Teoria dei numeri 1 — Basic [Tess]

Note Title 06/05/2021

Congruenze

dato un numero $m \in \mathbb{Z}_{>0}$ detto modulo

relazione di equivalenza in $\mathbb{Z}$

$a \equiv b \pmod m$ quando $m \mid a-b$

Segue che le somme e i prodotti si comportano bene

$(a+b)_{\bmod m} = a_{\bmod m} + b_{\bmod m}$

$(a \cdot b)_{\bmod m}$ " "

Attenzione alla divisione:

non posso aspettarmi che se $a \equiv b \pmod m$

e $d \mid a$ e $d \mid b$

$a/d \equiv b/d \pmod m$

$8 \equiv 4 \pmod 4$

$8/2 \not\equiv 4/2 \pmod 4$

$ad \equiv bd \pmod m$ se $(d, m) = 1$

$\exists c$ t.c. $cd \equiv 1 \pmod m$

(inverso moltiplicativo)

$\Rightarrow a \equiv adc \equiv bdc \equiv b \pmod m$

se $d \mid m$ $m = dm'$

$\Rightarrow a \equiv b \pmod{m'}$

Note Title 06/05/2021

Gli inversi moltiplicativi ci permettono di usare le frazioni

IMO 2005 1 $\forall (n, 6) = 1$ trovare m t.c.

$$2^m + 3^m + 6^m \equiv 1 \quad (n)$$

$m = -1 \quad \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$

$\frac{1}{2}$ mod n deve essere l'unico numero t.c. $2 \cdot \frac{1}{2} \equiv 1 \quad (n)$

Tutto ciò funziona non solo su $\mathbb{Q}$, ma anche mod n t.c. $(n, 6) = 1$

Teorema Cinese del resto

Siano $(a, b) = 1$ allora il sistema di congruenze

$$\begin{cases} x \equiv y_0 \quad (a) \\ x \equiv z_0 \quad (b) \end{cases}$$

ammette un'unica soluz. mod ab

Quindi conviene sempre lavorare mod potenze di primi.

φ di Eulero

$\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ è definita da

$$\varphi(n) = \left| \{ i = 1, \dots, n \text{ t.c. } (i, n) = 1 \} \right|$$

Es: dimostrare che $\sum_{d \mid n} \varphi(d) = n$.

Proprietà fondamentale di φ: moltiplicatività

Lemma: $\forall\, a, b \in \mathbb{Z}_{>0}$ t.c. $(a,b) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Dim: Con TCR:

Quando calcolo $\varphi(ab)$ mi chiedo $1 \le i \le ab$ primi con ab

$$(i, ab) = 1 \iff \begin{cases} (i,a) = 1 \\ (i,b) = 1 \end{cases}$$

$$\left\{ i \text{ t.c. } (i,ab) = 1 \right\}_{1 \le i \le ab} \overset{+TCR}{\longleftrightarrow} \left\{ (i,j) \begin{matrix} 1 \le i \le a \\ 1 \le j \le b \end{matrix} \text{ t.c. } \begin{matrix} (i,a) = 1 \\ (j,b) = 1 \end{matrix} \right\}$$

esiste una bigezione per il TCR

$$\left\{ 1 \le i \le a : (i,a) = 1 \right\} \times \left\{ 1 \le j \le b : (j,b) = 1 \right\}$$

guardo le cardinalità:

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Es $\varphi(12) = \varphi(3 \cdot 4) = \varphi(3)\varphi(4) = 2 \cdot 2$

In generale $\varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$

Potenze mod m

assumiamo che $m = p^k$ dove p è primo

dato $a \in \mathbb{Z}/m$ (= classe di resto mod m)

$a^0, a^1, a^2, \ldots$ mod m

Oss: La successione deve ripetersi da un certo punto in poi

Pigeonhole: $\exists\, 0 \le i < j \le m$ t.c. $a^i \equiv a^j \pmod m$

Il termine $i+1$-esimo dipende unicamente da i-esimo

$$a^{i+1} \equiv a \cdot a^i$$

$\Rightarrow$ se $a^i \equiv a^j$, allora $a^{i+1} \equiv a^{j+1}$

Dunque esiste un periodo

$a^0, a^1, a^2, \ldots, a^i \ldots a^j$

periodo

Oss: Se ho una succ. del tipo $a_{n+2} = \lambda \cdot a_{n+1} + \mu a_n$
il termine $i+2$ dipende soltanto dalla classe di:

a_{i+1} e a_i

$(i, i+1)$ $(j, j+1)$

Oss: Se $(a, p^k) \neq 1$ $(p \mid a)$

allora la succ è definitivamente nulla (almeno dal k-esimo termine)

Oss: Se $(a, p^k) = 1$?

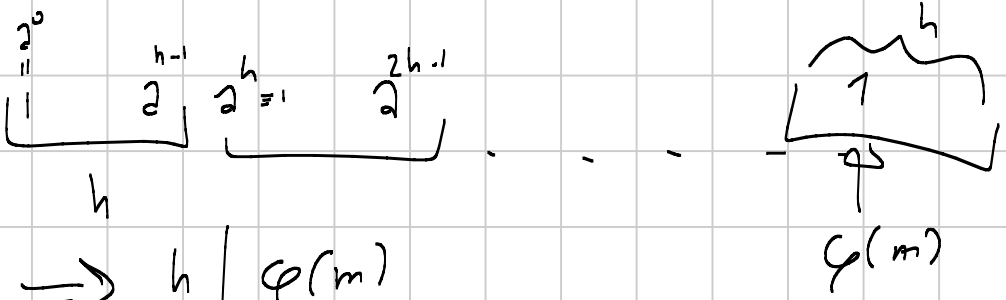
$a^i \equiv a^j \quad (p^k)$

$a^{i-1} \equiv a^{j-1} \quad (p^k)$

$a^0 = 1 \equiv a^{j-i}$ Non c'è l'ant. periodo.

Thm (Eulero - Fermat)

Se $(a, m) = 1$ allora $a^{\varphi(m)} \equiv 1 \quad (m)$.



$\Rightarrow h \mid \varphi(m)$

Questo h è detto $\operatorname{ord}_m(a)$ "ordine moltiplicativo"

L'inverso di a mod m è $a^{\varphi(m)-1} =: b$

$$ab = a^{\varphi(m)} \equiv 1 \qquad a^{\varphi(m)-1} \equiv \frac{1}{a}$$

Dim di Eulero-Fermat:

$$A = \{1 \le i \le m \text{ t.c. } (i,m) = 1\} = \{x_1, \dots, x_{\varphi(m)}\}$$

$$B = \{ax_1, ax_2, \dots, ax_{\varphi(m)}\}$$

in realtà $|B| = |A|$ $\qquad ax_i \equiv ax_j \Rightarrow x_i \equiv x_j \pmod m$

in effetti: $A = B$ $\qquad$ se fosse $(ax_i, m) \neq 1$

$\Rightarrow \exists p \mid m \quad p \mid ax_i \Rightarrow p \mid a \nmid p \mid x_i$

ora il prodotto è lo stesso

$$x_1 \cdot \dots \cdot x_{\varphi(m)} \equiv ax_1 \cdot \dots \cdot ax_{\varphi(m)} = a^{\varphi(m)} x_1 \cdot \dots \cdot x_{\varphi(m)}$$

$$\Rightarrow \qquad 1 \equiv a^{\varphi(m)}.$$

Se $n = p$ primo $\qquad \varphi(p) = p-1$

$$a^{p-1} \equiv 1 \pmod p \quad \forall\ (a,p) = 1$$

$$q(x) = x^{p-1} - 1 \in \mathbb{Z}[x]$$

Il teorema di F-F mi dice che tutti $1, \dots, p-1$ sono zeri di $q(x) \bmod p$

$$q(a) \equiv 0 \ (p) \quad \forall a = 1, \dots, p-1$$

se 1 è radice, allora $\quad q(x) = (x-1)\, q_1(x)$

se 2 è radice di $q \qquad q_1(x) = (x-2)\, q_2(x)$

ma implica che 2 sia radice di q_1!

alla fine ho fattorizzato $\quad x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1)$

Cor: Thm di Wilson: $(p-1)! \equiv -1 \pmod p \quad (p > 2)$

Basta valutare in 0: $\quad -1 \equiv (-1)(-2)\cdots(-p+1)$

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

Ottengo anche: $\quad 0 \equiv 1 + \dots + (p-1)$

$$0 \equiv \sum_{1 \le a \le b \le p-1} ab$$

$$1^2 + 2^2 + \dots + (p-1)^2 = \left(1 + \dots + p-1\right)^2 - 2 \sum_{1 \le a < b \le p-1} ab \equiv 0 \ (p)$$

Def: a è detto generatore moltiplicativo mod m se $(a,m)=1$ e $\{a^0, \dots, a^{\varphi(m)}\} = \{1 \le i \le m, (i,m)=1\}$

Oss: ciò è equivalente a dire che $ord_m(a) = \varphi(m)$

Es: Se $\exists$ un generatore g mod m allora $\forall k < \varphi(m)$

$$\sum_{\substack{a: \\ (a,m)=1}} a^k \equiv 0 \pmod m$$

Sol: Dato che esiste un g generatore, $a = g^b$ $\forall a \exists b$

$$\sum_{\substack{a: \\ (a,m)=1}} a^k \equiv \sum_{b=0}^{\varphi(m)-1} (g^b)^k = \sum_{b=0}^{\varphi(m)-1} (g^k)^b = \frac{(g^k)^{\varphi(m)} - 1}{g^k - 1}$$

questo concluderebbe se $(g^k - 1, m) = 1$, perché il num. è nullo mod m

Se m è primo funziona meglio perché non funziona solo quando $g^k - 1 \equiv 0 \pmod p$

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

$$ord_p g \mid k$$

$$p-1 \mid k$$

$p - 1 \le k$ non capita per ipotesi.

Es N2 -10: $D = \{ n > 1 : n \mid 2^n + 1 \}$

Mostrare che tutti i numeri in D sono multipli di 3

Sol: $2^n + 1 \equiv 0 \pmod{n}$

$2^n \equiv -1 \pmod{n}$

$2^{2n} \equiv 1 \pmod{n}$

$\text{ord}_n 2 \mid 2n$

$\text{ord}_n 2 \mid \varphi(n)$ (E-F)

Oss: se fosse $\text{ord}_n(2) = 2$

$\Rightarrow 2^2 \equiv 1 \pmod{n} \Rightarrow n \mid 3$

Sia $p \mid n$, il più piccolo primo

$2^n \equiv -1 \pmod{p}$

$2^{2n} \equiv 1 \pmod{p}$

$\text{ord}_p(2) \mid 2n$

$\text{ord}_p(2) \mid \varphi(p) = p - 1$

tolgo tutti i fattori primi di n

$\Rightarrow \text{ord}_p(2) \mid (2n, p-1) = (2, p-1) = 2$

perché $p > 2$

$2^2 \equiv 1 \pmod{p} \Rightarrow p = 3$

Quando esistono generatori?

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

E in nessun altro caso

Quanti generatori esistono in questi casi?

$g^0, g^1, \ldots, g^{\varphi(m)-1}$

g^i è generatore?

Mi basta controllare che g^i abbia ordine massimo $(= \varphi(m))$

$$(g^i)^{\varphi(m)} \equiv 1$$

voglio trovare gli i t.c. $(g^i)^k \not\equiv 1 \quad \forall k < \varphi(m)$

$$g^{ik}$$

Oss: Se ho un generatore, la moltiplicazione mod m corrisponde alla somma mod $\varphi(m)$

$g^0 g^1 \ldots g^{\varphi(m)-1}$

la corrisp.

$0 \; 1 \; \ldots \; \varphi(m)-1$

Basta trovare gli i t.c. $\exists k$ t.c. $ik \equiv 1 \quad (\varphi(m))$

voglio quindi: $(i, \varphi(m)) = 1$

Quindi: , se $\exists$ un generatore, ne esistono $\varphi(\varphi(m))$.

Studio dell'elevazione a potenza.

$$f: \mathbb{Z}/m^* \longrightarrow \mathbb{Z}/m^* \qquad \left(\mathbb{Z}/m^* = \text{le classi di resto primi con } m\right)$$

$$f(x) = x^k$$

Se $k=1$ è l'identità

Se $k = \varphi(m)$ f è la costante 1

Se $(k, \varphi(m)) = 1$ $\quad \exists\, h : hk \equiv 1 \ (\varphi(m))$

$$x \mapsto x^k \mapsto \left(x^k\right)^h = x^{kh} = x^{1 + N\varphi(m)} \equiv x^1 \ (m)$$

$$x^{\varphi(m)} \equiv 1 \ (m)$$

Questo significa che l'elevazione x^k è invertibile

$$g(f(x)) = x \Rightarrow f \text{ è iniettiva}$$

Es: Quanti sono i cubi mod 5!

$$\left|\{ i^3 : 0 \le i < 5 \mod 5 \}\right| \qquad (3, \varphi(5)) = 1$$

Cosa succede se $k \mid \varphi(m)$?

In questo caso f NON è iniettiva

se ho un generatore:

$$g^0, g^1, \dots, g^{\varphi(m)-1}$$

$$g^0, g^k, g^{2k}, \dots, g^{k(\varphi(m)-1)}$$

$\varphi(m) = kd$

allora $(g^d)^k = 1 = g^0$

dunque g^d è il primo numero che finisce in 1

se $(g^{d'})^k = 1 \Rightarrow \operatorname{ord} g \mid d'k < dk = \varphi(m)$

l'immagine di f ha cardinalità $\frac{\varphi(m)}{k}$ (se ho un gen.)

e le controimmagini di 1 sono $(g^d)^i$

e sono esattamente k.

Def: le immagini di f si chiamano residui k-esimi.

IMO 2021 1

Sono date delle carte numerate $n, n+1, n+2, \dots, 2n$ $(n \geq 100)$

e vengono divise in 2 pile.

Dimostrare che una delle pile contiene 2 carte la cui somma è un quadrato perfetto.

Sol: Voglio trovare un triangolo dentro $\{n, \dots, 2n\}$

$a, b, c \in$ ——————

$$\text{t.c.} \begin{cases} a+b = x^2 \\ b+c = y^2 \\ c+a = z^2 \end{cases}$$

scelgo x, y, z consecutivi; $x = k-1$, $y = k$, $z = k+1$

$b < a < c$

$$b = \frac{(k-1)^2 + k^2 - (k+1)^2}{2} = \frac{k^2 - 4k}{2}$$

$a = \dots$

$$c = \frac{(k+1)^2 + k^2 - (k-1)^2}{2} = \frac{k^2 + 4k}{2}$$

Risulta che a, b, c vanno bene purché k pari:

- $n \le b$
- $c \le 2n$

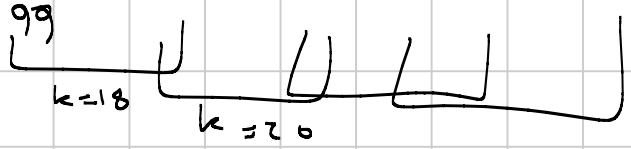
Per undato k pari funzionano tutti gli n t.c.

$$I(k) = \frac{k^2 + 4k}{4} \le n \le \frac{k^2 - 4k}{2} = S(k)$$

mi basta prendere k abbastanza grande da avere

$$S(k) \ge I(k+2) \iff k \ge 18$$

con $k = 18$ $\quad I(18) = 81 + 18 = 99$



□.

Esercizi:

da Esercitario parte 1 42, 45, 49, 52, 62, 63, 66

da Esercitario parte 2 N1: 3, 6, 10

" " N2: 1, 6, 10

da foglio 2021 : 1, 4, 5, 10, 11, 15

Correzione

Es 52 $n^k \equiv 2 \pmod{100}$ con $k > 1$

$$\begin{cases} n^k \equiv 2 \pmod 4 \\ n^k \equiv 2 \pmod{25} \end{cases}$$

se $n^k \equiv 2 \pmod 4$

$\Rightarrow n^k \equiv 2 \pmod 2 \Rightarrow n \equiv 0 \pmod 2$

$2^k \mid n^k$

$4 \mid n^k$ se $k \geq 2 \Rightarrow n^k \equiv 0 \pmod 4$

Es 62

$$\begin{cases} n \equiv 0 & (p_1^5) \\ n+1 \equiv 0 & (p_2^5) \\ n+2 \equiv 0 & \\ \vdots & \\ n+2012 = 0 & (p_{2013}^5) \end{cases}$$

Sol: prendere p_i primi fra loro (ad esempio primi)

si conclude con il TCR.

ES 63

- $\{2^k \mod 100\}$
- $\{2^k \mod 1000\}$
- $\{7^k \mod 100\}$

$2^k \mod 100$ in realtà studio $2^k \mod 4$ $\mod 25$

$\mod 4$ $2^0\ 2^1\ 2^2 \ldots$

$1\ 2\ \underbrace{0}_{\text{periodo}}\ 0\ 0 \ldots$ (antiperiodo)

$\mod 25$ $2^0\ 2^1\ 2^2\ 2^3\ 2^4\ 2^5 \ldots 2^{10} \ldots \quad 2^{20}$

$1\quad 2\quad 4\quad 8\quad 16\quad 7\quad -1\quad 1$

so che $2^{\varphi(25)} \equiv 1 \quad (25)$

$2^{20} \equiv 1 \quad (25)$

Es 66 $4^{(55^{666^{7777}})} \mod 23$

Sol: le potenze di 4 si ripetono mod 23 ogni $\text{ord}_{23} 4 = n$

poi calcolo $55^{666^{7777}} \mod n$

ora calcoliamo $\text{ord}_{23} 4 \mid \varphi(23) = 22$

devo decidere se è 11 o 22

non può essere 22 $\quad 4^{11} = 2^{22} \equiv 1$

altrimenti: $\text{ord}_{23} 2 = 44$

rimane da calcolare $55^{666^{7777}}$ mod 11 che è 0

quindi: $4^{\cdots} \equiv 4^0 = 1 \pmod{23}$

Es N1 - 6 $\quad MCD\left(\left\{p^4 - q^4 \text{ al variare di } p,q > 10 \text{ primi}\right\}\right)$

Quando si cerca un massimo occorre fornire 2 stime
la stima dal basso significa trovare un divisore comune
la stima dall'alto significa dire che non può essere più grande

mod 8	1	3	-3	-1
residui quadr	1	1	1	1

quind: $p^2 - q^2 \equiv 1 - 1 \equiv 0 \pmod 8$

quind: $p^4 - q^4 = (p-q)(p+q)(p^2+q^2)$
è multiplo di 2^4

mod 3 $\quad p^4 \equiv 1$

$p^4 - q^4 \equiv 1 - 1 \equiv 0$

mod 5 $\quad p^4 \equiv 1 \qquad p^4 - q^4 \equiv 0$

per ora $\quad 2^4 \cdot 3 \cdot 5 \mid MCD$

$MCD \mid \dots$

prendiamo $\quad p = 13 \quad q = 11$

$$p^4 - q^4 = 2 \cdot 24 \cdot 290 = 2^5 \cdot 3 \cdot 29 \cdot 5$$

con $p = 29$ e $q = 11$ scopriamo che 29 non va

$p = 17 \quad q = 13 \qquad 2^4 \parallel p^4 - q^4 \dots$

$$MCD \mid MCD\left(13^4 - 11^4,\ 29^4 - 11^4,\ 17^4 - 13^4\right) = 2^4 \cdot 3 \cdot 5$$