WC 2009 TEORIA DEI NUMERI

Titolo nota 29/01/2009

1 $p \geq 5$ primo. Allora

$$p^5 \mid \left[\binom{p^2}{p} - p\right]$$

$$\binom{p^2}{p} - p = \frac{p^2 (p^2-1) \cdot \ldots \cdot (p^2-(p-1))}{p\,(p-1)!} - p$$

Da dim.: $\dfrac{(p^2-1)\cdot \ldots \cdot (p^2-(p-1))}{(p-1)!} - 1$ è div. per p^4

Basta dim. che $p^4 \mid$ Num.

$$(p^2-1) \cdot \ldots \cdot (p^2-(p-1)) - (p-1)!$$

$$(1-p^2)(2-p^2) \cdot \ldots \cdot ((p-1)-p^2) - (p-1)! \quad \text{div. per } p^4$$

$$(p-1)! - \text{coeff.}\, p^2 + \text{roba} \cdot p^4 - (p-1)!$$

Basta dim. che $p^2 \mid$ coeff.

$$\text{coeff.} = \pm \sum_{k=1}^{p-1} \frac{(p-1)!}{k} \quad \text{div. per } p^2$$

Brutal mode: coeff div. per $p^2 \iff \displaystyle\sum_{k=1}^{p-1} \frac{1}{k}$ div. per p^2

$$\sum_{k=1}^{p-1} \frac{1}{k} = \frac{m}{n}, \quad \text{allora} \quad p^2 \mid m$$

$$\{1, 2, \ldots, p-1\} = \left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{p-1}\right\}$$

Quindi $\displaystyle\sum_{k=1}^{p-1} \frac{1}{k} \underset{\text{mod } p}{=} \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2}$ multiplo di p perché $p > 2$.

Accoppio i termini: $1 + \frac{1}{p-1}$ $\qquad \frac{1}{k} + \frac{1}{p-k} = \frac{p}{(p-k)k}$

$\frac{1}{2} + \frac{1}{p-2}$

$\sum \frac{1}{k}$ è la somma di $\frac{p-1}{2}$ frazioni con p al num. $\Rightarrow$ div. per p

$$\sum_{k=1}^{p-1} \frac{1}{k} = \sum_{k=1}^{\frac{p-1}{2}} \frac{p}{(p-k)k} = p \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(p-k)k}$$

Al numeratore ci deve essere p

Brutal mode: $\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)} \underset{\text{mod } p}{=} -\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} = (\star)$

Quando k va da 1 a $\frac{p-1}{2}$, k^2 descrive tutti i residui quadratici mod p. Quindi anche $\frac{1}{k^2}$ descrive tutti i residui quadratici

$$(\star) = -\sum_{k=1}^{\frac{p-1}{2}} k^2 = -\frac{p-1}{2}\frac{p+1}{2} \cdot p \cdot \frac{1}{6}$$

Se $p \geq 5$ questa è divisibile per p,

— o — o —

$$\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{m}{[(p-1)!]^2}$$

Moltiplico per $[(p-1)!]^2$

$$[(p-1)!]^2 \sum_{k=1}^{p-1} \frac{1}{k^2} = m \qquad \sum_{k=1}^{p-1} \left[\frac{(p-1)!}{k}\right]^2$$

INTERI

$$\{1, 2, \dots, p-1\} = \left\{\frac{(p-1)!}{1}, \frac{(p-1)!}{2}, \dots, \frac{(p-1)!}{(p-1)}\right\}$$

— o — o —

$$\sum_{k=1}^{p-1} \frac{1}{k} = \frac{m}{n} \Rightarrow p^2 \mid m \quad (\text{se } p \geq 5)$$

FATTO 1

$$\sum_{k=1}^{p-1} (k)^a = \begin{cases} 0 & \text{altrimenti} \\ -1 & \text{se } (p-1) \mid a \end{cases}$$

si dimostra usando il generatore per ricondurre la somma ad una geometrica

$$\sum k^a = \sum g^{ka}$$

— o — o —

2 **LEMMA** n intero >0, p primo

$2^n = a^p + b^p$ a, b interi >0

Allora $n = kp+1$

[Idea: se $n = kp+1$ $a = b = 2^k$ e allora
$a^p + b^p = 2^{kp} + 2^{kp} = 2^{kp+1}$]

Dim. Scrivo $a = 2^R \alpha$ $b = 2^\ell \beta$
Si vede facilmente che $R = \ell$

$2^n = 2^{Rp} \alpha^p + 2^{Rp} \beta^p$ semplifico $2^{n'} = \alpha^p + \beta^p$

Posso supporre $2^n = a^p + b^p$ con a e b dispari

p dispari $2^n = (a^p + b^p) = (a+b)\underbrace{(a^{p-1} - \dots + b^{p-1})}$

p fattori, quindi il termine è dispari

Inoltre $(a^{p-1} - a^{p-2}b + a^{p-3}b^2 - a^{p-4}b^3 + \dots)$
$= a^{p-2}(a-b) + a^{p-4}b^2(a-b) + \dots + \dots + b^{p-1}$

wlog $a \geq b$ .. si esce difficilmente...

Se $(\dots) = 1$, allora $a^p + b^p = a+b \Rightarrow a = b = 1$

Se $p = 2$ $a^2 + b^2 \equiv 2 \pmod 4$, quindi $n = 1$ e $a = b = 1$

N.B. Il lemma vale per p qualunque (anche non primo) con la stessa dimostrazione

— o — o —

$S = \{p_1, \dots, p_k\}$ $n = 2^{p_1 \cdot \dots \cdot p_k + 1}$

Allora $2^{p_1 \cdots p_k + 1} = a^p + b^p$ si risolve se e solo se

esponente -1 = multiplo di p, quindi se e solo se $p \in S$,

Esercizio 3 Per quali valori di u si ha che $x^3 + ux$ è iniettivo modulo 107.

$$x^3 + ux = y^3 + uy \qquad x^3 - y^3 = u(y-x)$$

$$(x-y)(x^2+xy+y^2) = -u(x-y)$$

Voglio che ci sia uguaglianza con $x \neq y$. Devo risolvere

$$\boxed{x^2 + xy + y^2 = -u}$$

↗ se ho sol. con $x \neq y \Rightarrow$ NO INIETTIVA

↘ se non ho sol. con $\neq \neq y \Rightarrow$ INIETTIVA

Tutto si riduce a trovare l'immagine di $x^2+xy+y^2 \pmod{107}$

$x^2 + xy + y^2 = k$ BANALE: se k è un residuo quadratico $\neq 0$, allora c'è soluzione del tipo $(x,0)$

Resta da vedere se esistono NON residui nell'immagine

Oss. Se $x^2 + xy + y^2 = k \leftarrow$ NON RESIDUO, allora $x \neq y$.

Se fosse $x = y$, allora $k = \boxed{3}x^2$

↓ residuo (mod 107)

$324 \equiv 3 \pmod{107}$ $\quad 324 = 18^2$ (altrimenti reciprocità quadratica)

RES · RES = RES.

NON RES · NON RES = RES

NON RES · RES = NON RES.

$$\text{RES} \iff g^{\text{PARI}}$$

NON RESIDUO FISSO · RESIDUO = $\frac{p-1}{2}$ cose diverse che sono tutti non residui

NON RESIDUO FISSO · NON RESIDUO VARIAB. = $\frac{p-1}{2}$ cose diverse dalle precedenti che quindi sono tutte residui

Oss. 2 I k ottenibili come x^2+xy+y^2 sono un insieme chiuso per moltiplicazione. Sono anche quelli scrivibili come $4x^2+4xy+4y^2 = (2x+y)^2 + 3y^2$

Le cose che si scrivono come A^2+3B^2 sono chiuse per moltiplicazione

$$A^2+3B^2 = (A+\sqrt{-3}B)(A-\sqrt{-3}B)$$
$$C^2+3D^2 = (C+\sqrt{-3}D)(C-\sqrt{-3}D)$$

$$(A^2+3B^2)(C^2+3D^2) = [(A+\sqrt{-3}B)(C+\sqrt{-3}D)][\ \dots\ ]$$
$$(X+\sqrt{-3}Y) \qquad (X-\sqrt{-3}Y)$$

$$X = AC-3BD \qquad Y = AD+BC$$

Oss. 3 Se io so costruire un non residuo ho costruito tutto.

$x=9 \quad y=2 \qquad x^2+xy+y^2 = 81+18+4 = 103 \equiv -4$

$-4 = 4 \cdot (-1)$

↑ RES ↑ NON RES. ($107 \equiv 3 \mod 4$)

Oss. 4 Provo con (x, Rx)

$$x^2+xy+y^2 = x^2(R^2+R+1)$$

Qual è l'immagine di $R^2+R+1 \pmod{107}$?
È la "stessa" di $4R^2+4R+4 = (2R+1)^2+3$
Per assurdo ci siano solo residui nell'immagine. Allora
$(2R+1)^2+3 =$ residuo
cioè si ha sempre che residuo $+3 =$ residuo
Per $R=1$ se $12 \in \mathrm{Im}$, allora 12 è immagine di un $R \neq 1$.

$\Rightarrow$ questo vuol dire che $0, 3, 6, 9, \dots$ sono tutti residui
$\Rightarrow$ tutti residui.

Oss. 5 Per la dim. bastava usare $(x, 2x)$ $(x, 3x)$

$x^2+y^2+xy=0$ → se $y=0$, allora $x=0$ e sono uguali
→ se $y\neq 0$

$\left(\frac{x}{y}\right)^2+\frac{x}{y}+1=0$, cioè $z^2+z+1=0$ e questa non ha soluzioni perchè -3 non è residuo !!!

— o — o —

Quando x^k è iniettiva mod p?

⇕

$(p-1,k)=1$

x^k è iniettiva $(\text{mod } m) \iff (\Phi(m),k)=1$.