Kódoláselmélet 2020 szeptember 23

RSA kódoláshoz egyedi nagy prímszámok kellenek.

Van elég prímszám, mert nagy prímszámtétel szerint

$$\pi(x) \sim \frac{x}{\ln x}$$

$$\pi(x) = |\{p \mid p \text{ prím}, p \le x\}|$$

100 jegyű páratlan számok kb. 1/115 része prím

$a = 2, 3, 5, 7$ elég egészen $3\cdot 10^9$-ig

Def: p páratlan prímjelölt, $p-1 = 2^r \cdot m$, $2 \nmid m$

Az $1 \le a \le p-1$ egész átmegy a Miller-Rabin teszten, ha az $a^m, (a^m)^2, (a^m)^4, \dots, (a^m)^{2^r} \bmod p$ sorozatban megjelenik az 1 és előtte -1 van (kivéve ha az első volt 1-es)

$$?, ?, \dots, ?, -1, 1, 1, \dots, 1$$

Különben azt mondjuk, hogy a megbukik a teszten.

Tétel: Ha p páratlan prím, akkor minden $1 \le a \le p-1$ átmegy a teszten.

Biz:

$$(a^m)^{2^r} = a^{2^r \cdot m} = a^{p-1} \equiv 1 \bmod p$$

kis Fermat-tétel

$$x^2 \equiv 1 \bmod p$$

$$p \mid x^2 - 1 = (x+1)(x-1)$$

$$x \equiv \pm 1 \bmod p$$

azaz 1-es előtt vagy megint 1-es van vagy -1

<u>Tétel (Miller–Rabin)</u> Ha n páratlan összetett szám, akkor az $A = \{a \mid 1 \le a \le n-1 \text{ és } \text{lnko}(a,n) = 1\}$ elemeinek legalább 3/4 része megbukik a teszten.

<u>Megj.</u> $\text{lnko}(a,n)=1$ feltétel nem szükséges, mert ha $\text{lnko}(a,n) \neq 1$ akkor a biztos megbukik.

<u>Tétel (Gyengített Miller–Rabin)</u> ... az elemek fele bukik.

$n-1 = 2^r \cdot m$ és $2 \nmid m$

<u>Első eset</u>: $n = st$ ahol $\text{lnko}(s,t) = 1$, $s,t \ge 3$

$$n-1 \in A \quad \text{és} \quad (n-1)^{2^0 \cdot m} \equiv (-1)^m = -1 \pmod{n}$$

azaz létezik $i \in \{0, \dots, r\}$ és $a \in A$ hogy $a^{2^i m} \equiv -1 \pmod{n}$

Legyen h az ilyen i-k maximuma és rögzítünk egy $b \in A$ elemet amelyre $b^{(2^h \cdot m)} \equiv -1 \pmod{n}$.

Állítjuk, hogy van olyan $a \in A$ amely megbukik a teszten úgy, hogy $a^{2^h \cdot m} \not\equiv \pm 1 \pmod{n}$. Ez tényleg bukás, mert h választása miatt -1 nem lehet később a sorozatban, de korábban se, mert a négyzetre emelés során az 1-re változott volna, és csupa 1-es sem lehet.

Legyen a az $\begin{cases} a \equiv b \mod s \\ a \equiv 1 \mod t \end{cases}$ megoldása. A kínai maradéktétel szerint van megoldás.

Ha $a^{(2^h \cdot m)} \equiv 1 \mod n$, akkor (3)

$1 \equiv a^{2^h \cdot m} \equiv b^{2^h \cdot m} \equiv -1 \pmod s$ ami ellentmondás, mert $s \geq 3$.

Ha $a^{2^h \cdot m} \equiv -1 \mod n$, akkor

$-1 \equiv a^{2^h \cdot m} \equiv 1^{2^h \cdot m} = 1 \pmod t$ ami megint ellentmondás.

Mivel $a \equiv 1 \mod t$, ezért $\underline{\text{lnko}(a,t) = 1}$

Mivel $b \in A$, azaz $\text{lnko}(b, s) = 1$ és $a \equiv b \pmod s$ ezért $\underline{\text{lnko}(a,s) = 1}$. Azaz $\text{lnko}(a, n) = 1$ így $\underline{a \in A}$.

Ezzel megmutattuk, hogy a megbukik a teszten.

Legyen $G = \{x \in \mathbb{Z}_n^* \mid x^{2^h \cdot m} \in \{1, -1\}\}$ ← részcsoportja $\mathbb{Z}_n^*$-nak.

Tudjuk, hogy $\bar{a} \notin G$, azaz G indexe legalább kettő a $\mathbb{Z}_n^*$ csoportban. Tehát $\mathbb{Z}_n^*$ elemeinek legalább a fele G-n kívül van, és ezek ~~mid~~ mindegyikére megbukik a teszt.

<u>Második eset</u>: $n = p^k$ prímhatvány ahol $k \geq 2$.

Legyen g primitív gyök modulo p^k. Ha g átmenne a teszten, akkor $g^{n-1} = g^{p^k - 1} \equiv 1 \mod n$. De g rendje $\varphi(n) = p^k - p^{k-1}$, azaz $g^{p^k - p^{k-1}} \equiv 1 \mod n$. A két kitevőt kivonva $g^{(p^{k-1} - 1)} \equiv 1$ azaz $p^{k-1} - 1 \equiv 0 \mod \varphi(n)$. Ez ellentmondás. Legyen $G = \{x \in \mathbb{Z}_n^* \mid x^{n-1} = 1\}$. G részcsoportja $\mathbb{Z}_n^*$-nak és $g \notin G$. A folytatás ugyanaz mint az első esetben.

Példa: Ellenőrizzük le a Miller-Rabin teszttel, hogy az $n = 561 = 3 \cdot 11 \cdot 17$ prímszám-e.

$$n-1 = 560 = \boxed{2^4} \cdot \boxed{5 \cdot 7} \qquad r = 4, \quad m = 35$$

Válasszuk az $a=2$-t. $\quad a^m \equiv ?\ (\mathrm{mod}\ n)$

$$\begin{array}{ll}
a^1 \equiv 2 & a^{16} \equiv 256^2 \equiv 460 \mod 561 \\
a^2 \equiv 4 & a^{32} \equiv 460^2 \equiv 103 \mod 561 \\
a^4 \equiv 16 & \boxed{a^{35}} \equiv 103 \cdot 4 \cdot 2 \equiv 263 \mod 561 \\
a^8 \equiv 256 & a^{2\cdot 35} \equiv 263 \cdot 263 \equiv 166 \mod 561 \\
 & a^{4\cdot 35} \equiv 166 \cdot 166 \equiv \boxed{67} \mod 561 \\
 & a^{8\cdot 35} \equiv 67 \cdot 67 \equiv 1 \mod 561 \\
 & a^{n-1} = a^{16\cdot 35} \equiv 1 \cdot 1 \equiv 1 \mod 561
\end{array}$$

Tehát n nem prímszám.

Def: Az n összetett számot Carmichael-számnak nevezzük, ha bármely a egészre ha $\mathrm{lnko}(a,n)=1$ akkor $a^{n-1} \equiv 1\ (\mathrm{mod}\ n)$.

Megj: Az összetettséget leszámítva a fenti tulajdonságot a prímek is tudják (kis Fermat-tétel)

Áll: 561 Carmichael szám (legkisebb)

Köv: A Miller-Rabin tesztet nem lehet úgy egyszerűsíteni, hogy csak az a^{n-1} hatványt számoljuk ki.

Tétel (Korselt)

Egy összetett pozitív n egész akkor és csak akkor Carmichael-szám, ha négyzetmentes és $p \mid n$ minden p prímosztójára $p-1 \mid n-1$.

Biz.: (1) Tegyük fel, hogy n Carmichael-szám és $n = p^k m$, $k \geq 2$ és ~~$\text{lnko}(p,m)=1$~~ $p \nmid m$.

A Kínai maradéktétel szerint

$$\begin{cases} a \equiv p+1 \mod p^k & \Rightarrow \text{lnko}(a,p^k)=1 \\ a \equiv 1 \mod m & \Rightarrow \text{lnko}(a,m)=1 \end{cases}$$

megoldható. De akkor, azaz $\text{lnko}(a,n)=1$.

Mivel n Carmichael szám, ezért $a^{n-1} \equiv 1 \mod n$.

$1 \equiv (p+1)^{n-1} \mod p^2$ és $(p+1)^{n-1} \equiv 1+(n-1)p \mod p^2$ Binomiális tételből

azaz $(n-1)p \equiv 0 \mod p^2$ ami ellentmondás, mert $p \nmid n-1$.

(2) Tegyük fel, hogy $n = pm$ és $p \nmid m$.

Legyen b primitív gyök modulo p, azaz

$$b^{p-1} \equiv 1 \pmod p \text{ és } o(b) = p-1.$$

A Kínai maradéktétel szerint

$$\begin{cases} a \equiv b \mod p & \Rightarrow \text{lnko}(a,p)=1 \\ a \equiv 1 \mod m & \Rightarrow \text{lnko}(a,m)=1 \end{cases}$$

$a^{n-1} \equiv 1 \mod p$

megoldható, azaz $a^{n-1} \equiv 1 \mod n$.

De akkor $b^{n-1} \equiv 1 \mod p$ és a rend miatt $\underline{p-1 \mid n-1}$.

3 Tegyük fel, hogy n négyzetmentes, és minden $p \mid n$ prímosztóra $p-1 \mid n-1$. Legyen $\text{lnko}(a,n)=1$. Ekkor minden $p \mid n$ osztóra $\text{lnko}(a,p)=1$, azaz $a^{p-1} \equiv 1 \mod p$. De $p-1 \mid n-1$, ezért $a^{n-1} \equiv 1 \pmod p$ és ez minden $p \mid n$ prímre teljesül, azaz

$$a^{n-1} \equiv 1 \mod n = \underbrace{p_1 p_2 \cdots p_k}_{\text{különböző prímek}}.$$

■

Áll: Minden Carmichael szám páratlan és legalább három különböző prímosztója van.

Biz Ha $n = 2\underbrace{p_1 p_2 \cdots p_k}_{\text{páratlan különböző prímek}}$,

akkor $\underbrace{p_1 - 1}_{\text{páros}} \mid \underbrace{n-1}_{\text{páratlan}}$, ami ellentmondás.

Ha $n = pq$ és $p < q$, akkor

$$q-1 \mid n-1 = pq-1 = p(q-1)+p-1$$

azaz $q-1 \mid p-1$, ami ellentmondás. ■

Köv: $561 = 3 \cdot 11 \cdot 17$ Carmichael-szám, mert

$$3-1 = 2 \mid 560$$
$$11-1 = 10 \mid 560$$
$$17-1 = 16 \mid 560.$$

Def.: Legyen p páratlan prím és a egész.
Az a kvadratikus maradék modulo p, ha
$x^2 \equiv a \mod p$ megoldható (négyzetnek a maradéka).

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ha } a \text{ kvadratikus maradék és } a \not\equiv 0 \mod p \\ -1 & \text{ha nem kvadr. maradék} \\ 0 & \text{ha } a \equiv 0 \mod p. \end{cases}$$

Legendre szimbólum.

kis Fermat-tétel
$a \not\equiv 0 \mod p$ $\quad a^{p-1} \equiv 1 \pmod p$

Áll: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ és $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$
(ekvivalens definíció)

Példa: $\mathbb{Z}_7$-ben

	x	x^2	$\left(\frac{x}{7}\right)$	$\log_g x \mod 6$
	0	0	0	—
$g^6 = g^0 =$	1	1	1	0
$g^2 =$	2	4	1	2
$g^1 =$	3	2	−1	1
$g^4 =$	4	2	1	4
$g^5 =$	5	4	−1	5
$g^3 =$	6	1	−1	3

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = [3]$

fele kvadratikus maradék, fele nem.

$g = 3$

$k \equiv 2n \pmod 6$

$g^{2n} = (g^n)^2 = g^k$ kvadratikus maradék mod p $\iff$ $k \equiv 0 \pmod 2$

Tétel p páratlan prímre

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

kvadratikus reciprocitás

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$$a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$