ORDINE MOLTIPLICATIVO

mercoledì 21 agosto 2024

- **PICCOLO TEOREMA DI FERMAT**

Se p primo e $p \nmid a$ allora $a^{p-1} \equiv 1 \pmod p$

- **FUNZIONE DI EULERO**

$\varphi(n)$ = quantità di interi tra 1 e n coprimi con n

ES: p primo $\Rightarrow \varphi(p) = p-1$

$\varphi(p^k) = p^k - p^{k-1}$ $\qquad \varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$

a, b coprimi $\Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

- **TEOREMA DI EULERO**

$MCD(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv_n 1$

DEF: Se $MCD(a,n)=1$ definiamo l'ordine moltiplicativo di a modulo n il più piccolo intero (positivo) k tale che $a^k \equiv 1 \pmod n$ $\qquad ord_n a = O_n(a)$

T. Se $MCD(a,n) \neq 1$ tale numero non esiste perché l'equazione $a \cdot x \equiv_n 1$ non ha soluzioni.

- Se $MCD(a,n)=1$ esiste sempre per il t. di Eulero

ES: $ord_5 3 = ?$

$3^{\varphi(5)} \equiv 1$ $\qquad$ ($3^4 \equiv 1$)

$3^2 = 9 \equiv 4 \pmod 5$

$3^3 \equiv 27 \equiv 2 \pmod 5$ $\qquad ord_5 3 = 4$

TEOREMA $\quad a^m \equiv_n 1 \iff ord_n a \mid m$

DIM: $k = ord_n a$

$\Leftarrow$ $\quad a^m \equiv a^{k \cdot h} \equiv (a^k)^h \equiv 1 \pmod n$

$\Rightarrow$ divisione euclidea di m per k:

$m = k \cdot q + r \qquad 0 \leq r < k$

$1 \equiv a^m \equiv a^{k \cdot q + r} \equiv (a^k)^q \cdot a^r \equiv 1 \cdot a^r \equiv a^r \Rightarrow r = 0$ quindi k è il minimo >0

$1 \equiv a^m \equiv a^{k\cdot q + r} \equiv (a^k)^q \cdot a^r \equiv 1 \cdot a^r \equiv a^r \Rightarrow r = 0$ perché k è il minimo >0

$\Rightarrow k \mid m$ □

ES: Calcolare $k = \text{ord}_{18} 13$

sappiamo che $13^{\varphi(18)} \equiv 1 \pmod{18} \Rightarrow k \mid \varphi(18) = \varphi(2)\cdot\varphi(9) = 1\cdot(9-3) = 6$

$k \mid 6 \Rightarrow k = \cancel{1}, 2, 3, 6$

$13^2 \equiv (-5)^2 = 25 \equiv 7 \pmod{18}$

$13^3 \equiv 7 \cdot 13 \equiv 91 \equiv 90+1 \equiv 1 \pmod{18} \Rightarrow \text{ord}_{18} 13 = 3$

TEOREMA:

1) $\text{ord}_m a^m = \dfrac{\text{ord}_m a}{MCD(m, \text{ord}_m a)}$

2) $\text{ord}_m a^{-1} = \text{ord}_m a$

ES: $\text{ord}_5 64 = \text{ord}_5(2^6) = \dfrac{\text{ord}_5 2}{MCD(6, \text{ord}_5 2)} = \dfrac{4}{MCD(6,4)} = \dfrac{4}{2} = 2$ $\quad \text{ord}_5 2 = 4 \quad 2^2 = 4$, $2^4 \equiv_5 16 \equiv_5 1$

ES: p primo tale che $p \equiv_4 3$

determinare le soluzioni intere di $a^2 \equiv -1 \pmod p$

SVOLG:

$a^4 \equiv_p 1 \Rightarrow \text{ord}_p a \mid 4$ $\quad \text{ord}_p a = \begin{cases} 1 \Rightarrow a \equiv 1 & 1^2 \equiv -1 \text{ NO} \\ 2 \Rightarrow a^2 \equiv 1 & \text{NO} \\ 4 \end{cases}$

$\text{ord}_p a = 4$

$a^{p-1} \equiv 1 \pmod p \Rightarrow \text{ord}_p a \mid p-1 \Rightarrow 4 \mid p-1$ $\quad p-1 \equiv_4 0$ $\quad p \equiv_4 1$ IMP

$S = \emptyset$

PERIODI DECIMALI

Qual è la lunghezza del periodo di $\dfrac{a}{b}$ $\quad a, b \in \mathbb{Z}$ $\quad MCD(a,b) = 1$

$\dfrac{a}{b} = \boxed{n + 0,d_1 d_2 d_3 d_4 \ldots}$ $\quad n \in \mathbb{Z}$

$\frac{a}{b} = \boxed{m + 0,d_1 d_2 d_3 d_4 \dots}$ $\quad m \in \mathbb{Z}$

- se $MCD(b,10)=1$ allora $\exists k = ord_b 10 \Rightarrow 10^k \equiv 1 \pmod b$

$b \mid 10^k - 1$

$$\Rightarrow \underbrace{(10^k-1)\cdot\frac{a}{b}}_{\in\mathbb{Z}} = \underbrace{(10^k-1)m}_{\in\mathbb{Z}} + \boxed{\underbrace{(10^k-1)\cdot 0,d_1d_2d_3\dots}_{\in\mathbb{Z}}}$$

$\Rightarrow d_1 d_2 d_3 \dots d_k, d_{k+1} d_{k+2} \dots - 0,d_1 d_2 d_3 \dots \in \mathbb{Z}$

$\Rightarrow d_{k+1} = d_1$, $d_{k+2} = d_2$, ... hanno lo stesso periodo $\Rightarrow$ la lunghezza del periodo è $k = ord_b 10$

- se $MCD(b,10) \neq 1$

$b = 2^x \cdot 5^y \cdot c$ $\quad MCD(c;10)=1$

$$\frac{a}{b} = \frac{a}{2^x \cdot 5^y \cdot c} = \frac{A}{2^x \cdot 5^y} + \frac{B}{c}$$

decimale finito $\quad$ decimale periodico, di periodo $ord_c 10$

TEOREMA: la lunghezza del periodo della frazione $\frac{a}{b}$ con $MCD(a,b)=1$, $b = 2^x \cdot 5^y \cdot c$, $MCD(c,10)=1$, è $\boxed{l = ord_c 10}$

ES: quante cifre ha il periodo di $\frac{1}{2024}$

$2024 \mid 2^3$
$253 \mid 11$
$23 \mid 23$
1

$2024 = 2^3 \cdot 11 \cdot 23$ $\quad l = ord_{253} 10$

$\varphi(253) = \varphi(11)\cdot\varphi(23) = 10 \cdot 22 = 220$

$\cancel{1} \cdot 220$
$2 \cdot 110$
$4 \cdot 55$
$5 \cdot 44$
$10 \cdot 22$
$11 \cdot 20$

$10^2 = 100$ $\quad 253 \cdot 4 = 1012$

$10^3 = 1000 \equiv -12 \pmod{253}$

$253 \cdot 3 = 759$

$10^4 = 1000 \cdot 10 \equiv -12 \cdot 10 \equiv -120$

$10^5 \equiv -1200 \equiv -180$

$10^{10} \equiv (10^3)^3 \cdot 10 \equiv (-12)^3 \cdot 10 \equiv -1728 \cdot 10 \equiv -210 \cdot 10 \equiv -2100 \equiv -76$

$10^{11} \equiv -76 \cdot 10 \equiv -760 \equiv -1$

$10^{22} \equiv 1$ $\quad l = ord_{253} 10 = 22$

TEOREMA DI LUCAS (test di primalità)

$10^{22} \equiv 1 \quad l = ord_{253} 10 = 22$

TEOREMA DI LUCAS (test di primalità)

se $\exists a \in \mathbb{Z}$ t.c. $a^{m-1} \equiv_m 1$ e che

$\forall d$ divisore di $m-1$ $\quad a^{\frac{m-1}{d}} \not\equiv_m 1$ allora m è primo.

DIM: $\quad ord_m a \mid m-1 \Rightarrow m-1 = k \cdot ord_m a$

supponiamo p.a. che $k \neq 1$

sia d divisore primo di k $\quad a^{\frac{m-1}{d}} \equiv a^{\frac{k \cdot ord_m a}{d}} \equiv \left(a^{ord_m a}\right)^{k/d} \equiv 1$ assurdo

$\Rightarrow k = 1 \Rightarrow ord_m a = m-1$

$m-1 = ord_m a \mid \varphi(m) \leq m-1 \Rightarrow \varphi(m) = m-1 \Rightarrow m$ è primo $\square$

GENERATORI

DEF: $MCD(a, m) = 1$

a è un generatore modulo m se $ord_m a = \varphi(m)$

(significa che $a^1, a^2, a^3, \dots, a^{\varphi(m)}$ sono tutti distinti modulo m, in particolare
($a^{\varphi(m)} \equiv 1$)
sono tutti i $\varphi(m)$ interi coprimi con m)

ES: $m = 9$ possibili generatori $2, 4, 5, 7, (8)$ $\quad \varphi(9) = 9-3 = 6$
($8 \equiv -1$)

$2^2 = 4$

$2^3 = 8 \equiv -1$

$2^6 \equiv (-1)^2 \equiv 1 \quad ord_9 2 = 6 = \varphi(9) \Rightarrow 2$ è un generatore modulo 9.

ES: $m = 8$ possibili generatori: $3, 5, (7)$ $\quad \varphi(8) = 8-4 = 4$
($7 \equiv -1$)

$3^2 = 9 \equiv_8 1 \quad ord_8 3 = 2$

$5^2 = 25 \equiv_8 1 \quad ord_8 5 = 2 \qquad 8$ non ha generatori.

TEOREMA esistono generatori modulo m se e solo se

$m =$
- 2
- 4
- p^k con p primo dispari
- $2 \cdot p^k$ " " " "

$2 \cdot p^k$ " " " "

Quindi 8, 12, 15, 16, 20, 21, 24, 28, 30... non hanno generatori

ESERCIZIO: Se n ha generatori, ne ha $\varphi(\varphi(n))$.

DIM: sia a un generatore $\Rightarrow a^1, a^2, a^3, \dots, a^{\varphi(n)}$ sono distinti $(\bmod n)$ (con $a^{\varphi(n)} \equiv 1$)

consideriamo a^m: $\operatorname{ord}_n a^m = \dfrac{\operatorname{ord}_n a}{MCD(m, \operatorname{ord}_n a)} = \dfrac{\varphi(n)}{MCD(m, \varphi(n))}$

Quindi a^m è un generatore $\Leftrightarrow \operatorname{ord}_n a^m = \varphi(n) \Leftrightarrow MCD(m, \varphi(n)) = 1$

Tali esponenti sono in totale $\varphi(\varphi(n))$ □

ES:

1) determinare gli interi positivi n tali che $n \mid 2^n - 1$

2) calcolare $MCD\{n \in \mathbb{N} : n \geq 2 \text{ e } n \mid 12^n + 1\}$

3) dimostrare il teorema di Wilson: se p primo allora $(p-1)! \equiv_p -1$ (con i generatori)

4) test senior 2004: determinare il più piccolo $n \geq 2004$ t.c. $3^n - 1$ è multiplo di 11