Kódoláselmélet 2020 október 7

Fermat faktorizáció kritikus lépése:

Keressünk sok b_i egészet úgy, hogy $\mathrm{mod}(b_i^2, n)$ abszolútértéke kicsi legyen.

$$b_i = \lfloor \sqrt{kn} \rfloor \quad \text{vagy} \quad \lceil \sqrt{kn} \rceil \quad \text{kis } k \text{ egészre.}$$

$$b_i = \sqrt{kn} + \varepsilon \Rightarrow b_i^2 = kn + 2\varepsilon\sqrt{kn} + \varepsilon^2$$

$|\varepsilon| < 1$ $\mathrm{mod}(b_i^2, n) \sim 2\varepsilon\sqrt{kn}$ ami nem kicsi ha k nagy.

Cél: Olyan b_i-ket keresni, hogy $|\mathrm{mod}(b_i^2, n)| < 2\sqrt{n}$.

Lánctörtes módszer

Adott $a \in \mathbb{R}$ lánctörtes közelítése

$b_0 = \lfloor a \rfloor$ $a_0 = a - b_0$ $0 \leq a_0 < 1$

$b_1 = \lfloor 1/a_0 \rfloor$ $a_1 = 1/a_0 - b_1$ $0 \leq a_1 < 1$

$b_2 = \lfloor 1/a_1 \rfloor$ $a_2 = 1/a_1 - b_2$

$\vdots$

$$a = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \dots \cfrac{1}{b_n + a_n}}} = b_0 + \frac{1}{b_1+}\,\frac{1}{b_2+}\cdots\frac{1}{b_n+a_n}$$

$[b_0; b_1, b_2, \dots, b_n]$

$b_i \in \mathbb{Z}$

jelölés

Példa $a = \sqrt{2} + 1$

$$\sqrt{2} + 1 = 2 + \frac{1}{2+}\,\frac{1}{2+}\,\frac{1}{2+}\cdots$$

$b_0 = 2$, $a_0 = \sqrt{2} - 1$

$$1/a_0 = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2} + 1 = a$$

Példa $\sqrt{3} = 1 + \frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{2+}\,\cdots$

Áll: ~~Csak~~ Pontosan a racionális számoknak véges a lánctörtes felírása.

Tétel (Lagrange) Az $a \in \mathbb{R}$ lánctörtes felírásában a b_i egészek sorozata pontosan akkor periodikus, ha a benne van $\mathbb{Q}$ egy másodfokú bővítésében.

Tétel Legyen $b_0, b_1, b_2, \ldots$ pozitív egészek tetszőleges sorozata és

$$h_{-2} = 0, \quad h_{-1} = 1, \quad h_n = b_n h_{n-1} + h_{n-2}$$

$$k_{-2} = 1, \quad k_{-1} = 0, \quad k_n = b_n k_{n-1} + k_{n-2}$$

Ekkor

1. $$b_0 + \frac{1}{b_1+}\,\frac{1}{b_2+}\cdots\frac{1}{b_n+} = \frac{h_n}{k_n}$$
2. $\mathrm{lnko}(h_n, k_n) = 1$
3. $k_n h_{n-1} - k_{n-1} h_n = (-1)^n$
4. Ha a b_i-k az $a \in \mathbb{R}$ lánctörtes közelítése, akkor $\frac{h_n}{k_n} \to a$ ahogy $n \to \infty$.

Tétel Ha $n \in \mathbb{N}$ nem négyzetszám és az $a = \sqrt{n}$ lánctörtes alakjában vesszük a $\frac{h_n}{k_n}$ közelítéseket akkor $|\mathrm{mod}(h_i^2, n)| < 2\sqrt{n}$.

Köv számlálók sorozata tökéletes a Fermat faktorizációhoz és rekurzívan számolható.

Pollard ρ-módszere faktorizációra

Legyen n nagy páratlan összetett szám, és $f : \mathbb{Z}_n \to \mathbb{Z}_n$ "véletlen függvényként viselkedő" polinomfüggvény. f ne legyen lineáris, de pl. jó és közkedvelt az $f(x) = x^2 + 1$ választás.
Egy $x_0 \in \mathbb{Z}_n$ elemből kiindulva képezzük az

ez az n nem az az n $\longrightarrow$ $x_{k+1} = f(x_k)$ sorozatot.

Ha $x_i \neq x_j$ $\mathbb{Z}_n$-ben, de $\mathrm{lnko}(n, x_i - x_j) \neq 1$ akkor találtunk egy ~~közös~~ valódi osztót (mert $|x_i - x_j| < n$).

Példa: $n = 91$, $f(x) = x^2 + 1$, $x_0 = 1$

$x_1 = 2$, $x_2 = 5$, $x_3 = 26$

Minden lehetséges $i \neq j$-re kiszámoljuk az lnko-t.
Itt $\mathrm{lnko}(91, 26-5) = 7$, van egy valódi osztó.

Áll: Nem kell minden x_j-t minden előző x_i-vel párba állítani, mert ha $x_i \equiv x_j \bmod r$ és $r \mid n$, akkor $x_{i+1} \equiv x_{j+1} \bmod r$.

$i' = 2^k - 1$
$j' = j - i + i'$

Itt használjuk ki, hogy f polinomfüggvény, mert megőrzi a kongruenciát.

Ha $2^k \leq j < 2^{k+1}$, akkor választjuk $i = 2^k - 1$-et.
Így maximum kétszer olyan hosszú $x_0, x_1, x_2, \dots$ sorozatot kell néznünk, de csak lineáris sok lnkot számolunk!

Tétel: Ahhoz, hogy n-et a ρ-módszerrel p valószínűséggel sikerüljön faktorizálni elegendő a sorozat $2\cdot\sqrt{-2\log(1-p)}\cdot\sqrt[4]{n}$ tagját kiszámolnunk. Ha $p=1/2$, akkor ez kb. $2{,}355\cdot\sqrt[4]{n}$ tagot jelent.

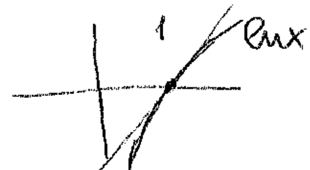
Biz Legyen r valódi osztója n-nek, $r\le\sqrt{n}$. Keressük az a legkisebb k, hogy egy r-elemű halmazból (a mod r maradékosztályok) egymás után k elemet kivéve véletlenszerűen (itt használjuk, hogy f "véletlen függvényként viselkedik") p valószínűséggel lesz az elemek között legalább két azonos. Tehát k elég nagy, hogy

Nem versenyképes a Fermat faktorizációval
$n\approx 10^{200}$

Pollard	
$\approx 10^{50}$ lépés	$O(10^{23})$ lépés

kedvezőtlen esetek $\to$
$$\frac{r(r-1)(r-2)\dots(r-k+1)}{r^k}\le 1-p$$
összes eset $\to$

Vegyük mindkét oldal logaritmusát és felhasználva a $\log(1-u)<-u$ azonosságot a $0<u<1$ intervallumon



$$\log\frac{r}{r}+\log\frac{r-1}{r}+\dots+\log\frac{r-k+1}{r}=$$
$$=\log 1+\log\left(1-\frac{1}{r}\right)+\log\left(1-\frac{2}{r}\right)+\dots+\log\left(1-\frac{k-1}{r}\right)\le$$
$$\le -0-\frac{1}{r}-\dots-\frac{k-1}{r}=-\frac{(k-1)k}{2r}\approx\boxed{\frac{-k^2}{2r}\overset{?}{<}\log(1-p)}$$

Ez teljesül, ha $k\ge\sqrt{-2r\log(1-p)}$. De $\sqrt{n}\ge r$, azaz ez teljesül, ha $k\ge\sqrt{-2\log(1-p)}\,\sqrt[4]{n}$. A 2-es szorzó i 2-hatvány-1 választása miatt van

Diszkrét logaritmus

Def Legyen $G=[g]$ egy multiplikatívan írt ciklikus csoport és $|G|=n$. Ekkor $b \in G$ elemre

$$\log_g b = k \in \mathbb{Z}_n \qquad G=\{\underset{g^n}{\overset{\shortparallel}{1}}, g, g^2, \dots, g^{n-1}\}$$

azt jelenti, hogy $g^k = b$ (k egyértelműen meghatározott modulo n). Ez a <u>diszkrét logaritmus</u> (vagy <u>index</u>).

<u>Példa</u>: $GF(p^k)$ test multiplikatív csoportja ciklikus.

Itt a hatványozás gyorsan megy, de a diszkrét logaritmus kiszámítására nem ismert gyors algoritmus.

<u>Megj</u>: Van olyan ciklikus csoport, ahol a diszkrét logaritmus számítása gyors, pl. $(\mathbb{Z}_n;+)$ de ezt additívan írjuk.

$$GF^*(p^k) \cong (\mathbb{Z}_{p^k-1};+)$$

$$\shortparallel$$

$$\{\underset{g^{p^k-1}}{\overset{\shortparallel}{1}}, g, g^2, \dots, g^{p^k-2}\}$$

itt lassú számolni logaritmust

itt meg gyors.

<u>Megj</u>: Ha p páratlan prím, akkor $GF^*(p^k)$-ban diszkrét logaritmust számolni hasonló nehézségű, mint p^k nagyságrendű számok faktorizációja.

$GF^*(2^k)$-ban ez lényegesen egyszerűbb.

Diffie-Hellman kulcsváltás

A és B nyílt csatornát felhasználva egy közös titokban (kulcsban) szeretne megállapodni.

Publikus $q = p^k$ nagy prímhatvány és a $GF^*(q)$ véges test multiplikatív csoportjának egy g generátor eleme.

Titkos A választ $a \in \mathbb{Z}_{q-1}$ titkos elemet
B b

majd A elküldi g^a-t B-nek, és B g^b-t A-nak.
Mind a ketten kitudják számolni

$$(g^a)^b = g^{ab} = (g^b)^a\text{-t}$$ gyorsan.

Az ellenség nem tudja g és g^a ismeretében a-t meghatározni könnyen (diszkrét logaritmus).

Massey-Omura rejtjelrendszer

A egy $x \in GF^*(q)$ üzenetet akar küldeni B-nek.

Publikus $q = p^k$ nagy prímhatvány és $GF^*(q)$ g generátora.

Titkos A és B is választ egy $e, d \in \mathbb{Z}_{q-1}$ elempárt, hogy $ed \equiv 1 \mod q-1$.

$x \in GF^*(q)$ az üzenet

A elküldi $y = x^{e_A}$-t B-nek.

B $z = y^{e_B}$-t A-nak

A $s = z^{d_A}$-t B-nek

B kiszámítja $t = s^{d_B}$-t.

Áll: $x = t$, mert $t = x^{e_A e_B d_A d_B} = x^{1 \cdot 1} = x$.

A támadó láthatja y, z, s-et és ha tudna diszkrét logaritmust számolni, akkor e_B és d_A-t megkapná és onnét az $ed \equiv 1 \mod q-1$ kongruenciát megoldva minden titkot tud.

<u>ElGamal rejtjelrendszer</u>

Bárki küldhet A-nak titkos üzenetet.

<u>Publikus</u> $q = p^k$ és $GF^*(q)$ egy g generátora továbbá g^e ahol

<u>Titkos</u> $e \in \{1, \dots, q-1\}$ titkos, csak A tudja.

A küldő választ véletlenszerűen $k \in \{1, \dots, q-1\}$ kitevőt és elküldi $(g^k, x \cdot (g^e)^k)$-t A-nak.

A g^k-ból kiszámolja $g^{ek} = (g^e)^k$-t, és azzal osztva megkapja az x üzenetet.

<u>MINDIG</u>: Az autentikáció minden esetben fontos!!!

Silver-Pohlig-Hellman algoritmus

Diszkrét logaritmus kiszámolása $GF(q)$-ban amikor $q-1$ minden prímtényezője kicsi. (pl $q=257$)

Legyen $q-1 = p_1^{k_1} \underbrace{p_2^{k_2} \cdots p_r^{k_r}}$ prímhatvány tényezős felbontás.

Adott $g \in GF^*(q)$ primitív elem és $y \in GF^*(q)$. Keressük $x \in \mathbb{Z}_{q-1}$ elemet, hogy $g^x = y$.

Elég x-et mod $p_i^{k_i}$ értékekre meghatározni, mert onnét kínai maradéktételből megvan a jó x.

Rögzítsünk egy $p^k = p_i^{k_i}$ prímhatványt.

$p \mid q-1$

A $GF(q)$ testben az $x^p - 1$ polinomnak p db gyöke van, ezek az $\varepsilon_0 = 1, \varepsilon_1 = g^{\frac{q-1}{p}}, \varepsilon_2 = \varepsilon_1^2, \ldots, \cancel{\varepsilon_{p-1}}$

$$\varepsilon_0 = 1, \quad \varepsilon_1 = g^{\frac{q-1}{p}}, \quad \varepsilon_2 = \varepsilon_1^2, \ldots, \varepsilon_{p-1} = \varepsilon_1^{p-1}$$

$$\varepsilon_1^p = g^{q-1} = 1$$

ezek a p-edik egységgyökök.

$$\mathrm{mod}(x, p^k) = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1}$$

p-alapú számrendszerben felírva

ahol $0 \le x_i < p$

Tudjuk $y = g^x$ $\qquad x - c \cdot p^k$

$$y^{\frac{q-1}{p}} = g^{x \cdot \frac{q-1}{p}} = g^{(x \bmod p^k) \cdot \frac{q-1}{p}}$$

$$= g^{(x - cp^k) \cdot \frac{q-1}{p}} = g^{x \frac{q-1}{p}} \cdot \underbrace{\boxed{g^{\left(\frac{q-1}{p} \cdot p\right) p^{k-1} c}}}_{1}$$

$$= g^{(x_0 + x_1 p + x_2 p^2 + \dots) \cdot \frac{q-1}{p}}$$

$$= \boxed{g^{x_0 \cdot \frac{q-1}{p}}} \cdot \underbrace{g^{x_1 \overbrace{p \frac{q-1}{p}}^{q-1}}}_{1} \cdot \underbrace{g^{x_2 \overbrace{p^2 \frac{q-1}{p}}^{p(q-1)}}}_{1} \cdot \dots \underbrace{\quad}_{1}$$

$$\left(g^{\frac{q-1}{p}}\right)^{x_0}$$ azaz valamelyik p-edik egységgyök

Amelyik p-edik egységgyök, abból megvan x_0

Következő lépés $\frac{g^x}{g^{x_0}} = g^{x - x_0}$

$$\mathrm{mod}(x - x_0, p^k) = 0 + x_1 p + x_2 p^2 + \dots + x_{k-1} p^{k-1}$$

$$\left(g^{x - x_0}\right)^{\frac{q-1}{p^2}} = g^{x_1 \cdot \frac{q-1}{p}} \cdot 1 \cdot \dots \cdot 1$$

kitevő az $q-1$ többszöröse.

Ebből megvan x_1.

És így tovább. Ezzel kiszámolható a diszkrét log. ∎