Teoria Dei Numeri 2 - BASIC

Titolo nota 06/09/2018

erFuricksen

TEOREMA CINESE DEL RESTO

$$\begin{cases} x \equiv a_1 \ (n_1) \\ x \equiv a_2 \ (n_2) \end{cases}$$

Se $(n_1, n_2) = 1$.

Cerco x_1 t.c. $\begin{cases} x_1 \equiv 0 \ (n_1) \\ x_1 \equiv a_2 \ (n_2) \end{cases}$, cerco x_2 t.c. $\begin{cases} x_2 \equiv a_1 \ (n_1) \\ x_2 \equiv 0 \ (n_2) \end{cases}$

$x_1 + x_2 = x \implies$ è soluzione!

Se non troviamo subito x_1, x_2, posso cercare y_1, y_2 t.c.

$\begin{cases} y_1 \equiv 0 \ (n_1) \\ y_1 \equiv 1 \ (n_2) \end{cases}$ $\begin{cases} y_2 \equiv 1 \ (n_1) \\ y_2 \equiv 0 \ (n_2) \end{cases}$ e poi prendo $x_1 = a_1 y_1$ $x_2 = a_2 y_2$.

$x + k \cdot n_1 n_2$ $k \in \mathbb{Z}$

Se avessi più equazioni

$\begin{cases} x \equiv a_1 (n_1) \\ x \equiv a_2 (n_2) \\ x \equiv a_3 (n_3) \end{cases}$ con n_1, n_2, n_3 coprimi a 2 a 2

dobbiamo trovare una sol. nella forma $x_1 + x_2 + x_3 + k n_1 n_2 n_3$

(pongo $x_1 \equiv \begin{cases} a_1 (n_1) \\ 0 \ (n_2) \\ 0 \ (n_3) \end{cases}$ ....)

$$\begin{cases} x \equiv 1 (3) \\ x \equiv 2 (5) \\ x \equiv 5 (7) \end{cases} \qquad x_1 = 70 \qquad x_2 = 42 \qquad x_3 = 75$$

$$x = x_1 + x_2 + x_3 + k \cdot 105 = $$
$$= 187 + 105k \equiv 82 (105)$$

Se n_1, n_2 non sono coprimi?

$$\begin{cases} x \equiv 7 (10) \\ x \equiv 8 (15) \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 (2) \\ x \equiv 2 (5) \\ x \equiv 3 (5) \\ x \equiv 2 (3) \end{cases} \Longrightarrow \text{ non ha sol!}$$

Se avessi avuto

$$\begin{cases} x \equiv 7 (10) \\ x \equiv 7 (15) \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 (2) \\ x \equiv 2 (5) \\ x \equiv 1 (3) \\ x \equiv 2 (5) \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 (2) \\ x \equiv 1 (3) \\ x \equiv 2 (5) \end{cases}$$

Per quali $n \in \mathbb{N}$ $\quad 1 + n + \frac{n^2}{2} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!} \in \mathbb{Z}$

è equivalente a $\quad 6! \mid 6! + 6! \cdot n + \frac{6!}{2} n^2 + 5! n^3 + \underbrace{30 n^4 + 6n^5 + n^6}_{= p(n)}$

$$p(n) \equiv 6n^5 + n^6 (5) \equiv n^5 + n^6 (5) \equiv n^5(n+1) \quad (5)$$

$$\Longrightarrow p(n) \equiv 0 \Longrightarrow 5 \mid n^5(n+1) \Longrightarrow 5 \mid n \ \vee \ 5 \mid n+1$$

mod 3 $\quad n^6 \equiv 0 (3) \Longrightarrow 3 \mid n \Longrightarrow 9 \mid p(n) \Longrightarrow n \equiv 0 (3).$

mod 2 (uguale) $\quad n \equiv 0 (2) \quad$ (se controllo ogni volta che in un coefficiente ho meno di 2^4 riacquisto fattori 2 da n^k).

$\Longrightarrow n \equiv 0 (2)$ è sufficiente

$$\begin{cases} n \equiv 0\ (2) \\ n \equiv 0\ (3) \\ n \equiv 0\ (5) \end{cases} \quad \vee \quad \begin{cases} n \equiv 0\ (2) \\ n \equiv 0\ (3) \\ n \equiv -1\ (5) \end{cases}$$

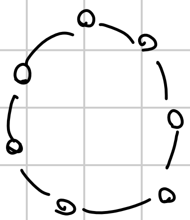
$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$n \equiv 0\ (30) \qquad\qquad\qquad n \equiv -6\ (30).$$

... Torniamo un attimo a N1 ...

$$\begin{cases} a \equiv 1(3) \\ a \equiv 0(7) \\ a \equiv 6(19) \end{cases} \Longrightarrow \text{per teorema cinese c'è soluzione!}$$

TEOREMA DI FERMAT



p perline, a possibili colori

Quante sono le collane a meno di rotazione?

Ci sono a collane tutte dello stesso colore.

Se le perline non sono tutte dello stesso colore, ruotando ottengo p diverse collane (perché p primo).

$$\Longrightarrow \quad \frac{a^p - a}{p} \text{ collane!}$$

$$\Longrightarrow \quad \frac{a^p - a}{p} \text{ deve essere intero!} \quad \Longrightarrow \quad a^p \equiv a\ (p)$$

TEOREMA DI FERMAT: Dati p primo, $a \in \mathbb{N}$, $p \nmid a$

$$\Longrightarrow \quad a^p \equiv a\ (p).$$

DIM: per induzione su a: per $a=0$ è vero.

per $a+1$ $\quad (a+1)^p = \sum_{k=0}^{p} a^k \cdot \binom{p}{k}$, ma $p \mid \binom{p}{k} \ \forall k \neq 0, p$

perché se $k \neq 0, p$ $\quad \binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow k, p-k < p \Rightarrow$

$\Rightarrow p \nmid k!$ e $p \nmid (p-k)!$, ma $p \mid p! \Rightarrow p \mid \binom{p}{k}$

$\Rightarrow (a+1)^p \equiv a^p + 1 \underset{\text{ip. induttiva}}{\equiv} a+1 \ (p)$. $\square$

ES: Quanto vale $2^{2018} \pmod 7$?

$$2^{2018} = 2^{2016+2} = 2^{6 \cdot \frac{2016}{6} + 2} \equiv (2^6)^{2016/6} \cdot 4 \equiv 1^{\frac{2016}{6}} \cdot 4 \equiv 4 \ (7)$$

φ di EULERO

$\varphi : \mathbb{N}^+ \to \mathbb{N} \qquad \varphi(n) = |\{1 \leq x \leq n, \ (x,n) = 1\}|$

ES: $\varphi(1) = 1 \qquad \varphi(6) = 2 \qquad \varphi(10) = 4 \qquad \varphi(7) = 6$.

OSS: Se p è primo $\quad \varphi(p) = p-1$

Se p è primo $\quad \varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p-1)$

DEF: φ è moltiplicativa se $\forall (a,b) = 1 \quad \varphi(ab) = \varphi(a)\varphi(b)$

Se $(a,b) = 1 \qquad \varphi(ab) = |\{\text{elementi coprimi con } ab\}| =$

$= |\{\text{el. copr. con } a \text{ e con } b\}|$ quindi cerco delle coppie di resti mod a e mod b (x,y) t.c. $(x,a)=1$ $(y,b)=1$. Fissata una coppia (x,y) per il teorema cinese $\exists!\, w$ mod ab t.c. $\begin{cases} w \equiv x\,(a) \\ w \equiv y\,(b) \end{cases}$ e viceversa, da w $\exists!\,(x,y)$.

$\Rightarrow$ c'è una biiezione fra le classi di resto coprime con ab e le coppie di resti coprimi con a e b.

Quante sono? $\varphi(a)\varphi(b)$, ma anche $\varphi(ab)$

$\Rightarrow$ $\varphi(ab)=\varphi(a)\varphi(b)$.

Ma allora dato n generico, $n = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$

$$\Rightarrow \varphi(n)=\varphi(p_1^{\alpha_1})\cdot\ldots\cdot\varphi(p_k^{\alpha_k}) = \prod_{i=1}^{k} p_i^{\alpha_i-1}(p_i-1) = \prod_{i=1}^{k} p_i^{\alpha_i}\cdot\frac{p_i-1}{p_i} =$$
$$= n\cdot\frac{(p_1-1)}{p_1}\cdot\ldots\cdot\frac{(p_k-1)}{p_k} = n\cdot\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

TEOREMA DI EULERO-FERMAT

Dati $a,n\in\mathbb{N}$ $(a,n)=1$ $\Rightarrow$ $a^{\varphi(n)}\equiv 1\,(n)$.

DIM: $A=\{[b_1],[b_2],\ldots,[b_{\varphi(n)}]\}$ = insieme classi di resto coprime mod n

Vale che $[a]\in A$, considero $A'=\{[ab_1],[ab_2],\ldots,[ab_{\varphi(n)}]\}$

Sicuramente $(ab_i,n)=1$ $\forall i$ $\Rightarrow$ $A'\subseteq A$.

Se per assurdo $ab_i\equiv ab_j$ per $i\neq j$, esiste a^{-1} inverso molt. di a $\Rightarrow$ $a^{-1} a b_i \equiv a^{-1} \cdot a b_j$ $\Rightarrow$ $b_i \equiv b_j$ assurdo.

$\Rightarrow$ $a b_i \not\equiv a b_j$ $\forall i \neq j$ $\Rightarrow$ A' ha $\varphi(n)$ elementi $\Rightarrow A' = A$.

Allora $\prod_{x \in A} x = \prod_{x \in A'} x$ $\Rightarrow$ $b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)} \equiv a b_1 \cdot a b_2 \cdot \ldots \cdot a b_{\varphi(n)}$

$\prod b_i \equiv a^{\varphi(n)} \cdot \prod b_i$, ma $(\prod b_i, n) = 1$ $\Rightarrow$ posso dividere

$\Rightarrow$ $a^{\varphi(n)} \equiv 1 \ (n)$. $\square$

- Sia n un numero che in base 10 è del tipo $30x070y03$ con x, y cifre. Sappiamo che $37 \mid n$, determinare $\max(x+y)$

$n = 300070003 + 100(10^4 \cdot x + y) = 3 \cdot 10^8 + 7 \cdot 10^4 + 3 + 10^2 (10^4 x + y)$

$1000 = 1 + 999 = 1 + 27 \cdot 37 \equiv 1 \ (37)$

$\Rightarrow$ $n \equiv 300 + 70 + 3 + 100(10x + y) \ (37) \equiv$

$\equiv 3 + 1000x + 100y \equiv 3 + x + 100y \ (37) \equiv$

$\equiv 3 + x - 11y \ (37)$ $\qquad$ $100y + x \equiv -3 \ (37)$

$\Downarrow$

$y0x$

Def: Si chiama ordine moltiplicativo di a mod n

$\text{ord}_n(a)$ il più piccolo intero positivo t.c. $a^{\text{ord}_n(a)} \equiv 1 (n)$.

oss: $a^{\varphi(n)} \equiv 1 (n)$ non è detto che $\varphi(n)$ sia l'ordine!

Es: $2^6 \equiv 1\ (7)$ $\quad \mathrm{ord}_7(2) = 3 \quad (2^3 \equiv 1\ (7))$.

oss: $\mathrm{ord}_n(a) \mid \varphi(n)$, infatti se così non fosse

$k = \mathrm{ord}_n(a) \qquad \varphi(n) = k\cdot\alpha + r \qquad 0<r<k$

$1 \equiv a^{\varphi(n)} \equiv a^{k\alpha + r} \equiv a^r$ assurdo! perché $r<k$.

In generale, $\exists a$ t.c. $\mathrm{ord}_n(a) = \varphi(n)$? dipende da n.

Se n è primo sì! $\Rightarrow \forall p$ primo $\exists a$ t.c. $\mathrm{ord}_p(a) = p-1$.

Def: Un tale a è detto generatore mod n.

BMO 2018 # 4

Determinare tutte le coppie (p,q) con p, q primi, per cui

$$3p^{q-1} + 1 \mid 11^p + 17^p$$

Sia r un primo t.c. $r \mid 3p^{q-1}+1 \Rightarrow$

$\Rightarrow r \mid 11^p + 17^p$, o $p \mid r-1$ oppure $p \nmid r-1$

Se $p \nmid r-1 \quad (p, r-1) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ t.c. $1 = ap + b(r-1)$

$\Rightarrow 11^p \equiv -17^p\ (r) \qquad -\left(\frac{17}{11}\right)^p \equiv 1\ (r) \qquad \left(\frac{17}{11}\right)^p \equiv -1\ (r)$

$11^{ap} \equiv (-17^p)^a \qquad 11^{ap} \equiv 11^{ap+b(r-1)} \equiv 11\ (r)$

$(-17^p)^a \equiv (-17)^{pa} \equiv (-17)^{pa + b(r-1)} \equiv -17\ (r)$

$11^{ap+b(r-1)} = 11^{ap} \cdot 11^{b(r-1)}$

$11 \equiv -17\ (r) \qquad 28 \equiv 0\ (r)$

$\Longrightarrow \quad r = 2 \quad \vee \quad r = 7 .$

Se $p = 2 \quad 11^2 + 17^2 = 410 = 2 \cdot 5 \cdot 41 \quad \dots$ ecc... numero finito di casi

$\Longrightarrow$ ... non ci sono soluzioni ..

Se $p \neq 2 \quad 11^p + 17^p \equiv 11 + 17 \ (8) \equiv$ $\left((2n+1)^2 = 4n^2 + 4n + 1 = = 4n(n+1) + 1 \equiv 1 \ (8) \right)$

$\equiv 4 \ (8)$

$\boxed{\text{CASO } 1} \ \boxed{q \neq 2} \quad 3p^{q-1} + 1 \equiv 3 + 1 \equiv 4 \ (8) .$

Se $r = 7 \quad 7 \mid 3p^{q-1} + 1 \Longrightarrow p \neq 7 \quad 7 \mid 11^p + 17^p$

$11^p + 17^p = 28 \left(\underbrace{11^{p-1} - 11^{p-2} \cdot 17 + \dots - 11 \cdot 17^{p-2} + 17^{p-1}}_{} \right)$

ci piacerebbe che lui $\not\equiv 0 \ (7)$.

$17 \equiv -11 \ (7) \Longrightarrow 11^{p-1} - 11^{p-2} \cdot 17 + \dots + 17^{p-1} \equiv$

$\equiv 11^{p-1} + 11^{p-1} + \dots + 11^{p-1} \equiv p \cdot 11^{p-1} \not\equiv 0 \ (7)$

$\Longrightarrow$ c'è un solo 7 in $11^p + 17^p \Longrightarrow$

$\Longrightarrow$ c'è al più un 7 in $3p^{q-1} + 1$.

$3p^{q-1} + 1 = 4 \cdot 7^\alpha \cdot \underbrace{(\dots)}_{1 \bmod p} \equiv 4 \cdot 7^\alpha \ (p) \quad \alpha \in \{0, 1\}$

Tuttavia $3p^{q-1} + 1 \equiv 1 \ (p) \Longrightarrow$

$\Longrightarrow \quad 4 \equiv 1 (p) \quad \vee \quad 4 \cdot 7 \equiv 1 (p) \quad (27 \equiv 0 (p))$

$\Longrightarrow \quad p = 3$!!! $\quad 11^3 + 17^3 = 28 (121 + 289 - 11 \cdot 17)$

... si fa ... unica sol. $(3, 3)$.

$\boxed{\text{CASO 2} \mid q=2}$ $\qquad 3p+1 \mid 11^p + 17^p \equiv 4\ (8)$

$$p \not\equiv -\tfrac{1}{3}\ (8).$$

$$3p+1 = 2^\alpha \cdot 7^\beta \cdot \underbrace{(\ldots)}_{\equiv 1(p)} \implies 2^\alpha \cdot 7^\beta \equiv 1\ (p) \qquad \alpha \in \{1,2\},\ \beta \in \{0,1\}$$

il caso $\alpha = 2$ già fatto prima.

$\alpha = 1 \implies 2 \equiv 1\ (p) \vee 14 \equiv 1\ (p) \implies p = 13$

$\implies 40 \mid 11^{13} + 17^{13} \qquad 8 \mid 40$ ma $8 \nmid 11^{13} + 17^{13}$. No sol.

- $D = \{ n \in \mathbb{N} : n \mid 2^n + 1 \}$

(a) Determinare tutti i primi $p \in D$.

$$p \mid 2^p + 1 \qquad 2^p + 1 \equiv 2 + 1 = 3 \equiv 0\ (p) \implies p = 3.$$

(b) Determinare tutti i $p^k \in D$

$$p^k \mid 2^{p^k} + 1 \implies p \mid 2^{p^k} + 1$$

INDUZIONE

$$2^{p^k} = \left(2^{p^{k-1}}\right)^p \equiv 2^{p^{k-1}}\ (p) \ \ldots\ldots \ 2^{p^k} \equiv 2\ (p)$$

$$\implies 0 \equiv 2^{p^k} + 1 \equiv 2 + 1 \equiv 3\ (p) \implies p = 3.$$

Cerco k t.c. $3^k \mid 2^{3^k} + 1$ $\qquad$ per $k = 0$ $\ 3^0 = 1 \mid 2^{3^0} + 1$.

Per $k+1$ $\qquad 2^{3^{k+1}} + 1 = \underbrace{\left(2^{3^k} + 1\right)}_{\text{divisibile per } 3^k}\left(2^{2\cdot 3^k} - 2^{3^k} + 1\right)$

Ci basta $\ 2^{2\cdot 3^k} - 2^{3^k} + 1 \equiv 0\ (3)$ $\qquad$ che è sempre vero

$$\underset{1}{\equiv} \quad \underset{-2}{\equiv} \quad \underset{+1}{\equiv} \quad \equiv 0$$

$$\implies 3^k \in D \quad \forall k.$$

ESERCIZI : · FINIRE QUELLO DI PRIMA (PAG 43 ES 10)

· PAG 12 ES 61 · PAG 42 ES 10

· PAG 43 ES 7 - 9

BONUS 1 : Trovare tutti gli $a, b \in \mathbb{Z}^+$ t.c., dato il polinomio

$$P(n) = \frac{n^5+a}{b}, \quad \exists n \in \mathbb{Z} \text{ per cui } P(n), P(n+1), P(n+2) \in \mathbb{Z}$$

BONUS 2 : Trovare tutti gli x, y primi t.c.

$$x^y - y^x = xy^2 - 19$$

BONUS 3 : Mostrare che esistono infiniti $n \in \mathbb{N}$ composti tali che $n \mid 3^{n-1} - 2^{n-1}$

$3 + 100y + x \equiv 0 \ (37)$ $\qquad$ $30 + y + 10x \equiv 0 \ (37)$

$y + 10x \equiv 7 \ (37)$ $\qquad$ $y + 10x \to 7, 44, 81$

- $pq \mid 2^{pq} + 1 \quad \to \quad 2^{pq} + 1 \equiv 0 \ (p) \quad 2^q + 1 \equiv 0 \ (p)$

Se $p \neq 3$ allora $q \mid ord_p(2) \mid p-1$, allo stesso modo

se $q \neq 3$ $p \mid q-1$. $\Rightarrow q < p$ e $p < q$ assurdo

WLOG $p = 3$ $\quad q \mid 2^3 + 1 = 9 \quad q = 3$.

$2^q + 1 \equiv 0 \ (p) \quad 2^q \equiv -1 \ (p) \quad 2^{2q} \equiv 1 \ (p) \Rightarrow ord_p(2) \mid 2q$

se $q \nmid ord \Rightarrow ord \mid 2 \Rightarrow ord = 1 \vee ord = 2 \Rightarrow$

$\Rightarrow 2 \equiv 1 \ (p) \vee 4 \equiv 1 \ (p) \Rightarrow p = 3$.

$\Rightarrow$ se $p \neq 3$ $\quad q \mid ord$ ... BLA BLA ...

- $n \mid 2^n + 1$ $\quad$ sia p un primo t.c. $p \mid n \Rightarrow$

$$\Rightarrow \quad 2^n + 1 \equiv 0 \ (p) \qquad 2^{p \cdot \frac{n}{p}} + 1 \equiv 0 \qquad 2^{\frac{n}{p}} + 1 \equiv 0 \ (p)$$

se $p^k \parallel n$ $\quad \left(p^k \mid n, \ p^{k+1} \nmid n\right)$ $\qquad 2^{\frac{n}{p^k}} + 1 \equiv 0 \ (p)$

$$2^n \equiv 2^{\frac{n}{p} \cdot p} \equiv 2^{\frac{n}{p}} \equiv 2^{p \cdot \frac{n}{p^2}} \equiv 2^{\frac{n}{p^2}} \ldots \quad \uparrow$$

$$2^{2 \cdot \frac{n}{p^k}} \equiv 1 \ (p) \qquad ord_p(2) \mid p-1 \qquad ord_p(2) \mid 2 \cdot \frac{n}{p^k}$$

IDEA: scelgo p il più piccolo primo t.c. $p \mid n$, $\quad p \neq 2$

perché sì., $\quad p \geq 3$ $\quad$, siccome è il più piccolo

$\forall q$ primo, $q \mid \frac{n}{p^k}$, $\quad q > p$ $\quad$, quindi $q \nmid ord_p(2)$,

perché se valesse $q \mid ord_p(2) \Rightarrow q \mid p-1 \Rightarrow p > q$ assurdo

$$\Rightarrow \left(\frac{n}{p^k}, ord_p(2)\right) = 1 \Rightarrow ord_p(2) \mid 2 \Rightarrow$$

$$\Rightarrow \quad 2 \equiv 1 \ (p) \ \vee \ 4 \equiv 1 \ (p) \quad \Rightarrow \quad p = 3.$$

- $p^2 q \mid 2^{p^2 q} + 1$ $\qquad p \neq q$

1) $\quad 2^{9q} + 1 \equiv 0 \ (9q) \qquad 2^9 + 1 \equiv 0 \ (q) \qquad 513 \equiv 0 \ (q)$

$$513 = 171 \cdot 3 = 57 \cdot 9 = 27 \cdot 19 \quad \Rightarrow \quad q = 19$$

$$99 \equiv 3 \ (6) \qquad 6 = \varphi(9) \quad \Rightarrow \quad 2^{99} \equiv 2^3 \ (9) \equiv -1 \ (9)$$

$\Rightarrow (p, q) = (3, 19)$ è sol.

2) $\quad 2^{3p^2} + 1 \equiv 0 \ (3p^2) \qquad 2^3 + 1 \equiv 0 \ (p) \quad \Rightarrow \quad p = 3$ no sol.

$A = 5^n + 3^n + 1$. $A \equiv 2^n + 1 \; (3)$ e vogliamo $A \not\equiv 0$

se n dispari $3 | A$ no! $\Rightarrow$ n pari $\Rightarrow$ $A \equiv 2 \,(3)$

$3^n + 1 \not\equiv 0 \,(5)$ $\quad 3^n \not\equiv -1 \,(5)$ $\Rightarrow$ $n \not\equiv 2 \,(4)$ $\Rightarrow$ $n \equiv 0 \,(4)$

$A \not\equiv 0 \,(7)$ $\quad 5^n + 3^n + 1 \equiv (-2)^n + 3^n + 1 \equiv 2^n + 3^n + 1 \equiv$

$\equiv 2^n + (-4)^n + 1 \equiv 4^n + 2^n + 1 \;(7)$

Se valesse $A \equiv 0 \,(7)$ allora $4^n + 2^n + 1 \equiv 0 \,(7)$

$\Rightarrow$ $2^{2n} + 2^n + 1 \equiv 0$ $\qquad 2^n = \begin{cases} 2 \\ 4 \\ 1 \end{cases}$

1) $2^n = 2$ $\Rightarrow$ $A \equiv 2^2 + 2 + 1 \equiv 0 \,(7)$

2) $2^n = 4$ $\Rightarrow$ $A \equiv 4^2 + 4 + 1 \equiv 2 + 4 + 1 \equiv 0 \,(7)$

3) $2^n = 1$ $\Rightarrow$ $A = 1 + 1 + 1 \equiv 3 \,(7)$

$\Rightarrow$ $\mathrm{ord}_7(2) | n$ $\Rightarrow$ $3 | n$.

- $p_1^n , p_2^n , \dots , p_m^n$ cerchiamo a t.c.

$p_1^n | a$ $\quad a + d \equiv 0 \,(p_2^n)$ $\quad a + 2d \equiv 0 \,(p_3^n)$ ... $a + (m-1)d \equiv 0 \,(p_m^n)$

- $\forall p$ primo $\exists \infty \; n$ t.c. $p | 2^n - n$

$2^n \equiv n \,(p)$ $\qquad n \equiv 1 \,(p)$ $\qquad 2^n \equiv 1 \,(p)$ mi basta

$p - 1 | n$ $\qquad \begin{cases} n \equiv 1 \,(p) \\ n \equiv 0 \,(p-1) \end{cases}$

ce n'è anche infinite del tipo $\begin{cases} n \equiv 2 \,(p) \\ n \equiv 1 \,(p-1) \end{cases}$

- $\exists \infty$ n composti: $n \mid 3^{n-1} - 2^{n-1}$.

$n = 3^k - 2^k$ $\qquad 3^k - 2^k \mid 3^{3^k - 2^k - 1} - 2^{3^k - 2^k - 1}$

che è vero se $k \mid 3^k - 2^k - 1$

$k = 2^\alpha$ $\qquad 3^k - 2^k - 1 = 3^{2^\alpha} - 2^{2^\alpha} - 1$ $\qquad 2^{2^\alpha} \equiv 0 \ (2^\alpha)$

se $\alpha > 1$ $\quad 2^\alpha > \alpha \Rightarrow 2^{2^\alpha} \equiv 0 \ (2^\alpha)$, quindi vorrei

$3^{2^\alpha} - 1 \equiv 0 \ (2^\alpha)$ $\qquad 3^{2^\alpha} \overset{\text{speranze}}{\equiv} 1 \ (2^\alpha)$ $\qquad \varphi(2^\alpha) = 2^{\alpha-1} \mid 2^\alpha$

$\Rightarrow 3^{2^\alpha} \equiv 1 \ (2^\alpha)$ è vero.

$n = 3^{2^\alpha} - 2^{2^\alpha}$ vanno bene, e sono composti perché per

$\alpha > 2$ $\qquad \underbrace{3^2 - 2^2}_{=5} \mid 3^{2^\alpha} - 2^{2^\alpha}$ e $3^{2^\alpha} - 2^{2^\alpha} > 3^2 - 2^2$.