Teoria dei Numeri 2 - MEDIUM

Titolo nota 07/09/2009

ORDINE MOLTIPLICATIVO MODULO p

Dato a con $(a,p)=1$ si dice $\mathrm{ord}_p(a)$ il + piccolo intero $n>0$ tale che

$$a^n \equiv 1 \pmod p$$

<u>Proprietà</u>: ① $\mathrm{ord}_p(a) \mid (p-1)$

② Dato un qualunque intero m tale che $a^m \equiv 1 \pmod p$ si ha che $\mathrm{ord}_p(a) \mid m$

Altro modo di dire la stessa cosa: l'insieme

$$\{ m \in \mathbb{N} \text{ t.c. } a^m \equiv 1 \pmod p \}$$

sono tutti e soli i multipli di $\mathrm{ord}_p(a)$

<u>Corollario</u> Se $a^k \equiv a^l \pmod p$ e $(a,p)=1$, allora $\mathrm{ord}_p(a) \mid (k-l)$.

— o —

<u>Domanda</u>: se $d \mid (p-1)$, è vero che esiste a t.c. $\mathrm{ord}_p(a)=d$?

VERO MA NON BANALE: conseguenza dell'esistenza di un generatore, cioè un elemento g t.c. $\mathrm{ord}_p(g)=p-1$ (il che implica che le potenze $g^1, \dots, g^{p-1}$ sono tutte distinte, quindi sono tutte le classi (non nulle) mod p.)

Dato g, considero $g^{\frac{p-1}{d}} = a$. Allora $\mathrm{ord}_p(a)=d$

È chiaro che $a^d = g^{p-1} \equiv 1 \quad (p)$

Supponiamo che l'ordine sia un divisore d' di d. Allora

$$a^{d'} = g^{\boxed{\frac{p-1}{d}\cdot d'}} \not\equiv 1 \text{ perché } g \text{ è generatore}$$

esponente $< p-1$

—o—o—

<u>Esercizio</u> Sia $p = 37$. Considero $a \to a^3$

È iniettiva (mod 37)? È surgettiva? (Da $\{0, 1, \dots, 36\}$ in sè)

<u>Oss.</u> È iniettiva $\Leftrightarrow$ è surgettiva (perché l'insieme di partenza e l'insieme di arrivo hanno lo stesso numero di elementi)

Vediamo se è iniettiva: $a^3 = b^3$. Vorremmo dividere per b^3.
Possibile se $(b, p) = 1$. Ci sono 2 casi
* $b = 0$ e allora banalmente $a = 0$
* $b \neq 0$, allora $(b, p) = 1$, allora moltiplico per l'inverso di b^3

$$(ab^{-1})^3 \equiv 1 \pmod{37}, \text{ ma allora } \operatorname{ord}_{37}(ab^{-1}) \mid 3$$

D'altra parte $\operatorname{ord}_{37}(ab^{-1}) \mid p-1 = 36$.
Quindi l'ordine può essere $\nearrow 1$ $\searrow 3$

Se $\operatorname{ord}_{37}(ab^{-1}) = 1 \Rightarrow ab^{-1} \equiv 1 \Rightarrow a \equiv b$
" " $= 3 \Rightarrow ab^{-1}$ è uno degli elementi di ordine 3
Esistono elementi k che hanno ordine 3 $(g^{12}) \Rightarrow$
ab^{-1} può non essere $1 \Rightarrow$ NON INIETTIVA.

—o—o—

Quanti sono gli elementi di ordine 3 mod 37? $\Phi(3)$!!!

Saranno elementi del tipo g^k. Basta trovare k

$$(g^k)^3 \equiv 1 \Leftrightarrow g^{3k} \equiv 1 \Leftrightarrow (p-1) \mid 3k \Leftrightarrow$$

$$\frac{p-1}{3} \mid k, \quad \text{cioè} \quad k = \frac{p-1}{3}, \quad k = \frac{2(p-1)}{3}, \quad k = \frac{\cancel{3}(p-1)}{\cancel{3}}$$

NO ord $= 1$.

Più in generale: quando $a \to a^k$ è iniettiva (quindi anche surgettiva) modulo p?

Risposta $\Leftrightarrow$ $(k, p-1) = 1$

Dim. $a^k \equiv b^k \pmod p \rightsquigarrow (ab^{-1})^k \equiv 1 \pmod p$

$\rightsquigarrow \mathrm{ord}_p(ab^{-1}) \mid k$ e inoltre $\mathrm{ord}_p(ab^{-1}) \mid (p-1)$ (fatto gen.)

$\rightsquigarrow \mathrm{ord}_p(ab^{-1}) \mid \mathrm{MCD}(k, p-1) = 1$

$\rightsquigarrow \mathrm{ord}_p(ab^{-1}) = 1 \rightsquigarrow ab^{-1} \equiv 1 \pmod p \rightsquigarrow a = b$

— o — o —

Consideriamo $a \to a^k$ in un caso in cui $(k, p-1) = d > 1$

Domande:

① quanti sono gli elementi nell'immagine? $\boxed{\frac{p-1}{d} \quad (+1)}$

② quali sono gli elementi dell'immagine? $0 + \{b : b^{\frac{p-1}{d}} \equiv 1\}$

③ dato $b \in$ immagine, quanti sono gli a t.c. $a^k = b$? $\boxed{d}$

Oss. preliminare: $0 \in$ immagine, e solo $a = 0$ è t.c. $a^k \equiv 0$.

Primo fatto: la risposta alla ③ è la stessa $\forall\, b \neq 0$ nell'immagine.

Vediamo il caso $b = 1$. Devo risolvere $a^k \equiv 1 \ (p)$

Scrivo $a = g^\alpha \rightsquigarrow g^{k\alpha} \equiv 1 \ (p) \rightsquigarrow k\alpha =$ multiplo di $(p-1)$

Ora k e $p-1$ sono multipli di d. Scrivo

$k = Ad \qquad (p-1) = Bd \qquad$ con $(A, B) = 1$

$k\alpha = H(p-1) \leftrightsquigarrow A\cancel{d}\alpha = HB\cancel{d} \rightsquigarrow B \mid \alpha$

Come α posso scegliere un qualunque esponente multiplo di B

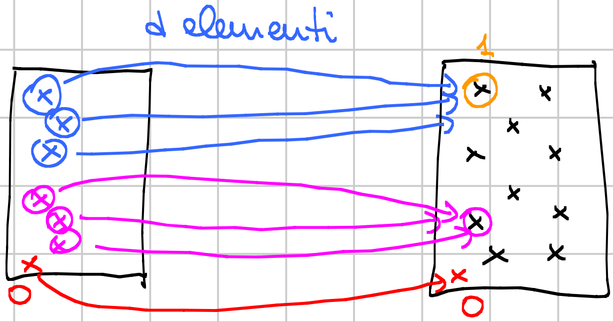
Conclusione: $a^k \equiv 1 \pmod p \iff a = g^\alpha$ con α multiplo di $\frac{p-1}{d} = B$

In tutto abbiamo d elementi !!!

—o—o—

Risolvo ora $a^k = b$ con un qualunque $b \in$ immagine, dunque con $b = c^k$

$a^k = c^k \rightsquigarrow (ac^{-1})^k \equiv 1 \rightsquigarrow ac^{-1}$ è uno dei d elementi che vanno a finire in 1, cioè $a = c \cdot$ uno dei d...



Quindi $a \to a^k$ (tolta la classe 0) è una funzione d to 1

Quanti sono gli elementi non nulli nell'immagine? Sono $\frac{p-1}{d}$

$\boxed{\text{Risposta alla domanda (2)}}$ Gli elementi nell'immagine sono tutti e soli quelli che hanno ordine che divide $\frac{p-1}{d}$

Perché? $a = g^\alpha$, quindi un elemento dell'immagine si scrive come $g^{k\alpha}$. Quale ordine può avere $g^{k\alpha}$?

$(g^{k\alpha})^n \equiv 1 \rightsquigarrow k\alpha n \equiv H(p-1) \rightsquigarrow \cancel{d}A\alpha n = H\cancel{d}B$

$\rightsquigarrow \alpha n$ è multiplo di B $\qquad n = \frac{HB}{\alpha A}$. Voglio che sia divisore di B.

Consideriamo $g^{k\alpha}$, cioè $g^{dA\alpha}$. Un esponente che di sicuro realizza

$$(g^{k\alpha})^m \equiv 1 \text{ è } m = \frac{p-1}{d}. \text{ Infatti}$$

$$(g^{k\alpha})^{\frac{p-1}{d}} = (g^{\cancel{d}A\alpha})^{\frac{p-1}{\cancel{d}}} = g^{(p-1)A\alpha} \equiv 1$$

Per la proprietà generale, tutti gli esponenti che vanno bene sono multipli dell'ordine, quindi

$\frac{p-1}{d}$ è multiplo dell'ordine.

Viceversa, se $\frac{p-1}{d}$ è multiplo dell'ordine di b, allora b sta nell'immagine.

— o — o —

Dato p, dato un divisore d di $p-1$, sappiamo che ci sono elementi di ordine d. Quanti sono?

Risposta: ci sono
* esattamente d elementi a tali che $a^d \equiv 1 \ (p)$
* di questi, esattamente $\phi(d)$ hanno ordine proprio d.

$a = g^\alpha \qquad a^d \equiv 1 \iff g^{\alpha d} \equiv 1 \iff \alpha d = H(p-1)$

$\iff \alpha = H \underbrace{\boxed{\frac{p-1}{d}}}_{\text{intero}} \iff \alpha$ è multiplo di $\frac{p-1}{d}$ (H può valere $1, 2, \dots, d$)

Questo mostra che $|\{a : a^d \equiv 1\}| = d$

Esaminiamo $\frac{p-1}{d}, \ 2\frac{p-1}{d}, \ 3\frac{p-1}{d}, \dots,$

Qual è l'ordine di un elemento del tipo $H\frac{p-1}{d}$.
Tutto dipende se $(H,d) = 1$ oppure no. Io voglio che $\frac{H}{d} \cdot M$ sia intero. Se $(H,d) = 1$ sono costretto ad usare $M = d$.
Se invece $(H,d) > 1$ posso usare un $M < d$.

LEMMA DI GUADAGNO DI UN PRIMO

Titolo nota 07/09/2009

$\boxed{\text{Sia } p \text{ un primo}}$

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

Domanda: quando a x do dei valori interi, quali sono i possibili fattori primi q che dividono $f(x)$?

Detto meglio: determinare l'insieme dei primi q per cui esiste almeno un x tale che $q \mid f(x)$.

Risposta: solo p ed i primi congrui ad 1 modulo p

Seconda domanda: come sopra con $q^2 \mid f(x)$

Risposta: tutti e soli i primi $q \equiv 1 \ (p)$.
Inoltre se $p \mid f(x)$, allora $f(x) \equiv p \pmod{p^2}$, quindi se $f(x)$ è multiplo di p, di sicuro non è multiplo di p^2.

— o — o —

Dim $\boxed{\text{Passo 1}}$

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

Supponiamo che $q \mid f(x)$. A maggior ragione $q \mid (x^p - 1)$, cioè

$$x^p \equiv 1 \pmod q$$

ma allora $\mathrm{ord}_q(x) \mid p$, ma allora

$$\mathrm{ord}_q(x) = \begin{cases} 1 \\ p \end{cases}$$

Se $\mathrm{ord}_q(x) = 1$, allora $x \equiv 1 \pmod q$, allora $f(x) \equiv p \pmod q$. Poiché $q \mid f(x)$ per forza $q = p$

Se $\mathrm{ord}_q(x) = p$, poiché in generale $\mathrm{ord}_q(x) \mid q-1$ abbiamo che $p \mid (q-1)$, cioè $q \equiv 1 \pmod p$

Riassumendo: abbiamo dimostrato che

$$q \mid f(x) \implies \begin{cases} q = p \\ q \equiv 1 \quad (p) \end{cases}$$

$\boxed{\text{Passo 2}}$ Viceversa del passo 1.

Se $q = p$, allora esiste x t.c. $q \mid f(x)$. Basta prendere $x = 1$.
Se $q \equiv 1 \pmod p$, come posso trovare x tale che $q \mid f(x)$?
Posso fare in modo che

$$q \mid x^p - 1 \qquad ?$$

Essendo p un divisore di $q-1$, esistono elementi di ordine p modulo q (lezione precedente).

$$q \mid x^p - 1 \qquad \text{cioè} \qquad q \mid (x-1) f(x)$$

Per concludere basta che $q \nmid (x-1)$, cioè $x \not\equiv 1 \quad (q)$
Basta escludere la classe 1 e si trovano x buoni.
Volendo: prendo g un generatore modulo q e definisco

$$x = g^{\frac{q-1}{p}} \qquad (\text{è diverso da } 1, \text{ e } x^p \equiv 1 \quad (q))$$

$\boxed{\text{Passo 3}}$ $q^2 \mid f(x)$: è chiaro che $q \begin{cases} = p \\ \equiv 1 \quad (p) \end{cases}$

Dimostriamo che per tutti i $q \equiv 1 \pmod p$ esiste x tale che $q^2 \mid f(x)$. Come prima facciamo in modo che

$$q^2 \mid (x^p - 1) \qquad \text{ma } q \nmid (x-1)$$

$$q^2 \mid \underbrace{(x-1)}_{\text{niente } q} \underbrace{f(x)}_{q^2 \text{ deve stare qui}}$$

Ora $q^2 \mid (x^p-1) \iff x^p \equiv 1 \quad (q^2)$

Modulo q^2 esiste il generatore (esiste mod $2, 4, \overbrace{p^\alpha, 2p^\alpha}^{p \text{ Dispari}}$)

Dato g, prendo

$$x = g^{\frac{q(q-1)}{p}}$$

Quando elevo alla p ho $x^p = g^{q(q-1)} = g^{\phi(q^2)} = 1 \quad (q^2)$

Può essere $x \equiv 1 \pmod q$? Come prima sarebbe $f(x) \equiv p \pmod q$, quindi $p = q$ che abbiamo escluso ponendo $q \equiv 1 \quad (p)$.

$\boxed{\text{Passo 3bis}}$ Stessa cosa con q^k (k esponente qualunque).

$\boxed{\text{Passo 4}}$ Resta da far vedere che $p \mid f(x) \Rightarrow f(x) \equiv p \pmod{p^2}$

Back to step 1: $p \mid f(x) \Rightarrow p \mid (x^p - 1)$

$$x^p \equiv x \pmod p \qquad x^p - 1 \equiv x - 1 \pmod p,$$

quindi $x \equiv 1 \pmod p$, quindi $x = kp+1$

$$
\begin{aligned}
f(x) &= 1 + x + x^2 + x^3 + \dots + x^{p-1} \\
&= 1 + (1+kp) + (1+kp)^2 + (1+kp)^3 + \dots + (1+kp)^{p-1} \\
&= 1 + (1+kp) + (1+2kp) + (1+3kp) + \dots \qquad + p^2 \cdot \text{ROBA} \\
&= \underset{\uparrow}{p} \qquad + kp(0 + 1 + 2 + 3 + \dots + p-1) + p^2 \cdot \text{ROBA}
\end{aligned}
$$

somma di tutti gli 1

$$= p \qquad + kp \frac{p(p-1)}{2} + \text{ROBA} \cdot p^2 \equiv p \pmod{p^2}$$

$\boxed{\text{se } p \neq 2}$

Lemma di guadagno di un primo. Consideriamo $x-1$ e $f(x)$, cioè i 2 fattori della scomposizione

$$x^p - 1 = (x-1)\, f(x)$$

Allora in $f(x)$ è presente almeno un fattore primo che non c'era in $(x-1)$, tranne nel caso

$$3^2 - 1 = \underbrace{(3-1)}_{(x-1)} \cdot \underbrace{(3+1)}_{f(x)} \qquad 9-1=8$$

In solo questo i fattori di $f(x)$ erano già tutti presenti in $x-1$.

Dim. Quali fattori primi possono stare sia in $x-1$ sia in $f(x)$? SOLO p. Se un fattore primo q sta in $x-1$ e $f(x)$, allora $x \equiv 1 \pmod q \rightsquigarrow f(x) \equiv p \pmod q \rightsquigarrow$ solito step 1.

$$\underbrace{(x-1)}_{\text{potenza di } p \,\cdot\, \text{ROBA}} \cdot \underbrace{f(x)}_{\text{potenza di } p}$$

sappiamo che $f(x) \equiv p \ (p^2)$, quindi per forza $f(x) = p$

$$\underset{p \cdot \text{ROBA}}{(x-1)} \cdot \underset{p}{f(x)}$$

In ogni caso $|x-1| \geq |f(x)|$, il che è possibile solo in pochi casi...

$$\begin{aligned} f(x) &= x^{p-1} + x^{p-2} + x^{p-3} + x^{p-3} + \dots + x^2 + x + 1 \\ &= x^{p-1} + x^{p-3}(x+1) + x^{p-5}(x+1) + \dots + (x+1) \\ &= x^{p-1} + (x+1)(x^{p-3} + x^{p-5} + \dots + 1) \end{aligned}$$

—o—o—

$\boxed{\text{IMO } 2000 - 5}$ $n \mid (2^n + 1)$ Esistono soluzioni n che contengono un numero arbitrario di primi

Soluzione piccola: $3 \mid 2^3 + 1$

$9 \mid 2^9+1 \qquad 2^9+1 = \underbrace{(2^3+1)}_{9}(2^6-2^3+1)$

$2^9+1 = 513 = 27 \cdot 19$

Supponiamo di avere un n per cui $n \mid 2^n+1$.
Proviamo con $3n$

$$\underbrace{2^{3n}+1}_{\uparrow\ \text{qui c'è } 3n} = \underbrace{(2^n+1)}_{n}\underbrace{(2^{2n}-2^n+1)}_{3} \qquad \text{quindi } 3n \mid 2^{3n}+1$$

Per il lemma di guadagno di un primo esiste un fattore primo p che sta in $2^{3n}+1$, ma mai sta in 2^n+1

Quindi oltre a $3n$ ho guadagnato la soluzione $3np$, perché

$$3np \mid 2^{3np}+1$$

$$2^{3np}+1 = \underbrace{(2^{3n}+1)}_{\uparrow \text{c'è } 3n \quad \uparrow \text{c'è } p} \cdot \text{ROBA}$$

. Sono passato da n a $3np$

Titolo nota 07/09/2009

$$\boxed{\begin{array}{l} \text{Somma potenze } k\text{-esime modulo } p \qquad p \text{ primo} \\ \displaystyle\sum_{n=1}^{p} n^k \equiv \sum_{n=1}^{p-1} n^k \equiv \ ? \pmod p \\ \text{Risposta: } ? = \begin{cases} 0 & \text{se } k \text{ non è multiplo di } p-1 \\ -1 & \text{se } k \text{ è multiplo di } p-1 \end{cases} \end{array}}$$

Caso banale: se k è multiplo di $p-1$, allora

$$1^k + 2^k + 3^k + \dots + (p-1)^k \equiv 1 + 1 + 1 + \dots + 1 \equiv p-1 \equiv -1 \ (p)$$

Casi piccoli: $k=1$ $\qquad 1+2+3+\dots+(p-1)$ $\boxed{\text{è multiplo di } p \text{ se } p>2}$

DIM 1: ACCOPPIAMENTO. Se p è dispari li accoppio (i con $p-i$)

$$\cancel{i} + p - \cancel{i} = p \qquad \text{Ogni coppia ha somma } p$$

multiplo di p

DIM. 2: FORMULA $\displaystyle\sum_{n=1}^{N} n = \frac{N(N+1)}{2}$; $\displaystyle\sum_{n=1}^{p-1} n = \frac{(p-1)p}{2}$

DIM 3: GENERATORE Sia g un generatore mod p. Allora

$$\{1,2,3,\dots,p-1\} = \{g^1, g^2, \dots, g^{p-1}\}, \text{ quindi}$$

$$\sum_{n=1}^{p-1} n \equiv \sum_{n=1}^{p-1} g^n = g + g^2 + \dots + g^{p-1} = g(1+\dots+g^{p-2})$$

formula somma progr. aritm. $\rightarrow = g\,\dfrac{\boxed{g^{p-1}-1}}{\boxed{g-1}}$

qui c'è p

Non ci sono p

$\boxed{\text{DIM 4 : SOLITA MOLTIPLICAZIONE}}$

$$\{1, 2, 3, \dots, p-1\} = \{2, 2\cdot 1, 2\cdot 3, \dots, 2\cdot(p-1)\}$$

È come dire che $x \to 2x$ è iniettiva e surgettiva mod p

$$2a \equiv 2b \iff 2(a-b) \equiv 0 \quad (p) \iff a-b \equiv 0 \quad (p) \iff a \equiv b \ (p)$$

2 è invertibile perché p è dispari

Ma allora
$$\sum_{n=1}^{p-1} n \equiv \sum_{n=1}^{p-1} 2n = 2\sum_{n=1}^{p-1} n \quad (\text{mod } p)$$

$$S \equiv 2S \quad (\text{mod } p) \implies S \equiv 0$$

[Piccolo Fermat : $\cancel{1\cdot 2\cdot 3 \cdots} (p-1) \equiv 2\,(2\cdot 2)\cdot(2\cdot 3)\cdots[2\cdot(p-1)]$
$\equiv 2^{p-1}\, \cancel{1\cdot 2\cdot 3 \cdots (p-1)}$]

—o—o—

$\boxed{\text{Caso } k=2}$ Quali dim. si riciclano

* Accoppiamento: $i^2 + (p-i)^2 \rightsquigarrow$ MALE

* Formula: $$1^2+2^2+3^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$$
$$1^2+2^2+\dots+(p-1)^2 = \frac{(p-1)p(2p-1)}{6}$$

Multiplo di p se $p \neq 2$ e $p \neq 3$

* Generatore: $$g^2+g^4+g^6+\dots+g^{2(p-1)} = g^2\,\frac{\boxed{g^{2(p-1)}-1}}{\boxed{g^2-1}}$$

p c'è

niente p se $p>3$

Formula di prima con g^2 invece di g

* Moltiplicare $\{1, 2, 3, \dots, p-1\} = \{2, 4, 6, \dots, 2(p-1)\}$

$$1^2+2^2+3^2+\dots+(p-1)^2 \equiv 2^2+2^2\cdot 2^2+2^2\cdot 3^2+\dots+2^2(p-1)^2$$
$$\equiv 2^2\left(1^2+2^2+3^2+\dots+(p-1)^2\right)$$
$$S \equiv 2^2 S \qquad \text{FUNZIONA!}$$

$\boxed{\text{Caso generale}}$ Esponente k

Accoppiamento: NO

Formula: Sì (forse si riesce a partire dalla formula ricorrente)

Generatore: --- $= g^k \dfrac{g^{k(p-1)}-1}{g^k-1}$ ← p c'è

p non c'è se k non è multiplo di p-1

Moltiplicazione:

$$S = 2^k S$$ funziona se $2^k \neq 1$ che è seccante.

Se invece di 2 uso il generatore:

$$S = g^k \cdot S$$ funziona se $g^k \neq 1$, quindi se k non è multiplo di p-1.

—o—o—

Cambia molto per k negativo?

$\boxed{k=-1}$

$$1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1} = \frac{m}{n}$$ m è multiplo di p

Fare i furbi $x \to \frac{1}{x}$ è iniettiva e surgettiva

(richiede uso border line delle frazioni modulo p)

* Accoppiamento: funziona benissimo
+ Anche moltiplicare per 2 funziona

$$1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1} = \frac{a_1+\dots+a_{p-1}}{(p-1)!}$$

a_i = prodotto di tutti meno l' i-esimo

Quando moltiplico per 2 i nuovi a_i diventano i vecchi a_i moltiplicati per 2^{p-2}. Questo si raccoglie poi si ragiona come prima.

—o—o—

Sia $P(x)$ un polinomio. Calcolo

$$\sum_{n=0}^{p-1} P(n) \equiv 0 \quad (\text{modulo } p)$$

VERO : * sempre se $\deg(P) \leq p-2$
* sempre se $P(x)$ NON contiene monomi con esponente multiplo di $(p-1)$.
* altrimenti dipende.

Se $P(x)$ è un monomio $a x^k$ è il caso precedente (se $k=0$ basta osservare che ci sono p addendi)

In generale basta raccogliere monomio per monomio.

Generalizzazione ovvia: se $a_0, a_1, \dots, a_{p-1}$ rappresentano tutte le classi modulo p, allora

$$\sum_{n=0}^{p-1} P(a_n) \equiv \sum_{n=0}^{p-1} P(n).$$

— o — o —

Trovare il + piccolo n t.c. $2009^n \equiv 1 \pmod{2^{2009}}$
Più in generale: trovare la max potenza di p che divide $a^n - 1$

Esempio: trovare la max potenza di 2 che divide $2009^n - 1$.

$\boxed{\text{Fatto 1}}$ Sia $n = 2^k \cdot d$ con d dispari. La max potenza di 2 che divide $2009^n - 1$ è uguale alla max potenza di 2 che divide $2009^{2^k} - 1$. In poche parole: d NON conta nulla

$$2009^{2^k d} - 1 = \left(2009^{2^k} - 1\right)(\text{ROBA})$$

somma di d cose DISPARI

$\boxed{\text{Fatto 2}}$ La max potenza di 2 che divide $2009^{2^{k+1}}-1$ e
1 + " " " " " " " $2009^{2^k}-1$

$$2009^{2^{k+1}}-1 = \underbrace{\left(2009^{2^k}-1\right)}_{\text{FATTORI 2 PRECEDENTI}}\boxed{\left(2009^{2^k}+1\right)}$$

è un □, quindi è $\equiv 1 \mod 4$

È $2 \pmod 4$

Quindi si guadagna un fattore 2 per volta da 1 in poi

$k=0 \quad 2009^{2^0}-1 = 2008 \rightsquigarrow 3$ fattori 2
$k=1 \quad 2009^{2^1}-1 = 2008 \cdot 2010 \rightsquigarrow 4$ fattori 2

Da qui in poi se ne guadagna 1 per volta

$$2009^{2^k \cdot d} \rightsquigarrow k+3 \text{ fattori } 2.$$

Funziona con ogni altro primo p invece di 2 purché $(p, 2009)=1$

Passi fondamentali: scrivo $n = p^k \cdot d$ dove $(d,p)=1$

→ $a^{p^k \cdot d}-1$ ha lo stesso numero di fattori p di a^{p^k}

→ $a^{p^{k+1}}-1$ ha un fattore p in più (esattamente) rispetto a a^{p^k}

$$a^{p^{k+1}}-1 = \underbrace{\left(a^{p^k}-1\right)}_{\text{fattori } p \text{ precedenti}} \cdot \underbrace{\text{roba}}_{\text{congruo a } p \text{ modulo } p^2}$$