Teoria dei Numeri 2 - Basic (ma_go)

Titolo nota 10/09/2009

<u>def</u> ϕ di Eulero.

$$\phi(n) = \#\{k \text{ intero},\ k \leq n \mid MCD(k,n)=1\}$$

<u>es</u> $\phi(1) = \#\{k \leq 1 \mid (k,1)=1\} = \#\{1\} = 1.$

$\phi(2) = \#\{k \leq 2 \mid (k,2)=1\} = \#\{1\} = 1$

$\phi(3) = \#\{1,2\} = 2$

$\phi(4) = \#\{1,3\} = 2$

$\phi(p)$, p <u>primo</u> ?

$$\{k \leq p \mid (k, p) = 1\} = \{1, \dots, p-1\}$$

$$\boxed{\phi(p) = p-1.}$$

$\phi(p^k)$? p primo

$$\{h \leq p^k \mid (h, p^k) = 1\} = \{\text{tutti}\} - \{\text{multipli di } p\} =$$

$$p^k - p^k/p = \underline{\underline{p^k - p^{k-1}}}.$$

Teorema cinese del resto.

"smontare e rimontare congruente"

$$\begin{cases} x \equiv 0 \ (m) \\ x \equiv 0 \ (n) \end{cases}$$

m, n coprimi.

$$\begin{cases} m \mid x \\ n \mid x \end{cases} \iff m \cdot n \mid x \iff x \equiv 0 \ (m \cdot n).$$

$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases} \quad ?$$

$$\begin{cases} x \equiv 3 \ (36) \\ x \equiv 12 \ (100) \end{cases} \quad ?$$

<u>NON</u> ha soluzione

dalla I x è dispari

II x è pari

$$\begin{cases} x \equiv 7 & (1001) \\ x \equiv 132 & (140) \end{cases} \quad ?$$

$$\boxed{1001 = 7 \cdot 11 \cdot 13}$$

<u>th</u> (Teorema cinese del resto)

$$\begin{cases} x \equiv a & (m) \\ x \equiv b & (n) \end{cases} \qquad (m, n) = 1$$

allora esiste ed è <u>unica</u> la classe di resto x mod $m \cdot n$ che risolve il sistema

<u>es</u>

$$\begin{cases} x \equiv 37 & (\text{mod } 257) \\ x \equiv 42 & (\text{mod } 65537) \end{cases}$$

esiste un unico intero x (unico a meno di multipli di $257 \cdot 65537$) che risolve il sistema.

<u>es 2</u> Se noi chiediamo $x \equiv 12 \ (300)$.

se sappiamo trovare $\left\{\begin{array}{l} \bar{x} \equiv 0 \quad (3) \\ \bar{x} \equiv 12 \quad (100) \end{array}\right.$ allora

intero, non classe di resto

automaticamente abbiamo trovato <u>tutti</u> gli x che soddisfano il sistema (che sono $\bar{x} + 300k$ con k intero).

dim (teorema cinese del resto)

$$(*)\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

esistono $\overline{m}$ inverso di m modulo n

[perché? perché $(m,n)=1$]

esiste $\overline{n}$ inverso di n mod m.

$$x_0 = m \cdot \overline{m} \cdot b + n \cdot \overline{n} \cdot a.$$

(intero)

x mod m?

$\equiv 0.$

$\equiv 1$ mod m $\Rightarrow \equiv a \ (m)$

$\equiv b$, perché $\overline{m} \cdot m \equiv 1$!

$\equiv 0 \Rightarrow \equiv b \ (n)$

Abbiamo trovato "esplicitamente" una soluzione! Conoscendo l'inverso mod m/n.

$$\begin{cases} y \equiv 0 \mod m \\ y \equiv 0 \mod n \end{cases} \iff y \equiv 0 \pmod{m \cdot n}.$$

$$\boxed{x - x_0 = y} \leftarrow \text{sostituzione!}$$

$$\begin{cases} x \equiv a \equiv x_0 \pmod m \\ x \equiv b \equiv x_0 \pmod n \end{cases} \leadsto \begin{cases} x - x_0 \equiv 0 \ (m) \\ x - x_0 \equiv 0 \ (n) \end{cases}$$

$$\begin{cases} y \equiv 0 & (m) \\ \quad " & (n) \end{cases} \iff \cancel{y} \equiv 0 \pmod{m \cdot n}.$$

cioè se x risolve $(*)$ $\Rightarrow$ necessariamente $x \equiv x_0 \pmod{m \cdot n}$. $\square$

mini-generalizzazione

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_N \pmod{m_N} \end{cases} \qquad (m_i, m_j) = 1 \quad (**) \quad \forall\, i \neq j.$$

ne faccio 2 alla volta!

$$\begin{cases} x \equiv b_1 \pmod{m_1 \cdot m_2} \\ \text{stesse equazioni} \end{cases}$$

$(\dots)$ = <u>INDUZIONE SU N</u>

Abbiamo "dimostrato" che il sistema $(**)$ ha un'unica soluzione mod $m_1 \cdot m_2 \cdot \ldots \cdot m_N$. $\square$

es | vogliamo dire se esistono 2009 interi consecutivi tali che il primo sia divisibile per 2^2, il secondo per 3^3, il terzo per 5^5, poi 7^7 ...

Sol Supponiamo di avere questi 2009 interi cons. $\{n, n+1, \ldots, n+2008\}$, e devono soddisf.

$$n \equiv 0 \pmod{2^2}$$

$$n+1 \equiv 0 \pmod{3^3} \ldots$$

$$\left\{ n \equiv k \pmod{p_{k+1}^{\,p_{k+1}}} \right. \qquad \forall k = 0, \dots, 2008$$

$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \dots$

$\Rightarrow$ "sistema da teorema cinese".

abbiamo moduli a due a due coprimi!

(teorema cinese!

$\Rightarrow$ esiste una soluzione. (NON esplicita) $\square$.

es 2 Prendiamo l, n, d interi positivi.

Voglio dimostrare che esiste una progressione aritmetica di lunghezza l e ragione d

tale che ogni elemento della progr. sia divisibile per una potenza n-esima.

<u>Sol</u> Prendiamo ℓ primi distinti $p_1, \dots, p_\ell$.

$$X_1 \equiv 0 \pmod{p_1^n}$$
$$X_2 \equiv 0 \pmod{p_2^n}$$
$$\vdots$$
$$X_\ell \equiv 0 \pmod{p_\ell^n}$$

$\Longleftrightarrow$

$$\begin{cases} X_1 \equiv 0 & (p_1^n) \\ X_1 \equiv -d & (p_2^n) \\ X_1 \equiv -2d & (p_3^n) \\ \vdots \\ X_1 \equiv (1-\ell)d & (p_\ell^n). \end{cases}$$

$$X_2 = X_1 + d$$
$$X_3 = X_1 + 2d$$
$$\vdots$$
$$X_\ell = X_1 + (\ell-1)d$$

$$\boxed{\text{sistema da teorema cinese}}$$

ESISTE una soluzione.

es (esercizio) Dimostrare che esistono 2010 interi consecutivi nessuno dei quali è una potenza perfetta.

---

e la ϕ?

$\phi(n) =$ quanti gli interi coprimi con n?

fattorizzo $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.

Cosa vuol dire h <u>coprimo</u> con n?

h coprimo con $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$.

h coprimo con $n \Rightarrow h \equiv a_1 \pmod{p_1^{\alpha_1}}$

con $0 < a_1 \leq p_1^{\alpha_1}$ e a_1 <u>coprimo</u> con $p_1^{\alpha_1}$.

a_2 coprimo con p_2 $\leftarrow$ $h \equiv a_2 \pmod{p_2^{\alpha_2}}$

$\vdots$

a_k coprimo con p_k $\leftarrow$ $h \equiv a_k \pmod{p_k^{\alpha_k}}$.

Se noi abbiamo h coprimo con n allora abbiamo k classi di resto (modulo i $p_i^{\alpha_i}$)

Operare col modulo.

MA ① mod p^α scoppiano contando le classi di resto invertibili

② il teorema cinese ci dice che possiamo ristabilire in modo univoco delle classi di resto mod $p_i^{\alpha_i}$ alle classi di resto mod n

$\Updownarrow$

agli interi $0 \leq \_ < n$
$1 \leq \_ \_ \leq n$

quindi ① scoppiano contando le classi di resto inv mod $p_i^{\alpha_i}$ $\boxed{p_i^{\alpha_i} - p_i^{\alpha_i - 1}}$

(2) a ciascuna scelta di k classi di resto inv ne associo una unica mod n invertibile.

Conclusione: quant'è $\phi(n)$?

abbiamo $p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$ scelte per la 1^a classe.

$p_2^{\alpha_2} - p_2^{\alpha_2 - 1}$ " " " 2^a " .

⋮

$p_k^{\alpha_k} - p_k^{\alpha_k - 1}$ " " " k^a " .

$$\phi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) =$$

$$= p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) =$$

$$= p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \left(1 - 1/p_1\right) \cdot \left(1 - 1/p_2\right) \cdot \ldots \left(1 - 1/p_k\right)$$

$$= \underline{\underline{n \left(1 - 1/p_1\right)\left(1 - 1/p_2\right) \cdots \left(1 - 1/p_k\right)}}.$$

<u>es</u>

$$120 - \frac{120}{2} - \frac{120}{3} - \frac{120}{5} + \frac{120}{6} + \frac{120}{10} + \frac{120}{15} -$$

$$- \frac{120}{30} = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right).$$

moltiplicatività

$(m, n) = 1$

$$\phi(mn) = ?$$

abbiamo k coprimo con mn $\longleftrightarrow$ k coprimo con m, k coprimo con n

$$\begin{cases} k \equiv a \pmod m & a \text{ inv.} \\ k \equiv b \pmod n & b \text{ inv.} \end{cases}$$

per lo stesso trucchetto

$\phi(m) \cdot \phi(n)$ scelte

$$\phi(mn) = \phi(m)\,\phi(n) \text{ se } (m, n) = 1$$

ϕ è moltiplicativa

$m = n = p$ primo. $\longrightarrow$ non è completamente moltiplicativa.

Cerchiamo le classi di resto mod p^2

invertibili $\quad \underline{\underline{p^2 - p}} \neq \phi(m) \cdot \phi(n) = (p-1)^2.$

FOLKLORE: $\quad n$ intero.

$$\sum_{d \mid n} \phi(d) = ?$$

$n = 1 \qquad \phi(1) = 1$

$n = 2 \qquad \phi(1) + \phi(2) = 1 + 1 = 2$

$n = 6 \qquad \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$

$n = 10 \qquad \phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$

quelle somme fa $\underline{n}$.

<u>dim</u> per induzione: sul numero di fattori primi (distinti) di $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$

- caso base: $\boxed{k = 1}$ $\qquad n = p_1^{\alpha_1} = p^{\alpha}$.

$$\sum_{d \mid n} \phi(d) = \sum_{i=0}^{\alpha} \phi(p^i) = \sum_{\ldots} p^i - p^{i-1} =$$

$$(p^{\alpha} - \cancel{p^{\alpha-1}}) + (\cancel{p^{\alpha-1}} - \cancel{p^{\alpha-2}}) + \cancel{\ldots} \cancel{+} \cancel{p} - \cancel{1} + \overset{= \phi(1).}{1} = p^{\alpha}.$$

- passo induttivo $\qquad n = p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} \qquad p_k^{\alpha_k}$

$$\sum_{d \mid n \cdot p_k^{\alpha_k}}' \phi(d) = \sum_{d', d''}' \phi(d' \cdot d'') = \sum' \phi(d') \cdot \phi(d'')$$

$$d = d' \cdot d''$$

$d' \mid n$ $\qquad$ $d'' \mid p_k^{\alpha_k}$

primi tra loro

$$= \left(\sum_{d' \mid n}' \phi(d')\right) \cdot \left(\sum_{d'' \mid p_k^{\alpha_k}}' \phi(d'')\right)$$

$\boxed{\text{per ipotesi}}$

Sappiamo calcolare entrambi i fattori

$$= n \cdot p_k^{\alpha_k}$$

$\square$

2 prendo un primo 17

$2^0, 2^1, 2^2, 2^3, \ldots$ che succede?

$1 \rightsquigarrow 2 \rightsquigarrow 4 \rightsquigarrow 8 \rightsquigarrow 16 \equiv -1 \rightsquigarrow -2 \rightsquigarrow -4 \rightsquigarrow -8 \rightsquigarrow$

$\rightsquigarrow -16 \equiv 1$

$1 \to 2 \to 4 \to 8 \to -1 \to -2 \ldots$

periodo 8.

2 mod 13

$1 \rightsquigarrow 2 \rightsquigarrow 4 \rightsquigarrow 8 \rightsquigarrow 16 \equiv 3 \rightsquigarrow 6 \rightsquigarrow 12 \equiv -1 \rightsquigarrow -2 \rightsquigarrow -4 \rightsquigarrow -8 \ldots$

$\rightsquigarrow -16 \rightsquigarrow 10 \rightsquigarrow 20 \equiv 7 \rightsquigarrow 14 \equiv 1$ e si ricomincia

con periodo $\underline{12}$.

prendiamo un intero a e un intero n $\boxed{\text{coprimo}}$ con a.

$1, a, a^2, \dots, a^k \dots$ abbiamo n classi di resto..

$1, a, a^2, \dots, a^n$ vanno infilate in n classi di resto. $\Longrightarrow \exists h \neq k$ tali che $a^k \equiv a^h \pmod{n}$

quindi da un certo punto in poi la successione delle potenze è periodica. (vero $\forall a, n$).

Se $(a, n) = 1 \Longrightarrow a$ è invertibile.

a^k è invertibile $\forall k$ (l'inverso di a^k è (l'inverso di $a)^k$).

$$a^k \equiv a^h \rightsquigarrow a^k \cdot \mathrm{inv}(a^k) \equiv a^h \cdot (\mathrm{inv}\, a^k)$$

divido per a^k

$$a^h \cdot \mathrm{inv}(a^h) \equiv 1 \mod (n)$$

$h > k$ (possiamo supporlo) $k + d = h$

$$a^h \equiv a^k$$

$$a^d \cdot \cancel{a^k} \equiv \cancel{a^k} \quad (\mathrm{mod}\ n)$$

perché sono invertibili

cioè $a^d \equiv 1 \quad (\mathrm{mod}\ n)$.

$\rightarrow$ la successione dei resti è periodica.

prendiamo il <u>minimo</u> $d>0$ tale che $a^d \equiv 1$.

allora $a^k \equiv 1 \iff k = d \cdot m$ m <u>intero</u>.

<u>def</u> d ha un nome: <u>ordine</u> (moltiplicativo)

di a modulo n: $d = \mathrm{ord}_n((a))$.

$\mathrm{ord}_{17}(2) = 8$ | visti prima.

$\mathrm{ord}_{13}(2) = 12$

<u>th</u> (Piccolo teorema di Fermat)

$a^p \equiv a \pmod p \quad \forall a$. ($p$ primo) equiv. $\quad a^{p-1} \equiv 1 \pmod p \quad \forall (a,p)=1.$

dim 1 (NOIOSA): $\quad 0^p \equiv 0 \pmod p.$

$$1^p \equiv 1 \pmod p$$

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots \binom{p}{k} \cdots + \binom{p}{1} x y^{p-1} + y^p.$$

? ? ?

sono tutti div. per p.

se $k \geq 1$, $k \leq p-1$ $\quad \binom{p}{k} = \dfrac{p!}{(p-k)!\,k!} \quad \leftarrow$ divisibile per p!

$$2^p = (1+1)^p = 1^p + \cancel{\underset{\equiv 0}{\binom{p}{1}}\cdot 1^{p-1}\cdot 1} + \cancel{\underset{\equiv 0}{\dots}} + \cancel{\underset{\equiv 0}{\binom{p}{p-1}}\, 1\cdot 1^{p-1}} + 1^{p} \equiv 2$$

$$(n+1)^p \overset{?}{\equiv} n+1$$

$\hookrightarrow$ $n^p + 1^p \equiv n+1$ (per induzione). $\square$

<u>dim 2</u> (!!!). <u>Contiamo</u> le collane di p perle di a colori.

Se apriamo le collane: a^p scelte.

Se chiudiamo abbiamo 2 possibilità.

(M) la collana è <u>monocromatica</u>: a possibilità

(N) " " non è " : $a^p - a$ (aperte).

ad ogni collana non monocromatica chiusa corrispondono p collane n.m. aperte

$$\frac{a^p - a}{p} \quad \text{collane NON monocr. chiuse.}$$

$\downarrow$

intero $\Rightarrow p \mid a^p - a$

$$a^p \equiv a \pmod p \qquad \square \; !!!$$

<u>ordine moltiplicativo</u>: $a^k \equiv 1 \pmod{n}$

allora k è un multiplo di $\mathrm{ord}_n(a)$.

$n = p$ primo. $a^k \equiv 1 \pmod{p}$

abbiamo appena scoperto $a^{p-1} \equiv 1 \pmod{p}$

$$\boxed{\mathrm{ord}_p(a) \mid p-1}$$

$\mathrm{ord}_{17}\, 2 = 8 \mid 16 = 17 - 1$

$\mathrm{ord}_{13}\, 2 = 12 \mid 13 - 1$

(becco <u>tutte</u> le classi di resto $\neq 0$)

es $\underbrace{111\ldots111}_{n \text{ cifre}} = A_n$ per ogni $p \neq 2, 5$ esiste un numero della forma divisibile per p.

Sol (non costruttiva) $9 \cdot A_n = 99\ldots99$

$$9 \cdot A_n + 1 = 10^n \qquad A_n = \frac{10^n - 1}{9}.$$

$p = 3$ (111 funziona).

$p \neq 2, 3, 5$ 10 è coprimo con p.
9 è coprimo con p.
$\downarrow$
9 invertibile

$$A_n \equiv (10^n - 1)\cdot(\text{inverso di } 9) \pmod p.$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \overset{\shortparallel}{a}$$

$n = p-1$? che succede ?

succede che $A_{p-1} \equiv (\underset{\substack{|||\\ 1}}{10^{p-1}} - 1)\cdot a \equiv 0$ mod p.

per Fermat!

cioè $p \mid A_{p-1}$. $\square$

es 2 $37 \overset{?}{\mid} 2^{17} - 1$?

Sappiamo che $2^{36} \equiv 1 \pmod{37}$

$\mathrm{ord}_{37} 2 \mid 36$

se $37 \mid 2^{17} - 1$ otteniamo $2^{17} \equiv 1 \pmod p$

cioè $\mathrm{ord}_{37} 2 \mid 17 \Rightarrow \mathrm{ord}_{37} 2 = 1$

$2^1 \equiv 1 \ (37)$ NO!

$37 \nmid 2^{17} - 1$!! $\square$

ES $1432^{1432} \pmod{1001}$?

$1001 = 7 \cdot 11 \cdot 13$.

per sapere quanto fa basta sapere

$$1432^{1432} \mod 7,\ 11,\ 13.$$

$6 = 7-1$

mod 7) $1432^{1432} \equiv 4^{1432} \equiv 4^{6k+r} \equiv 4^{r} \equiv$

$$4^4 \equiv (4^2)^2 \equiv 2^2 \equiv 4$$

mod 11) $1432^{1432} \equiv 2^{1432} \equiv 2^{2} \equiv 4$

mod 13) $1432^{1432} \equiv 2^{1432} \equiv 2^{4} \equiv 16 \equiv 3$

$$\begin{cases} x \equiv 4 & (7) \\ x \equiv 4 & (11) \\ x \equiv 3 & (13) \end{cases} \quad x \equiv 4 \pmod{77}.$$

"D"

es Dimostrare che $p^p - 1$ ha almeno un fattore primo della forma $kp+1$.

Sol Prendiamo un primo $q \mid p^p - 1$.

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

A) $\mathrm{ord}_q\, p \mid p \longrightarrow$ o $\mathrm{ord} = 1$
o $\mathrm{ord} = p$

B) $\mathrm{ord}_q\, p \mid q-1$

se $\mathrm{ord}_q\, p = 1$ $\qquad p \equiv 1 \pmod q$

cioè $\qquad q \mid p-1$

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

$p-1$: div. per q

$p^{p-1}+p^{p-2}+\dots+p+1$: **Non** div. per q!!

$$p^{p-1}+p^{p-2}+\dots+p+1 \equiv 1+1+\dots+1+1 \pmod q$$

$$\equiv p \pmod q.$$

Se prendiamo un fattore primo q del secondo fattore d'avan. $\mathrm{ord}_q(p) = p$.

$$p = \mathrm{ord}_q(p) \mid q-1$$

$$q = pk+1 \qquad \square$$

$$\phi(p) \overset{?}{=} p-1$$

p.t.F: $a^{\phi(p)} \equiv 1 \pmod p$ $\pi(a,p)=1$.

gen. $(a,m)=1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$.

in altri termini $\mathrm{ord}_m a \mid \phi(m)$.

es $N = 5^{5^{5^{5^5}}}$: quali sono le ultime 5 cifre di quella bestia?

sol dobbiamo trovare la classe di resto di N modulo $10^5 = 5^5 \cdot 2^5$.

$\boxed{\text{Cinese}}$. ci basta sapere cosa fa $N \bmod 2^5$
$N \bmod 5^5$

Gratis: $N \equiv 0 \pmod{5^5}$.

Non-gratis. $N \bmod (2^5)$

$N = 5^{(5^{5^{5^5}})} \bmod 32$ ci serve sapere quanto fa

$5^{5^{5^5}}$ $\bmod \phi(32) = \bmod 16$

5^{5^5} $\bmod 8 (= \phi(16))$

5^5 $\bmod 4$
$\equiv$
1 $\bmod 4$ $\Big\} \equiv 1 \bmod 4$

$5^{5^5} \equiv 5^1 \pmod 8$

$$5^{5^{5^5}} \equiv 5^5 \pmod{16}$$

$$5^2 \cdot 5^2 \cdot 5 \equiv 9 \cdot 9 \cdot 5 \equiv 9 \cdot -3 \equiv -27 \equiv$$
$$\equiv 5 \pmod{16}$$

$$N = 5^{5^{5^{5^5}}} \equiv 5^5 \pmod{32} \equiv 25 \cdot 125 \equiv -3 \cdot 25 \equiv$$
$$\equiv -75 \equiv 21 \pmod{32}.$$

cioè dobbiamo risolvere
$$\begin{cases} X \equiv 21 \pmod{32} \\ X \equiv 0 \pmod{5^5} \end{cases}$$

$\square$

Fissato p è un primo

es Dimostrare che esistono infiniti n

tali che $2^n \equiv n \pmod{p}$.

$p \mid 2^n - n$.

$$\begin{cases} n \equiv 1 \pmod{p} \\ 2^n \equiv 1 \pmod{p} \end{cases}$$ ci basta $n \equiv 0 \pmod{p-1}$

$$\begin{cases} n \equiv 0 \pmod{p-1} \\ n \equiv 1 \pmod{p} \end{cases}$$

coprimi perché la diff. è 1!

ha soluzione unica mod $p(p-1)$

se n_0 è una soluzione anche $n_0 + kp(p-1)$ lo
è $\forall k$.

Residui quadratici / cubici / ~~k~~-esimi mod p.

quanti e quali sono i residui quadratici
mod p?

a classe di resto $\neq 0$ mod p.

$a^2 \equiv b^2 \pmod p$ allora vuol dire che

$a^2 - b^2 \equiv 0 \pmod p \Rightarrow (a-b)(a+b) \equiv 0 \ (p)$

o $(a-b) \equiv 0 \ (p)$ o $(a+b) \equiv 0 \pmod p$

o $a \equiv b \pmod p$ o $a \equiv -b \pmod p$.

$a \equiv \pm b \pmod p$ è chiaro che $a^2 \equiv b^2 \ (p)$

$$
\begin{array}{cccccc}
 & 1 & 2 & 3 & \dots & \frac{p-1}{2} \\
0 & p-1 & p-2 & p-3 & \dots \quad \frac{p+3}{2} & \frac{p+1}{2}
\end{array}
$$

stessa classe di resto

idem

stessa classe di resto

due classi diverse hanno quadrati diversi

quindi i residui quadratici (cioè le classi di resto dei quadrati) mod p sono

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

$p > 2$

$\boxed{p>2}$

prendiamo la classe di resto di a^2.

$$(a^2)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

oss i residui quadratici $\neq 0$ sono radici dell'equazione

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

$\downarrow$

ha al più $\frac{p-1}{2}$ radici e gliene abbiamo trovate $\frac{p-1}{2}$, quindi i residui quadratici sono **tutte** le radici di $x^{\frac{p-1}{2}} - 1$.

In altri termini, se avete una classe di resto a e volete controllare se è un residuo quadratico ne fate la potenza $\frac{p-1}{2}$.

$$x = a^{\frac{p-1}{2}} \equiv ?$$

$$x^2 \equiv 1 \pmod p$$
$$\Downarrow$$
$$x \equiv \pm 1 \pmod p.$$

$\boxed{\text{Criterio di Eulero}}$ x è un residuo quadratico mod $p \iff x^{\frac{p-1}{2}} \equiv 1 \pmod p$.

$$\mathrm{ord}_{13} 2 = 12 \implies 2^{6 = \frac{p-1}{2}} \not\equiv 1$$ quindi 2 <u>non</u> è un residuo quadratico mod 13.

$\mathrm{ord}_{17} 2 = 8 \Rightarrow 2^8 \equiv 1 \Rightarrow 2$ $\underline{\underline{\text{è}}}$ un

residuo quadratico mod 17. $6^2 = 36 \equiv 2 \pmod{17}$

<u>es</u> Per quali p $\quad -1$ è un residuo quadratico?

$$(-1)^{\frac{p-1}{2}} \quad \begin{cases} p-1 \text{ è div. per } 4 \Rightarrow \text{sì!} \\ p-1 \ \underline{\text{non}} \text{ è div per } 4 \Rightarrow \text{No! } (p>2) \end{cases}$$

<u>es</u> • 3 $\quad -1$ non è residuo quadratico mod 3:

$$0^2 = 0$$

$$(\pm 1)^2 \equiv +1 \not\equiv -1 \pmod 3$$

• 5 $\quad 2^2 \equiv 4 \equiv -1 \pmod 5$.

• 7 $\quad 0^2 \equiv 0, \ (\pm 1)^2 \equiv 1, \ (\pm 2)^2 \equiv 4, \ (\pm 3)^2 \equiv 2 \ldots$

es $p \mid a^2+b^2$ con almeno uno tra a e b non divisibile per p.

Allora p è della forma $4k+1$.

Supp. che $a \not\equiv 0 \mod p$. $\Rightarrow a$ inv. mod p
$c \cdot a \equiv 1 \pmod p$.

$$a^2+b^2 \equiv 0 \pmod p$$

$$\underbrace{c^2 \cdot a^2}_{\substack{\shortparallel \\ 1}} + (cb)^2 \equiv 0 \pmod p$$

$$\Downarrow$$

$(cb)^2 \equiv -1 \pmod p$ cioè -1 residuo quadratico mod p.

Quindi $p \equiv 1 \mod 4$. $p = 4k+1$.

$\forall\, p = 4k+1 \quad \exists\, a, b$ t.c. $\quad p \mid a^2 + b^2$.

esiste a tale che $\quad a^2 \equiv -1 \pmod p$.

$$a^2 + 1^2 \equiv -1 + 1 \equiv 0 \pmod p.$$

se $\quad a < p \implies a^2 + 1 < p^2$, cioè $p \,\|\, a^2 + b^2$

Quindi $\boxed{\exists\, a, b \text{ t.c. } p \,\|\, a^2 + b^2 \iff p \equiv 1 \pmod 4}$.

<u>th</u> $\quad \forall p$ primo esiste g classe di resto mod p tale che $\quad \mathrm{ord}_p\, g = p - 1$.

<u>def</u> $\quad g$ si chiama <u>generatore</u> mod p.

<u>oss</u> i residui quadratici sono g^{2k} per $k = 0, \dots, \frac{p-1}{2}$.

+ lo 0.

<u>th</u> esiste un generatore mod m se e solo se

$$m \in \{2, 4, p^k, 2p^k\}$$

primo dispari.

<u>es</u> Quanti sono i generatori mod p?

<u>sol</u> g^h tali che $\operatorname{ord} g^h = p-1$

se $(h, p-1) = d > 1$, allora $h = d \cdot h'$

$$\left(g^h\right)^{\frac{p-1}{d}} \equiv 1 \pmod p$$

$$\| $$

$$g^{\cancel{d}\cdot h' \cdot \frac{p-1}{\cancel{d}}} \equiv \left(g^{p-1}\right)^{h} \equiv 1 \pmod p.$$

se $d = (h, p-1) = 1$?

Succede che h è invertibile $(\text{mod } p-1)$!

Cioè esiste un ℓ tale che $h\ell \equiv 1 \pmod{p-1}$

$$\left(g^h\right)^{\ell} = g^{h\ell} = g^{(p-1)\cdot \text{intero} + 1} \equiv \cancel{\left(g^{p-1}\right)^{\text{intero}}} \cdot g \equiv$$

$$g \pmod p.$$

Se vogliamo ottenere g^k, facciamo $\left(g^h\right)^{\ell k} \equiv$

$$\equiv \left(g^{hl}\right)^k \equiv g^k \pmod{p}.$$

<u>Concludendo</u>: tutti i generatori sono della forma g^h con $(h, p-1) = 1$.

$\phi(p-1)$.

$\longrightarrow$ in generale, se c'è un generatore ce ne sono $\phi(\phi(m))$.

$\square$

<u>es</u> $D = \{ n \in \mathbb{N} \mid n \mid 2^n + 1 \}$

- troviamo i primi in D.

sol. $p \in D$ - $2^p + 1 \equiv 0 \pmod p$.

$2^p \equiv -1 \pmod p$

$2^{2p} \equiv 1 \pmod p$ aoi

$\mathrm{ord}_p 2 \mid 2p$

$\mathrm{ord}_p 2 \mid p-1$

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

due cai: $\mathrm{ord}_p 2 = 1$ $\quad 2 \equiv 1 \pmod p$ $\boxed{\text{imp}}$

$\mathrm{ord}_p 2 = 2$ $\quad 2^2 \equiv 1 \pmod p$

$4 \equiv 1 \pmod p \Rightarrow p = 3$.

$$\boxed{2^3+1=9} \quad \text{ok.} \qquad \mathbb{P}^{\text{primi}} \cap D = \{3\}.$$

- trovando le potenze dei primi in D.

$$2^{p^k}+1 \equiv 0 \pmod{p^k}.$$

$$\equiv 0 \pmod{p}$$

$$2^{p^k} \equiv 2 \quad (\text{per fermat + induzione})$$

$$2+1 \equiv 0 \pmod{p} \Rightarrow p=3.$$

si dimostra per induzione che $3^k \mid 2^{3^k}+1 \ \forall k$.

$$\left(2^{3^k}+1\right) = \left(2^{3^{k-1}}+1\right) \cdot \left(2^{2 \cdot 3^{k-1}} - 2^{3^{k-1}} + 1\right)$$

$A = 2^{3^{k-1}}$ $\qquad = A^3 + 1 = (A+1)(A^2 - A + 1)$

Per ipotesi induttiva $(A+1)$ è multiplo di 3^{k-1}.

il fattore a dx è $A^2 - A + 1$

A è coprimo con 3. Quindi $A^2 \equiv 1 \pmod 3$

$A \equiv -1 \pmod 3$ $\qquad A = 2^{3^{k-1}} = (-1)^{\text{dispari}} \equiv -1 \, (m)$

$A^2 - A + 1 \equiv 0 \; (3)$

$(A+1)(A^2 - A + 1)$ ha guadagnato un fattore 3 rispetto ad $A+1$.

Abbiamo dimostrato $3^{k+1} \mid 2^{3^k} + 1$.

- trovare i prodotti di due primi in D.

oss se $n \in D$, allora $3 \mid n$.

dim oss p.p.p. = più piccolo primo.

prendiamo il p.p.p. che divide n.

$$2^n + 1 \equiv 0 \pmod p.$$

Siccome $2^n \equiv -1 \pmod n$, allora

$$\boxed{2^{2n} \equiv 1} \pmod n \Rightarrow \mathrm{ord}_p 2 \mid 2n$$

$$\left.\begin{array}{l} \mathrm{ord}_p\, 2 \mid 2n \\ \mathrm{ord}_p\, 2 \mid p-1 \end{array}\right\} \Rightarrow \begin{array}{c} \mathrm{ord}_p\, 2 \\ \parallel \\ 2 \end{array} \mid 2 .$$