Teoria dei Numeri 2 - Basic

Note Title 9/6/2017

Tess

Es: quanti sono gli interi $2001 \le n \le 2099$ t.c.

(TI 14) $1 + n + \frac{n^2}{2!} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!} \in \mathbb{Z}$

Sol: Oss: $6!\, p(n) \in \mathbb{Z}$

Idea: guardare ogni primo

(sono solo $p \mid 6!$, $2, 3, 5$)

Proviamo con $p=5$

$6! + 6!n + \frac{6!}{2!} n^2 + \dots + 6 \cdot n^5 + n^6 \equiv 0 \quad (5)$

$n^5 + n^6 \equiv 0 \quad (5)$

$\iff 5 \mid n^5 \cdot (n+1) \iff 5 \mid n \ \vee \ 5 \mid n+1$

$\iff n \equiv 0 \ \vee \ n \equiv -1 \quad (5)$

Proviamo con $p=3$

dovrei guardare mod 9, intanto guardo mod 3

$\dots \quad 3 \mid n^6 \implies n \equiv 0 \ (3)$

lo stesso si vede per $p=2$, $n \equiv 0 \ (2)$

$$\begin{cases} n \equiv 0 \quad (2) \\ n \equiv 0 \quad (3) \\ n \equiv 0 \quad (5) \end{cases} \qquad \begin{cases} n \equiv 0 \quad (2) \\ n \equiv 0 \quad (3) \\ n \equiv -1 \quad (5) \end{cases}$$

Th (Cinese del resto):

se ho un sistema di congruenze:

$$\begin{cases} x \equiv a_1 \quad (m_1) \\ x \equiv a_2 \quad (m_2) \end{cases}$$

se $(m_1, m_2) = 1$ allora $\exists$ unica sol. x modulo $m_1 \cdot m_2$

Dim: cerco $x = h m_1 + a_1$

voglio trovare h t.c. $x \equiv a_2 \quad (m_2)$

$$h m_1 + a_1 \equiv a_2 \quad (m_2)$$

$$h m_1 \equiv a_2 - a_1$$

$\exists$ l'inverso molt. di m_1 mod m_2 (m_1, m_2 sono coprimi)

$$\Rightarrow h \equiv (a_2 - a_1)\, m_1^{-1} \quad (m_2)$$

Ora $x = h m_1 + a_1$ sicuramente funziona

Per l'unicità: supponiamo che x_0, x_1 siano soluzioni del sistema, allora

$$x_0 \equiv x_1 \pmod{m_1 \cdot m_2} \iff m_1 m_2 \mid x_0 - x_1$$

$$\iff m_1 \mid x_0 - x_1 \quad \wedge \quad m_2 \mid x_0 - x_1$$

perché $(m_1, m_2) = 1$

ma queste condizioni traducono l'ipotesi.

Oss: Cosa faccio se mi ritrovo moduli non coprimi?

Es:
$$\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases}$$

$$\rightarrow \begin{cases} x \equiv 7 \pmod{2} \\ x \equiv 7 \pmod{5} \\ x \equiv 8 \pmod{3} \\ x \equiv 8 \pmod{5} \end{cases}$$

problema $\Rightarrow$ No soluzioni

Es: (IMO 2016.4)

$P(n) = n^2 + n + 1$ det. il min b t.c.

$\{P(a+1), P(a+2), \dots, P(a+b)\}$ sia "profumato"

per un opportuno a intero non negativo.

Sol: [...]

min $b = 6$

non si fa di meglio usando tecniche di N1

vedi N1.8

si ricava che $(p(n), p(n+1)) = 1$

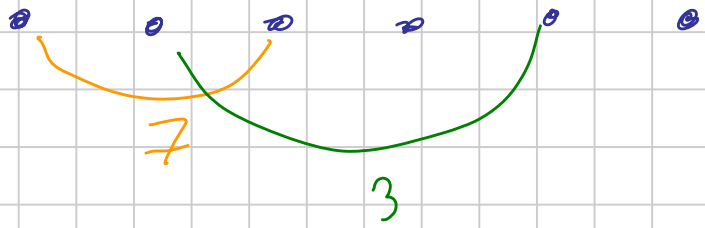
$(p(n), p(n+2)) \mid 7$

$(p(n), p(n+3)) \mid 3$

⋮

se $n \equiv 2 \ (7)$ allora ho il 7

se $n \equiv \_ \ (3)$



Per il th cinese: $\begin{cases} a+1 \equiv 2 \ (7) \\ a+2 \equiv \_ \ (3) \end{cases}$ □

Potenze mod n

Non è vero che $a \equiv b, \ c \equiv d \ (n) \Rightarrow a^c \equiv b^d \ (n)$

Però osserviamo che $a^0, a^1, a^2 \ldots$ è definit. periodica

Dim:

Oss1: $a^{n+1} \equiv f(a^n) \ (m)$

Oss2: per Pigeonhole devono esistere $n_1, n_2 \geq 0$ t.c. $a^{n_1} \equiv a^{n_2} \ (m)$

Quindi: Oss 1 + Oss 2 $\Rightarrow$ la succ. è periodica

Oss: qualche volta il periodo inizia subito.

Se $(a, m) = 1$ allora $a^{n_1} \equiv a^{n_2}$

ottengo $a^{n_1 - 1} \equiv a^{n_2 - 1}$

$\dots \quad a^0 \equiv 1 \equiv a^{n_2 - n_1}$

Quando $m = p$ un primo succede sempre se $a \not\equiv 0$

Oss: ora so solamente che $\exists\ n_1, n_2 \leq m+1$

e dipendono in modo misterioso da a

La ϕ di Eulero

La ϕ è una funzione $: \mathbb{Z}_{>0} \to \mathbb{N}$

$$\phi(n) = \left| \{ 0 < m \leq n : (m, n) = 1 \} \right|$$

Es: $n = 5$ $\quad 1, 2, 3, 4, \cancel{5}$ quali sono primi con 5? (tutti)

$\Rightarrow \phi(5) = 4$

$n = 10$ $\quad 1, 2, 3, 4, 5, 6, 7, 8, 9, \cancel{10}$ $\quad$ 10

$\phi(10) = 4$

Oss: se $n = p$ un primo, $\phi(p) = p-1$

$n = p^2$, $\phi(p^2) = (p-1)\frac{p^2}{p} = p^2 - p^{2-1}$

Oss: Quanto vale $\sum_{d \mid n} \phi(d) = ?$ n

Es: $n = 10$

$d = 1, 2, 5, 10$ $\quad \sum \phi(d) = 10$

$\phi(d) = 1, 1, 4, 4$

$n = p$ $\quad \sum \phi(d) = \phi(1) + \phi(p) = 1 + p - 1 = p$

Dim: $n = 10$ $\quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

- primi con 10
- $(d, n) = 2$
- $(d, n) = 5$
- $(d, n) = 10$

x casa: scrivetela per bene.

Fatto: la funzione ϕ è moltiplicativa

$$\phi(ab) = \phi(a)\phi(b) \quad \text{se } (a, b) = 1$$

Dim: induzione estesa

Es $n = 10 = 2 \cdot 5$

$10 = \phi(10) + \phi(5) + \phi(2) + \phi(1)$

$\begin{cases} 5 = \phi(5) + \phi(1) \\ 2 = \phi(2) + \phi(1) \end{cases}$

$10 = \phi(5)\phi(2) + \phi(5)\phi(1) + \phi(2)\phi(1) + \phi(1)\phi(1)$

$+ \phi(5\cdot 1) + \phi(2\cdot 1) + \phi(1\cdot 1)$

il confronto di ↗ ↗ conclude

Ora so calcolare la ϕ ovunque

Es: $\phi(12) = \phi(4)\phi(3) = 2\cdot 2 = 4$.

Th (Eulero-Fermat):

sia $(a, m) = 1$ mi stavo chiedendo quali potessero essere i periodi della succ. $a^0, a^1, \dots$

$$a^{\phi(m)} \equiv 1 \quad (m)$$

Dim: Idea: → $n_1, n_2, \dots, n_{\phi(m)}$ sono le classi di resto coprime

→ $an_1, an_2, \dots, an_{\phi(m)}$

Oss: → ho ancora classi prime con m

Oss: → le classi scritte sono tutte distinte:

$$2n_i \equiv 2n_j$$

$$\Rightarrow n_i \equiv n_j \quad (\text{molt. per } 2^{-1}, \text{che esiste...})$$

Idea: moltiplico → e →

$$n_1 \cdot \ldots \cdot n_{\phi(m)} \equiv 2^{\phi(m)} \cdot n_1 \cdot \ldots \cdot n_{\phi(m)} \quad (m)$$

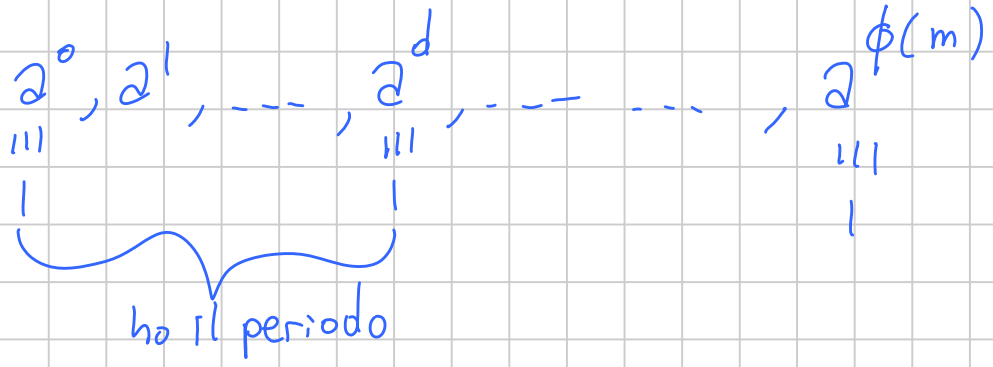
da cui ... $\quad 1 \equiv 2^{\phi(m)}$ □

Th (Piccolo Teorema Fermat)

se $m = p$ $\quad 1 \equiv 2^{p-1}$ $\quad$ se $p \nmid 2$

$2 \equiv 2^{p}$ $\quad \forall\, 2$

Oss fondamentale: i periodi delle potenze di 2 dividono $\phi(m)$



Def: l'intero d che sia il + piccolo >0 t.c.

$2^d \equiv 1 \ (m)$ si chiama $\text{ord}_m(2)$

Oss di prima: $\text{ord}_m(2) \mid \phi(m)$

Es: N2.10

$$D = \{ n : n \mid 2^n + 1 \}$$

Sol: sia $n \in D$

$\rightarrow 2^n \equiv -1 \quad (n)$

$2^{2n} \equiv 1 \quad (n)$

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

$\mid \phi(n)$

$\rightarrow \text{ord}_n(2) \nmid n$

sia p un primo che $\mid n$ allora

$2^n \equiv -1 \quad (n) \Rightarrow 2^n \equiv -1 \quad (p)$

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

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

se prendevo p il + piccolo primo $\mid n$

allora $(p-1, n) = 1$

chi sarà $(p-1, 2n) \mid 2$

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

$\Rightarrow \quad 2^2 \equiv 1 \quad (p) \qquad$ (def. di $\mathrm{ord}_p(2)$)

$p = 3$

Domanda: se è vero che $2^{p-1} \equiv 1 \quad (p)$ esistono interi 2 di ordine esattamente $p-1$? SÌ (non ovvissimo)

$\Leftrightarrow \quad 2^{\phi(n)} \equiv 1 \quad (n)$

$\Leftrightarrow \quad \mathrm{ord}_n(2) = \phi(n)$?

Non sempre...

La risposta alla 1ª domanda porta a

Def: se $\mathrm{ord}_p(2) = p-1$ 2 è "generatore" mod p

cioè $\{2^0, 2^1, \dots, 2^{p-2}\} = \{1, 2, \dots, p-1\}$

Domanda: $\mathbb{Z}/p \to \mathbb{Z}/p$ ($\mathbb{Z}/p$ sono le classi di resto mod p)

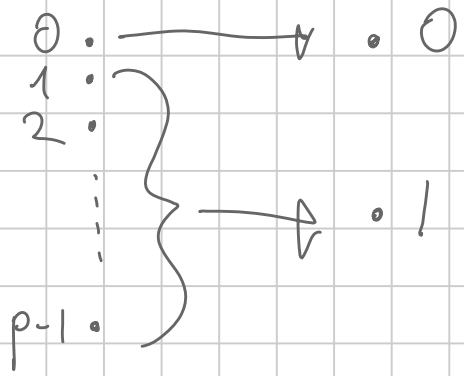
$n \longmapsto n^2$

$n \longmapsto n^3$

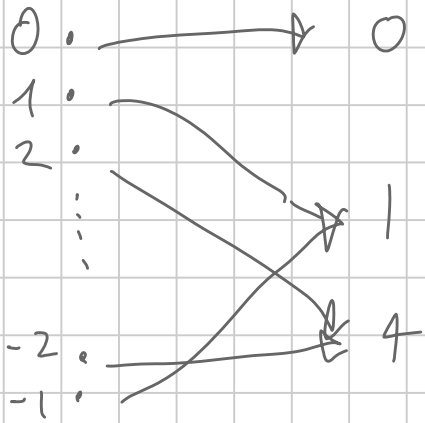
$n \longmapsto n^2$

Quand'è che queste funzioni sono iniettive/surgettive?

Nel caso $a = p-1$ ottengo sempre 1 (oppure 0)



nel caso $a = 2$



Stesso discorso per tutti i $d \mid p-1$

Se invece $(a, p-1) = 1$ allora la mappa è iniet.

mi chiedo l'iniettività $r_1^a \overset{?}{\equiv} r_2^a \pmod p$

$r_1^{a+(p-1)} \equiv r_2^{a+(p-1)} \pmod p$

assunto $r_1, r_2 \neq 0$ $\quad (r_1 \cdot r_2^{-1})^a \equiv 1 \pmod p$

$x^a \equiv 1 \pmod p$

però $(a, p-1) = 1$ esiste $b = a^{-1} \bmod p-1$

$\exists b$ t.c. $ab \equiv 1 \pmod{p-1}$

$$1 \equiv (x^a)^b \equiv x^{ab} \equiv x^{1+h(p-1)} \equiv x^1$$

$$\Rightarrow \quad 1 \equiv x \quad \Rightarrow \quad r_1 \equiv r_2$$

Ancora disuguaglianze!

Fatto ovvio: $n \mid m \Rightarrow \begin{cases} m = 0 \\ |n| \leq |m| \end{cases}$

Es: BMO 2017.3

Trovare tutte le funzioni $f: \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ t.c.

$$n + f(m) \mid f(n) + n f(m) \qquad \forall\, n, m > 0$$

Sol: Oss: $n \mid m \Rightarrow n \mid m - n$

$$n + f(m) \mid \left[f(n) + n f(m) \right] - (n + f(m))\, n$$

$$\mid f(n) - n^2$$

no m

Ora fisso $n = n_0$ e vedo che succede

$$n_0 + f(m) \mid f(n_0) - n_0^2$$

uso la dis: $\Rightarrow f(n_0) - n_0^2 = 0$

$$n_0 + f(m) \leq |f(n_0) - n_0^2|$$

$$\Downarrow$$

$$f(m) \leq C \qquad \forall\, m$$

Ora sappiamo che $f(m)$ è limitata ←

oppure $f(n) = n^2$ sempre

Caso ←

Oss: per pigeonhole, $\exists\, a \in \mathbb{Z}_{>0}$ t.c.

per ∞ valori di m $f(m) = a$

Prendo al posto di n questi valori:

$$n + f(m_0) \mid a + n f(m_0)$$

$$n + f(m_0) \mid \left(a + n f(m_0)\right) - \left(n + f(m_0)\right) f(m_0)$$

$$\mid a - f(m_0)^2$$

$$a = f(m_0)^2$$

$$n + f(m_0) \leq |a - f(m_0)^2|$$

$$\Downarrow$$

$$n \leq C$$

Caso assurdo

Quindi: $2 = f(m)^2$ per ogni m.

Esercizi

P. 12 61, 66

P. 43 4, 9, 10 (c), 10 (b)

P. 42 10

Bonus 3

Dimostrare che NON esistono generatori mod $p \cdot q$ con $p, q > 2$ primi distinti.

Bonus 1 (TF 2016)

Quanto vale $\sum_{k=0}^{1000} k^{2016} \mod 11$?

Bonus 2

Trovare tutte le $f: \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ t.c.

i) $f(n!) = f(n)!$ $\forall n$

ii) $m - n \mid f(m) - f(n)$ $\forall m, n$

Correzione

Es 61 $5^n + 3^n + 1 = \text{primo} \Rightarrow 12 \mid n$

Oss: mod m 5^n e 3^n (e 1) sono periodiche

mod qualcosa, sicuramente mod $\phi(m)$

Cerco m t.c. $4 \mid \phi(m)$ e $3 \mid \phi(m)$ (anche m diversi)

Però, sicuramente scelgo m una potenza di primo

(Per il th Cinese)

[sol: $m = 5, 7$]

66: $Y \equiv 13^0 + \dots + 13^{666} \pmod{19}$ Quanto è Y?

$\|$

$1 + x + \dots + x^{666}$

voglio moltiplicare per $x-1$ e dividere

$Y(x-1) \equiv x^{667} - 1$

... con in mente il seguente passaggio finale:

$YA \equiv B \Rightarrow Y \equiv B \cdot A^{-1}$

per calcolare B, $x^{667} \equiv x^{(667 \bmod \phi(19))} \equiv x^{\dots}$

Es 4: quali sono le ultime 5 cifre di: $5^{5^{5^5}}$?

Tesi $\Leftrightarrow$ Calcolare $X \equiv 5^{5^{5^5}} \pmod{10^5}$

Oss: th Cinese faccio (5^5) e (2^5)

Oss: le potenze di 5 sono periodiche

antiperiodo, poi costante 0

periodo $| \phi(2^5)$

2^4

Oss + fine: i periodi mod 2^n sono più piccoli di 2^{n-1}, sono infatti al massimo 2^{n-2} (vedi Medium)

Es 9: dim. che $\forall n, d, m \quad \exists a$

$a, a+d, a+2d, \dots, a+(m-1)d$

$p_1^n \mid a$; $p_2^n \mid a+d$ — —

$$\Leftarrow \begin{cases} a \equiv 0 & (p_1^n) \\ a \equiv -d & (p_2^n) \\ \vdots \\ a \equiv -(m-1)d & (p_m^n) \end{cases}$$

e la soluzione esiste per th Cinese, perché

$p_1^n, p_2^n, \dots, p_m^n$

sono a 2 a 2 coprimi

Es N1.10 trovare tutte le soluzioni di $y^2 = x^5 - 4$

Oss: le disuguaglianze NON aiutano (banalmente)

Oss: non ci sono soluzioni piccole

⇓

spero che non ci siano soluzioni

$\Rightarrow$ cerco un assurdo mod m opportuno

Oss: se provo un m t.c. $2 \mapsto 2^2$, $2 \mapsto 2^5$ non sono surgettive ho speranze

$\Rightarrow$ devo cercare m t.c. $2 \mid \phi(m)$, $5 \mid \phi(m)$

es: $m = 11$

Bonus 1: $X = \sum_{k=0}^{1000} k^{2016} \mod 11$

Oss: $X \equiv \frac{1001}{11} y$

dove $y = \sum_{k=0}^{10} k^{2016}$

Oss: $\phi(11) = 10$ $\quad k^{2016} \equiv k^6$ (se $11 \nmid k$)

rimane $1^6 + 2^6 + \dots + 10^6 \mod 11$

sia g un generatore mod 11, allora

$1^6 + \dots + 10^6 \equiv (g^0)^6 + (g^1)^6 + \dots + (g^{p-2})^6$

ora finisco moltiplicando per

$1 - (g^0)^6 \not\equiv 0$ perché $g^6 \not\equiv 0$

perché $\text{ord}_{11}(g) = 10$

... fa $\underline{0}$ $\quad 1 - (g^{p-1})^6 \equiv 0$

Bonus 2 (BMO 2012.4)

$f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$:

- $f(n!) = f(n)!$
- $n - m \mid f(n) - f(m)$

Oss: ... $f(1) = 1 \vee 2$
$f(2) = 1 \vee 2$

ci sono 4 casi:

faccio il + difficile: $f(1) = 1$, $f(2) = 2$

... si riesce a dire che $f(3) = 3$ ...

quindi: $f(3!) = f(3)! = 3!$

$\Rightarrow$ $f((3!)!) = (3!)!$

quindi: $\exists \infty$ m t.c. $f(m) = m$

$n - m \mid f(n) - f(m)$

fisso $n = n_0$, pongo m tra questi ∞ interi:

$$n_0 - m \mid f(n_0) - m$$

$$\mid f(n_0) - m - n_0 + m$$

$$\Rightarrow \begin{cases} f(n_0) = n_0 \\ |n_0 - m| \leq |f(n_0) - n_0| \end{cases}$$

$\Rightarrow m \leq C$ per $m > n_0$

assurdo perché m può essere arbitr. grande

$\Rightarrow$ ho solo $f(n) = n$.