

Congruenze e struttura moltiplicativa

Def

$$x \equiv y \pmod{m} \quad \text{quando} \quad m \mid x - y$$

Def

$$a \mid b \quad \text{quando} \quad \exists c \in \mathbb{Z} \text{ t.c. } b = ac$$

Proprietà utili:

$$x \equiv y \text{ e } z \equiv w \pmod{m} \Rightarrow \begin{aligned} x+z &\equiv y+w \pmod{m} \\ xz &\equiv yw \end{aligned}$$

Thm (cinese del resto):

$$* \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

$$\text{e } (m_i, m_j) = 1 \quad \forall i \neq j$$

(coprimi)

Allora $\exists!$ x t.c. x soddisfa tutte le congruenze del sistema $*$ modulo $m_1 \cdot m_2 \cdot \dots \cdot m_n$

Es. numerico

$$m_1 = 2 \quad m_2 = 5$$

$$m_1 \cdot m_2 = 10$$

$$(0, 0)$$

$$(1, 1)$$

$$(0, 2)$$

$$(1, 3)$$

$$(0, 4)$$

$$(1, 0)$$

$$(0, 1)$$

$$(1, 2)$$

$$(0, 3)$$

$$(1, 4)$$



0
1
2
3
4
5
6
7
8
9

Dim: per induzione sul numero di equazioni n

Basta dimostrare il caso $n=2$

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

Supponiamo che la funzione

$$\begin{aligned} \{ \text{classi mod } m_1 m_2 \} &\rightarrow \{ \text{classi mod } m_1 \} \times \{ \text{classi mod } m_2 \} \\ x &\mapsto (x_{(mod m_1)}, x_{(mod m_2)}) \end{aligned}$$

Se non fosse iniettiva, allora esistono $x \neq y \quad (m_1 \cdot m_2)$

$$\begin{aligned} \text{t.c.} \quad x &\equiv y & (m_1) \\ x &\equiv y & (m_2) \end{aligned}$$

$$x - y =: d$$

$$d \equiv 0 \quad (m_1) \quad m_1 \mid d \quad \text{sapendo che } (m_1, m_2) = 1$$

$$d \equiv 0 \quad (m_2)$$

$$m_2 \mid d$$

$$k_2 m_2 = d = k_1 m_1$$

$$d \neq 0 \quad (m_1 m_2)$$

$$m_2 \mid k_1 \Rightarrow k_1 = k_3 m_2$$

$$d = k_3 m_2 m_1$$

□

Come si comportano le potenze mod m ?

$$a^0, a^1, \dots, a^k, \dots \quad \text{mod } m$$


Thm (Eulero - Fermat):

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

$$\text{Def: } \varphi(n) := |\{x: 1 \leq x \leq n \text{ e } (x, n) = 1\}|$$

(è una funzione da $\mathbb{N}$ a $\mathbb{N}$)

$$\text{Es: se } p \text{ è primo, } \varphi(p) = p - 1$$

$$\text{Dim: } C := \{ x: 1 \leq x \leq m, (x, m) = 1 \}$$

$$f: C \rightarrow \{ \text{classi d. resto mod } m \}$$

$$f(x) = 2 \cdot x$$

$$\text{I) } f(C) \subseteq C$$

$$\text{II) } f(C) = C$$

$$\underbrace{\prod_{x \in C} x}_y = \prod_{x \in C} (2 \cdot x) = 2^{|C|} \prod_{x \in C} x$$

$$y \equiv 2^{|C|} y \pmod{m},$$

$$(y, m) = 1 \Rightarrow \exists z \text{ t.c. } zy \equiv 1 \pmod{m}$$

$$\Rightarrow zy \equiv 2^{|C|} zy$$

$$1 \equiv 2^{|C|} \pmod{m}, \text{ ma } |C| = \varphi(m).$$

$$f \text{ è iniettiva poiché da } 2x \equiv 2y \pmod{m}$$

$$\text{ottengo } 2ax \equiv 2ay \pmod{m} \Rightarrow x \equiv y \pmod{m}$$

(basta prendere l'inverso moltiplicativo di 2 mod m, cioè quella classe b t.c. $2b \equiv 1 \pmod{m}$)

IMO 2005, 4

Determinare tutti gli interi positivi relativamente primi

a tutti i termini della successione

$$a_n = 2^n + 3^n + 6^n - 1 \quad \forall n \geq 1$$

$$\text{Sol: } x \text{ t.c. } (x, a_n) = 1 \quad \forall n$$

Cerchiamo intanto i primi che possono funzionare

$$p \text{ primo t.c. } (p, a_n) = 1 \quad \forall n$$

cerchiamo intanto $p \neq 2, 3$

$$a_{p-1} \equiv 1 + 1 + 1 - 1 \equiv 2 \pmod{p}$$

$$a_p \equiv 10$$

$$a_{p-2} \equiv 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$$

$$2 \cdot \underbrace{2^{p-2}}_{= 1/2} = 2^{p-1} = 1$$

$$= 1/2 + 1/3 + 1/6 - 1 = 2_{p-2} \quad (p)$$

$$6 \cdot 2_{p-2} = 3 + 2 + 1 - 5 = 0$$

$$p \mid 6 \cdot 2_{p-2} \Rightarrow p \mid 2_{p-2}$$

$\Rightarrow$ se x funziona, gli unici fattori primi che può avere sono 2 e 3

(si conclude guardando bene 2 e 3).

Def: $\text{ord}_m(2)$ è l'ordine moltiplicativo di 2 modulo m
(è definito per ogni $2, m$ interi positivi primi fra loro)
è il più piccolo intero $x > 0$ t.c. $2^x \equiv 1 \pmod{m}$

Oss: ogni y t.c. $2^y \equiv 1 \pmod{m}$ è mult. pl. dell' $\text{ord}_m(2)$

infatti $y = q \cdot \theta + r$ (la divisione con resto)

$$1 \equiv 2^y = 2^{q \cdot \theta + r} = (2^\theta)^q \cdot 2^r = 1^q \cdot 2^r = 2^r$$

dato che $0 \leq r < \theta$ e θ era il più piccolo positivo, allora $r = 0$

$$\text{ord}_m(2) \mid \varphi(m)$$

Modulo un primo p , le cose si comportano bene.

$$p \mid ab \Rightarrow p \mid a \vee p \mid b$$

con le congruenze ho

$$ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \vee b \equiv 0 \pmod{p}$$

Conseguenza: un polinomio di grado $\leq d$ ha al più d radici mod p

$$q(x) = (x - r_1) t(x)$$

se x_0 è una radice di $q(x)$

$$0 \equiv q(x_0) \equiv (x_0 - r_1) t(x_0) \pmod{p}$$

$$P(x) = x^{p-1} - 1$$

$P(x)$ ha come radici: $\{1, \dots, p-1\}$

$$x^{p-1} - 1 = (x-1)(x-2) \dots (x-(p-1))$$

(conseguenza: teorema di Wilson)

Esistono sempre classi di ordine massimo ($= p-1$)

Dim: le classi di ordine k soddisfano

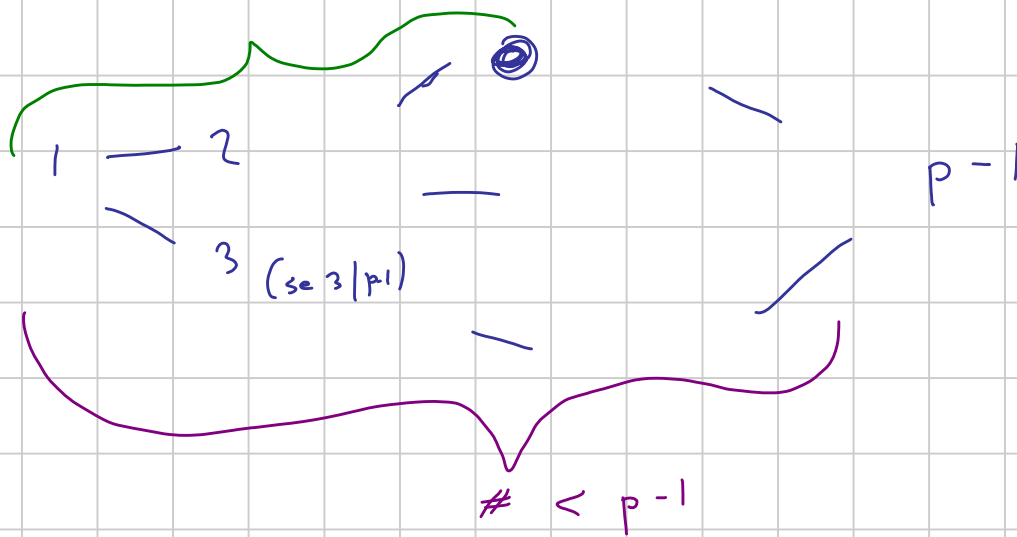
$$x^k \equiv 1 \pmod{p}$$

$$\text{e } x^h \not\equiv 1 \pmod{p} \quad \forall h < k$$

$$x^h - 1 \mid x^k - 1 \quad (h \mid k)$$

contiamo le classi mod p un ordine alla volta

$$\begin{array}{ccc} \text{ord} = & 1 & 2 & & d \mid p-1 & & p-1 \\ & \{1\} & \{-1\} & & & & \end{array}$$



Esercizio: $n = \phi(1) + \dots + \phi(d) + \dots + \phi(n)$
 dove la somma varia per ogni $d | n$

ES: se m non è primo (e non potenza di primo)
mi aspetto che l'ordine massimo sia molto più basso di $\varphi(m)$

$$2^x \equiv 1 \pmod{m} \quad (m = m_1 \cdot m_2) \\ (m_1, m_2) = 1$$

$$2^x \equiv 1 \pmod{m_1}$$

$$2^x \equiv 1 \pmod{m_2}$$

mi basta avere che $\text{ord}_{m_1}(2) \mid x$
 $\text{ord}_{m_2}(2) \mid x$

$$\text{lcm}(\text{ord}_{m_1}, \text{ord}_{m_2}) \mid x$$

basta $\text{lcm}(\varphi(m_1), \varphi(m_2)) \mid x$

$$< \varphi(m)$$

Oss: $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$ (se $(m_1, m_2) = 1$)

Oss: $\varphi(n)$ è pari $\forall n \geq 2$

(es. se $(x, n) = 1$ anche $(n-x, n) = 1$)
 $x, n-x$ sono diversi se n non è pari.

Numeri di Carmichael

sono interi n t.c. $2^{n-1} \equiv 1 \pmod{n} \quad \forall (2, n) = 1$
e n non è primo

Es: dimostrare che 561 è un numero di Carmichael

Es: trovare il successivo numero di Carmichael

$$N2.10 \quad \{n : n \mid 2^n + 1\} =: D$$

$$2^n + 1 \equiv 0 \quad (n)$$

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

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

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

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

prendiamo $p \mid n$

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

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

$$\mid \varphi(p) = p-1$$

sia p il più piccolo primo che divide n

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

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

$$2^2 \equiv 1 \quad (p) \Rightarrow p = 3$$

troviamo tutte le potenze di primi in D

è vero che $3^x \in D$?

$$9 \in D? \quad 9 \mid 2^9 + 1?$$

$$n = 3^k \quad ? \quad 2^n + 1 = 2^{3^{n'}} + 1 = (2^{n'} + 1)(y^2 - y + 1)$$

$$n' = 3^{k-1}$$

$$\text{per ipotesi induttiva} \quad 3^{k-1} \mid 2^{n'} + 1$$

$$\text{se avessi:} \quad 3 \mid y^2 - y + 1$$

ottenere: ipotesi del passo induttivo

$$\text{è vero se } y \equiv 2 \quad (3)$$

$$y = 2^{n'}$$

quindi: $y \neq 0 \quad (3)$

$y \equiv 1 \quad (3) \Leftrightarrow n'$ fosse pari.

BMO 2018.4 Trovare tutte le coppie di primi (p, q) t.c.

$$3p^{q-1} + 1 \mid 11^p + 17^p$$

Accenni: della soluzione:

se un primo $l \mid 11^p + 17^p$

$$11^p + 17^p \equiv 0 \quad (l)$$

$$11^p \equiv -17^p \quad (l) \quad (\text{se } (l, 17) = 1)$$

$$(11/17)^p \equiv -1 \quad (l)$$

$$(11/17)^{2p} \equiv 1 \quad (l)$$

$\text{ord}_l(11/17) \mid 2p$
 $\neq p \quad (\text{se } l \neq 2)$

caso 1: $\text{ord} = 2 \quad (11/17)^2 \equiv 1 \quad (l) \quad (11/17) \neq 1$

$$11^2 \equiv 17^2$$

$$11^2 - 17^2 \equiv 0$$

$$11 \not\equiv 17$$

$$11 - 17 \not\equiv 0$$

$$11 + 17 \equiv 0 \quad (l) \Rightarrow l = 7$$

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

Ora studiamo meglio la fattorizzazione di: $3p^{q-1} + 1 = 2^\alpha \cdot 7^\beta \cdot \prod p_i^{e_i}$

$$p_i \equiv 1 \quad (2p)$$

Esercizi:

TCR N2.9

TCR + str. molt. 60, 61, 63, 66, N2.1, N2.4, N2.6

str. molt. N1.10, N2.7, N2.10 (e)

Concludere Bmo 2018.4

IMO 2005.4

IMO 2000.5 : Esiste un intero positivo n con esattamente 2000 fattori primi distinti t.c. $n \mid 2^n + 1$

Trovare tutte le soluzioni intere non negative di: (a, b, c, d) t.c.
 $2^a + 3^b + 5^c = 7^d$

Oss: mod 8 chi sono i quadrati?

pari $\rightarrow 0, 4$

dispari $\rightarrow 1$
 $1, 3, 5, 7$

$$2^n \pmod{8} \quad (2, 8) = 1$$
$$\text{ord}_8(2) \mid 2 \quad (2, 2) = 1$$

$$x^2 - 1 \equiv 0 \pmod{8}$$
$$(x-1)(x+1)$$

$$\left(\text{Euler-Fermat } x^4 \equiv 1 \pmod{8} \right)$$

trovare $S^{5^{5^{\dots}}} \pmod{2^5}$, $S^{5^{5^{\dots}}} \equiv S^5 \pmod{32}$

$$S^n \equiv S^{n-2^3} \pmod{2^5}$$
$$S^{5^5} \equiv 1 \pmod{8}$$

mod 7

x^0	x^1	x^2	x^3	x^4	x^5	x^6
1	0	0	0	0	0	0
1	1	1	1	1	1	1
1	2	4	1	2	4	1
1	3	2	6	4	5	1
1	4	2	1	4	2	1
1	5	4	6	2	3	1
1	6	1	6	1	6	1

$$x^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow x \text{ è residuo quadratico } (p)$$

Quando $f(x) = x^k$ è iniettiva/suriettiva/biiettiva (mod p)

$$x^k \equiv y^k \pmod{p} \Rightarrow x \equiv y \pmod{p} \text{ per quali } k?$$

$$\text{se } (k, p-1) = 1 \quad \exists h \text{ t.c. } kh \equiv 1 \pmod{p-1}$$

$$x^k \equiv y^k \Rightarrow (x^k)^h \equiv (y^k)^h \Rightarrow x^{kh} \equiv y^{kh} \Rightarrow x^1 \equiv y^1$$

Per dimostrare gli altri claim, torna utile usare una classe $g \pmod{p}$ che abbia ordine $= p-1$

$$\{ \underbrace{g^0, g^1, \dots, g^{p-2}}_{\# = p-1} \} = \{ 1, \dots, p-1 \}$$

g lo chiamo generatore mod p

Esempio: Come si comporta $x \mapsto x^3$

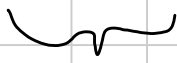
Prendo un generatore g

$$3 \nmid p-1 \quad (\text{visto})$$

$$\begin{array}{c|c} g^0, g^1, & \dots, g^{p-2} \\ g^0, g^1, & \dots, g^{3(p-2)} \end{array}$$

$$3 \mid p-1$$

$$g^{\frac{p-1}{3}}$$



61 : supponiamo che $5^n + 3^n + 1$ s.2 primo
dimostrare che $12 \mid n$

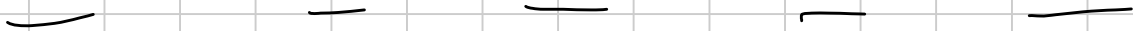
se voglio cose periodiche di periodo mol di 4

m: conviene cercare primi o potenze di primi t.c.

$$4 \mid \varphi(m) \quad 5, 8, 13$$

$$16$$

$$3 \mid \varphi(m) \quad 7, 9, 13$$



Come si comportano le potenze di $x \bmod p^h$?

$(x, p) = 1 \rightarrow$ periodico per Eulero-Fermat

$p \mid x$ c'è un anti-periodo finché x^n ha almeno h fattori p
e poi è 0 costante

Trovare tutte le soluzioni di: $2^a + 3^b + 5^c = 7^d$

Sol: mod 4 : se $2 \nmid d$ $(-1)^b + 1 \equiv (-1)^d$, no soluzioni

$$2 \equiv 1$$

$$2 + (-1)^b + 1 \equiv (-1)^d \text{ no soluzioni}$$

$$\Rightarrow 2 \equiv 0$$

$$1 + 3^b + 5^c = 7^d$$

$$\text{mod } 3, \text{ se } b \geq 1 \quad 1 + 2^c \equiv 1 \pmod{3}, \text{ no soluzioni}$$

$$\Rightarrow b = 0$$

$$2 + 5^c = 7^d$$

ora osserviamo che $c=1 \Rightarrow d$ porta una soluzione

$$\text{mod } 25, \text{ se } c \geq 2$$

$$2 \equiv 7^d \pmod{25}$$

$$2 \equiv (2+5)^d \pmod{25} \Rightarrow 2 \equiv (2+5)^d \pmod{5}$$

$$2 \equiv 2^d$$

$$\Rightarrow d \equiv 1 \pmod{4}$$

$$\begin{array}{l} \text{pot } 2 \\ 2^0 \equiv 1 \\ 2^1 \equiv 2 \\ 2^2 \equiv 4 \\ 2^3 \equiv 3 \end{array}$$

$$2 \equiv (2+5)^{1+d'}$$

$$2 \equiv (2+5)^{1+d'} \pmod{25}$$

$$(2+5)^{d'} \equiv 1 \pmod{25}$$

$$2 \equiv 2+5 \pmod{25} \text{ assurdo, no soluzioni}$$