# SENIOR 2011 – TEORIA DEI NUMERI 2 (Basic)

Titolo nota 07/09/2011

## TEOREMA CINESE DEL RESTO (CRT)

Sistema di congruenze: cerco $x$ intero t.c.

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

Si intende che $a_1, \dots, a_n$ sono dati e anche i moduli $m_1, \dots, m_n$ sono dati

**Teorema** Se i moduli sono a 2 a 2 coprimi, cioè $\overbrace{(m_i, m_j)}^{MCD} = 1$ per ogni $1 \le i < j \le n$, allora il sistema ammette soluzione unica modulo $m_1 \cdot \dots \cdot m_n$.

**Dim.** **Unicità** Siano $x$ e $y$ 2 sol. Allora $x - y \equiv 0 \pmod{m_i}$ per ogni $i = 1, \dots, n$, quindi $x - y = k\, m_1 \cdot \dots \cdot m_n$.

**Esistenza 1** Induzione su $n$. Per $n = 1$ non è difficile...
Supponiamo di saper risolvere un sistema di $n$ congruenze, e aggiungiamo $x \equiv a_{n+1} \pmod{m_{n+1}}$.
La soluzione del sistema di $n$ congruenze sarà

$$y + k\, m_1 \cdot \dots \cdot m_n$$

Ora cerco $k$ in modo tale che

$$y + k\, m_1 \cdot \dots \cdot m_n \equiv a_{n+1} \pmod{m_{n+1}}$$

cioè

$$k\, m_1 \cdot \dots \cdot m_n \equiv a_{n+1} - y \pmod{m_{n+1}}$$

Poiché $m_{n+1}$ è coprimo con i moduli precedenti, esiste (di sicuro) l'inverso di $m_1 \cdot \dots \cdot m_n \pmod{m_{n+1}}$
Basta moltiplicare per quello!

**Esistenza 2** Divide et impera! Risolvo nel caso $a_1 = 1$ e $a_2 = \dots = a_n = 0$. La sol. sarà del tipo

$$x = k\, m_2 \cdot \dots \cdot m_n$$

Cerco $k$ in modo che $x \equiv 1 \pmod{m_1}$.

Basta prendere $k$ = inverso di $m_2 \cdot \dots \cdot m_n \pmod{m_1}$.

Per ogni $i = 1, \dots, n$ sia $x_i$ la soluzione con $a_i = 1$ e tutti gli altri 0. Allora

$$x = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$$

A cosa è congruo $x$ modulo $m_i$?

$$x \equiv a_i x_i \equiv a_i \pmod{m_i}$$

— o — o —

**Esempio**
$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod{10} \end{cases}$$

$x = 2 + 3a$. Sistemo la 2ª: $2 + 3a \equiv 3 \pmod 7$

$3a \equiv 1 \pmod 7$ $\quad a \equiv 5 \pmod 7$, quindi

$x = 2 + 3a = 2 + 3(5 + 7b) = 17 + 21b$

Sistemo la 3ª: $17 + 21b \equiv 1 \pmod{10}$ $\quad 21b \equiv -16 \pmod{10}$

$b \equiv 4 \pmod{10}$ $\Rightarrow$ $x = 17 + 21(4 + 10c) = 101 + 210c$.

— o — o —

**Oss.** Se i moduli non sono primi tra di loro, allora il sistema può avere o non avere soluzioni.

Basta spezzare le varie congruenze rispetto ai fattori primi degli $m_i$ e vedere se le condizioni sono compatibili

**Esempio**
$$\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 12 \pmod{15} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 2 \\ x \equiv 12 \pmod 5 \\ x \equiv 12 \pmod 3 \end{cases}$$

$x \equiv 3 \pmod{10}$

$x \equiv 12 \pmod{15}$

INCOMPATIBILI

(quindi nessuna soluzione)

$$\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 12 \pmod{15} \end{cases} \qquad \begin{cases} x \equiv 7 \pmod 5 \\ x \equiv 7 \pmod 2 \\ x \equiv 12 \pmod 5 \\ x \equiv 12 \pmod 3 \end{cases} \quad \text{ok} \qquad \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 3 \end{cases}$$

La soluzione è $x \equiv 27$ modulo 30.

— o — o —

**Fatto generale** Sia $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Allora conosco $x$ modulo $m$ se e solo se conosco $x$ modulo $p_i^{k_i}$ per ogni $i = 1, \dots, r$.

— o — o —

**$\Phi$ di Eulero** Sia $n$ un intero positivo. Si definisce

$$\Phi(n) = \#\{ m : 1 \le m \le n \text{ e } (m, n) = 1 \}$$

= numero degli interi tra 1 ed $n$ che sono relativamente primi con $n$.

Casi facili: $\Phi(p) = p - 1$ per ogni primo $p$.

$$\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

($p^k$: tutti; $p^{k-1}$: quelli multipli di $p$)

per ogni potenza di un primo $p$

**Fatto fondamentale**: $\Phi$ è una funzione moltiplicativa, cioè

$$\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b) \quad \text{per ogni } a \text{ e } b \text{ coprimi}$$

**Corollario** Se $n = p_1^{k_1} \cdots p_r^{k_r}$, allora

$$\Phi(n) = \Phi(p_1^{k_1}) \cdots \Phi(p_r^{k_r}) = p_1^{k_1 - 1}(p_1 - 1) \cdots p_r^{k_r - 1}(p_r - 1)$$

$$= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Dim. fatto fondamentale. Conosco $m$ modulo $ab$ se e solo se conosco $m$ modulo $a$ e modulo $b$.

Inoltre $(m, ab) = 1$ se e solo se $(m, a) = 1$ e $(m, b) = 1$.

Tutto ciò segue dal CRT.

Quindi

$$\{\text{Classi coprime con } ab\} = \{\text{Classi coprime con } a\} \cdot \{\text{Classi coprime con } b\}$$

ha $\phi(ab)$ elem. $\phi(a)$ elem. $\phi(b)$ elem.

— o — o —

Esempi
$$\phi(10) = \phi(2)\cdot\phi(5) = 1\cdot 4 = 4$$
$$\phi(25) = 25 - 5 = 20$$
$$\phi(100) = \phi(4)\cdot\phi(25) = 2\cdot 20 = 40$$
$$\phi(2000) = \phi(16)\cdot\phi(125) = (16-8)(125-25) = 8\cdot 100 = 800$$
$$\phi(360) = \phi(8\cdot 5\cdot 9) = \phi(8)\cdot\phi(5)\cdot\phi(9) = 4\cdot 4\cdot 6 = 96$$

— o — o —

Le classi coprime con $m$ sono le classi invertibili modulo $m$, e sono le classi dove fare la struttura moltiplicativa

— o — o —

Esempio 1 Dim. che per ogni intero positivo $n$ esisto $n$ interi consecutivi divisibili per un quadrato perfetto non banale.

Siano $x+1, x+2, \dots, x+n$ gli interi cercati. Scelgo $n$ primi distinti $p_1, p_2, \dots, p_n$ e impongo

$$x+1 \equiv 0 \pmod{p_1^2} \qquad x \equiv -1 \pmod{p_1^2}$$
$$x+2 \equiv 0 \pmod{p_2^2} \qquad x \equiv -2 \pmod{p_2^2}$$
$$\vdots \qquad\qquad \vdots$$
$$x+n \equiv 0 \pmod{p_n^2} \qquad x \equiv -n \pmod{p_n^2}$$

**Esempio 2** Per ogni $n$ esistono $n$ interi consecutivi ciascuno dei quali NON è una potenza perfetta.

**Dim. 1 (CRT)** Come prima impongo $x+i \equiv p_i \pmod{p_i^2}$ per $i = 1, \dots, n$. Così $p_i$ compare con esponente uno nella fattorizzazione di $x+i$.

**Dim. 2 (conteggio)** In $1, 2, \dots, n$, quante sono circa le potenze perfette?

Saranno al max $\sqrt{n} + \sqrt[3]{n} + \sqrt[4]{n} + \dots + \sqrt[k]{n}$ dove $k = \log_2 n$

Quindi

Numero potenze perfette minori od uguali di $n$ $\leq$ $\boxed{\sqrt{n} \cdot \log_2 n}$

↓ Questo numero è molto minore di $n$, cioè

$$\lim_{n \to +\infty} \frac{\sqrt{n} \cdot \log_2 n}{n} = 0$$

Quindi tra le potenze perfette ci devono essere dei buchi enormi.

Conclusione stile pigeonhole: scelgo $n$ grande tale che $\sqrt{n} \log_2 n \leq \frac{n}{11}$. Ora divido $1, \dots, n$ in

$\frac{n}{10}$ blocchi di 10 interi consecutivi. Almeno 1 blocco non contiene una potenza perfetta.

— o — o —

**IMO 1989-5** Per ogni $n$ esistono $n$ interi consecutivi nessuno dei quali è primo o potenza di un primo.

Prendo $p_1, \dots, p_n, q_1, \dots, q_n$ $2n$ primi distinti e impongo

$$x + i \equiv 0 \pmod{p_i q_i}.$$

— o — o —

# STRUTTURA MOLTIPLICATIVA MODULO $m$

Si riduce facilmente alla struttura modulo $p^k$.

Prendo $(a,m)=1$ e considero $a^0, a^1, a^2, a^3, \dots$
Sono tutte classi coprime con $m$.
Prima poi una classe si ripete (pigeonhole).
Se $a^k \equiv a^R \pmod m$, con wLOG $R<k$, allora

$$a^k - a^R = bm, \text{ cioè } a^R(a^{k-R}-1) = bm$$

Poiché $(a,m)=1$ dovrà essere $a^{k-R}-1 \equiv 0 \pmod m$,
quindi la classe 1 è la prima a ripetersi.

Pongo $\operatorname{ord}_m(a)$ il più piccolo $k$ positivo t.c. $a^k \equiv 1 \pmod m$.

Fatto generale. Se $(a,m)=1$, allora $\operatorname{ord}_m(a) \mid \phi(m)$

Dim Siano $\{x_1, x_2, \dots, x_{\phi(m)}\}$ tutte le classi coprime con $m$
Allora $\{ax_1, ax_2, \dots, ax_{\phi(m)}\}$ sono le stesse classi, eventualmente permutate (se fosse $ax_i \equiv ax_j$ sarebbe $a(x_i - x_j) = bm$, ma ciò può essere perché $(a,m)=1$ e $x_i - x_j$ è troppo piccolo per essere divisibile per $m$).
Quindi

$$x_1 \cdot \dots \cdot x_{\phi(m)} = ax_1 \cdot \dots \cdot ax_{\phi(m)} = a^{\phi(m)} \cdot x_1 \cdot \dots \cdot x_{\phi(m)}$$

Se semplifico $x_1 \cdot \dots \cdot x_{\phi(m)}$ (che è coprimo con $m$) ottengo

$$\boxed{a^{\phi(m)} \equiv 1 \pmod m}$$ estensione del FLT.

Per la periodicità gli esponenti $k$ t.c. $a^k \equiv 1 \pmod m$ sono tutti e soli i multipli dell'ordine, quindi $\phi(m)$ è multiplo di $\operatorname{ord}_m(a)$.

—o—o—

**Teorema di Wilson** Se $p$ è primo, allora $(p-1)! \equiv -1 \ (p)$

**Dim.** $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1)$. Se accoppio ogni termine con il suo inverso il prodotto viene 1. Questo vale per tutti i termini che non sono inversi di se stessi.
Qui è inverso di se stesso? Deve essere $x^2 \equiv 1 \ (p)$, cioè $x^2 - 1 = kp$, cioè $(x+1)(x-1) = kp$, cioè $x = \pm 1 \ (p)$.

— o — o —

**Achtung!** Modulo $m$ non è vero in generale che $x^2 \equiv 1 \ (m)$ ha come soluzioni solo $x \equiv \pm 1 \ (m)$

**Esempio** Risolvere $x^2 \equiv 1 \pmod{40}$

Per il CRT è equivalente a risolvere $\begin{cases} x^2 \equiv 1 \pmod 8 \\ x^2 \equiv 1 \pmod 5 \end{cases}$

$\begin{cases} x \equiv 1, 3, 5, 7 \pmod 8 \\ x \equiv \pm 1 \pmod 5 \end{cases}$ Quindi in totale ho 8 soluzioni.

— o — o —

**GENERATORI** Se $(a, m) = 1$ e $\mathrm{ord}_m(a) = \phi(m)$ si dice che $a$ è un **generatore** modulo $m$.

Questo vuol dire che facendo le potenze di $a$ con esponente che va da 1 a $\phi(m)$ (oppure da 0 a $\phi(m) - 1$) ottengo TUTTE le classi coprime con $m$.

**Teorema** Esiste un generatore se e solo se $m = 2, 4, p^k, 2p^k$ (con $p$ primo dispari e $k \geq 1$).

— o — o —

**Esempi** $-1$ è generatore mod 4, 2 è gen. mod 3, 2 è gen. mod 5, 2 non è generatore mod 7 in quanto $\mathrm{ord}_7 2 = 3$, ma 3 è gen. mod. 7.

— o — o —

**Esercizio** Determinare se 2 è un generatore mod 37.

Considero $\text{ord}_{37}\, 2$. Di sicuro è un divisore di 36. Se non fosse 36, allora dividerebbe o 18 o 12

**Fatto generale** Se $d \mid n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ e $d \neq n$, allora $d \mid \frac{n}{p_i}$ per un qualche $i$.

Quindi se divide 36 e non è 36, allora divide $\frac{36}{2}$ o $\frac{36}{3}$.
Quindi mi basta dimostrare che

$2^{12} \not\equiv 1 \pmod{37}$ e $2^{18} \not\equiv 1 \pmod{37}$

Ora $2^6 = 64 \equiv -10 \pmod{37}$, quindi $2^{12} \equiv 100 \equiv -11 \pmod{37}$

$2^{18} \equiv -1000 \equiv -1 \pmod{37}$

Conseguenza: la congruenza $2^x \equiv a \pmod{37}$ ha soluzione per ogni $(a, 37) = 1$.

— o — o —

Perché non esiste un generatore mod 77? Dovrebbe avere ordine $\phi(77) = \phi(7) \cdot \phi(11) = 60$.
La classe mod 77 dipende da quella mod 7 e mod 11.
Le potenze di un certo $a$ ciclano con periodo 6 mod 7 e periodo 10 mod 11,
quindi di sicuro $a^{30} \equiv 1 \pmod{77}$ per ogni $(a, 77) = 1$.
Quindi per ogni $(a, 77) = 1$ si ha che $\text{ord}_{77}(a) \mid 30$.

**Oss. 1** Esiste sempre un elemento di ordine 30 mod 77.
Basta che sia congruo ad un gen. mod 7 e un gen. mod. 11.

**Oss. 2** Lo stesso ragionamento dice che il massimo ordine modulo un certo $n$ è il m.c.m. delle $\phi$ delle potenze dei primi che compongono $n$.

**Fatto generale** Se $g$ è un generatore mod $p$, allora $g$ oppure $g+p$ è un generatore mod $p^2$.

**Dim.** Devo dimostrare che $\text{ord}_{p^2}(g) = \phi(p^2) = p(p-1)$.
Ora se $g^k \equiv 1 \ (p^2)$, allora $g^k \equiv 1 \ (p)$, quindi $k$ è multiplo di $\text{ord}_p(g) = p-1$ (perché $g$ è gen. mod $p$).
Quindi ho 2 possibilità:
$\text{ord}_{p^2}(g) = p-1$ oppure $\text{ord}_{p^2}(g) = p(p-1)$.
Se sono nel primo caso provo con $g+p$. Lo stesso ragionamento di prima mi porta a dire che
$\text{ord}_{p^2}(g+p) = p-1$ oppure $\text{ord}_{p^2}(g+p) = p(p-1)$
Se fossi nel primo caso vorrebbe dire che

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

$$= g^{p-1} + (p-1)g^{p-2} \cdot p + \text{roba con } p^2$$

↕ perché sono nel 1° caso

$$\equiv 1 - g^{p-2} \pmod{p^2}$$

Questo vorrebbe dire che $g^{p-2} \equiv 0 \pmod{p^2}$, che è assurdo.

—o—o—

**Fatto generale** Se $g$ è generatore mod $p$ e mod $p^2$, allora $g$ è generatore mod $p^k$ per ogni $k \geq 1$.

**Esempio:** 2 è gen. modulo $3^{50}$.

—o—o—

Quanti sono i generatori modulo $p$? Sono $\phi(\phi(p))$.

Sia $g$ un generatore. Ogni altro elemento si scrive come $a = g^k$
Se $(k, p-1) = d > 1$, allora $a$ non è generatore. Infatti

$$a^{\frac{p-1}{d}} = g^{k\frac{p-1}{d}} = g^{\boxed{\frac{k}{d}}(p-1)} = \left[g^{p-1}\right]^{\frac{k}{d}} \equiv 1 \pmod p$$

(intero)

quindi $\operatorname{ord}_p(a) \mid \frac{p-1}{d}$ e quindi è $< p-1$.

Viceversa, se $(k, p-1) = 1$, allora $a = g^k$ è generatore.

Supponiamo che $a^\alpha \equiv 1 \pmod p$. Allora $g^{k\alpha} \equiv 1 \ (p)$.

Allora $k\alpha = b(p-1)$, ma essendo $(k, p-1) = 1$ dovrà essere $p-1 \mid \alpha$, quindi $\alpha \geq p-1$.

— o — o —

Esempio Sia $p = 37$, sia $g$ un generatore mod 37

$$g^0, g^1, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, \dots$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$

$$1 \quad 36 \quad 18 \quad 12 \quad 9 \quad 36 \quad 6 \quad 36 \quad 9 \quad 4 \quad 18 \quad \text{ordini}$$

— o — o —

Esercizio $x^9 \equiv a \pmod{37}$ ha soluzione se e solo se

$$\operatorname{ord}_{37}(a) \mid 4 \iff a^4 \equiv 1 \ (37)$$

In particolare $x^9 \equiv 6 \pmod{37}$ ha sol. perché $6^4 = 36^2 \equiv 1 \ (37)$

— o — o —

Fatto generale Si ha che $-1$ è residuo quadratico mod $p$

$$\iff p \equiv 1 \ (4) \quad \text{oppure } p = 2.$$

Dim. $x^2 \equiv -1 \ (p) \qquad x^4 \equiv 1 \ (p)$

$\Rightarrow \operatorname{ord}_p(x) \mid 4$ e $\operatorname{ord}_p(x)$ non è 1 o 2 se $p \neq 2$

$\Rightarrow \operatorname{ord}_p(x) = 4$

$\Rightarrow 4 \mid p-1$, cioè $p \equiv 1 \ (4)$ (perché $\operatorname{ord} \mid \phi$)

**Fatto generale** Si ha che $x^4 \equiv -1 \pmod p$ ha soluzione $\iff$ $p \equiv 1 \pmod 8$ oppure $p = 2$.

Achtung! Vale solo con i fattori 2.

**Fatto generale** Come sono fatti i primi che dividono $a^2+b^2$?
" " " $a^4+b^4$?
" " " $a^8+b^8$?

O sono primi che dividono $a$ e $b$, oppure sono $\equiv 1 \pmod 4$ nel 1° caso, $\pmod 8$ o $\pmod{16}$ nel 2° e 3° caso.

**Dim.** Sia $p \mid a^2+b^2$, e supponiamo $p \nmid a$ e $p \nmid b$.
Questo dice che

$$a^2 \equiv -b^2 \pmod p$$

Quindi esiste $c$ ($=$ a. inverso di $b$) tale che

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

$\Rightarrow -1$ è residuo quadratico $\Rightarrow$ $p \equiv 1 \pmod 4$.

— o — o —

Esistono $\infty$ primi $\equiv 3 \pmod 4$ Se fossero solo $p_1, \dots, p_n$, prendo

$$4 p_1 \cdot \dots \cdot p_n - 1 \qquad (\equiv 3 \bmod 4 \text{ e ha nuovo primo})$$

Esistono $\infty$ primi $\equiv 1 \pmod 4$. Non basta considerare

$4 p_1 \cdot \dots \cdot p_n + 1$, perché questo ha fattori nuovi che potrebbero essere $\equiv 3 \pmod 4$. Basta però considerare

$$(2 p_1 \cdot \dots \cdot p_n)^2 + 1$$

Essendo $\square + 1$, tutti i suoi fattori primi sono $\equiv 1 \pmod 4$.

— o — o —

**BMO 2009 – 1** $3^x - 5^y = z^2$ $x, y, z$ interi positivi

$z$ è pari. Facendo mod 4: $(-1)^x - 1 \equiv 0 \pmod 4$

$\Rightarrow x$ è pari $\Rightarrow x = 2a$

$$3^{2a} - z^2 = 5^y \Rightarrow (3^a + z)(3^a - z) = 5^y$$

$$\Rightarrow \begin{cases} 3^a + z = 5^{y_1} \\ 3^a - z = 5^{y_2} \end{cases} \Rightarrow 2 \cdot 3^a = 5^{y_1} + 5^{y_2} \Rightarrow$$ il più piccolo esponente $y_2 = 0$

$$\Rightarrow 2 \cdot 3^a = 5^y + 1$$ ($a = y = 1$ è una soluzione)

Prendo mod 9 perchè le cose cambiano quando $a \geq 2$.

$5^y \equiv -1 \pmod 9 \Rightarrow y \equiv 3 \pmod 6$

Quando modulo 7 perchè $\phi(7) = \phi(9)$

Essendo $y \equiv 3 \pmod 6$ ho che $5^y \equiv -1 \pmod 7$, quindi RHS è $\equiv 0 \bmod 7$, mentre LHS $= 2 \cdot 3^a$ non lo è. Quindi no altre soluzioni

Altra soluzione: $5^y \equiv -1 \pmod{3^a}$

$5^{2y} \equiv 1 \pmod{3^a}$

$\Rightarrow \operatorname{ord}_{3^a}(5) \mid 2y$

Ora $\operatorname{ord}_{3^a}(5) = \phi(3^a) = 2 \cdot 3^{a-1}$ (questo perchè 5, essendo generatore mod 9, lo è pure mod $3^a$ per ogni $a$)

$\Rightarrow 2 \cdot 3^{a-1} \mid 2y \Rightarrow 3^{a-1} \mid y$

Quindi $5^y + 1 \geq 5^{3^{a-1}} + 1$ e questo è ben presto molto più grande di $2 \cdot 3^a$

(le disuguaglianze vanno scritte e dimostrate).

— o — o —

# Esercizio FONDAMENTALE (PPP)

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

① Trovare tutti i primi $p \in D$.

$$p \in D \iff 2^p + 1 \equiv 0 \ (p) \overset{FLT}{\iff} 2 + 1 \equiv 0 \ (p) \iff p = 3.$$

② Trovare tutti i $p^k \in D$.

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

Devo vedere per quali $k$ ho che $3^k \mid 2^{3^k} + 1$

$k=1$ $\quad 3 \mid 2^3 + 1$ $\quad$ ok

$k=2$ $\quad 9 \mid 2^9 + 1 = 513$ $\quad$ ok $\qquad 513 = 9 \cdot 57 = 3^3 \cdot 19$

Fatto generale: $3^{k+1} \,\|\, 2^{3^k} + 1$ per ogni $k \geq 0$.

↓ divide esattamente

Induzione: $n = 1$ $\quad$ ok

$n \implies n+1$

$$2^{3^{k+1}} + 1 = \left[2^{3^k}\right]^3 + 1 \qquad a^3 + 1 = (a^2 - a + 1)(a+1)$$

$$= \underbrace{\left(2^{3^k} + 1\right)}_{3^{k+1} \,\|\, \uparrow} \cdot \underbrace{\left(2^{2 \cdot 3^k} - 2^{3^k} + 1\right)}_{\text{devo dim. che } 3 \mid \text{il termine}}$$

Essendo $a \equiv -1 \ (3)$ sarà $a = 3b - 1$, quindi

$$a^2 - a + 1 = (3b-1)^2 - (3b-1) + 1 = 9b^2 - 6b + 1 - 3b + 1 + 1$$
$$= 9b^2 - 9b + 3 \equiv 3 \pmod 9$$

Quindi $3^k \in D$ per ogni $k$.

Fatto ancora più generale Qual è la max potenza di 3 che divide $2^n+1$ ?

Se $n$ è pari, non è nemmeno divisibile per 3.
Se $n$ è dispari lo scrivo come $n = 3^k \cdot d$, con $3 \nmid d$.
Allora la massima potenza è $3^{k+1}$, cioè $d$ è come se non ci fosse. Per dim. si usa la scomposizione $a^d+1 = (a+1)\cdot(\dots)$.

③ Dimostrare che tutti gli elementi di D sono multipli di 3.

Dim. Sia $n \in D$ e sia $p$ il + piccolo primo che divide $n$.

$$n \in D \Leftrightarrow 2^n+1 \equiv 0 \ (n) \Rightarrow 2^n \equiv -1 \ (n)$$
$$\Rightarrow 2^n \equiv -1 \ (p)$$
$$\Rightarrow 2^{2n} \equiv 1 \ (p)$$

$\text{ord}_p(2) \mid 2n$
$\text{ord}_p(2) \mid (p-1)$

Supponiamo per assurdo che $(\text{ord}_p(2), n) = d > 1$.
Allora $d$ dovrebbe dividere sia $n$, sia $(p-1)$, ma questo non è possibile perché $p$ è il PPP.
Quindi $\text{ord}_p(2) = 1$ oppure $\text{ord}_p(2) = 2$

$2 \equiv 1 \ (p)$ NO

$2^2 \equiv 1 \ (p)$ $p = 3$.

④ Determinare tutti gli $n = pq \in D$, con $p$ e $q$ primi distinti

Dim: WLOG $p = 3$, quindi considero $2^{39} \equiv -1 \ (39)$

$2^{39} \equiv -1 \ (3)$ Banale perché 39 è dispari
$2^{39} \equiv -1 \ (q)$ FLT: $2^{39} \equiv 2^3 \equiv -1 \ (q) \Rightarrow q = 3 = p$.

⑤ Determinare tutti gli $n = p^2 q \in D$, con $p$ e $q$ primi dist.

DIM: devo considerare $3p^2$ e $9q$

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

$$2^{9q} \equiv -1 \ (9q) \Rightarrow 2^{9q} \equiv -1 \ (9)$$
$$2^{9q} \equiv -1 \ (q) \overset{FLT}{\Rightarrow} 2^9 \equiv -1 \ (q)$$
$$513 \equiv 0 \ (q)$$

$\Rightarrow q = 19$. Si tratta di verificare che 19 risolve anche la 1ª congruenza, ma questo si fa.

—o— o —

**IMO 1990 – 3** Trovare tutti gli $n \in \mathbb{N}$ t.c. $n^2 \mid 2^n + 1$

Sol. $2^n + 1 \equiv 0 \ (n^2) \Rightarrow 2^n + 1 \equiv 0 \ (n) \Rightarrow n \in D$ di prima
$\Rightarrow n$ è dispari e multiplo di 3, quindi
$n = 3^k \cdot d$, con $3 \nmid d$.
Se $n$ è soluzione del problema, sarebbe

$$(3^k \cdot d)^2 \mid 2^{3^k d} + 1 \quad \Rightarrow \quad 3^{2k} \mid \underbrace{2^{3^k d} + 1}$$

la max potenza di 3 è $3^{k+1}$, quindi per $k \geq 2$ è assurdo.

—o —o —

**IMO 2000 – 5** Dimostrare che l'insieme $D$ di prima contiene elementi $n$ divisibili per 2000 ~~fattori~~ primi

Dim. che esiste un elemento con 3 fattori primi. Con 2 fattori primi abbiamo $9 \cdot 19 = 3^2 \cdot 19$

$$2^{3^3 \cdot 19} + 1 = \left[2^{3^2 \cdot 19}\right]^3 + 1 = \underbrace{\left(2^{3^2 \cdot 19} + 1\right)(\ldots)}_{\text{div. per } 3^4 \cdot 19}$$

# Lemma di guadagno di un primo

$$a^3+1 = (a+1)(a^2-a+1)$$

Tutti i primi che dividono $(a+1)$ dividono anche $(a^3+1)$.
Però $(a^3+1)$ ha un fattore primo in +, tranne nel caso

$$2^3+1 = (2+1)(4-2+1)$$

— o — o —

**IMO 2008-3** Esistono infiniti $n$ per cui $n^2+1$ ha un fattore primo $\geq 2n+\sqrt{2n}$.

Dim. Sia $p$ il fattore. Allora $-1$ è residuo quadratico mod $p$.
Quindi $p \equiv 1 \pmod 4$.

Prendo un qualunque $p \equiv 1 \pmod 4$. So che $n^2 \equiv -1 \ (p)$ ha soluzione, anzi ha 2 soluzioni, di cui una è $n \leq \frac{p-1}{2}$.
Questo da solo dice che $p \geq 2n+1$.
In generale sarà $n = \frac{p-k}{2}$ per un opportuno $k$.

$$n^2+1 \equiv 0 \ (p) \iff \frac{p^2-2pk+k^2}{4} + 1 \equiv 0 \ (p)$$

$$\iff \frac{p^2-2pk+k^2+4}{4} \equiv 0 \ (p)$$

$$\iff k^2+4 \equiv 0 \ (p)$$

$$\implies k^2+4 \geq p$$

$$n = \frac{p-k}{2} \implies p = 2n+k$$

$$k^2+4 \geq p = 2n+k \implies k^2+4-k \geq 2n$$

tolti i casi $k = 1, 2, 3, 4$ abbiamo che

$k^2 \geq k^2+4-k \geq 2n$, quindi $k \geq \sqrt{2n}$ e $p = 2n+k \geq 2n+\sqrt{2n}$.

— o — o —