Senior 2012 – TdN 1 – Medium

Titolo nota 03/09/2012

Congruenze modulo un numero primo p.

Esempio: $p = 11$. Quadrati modulo 11?

$(\pm 1)^2 \equiv 1 \quad (\pm 2)^2 = 4 \quad (\pm 3)^2 \equiv -2 \quad (\pm 4)^5 \equiv 5 \quad (\pm 5)^2 \equiv 3$

$0^2 \equiv 0$

$1 + 4 - 2 + 5 + 3 = 11 \equiv 0 \pmod{11}$

p primo, $S_k = \sum_{x=0}^{p-1} x^k$

Consideriamo la classe di congruenza di S_k.

($p = 11 \quad k = 2 \quad S_k \equiv 0$)

1° caso $p-1 \mid k$

$x = 0 \to x^k \equiv 0 \qquad x \not\equiv 0 \to x^k \equiv 1$

$S_k = 0 + 1 + 1 + \dots + 1 = p - 1 \equiv -1 \pmod{p}$

2° caso $p-1 \nmid k$

Fatto: $\exists\, x_0 \not\equiv 0$ tale che $x_0^k \not\equiv 1 \pmod{p}$.

$x_0^k \equiv a \not\equiv 1 \pmod{p}$

$$S_k \equiv \sum_{x=0}^{p-1} x^k \equiv \sum_{x=0}^{p-1} (x_0 x)^k \equiv x_0^k \sum_{x=0}^{p-1} x^k$$

($x \to x_0 x$ è iniettiva: $x_0 x \equiv x_0 y \to x_0(x-y) \equiv 0$

$x_0 \not\equiv 0 \qquad x \equiv y$).

$S_k \equiv \alpha_0^k S_k \qquad (\alpha_0^k - 1) S_k \equiv 0$

$a \not\equiv 1 \qquad (a-1) S_k \equiv 0$

Quindi $S_k \equiv 0$

$f(x)$ polinomio a coefficienti interi

p primo

Ipotesi: $f(0) \equiv 0 \pmod p$

$f(1) \equiv 1 \pmod p$

$f(x) \equiv 0, 1 \pmod p \quad \forall x$.

Tesi: $\deg f \geq p-1$.

Assurdo; Supponiamo $\deg f < p-1$.

$$f(x) = \sum_{i=0}^{p-2} a_i x^i$$

$$\sum_{x=0}^{p-1} f(x) = \sum_{i=0}^{p-2} a_i \underbrace{\sum_{x=0}^{p-1} x^i}$$

Se $p-1 \nmid i$ (ossia $i \neq 0$) allora $\sum_{x=0}^{p-1} x^i \equiv 0$

Rimane il caso $i=0$

$$(p-1) a_0 \equiv 0$$

Però, se ci sono a valori $\equiv 0$, b valori $\equiv 1$, $\Sigma \equiv b \neq 0$

Esempio: $f(x) = x^{p-1}$

Funzioni $F : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$

$\#$ funzioni $= p^p$

Funzioni polinomiali

Se f, g sono p-linee, quando succede che

$f(x) = g(x) \quad \forall x$?

$(f-g)(x) = 0 \quad \forall x = 0, 1, \dots, p-1$

$h = f - g$ è divisibile per $x(x-1)\dots(x-(p-1))$

$\equiv x^p - x$

Concludiamo le funzioni polinomiali

$x \to f(x) \qquad x \to g(x)$

sono uguali se e solo se

$x^p - x \mid f - g$.

Le funzioni polinomiali distinte sono tante quanti i resti della divisione per $x^p - x$

$=$ poli di grado $\leq p-1$ $\qquad \# = p^p$.

---

p primo, n variabili

$$\begin{cases} F_1(x_1, \dots, x_n) = 0 \\ \dots \\ F_k(x_1, \dots, x_n) = 0 \end{cases}$$

equazioni in $\mathbb{Z}/p\mathbb{Z}$

$F_1, \dots, F_k$ polinomi

TEOREMA (Chevalley–Warming):
Se V è l'insieme delle soluzioni del sistema ($V \subseteq (\mathbb{Z}/p\mathbb{Z})^n$) e se $\sum_{i=1}^{k} \deg F_i < n$ allora $|V| \equiv 0 \pmod p$.

DIM: Consideriamo $P = \prod_{i=1}^{k} (1 - F_i^{p-1})$

Se $\underline{x} = (x_1, \dots, x_n) \in V$ allora $P(\underline{x}) = 1$.

Se $\underline{x} = (x_1, \dots x_n) \notin V$ allora $P(\underline{x}) = 0$.

$$|V| \equiv S(P) \pmod p$$

dove $S(P) = \sum_{\underline{x} \in (\mathbb{Z}/p\mathbb{Z})^n} P(\underline{x})$.

$$\deg P = (p-1) \sum_{i=1}^{k} \deg F_i < (p-1)n$$

Un monomio di P sarà del tipo

$$X_1^{a_1} \cdots X_n^{a_n} \quad \text{con} \quad a_1 + \dots + a_n < (p-1)n$$

Quindi per ogni monomio, esiste i tale che $a_i < (p-1)$

somma dei valori di P = somma su tutti i monomi della somma dei valori di ogni monomio.

Supponiamo per esempio: $a_1 < p-1$

$$\sum_{\underline{x} \in (\mathbb{Z}/p\mathbb{Z})^n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = \left(\sum_{x_1} x_1^{a_1}\right) \left(\sum_{(x_2, \dots x_n)} x_2^{a_2} \cdots x_n^{a_n}\right)$$

$$\sum_{x_1} x_1^{a_1} = 0$$

Conseguenza: Se il sistema è omogeneo (o anche se tutti gli F_i non hanno termine noto),

allora esiste una soluzione non banale ($\neq 0$).

Problema (Shortlist IMO 2003, N8)

- p primo
- $A \subseteq \mathbb{N}$ (A finito)
- l'insieme dei divisori primi degli elementi di A ha al più $p-1$ elementi
- il prodotto di un sottoinsieme non vuoto degli elementi di A non è MAI una potenza p-esima.

Domanda: quanti elementi al massimo può avere A?

Tentativo di trovare esempi: $p = 3$ $\quad A \subseteq \{2^a 3^b\}$

$2, 3, 2^4, 3^4$ $\qquad r = p-1$

$p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

Generalizzazione:

$$\underbrace{p_1, p_1^{p+1}, \dots, p_1^{(r-1)p+1}}_{r}, \dots, \underbrace{p_r, p_r^{p+1}, \dots, p_r^{(r-1)p+1}}$$

Questo esempio dà $r^2 = (p-1)^2$ elementi in A

Supponiamo adesso, per assurdo, che $|A| \geq r^2+1$.

$x_i \in A \qquad x = p_1^{a_{i1}} p_2^{a_{i2}} \cdots p_r^{a_{ir}} \longrightarrow (a_{i1}, a_{i2}, \dots, a_{ir}) = v_i$

Prodotto = potenza p-esima

$$\sum_i a_{i1} y_i \equiv 0 \pmod p \qquad y_i = 0, 1$$

$$\sum a_{i2} y_i \equiv 0 \pmod p$$

$$\sum a_i \cdot y_i \equiv 0 \pmod p$$

$p_1^2 p_2^3 p_3^4 \qquad p_1^7 p_2^{11} p_3^5 \qquad p_1^4 p_2^3 p_3^1$

$p_1^{2x+3y+4z} \quad p_2^{3x+y+3z} \quad p_3^{4x+5y+z}$

$$\begin{cases} F_1 = \sum_{i=1}^{r^2+1} a_{i1} x_i^r \equiv 0 \pmod p \\ \vdots \\ F_r = \sum_{i=1}^{r^2+1} a_{ir} x_i^r \equiv 0 \pmod p \end{cases} \qquad r = p-1$$

somma dei gradi : r^2

n° variabili : r^2+1

$x^p \equiv x \pmod p \quad \forall x \quad$ (LFT)

$x^n \equiv x \pmod p \quad \forall x \quad \Leftarrow \quad n \equiv 1 \pmod{(p-1)}$

$n = 1 + k(p-1) \qquad x^{1+k(p-1)} \equiv x \iff x^{k(p-1)} \equiv 1$

$(x \not\equiv 0)$

p primo $\Rightarrow \exists\, x$ t.c. $\operatorname{ord}_p(x) = p-1$.

$G = (\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) - \{0\}. \qquad |G| = p-1$

$\forall x \qquad \operatorname{ord}(x) \mid p-1.$

$\operatorname{ord}(x) = d$

Se $\operatorname{ord}_p(x) = d$, allora x è sol. di $T^d - 1 \in \mathbb{Z}/p\mathbb{Z}[T]$
(polinomio a coeff in $\mathbb{Z}/p\mathbb{Z}$ nella variabile T).

Ci sono al più d radici di questo polinomio.

Due casi: non c'è un el. di ordine d

c'è un el di ordine d α

$\alpha^d - 1 = 0 \quad \alpha^d = 1 \quad T^d - 1$

$\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ è l'insieme delle soluzioni di $T^d - 1 = 0$

α^i ha ordine $d \iff (i, d) = 1$

$N_d = $ n° degli el di ordine d

$$N_d = \begin{cases} 0 \\ \phi(d) \end{cases}$$

$$|G| = \sum_{d \mid p-1} |N_d|$$

$$m = \sum_{d \mid m} \phi(d)$$

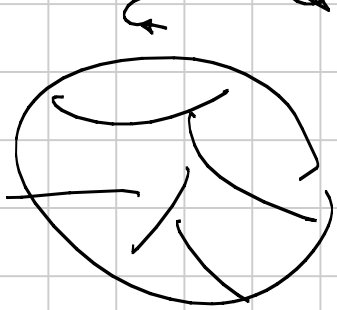
$m = p-1$

$$p-1 = \sum_{d \mid p-1} |N_d| = \begin{cases} 0 \\ \phi(d) \end{cases}$$

$|N_d| = \phi(d) \quad \forall d$

$|N_{p-1}| = \phi(p-1) > 0.$

$G = (\mathbb{Z}/p\mathbb{Z})^*$



Formula generale:

$$m = \sum_{d \mid m} \phi(d)$$

Considero $\mathbb{Z}/m\mathbb{Z}$: ha m elementi

Se $x \in \mathbb{Z}/m\mathbb{Z}$, allora $\text{ord}(x) = d \mid m$.

$k \in \mathbb{Z}/m\mathbb{Z}$ $\text{ord}(k)$ = minimo intero positivo ℓ tale che $\ell k \equiv 0 \pmod m$

$\text{ord}(k) = \ell$

$kx \equiv 0 \pmod m \iff x \equiv 0 \left(\text{mod } \frac{m}{(k,m)}\right)$

$6x \equiv 0 \pmod{15} \iff 2x \equiv 0 \pmod 5$

$\iff x \equiv 0 \pmod 5$

$m = 60$ el di ord 10

sicuramente $10x \equiv 0 \pmod{60}$

$x \equiv 0 \pmod 6$

$0, 6, 12, \dots, 54$ $\quad 6t$

ord $= 10 \iff (t, 10) = 1$. $\quad \varphi(10)$

$x^n \equiv x \pmod p \ \forall x \iff n \equiv 1 \pmod{(p-1)}$

Domanda: dato un modulo m, esiste $n > 1$ tale

$x^n \equiv x \pmod m \quad \forall x$???

La condizione è: m "libero da quadrati"

$m = p_1 p_2 \cdots p_k$ p_i primi distinti.

Suff. teorema cinese

$$x^n \equiv x \pmod m \iff \begin{cases} x^n \equiv x \pmod{p_1} \\ \dots \\ x^n \equiv x \pmod{p_k} \end{cases}$$

$$\iff \begin{cases} n \equiv 1 \pmod{p_1 - 1} \\ \vdots \\ n \equiv 1 \pmod{p_k - 1} \end{cases} \iff n \equiv 1 \bmod \{m.c.m.(p_1-1, \dots, p_k-1)\}$$

Nota se $p^2 \mid m$

p, p^2, p^3

$p^n \not\equiv p \pmod m \quad \forall n > 1$

RSA

"Mente" : scegli $N = pq$, prodotto di due primi distinti.

N è PUBBLICO

p, q SEGRETI

UTENTI : $X_1, \dots, X_k$

"INDIRIZZI" : $A_1, \dots, A_k$ numeri interi PUBBLICI

Codifica : $x \bmod N \to x^{A_i} \bmod N$

Decodifica : $(x^{A_i})^{B_i} \equiv x \pmod N$

$A_i B_i \equiv 1 \pmod{[p-1, q-1]}$

Chiavi $B_1, \dots, B_k$ sono SEGRETE

Elevare a potenza: A si scrive in base 2

$$x,\ x^2,\ x^4,\ x^8,\ \dots,\ x^{2^{n-1}} = x^{2^n}\cdot x^{2^{n-1}}$$

Se conosco $(p-1)(q-1)$ sarei a posto

$$\| \\ pq - (p+q) + 1$$

$$\| \\ N - (p+q) + 1$$

~~A_1~~ B_1 manda un messaggio a X_2

A_1, B_1 $\qquad$ A_2, B_2

FIRMA DIGITALE: $\quad f \to f^{B_1 A_2}$

$$\left(f^{B_1 A_2}\right) \to \left(f^{B_1 A_2}\right)^{B_2 A_1} = f.$$

Esercizio

$a > 1$ intero

$p^\alpha \| a - 1$ $\qquad$ (p primo)

Qual è la potenza α_n di p che divide esattamente

$p^{\alpha_n} \| a^n - 1$ ...?

$2 \| 3 - 1$ $\qquad$ $2^3 \| 3^2 - 1$

Se p è dispari, e $\alpha > 0$

$$a - 1 = p^{\alpha} b \qquad (b, p) = 1$$

$$a = 1 + p^{\alpha} b$$

Se $(n, p) = 1$ $\qquad a^n = (1 + p^{\alpha} b)^n = 1 + n p^{\alpha} b + \binom{n}{2} p^{2\alpha} b^2 - \cdots$

$$p^{\alpha} \parallel a^n - 1$$

Se $n = p$

$$(1 + p^{\alpha} b)^p = 1 + p \cdot p^{\alpha} b + \binom{p}{2} p^{2\alpha} b^2 + \cdots$$

$$p^{\alpha+1} \qquad p^{2\alpha+1} \qquad (p \neq 2)$$

Se $p = 2$ TUTTI SUCCEDONE

$$p^{\alpha+1} \qquad p^{2\alpha}$$

$$\alpha + 1 = 2\alpha$$

$$\boxed{\alpha = 1}$$