Teoria dei Numeri 1 - Medium

Titolo nota 03/09/2014

Polinomi in $\mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x] = \mathbb{Z}/(p)[x]$

Espressione formale

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

con gli $a_i \in \mathbb{F}_p$

Si può calcolare $p([n])$ dove $[n]$ è una classe di resto mod p

Cosa funziona? TUTTO

- Un pol. di grado n ha $\leq n$ radici
- Principio di identità dei polinomi: ⚠

  Vale con le giuste ipotesi sul grado

Esempio: $x^p - x$ coincide (come funzione, non come polinomio) con 0

- Divisione con resto, Ruffini, fattorizzaz. unica

Esercizio Sia $f: \mathbb{F}_p \longrightarrow \mathbb{F}_p$. Allora esiste $q(x) \in \mathbb{F}_p[x]$ tale che per ogni $[n] \in \mathbb{F}_p$ si abbia $q(n) = f(n)$.

Soluzione Quante sono le funzioni? p^p

Quando succede che due polinomi $q_1(x)$, $q_2(x)$ rappresentano la stessa funzione?

$q_1(n) = q_2(n)$ per $n = 0, 1, 2, \dots, p-1$

$$\Rightarrow \quad q_1(x) - q_2(x) = \underbrace{x(x-1)(x-2)\cdots(x-(p-1))}_{x^p - x} r(x)$$

$x^p - x$ e $\prod_{i=0}^{p-1}(x-i)$ hanno lo stesso grado, stesse radici, stesso coeff. di grado massimo

Ci interessano solo le classi di resto modulo $x^p - x$.

Quindi due polinomi diversi di grado $\leq p-1$ rappresentano funzioni diverse

$$\{\text{polinomi di grado} \leq p-1\} \xrightarrow[\varphi]{\text{iniettiva}} \{\text{funzioni}\}$$

$|\{\text{polinomi}\}| = p^p \qquad |\{\text{funzioni}\}| = p^p$

Quindi φ è bigettiva (in particolare è surgettiva)

Esercizio stupido $\binom{p-1}{j} \equiv (-1)^j \pmod p$

Considero $(1+x)^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} x^j$

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

Uguaglianza tra polinomi $\Rightarrow$ ug. dei coeff. (mod p)

GENERATORI MOD p

Sostengo che per ogni k che divide $p-1$ ci siano esattamente $\varphi(k)$ elementi di ordine k

Induzione : $k=1$ OK

$$\left\{\begin{array}{l}\text{elementi di ordine} \\ \text{che divide } k\end{array}\right\} = \left\{\text{radici di } x^k - 1\right\}$$

Quante radici ha $x^k - 1$?

$$\underbrace{x^{p-1} - 1}_{p-1 \text{ radici}} = \underbrace{(x^k - 1)}_{\leq k \text{ rad.}} \cdot \underbrace{r(x)}_{\leq p-1-k \text{ radici}}$$

Quindi $x^k - 1$ ha esattamente k radici

$$x^k - 1 = \prod_{ord_p(r) | k} (x - r) = \prod_{ord(r) = k} (x - r) \times \prod_{\substack{ord(r) | k \\ ord(r) \neq k}} (x - r)$$

Gradi : LHS ha grado k

RHS " " n° el. di ordine k $+ \sum_{\substack{j | k \\ j \neq k}} n^\circ$ di elem. di ord j

$$\Rightarrow \cancel{k} = (n^\circ \text{ di elem. ord } k) + \sum_{\substack{j|k \\ j\neq k}} \varphi(j)$$

$$= \qquad '' \qquad + \underbrace{\sum_{j|k} \varphi(j)}_{\cancel{k}} - \varphi(k)$$

$\square$

In particolare, ci sono $\varphi(p-1)$ generatori

GENERATORI MOD m

$$x^{\varphi(m)} \equiv 1 \ (m) \quad \text{per ogni} \quad (x, m) = 1$$

Un generatore e' un elemento (coprimo con m) di ordine esattamente $\varphi(m)$. Esiste se e solo se m e'

* 2 o 4
* p^n o $2p^n$ con p primo dispari

Residui quadratici (e superiori)

Si dice che a è un residuo quadratico mod p se esiste n tale che $n^2 \equiv a \ (p)$

Sono $\underset{\text{lo zero}}{1} + \underset{\text{quelli seri}}{\frac{p-1}{2}}$

$$\{0, 1, 2, \dots, (p-1)\} \xrightarrow{\square} \text{Residui Quadratici}$$

Cosa fa fallire l'iniettività?

$$x_1^2 \equiv x_2^2 \pmod p$$

$$\iff (x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod p$$

$$\iff p \mid x_1 - x_2 \quad \text{o} \quad p \mid x_1 + x_2$$

Se mi restringo a $\{0, 1, \dots, \frac{p-1}{2}\}$ la funz. $\square$ è iniettiva e surgettiva (perché se $n^2 \equiv a$ e $n \in \{\frac{p+1}{2}, \frac{p+3}{2}, \dots, p-1\}$, allora $a \equiv (-n)^2$ e $-n \in \{1, 2, \dots, \frac{p-1}{2}\}$

$$\Rightarrow |RQ| = 1 + \frac{p-1}{2}$$

SIMBOLO DI LEGENDRE

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ è RQ mod } p \\ -1, & \text{se } a \text{ NON è RQ `` ''} \\ 0, & \text{se } p \mid a \end{cases}$$

$\boxed{p \neq 2}$

Proprietà: * $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

* (Criterio di Eulero) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Oss: Eulero $\Rightarrow$ Moltiplicatività

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \bmod p$$

Siccome LHS, RHS $\in \{0, 1, -1\}$, la congruenza è una uguaglianza.

Esempio: almeno uno tra 2, 3 e 6 è RQ mod p per ogni primo.

Se 2 non è RQ e 3 nemmeno, allora

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1) = 1$$

Dimostrazione di Eulero

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \bmod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \in \{+1, -1\}$$

Consideriamo $\underbrace{x^{\frac{p-1}{2}} - 1}_{q(x)}$ (come polinomio mod p)

Ha al max $\frac{p-1}{2}$ radici, e tutti i quadrati sono radici: $\square^{\frac{p-1}{2}} - 1 \equiv (n^2)^{\frac{p-1}{2}} - 1$

$$\equiv n^{p-1} - 1 \equiv 0 \ (p)$$

Quindi $q(x) \equiv 0 \pmod p \iff x$ e' RQ

$$\Updownarrow$$

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p$$

In termini di generatori: $x \equiv g^k \mod p$

e x e' RQ $\iff$ k e' pari

$$\Updownarrow \qquad\qquad \Updownarrow$$

$$x^{\frac{p-1}{2}} \equiv 1 \ (p) \iff g^{k \cdot \frac{p-1}{2}} \equiv 1 \pmod p$$

Quando e' che -1 e' un RQ?

Risposta: se e solo se $p \equiv 1 \ (4)$, perche'

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

$+1$ se e solo se $\frac{p-1}{2}$ e' pari

$\iff p \equiv 1 \mod 4$

Esercizio $x^2 = y^3+7$

$$x^2+1 = y^3+8 = (y+2)(y^2-2y+4)$$

Mod 8 $\quad x^2 \equiv y^3+7 \mod 8$

Se y fosse pari, MALE

(x e' multiplo di 4)

Se $y \equiv 1 \mod 4$, allora $y+2 \equiv 3(4)$ e

c'e' (nel fattore di dx) almeno un primo $p \equiv 3\ (4)$. Mod p abbiamo

$$x^2+1 \equiv 0\ (p)$$

$$-1 \equiv x^2\ (p),$$

che contraddice $\left(\frac{-1}{p}\right) = -1$

Se $y \equiv 3 \mod 4$, $\quad y^2-2y+4 \equiv 3\ (4)$ e

si conclude allo stesso modo.

Quindi non ci sono soluzioni

Che dire di $\left(\frac{2}{p}\right)$?

$$-1 \equiv (p-1)! \equiv (p-1)!!\,(p-2)!!$$

Wilson

$$\equiv (2\cdot 4\cdot 6\cdot \ldots \cdot p-1)\,(p-2)!!$$

$$\equiv 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\,(p-2)!!$$

$$1\cdot 3\cdot 5\cdot 7\cdot 9 = 1\cdot 3\cdot 5\cdot(-4)(-2) \quad (p=11)$$

$$= \left(\frac{11-1}{2}\right)!$$

$$1\cdot 3\cdot 5\cdot 7\cdot 9\cdot \underbrace{11}_{(-8)}\cdot \underbrace{13}_{(-6)}\cdot \underbrace{15}_{(-4)}\cdot \underbrace{17}_{(-2)} \qquad p=19$$

$$1\cdot 3\cdot 5\cdot 7\cdot 9\cdot 11 \qquad p=13$$

$$(p-2)!! = \begin{cases} (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! & \frac{p-1}{2} \text{ pari} \\ (-1)^{\frac{p-3}{4}} \left(\frac{p-1}{2}\right)! & \frac{p-1}{2} \text{ dispari} \end{cases}$$

$$-1 \equiv 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\,(p-2)!!$$

$$\equiv 2^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \cdot \begin{cases} (-1)^{\frac{p-1}{4}} & p\equiv 1\ (4) \\ (-1)^{\frac{p-3}{4}} & p \equiv 3\ (4) \end{cases}$$

$$\equiv 2^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \cdot (p-1)! \cdot \begin{cases} (-1)^{(p-1)/4} \\ (-1)^{(p-3)/4} \end{cases}$$

$$\Rightarrow \quad 2^{\frac{p-1}{2}} \equiv \cancel{(-1)}\,\cancel{(-1)}\,(-1)^{\frac{p-1}{2}} \begin{cases} (-1)^{(p-1)/4} \\ (-1)^{(p-3)/4} \end{cases}$$

Dipende solo da p mod 8

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv \begin{cases} +1, & \text{se } p \equiv \pm 1 \ (8) \\ -1, & \text{se } p \equiv \pm 3 \ (8) \end{cases}$$

Residui "superiori"

a è residuo k-esimo se $\exists n$ tale che

$n^k \equiv a \mod p$

Sono $1 + \frac{p-1}{(p-1,k)}$

Residui cubici mod 17 : TUTTI!

Ogni classe di resto si scrive g^k per un certo k. Posso scegliere $k \equiv 0$ (3)?

Se $n \equiv g^k$, n è anche $\equiv g^{k+(p-1)}$
$\equiv g^{k+2(p-1)}$

e siccome $p-1 \not\equiv 0$ (3) (almeno) uno tra

$k, \ k+16, \ k+32$ è $0 \mod 3$

"Criterio di Eulero" n è un residuo k-esimo $\iff$ $n^{\frac{p-1}{(k,p-1)}} \equiv 1 \mod p$

Esercizi

BMO 2014/2 $\quad 2014 = \frac{a^3+2b^3}{c^3+2d^3}$

$2014 = 2 \cdot 19 \cdot 53$

$$2014\,(c^3+2d^3) = a^3+2b^3$$

Mod 19: $\quad 0 \equiv a^3+2b^3 \mod 19$

Moralmente, $\quad -2 \equiv \left(\frac{a}{b}\right)^3 \mod 19$

in gara: "se $b \not\equiv 0 \mod 19$"

-2 e' residuo cubico mod 19 $\iff$ $(-2)^6 \equiv 1 \ (19)$

$\overset{\text{///}}{64}$

$\iff$ NO $\quad$ (Siccome $(-2)^{\frac{19-1}{(3,18)}} \not\equiv 1 \mod 19$,

-2 NON e' residuo cubico mod 19)

$\Rightarrow b \equiv 0 \ (19) \Rightarrow a \equiv 0 \ (19)$

E ora discesa infinita. (FATELA!)

RMM 2013/1

Sia a un intero positivo.

$x_1 = a, \quad x_{n+1} = 2x_n+1, \quad y_n = 2^{x_n}-1$

Qual e' il piu' grande k per cui esiste a tale che $y_1, y_2, \ldots, y_k$ siano tutti primi

$a = 2 \longrightarrow \quad y_1 = 3, \quad y_2 = 31$

Osservazione: Se gli y_n sono primi, anche gli x_n sono primi

Per assurdo: y_1, y_2, y_3 primi

$$y_2 = 2^{x_2} - 1 \equiv 2^{\frac{x_3-1}{2}} - 1 \mod x_3 \quad (*)$$

x_3 divide y_2 se 2 e' RQ mod x_3

perché $2^{\frac{x_3-1}{2}} \equiv \left(\frac{2}{x_3}\right) \mod x_3 \quad (*)$

Vogliamo $\left(\frac{2}{x_3}\right) = 1$, cioe' $x_3 \equiv \pm 1 \pmod 8$

Parto da $x_1 \rightsquigarrow \underbrace{2x_1+1}_{\equiv 3 \bmod 4} \rightsquigarrow \underset{\equiv 7 \bmod 8}{2(2x_1+1)+1}$

Quindi: x_1 e' primo, quindi o $x_1 = 2$ o x_1 dispari. $x_1 = 2$ si prova a mano.

$$x_1 \text{ dispari} \Rightarrow x_3 \equiv 7 \ (8) \overset{(*)}{\Rightarrow} x_3 \mid y_2$$

$$\Rightarrow \underset{\substack{\parallel \\ 2x_2+1}}{x_3} = y_2 = 2^{x_2} - 1$$

Questo e' possibile solo per $x_2 = 3$, ma non funziona

IMO 2006/4 $\quad y^2 = 1 + 2^x + 2^{(2x+1)}$

Mod 2^x : $y^2 \equiv 1 \mod (2^x)$

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

quasi coprimi: uno dei due è $\equiv 0 \ (2^{x-1})$

$y = \pm 1 + K \cdot 2^{x-1}$

$\cancel{1} \pm K \cdot 2^x + K^2 \cdot 2^{2(x-1)} = \cancel{1} + 2^x + 2^{2x+1}$

A mano : $x \leq 2$

$\pm K + K^2 \cdot 2^{x-2} = 1 + 2^{x+1}$

$\leq$ ← wlog $K>0$

$\underbrace{K\left(\frac{K}{4} 2^x - 1\right)}_{\text{crescente in } K.} \geq 4(2^x - 1)$

crescente in K. Per $K=4$

Quindi: o $x \leq 2$ o $K \leq 3$ (A MANO)

LEMMA LTE ("lifting the exponent")

Notazione: $v_p(n)$ = l'esponente di p nella fattorizzazione di n

* $v_p(ab) = v_p(a) + v_p(b)$

* $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

con = se $v_p(a) \neq v_p(b)$

$$a = p^{v_p(a)} \cdot r, \quad b = p^{v_p(b)} \cdot s$$

$$v_p(a) > v_p(b)$$

$$a+b = p^{v_p(b)} \underbrace{\left(p^{v_p(a)-v_p(b)} r + s\right)}_{\not\equiv 0 \ (p)}$$

Enunciato • p primo dispari

• a, b NON multipli di p

• $p \mid a-b$

Allora $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$

Corollario Se n è dispari, lo applico a "a" e "$-b$" e quindi vale anche con il $+$

$$\left(\begin{array}{c} p \nmid a,\ p \nmid b,\ p \mid a+b \\ v_p(a^n + b^n) = v_p(a+b) + v_p(n) \\ n \text{ dispari} \end{array} \right)$$

Dimostrazione

Caso $n=p$ $\qquad a-b = kp^{v}$ con $(k,p)=1$, $\quad v = v_p(a-b)$

$$a^p - b^p = (b+kp^v)^p - b^p =$$

$$= b^p + p\cdot b^{p-1}\cdot(kp^v) + \sum_{j=2}^{p} \underbrace{\binom{p}{j}} b^{p-j} \underbrace{(k\cdot p^v)^j} - b^p$$

$$v_p(a^p-b^p) = v_p\left(kb^{p-1}\cdot p^{v+1} + p^{2v+1}(\dots)\right)$$

$$= v+1 = v_p(a-b)+1$$

Caso $(n,p)=1$ $\qquad a^n - b^n =$

$$= \cancel{b^n} + n\cdot b^{n-1}\cdot(kp^v) + \sum_{j=2}^{n} \binom{n}{j} b^{n-j} \underbrace{(k\cdot p^v)^j} \cancel{-b^n}$$

$$v_p(a^n-b^n) = v = v_p(a-b)$$

Caso generale "Induzione"

$$n = p^{v_p(n)}\cdot r \quad \text{con} \quad (r,p)=1$$

$$v_p(a^n-b^n) = v_p\left(\left(a^{p^{v_p(n)}}\right)^r - \left(b^{p^{v_p(n)}}\right)^r\right)$$

caso $(n,p)=1$

$$= v_p\left(a^{p^{v_p(n)}} - b^{p^{v_p(n)}}\right)$$

caso $n=p$ applicato $v_p(n)$ volte

$$= v_p(a-b) + v_p(n)$$

$$v_p\left(a^{p^2} - b^{p^2}\right) = v_p\left((a^p)^p - (b^p)^p\right)$$

$$= v_p\left(a^p - b^p\right) + 1$$

$$= v_p(a-b) + 2$$

GUADAGNO DI UN PRIMO

p primo dispari

"a^p+b^p ha un fattore primo che $a+b$ non ha, a meno che $a=2$, $b=1$, $p=3$ oppure $a=b=1$"

$$a^p+b^p = \left(\frac{a^p+b^p}{a+b}\right)(a+b)$$

Dimostrazione Sia q un fattore primo di $a+b$

Per LTE, $v_q\left(\frac{a^p+b^p}{a+b}\right) = v_q(a^p+b^p) - v_q(a+b)$

$$= v_q(a+b) + v_q(p) - v_q(a+b)$$

$$= v_q(p)$$

Conclusione: $a+b$, $\frac{a^p+b^p}{a+b}$ sono coprimi tranne al più un singolo fattore p.

Se (per assurdo) $\frac{a^p+b^p}{a+b}$ non ha fattori primi "nuovi" (risp. ad $a+b$), allora $\frac{a^p+b^p}{a+b} = \begin{cases} p \\ 1 \end{cases}$

Se $a \geq 2$, $b \geq 2$ abbiamo $a^p > ap$

$b^p > bp$

e sommandole ASSURDO. Quindi $\min\{a,b\}=1$

$a=1, \quad b\geq 2 \qquad 1+b^p = p(1+b)$

$$\begin{aligned} 1+b^p = 1+[1+(b-1)]^p &\geq 1+1+p(b-1) \\ &\quad + \frac{p(p-1)}{2}(b-1)^2 \end{aligned}$$

$$2p \geq 2+p\,\frac{(p-1)}{2}(b-1)^2 \geq p\left(\frac{p-1}{2}\right)(b-1)^2$$

$$2 \geq \left(\frac{p-1}{2}\right)(b-1)^2 \implies \begin{array}{l} (b-1)\leq 1 \\ \frac{p-1}{2}\leq 2 \end{array}$$

... si trattano a mano i casi piccoli.

GENERATORI MOD p^n ($p \neq 2$)

(1) Fatto: esiste un gen. mod p^n

(2) Fatto migliore: se g è un generatore mod p allora o g o $g+p$ è un generatore modulo p^2

(3) Fatto ancora migliore: se h genera mod p^2, genera anche mod p^n per ogni n

Dim di (2) $g^{p-1} \equiv 1 \mod p$. Per essere gen mod p^2: $g^{p-1} \not\equiv 1 \mod p^2$ $(*)$

Claim: $(*)$ è condizione sufficiente per generare mod p^2, ammesso che g generi modulo p

Qual è l'ordine di g mod p^2?

$\text{ord}_{p^2}(g)$ è multiplo di $\text{ord}_p(g) = p-1$

$$(p-1) \mid \text{ord}_{p^2}(g) \mid \varphi(p^2) = p(p-1)$$

non è un uguale

Quindi $\text{ord}_{p^2}(g) = p(p-1)$ e g genera.

Ci siamo ridotti a: "se g genera mod p,
o $g^{p-1} \not\equiv 1 \mod p^2$ o $(g+p)^{p-1} \not\equiv 1 \ (p^2)$"

Supponiamo quindi $g^{p-1} \equiv 1 \ (p^2)$. Allora

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1) g^{p-2} p + \text{termini in } p^2$$

$$\equiv 1 + \underbrace{p(p-1) g^{p-2}}_{\substack{\text{non è zero mod } p^2 \\ \text{perché ha esattamente} \\ \text{un fattore } p}} \pmod{p^2}$$

$$\not\equiv 1$$

Se g genera mod p^2, genera mod p^n.

$$g^{p-1} \not\equiv 1 \ (p^2) \qquad g^{p-1} \equiv 1 \ (p)$$

$$v_p\left(g^{p-1}-1\right) = 1$$

Quanto vale $\operatorname{ord}_{p^n}(g)$?

$$\operatorname{ord}_{p^n}(g) = (p-1)\cdot p^r$$

Tesi $\iff \operatorname{ord}_{p^n}(g) = \varphi(p^n) = (p-1)\,p^{n-1}$

$\iff r = n-1$. Stimiamo r:

$$g^{(p-1)p^r} \equiv 1 \mod p^n$$

$$n \le v_p\left(g^{(p-1)p^r}-1\right) = v_p\left(\left(g^{(p-1)}\right)^{p^r} - 1^{p^r}\right)$$

$$\overset{\text{LTE}}{=} v_p(p^r) + v_p\left(g^{p-1}-1\right)$$

$$= r+1$$

$\Rightarrow \quad r \geqslant n-1$

SNS 2014/1 $\qquad a^7+b^7=7^c \qquad a,b,c\geq 1$

$$\underbrace{a^7+b^7}_{\displaystyle \left(\frac{a^7+b^7}{a+b}\right)(a+b)}$$

- $a+b$ = potenza di 7 $(\neq 1)$
- Guadagno di un primo $\Rightarrow \frac{a^7+b^7}{a+b}$ ha un fattore primo $\neq 7$, quindi non è una potenza di 7

NO SOLUZIONI

Esercizio $\quad a^7+b^7=7^c 3^d$

Es $\quad x^5+4^y=2013^z \quad (2013=3\cdot 11\cdot 61)$

Mod 11: $\quad x^5+4^y\equiv 0 \pmod{11}$

$\ulcorner$ $\text{ord}_{11}(4)=5$: perché?

$$\text{ord}_{11}(4) \mid 10$$

$$4^5 \equiv 4^{\frac{11-1}{2}} \equiv 1 \quad (11) \quad (\text{Eulero})$$
$\llcorner$

$4^y \not\equiv -1 \pmod{11}$ perché $4^y=\square$ e -1 non lo è (perché $11\equiv 3 \pmod 4$)

Unica configurazione ammessa: $\quad x^5\equiv -1 \quad (11)$

$$4^y \equiv 1 \quad (11)$$

$\Rightarrow \quad 5 \mid y \qquad y = 5a$

$$(x+4^a)\left(\frac{x^5+4^{5a}}{x+4^a}\right) = 2013^z = 3^z\, 11^z\, 61^z$$

coprimi! In generale potrebbero avere in comune un fattore 5, ma $5 \nmid \text{RHS}$

Se $x+4^a \equiv 0 \pmod{11^z}$

$$\Rightarrow \quad x^5+4^{5a} \geq 2\left(\frac{x+4^a}{2}\right)^5 \geq \frac{1}{16}\, 11^{5z}$$

$$\gg 2013^z$$

Sennò, $x+4^a = 3^z$, ma allora

$$x^5+4^{5a} \leq (x+4^a)^5 \leq \underbrace{243}_{3^5}{}^z \ll 2013^z$$

IMO 2000

Domanda: esiste un n con esattamente 2000 fattori primi diversi e t.c. $n \mid 2^n+1$?

Risposta: $\boxed{\text{Sì}}$

$p \mid 2^p+1 \Rightarrow p \mid 3 \Rightarrow p=3$

$n=3$ rispetta $3 \mid 2^3+1$

Osservazione: se abbiamo n : $n \mid 2^n+1$ e p è un fattore primo di 2^n+1 che n non ha, allora np rispetta $np \mid 2^{np}+1$

Basta dim che $p \mid 2^{np}+1$, $n \mid 2^{np}+1$

$$1+2^{np} \underset{FLT}{\equiv} 1+2^n \equiv 0 \pmod p$$

$\hookleftarrow$ $p \mid 2^n+1$ per ipotesi

$$n \mid 2^n+1 \mid (2^n)^p+1^p$$

Per inizializzare la ricorrenza prendo $n=9$

$$9 \mid 2^9+1$$

Ora $2^9+1 = (2^3+1)\left(\frac{2^9+1}{2^3+1}\right)$ ha un fattore primo $\neq 3$ (dicono 19)

$n_1 = 9 \qquad n_2 = 9 \cdot 19$

$$2^{n_2} + 1 = \left(\frac{(2^{n_1})^{19} + 1}{2^{n_1} + 1} \right) (2^{n_1} + 1)$$

ha un fattore primo che $2^{n_1}+1$ non ha

Ma $n_1 \mid 2^{n_1}+1$, quindi questo fattore primo p non sta neppure in n_1.

D'altro canto, n_2 è $n_1 \times$ un fattore primo di $2^{n_1}+1$. Quindi $p \nmid n_1$, $p \nmid 2^{n_1}+1$

$\Rightarrow p \nmid n_2$, e quindi posso prendere

$$n_3 = p n_2$$

+ Induzione

Es Esistono infiniti n tali che

$$n \nmid 2^n+1, \qquad n \mid 2^{2^n+1}+1$$

Soluzione

$a_n = 2^{3^n}+1$ e p_n un primo che divide a_n ma non a_{n-1} (guad di un primo)

Prendo $b_n = p_n \cdot 3^{n-1}$

(1) $b_n \nmid 2^{b_n}+1$

(2) $b_n \mid 2^{2^{b_n}+1}+1$

(1) $2^{b_n}+1 = \left(2^{3^{n-1}}\right)^{p_n}+1 \equiv 2^{3^{n-1}}+1$

$\equiv a_{n-1} \not\equiv 0 \ (p_n)$

(2) $3^{n-1} \overset{?}{\mid} 2^{2^{b_n}+1}+1 \iff v_3\left(2^{2^{b_n}+1}+1\right) \geq n-1$

$$v_3\left(2^{2^{b_n}+1}+1\right) \overset{LTE}{=} v_3(2+1)+v_3(2^{b_n}+1) = 1+v_3(2+1)+v_3(b_n) = 2+(n-1) = n+1$$

$p_n \overset{?}{\mid} 2^{2^{b_n}+1}+1 \qquad p_n \mid 2^{3^n}+1$

$$v_3\left(2^{b_n}+1\right) = v_3(2+1) + v_3(b_n) = n$$

$$2^{b_n}+1 = 3^n \cdot c$$

$p_n \overset{?}{\mid} 2^{c\cdot 3^n}+1$: sì, perché

$$p_n \mid 2^{3^n}+1 \mid 2^{3^n\cdot c}+1$$

IMO 2003 / 6

Sia p un numero primo. Esiste un primo q tale che per ogni n $\quad n^p - p \not\equiv 0 \pmod q$

Soluzione Tesi: p non e' un residuo p-esimo modulo q. In particolare $p \mid q-1$ (altrimenti, il numero dei residui p-esimi mod q sarebbe $1 + \frac{q-1}{(q-1,p)} = q$ e tutto, in particolare p, sarebbe un residuo p-esimo)

Criterio di Eulero generalizzato:

$$p^{\frac{q-1}{p}} \not\equiv 1 \pmod q$$

$\iff \operatorname{ord}_q(p) \nmid \frac{q-1}{p}$

Prova: prendo $\operatorname{ord}_q(p)$ un primo

Mica tanto facile! L'ordine di p mod q divide $q-1$, ma non deve dividere $\frac{q-1}{p}$

Hope: riesco a trovare q t.c. $\operatorname{ord}_q(p) = p$

e $q \not\equiv 1 \bmod p^2$ $\left(\iff p \nmid \frac{q-1}{p}\right)$

$p^p \equiv 1 \mod q \Rightarrow$ se un tale q esiste, è un fattore di $p^p - 1$.

Cerchiamo un q che divida $\frac{p^p-1}{p-1}$ e non sia $\equiv 1 \ (p^2)$. Esiste?

Se non esistesse, $\frac{p^p-1}{p-1}$ sarebbe $\equiv 1 \ (p^2)$

Ma non è vero: $1 \equiv \frac{p^p-1}{p-1} \pmod{p^2}$

$$\Rightarrow \underbrace{p - \cancel{1}}_{\equiv\, p} \equiv \underbrace{p^p - \cancel{1}}_{\equiv\, 0} \pmod{p^2},$$

$\boxed{\text{ASSURDO}}$

Quindi $\exists\, q : \operatorname{ord}_q(p) = p,\ p^2 \nmid q-1$, e un tale q funziona (per Eulero)