BĂRBULESCU MIHAI
AAC

Recapitulare

Def: Un grup G este format din $(G, \circ)$ unde $\circ$ e o lege de compoziție. G este grup dacă:

1) $\circ : G \times G \to G$ e asociativă: $\forall a, b, c \in G$
$(a \circ b) \circ c = a \circ (b \circ c)$

2) $\circ$ are un elem neutru notat $1 \in G$

3) Orice elem din G e inversabil: $\forall a \in G$. $1a = a1 = a$ și $\exists b \in G$ a.î. $ab = 1$

Obs: G e grup abelian dacă $\circ$ e comutativă ($a \circ b = b \circ a$ $\forall a, b \in G$)

Def: Se numește inel o mulțime nevidă R înzestrată cu 2 operații algebrice $+ : R \times R \to R$ și $\bullet : R \times R \to R$ care:

1) $(R, +)$ grup abelian

2) $\bullet$ e operație asociativă

3) $\forall a, b \in R$ avem distributivitate $\begin{cases} a \bullet (b+c) = ab + ac \\ (a+b) \bullet c = a \bullet c + b \bullet c \end{cases}$

În plus $\begin{cases} \exists\, 0 \in R \text{ elem neutru față de } + \\ \exists\, 1 \in R \text{ — } 1 \text{ — } \text{ — } \text{ — } \text{ — } 0 \end{cases}$

- **Domeniu de integritate**: inel cu cel puțin 2 elem și fără divizori ai lui 0 $\left(\begin{matrix} x \neq 0, y \neq 0 \\ x, y \in R \end{matrix} \right| \Rightarrow xy \neq 0$

- **Corp**: Un inel în care orice element (în afară de 0) are invers față de $\bullet$ (înmulțire)

• <u>Inel factorial</u>: Un domeniu de integritate în care orice element nenul și neinversabil e produs de elem prime din R:
$a \neq 0$, $a \in R$ neinversabil:

$$a = u \prod_{i \in I} p_i^{m_i}$$

$u \in U(R)$, $U(R)$ = mult elem inversabile din R
$m_i \geq 0$

CMMDC: Fie $a, b \in R$ scrise sub forma:
+
CMMMC:

$$a = u \prod p_i^{m_i}$$
$$b = v \prod p_i^{n_i}$$

$$d = \prod_{i \in I} p_i^{\min(m_i, n_i)}, \quad m = \prod_{i \in I} p_i^{\max(m_i, n_i)}$$

• <u>Idealul</u>: Pentru un inel R și $I \subset R$ o submulțime nevidă
I este ideal dacă e închis față de $+, \cdot$:

1° $\forall x, y \in I \Rightarrow x + y \in I$
2° $\forall a \in R$, $x \in I \Rightarrow ax \in I$ (ideal la stânga)
$xa \in I$ (ideal la dreapta)

(T) Într-un inel factorial R fie $a, b \in R$ și <u>$d = \text{cmmdc}(a,b)$</u>
atunci <u>$\exists x, y \in R$</u> a.î. $\boxed{d = ax + by}$

<u>Obs</u>: Într-un corp toate elem sunt inversabile. Corpul este un caz particular de inel factorial. Elem neutru în corp e $\hat{1}$
Atunci pt $a, b \in K$ corp $\hat{1} = ax + by \Rightarrow a, b$ inverse unul față de celălalt. $\exists$ (1)

Ex de inel factorial și corp: $\mathbb{Z}_m$, m nr prim

Ex: $\mathbb{Z}_3 = \{\{\dots,-3,0,3,\dots\},\{\dots,-2,1,4\dots\},\{\dots,-1,2,5\dots\}\}$

Det inversului x pt elementul $a \in \mathbb{Z}_m$, folosind ecuația

$ax+by = \gcd(a,b) = d$

$ax \equiv 1 \pmod m \Leftrightarrow ax-1 = qm \Leftrightarrow ax - qm = 1$

Alg lui Euclid pt a găsi g, x, y unde $g = \gcd(a,b)$ ai?

$ax + by = g$

Avem nevoie, întâi de algoritmul care det câtul și restul (q, r) pt două numere a, b cu $b \neq 0$ cu $0 \leq r < |b|$, $a = bq + r$

Ex: cmmdc (2261, 1275)

$2261 = 1 \cdot 1275 + 986 \Rightarrow q = 1,\ r = 986$

Dacă $\begin{matrix} d \mid 2261 \\ d \mid 1275 \end{matrix} \Rightarrow d \mid 986$

cmmdc(2261, 1275) =

= cmmdc (1275, 986)

$1275 = 1 \cdot 986 + 289$

$986 = 3 \cdot 289 + 119$

$289 = 2 \cdot 119 + 51$

$119 = 2 \cdot 51 + 17$

= cmmdc (986, 289)

= cmmdc (289, 51) =

= cmmdc (51, 17) = 17

(pt că 17 | 51)

Deci cmmdc (2261, 1275) = 17

Pt rezv ec $ax + by = g$, $g = \text{cmmdc}(a,b)$

$a > b \geq 0$

1. Inițial $x=1,\ y=0,\ r=0,\ s=1$

2. Dacă $b=0 \Rightarrow g=a$. Stop

3. $a=qb+c \qquad 0 \le c < b$

4. $(a,b,r,s,x,y) = (b,c,x-qr,y-qs,r,s)$
(shift)

Exemplu: Rez ec $130x+61y = cmmdc(130,61)$

$cmmdc(130,61)=1$

$130 = 2\cdot 61 + 8$ → $8 = 130 - 2\cdot 61$

$61 = 7\cdot 8 + 5$ → $5 = -7\cdot 130 + 15\cdot 61$

$8 = 1\cdot 5 + 3$ → $3 = 8\cdot 130 - 17\cdot 61$

$5 = 1\cdot 3 + 2$ → $2 = -15\cdot 130 + 32\cdot 61$

$3 = 1\cdot 2 + 1$ → $1 = 23\cdot 130 - 49\cdot 61$

$\Rightarrow x=23,\ y=-49$ o sol pt $130x+61y=1$

$(1,-2)$

$(-7,15) = (0,1) - 7(1,-2)$

$(8,-17) = (1,-2) - 1(-7,15)$

$(-15,32) = (-7,15) - 1(8,-17)$

$(23,-49) = (8,17) - 1(-15,32)$

Inversa modulo n: $ax \equiv 1 \pmod n$. Găsirea lui x se face prin rez ecuației $ax+ny=1$

(T) Corpuri finite ∃ doar dacă au p^n elem, n întreg, p prim

Ex: Poți avea corp finit cu 11 elem → GF(11)

81 elem, $81 = 3^4$ → $GF(81) = GF(3^4)$

Dar nu poți cu 12 elem $12 = 2^2 \cdot 3$

Corpul AES: $GF(2^8) = GF(256)$

Tipuri de corpuri finite $G(p^m)$ { caz part. $m=1$: $GF(p)$ (corpuri prime); $m>1$ ("extension fields")

↳ foarte importante: $GF(2^m)$; $p=2$ → cel mai mic nr prim

Obs: Într-un corp $GF(p)$ $(\mathbb{Z}_p)$ toate elem diferite de 0 au <u>invers</u> (p prim). Elem unui corp $GF(p) = \{0, 1, 2, \dots, p-1\}$. Aritmetica se face <u>modulo p</u>

GF(2) e echiv cu poarta XOR

<u>Inversarea</u>: Fie $a \in GF(p)$. Atunci a^{-1} trebuie să respecte $a \cdot a^{-1} \equiv 1 \pmod p$

Ex: Găsiți inversul în corpul $\mathbb{Z}_{61}$ a elem 17

Trebuie rezv ec $17x \equiv 1 \pmod{61} \Leftrightarrow 17x + 61y = 1$

$61 = 3 \cdot 17 + 10 \longrightarrow 10 = 61 - 3 \cdot 17$

$17 = 1 \cdot 10 + 7 \longrightarrow 7 = -61 + 4 \cdot 17$

$10 = 1 \cdot 7 + 3 \longrightarrow 3 = 2 \cdot 61 - 7 \cdot 17$

$7 = 2 \cdot 3 + 1 \longrightarrow 1 = -5 \cdot 61 + 18 \cdot 17$

Deci $17 \cdot 18 + 61(-5) = 1 \Rightarrow \boxed{x = 18}$ o soluție a ecuației $17x \equiv 1 \pmod{61}$

Concluzii. Într-un corp $\mathbb{Z}_p$, p prim, care e și inel factorial, dar și corp Galois (dacă are nr finit de elem), pt a det inversul unui număr $a \in \mathbb{Z}_p$ trebuie rezv ecuație

$ax \equiv 1 \pmod{p}$

care e echivalentă cu rezv ec.

$ax + py = 1$

$1 = cmmdc(a, p)$

Pentru AES folosim corpul finit [redacted] $GF(2^8)$, deci un corp Galois extins.