N2

M. GOLLA

Titolo nota 10/09/2008

$(m, n) = 1$ interi coprimi

$$\begin{cases} x \equiv 0 & (m) \\ x \equiv 0 & (n) \end{cases}$$

quali sono le soluzioni intere di questo sistema?

$$\left.\begin{array}{l} m \mid x \\ n \mid x \end{array}\right| \iff m \cdot n \mid x \iff x \equiv 0 \quad (m \cdot n)$$

Il teorema cinese del resto è una generalizzazione di questo fatto.

Teo

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \qquad \text{con} \quad (m_1, m_2) = 1$$

allora esiste un'unica soluzione mod $m_1 \cdot m_2$,

$\exists!$ a intero $(\text{mod } m_1 \cdot m_2)$ t.c. $x \equiv a \pmod{m_1 \cdot m_2}$

es

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 1 \pmod{13} \end{cases} \qquad (12, 13) = 1$$

esiste un'unica soluzione $x \equiv 1 \ (156)$

<u>dim</u> (teorema cinese) Usando Bézout.

Stiamo cercando $x \equiv a_1 \pmod{m_1}$

cioè esiste k tale che $x = a_1 + km_1$

$x \equiv a_2 \pmod{m_2}$

cioè esiste h tale che $x = a_2 + hm_2$

Mettendo insieme le due equazioni,

$$a_2 + hm_2 = x = a_1 + km_1$$

cioè cerchiamo h, k interi tali che $hm_2 - km_1 = a_1 - a_2$.

Questi h, k li possiamo trovare perché $(m_1, m_2) = 1$
(Bézout)

Abbiamo dimostrato l'esistenza delle soluzioni

Unicità?

Prendiamo x_1, x_2 due soluzioni.

$$x_1 - x_2 \equiv a_1 - a_1 \pmod{m_1} \Rightarrow x_1 - x_2 \equiv 0 \ (m_1)$$

$$x_1 - x_2 \equiv \underline{\underline{0}} \pmod{m_2} \Rightarrow x_1 - x_2 \equiv 0 \ (m_2)$$

cioè $x_1 - x_2 \equiv 0 \pmod{m_1 m_2}$. $\square$

Nei casi pratici $\longrightarrow$ Algoritmo di Euclide

Fate l'algoritmo di Euclide per trovare h, k tali che $hm_1 + km_2 = 1$.

E poi moltiplicate per $a_1 - a_2$.

--- o --- o ---

Generalizzazioni: possiamo generalizz. a più equazioni, applicando ripetutamente il teorema cinese (= INDUZIONE).

Th Dati $m_1, \dots, m_k$ interi a due a due coprimi, $a_1, \dots, a_k$ interi

$\exists!$ intero $x \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_k}$

tale che

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k}. \end{cases}$$

$\square$

problema È vero che per ogni $N \geq 1$ esistono N interi interi **consecutivi** dei quali esattamente uno sia una potenza perfetta?

risposta **SÌ**

dim **IDEA** Ne troviamo M consecutivi che non siano potenze perfette, e vinciamo

Beh, se ne abbiamo M consecutivi, andiamo avanti fino alla prima potenza perfetta.

Come facciamo a trovarne M consecutivi non potenze perfette?

Beh, se $x \equiv p \pmod{p^2}$, x NON è una pot. perfetta.

Basta prendere M primi diversi, $p_1, \dots, p_M$
e richiedere che

$$
\begin{aligned}
x \equiv p_2 - 1 \leftarrow \\
x \equiv p_3 - 2 \leftarrow \\
x \equiv p_M - M + 1 \leftarrow
\end{aligned}
\quad
\begin{cases}
X \equiv p_1 \pmod{p_1^2} \\
X + 1 \equiv p_2 \pmod{p_2^2} \\
\vdots \\
X + M - 1 \equiv p_M \pmod{p_M^2}
\end{cases}
$$

moduli coprimi

Quindi il TCR ci assicura che c'è un intero tale che $\{x, \dots, x+M-1\}$ non contiene potenze perfette. $\square$

__problema__ Dimostrare che per ogni n, m, d interi positivi esiste una progressione aritmetica (x_k) di lunghezza $n+1$, di ragione d tale che x_k è divisibile per una potenza m-esima di un intero >1.

__dim__ Scegliamo $p_0, p_1, \dots, p_n$ primi distinti

Vogliamo: $p_0^m \mid x_0$, $p_1^m \mid x_1, \dots, p_n^m \mid x_n$.

Riscrivendo:

$$x_0 \equiv 0 \pmod{p_0^m}$$

$$x_0 + d = x_1 \equiv 0 \pmod{p_1^m} \iff x_0 \equiv -d \ (p_1^m)$$

$$x_0 + 2d = x_2 \equiv 0 \pmod{p_2^m} \iff x_0 \equiv -2d \ (p_2^m)$$

$$\vdots$$

$$x_n \equiv 0 \pmod{p_n^m} \iff x_0 \equiv -nd \ (p_n^m)$$

$$\Rightarrow \begin{cases} x_0 \equiv 0 & (p_0^m) \\ x_0 \equiv -d & (p_1^m) \\ \vdots \\ x_0 \equiv -nd & (p_n^m) \end{cases} \xrightarrow{TCR} \text{Abbiamo vinto } \square$$

(non ottimale, ma funziona)

ϕ di Eulero:

Def: Dato n intero positivo, $\phi(n)$ è il numero di interi k $1 \le k \le n$ coprimi con n (cioè $(n,k)=1$)

es $\phi(1) = 1$
$\phi(2) = 1$
$\phi(3) = 2$
$\phi(4) = 2$

$\phi(p) = p-1$
$\phi(p^k) \overset{?}{=} p^k - p^{k-1}$
$= p^k(1 - 1/p)$

Come si calcola la ϕ?

Prendiamo $n = p_1^{\alpha_1} \cdots p_h^{\alpha_h}$ con $\alpha_i > 0$

Quanti i numeri $k \leq$ coprimi con n?

Quando $p_1 \nmid k$, $p_2 \nmid k$, $\dots$, $p_h \nmid k$

Contiamo questi numeri:

$$n - \frac{n}{p_1} - \frac{n}{p_2} - \dots - \frac{n}{p_h} + \sum_{i<j} \frac{n}{p_i p_j} - \sum \frac{n}{p_i p_j p_k} + \dots =$$

$$n \left(1 - \sum 1/p_i + \sum 1/p_i p_j - \dots \right) =$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_h}\right).$$

$$\phi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_h^{\alpha_h}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_h}\right) =$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) \cdot \ldots \cdot p_h^{\alpha_h}\left(1-\frac{1}{p_h}\right) =$$

$$\phi(p_1^{\alpha_1}) \cdot \ldots \cdot \phi(p_h^{\alpha_h}) =$$

La ϕ è moltiplicativa: cioè

se (m, n) sono primi tra loro

$$\phi(m \cdot n) = \phi(m)\,\phi(n).$$

Vantaggi: per calcolare una funzione moltiplicativa basta calcolarla sulle potenze dei primi.

— o —— o —— o ——

Cosa conta la ϕ?

Conta le classi di resto "invertibili"

Nel senso che conta i k tra $1 \leq .. \leq n$ tali che esiste a con $a \cdot k \equiv 1 \pmod{n}$.

Vogliamo indagare come si comportano le classi di resto mod p rispetto alla moltiplicazione, e in particolare come si comportano le potenze.

Dato x intero, $p \nmid x$ ($x \not\equiv 0 \ (p)$, equivalente a x invertibile), chiamiamo

$\mathrm{ord}_p\, x$ (ordine di x modulo p)

il più piccolo intero $k>0$ tale che

$$x^k \equiv 1 \pmod p$$

$x^1, x^2, \dots, x^p \rightsquigarrow$ stanno in $p-1$ classi di resto. (perché $p \nmid x \Rightarrow p \nmid x^k$ per nessun k).

Quindi ci sono h, k tali che $x^h \equiv x^k \ (p)$.

$$x^{h-k} \equiv 1 \ (p).$$

Se $x^m \equiv 1 \ (p)$ allora $\mathrm{ord}_p x \mid m$.

$$\underbrace{x^m \equiv 1}_{\text{ipot.}}, \quad \underbrace{x^{\mathrm{ord}\, x} \equiv 1}_{\text{def}} \Rightarrow x^{hm} \cdot x^{k\, \mathrm{ord}\, x} \equiv 1 \ (p).$$

$$\mathrm{ord}_p x = (\mathrm{ord}_p x, m). \Longleftarrow x^{hm + k\, \mathrm{ord}\, x} \equiv 1 \ (p)$$

Oss Le potenze sono periodiche (mod p), e il periodo è l'ordine.

th (Piccolo teorema di Fermat)

$$x^{p-1} \equiv 1 \pmod p \quad [(x,p)=1]$$

Riformulando $\mathrm{ord}_p x \mid p-1 = \phi(p)$.

dim Prendiamo x $\{1, \dots, p-1\}$

$\{1\cdot x, \dots, (p-1)\cdot x\}$ cos'è?

x è invertibile, quindi l'insieme delle classi di resto $\{1, \dots, p-1\} \overset{\text{mod } p}{=} \{x, \dots, (p-1)x\}$

$$1 \cdot 2 \cdot \ldots \cdot p-1 = x \cdot 2 \cdot x \cdot \ldots \cdot (p-1) \cdot x =$$

$$= x^{p-1} \left(1 \cdot \ldots \cdot (p-1)\right).$$

$$\Downarrow$$

$$x^{p-1} \equiv 1 \pmod{p}.$$

<u>es</u> $1 + 3^n + 5^n$ primo $\Rightarrow$ $12 \mid n$.

$n = 0$: $1 + 1 + 1 = 3$

$n = 1$: $1 + 3 + 5 = 9$ $\longleftarrow$ div. per 3

$\longrightarrow$ $n = 2$: $1 + 9 + 25 = 35$ $\longleftarrow$ div per 5, 7

$n = 3$: $1 + 27 + 125 = 153$ $\longleftarrow$ div. per 3, 17.

$$1 + \cancel{3^{2k+1}} + 5^{2k+1} \equiv 1 + (-1)^{2k+1} \pmod{3}$$

$$\cancel{3^{2k+1}} \downarrow 0 \qquad 5^{2k+1} \downarrow \underline{\phi(3) = 2} \qquad (-1)^{2k+1} = -1 \qquad \equiv 0$$

Lavoriamo modulo 5:

$$1 + 3^n + \cancel{5^n} \equiv ? \pmod 5$$

$\phi(5) = 4$ cosa fa 3^n per $n = 0, 1, 2, 3$.

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv -1, \quad 3^3 \equiv 2$$

n è ~~pa~~ pari ma <u>non</u> divisibile per 4

$$n = 4k+2$$

$$1 + 3^n = 1 + \underbrace{(3^4)^k}_{\equiv 1 \pmod 5} \cdot 3^2 \equiv 1 + 3^2 \ (5).$$

Se n non è divisibile per 4, o 3, o 5 dividono $1 + 3^n + 5^n$.

mod 7?

$$1 + 3^n + 5^n \pmod 7$$

$\phi(7) = 7 - 1 = 6$ questa cosa è periodica di periodo 6.

	$n=0$	$n=1$	$n=2$	3	$n=4$	5
$3^n \longrightarrow$	1	3	$\boxed{2}$	-1	$\boxed{4}$	5
$5^n \longrightarrow$	1	-2	$\boxed{4}$	-1	$\boxed{2}$	3
			$1+2+4$		$1+4+2$	

Se $n \equiv \pm 2 \pmod 6$

$7 \mid 1 + 3^n + 5^n$

Se $n \equiv \pm 2 \pmod 6 \longrightarrow$ quel numero non è un primo.

Riassumendo: abbiamo escluso i dispari
abbiamo escluso i non divisibili
per 4, e i pari non
divisibili per 3.

Restano solo i multipli di 12.

Dice che se $1+3^n+5^n$ è primo
ALLORA $12 \mid n$. Non dice che
$1+3^{12k}+5^{12k}$ è primo per ogni k. No.

problema Fissiamo p primo

E' vero che esistono infiniti

n tali che $p \mid \underline{2^n - \underline{n}}$?

risposta SÌ!

idea Limitiamoci agli $n \equiv 1 \ (p)$.

Se $n \equiv 1 \pmod p$, cerchiamo

n tale che $2^n \equiv 1 \pmod p$

(cioè $p \mid 2^n - 1 \equiv 2^n - n$).

A questo punto, abbiamo praticamente vinto: basta che $p-1 \mid n$.

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

$$\begin{cases} n \equiv 1 \pmod p \\ n \equiv 0 \pmod{p-1} \end{cases}$$

$(p, p-1) = 1 \implies$ esiste la soluzione

Avendo n, $n + (p-1)p$ va bene. $\square$

Analogie che si hanno mod n / mod p.

Caso corollario: tutti i numeri $1 \leq k \leq p$ sono coprimi con p.

NON tutti i numeri $1 \leq k \leq m$ sono coprimi con m.

OSS (x, m) sono coprimi, le potenze di x continuano ad essere periodiche modulo m.

(identica dimostrazione)

oss 2 Il periodo (ordine) non dividerà in generale $m-1$ però (con la stessa identica dimostrazione)

th $$x^{\phi(m)} \equiv 1 \pmod{m}.$$

Qui torna la ϕ.

problema abbiamo a n interi

Costruiamo la successione

$a, \quad a^e, \quad a^{e^e}, \ldots$

Dimostrare che questa successione è costante (da un certo punto in poi) mod n.

Se $n = p^2$, $e = p$ $\qquad e \equiv p$,

$$a^e \equiv 0 \quad (p^2).$$

$a = db$, con $d = (a, n)$

D = prodotto di tutti i primi che dividono d con gli esponenti con cui dividono n.

$a = 6, \quad n = 20 \qquad d = 2, \quad D = 4$

$a = 42, \quad n = 980 \qquad d = 14, \quad D = 196$

$n = D \cdot m.$

Consideriamo la successione mod m, e mod D.

mod D la successione diventa 0.

(gli esponenti dei primi crescono).

Prendiamo $p \mid \cancel{a}$, $\quad p^\alpha \| D$

Ad un certo punto, $p^\alpha \mid a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}$

Vale per ogni $p \mid D$, quindi la successione è definitivamente 0 (è 0 da un certo punto in poi)

Max m : $(m, a) = 1$. perché abbiamo tolto a n tutti i fattori primi in comune con a.

Ci basta dimostrarlo per $(a, m) = 1$.
(perché i primi in comune non rompono le scatole)

(a_k) → la nostra successione.

è costante se la successione

degli esponenti è costante mod $\phi(n)$.

Da un certo punto in poi, se gli esponenti sono costanti mod $\phi(n)$

Da un certo punto in poi, $esp_k - esp_{k+1}$ è un multiplo della $\phi(n)$.

$$a_{k+1} = a^{esp_{k+1}} = a^{esp_k + \alpha\phi(n)} =$$

$$= a^{esp_k} \cdot \left(a^{\phi(n)}\right)^{\alpha} = a^{esp_k} = a_k$$

~~di po~~ La successione degli esponenti è la successione a_k stessa.

Cioè ci basta dimostrare che Q_k è

costante mod $\phi(n)$.

Il ragionamento circolare.

Formalmente: INDUZIONE ESTESA su n.

Supponiamo che sia vera la tesi per $k \leq n$.

Allora in particolare Q_k è costante

mod $\phi(n)$. $\longrightarrow$ abbiamo vinto. $\square$

Struttura moltiplicativa <u>mod p</u>. [primo]

<u>Th</u> (Ciclicità) Esiste un generatore modulo p.

<u>Cioè</u> Esiste g intero tale che

$\{g, g^2, g^3, \ldots, g^{p-1}\}$ sia l'insieme di tutte le classi di resto $\neq 0$ modulo p.

<u>es</u> mod 2 : c'è una classe di resto $\neq 0$.

mod 3 : ce ne sono 2 $g \equiv -1 \ (3)$.

mod 5 : basta prendere $g = 2$.

$2, \quad 2^2 = -1, \quad 2^3 \equiv -2, \quad 2^4 \equiv 1 \pmod 5$

2 è un generatore $\pmod 5$

Quando g è un generatore mod p?

Basta controllare a $\phi(p)/q$ [al variare dei q <u>primi</u> che dividono la $\phi(p)$]

Basta controllare che $g^{\phi(p)/q} \not\equiv 1 \pmod p$

<u>Perché?</u>

es 1. Quanti sono i residui quadratici mod p?

2. Quanti i residui k-esimi?

1. Lo 0 è un residuo quadratico. (ed è il quadrato di 0).

Per gli altri, chiamo g un generatore mod p.

Una classe di resto è della forma g^k, e il suo quadrato è g^{2k}.

La domanda diventa: quanti sono i numeri della forma g^{2k}?

$\longrightarrow$ quanti sono i numeri del tipo

$2k \pmod{\phi(p)}$? (cioè mod $p-1$)?

Sono $\boxed{\dfrac{p-1}{2}}$

Quindi i residui quadratici sono $\dfrac{p+1}{2}$

La domanda 2 ha qualche piccola complicazione, ma è la stessa cosa.

[la risposta dipende da $MCD(p-1, k)$.

* Domanda: quando -1 è un residuo quadratico?

Oss -1 è sempre una somma di due quadrati $\pmod p$.

(se e solo se)

* Risposta, ~~ss~~ solo è quando $p \equiv 1 \pmod 4$.

Perché? $g^{2k} \equiv -1 \pmod p$, dove

g è un generatore

$g^{4k} \equiv 1 \pmod p$. $\Rightarrow \Phi(p)$ è divisibile

per 4.

Vogliamo far vedere che se $g^{2k} \equiv -1 \Rightarrow 4 \mid p-1$.

$$2k \not\equiv 0 \pmod{p-1} \qquad \Big| \qquad k \not\equiv 0 \ \left(\tfrac{p-1}{2}\right)$$

$$4k \equiv 0 \pmod{p-1} \qquad \Big| \qquad 2k \equiv 0 \ \left(\tfrac{p-1}{2}\right).$$

Se (per assurdo) $\frac{p-1}{2}$ dispari, 2 invertibile mod $\frac{p-1}{2}$, cioè

$k \equiv 0 \pmod{\frac{p-1}{2}} \Longleftrightarrow 2k \equiv 0 \pmod{\frac{p-1}{2}}$.

Altra frase. Se $p \equiv 1 \pmod 4$, cosa fa $g^{\frac{p-1}{2}}$? $x = g^{\frac{p-1}{2}}$.

$$x^2 = \left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} = 1 \pmod p$$

$(x^2 - 1) \equiv 0 \pmod p$

- $x \equiv 1$ no, perché g generatore
- $x \equiv -1$

Sfruttiamo $4 \mid p-1$, per dire che

$$\frac{p-1}{2} = 2 \cdot \frac{p-1}{4} \qquad x \equiv -1 \equiv \left(g^{\frac{p-1}{4}}\right)^2.$$

cioè è un residuo quadratico. $\square$

Torniamo ai residui k-esimi.

Quanti sono i residui k-esimi mod p?

Stiamo cercando quanti sono i residui della forma g^{hk} (al variare di h)

$\Updownarrow$

Quanti sono i numeri della forma

$k \cdot h$ (modulo $p-1$).

Prendiamo $d = (p-1, k)$.

$k = d \cdot k'$ $\quad \left(k', \frac{p-1}{d}\right) = 1$.

I numeri della forma $k \cdot h$ $(p-1)$ sono

i numeri della forma $k' \cdot h$ $\left(\frac{p-1}{d}\right)$

Ma k' è invertibile mod $\frac{p-1}{d}$, quindi

i residui k-esimi sono $1 + \frac{p-1}{d} = \frac{p-1}{(k, p-1)} + 1$.

$\boxed{\text{lo } 0}$

ex $p^p - 1$ ha un fattore primo $\equiv 1 \pmod{p}$.

Sol Prendiamo $q \mid p^p - 1$.

Allora $p^p \equiv 1 \pmod{q}$.

Cioè $\mathrm{ord}_q p \mid p$ $\begin{cases} 1 \longrightarrow \text{caso "cattivo"} \\ p \longrightarrow \text{caso buono} \end{cases}$

Se $\mathrm{ord}_q p = 1$, $p^1 \equiv 1 \ (q)$

Viceversa se $\mathrm{ord}_q p = p$, vuol dire che $p \mid q-1$, cioè $q-1 \equiv 0 \ (p)$, cioè $q \equiv 1 (p)$

Caso cattivo? $q \mid p^p - 1 = (p-1)(p^{p-1} + p^{p-2} + \dots + p + 1)$

e scegliamo $q \mid \underline{p^{p-1} + \dots + 1} = S$

Supponiamo che q sia un primo cattivo.

$$\underline{p \equiv 1 \ (q)}, \quad S \equiv p^{p-1} + \dots + 1 \equiv \underbrace{1^{p-1} + \dots + 1}_{p \text{ addendi}} \equiv$$

$$p \equiv 0 \pmod q$$

assurdo

$$\underline{p \equiv 0 \pmod q}.$$

— o — o — o —

C'è un generatore (modulo $\underline{p}$)

E vi ho detto che non è vero per m generico.

E' vero che c'è un generatore (delle classi invertibili) <u>solo</u> per $m = 2, 4, p^k, 2 \cdot p^k$ (p primo "DISPARI", k intero positivo).

$m = a \cdot b$, con a, b non potenze di 2, primi tra loro,

allora m non ammette un generatore

Prendiamo $(x, m) = 1$.

$$x^{\frac{\phi(m)}{2}} \quad (\text{sicuramente } \phi(m) \text{ è pari}).$$

Se ↑ fa 1 per ogni x, sicuramente

m non ammette generatori

$$x^{\frac{\phi(m)}{2}} \pmod{a} \qquad \phi(m) = \phi(a) \cdot \phi(b)$$

perché a, b coprimi per ipotesi!

Quindi $x^{\frac{\phi(m)}{2}} = x^{\phi(a) \cdot \frac{\phi(b)}{2}} \to$ intero!

Cioè $\quad x^{\phi(m)/2} \equiv \left(x^{\phi(a)}\right)^{\phi(b)/2} \equiv 1^{\phi(b)/2} \equiv 1 \ (a)$

$$x^{\phi(m)/2} \equiv 1 \quad (b).$$

$y = x^{\phi(m)/2}$ $\qquad \begin{cases} y \equiv 1 & (a) \\ y \equiv 1 & (b) \end{cases}$

$$\Downarrow \text{TCR}$$

$$x^{\phi(m)/2} \equiv 1 \quad (\text{mod } m).$$

x <u>NON</u> è un generatore

Sapendo che c'è un generatore mod p,
quanti sono i generatori?
Sono $\phi(\phi(p))$. :)

Come si fa?
Se abbiamo un generatore, gli altri generatori
cioè esiste k tale che $g' = g^k$
Cioè, per quali k g^k è ancora un generatore?
Per i k coprimi con $\phi(p)$.
Se g^k è un generatore allora deve prendere

anche g, cioè $\exists\, a$ tale che $g^{ak} = g$

cioè $ak \equiv 1 \pmod{\phi(p)}$.

(perché le potenze di x sono periodiche di periodo $\mathrm{ord}_p x \pmod p$, e $\mathrm{ord}_p g = \phi(p)$ per definizione di generatore)

$\to$ Cioè k invertibile mod $\phi(p)$.

Se k invertibile, si torna indietro!

Quindi g^k genera $\Longleftrightarrow (k, \phi(p)) = 1$.

Quanti sono i k? Sono $\phi(\phi(p))$. $\square$