Ancora congruenze

Note Title 10/30/2017

- Determinare, al variare di $k \in \mathbb{N}$, le soluzioni di

$$\begin{cases} x^k \equiv x \mod 7 \\ x^3 \not\equiv x \mod 7 \end{cases}$$

① $x \not\equiv 0 \mod 7$

$$\begin{cases} x \not\equiv 0 \\ x^{k-1} \equiv 1 \mod 7 \\ x^2 \not\equiv 1 \mod 7 \end{cases}$$

② $x^2 \not\equiv 1 \iff x \not\equiv 1,\ x \not\equiv -1 \mod 7$

③ $\text{ord}_7(x) \mid \varphi(7) = 6$ piccolo di Fermat

$\text{ord}_7(x) \nmid 2$

$\text{ord}_7(x) \mid k-1$

$\Rightarrow \text{ord}_7(x) \in \{3, 6\} \Rightarrow 3 \mid k-1$

Condizione necessaria per l'esistenza di soluzioni: $3 \mid k-1$

④ Due casi: $6 \mid k-1$ e $3 \mid k-1$ ma $2 \nmid k-1$

⑤ $k \equiv 1 \ (6)$ ⑥ $k \equiv 4 \ (6)$

Caso (a): $\begin{cases} x^{6h} \equiv 1 \mod 7 \\ x \not\equiv 0 \ (7) \\ x^2 \not\equiv 1 \mod 7 \end{cases}$ $(k = 6h+1)$

Soluzioni: $x \equiv \pm 2, \pm 3 \mod 7$

Caso (b): $\begin{cases} x^{6h+4-1} \equiv 1 \mod 7 \\ x^2 \not\equiv 1 \mod 7 \end{cases}$ $(k = 6h+4)$

$\begin{cases} x^3 \equiv 1 \ (7) \\ x^2 \not\equiv 1 \ (7) \end{cases}$

Classi di resto: ~~0~~ ~~1~~ 2 ~~3~~ 4 ~~5~~ ~~6~~

OK OK

Potenze di 3: 1 3 2 -1 -3 -2 1 ...

5: 1 -2 -3 -1 2 3 1 ...

$\text{ord}_7(3) = \text{ord}_7(5)$ perché sono inversi

Soluzioni: $\begin{cases} \text{nessuna, se } 3 \nmid k-1 \\ x \equiv \pm 2, \pm 3 \text{ se } 6 \mid k-1 \\ x \equiv 2, 4 \text{ se } k \equiv 4 \ (6) \end{cases}$

- $$\begin{cases} aX \equiv 4 \mod 25 \\ X^2 + a \equiv 0 \mod 15 \end{cases}$$

(i) Determinare per quali a c'è soluzione

(ii) Trovare soluz. per $a = -1$

$$\begin{cases} aX \equiv 4 \mod 25 \\ X^2 + a \equiv 0 \mod 3 \\ X^2 + a \equiv 0 \mod 5 \end{cases}$$

compatibili?

a è invertibile modulo 5 (dalla 1ª eqz.)
modulo 25

$a \equiv \underbrace{-X^2}_{\text{quali valori può assumere (mod 5)?}} \mod 5$

$X \equiv \cancel{0}, 1, 2, 3, 4 \qquad -X^2 \equiv -1, 1, 1, -1$

Quindi $a \equiv \pm 1 \mod 5$

Se $a \equiv 1 \mod 5$, dalla 1ª eqz. trovo

$$aX \equiv 4 \ (5) \iff X \equiv -1 \ (5)$$

che è incompatibile con $\underbrace{X^2}_{(-1)^2} + \underbrace{a}_{1} \equiv 0 \ (5)$

Resta l'unica possibilità $a \equiv -1 \ (5)$

Funzionerà?

$$\begin{cases} aX \equiv 4 \ (25) \\ a \equiv -1 \ (5) \\ a + X^2 \equiv 0 \ (5) \end{cases}$$

$$\begin{cases} aX \equiv 4 \ (25) \\ a \equiv -1 \ (5) \\ X^2 \equiv 1 \ (5) \end{cases}$$

$$\begin{cases} -X \equiv 4 \ (5) \iff X \equiv 1 \ (5) \\ a \equiv -1 \ (5) \\ 1^2 \equiv 1 \ (5) \\ aX \equiv 4 \ (25) \end{cases}$$

OK!

Manca la condizione modulo 3!

$X^2 + a \equiv 0 \ (3)$

$a \equiv 0 \ (3) \to X \equiv 0 \ (3)$

c'è soluzione

$a \equiv 1 \ (3) \quad X^2 \equiv 2 \ (3)$

no soluzione

$a \equiv 2 \ (3) \quad X^2 \equiv 1 \ (3)$

c'è soluzione

Soluzioni esistono $\overset{TCR}{\iff}$ $\begin{cases} a \equiv -1 \ (5) \\ a \equiv 0, 2 \ (\text{mod } 3) \end{cases}$

(ii) Caso $a = -1$: soluzioni ci sono (vedi ↑)

$$\begin{cases} -x \equiv 4 \quad (25) \\ x^2 - 1 \equiv 0 \quad (3) \end{cases} \qquad x^2 - 1 \equiv 0 \quad (5)$$

$$\begin{cases} x \equiv -4 \quad (25) \\ x^2 \equiv 1 \quad (3) \end{cases} \Longrightarrow \quad x^2 - 1 \equiv (-4)^2 - 1 \equiv 15 \equiv 0 \ (5)$$

$$\begin{cases} x \equiv -4 \quad (25) \\ x \equiv 1 \quad (3) \end{cases} \text{ o } x \equiv -1 \ (3)$$

$$\begin{cases} x \equiv -4 \ (25) \\ x \equiv 1 \quad (3) \end{cases} \quad \text{o} \quad \begin{cases} x \equiv -4 \ (25) \\ x \equiv -1 \quad (3) \end{cases}$$

$$\Uparrow \qquad\qquad\qquad\qquad \Uparrow$$

$$x \equiv 46 \quad (75) \qquad\qquad x \equiv -4 \ (75)$$

Quadrati modulo p

Sia $p > 2$.

Dim. che $x^2 \equiv y^2 \ (p) \iff x \equiv \pm y \pmod p$

Esempio $x^2 \equiv 1 \ (p) \iff x \equiv \pm 1 \bmod p$

Non è vero modulo m qualunque

$$x^2 \equiv y^2 \ (p) \iff p \mid x^2 - y^2 = (x-y)(x+y)$$

$$\overset{p \text{ primo}}{\iff} p \mid x-y \ \vee \ p \mid x+y$$

$$\iff x \equiv y \ (p) \ \vee \ x \equiv -y \ (p)$$

Def $a \in \mathbb{Z}/p\mathbb{Z}$ è un RESIDUO QUADRATICO se l'equazione $x^2 \equiv a \bmod p$ ha soluzione

Domanda Quanti sono i residui quadratici?

$$1 + \#\{\text{residui quadr. invertibili}\}$$

$$f : \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$

$$x \longmapsto x^2$$

$$\#\{\text{R.Q. inv.}\} = \#\,\mathrm{Im}(f)$$

Abbiamo visto che: se $a \in \mathrm{Im}\, f$, cioè

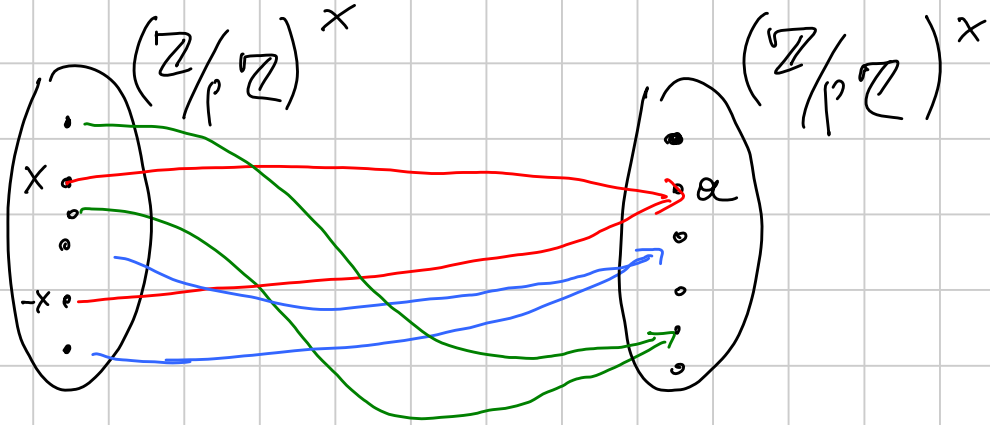
$$a \equiv x^2 \mod p$$

per qualche x $(a = f(x))$, allora

le soluzioni dell'eqz. $y^2 \equiv a \mod p$

sono x e $-x$

Ne segue che f è "2 - a - 1"



$$\#\text{ immagine di } f = \frac{1}{2}\#\left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \frac{1}{2}(p-1)$$

$$\#\text{ Residui Quadratici modulo } p = 1 + \frac{p-1}{2}$$

Esempio Sia x t.c. $x^2 \equiv 25 \mod (3\cdot 5\cdot 7\cdot 11)$.

Quante possibilità ci sono per $x \mod 3\cdot 5\cdot 7\cdot 11$?

$$\begin{cases} x^2 \equiv 25 & (3) \\ x^2 \equiv 25 & (5) \\ x^2 \equiv 25 & (7) \\ x^2 \equiv 25 & (11) \end{cases} \qquad \begin{cases} \boxed{x \equiv \pm 5 \ (3)} \\ x^2 \equiv 0 \ (5) \iff x \equiv 0 \ (5) \\ x \equiv \pm 5 \ (7) \\ x \equiv \pm 5 \ (11) \end{cases} \quad x \not\equiv 0 \ (3)$$

Otteniamo 8 sistemi, e.g. $\begin{cases} x \equiv -5 & (3) \\ x \equiv 0 & (5) \\ x \equiv 5 & (7) \\ x \equiv -5 & (11) \end{cases}$,

ognuno dei quali (TCR) ha un'unica soluzione modulo $3 \cdot 5 \cdot 7 \cdot 11$

In particolare, 25 ha 8 radici quadrate modulo $3 \cdot 5 \cdot 7 \cdot 11$

Cubi modulo $p \equiv 2 \ (3)$

Dim. che $x^3 \equiv y^3 \ (p) \iff x \equiv y \ (p)$

- Se $x^3 \equiv 0 \overset{x \equiv 0 (p)}{\Rightarrow}$ o $y^3 \equiv 0 \overset{y \equiv 0 (p)}{\Rightarrow} (p)$, allora p divide anche l'altro e quindi vale l'equivalenza
- Se $y \not\equiv 0 \ (p)$, posso moltiplicare la congruenza per $(y^{-1})^3$ e ottenere

$$(x/y)^3 \equiv 1 \bmod p$$

$$\begin{cases} \operatorname{ord}_p\left(\frac{x}{y}\right) \mid 3 & \text{(vedi eq 2)} \\ \operatorname{ord}_p\left(\frac{x}{y}\right) \mid p-1 & \text{(piccolo di Fermat)} \end{cases}$$

Dalla 1^a divisibilità troviamo $\operatorname{ord}_p\left(\frac{x}{y}\right) \in \{1, 3\}$.

Se $\operatorname{ord} = 3$, allora (dalla 2^a condizione)

troviamo $3 \mid p-1 \iff p \equiv 1 \ (3)$

ASSURDO perché per ipotesi $p \equiv 2 \ (3)$

Ne segue che $\operatorname{ord}_p(x/y) = 1 \Rightarrow x/y \equiv 1 \ (p)$

$$\Rightarrow x \equiv y \ (p).$$

Osservazione. L'ipotesi $p \equiv 2 \ (3)$ serve.

In effetti, per $p = 7$ si ha $1^3 \equiv 2^3 \equiv 4^3 \bmod 7$

Torniamo a $p \equiv 2 \ (3)$

$$f : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$
$$x \longmapsto x^3$$

f è iniettiva $\Rightarrow$ f surgettiva

Conclusione Per ogni $a \in \mathbb{Z}/p\mathbb{Z}$ l'equazione

$X^3 \equiv a \mod p$ ammette una soluzione, che è unica modulo p. $(p \equiv 2 (3))$

FATTO GENERALE Sia m un intero positivo, a un intero t.c. $(a, m) = 1$. Sia k un intero t.c. $(k, \varphi(m)) = 1$. Allora l'equazione $X^k \equiv a \mod m$ ha una soluzione, unica modulo m.

Oss Questo implica quello sopra prendendo m primo e $k = 3$

Esercizio Risolvere $X^7 \equiv 2 \mod 17$

Il criterio di prima ci dice che la soluzione è unica, perché $(7, \varphi(17)) = 1$

Come la trovo? Sappiamo che $\begin{cases} X^7 \equiv 2 \ (17) \\ X^{16} \equiv 1 \ (17) \end{cases}$

$1 = 7a + 16b = 7 \cdot 7 - 16 \cdot 3$

$$X \equiv X^1 \equiv X^{7\cdot 7 - 16\cdot 3} \equiv (X^7)^7 \cdot (X^{-3})^{16}$$

piccolo di Fermat

$$\equiv (X^7)^7 \equiv 2^7 \mod 17$$

$$\equiv 2^4 \cdot 2^3 \equiv (-1)\,8 \equiv 9 \quad (17)$$

Esempio Trovare le soluzioni di $X^5 \equiv 1 \quad (25)$.

Guardiamola modulo 5: $1 \equiv X^5 \equiv X \quad (5)$

↑ piccolo di Fermat

[Quindi $X \equiv 1, 6, 11, 16, 21 \mod 25$]

Scriviamo $X = 1 + 5K$. Allora

$$X^5 = 1^5 + \binom{5}{1} \cdot 1^4 \cdot 5K + \binom{5}{2} 1^3 (5k)^2$$

$$+ \binom{5}{3} 1^2 (5k)^3 + \binom{5}{4} (5k)^4 + (5k)^5$$

$$\equiv 1 \mod 25$$

Le soluzioni sono dunque $X \equiv 1 \quad (5)$

$$X \equiv 1, 6, 11, 16, 21 \quad (25)$$

Ordini moltiplicativi

Sia p un primo dispari.

Dim. che l'ordine di $1+p \mod p^n$ è p^{n-1}.

Cominciamo da $n=2$ ($n=1$ è banale).

$$(1+p)^k \equiv 1 \mod p^2$$

$$\| $$

$$1 + \binom{k}{1} \cdot p + \sum_{j=2}^{k} \binom{k}{j} p^j \equiv 1 + kp \quad (p^2)$$

Ora $1 + kp \equiv 1 \ (p^2) \iff kp \equiv 0 \ (p^2)$

$$\iff k \equiv 0 \ (p)$$

Quindi $\operatorname{ord}_{p^2}(1+p) = p$

Ora per induzione: $(1+p)^k \equiv 1 \ (p^3)$

$$\Downarrow$$

$$(1+p)^k \equiv 1 \ (p^2)$$

$$\Downarrow$$

$$p \mid k$$