30/11/2021

TM: IDENTITÀ di BEZEUT

se $d = MCD(a,b)$

$\Rightarrow \exists\, \alpha, \beta \in \mathbb{Z} : d = \alpha a + \beta b$

in $\mathbb{Z}_n$ tutti e solo gli elementi INVERTIBILI sono le classi di $\bar{a}$ con $MCD(a,n)=1$

(si dice anche che sono COPRIMI con n)

(ES)

$\mathbb{Z}_8$ $\bar{1}, \bar{3}, \bar{5}, \bar{7}$

$\mathbb{Z}_7$ $\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$

$1 = MCD(a,n)$

$\exists\, \alpha, \beta \in \mathbb{Z} : \bar{1} = \overline{\alpha a + \beta n}$

$= \overline{\alpha a} + \overline{\beta n}$

$= \bar{\alpha} \cdot \bar{a} + \bar{\beta} \cdot \bar{n} = \bar{0}$

$\bar{1} = \bar{\alpha} \cdot \bar{a}$

L'inverso di $\bar{a}$ è proprio $\bar{\alpha}$

$\underbrace{\overline{237}}_{a}$ è INVERTIBILE in $\mathbb{Z}_{\underbrace{6743}_{n}}$

$6743 = 237 \cdot \overset{q}{28} + \overset{r}{107}$

$237 = 107 \cdot 2 + 23$

$107 = 23 \cdot 4 + 15$

$23 = 15 \cdot 1 + 8$

6743	237
474	28
2003	
1896	
107	

$15 = 8 \cdot 1 + 7$

$8 = 7 \cdot 1 + 1$ ← se non viene 1 non è INVERTIBILE

$7 = 1 \cdot 7 + 0$

$MCD(6743, 237) = 1 \iff \overline{237}$ è INVERTIBILE in $\mathbb{Z}_{6743}$

$1 = 8 - 1 \cdot 7 \Rightarrow 1 = 8 - 1(15 - 1 \cdot 8)$

$7 = 15 - 1 \cdot 8$

$= 8 - 1 \cdot 15 + 1 \cdot 8$

$= 2 \cdot 8 - 1 \cdot 15$

$8 = 23 - 1 \cdot 15$

$= 2(23 - 1 \cdot 15) - 1 \cdot 15$

$= 2 \cdot 23 - 2 \cdot 15 - 1 \cdot 15$

$= 2 \cdot 23 - 3 \cdot 15$

$15 = 107 - 4 \cdot 23$

$= 2 \cdot 23 - 3(107 - 4 \cdot 23)$

$= 2 \cdot 23 - 3 \cdot 107 - 12 \cdot 23 =$

$= 14 \cdot 23 - 3 \cdot 107 =$

$23 = 237 - 2 \cdot 107$

$= 14(237 - 2 \cdot 107) - 3 \cdot 107 =$

$= 14 \cdot 237 - 31 \cdot 107$

$107 = 6743 - 28 \cdot 237$

$= 14(237) - 31((6743) - 28 \cdot (237))$

$= 14(237) - 31(6743) + 868(237)$

$(1) = 882(237) - 31(6743) =$

$\alpha \quad a \quad \beta \quad b$

L'INVERSO di 237 in $\mathbb{Z}_{6743} = \overline{882}$

ES

1151 è inv. in $\mathbb{Z}_{2781}$?

$2781 = 1151 \cdot 2 + 479$

$1151 = 479 \cdot 2 + 193$

$479 = 193 \cdot 2 + 93$

$103 = 93 \cdot 2 + 7$

$67 = 7 \cdot 13 + 2$

$46 = 2 \cdot 3 + 1$

$21 = 1 \cdot 2 + 0$

$(1) = (46) - 3 \cdot (2)$

$(2) = (67) - 13 \cdot (7)$

$= (46) - 3((67) - 13(7))$

$= (46) - 3(67)$

$\mathbb{Z}_n$ se n non è primo allora $\mathbb{Z}_n$ non è un CAMPO

$(\mathbb{R}^*, \odot)$

$\mathbb{Z}_p^*$

DEF:
Se K è un CAMPO allora K^* è un GRUPPO COMMUTATIVO CHE PRENDE IL NOME di GRUPPO moltiplicativo del CAMPO K

DEF
$(A, \odot)$ un GRUPPO allora si dice CICLICO se

$$\exists\, u \in A : \forall\, a \in A \Rightarrow a = \underbrace{u \odot u \odot u \dots \odot u}_{\text{un certo numero di VOLTE } n} = u^n$$

$(\mathbb{Z}_{10}, \oplus)$ è un GRUPPO CICLICO

GENERATORE $\Rightarrow \bar{1}$ $\quad$ $\bar{2}$ non lo è

$$\bar{a} = \underbrace{\bar{1} + \bar{1} + \bar{1} \dots \bar{1}}_{a \text{ volte}} = a \cdot \bar{1}$$

in $(\mathbb{Z}_n, \oplus)$
$\bar{1}$ è un GENERATORE

$(\mathbb{Z}_n^*, \odot)$

se $n = p$ PRIMO
allora $\mathbb{Z}_p$ è CAMPO
e $(\mathbb{Z}_n^*, \odot)$ è un GRUPPO CICLICO

ES

$(\mathbb{Z}_3^*, \odot) = \{\bar{1}, \bar{2}\}$

$\bar{2}, \bar{2}^2 = \bar{1}$

$\bar{1}, \bar{1}, \bar{1} \ldots \neq \mathbb{Z}_3^*$

ES

$(\mathbb{Z}_5^*, \odot) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\{\bar{4}, \bar{1}, \bar{4}, \bar{1}, \bar{4}, \ldots\}$ no gen.

$\{\bar{2}, \bar{4}, \bar{3}, \bar{1}\}$ $\bar{2}$ è un GENERATORE

Un generatore di $\{\mathbb{Z}_p^*, \odot\}$ prende il nome di ELEMENTO PRIMITIVO

DEF:

La funzione φ di EULERO è definita da $\varphi: \mathbb{N} \to \mathbb{N}$

$$n \to \#\{i \mid 1 \leq i \leq n-1 \mid MCD(n, i) = 1\}$$

$3 \mapsto 2$

$4 \mapsto 2$ $\quad MCD(4,2) = 2$ NO

$5 \mapsto 4$

$P \mapsto P-1$ $\quad \varphi(P) = P-1$ per un numero primo i più piccoli non hanno FATTORI COMUNI

IN $\mathbb{Z}_n$ gli ELEMENTI INVERTIBILI SONO TUTTI e SOLI GLI ELEMENTI $1 \leq a \leq n-1$ T.C. $MCD(a, n) = 1$

$R_n \leftarrow$ GRUPPO dei elementi invertibili in $\mathbb{Z}_n$

$\varphi(n) = |R_n|$

$\varphi(p) = p-1 \Rightarrow p^1 - p^0 = p-1$

se p, q sono t.c. il $MCD(p,q) = 1$ allora

$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$

$\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6$

$\varphi(20) = \varphi(2 \cdot 10) = \varphi(2) \cdot \varphi(10)$

$\hookrightarrow \varphi(4 \cdot 5) = \varphi(4) \cdot \varphi(5) =$

se p è PRIMO

$\varphi(p^2) = p^2 - p^{2-1}$

$\varphi(4) = 2^2 - 2^1 = 2$

$\varphi(25) = 5^2 - 5^1 = 20$

$\varphi(n) = \varphi(p_1^{i_1} \cdots p_r^{i_r}) = \varphi(p_1^{i_1}) \cdots \varphi(p_r^{i_r})$

$= (p_1^{i_1} - p_1^{i_1 - 1})$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) =$$

$$= (2^2 - 2^1) \cdot (5^2 - 5) = 2 \cdot 20 = 40$$

$|R_n| = \varphi(n)$

$\bar{a}^{\frac{\varphi(n)}{q}} \neq \bar{1}$ allora $\bar{a}$ è un GENERATORE per ogni q divisore PRIMO di $\varphi(n)$

$\mathbb{Z}_8$ $\qquad |R_8| = \varphi(8) = 2^3 - 2^2 = 4$

$\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\bar{a}^2 \neq 1$ ← NO $3^2 = 9$ in modulo $8 = \bar{1}$

È SODDISFATTA? NO 5^2 //

NO 7^2 //

$\mathbb{Z}_{12}$ $\qquad |R_{12}| = \varphi(12) = 2 \cdot 2 = 4$

$\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

$\bar{a}^{\frac{\varphi(n)}{q}} = \bar{a}^2 \neq 1$

$\mathbb{Z}_{28}$ $\qquad |R_{28}| = \varphi(28) = 2 \cdot 6 = 12$

$\bar{a}^{\frac{12}{2}} \neq 1$

$\bar{a}^{\frac{12}{3}} \neq 1$