equiv 1 \pmod p \\ x \equiv -1 \pmod q \end{array}\right| \qquad \left.\begin{array}{l} x \equiv -1 \pmod p \\ x \equiv 1 \pmod q \end{array}\right|$$

S pomočjo Kitajskega izreka o ostankih dobimo še dve (netrivialni) rešitvi.

RABINOV KRIPTOSISTEM

Temelji na tem, da je težko razbiti veliko število na produkt dveh praštevil.

$n = p \cdot q, \qquad p \neq q, \qquad p, q \equiv 3 \pmod 4$

$\mathcal{P} = \mathcal{C} = Z_n$

$\mathcal{K} = \{(n, p, q, B);\ 0 \leq B \leq n-1\}$

Za izbran ključ $K = (n, p, q, B)$:

$e_K(x) = x(x+B) \pmod n$

$d_K(y) = \sqrt{\frac{B^2}{4} + y} - \frac{B}{2}$

Javno: n, B tajno: p, q

Trditev 5 *Naj bo $\omega^2 \equiv 1 \pmod n$ netrivialen koren (kongruenca ima 4 rešitve: 1, -1 in še dve netrivialni), in $x \in Z_n$. Potem velja:*

$$e_K(\omega(x + \frac{B}{2}) - \frac{B}{2}) = e_K(x).$$

Imamo 4 čistopise, ki ustrezajo tajnopisu $e_K(x)$:
x, $-x-B$, $\omega(x+\frac{B}{2})$ in $-\omega(x+\frac{B}{2})$.
V splošnem se ne da ugotoviti, kateri je pravi.

Dekripcija

Imamo tajnopis y
Iščemo x: $x^2 + Bx \equiv y \pmod{n}$.

Poenostavimo: $x = x_1 - \frac{B}{2}$
$x_1^2 \equiv \frac{B^2}{4} + y \pmod{n}$
$C = \frac{B^2}{4} + y$.

Iščemo kvadratne korene enačbe:

$$\boxed{x_1^2 \equiv C \pmod{n}}$$

To je ekvivalentno sistemu:

$$\left.\begin{array}{l} x_1^2 \equiv C \pmod{p} \\ x_1^2 \equiv C \pmod{q} \end{array}\right|$$

Eulerjev izrek:
$C^{(p-1)/2} \equiv 1 \pmod{p}$
Predpostavka: $p \equiv 3 \pmod{4}$

$\downarrow$

$\Rightarrow \quad (\pm C^{(p+1)/4})^2 \equiv C \pmod{p}$

$$\left.\begin{array}{l} x_1 \equiv x_{1,2} \pmod{p} \\ x_1 \equiv x_{3,4} \pmod{q} \end{array}\right|$$

$\Rightarrow$ korena prve enačbe sta:
$x_{1,2} = \pm C^{(p+1)/4}$
korena druge enačbe pa:
$x_{3,4} = \pm C^{(q+1)/4}$

$\Downarrow$ Kitajski izrek o ostankih

x_1, x_2, x_3, x_4

PRIMER

$n = 77 = 7 \cdot 11, \quad B = 9$

$e_K(x) = x^2 + 9x \pmod{77}$

$$d_K(y) = \sqrt{\frac{B^2}{4} + y} - \frac{B}{2} = \sqrt{1+y} - 43 \pmod{77}$$

Tajnopis: $y = 22$

Poiskati moramo rešitve

$$\left.\begin{array}{l} x^2 \equiv 23 \pmod{7} \\ x^2 \equiv 23 \pmod{11} \end{array}\right| \qquad \begin{array}{c} (x \equiv \pm 4 \pmod{7}) \\ (x \equiv \pm 1 \pmod{11}) \end{array}$$

Dobimo štiri sisteme enačb kot:

$$\begin{array}{l} x \equiv 4 \pmod{7} \\ x \equiv 1 \pmod{11} \end{array}$$

Po Kitajskem izreku o ostankih:

$$x = 4 \cdot 11 \cdot (11^{-1} \bmod 7) + 1 \cdot 7 \cdot (7^{-1} \bmod 11)$$

Vse rešitve so:

$x_1 = 67 \pmod{77}$

$x_2 = 10 \pmod{77}$

$x_3 = 32 \pmod{77}$

$x_4 = -32 \pmod{77}$

Dekodirani tekst:

$$\begin{array}{rlll} d_K(y) = & 67 - 43 & \pmod{77} & = 24 \\ & 10 - 43 & & = 44 \\ & 32 - 43 & & = 66 \\ & 45 - 43 & & = 2 \end{array}$$

Varnost Rabinovega kriptosistema
Hipotetični algoritem A za dekripcijo Rabinovega kriptosistema lahko uporabimo kot orakelj v algoritmu tipa Las Vegas za faktorizacijo števila n z verjetnostjo vsaj 1/2.

1. Izberemo r, $1 \leq r \leq n-1$
2. $y := r^2 - B^2/4 \pmod{n}$ $\quad (y = e_K(r - B/2))$
3. $x := A(y)$
4. $x_1 := x + B/2 \quad (x_1^2 \equiv r^2 \pmod{n})$
5. Če velja $x_1 \equiv \pm r \pmod{n}$ potem
   ni odgovora
   sicer $(x_1 \equiv \pm\omega \cdot r \pmod{n}$, kjer je $\omega \equiv 1 \pmod{n}$
   netrivialni koren)
   $\gcd(x_1 + r_1, n) = p$ (ali q)

V zadnjem primeru $n | (x_1 - r)(x_1 + r)$, vendar $n \not| (x_1 - r)$ in $n \not| (x_1 + r) \quad \Rightarrow \gcd(x_1 + r, n) \neq 1$.

Verjetnost, da uspemo v enem koraku:
Def: $r_1 \sim r_2 \Leftrightarrow r_1^2 \equiv r_2^2 \pmod{n}$ $(r_1, r_2 \neq 0.)$
To je ekvivalenčna relacija, ekvivalenčni razredi v $Z_n \backslash \{0\}$ imajo moč 4: $[r] = \{\pm r, \pm\omega r\}$
Vsak element iz [r] nam da isto vrednost y. Orakelj A nam vrne x, $[x] = \{\pm x, \pm\omega x\}$

- $r = \pm x$: 4 ni odgovora
- $r = \pm\omega x$: dobimo odgovor

Ker r slučajno izberemo, je vsaka od teh možnosti enako verjetna $\Rightarrow$ verjetnost, da uspemo, je 1/2.

ALGORITMI ZA FAKTORIZACIJO ŠTEVIL

I. Poskušanje

Število n delimo z vsemi lihimi števili do $\sqrt{n}$.

$i := 3$
dokler $i \leq \sqrt{n}$
    če $i|n$: imamo faktor
    sicer $i := i + 2$

Algoritem je uporaben za manjše n (npr. $n \leq 10^{12}$.)
Časovna zahtevnost: k bitov $\Rightarrow 2^{k/2-1}$ deljenj.

II. Metoda $p - 1$ (Pollard, 1974)

Podatki: n (lih, želimo ga faktorizirati)
    B (meja)

Algoritem temelji na naslednjem preprostem dejstvu:
p praštevilo, $p|n$ in za vsako praštevilsko potenco q, ki deli $p - 1$, velja $q \leq B \Longrightarrow (p - 1)|B!$

PRIMER: $B = 9$, $p = 37$, $p - 1 = 36 = 2^2 \cdot 3^2$

$2^2 \leq B, 3^2 \leq B \Rightarrow 2^2 \cdot 3^2 | 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9$

ALGORITEM

Podatki: n, B
1. $a := 2$
2. $j = 2, ..., B$
$\quad a := a^j \pmod n \qquad (a \equiv 2^{B!} \pmod n)$
3. $d = \gcd(a-1, n) \qquad (\Rightarrow a \equiv 2^{B!} \pmod p)$
4. Če velja $1 < d < n$: d je faktor n
sicer: ni uspeha

Če $B \geq \sqrt{n} \;\Rightarrow$ vedno uspemo, vendar algoritem ni učinkovit.

$$\left.\begin{array}{ll} a & \equiv 2^{B!} \pmod p \\ 2^{p-1} & \equiv 1 \pmod p \ \text{(Fermat)} \end{array}\right\} \ker(p-1)|B! \Rightarrow a \equiv 1 \pmod p$$

$$\left.\begin{array}{l} p|(a-1) \\ p|n \end{array}\right\} \Rightarrow p|d = \gcd(a-1, n)$$

Dobimo faktorizacijo, razen če je $a = 1$.

Časovna zahtevnost

- $B - 1$ eksponentov po modulu $n \Rightarrow 2\log_2 B$ množenj po modulu n
- največji skupni delitelj - $O((\log n)^3)$ za Evklidov algoritem
- skupaj $O(B \log B (\log n)^2 + (\log n)^3)$
- Če je $B \approx (\log n)^i$, je algoritem polinomski

PRIMER

$n = 143, B = 4$

$a \equiv 2^{2\cdot 3\cdot 4} \pmod{143}$
$a \equiv 131 \pmod{143}$

$a - 1 = 130$

$\gcd(130, 143) = 13$

III. Dixonov algoritem in kvadratno rešeto

Ideja: če najdemo $x \not\equiv \pm y \pmod{n}$ in $x^2 \equiv y^2 \pmod{n}$, potem je $\gcd(x-y, n)$ netrivialen faktor števila n.

Sestavimo bazo faktorjev
$\mathcal{B} = \{p_1, ..., p_B\}$, p_i "majhna" praštevila.
Naj bo C malo večji kot B (npr, $C = B + 10$)

Najdemo C kongruenc:

$$x_j^2 \equiv p_1^{\alpha_{1,j}} \times p_2^{\alpha_{2,j}} \times \cdots \times p_B^{\alpha_{B,j}} \pmod{n}, \ \ 1 \le j \le C$$

Označimo $a_j := (\alpha_{i,j} \bmod 2, \cdots, \alpha_{B,j} \bmod 2) \in (Z_2)^B$
Če najdemo podmnožico $\{a_1, \cdots, a_C\}$, v kateri se vektorji seštejejo v $(0, 0, \cdots, 0) \bmod 2$, potem bo produkt x_j uporabil vsak faktor iz $\mathcal{B}$ sodo mnogokrat.

Primer

$n = 15770708441$, $\mathcal{B} = \{2, 3, 5, 7, 11, 13\}$

$$\begin{aligned} 8340934156^2 &\equiv 3 \times 7 \pmod{n} \\ 12044942944^2 &\equiv 2 \times 7 \times 13 \pmod{n} \\ 2773700011^2 &\equiv 2 \times 3 \times 13 \pmod{n} \end{aligned}$$

$a_1 = (0, 1, 0, 1, 0, 0)$
$a_2 = (1, 0, 0, 1, 0, 1)$
$a_3 = (1, 1, 0, 0, 0, 1)$

$$a_1 + a_2 + a_3 = (0, 0, 0, 0, 0, 0) \bmod 2$$

$$(8340934156 \times 12044942944 \times 2773700011)^2 \equiv (2 \times 3 \times 7 \times 13)^2 \pmod{n}$$

$$9503435785^2 \equiv 546^2 \pmod{n}$$

$$\gcd(9503435785 - 546, 15770708441) = 115759$$

- Kako poiščemo ustrezno podmnožico $\{a_1, a_2, \cdots, a_C\}$:
  linearna odvisnost med vektorji (npr. z Gaussovo eliminacijo)

- $C > B + 1$: več različnih odvisnosti, lahko upamo, da bo vsaj ena dala faktorizacijo.

- Kako poiščemo x_j, da se dajo $x_j^2 \pmod n$ faktorizirati v $\mathcal{B}$?
  Kvadratno rešeto (Pomerance):
  Gledamo števila oblike $x_j = j + \lfloor\sqrt{n}\rfloor, \quad j = 1, 2, ...$
  Izberemo samo tista, ki dajo faktorizacijo v $\mathcal{B}$.

- $\mathcal{B}$ velik - večja možnost, da se da neko število faktorizirati v $\mathcal{B}$
  - potrebujemo več kongruenc, da najdemo linearno odvisnost
  -$|\mathcal{B}| \approx \sqrt{e^{\sqrt{ln\, n\, ln\, ln\, n}}}$

- Časovna zahtevnost: $O(e^{(1+o(1))\sqrt{ln\, n\, ln\, ln\, n}})$

Algoritmi za faktorizacijo v praksi

Kvadratno rešeto	$O(e^{(1+o(1))\sqrt{ln\,n\,ln\,ln\,n}})$
Eliptične krivulje	$O(e^{(1+o(1))\sqrt{ln\,p\,ln\,ln\,p}})$
Številsko rešeto	$O(e^{(1.92+o(1))(ln\,n)^{1/3}(ln\,ln\,n)^{2/3}})$

$o(1) \to 0$, ko $n \to \infty$
p - najmanjši praštevilski faktor n

$p \approx \sqrt{n}$: kvadratno rešeto in eliptične krivulje imata približno enako časovno zahtevnost. V tem primeru je ponavadi boljše kvadratno rešeto .

Faktorizacije velikih števil s kvadratnim rešetom: $(n = p{\cdot}q,\ p \approx q)$

69-mestno število	1983 (Davis, Holdredge, Simmons)
do 106 cifer	1989 (Lenstra, Manasse + pomočniki)
129 cifer	1994 (Atkins,Graff,Lenstra,Leyland+600 pomočnikov)

Eliptične krivulje:
$2^{2^{11}} - 1$ 1988 (Brent)

Številsko rešeto:
$2^{2^{9}} - 1$ 1990 (Lenstra, Lenstra, Manasse, Pollard)