TDN - Struttura moltiplicativa mod p

Titolo nota 31/08/2018

Obiettivo: fissato $a \in \mathbb{Z}$ con $a \not\equiv 0 \ (p)$

vogliamo studiare a^n mod p

ESEMPIO $a = 4, \quad p = 11$

$a^0 \equiv 1 \ (11), \quad a^1 \equiv 4 \ (11), \quad a^2 \equiv 5 \ (11),$

$a^3 \equiv 9 \ (11), \quad a^4 \equiv 36 \equiv 3 \ (11), \quad a^5 \equiv 1 \ (11),$

$a^6 \equiv 4 \ (11), \quad \dots$ in maniera periodica

⚠ Modulo m numero composto questo può non accadere:

$a = 2 \qquad a^n \bmod 20$

$1, \ 2, \ 4, \ 8, \ 16, \ 12, \ 4, \ 8, \ 16, \ \dots$

$\boxed{\text{FATTO 1}}$ Modulo p PRIMO la successione a^n è PERIODICA mod p

$\boxed{\text{DIM}}$ • $a \equiv 0 \ (p) \implies a^n \equiv 0 \ (p)$ per $n > 0$

• $a \not\equiv 0 \ (p) \qquad a^n \bmod p$

Esistono $h < K$ t.c. $a^h \equiv a^K \bmod p$

(pigeonhole)

Sappiamo che (siccome $(a, p) = 1$) esiste l'inverso di a mod p, che chiamiamo a^{-1}.

$$a^h \equiv a^k \bmod p \implies (a^{-1})^h \cdot a^h \equiv (a^{-1})^h a^k \ (p)$$

$$1 \equiv a^{k-h} \bmod p \quad \text{con } k-h>0 \qquad \square$$

DEF Dato a intero con $(a,p)=1$, si definisce **ORDINE (MOLTIPLICATIVO) di a mod p** il minimo $n>0$ per cui $a^n \equiv 1 \bmod p$

Si denota $\mathrm{ord}_p(a)$

$\boxed{\text{FATTO 2}}$ $a^n \equiv 1 \bmod p \iff \mathrm{ord}_p(a) \mid n$

$\boxed{\text{DIM}}$ $\Leftarrow$ Scriviamo $n = \mathrm{ord}_p(a)\cdot k$. Allora

$$a^n \equiv a^{\mathrm{ord}_p(a)\cdot k} \equiv \left(a^{\mathrm{ord}_p(a)}\right)^k \equiv 1^k \equiv 1 \ (p)$$

$\Rightarrow$ Scriviamo $n = \mathrm{ord}_p(a)\cdot k + r$,
$0 \le r < \mathrm{ord}_p(a)$

$$1 \equiv a^n \equiv \left(a^{\mathrm{ord}_p(a)}\right)^k \cdot a^r \equiv a^r \ (\bmod p)$$

Per minimalità di $\mathrm{ord}_p(a)$, questo vuol dire $r=0$, ovvero che $\mathrm{ord}_p(a) \mid n$ $\qquad \square$

PICCOLO TEOREMA DI FERMAT

(i) Sia a un intero, $a \not\equiv 0\ (p)$. Allora

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

(ii) Sia a un intero. Allora

$$a^p \equiv a \pmod p$$

$\boxed{\text{DIM}}$ $\{1, 2, \dots, p-1\} \xrightarrow{\cdot a} \{a, 2a, \dots, (p-1)a\}$

Oss I resti modulo p di $a, 2a, \dots, (p-1)a$ sono tutti diversi. Infatti:

$$ia \equiv ja \pmod p$$

$$\Rightarrow \quad i \equiv j \pmod p$$

con $1 \le i, j \le p-1 \quad \Rightarrow \quad i = j$

Conclusione: $\{a, 2a, \dots, (p-1)a\} = \{1, 2, \dots, p-1\}$

$$a \cdot (2a) \cdot \dots \cdot ((p-1)a) \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \quad (p)$$

$$\parallel\!\mid$$

$$a^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1)$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$$

$\Downarrow$ $\leftarrow$ $(p-1)!$ è coprimo con p

$$a^{p-1} \equiv 1 \pmod p \qquad \square$$

$\boxed{\text{COR}}$ Sia a non divisibile per p. Allora

$$\text{ord}_p(a) \mid p-1$$

$$\left[\text{FLT} \Rightarrow a^{p-1} \equiv 1 \ (p) \right]$$

GENERATORI mod p

Un GENERATORE mod p è un intero g il cui ordine modulo p sia esattamente $p-1$

In modo equivalente: g è un generatore se e solo se $g^0 \equiv 1, g^1, g^2, \dots, g^{p-2}$ mod p sono tutti distinti.

TEOREMA Esiste almeno un generatore mod p per ogni primo p.

Esempio $a = 2 \qquad p = 11$

$2^0 \equiv 1, \quad 2^1 \equiv 2, \quad \boxed{2^2 \equiv 4,} \quad 8, \quad 5, \quad \boxed{2^5 \equiv 10 \quad (11)}$

$9, \quad 7, \quad 3, \quad 6, \quad 1$

Oss $\text{ord}_{11}(2) = ?$ Per il FLT sappiamo che $\text{ord}_{11}(2) \mid 11 - 1 = 10$, quindi è uno fra

$\cancel{1}, \ \cancel{2}, \ \cancel{5}, \ 10$

Oss Per verificare se g sia o meno un generatore è sufficiente calcolare g^d con $d \mid p-1$ (in realtà bastano quelli della forma $\frac{p-1}{q}$ con q primo)

CONSEGUENZE

Fatto $X^2+1 \equiv 0 \pmod p$ si risolve se e solo se $p=2$ o $p \equiv 1 \pmod 4$

$\Rightarrow$ Possiamo supporre p dispari. Sia x_0 soluzione.

$$X_0^2 \equiv -1 \pmod p$$
$$X_0^4 \equiv 1 \pmod p$$

$$\mathrm{ord}_p(X_0) \mid 4 \Rightarrow \mathrm{ord}_p(X_0) = 1, 2, 4$$

Se fosse 1 o 2 si avrebbe

$$-1 \equiv X_0^2 \equiv 1 \mod p \qquad \text{ASSURDO}$$

Quindi $\mathrm{ord}_p(X_0) = 4 \xrightarrow{FLT} \mathrm{ord}_p(X_0) = 4 \mid p-1$

ovvero $p \equiv 1 \pmod 4$

$\Leftarrow$ Prendiamo g un generatore modulo p.

$$X = g^{\frac{p-1}{4}} \qquad \left[X^4 \equiv g^{\left(\frac{p-1}{4}\right)\cdot 4} \equiv 1 \mod p \right]$$

$\hookrightarrow \mathrm{ord}_p(X) \mid 4$

Se $\mathrm{ord}_p(X) < 4 \Rightarrow X^2 \equiv 1 \mod p$

$$\Rightarrow \quad g^{\frac{p-1}{2}} \equiv 1 \mod p,$$

assurdo perché g generatore

$$(x^2)^2 \equiv 1 \mod p \Rightarrow \underbrace{(x^2-1)}_{\text{non divisibile per } p} \cdot (x^2+1) \equiv 0 \pmod p$$

$$\Rightarrow \quad x^2+1 \equiv 0 \mod p.$$

Fatto 2 I quadrati mod p sono tutti e soli i resti della forma $(g^2)^k$