(Lecture 17) ② Algoritmul lui Euclid

BĂRBULESCU MIHAI
AAC

Scop: Fie ~~acgdo~~ $r_0, r_1 \in \mathbb{Z}$, găsiți cmmdc (r_0, r_1)

Ex: $r_0 = 27$, $r_1 = 21$

$27 = \boxed{3} \cdot 3 \cdot 3$
$21 = \boxed{3} \cdot 7$
} nu merge pt nr mari în practică. E greu de descompus în factori primi un nr mare

gcd

cmmdc $(r_0, r_1) \overset{!}{=}$ cmmdc $(r_0 \% r_1, r_1)$ = cmmdc $(r_1, r_0 \% r_1)$

Algoritm: input r_0, r_1 cu $r_0 > r_1$

```
i = 1
do
    i = i + 1
    r_i = r_{i-2} % r_{i-1}
while r_i ≠ 0
Return: cmmdc(r_0, r_1) = r_{i-1}
```

combinație liniară (ec. diofantică)

② Extended Euclidean Alg: Pt r_0, r_1 calc gcd $(r_0, r_1) = s r_0 + t r_1$

Idee: Calc (Irregular E.A.)

gcd (r_0, r_1) $r_0 = q_1 r_1 + r_2 \rightarrow r_2 = s_2 r_0 + t_2 r_1$

gcd (r_1, r_2) $r_1 = q_2 r_2 + r_3 \rightarrow r_3 = s_3 r_0 + t_3 r_1$

⋮ ⋮

Ultima iterație gcd $(r_{\ell-2}, r_{\ell-1})$ $r_{\ell-2} = q_{\ell-1} r_{\ell-1} + r_\ell \rightarrow r_\ell = s_\ell r_0 + t_\ell r_1$

$r_{\ell-1} = q_\ell r_\ell + \emptyset$

$r_\ell = \gcd(r_0, r_1) = s_\ell r_0 + t_\ell r_1 = s r_0 + t r_1$

Ex: $\gcd(973, 301) = 5 \cdot 973 + t \cdot 301 = 7$

r_0, r_1

Iteratia

i			
	r_0	r_1	r_2
2	$973 = 3 \cdot 301 + 70$		$\rightarrow r_2 = 70 = [1] 973 + (-3) 301$
		r_3	
3	$301 = 4 \cdot \underline{70} + 21$		$\rightarrow r_3 = 21 = ? \; 973 + ? \; 301$

$21 = 301 - 4 \cdot 70 =$

$= 301 - 4(1 \cdot 973 + (-3) 301) =$

$= -4 \cdot 973 + 13 \cdot 301$

		r_4	
4	$70 = 3 \cdot 21 + 7$		$\rightarrow r_4 = 7 = 70 - 3 \cdot 21 =$

GCD

$= 70 - 3(-4 \cdot 973 + 13 \cdot 301)$

$= (1 \cdot 973 + (-3) 301) + 12 \cdot 973 - 3 \cdot 13 \cdot 301$

$= 13 \cdot 973 - 42 \cdot 301$

5	$21 = 3 \cdot 7 + 0$	

STOP

Deci $\gcd(973, 301) = 7 = 13 \cdot 973 + (-42) \cdot 301$

Generalizare: La iteratia i

$r_{i-2} = s_{i-2} r_0 + t_{i-2} r_1$

$r_{i-1} = s_{i-1} r_0 + t_{i-1} r_1$

$r_{i-2} = q_{i-1} r_{i-1} + r_i$

$r_i = r_{i-2} - q_{i-1} r_{i-1} \Rightarrow$

La pasul urmator ...

$$r_i = s_{i-2} r_0 + t_{i-2} r_1 - q_{i-1}(s_{i-1} r_0 + t_{i-1} r_1) =$$

$$= \underbrace{(s_{i-2} - q_{i-1} s_{i-1})}_{s_i} r_0 + \underbrace{(t_{i-2} - q_{i-1} t_{i-1})}_{t_i} r_1$$

$$s_i \cdot r_0 + t_i \cdot r_1$$

Alg Euclid Extins : input r_0, r_1 cu $r_0 > r_1$

Initial : $s_0 = 1$, $t_0 = 0$ $\quad i = 1$

$s_1 = 0$ $\quad t_1 = 1$

Calc recursiv :

$s_i = s_{i-2} - q_{i-1} s_{i-1}$; $t_i = t_{i-2} - q_{i-1} t_{i-1}$, $i \geq 2$

do $i = i + 1$

$r_i = r_{i-2} \mod r_{i-1}$

$q_{i-1} = (r_{i-2} - r_i) / r_{i-1}$

$s_i = s_{i-2} - q_{i-1} s_{i-1}$

$t_i = t_{i-2} - q_{i-1} t_{i-1}$

while $r_i \neq 0$

Return : $\gcd(r_0, r_1) = r_{i-1}$; $s = s_{i-1}$; $t = t_{i-1}$

Calc inverselor (mod n) : $a^{-1} \equiv ? \pmod n$

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

Se fol EEA : $\gcd(\overset{r_0}{n}, \overset{r_1}{a}) = 1 = \underset{\uparrow}{s} n + \underset{\uparrow}{t} a \equiv 1 \pmod n$

$0 + t \cdot a \equiv 1 \pmod n$

$\uparrow$

a^{-1}

Param t din EEA e inversul lui r_1 mod r_0

Ex 1) Dorim să calc $12^{-1} \pmod{67}$ // inversul lui 12 în corpul $\mathbb{Z}_{67}$

12 și 67 sunt prime între ele: $\gcd(12,67) = 1$

$\gcd(12,67) = 1 = \underbrace{5 \cdot \underbrace{67}_{r_0}}_{} + \underbrace{t \cdot \underbrace{12}_{r_1}}_{}$

i		
2	$67 = 5 \cdot 12 + 7$	$7 = 1 \cdot 67 + (-5) \cdot 12$
3	$12 = 1 \cdot 7 + 5$	$5 = 12 - 1 \cdot 7 = 12 - (67 - 5 \cdot 12) = -1 \cdot 67 + 6 \cdot 12$
4	$7 = 1 \cdot 5 + 2$	$2 = 7 - 1 \cdot 5 = \ldots = 2 \cdot 67 - 11 \cdot 12$
5	$5 = 2 \cdot 2 + 1$	$1 = 5 - 2 \cdot 2 = \ldots = -5 \cdot 67 + 28 \cdot 12$

Deci $1 = -5 \cdot 67 + 28 \cdot 12 = \gcd(67,12) \Rightarrow$

$\Rightarrow 28$ e inversul lui 12 în $\mathbb{Z}_{67}$

$12^{-1} \equiv 28 \pmod{67}$

Verificare $12 \cdot 28 = 336 \equiv 1 \pmod{67}$

Ex 2) Dorim să calc inversul în corpuri Galois (folosite pt obț AES S-boxes), dar și pt curbele eliptice de la PKI)

Vrem să găsim inversul în corpul finit $GF(2^m)$. Datele de intrare sunt $A(x) \in GF(2^m)$ și polinomul ireductibil $P(x)$
Alg extins al lui Euclid dat polinoamele $s(x)$, $t(x)$ a.î

$$s(x)P(x) + t(x)A(x) = \gcd(P(x), A(x)) \underbrace{= 1}_{\text{pt că } P(x) \text{ e ireductibil}}$$

$$s(x)\cdot 0 + t(x)A(x) \equiv 1 \pmod{P(x)}$$

$$t(x) \equiv A^{-1}(x) \pmod{P(x)}$$

Exp: Dorim să calc inversul lui $A(x) = x^2$ în corpul finit $GF(2^3)$ cu $P(x) = x^3 + x + 1$ Inițial $\begin{cases} t_0(x) = 0 \\ t_1(x) = 1 \end{cases}$

Coeficienții polinoamelor sunt dați în $GF(2)$

$$x^3 + x + 1 = x \cdot x^2 + (x+1) \qquad t_2 = t_0 - q_1 t_1 = 0 - x \cdot 1 \equiv x$$

$$x^2 = x(x+1) + x \qquad t_3 = t_1 - q_2 t_2 = 1 - x \cdot x \equiv 1 + x^2$$

$$x + 1 = 1 \cdot x + 1 \qquad t_4 = t_2 - q_3 t_3 = x - 1 \cdot (1 + x^2)$$

$$x = 1 \cdot x + 0 \quad \text{stop} \qquad t_4 \equiv 1 + x + x^2$$

$$A^{-1}(x) = t_4(x) = x^2 + x + 1$$

$$t_4(x) \cdot x^2 = x^4 + x^3 + x^2 \equiv (x^2 + x) + (x+1) + x^2 \bmod P(x)$$
$$\equiv 1 \bmod P(x)$$

Inversarea în $GF(2^m)$ (în particular $GF(2^8)$) stă la baza operației Byte Substitution care conține AES S-Boxes