Teoria dei Numeri 2 - BASIC

DARKCRYSTAL

Titolo nota 08/09/2010

$$\begin{cases} x \equiv 0 \ (m_1) \\ x \equiv 0 \ (m_2) \end{cases}, \qquad (m_1, m_2) = 1$$

$$m_1 \mid x, \quad m_2 \mid x \implies m_1 m_2 \mid x$$

$$x \equiv 0 \ (m_1 \cdot m_2) \qquad\qquad a \equiv b \ (m_1 \cdot m_2)$$

$$\Updownarrow$$

$$m_1 \cdot m_2 \mid a - b$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad e \quad (m_1, m_2) = 1$$

$$\Updownarrow$$

$$x \equiv a \pmod{m_1 \cdot m_2}$$

$$x = a + k \cdot m_1 \cdot m_2$$

Teorema Cinese del Resto

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad e \quad (m_1, m_2) = 1$$

$$x = a_1 + h m_1, \qquad x = a_2 + k \cdot m_2$$

$$a_1 + h m_1 = a_2 + k \cdot m_2$$

$$a_1 - a_2 = k \cdot m_2 - h \cdot m_1 \qquad (A)$$

$$c \cdot m_2 - d \cdot m_1 = 1 \qquad \text{(Bézout)}$$

$$c \cdot (a_1 - a_2), \quad d \cdot (a_1 - a_2)$$

(k_0, h_0) soluz di ⊛

$$k = k_0 + \overline{x}, \qquad h = h_0 + y$$

$$m_2 \cdot \overline{x} - m_1 \cdot y = 0 \rightarrow m_2 \mid y, \quad m_1 \mid \overline{x}$$

$$x = \underbrace{a_1 + m_1 h_0} + \underbrace{m_1 y}_{\text{divisibile per } m_1 \cdot m_2}$$

Come trovo esplicit. le soluz?

$$\begin{cases} x \equiv a_1 & (m_1) \\ x \equiv a_2 & (m_2) \end{cases} \qquad x = A \cdot m_1 + B m_2$$

$$\begin{cases} \cancel{A \cdot m_1} + B m_2 \equiv a_1 & (m_1) \\ A \cdot m_1 + \cancel{B \cdot m_2} \equiv a_2 & (m_2) \end{cases} \qquad B \equiv m_2^{-1} \cdot a_1 \ (m_1)$$

$$\begin{cases} x \equiv 3 & (7) \\ x \equiv 2 & (5) \end{cases} \qquad x = 7A + 5B$$

$$\Updownarrow$$

$$x \equiv 17 \quad (35) \qquad \begin{cases} 5B \equiv 3 & (7) \\ 7A \equiv 2 & (5) \end{cases} \qquad \begin{cases} B \equiv 9 \equiv 2 \ (7) \\ A \equiv 1 \ (5) \end{cases}$$

$$x = 7 + 10 = 17$$

B è scelto a meno di multipli di 7,
5B a meno di multipli di 35.

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \vdots \\ x \equiv a_n \ (m_n) \end{cases}$$

$x \equiv a_1 \ (m_1),\ x \equiv a_2 \ (m_2) \rightarrow x \equiv b_1 \ (m_1 \cdot m_2)$

con gli m a due a due coprimi.

$$\Updownarrow$$

$$x \equiv a \quad (m_1 \cdot m_2 \cdot \ldots \cdot m_n)$$

$$x = A\, m_2 m_3 \ldots m_n + B\, m_1 m_3 \ldots m_n + \ldots$$

$$\begin{cases} x \equiv 5 \ (20) \\ x \equiv 6 \ (30) \end{cases} \xrightarrow{TCR} \begin{cases} x \equiv 0 \ (5) \\ x \equiv 1 \ (4) \\ x \equiv 0 \ (2) \\ x \equiv 0 \ (3) \\ x \equiv 1 \ (5) \end{cases}$$

IMPOSSIBILE

$$\begin{cases} x \equiv 4 \ (20) \\ x \equiv 14 \ (30) \end{cases} \xrightarrow{TCR} \begin{cases} x \equiv 0 \ (4) \\ x \equiv 4 \ (5) \\ \cancel{x \equiv 0 \ (2)} \\ x \equiv 2 \ (3) \\ \cancel{x \equiv 4 \ (5)} \end{cases} \Leftrightarrow x \equiv 44 \ (60)$$

Esercizi

1) Esistono 2010 interi consecutivi di cui il primo è divis. per 2^2, il secondo $\equiv 0 \ (3^3)$, il terzo $\equiv 0 \ (5^5)$, ...

$$\begin{cases} n \equiv 0 \ (4) \\ n+1 \equiv 0 \ (3^3) \\ n+2 \equiv 0 \ (5^5) \\ \vdots \end{cases} \Leftrightarrow \begin{cases} n \equiv 0 \ (2^2) \\ n \equiv -1 \ (3^3) \\ \vdots \end{cases}$$

Il TCR dice che $\exists$ una soluz., ed è unica mod $2^2 \cdot 3^3 \cdot 5^5 \cdot 7^7 \cdot \ldots$

2) Esistono 2010 interi consec. di cui esattam. 1 è una potenza perfetta.

Supponiamo che $n, n+1, \ldots, n+2009$ che NON sono potenze perfette. $\exists$ il più piccolo intero $m > n+2009$ che è una potenza perfetta.
Ma allora $\underbrace{n, n+1, \ldots, m}_{\text{più di } 2010}$ di cui esatt. 1 è potenza. Scelgo gli ultimi 2010.

Se x è una pot. perfetta, $x \not\equiv p \ (p^2)$ per ogni scelta di p primo.

Se $x \equiv p \ (p^2) \longrightarrow x \equiv p \ (p) \to p \mid x$.

Allora $p^2 \mid x$, cioè $x \equiv 0 \ (p^2)$.

Scegliamo $p_1, p_2, \ldots, p_{2010}$ primi distinti

$$\begin{cases} x \equiv p_1 \ (p_1^2) \\ x+1 \equiv p_2 \ (p_2^2) \\ x+2 \equiv p_3 \ (p_3^2) \\ \vdots \end{cases} \xrightarrow{\text{TCR}} \exists \text{ una soluz. } x$$

3) Esiste una progress. aritmetica di lunghezza l, ragione d t.c. ogni elemento e' divisibile per almeno una potenza n-esima

---

φ di Eulero

$$\varphi(n) = \left| \{0 < m \leq n : (m, n) = 1\} \right|$$

$\varphi(1) = 1$. $n = p$ primo? $\varphi(p) = p - 1$

$$\varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p-1) \qquad k \geq 1$$

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$$

$$(m, n) = 1 \longrightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

$$\varphi(\underbrace{p_1^{\alpha_1}} \cdot \underbrace{\ldots \cdot p_k^{\alpha_k}}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) =$$

$$= \ldots = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$$

$$\varphi(40) = \varphi(5) \cdot \varphi(8) = 4 \cdot 2^2 = 16$$

Funzione moltiplicativa $(m, n) = 1 \rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$

Funz. completam. moltipl. $f(mn) = f(m) \cdot f(n)$

$$6 = \varphi(9) \neq \varphi(3) \cdot \varphi(3) = 2 \cdot 2$$

$$X \equiv a \pmod{n \cdot m} \xleftrightarrow{\text{TCR}} \begin{cases} X \equiv a \ (m) \\ X \equiv a \ (n) \end{cases}$$

Se $1 = (a, m \cdot n)$, allora i rappr. priv. $\uparrow$ saranno coprimi con m, n

$$X \equiv 4 \ (15) \longrightarrow \begin{cases} X \equiv 1 \ (3) \\ X \equiv 4 \ (5) \end{cases}$$

$$\begin{cases} X \equiv a_1 \ (m) \\ X \equiv a_2 \ (n) \end{cases} \longrightarrow X \equiv a \ (m \cdot n)$$

Bigezione tra $\varphi(m \cdot n)$ e i sistemi $\begin{cases} X \equiv a_1 \ (m) \\ X \equiv a_2 \ (n) \end{cases}$

con $(a_1, m) = 1$, $(a_2, n) = 1$, $0 \leq a_1 < m$, $0 \leq a_2 < n$

$$\varphi(m) \cdot \varphi(n) = \varphi(m \cdot n)$$

$$\varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) =$$

$$= \underbrace{p_1^{\alpha_1 - 1}}(p_1 - 1) \cdot \underbrace{p_2^{\alpha_2 - 1}}(p_2 - 1) \cdot \ldots \cdot \underbrace{p_k^{\alpha_k - 1}}(p_k - 1)$$

$$= n \left(\frac{p_1 - 1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

φ di Eulero /2

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_k} +$$

$$+ \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \ldots - \sum \frac{n}{p_i p_j p_k} + \sum \frac{n}{p_i p_j p_k p_l} \ldots$$

(Principio Incl - Esclus.)

$$= n \underbrace{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)}$$

$$\varphi(m \cdot n) = m \underbrace{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)}\cdots \cdot$$

$$\cdot\, n \underbrace{\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_k}\right)}$$

$$= \varphi(m) \cdot \varphi(n)$$

$$\sum_{d|n} \varphi(d) = n$$

$n = p^m$
$$\sum_{k=0}^{m} \varphi(p^k) = \varphi(1) + \sum_{k=1}^{m} (p-1)p^{k-1} =$$

$$= 1 + (p-1)\left(1 + p + p^2 + \dots + p^{m-1}\right) =$$

$$= 1 + \cancel{(p-1)}\,\frac{p^m - 1}{\cancel{p-1}} = p^m = n$$

$$g(n) = \sum_{d|n} \varphi(d)$$ Hope: è moltiplicativa?

$g(p^k) = p^k$

$$g(n) = g(p_1^{\alpha_1}) \cdot \dots \cdot g(p_k^{\alpha_k}) =$$

$$= p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} = n$$

$(m, n) = 1 \qquad g(m \cdot n) = \sum_{d \mid m \cdot n} \varphi(d) =$

$$= \sum_{\substack{a \cdot b \mid m \cdot n \\ a \mid m \\ b \mid n}} \varphi(ab) = \sum_{a,b} \varphi(a)\varphi(b) =$$

$$= \sum_{a \mid m} \left[\sum_{b \mid n} \varphi(a)\, \varphi(b) \right] =$$

$$= \sum_{a \mid m} \left(\varphi(a) \underbrace{\sum_{b \mid n} \varphi(b)}_{} \right) = \left(\sum_{b \mid n} \varphi(b) \right) \left(\sum_{a \mid m} \varphi(a) \right) =$$

$$= g(m)\, g(n)$$

Struttura moltiplicativa mod m

$a^n \quad \text{mod } m$

$a^0, a^1, a^2, \dots, a^m, a^{m+1} \rightarrow$ periodica per pigeonhole

$a^k \equiv a^h \pmod m$

$2 = a, \quad \text{mod } 12$

$2, \underbrace{4, 8}, \underbrace{4, 8}, \dots$

1) Non ha un ordine : $\boxed{a^k \not\equiv 1 \ (12)}$

2) Non è periodica.

$$a^n \text{ mod } m \longleftrightarrow \begin{cases} a^n & \text{mod } 4 \\ a^n & \text{mod } 3 \end{cases}$$

$1, 2, 0, 0, \dots, 0$

Per quali a $\exists$ k t.c. $a^k \equiv 1 \pmod m$?

Per gli a t.c. $(a, m) = 1$

$a^k = 1 + h \cdot m$

Supponiamo che $(a, m) > 1$. Allora esiste $p | a$, $p | m$. Allora $p \mid a^k - h \cdot m = 1$

Viceversa, se $(a, m) = 1$, allora $a^h \equiv a^k \pmod m$

$h < k \rightarrow \underbrace{(a^{-1})^h a^h}_{\equiv 1} \equiv a^{k-h} \pmod m$

FLT (primi): $(a, p) = 1 \quad a^{p-1} \equiv 1 \ (p)$

Teorema di Eulero-Fermat Se $(a, m) = 1$, allora

$$a^{\varphi(m)} \equiv 1 \pmod m$$

$$\{1, a_2, a_3, \dots, a_{\varphi(m)}\} = A$$

mod 8: $\{1, 3, 5, 7\}$

$$\{1x, a_2 x, a_3 x, \dots, a_{\varphi(m)} x\} = B \quad \text{se } (x, m) = 1$$

$$a_h x \equiv a_k x \pmod m \rightarrow a_h \equiv a_k \ (m)$$

$$\underbrace{1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_{\varphi(m)}}_{Z} \equiv (1x)(a_2 x) \dots (a_{\varphi(m)} x) \quad (m)$$

$$Z \equiv Z \cdot x^{\varphi(m)} \pmod m$$

$$1 \equiv x^{\varphi(m)} \pmod m$$

Def $\mathrm{ord}_m(x)$ = min. intero positivo k t.c. $x^k \equiv 1 \pmod m$

$$\boxed{ord_m(x) \mid \varphi(m)}$$

$$ord_m(x) \leq \varphi(m) \leq m$$

Generatori Un generatore mod m e' un g t.c. $ord_m(g) = \varphi(m)$

$\underbrace{g^1, g^2, \dots, g^{\varphi(m)}}_{\varphi(m) \text{ residui}}$ sono tutti distinti

$\varphi(m)$ residui coprimi con m

Mod 5   2, 4, 3, 1   generatore!

4, 1   NO

Teo Esiste un generatore se e solo se m e' uno tra $2, 4, p^n, 2p^n$ con p primo dispari

Mod 8 non esiste un generatore, perché

$$a^2 \equiv 1 \pmod 8 \qquad (a, 2) = 1$$

Se g fosse gener. mod 16, g^k genererebbe tutto mod 16 $\Rightarrow$ genererebbe tutto mod 8

Generatori mod p. $\mathrm{ord}(g) = p-1$.

$$g^{p-1} \equiv 1 \ (p) \qquad \text{(inutile)}$$

$$\mathrm{ord}_p(g) \mid p-1. \qquad g^m \not\equiv 1 \ (p) \ \text{ se } m < p-1$$

$$p-1 = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$$

$$q_1^{\beta_1} \cdot \ldots \cdot q_k^{\beta_k} \quad \text{con almeno } 1 \ \beta < \alpha.$$

Basta provare che $g^{\frac{p-1}{q}} \not\equiv 1 \ (p)$, per $q \mid p-1$.

$$p = 19, \qquad p-1 = 18 \qquad g^{18} \equiv 1 \ (19)$$

$$1, 2, 3, 6, 9, 18 \qquad \frac{18}{9} \qquad \frac{18}{3}$$

Sia g gener. mod p. Allora

- o g o $g+p$ e' generatore mod p^2
- se h e' gener. mod p^2, allora e' generatore mod p^n per ogni n (p disp)

. $\mathrm{ord}_p \, g = p-1 \qquad g^{p-1} = 1 + kp$

Gener. mod p^2 ha ordine $\varphi(p^2) = p(p-1)$

$$\mathrm{ord}_{p^2}(g) \qquad g^h \equiv 1 \ (p^2) \rightarrow g^h \equiv 1 \ (p)$$

$p-1$

$\shortparallel$

$$\mathrm{ord}_p \, g \mid \mathrm{ord}_{p^2}(g) \mid p \cdot (p-1) = \varphi(p^2)$$

$$\mathrm{ord}_{p^2}(g) \begin{cases} \to p-1 & (1) \\ \to p\cdot(p-1) & \underline{\text{OK}} \end{cases}$$

(1) $g^{p-1} \equiv 1 \ (p^2) \longrightarrow g^{p-1} = 1 + h\cdot p^2$

$(g+p) \equiv g \ (p)$, $g+p$ e' un gen mod p

$\to p-1 \mid \mathrm{ord}_{p^2}(g+p) \mid p(p-1)$

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

$$= 1 - p\cdot g^{p-2} + \cancel{p^2(\dots)}$$

$$\not\equiv 1 \quad (p^2)$$

$p\cdot g^{p-2} \not\equiv 0 \ (p^2)$

$\mathrm{ord}_{p^2}(g+p)$ e' $p(p-1)$, cioe' $g+p$ genera

Quando è che -1 è un residuo quadrat? $(\text{mod } p)$

$\iff$ esiste a che risolve $a^2 \equiv -1 \ (p)$

$\Longrightarrow \quad a^4 \equiv 1 \ (p) \qquad \text{ord}_p(a) = 4$

$\text{ord} = 4 \mid \varphi(p) = p-1 \implies p \equiv 1 \ (4)$

(NECESS.)

Sia $p \equiv 1 \ (4)$ e sia g un gener.

$$a = g^{\frac{p-1}{4}} \qquad a^4 \equiv g^{p-1} \equiv 1 \ (p)$$

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

$$\downarrow$$

$$(a^2-1)(a^2+1) \equiv 0 \ (p) \rightarrow a^2+1 \equiv 0 \ (p)$$

$$\rightarrow a^2 \equiv -1 \ (p)$$

Quanti sono i generatori?

Tutti i residui si scrivono $g, g^2, g^3, \dots, g^{p-1}$

g^k è ancora un generatore?

Sia $a = \text{ord}_p(g^k)$. $\quad g^{ak} \equiv 1 \ (p)$

$\iff p-1 \mid ak$. Se $(k, p-1) = 1$,

allora $\searrow p-1 \mid a \mid p-1 \implies a = p-1$

g^k è ancora generatore se $\boxed{(k, p-1) = 1}$

Se invece $(k, p-1) = b > 1$, allora

$$\left(g^k\right)^{\frac{p-1}{b}} \equiv g^{(k/b)\cdot(p-1)} \equiv 1 \quad (p)$$

ma $\frac{p-1}{b} < p-1$

I generatori sono $\varphi(p-1) = \varphi(\varphi(p))$.

Esercizi

1) È vero che $37 \mid 2^{17} - 1$?

Se fosse vero, $2^{17} \equiv 1 \quad (37)$

$2^{36} \equiv 1 \quad (37)$

$\mathrm{ord}_{37}(2) \mid 17$, $\mid 36$ $\longrightarrow$ $\mathrm{ord}_{37}(2) = 1$

$\longrightarrow 2^1 \equiv 1 \quad (37)$ NO

2) $X \equiv 1432^{1432} \mod 1001 = 7 \cdot 11 \cdot 13$

$$\downarrow$$

$$\begin{cases} X \equiv 4^{1432} \equiv 4^4 \equiv 4 & (7) \\ X \equiv 2^2 \equiv 4 & (11) \\ X \equiv 2^4 \equiv 3 & (13) \end{cases}$$

$1432 \equiv 4 \pmod 6$

$1432 \equiv 4 \pmod{12}$

$$\downarrow$$

$$\begin{cases} X \equiv 4 & (77) \\ X \equiv 3 & (13) \end{cases} \longrightarrow X \equiv 81 \quad (1001)$$

3) Le ultime 5 cifre di $x = 5^{5^{5^{5}}}$?

$$X \bmod 10^5 \to \bmod 2^5, \quad \searrow \bmod 5^5$$

$X \bmod 2^5$ $\qquad 5^{16} \equiv 1 \ (32)$

Ci basta $5^{5^{5}} \equiv 5^5 \bmod 16 \equiv 5 \bmod 16$

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

$5^5 \equiv 1 \bmod 4$

$$\begin{cases} X \equiv 5^5 \bmod (32) \\ X \equiv 0 \equiv 5^5 \bmod 5^5 \end{cases} \qquad X \equiv 0\,3125 \ (100000)$$

4) $\text{Torre}_n(a) = a^{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}} \Big\}\, n$ volte

$\text{Torre}_n(a)$ è costante mod m da un certo n in poi.

Idea $\underbrace{\text{Torre}_n(a)}_{\text{cost. mod } m} = a^{\text{torre}_{n-1}(a)] \bmod \varphi(m)}$

Induzione (estesa) su m. Per $m = 1, 2$ ok

Se lo so fare per $\{1, 2, ---, m-1\}$ come lo faccio per m ?

Dico che $\text{torre}_n(a)$ sarà costante mod $\varphi(m)$

$\Rightarrow \quad a^{\text{Torre}_n(a)}$ è costante mod m

$\Rightarrow \quad \text{Torre}_{n+1}(a)$ " " " "

$$a^{\varphi(m)} \equiv 1 \pmod m$$

$$c \equiv d \ (\varphi(m)) \longrightarrow x^c \equiv x^d \ (m)$$

$$d = c + k\varphi(m) \qquad x^c \equiv x^c \cdot \underbrace{x^{k\varphi(m)}}_{1} \ (m)$$

$(m, a) = b$ $\qquad m = c \cdot n$

$(c, a) = 1$

- La congruenza mod c si fa
- " " " n si fa lo stesso

perché $a^{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}$ prima o poi $\equiv 0 \ (n)$

$\text{Torre}_n\, a$ è costante $\begin{cases} \text{sia mod } n \ (\equiv 0) \\ \text{sia mod } c \end{cases}$

Esercizi istruttivi

1) Sia $D = \{ n \in \mathbb{N} \mid n \mid 2^n + 1 \}$

a. Trovare primi $p \in D$

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

$$\iff 2 + 1 \equiv 0 \ (p) \qquad p \mid 3$$

b. Dimostr. che tutti gli elem. di D sono $\equiv 0 \, (3)$

$$n \mid 2^n + 1 \iff 2^n + 1 \equiv 0 \ (n) \qquad (*)$$

Idea: il piu' piccolo primo!! $\quad p \mid n$

$$(*) \Rightarrow 2^n + 1 \equiv 0 \ (p)$$

$$2^n \equiv -1 \ (p)$$

$$4^n \equiv 1 \ (p) \qquad \begin{cases} \text{ord}_p(4) \mid n \\ \text{ord}_p(4) \mid p-1 \end{cases}$$

$$\Rightarrow \text{ord}_p(4) \mid (n, p-1) = 1 \quad (\text{p.p.p.})$$

$$4^1 \equiv 1 \ (p) \Rightarrow p \mid 3$$

Variante $\quad n \mid 12^n + 1$. Allora $13 \nmid n$

c) Trova $n = p \cdot q$, $n \in D$.

$$n = 3q$$

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

Caso 1: $q = 3$. $\qquad 9 \overset{?}{\mid} 2^9 + 1 = 513$

Caso 2: $q \neq 3$ $\qquad \begin{cases} 2^{3q} + 1 \equiv 0 & (3) \\ 2^{3q} + 1 \equiv 0 & (q) \end{cases}$

$$(-1)^q + 1 \equiv 0 \ (3)$$

$$8^q + 1 \equiv 0 \ (q) \longrightarrow 8 + 1 \equiv 0 \ (q)$$

$$q \mid 9 \rightarrow q = 3 \quad (\text{fatto})$$

d) $n = p^2 \cdot q$, $p \neq q$ primi, $n \in D$

- $p = 3$, $n = 9q$ $\qquad 2^{9q} \equiv -1 \ (9q)$

$$\begin{cases} 2^{9q} \equiv -1 \ (9) \\ 2^{9q} \equiv -1 \ (q) \end{cases} \qquad \begin{cases} (-1)^q \equiv -1 \ (9) \\ (2^9)^q \equiv -1 \ (q) \end{cases}$$

$$\begin{cases} \text{ok} \\ 512 \equiv -1 \ (q) \end{cases} \qquad q \mid 513 = 9 \cdot 57 = 3^3 \cdot 19$$

$q = 19$

- $n = 3p^2$ $\qquad 2^{3p^2} \equiv -1 \ (3p^2)$

$$\Downarrow$$

$$2^{3p^2} \equiv -1 \ (p)$$

$$2^{3p^2} = (2^{3p})^p \equiv 2^{3p} \equiv 8^p \equiv 8 \ (p)$$

$$8 \equiv -1 \ (p) \longrightarrow p = 3$$

e) Trova $n = p^k$, $n \in D$. $\qquad n = 3^k$

Claim $\quad 3^k \mid 2^{3^k} + 1$

Induzione su k: $k=1,2$

$k \to k+1$: $3^{k+1} \mid 2^{3^{k+1}}+1$?

$$\underbrace{\left(2^{3^k}\right)}_{A}{}^3+1 = \underbrace{(A+1)}_{3^k}\underbrace{(A^2-A+1)}_{\text{devo guad. un } 3}$$

Ip. indutt: $3^k \mid 2^{3^k}+1 = A+1$

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

$3^{k+1} \parallel 2^{3^k}+1 \qquad v_3\left(2^{3^k}+1\right) = k+1$

2) $\dfrac{a^p-1}{a-1}$ con p primo dispari

$*$ $q \mid \dfrac{a^p-1}{a-1} \Rightarrow q \mid a^p-1$

$\Rightarrow a^p \equiv 1\ (q) \qquad \mathrm{ord}_q(a) \begin{cases} 1 \\ p \end{cases}$

- o $p \mid q-1 \Rightarrow q \equiv 1\ (p)$
- o $q \mid a-1$

$*$ $a^p-1 = (a-1)\left(\dfrac{a^p-1}{a-1}\right)$

$q \mid \mathrm{mcd}\left(a-1, \dfrac{a^p-1}{a-1}\right)$

$q \mid a-1, \quad q \mid \dfrac{a^p-1}{a-1} = 1+a+a^2+\dots+a^{p-1}$

$$a \equiv 1 \ (q)$$

$$\underbrace{1+1+1+\dots+1}_{p \text{ termini}} \equiv 0 \ (q) \qquad p \equiv 0 \ (q)$$

$$\left(a-1, \frac{a^p-1}{a-1}\right) = p^k$$

$$\ast \quad p \mid a-1 \ \rightarrow \ a = hp+1$$

$$\frac{a^p-1}{a-1} = \frac{(1+hp)^p-1}{hp} = \qquad p \mid \binom{p}{m}$$

$$= \frac{\cancel{1}+\binom{p}{1}hp + h^2p^{2+1}(\dots)\cancel{-1}}{hp} \qquad p \geq 3$$

$$= p + hp^2(\dots) \equiv p \pmod{p^2}$$

$$\Rightarrow \left(a-1, \frac{a^p-1}{a-1}\right) \begin{cases} 1 \\ p \end{cases}$$

$$\frac{a^p-1}{a-1} = p \qquad 1+a+a^2+\dots+a^{p-1} = p$$

Appena $a \geq 2$ <u>NO</u>

$a=1$ NON HA SENSO

$$a = -b$$

$$\frac{+b^p+1}{+b+1} = p \qquad p = \frac{b^p+1}{b+1} > \frac{b^p}{b+1} \geq \left(\frac{2}{3}\right) b^{p-1}$$

$$p > (2/3)\, b^{p-1}, \quad \text{con } b \geq 2$$

$$\boxed{p=3, \quad b=2} \qquad 2^3+1=3^2$$

3) $x^p+1=q^n$ con p, q primi dispari

$n \geq 2$

$$\begin{gathered} x^p+1=q^n \\ \shortparallel \\ (x+1)\left(\frac{x^p+1}{x+1}\right) \end{gathered} \qquad x+1=q^a, \quad \frac{x^p+1}{x+1}=q^b$$

- $p=q$
- $\frac{x^p+1}{x+1}$ ha un fattore primo che $x+1$ non ha, a meno $x=2$, $p=3 \rightarrow q=3$

$x=0$, $x=1$

$n=0$ NO

Test iniziale. 15) Determinare quale dei seguenti k è residuo quadratico mod 2^{2010}.

k ~~2000~~, ~~2005~~, ~~2010~~, ~~2015~~, 2020

$\underset{\equiv 2(4)}{2010}$

$$2^{2010} \mid x^2 - 2010 \rightarrow 4 \mid x^2 - 2$$

$$2^{2010} \mid x^2 - 2000 \qquad x = 4m$$

$$2^{2010} \mid 16(m^2 - 125)$$

$$2^{2006} \mid m^2 - 125 \longrightarrow 8 \mid m^2 - 125$$

$$m^2 - 5$$

$$2^{2010} \mid x^2 - 2020 \qquad 2^{2008} \mid x^2 - 505$$

Fatto a è residuo quadratico mod 2^k, $k \geq 3$

$\Longleftrightarrow$ $a \equiv 1 \ (8)$

Dim $a = y^2 + 2^k \cdot x \leftarrow$ ("a è un residuo quadr. mod 2^k")

- x è pari $\rightarrow$ ho vinto
- x è dispari.

$k \geq 3$

$$(y + 2^{k-1})^2 \equiv y^2 + 2y \cdot 2^{k-1} + \cancel{2^{2k-2}}$$

$$\equiv a - 2^k \cdot x + y \cdot 2^k \equiv$$

$$\equiv a + 2^k \underbrace{(y - x)}_{\text{fattore } 2} \equiv a \quad (2^{k+1})$$

16) $S_p = \{ n \in \mathbb{N} : n \leq p \text{ e } p \mid n^{35} + 1 \}$

Determinare i possibili valori di $|S_p|$ al variare di p primo ≥ 2010

$$n^{35} + 1 \equiv 0 \ (p) \qquad n = g^k$$

$$g^{35k} + 1 \equiv 0 \ (p)$$

$$g^{35k} \equiv -1 \ (p) \iff 35k \equiv \frac{p-1}{2} \ (p-1)$$

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

$$p-1 = \text{ord}_p(g) \leq \frac{p-1}{2}$$

$$\Rightarrow g^{\frac{p-1}{2}} \equiv -1 \ (p)$$

Contare le soluz. di $35k \equiv \frac{p-1}{2} \ (p-1)$

$$(p-1, 35) \in \{1, 5, 7, 35\}$$

- $(p-1, 35) = 1 \qquad k \equiv (35)^{-1} \left(\frac{p-1}{2}\right) \ (p-1)$

$$g^k = -1$$

- $(p-1, 35) = 5 \qquad 5k \equiv 7^{-1} \cdot \frac{p-1}{2} \ (p-1)$

$$k \equiv 7^{-1} \cdot \frac{p-1}{2 \cdot 5} \ \left(\frac{p-1}{5}\right)$$

$$k_0, \ k_0 + \frac{p-1}{5}, \ k_0 + 2 \cdot \frac{p-1}{5}, \ \ldots, \ k_0 + 4 \cdot \frac{p-1}{5}$$

- $(p-1, 35) = 7 \rightarrow 7$ soluz.
- $(p-1, 35) = 35 \rightarrow 35$ soluz

$$|S_p| = (p-1, 35)$$

Teo (Dirichlet) Se $(a,b)=1$, allora esistono infiniti primi della forma $an+b$

$n \cdot 35 + 1 \qquad \varphi(p) = 35 \cdot n$

$35n + 8 \qquad \varphi(p) = 35n + 7 \qquad 7 \mid \varphi(p)$

$5 \nmid \varphi(p)$

Lemmone Sia $q(x)$ è un polinomio di grado al più $p-2$ con p primo.

Allora $q(0) + q(1) + q(2) + \dots + q(p-1) \equiv 0 \ (p)$

Dim Idea: se è vero per i singoli monomi, sommando sui vari monomi lo sappiamo fare per $q(x)$ generico.

$ax \qquad \cancel{a}(1 + 2 + 3 + \dots + p-1) \equiv 0 \quad (p)$

- $\frac{(p-1)p}{2} \equiv 0 \quad (p)$
- $1 + (p-1) + 2 + (p-2) + \dots \equiv 0 \quad (p)$

X^n $\qquad 1^n + 2^n + \dots + (p-1)^n \equiv 0 \pmod{p}$

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

$$\equiv (g^n)^1 + (g^n)^2 + \dots + (g^n)^{p-2} + (g^n)^0 \equiv$$

$y = g^n$ $\qquad \equiv y^0 + y^1 + \dots + y^{p-2} \equiv \dfrac{y^{p-1} - 1}{y - 1} \equiv \text{(*)}$

ATTENZIONE!

Serve $y \neq 1$, per dividere.

$g^n \neq 1 \qquad n \leq p-2$

$$\text{(*)} \equiv (1-1) \cdot (y-1)^{-1} \equiv 0 \pmod{p}$$