

# TEORIA DEI NUMERI 2 (MEDIUM)

Titolo nota

07/09/2011

"VIETA - JUMPING"

Per ogni  $m > 0$  esistono infinite coppie  $(x, y)$

tali che  $x \cdot y \mid x^2 + y^2 + m$

$$(x, y) = (1, 1) \quad (m+1, 1)$$

$$x \mid y^2 + m, \quad y \mid x^2 + m$$

$$\frac{x^2 + y^2 + m}{xy} = m+2$$

$$x^2 + y^2 + m - (m+2)xy = 0$$

$$x^2 - x((m+2)y) + (y^2 + m) = 0$$

Per  $y=1$  l'equazione ha la sol  $x=1$

$$\text{Somma radici} = (m+2)y$$

$$(x=m+1, y=1) \\ (1, m+1)$$

$$x^2 - x((m+2)(m+1)) + ((m+1)^2 + m) = 0$$

Soluz.  $x=1$  che conosciamo

$$\text{altra} = (m+2)(m+1) - 1$$

$$(m^2 + 3m + 1, m+1)$$

Idea: se ho una relaz. di 2° grado e conosco una soluzione ne ho subito un'altra

$$\frac{a^2 + b^2}{1 + ab} = k \Rightarrow k \text{ e' un quadrato perfetto} \\ (a, b > 0)$$

Fissiamo  $k$  e supponiamo che  $(a, b)$  sia una soluzione.

$$a^2 + b^2 - k - kab = 0$$

$$a \geq b \quad (\bar{a}, b) \quad \text{con} \quad a \cdot \bar{a} = b^2 - k$$

$$a + \bar{a} = kb$$

$$\bar{a} = \frac{b^2 - k}{a} \leq \frac{a^2 - k}{a} < \frac{a^2}{a} = a$$

Può capitare che  $\bar{a} \leq 0$ ?

$$\text{Se } \bar{a} < 0 \rightarrow k = \frac{\bar{a}^2 + b^2}{1 + \bar{a}b} \Rightarrow k < 0 \quad \text{No}$$

$$\text{Se } \bar{a} = 0 \Rightarrow \frac{b^2 - k}{a} = 0 \Rightarrow \boxed{k = b^2}$$

Supponiamo che  $k$  si scriva  $\frac{a^2 + b^2}{1 + ab}$ .

Esiste una soluzione minima  $(a, b)$

Ma anche  $\left(\frac{b^2 - k}{a}, b\right)$  è soluzione  
e  $\frac{b^2 - k}{a} < a$ . Se  $b^2 - k \neq 0$  ho  
costruito una soluzione + piccola della  
minima, assurdo.

$$4ab - 1 \mid (4a^2 - 1)^2 \Rightarrow a = b$$

$$(4a^2 - 1)^2 \equiv 0 \pmod{4ab - 1}$$

$$(b, 4ab - 1) = 1$$

$$b^2 (4a^2 - 1)^2 \equiv 0 \pmod{4ab - 1}$$

$$(4a^2b - b)^2$$

$$0 \equiv (4a^2b^2 - b^2)^2 \quad \text{boh!}$$

$$4a \equiv 1/b \pmod{4ab - 1}$$

$$0 \equiv (4a^2 - 1)^2 \equiv \left(\frac{a}{b} - 1\right)^2 \pmod{4ab - 1}$$

$$(*) \quad 0 \equiv (a - b)^2 \pmod{4ab - 1}$$

$$\frac{(a - b)^2}{4ab - 1} = k \text{ intero} \quad (\text{Tesi: } k = 0)$$

Domanda: da (\*) non segue  $a \equiv b \pmod{4ab - 1}$ ?

$$4 \mid 6^2$$

$$4 \nmid 6$$

$$(a-b)^2 - k(4ab-1) = 0$$

$$a^2 - a(2b + 4kb) + b^2 + k = 0$$

Prendo  $(a, b)$  soluz. minima  $\uparrow$

$$(\bar{a}, b) \quad 0 < \bar{a} = \frac{b^2 + k}{2k} \leq a$$

$$b^2 + k \leq a^2$$

$$\frac{(a-b)^2}{4ab-1} = k \leq a^2 - b^2 \Leftrightarrow (a-b)^2 \leq (a-b)(a+b)(4ab-1)$$

Se  $a = b$  vale l'uguale

$$\text{Se } a \neq b \quad (a-b > 0) \quad a-b < (a+b)(4ab-1)$$

VERA

La soluz. minima fissato  $k$  deve avere  $a = b$

$$\Rightarrow k = 0 = \frac{(a-b)^2}{\dots}$$

$$\frac{x^2 + y^2 + z^2}{xyz} = k \Rightarrow k = 1 \text{ o } 3$$

$$x = y = z \rightsquigarrow \frac{3x^2}{x^3} = \frac{3}{x} \text{ che dà } 1, 3$$

$$x^2 + y^2 + z^2 = 2xyz$$

Modulo la potenza giusta di 2

$$x^2 + y^2 + z^2 \equiv 0 \pmod{2}$$

$x \equiv y \equiv z \equiv 0$ , esattamente 2 dispari

$\Rightarrow$  c'è un pari

$$x^2 + y^2 + z^2 \equiv 0 \pmod{4}$$

$\Rightarrow$  sono tutti pari

$$x = 2a, y = 2b, z = 2c$$

$$4(a^2 + b^2 + c^2) = \frac{4}{16} abc$$

DISCESA INFINITA!

$$\bullet x^2 + y^2 + z^2 = 2^k xyz$$

$\bullet$  Controllare le valutar. 2-adiche

$$x^2 + y^2 + z^2 - kxyz = 0 \quad (\text{simmetrica})$$

$$x \geq y \geq z$$

Prendo  $(x, y, z)$  soluz.

$$(\bar{x}, y, z)$$

$$x\bar{x} = y^2 + z^2 > 0$$

$$\bar{x} = \frac{y^2 + z^2}{x} \leq \frac{2x^2}{x} = 2x$$

$$x + \bar{x} = kyz$$

$$x, \bar{x} = \frac{1}{2} \left[ kyz \pm \sqrt{(kyz)^2 - 4(y^2 + z^2)} \right]$$

Le cose ci vanno male se  $x$  era la soluz. piccola, cioè se

$$y \leq x = \frac{1}{2} \left[ kyz - \sqrt{\dots} \right]$$

$$\cancel{2y} + \sqrt{(kyz)^2 - 4(y^2 + z^2)} \leq kyz - 2y$$

$$\cancel{(kyz)^2} - 4(y^2 + z^2) \leq \cancel{(kyz)^2} + 4y^2 - 4ky^2z$$

$$ky^2z - z^2 \leq 2y^2$$

$$y^2(kz - 2) \leq z^2$$

$$kz - 2 \leq \left(\frac{z}{y}\right)^2 \leq 1$$

$$\Rightarrow kz \leq 3 \Rightarrow \boxed{k \leq 3}$$

$$\frac{x^2 + y^2 + 1}{xy} = 3$$


---

$$\frac{a^2 + b^2 + c^2 + d^2}{1 + abcd} = n \quad (a, b, c, d > 0)$$

$$n = 2$$

$$a^2 + b^2 + c^2 + d^2 - n - nabcd = 0$$

Gli  $n$  che si rappr. sono (ammesso che esista  
no) tra quelli che fanno andare male VJ

$$(\bar{a}, b, c, d) \quad a \cdot \bar{a} = b^2 + c^2 + d^2 - n$$

$$\bar{a} < a?$$

$$b^2 + c^2 + d^2 - n < a^2 \quad (\text{ok})$$

Altrimenti  $b^2 + c^2 + d^2 \geq a^2 + n$

$b, c, d$  sono "non troppo piccoli" rispetto  
ad  $a$

$$bcd \geq a \quad n = \frac{a^2 + b^2 + c^2 + d^2}{1 + abcd} \leq \frac{4a^2}{1 + a^2} < 4$$

$$a^2 = b^2 + c^2 + d^2 - k, \quad k \geq 2$$

$$bcd \geq \sqrt{b^2 + c^2 + d^2 - 2} \geq \sqrt{b^2 + c^2 + d^2 - k}$$

" OL



$$\Gamma \quad b^2 c^2 d^2 \geq b^2 + c^2 + d^2 - 2$$

$$b^2 (c^2 d^2 - 1) \geq c^2 + d^2 - 2$$

$$\text{Se } c = d \geq 2$$

$$c^2 d^2 - 1 \geq 3$$

$$\exists b^2 + 2 \geq c^2 + d^2$$

$$\perp \text{ Se } c = d = 1$$

$$0 \geq 0 \quad \text{vera}$$

$$0 < \bar{a} < a$$

$$\bar{a} = \frac{b^2 + c^2 + d^2 - n}{0}$$

$$0 < \frac{a^2 + b^2 + c^2 + d^2}{1 + abcd} = n$$

$$0 < \frac{\bar{a}^2 + b^2 + c^2 + d^2}{1 + \bar{a}bcd}$$

$$\bar{a} \geq 0$$

$$\bar{a} = 0$$

$$(\text{succede per } n = b^2 + c^2 + d^2)$$

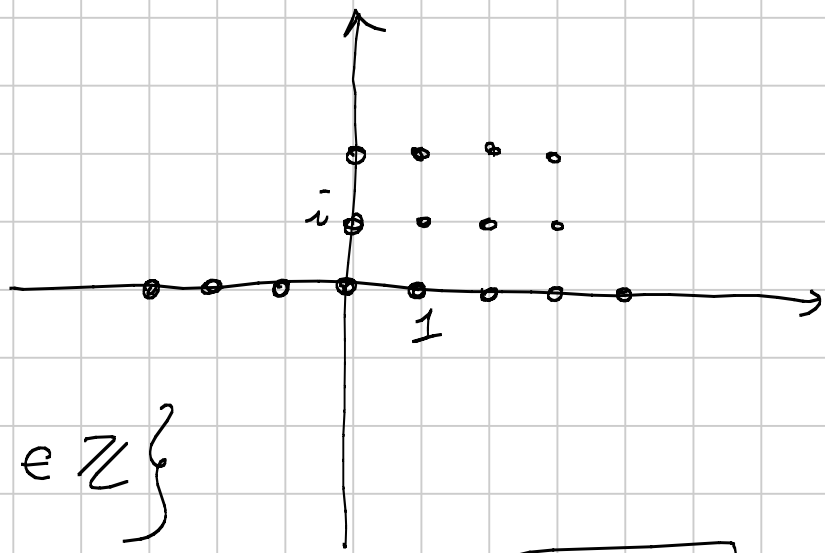
$$\text{Ma: } \bullet n < 4$$

$$\bullet n = b^2 + c^2 + d^2 \quad (b, c, d > 0)$$

Questi n̄ fanno!

# Interoi di Gauss

$$i^2 = -1$$



$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

$$\text{Norma complessa: } N(a + bi) = \sqrt{a^2 + b^2}$$

Si lavora con la norma quadrata

$$N(z_1 \cdot z_2) = N(z_1) N(z_2)$$

$$x^2 + y^2 = (x + iy)(x - iy)$$

In  $\mathbb{Z}[i]$  valgono

- la divisione euclidea
- la fattorizz. unica

Dati  $a$  e  $b \neq 0$   $\exists q, r$  con  $a = bq + r$

con  $N(r) < N(b)$  (o  $r = 0$ )

Primi:  $p = ab \Rightarrow a = p, b = 1$  o vicev.  
(in realtà è la def. di irriducibile)

Vera def.  $p \mid ab \Rightarrow p \mid a$  oppure  $p \mid b$   
(e  $p \neq \pm 1$ )

$$15 = (-3)(-5)$$

$$2 = (1+i) \cdot (1-i) = 1^2 + 1^2$$

$$-i (1+i)^2$$

Invertibili di  $\mathbb{Z} = \{1, -1\}$

Invertibili di  $\mathbb{Z}[i] = \{1, -1, i, -i\}$

$$(1+i) i = (i-1)$$

Sia  $z$  un invertibile. Esiste  $w$  con  $zw=1$

$$\Rightarrow N(zw) = 1$$

$$N(z) \cdot N(w) \Rightarrow N(z) = 1$$

$$z = x+iy \Rightarrow x^2 + y^2 = 1$$

$$5 = (2+i)(2-i)$$

Fatto: i primi di Gauss sono: ( $p = x+iy$ )

→ i primi  $p \in \mathbb{Z}$  con  $p \equiv 3 \pmod{4}$

→  $x^2 + y^2$  e' un numero primo (di  $\mathbb{Z}$ )

IRRIDUC = PRIMI

⊆ Sia  $p$  un primo. per assurdo  $p = a \cdot b$

⇒  $p|a$  oppure  $p|b$ ,  $a = kp$

$$p = kp \cdot b \Rightarrow 1 = k \cdot b$$

$$p = 1 \cdot p = (-1) (-p) = (i) (-ip) = (-i) (ip)$$

$\Rightarrow$  Sia  $p$  un irriducibile,  $p \mid a \cdot b$   
Se  $p \nmid a$  e  $p \nmid b$ ,  $(p, a) = 1$   
 $(p, b) = 1$

$$1 = mp + ha, \quad 1 = np + kb \quad (\text{Bézout})$$

$$1 = 1 \cdot 1 = (mp + ha)(np + kb)$$

$$= mnp^2 + hanp + mbkp + hkab$$

$$\Rightarrow p \mid 1 \quad \text{ASSURDO}$$

Prendiamo  $p \equiv 3 \pmod{4}$  ( $p \in \mathbb{N}$ )

$$0i + p = (a + bi)(c + di)$$

$$(0^2 + p^2) = (a^2 + b^2)(c^2 + d^2)$$

1

$p^2$

$p$

$p$

$p^2$

1

• fatt. falsa

non esiste

• fatt. falsa

$$p = a^2 + b^2$$

(No! Assurdo mod 4)

$p \equiv 1 \pmod{4}$  non sono primi di Gauss

$$\left(\frac{-1}{p}\right) = 1, \text{ esiste } x \in \mathbb{N} \text{ con } x^2 \equiv -1 \pmod{p}$$

$$\Rightarrow p \mid x^2 + 1 = (x+i)(x-i)$$

( $3i$  e' primo = primo vero  $\cdot$  unita')

Se  $p$  e' primo di Gauss,  $p \mid x+i$  (o  $x-i$ )

$$p(a+bi) = x+i \quad pb=1 \quad \underline{\text{NO}}$$

$\leadsto p$  non e' irriducibile  $\Rightarrow p = (a+bi)(c+di)$

$$p^2 = (a^2+b^2)(c^2+d^2)$$

1, p, p<sup>2</sup>

$$\Rightarrow \boxed{p = a^2 + b^2} \quad p = (a+bi)(a-bi)$$

Prendiamo un generico  $z = x + iy$  con  $x^2 + y^2 =$  primo (di  $\mathbb{Z}$ )

$z$  e' un primo di Gauss

$$z = z_1 \cdot z_2 \Rightarrow N(z) = N(z_1) \cdot N(z_2)$$

" p "

$\Rightarrow N(z_1) = 1$ , cioe'  $z_1$  e' un'unita' e la fatt. e' falsa.

(Dimostrare che  $1+i$  e' un primo)

Sia  $p = x + iy$  primo nel senso di Gauss.

$$p \mid x^2 + y^2 = \underbrace{p_1^{a_1} \cdot \dots \cdot p_k^{a_k}}_{\text{primi di } \mathbb{Z}}$$

↑  
primo di Gauss

( Fattorizziamo  $3 + i$ .  $3^2 + 1^2 = 10$

$$10 = (3 + i)(3 - i) = 2 \cdot 5 = (2 + i)(2 - i)(1 + i)(1 - i)$$

$1 + i$  divide  $3 + i$ ?

$$3 + i = 2 + (1 + i)$$

$$= (1 + i)(1 - i) + (1 + i)$$

$$= (1 + i)(2 - i)$$

$$p \mid p_1^{\alpha_1} \dots p_k^{\alpha_k} \Rightarrow p \mid p_1^{\alpha_1} \Rightarrow p \mid p_1$$

norme  $\rightarrow$

$$p_1 = p \cdot z$$

$$p_1^2 = N(p) \cdot N(z)$$

$\downarrow$

$$p_1, p_1^2$$

$p$  è primo  
con norma  
prima

$p = p_1 \in \mathbb{Z}$   
(a meno di unità)



$$p \equiv 1 \pmod{4} \Rightarrow p = a^2 + b^2$$

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

$$(a + bi)(c + di) = (ac - bd) + i(ad + bc)$$

Se  $n = 2^{\alpha} p_1^{\alpha_1} \dots p_k^{\alpha_k}$  con  $p_i \equiv 1 \pmod{4}$   
si rappresenta.

$$p^2 + 0^2. \quad \text{Anche } n = 2^{\alpha} \underbrace{p_1^{\alpha_1} \dots p_k^{\alpha_k}}_{\equiv 1 \pmod{4}} \underbrace{q_1^{2b_1} \dots q_k^{2b_k}}_{\equiv 3 \pmod{4}}$$

Supponiamo  $n = a^2 + b^2$  e sia  $p \mid n$ ,  $p \equiv 3 \pmod{4}$

$$a^2 + b^2 \equiv 0 \pmod{p} \rightarrow p \mid a, p \mid b$$

$$\rightarrow \left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p}$$

$\Downarrow$

$$\text{ord}_p\left(\frac{a}{b}\right) = 4 \mid p - 1$$

ASSURDO

$$a = pa_1, \quad b = pb_1$$

$$\left(\frac{n}{p^2}\right) = a_1^2 + b_1^2$$

$$x^2 + y^2 = z^2$$

$$\parallel \\ (x+iy)(x-iy)$$

$$\text{mcd}(x+iy, x-iy)$$

$$\parallel \\ \text{mcd}(2x, x+iy) = 1$$

$$\text{Se } p \mid 2x \text{ e } p \mid x+iy \begin{array}{l} \nearrow p \mid 2 \\ \searrow p \mid x \Rightarrow p \mid y \end{array}$$

$$x = p(a+bi) \Rightarrow x = \bar{x} = \bar{p} \overline{(a+bi)}$$

$$\overline{a+bi} = a-bi$$

$$\text{Otteniamo } \bar{p} \mid x \quad \underbrace{p\bar{p}}_{\in \mathbb{Z}} \mid x, \quad p\bar{p} \mid y$$

$$1+i \mid x+iy \Rightarrow 1+i \mid (x+iy) - y(1+i) \\ = x-y$$

$$1+i \mid x-y \Rightarrow 1-i \mid x-y \Rightarrow 2 \mid x-y$$

ATTENZIONE

$x, y$  entrambi dispari (assurdo mod 4)

$$x+iy = (m+in)^2 = (m^2-n^2) + i(2mn)$$

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

Abbiamo perso  $x+iy = (m+in)^2 \cdot$  le unità non banali

$$\begin{cases} y^3 - 11^x = 4 \\ x \text{ par} \end{cases} \pmod{5} \quad y^3 - 1 \equiv 4 \pmod{5}$$

$$\Rightarrow y^3 \equiv 0 \pmod{5} \Rightarrow 5 | y$$

$$5^3 - 4 = 121 \quad (x=2, y=5)$$

$$\text{Mod } 25? \quad -11^x \equiv 4 \pmod{25}$$

$$11^x \equiv 11^2 \pmod{25}$$

$$11^{x-2} \equiv 1 \pmod{25}$$

$$11, 11^2 \equiv -4, 11^3 \equiv -44 \equiv 6, 11^4 \equiv 16, 11^5 \equiv 1 \pmod{25}$$

$$y^3 - 11^{2z} = 4$$

$$y^3 = 11^{2z} + 4 = (11^z + 2i)(11^z - 2i)$$

$$\text{mcd}(11^z + 2i, 11^z - 2i) = \text{mcd}(2 \cdot 11^z, 11^z + 2i)$$

$$= \text{mcd}((1+i)(1-i)11^z, 11^z + 2i)$$

$$= \text{mcd}((1+i)(1-i), 11^z + 2i) =$$

$$= \text{mcd}(2, 11^z) = 1$$

$$(11^z + 2i) = (a+bi)^3 \Rightarrow \begin{cases} a^3 - 3ab^2 = 11^z \\ 3a^2b - b^3 = 2 \end{cases}$$

$$2 = b(3a^2 - b^2) \quad b|2$$

$$i = (-i)^3, \quad (-1) = (-1)^3, \quad (-i) = i^3$$

"Stime"

$$\frac{p(n)}{q(n)} \in \mathbb{Z} \text{ per infiniti valori di } n$$

$\Rightarrow q(x) \mid p(x)$  come polinomi

$$p(x) = q(x)r(x) + s(x), \quad \deg s(x) < \deg q(x) \\ \text{oppure } s(x) = 0$$

$$r(x), s(x) \in \mathbb{Z}[x]$$

$$\frac{p(n)}{q(n)} = \underbrace{r(n)}_{\mathbb{Z}} + \frac{s(n)}{q(n)} \in \mathbb{Z} \text{ infinite volte}$$

Per  $n$  molto grande  $\left| \frac{s(n)}{q(n)} \right| < 1$

$$s(x) = x^k + \dots \quad q(x) = x^h + \dots \quad h > k$$

$$\frac{s(n)}{q(n)} = \frac{x^k + \dots}{x^{h-k} (x^k + \dots)} \quad \text{limitata}$$

val  $\rightarrow +\infty$

Perciò  $s(n)/q(n) = 0$  infinite volte  $\Rightarrow s \equiv 0$

$p(n)$  è divisibile per infiniti primi

$$p(x) = a_n x^n + \dots + a_1 x + a_0$$

Caso facile:  $a_0 = 1$ , supponiamo solo finiti

primi  $q_1, \dots, q_k$

$$p(h q_1 \dots q_k) \equiv 1 \pmod{q_i}$$

Puo' capitare sia proprio  $= 1$ , ma al variare di  $h$  non sarà sempre  $= 1$ .

Caso  $a_0$  generico

$$p(a_0 x) =$$

$$= a_0 \left( a_0^{n-1} x^n + \dots + a_1 x + 1 \right)$$

$q_1, \dots, q_k$ . Fissiamo  $M$ .

Tra i numeri  $\leq M$  quanti si fattorizzano solo con i  $q_j$ ?

$$q_1^{a_1} \dots q_k^{a_k} \leq M$$

$$a_1 \leq \log_{q_1} M \leq \log_2 M$$

Sono al più  $(1 + \log_2 M)^k$

Quanti sono i valori assunti dal polin.  $e \leq M$ ?

$$p(x) = a_m x^m + \dots$$

$$x = 0, \dots, l \quad a_m l^m < M \quad l \sim \sqrt[m]{M/a_m}$$

$$l \geq c \cdot M^{1/m}$$

$$c \cdot M^{1/m} < (1 + \log_2 M)^k \quad \forall M$$

$$M = 2^{t \cdot n} \quad c \cdot 2^t < (1 + nt)^k \quad \underline{\underline{\text{NO}}}$$

(CONFRONTARE AMMISSIONE SNS)

---

Dato  $m$ ,

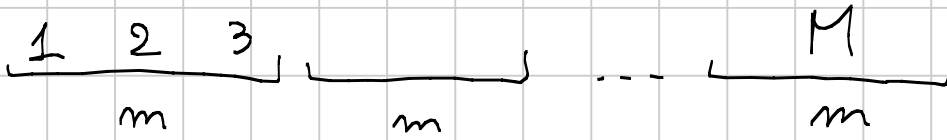
Esistono  $m$  interi consecutivi non della forma

$$a^5 + b^7 + c^{11}$$

Fisso  $M$ .  $\uparrow$  numeri  $\leq M$  quanti sono?

$$a \leq M^{1/5} \quad b \leq M^{1/7} \quad c \leq M^{1/11}$$

Non sono di più di  $M^{1/5} \cdot M^{1/7} \cdot M^{1/11}$ .



$$\text{Cassetti} = M/m$$

$$M \left( \frac{1}{5} + \frac{1}{7} + \frac{1}{11} \right) \stackrel{\alpha < 1}{\geq} \frac{M}{m} \quad \forall M$$

$$m \geq M^{1-\alpha} \quad \forall M \quad \text{per } M \text{ grande e' falsa!}$$

Esistono  $m$  interi cons. non potenze perfette

Fissiamo  $M$ . Le potenze perfette quante

$$\text{Sono?} \leq \sqrt{M} + M^{1/3} + \dots + M^{1/k}$$

$$2^k > M$$

$$k = \log_2 M$$

$$\leq \underbrace{(\log_2 M)}_{\text{n° termini}} \cdot \underbrace{M^{1/2}}_{\text{ogni termine}}$$

Se la tesi fosse falsa,  $M/m \leq M^{1/2} \log_2 M$ , che  
però diventa falsa DEFINITIVAMENTE



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

$$p_1, \dots, p_m$$

$$\left\{ \begin{array}{l} n \equiv p_1 \pmod{p_1^2} \\ n \equiv p_2 \pmod{p_2^2} \\ \vdots \\ n \equiv p_m \pmod{p_m^2} \end{array} \right.$$

$$\left\{ \begin{array}{l} n \equiv p_1 \pmod{p_1^2} \\ n \equiv p_2 \pmod{p_2^2} \\ \vdots \\ n \equiv p_m \pmod{p_m^2} \end{array} \right.$$

$$\left\{ \begin{array}{l} n \equiv p_1 \pmod{p_1^2} \\ n \equiv p_2 \pmod{p_2^2} \\ \vdots \\ n \equiv p_m \pmod{p_m^2} \end{array} \right.$$

TCR  
 $\Rightarrow \exists m$  soluz

Sia  $f: \mathbb{N} \rightarrow \mathbb{N}$  t.c. per ogni coppia  $a, b$

di interi  $a f(a) + 2ab + b f(b)$  è  
un quadr. perf.  $\Rightarrow f(n) = n \quad \forall n$

•  $a = p$  primo,  $b = 0$   $p f(p) = \square$

$$f(p) = p \cdot g(p)^2 \quad p \mid f(p)$$

•  $p f(p) + 2p + f(1) = m^2$

$$p f(p) + 4p + 2f(2) = n^2$$

Supponiamo  $f(p) \neq p \Rightarrow f(p) \geq 2p \Rightarrow m, n \geq \sqrt{2}p$

$$\begin{aligned} 2p + (2f(2) - f(1)) &= n^2 - m^2 \geq (m+1)^2 - m^2 \\ &= 2m+1 \geq 2\sqrt{2}p+1 \end{aligned}$$

Questo è falso per  $p$  abbast. grande.

$\Rightarrow f(p) = p$  per tutti i  $p$  grandi

• Per ogni  $a, p \gg 1$   $a^2 + 2ap + p^2 = \square$

$$a f(a) + 2ap + p^2 = \square$$

$\uparrow$   
 $p \cdot f(p)$

$$a(a - f(a)) = \text{differenza di } \square$$

$\uparrow$   
costante risp.  $p$

Da qui assurdo per  $p \rightarrow \infty$ , perché

$\square - \square$  va a  $+\infty$ , ma  $e^c$  costante.

Esiste una potenza di 2 che, in base 10, contiene le cifre 1372546 (per dire)

$$2^m = 137\dots = 1,37\dots \cdot 10^m$$

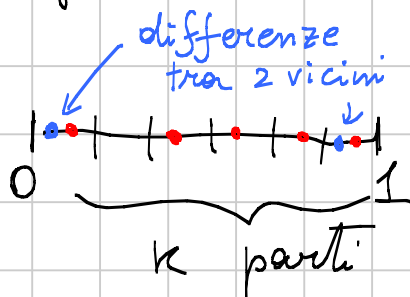
$$m \log_{10} 2 = m + \log_{10} (1,37\dots)$$

$\uparrow$  intero                       $\uparrow$   $0 < \cdot < 1$

Ci interessa  $\{n \cdot \log_{10} 2\} = \log_{10} (1,37\dots)$   
 $\uparrow$  quasi uguale

Con la successione  $\{n \cdot \log_{10} 2\}$  approssimo bene

ogni numero reale.



$\{n \log_{10} 2\}$  per  $k+1$  valori distinti di  $n$

Diciamo che  $m_0$  sia s.t. che  $\{m_0 \log 2\} < 1/k$

$$\{2m_0 \log 2\}, \{3m_0 \log 2\}$$