TEORIA DEI NUMERI MATTUTINA

Titolo nota 30/05/2007

$$2^{x^2-y} = y^2 - x \qquad y \equiv x \ (2)$$

SE $y = x^2$ $\quad 1 = x^4 - x = x(x^3-1)$

SE $x^2 > y$

$$x = \left(y + 2^{\frac{x^2-y}{2}}\right)\left(y - 2^{\frac{x^2-y}{2}}\right)$$

$x, y \geq 0$ $\qquad x < 2^{\frac{x^2-y}{2}} + y$ $\qquad$ PER $x \geq 3$

$y < x$ $\qquad < 2^{\frac{x^2-x}{2}} = 2^{\frac{x(x-1)}{2}}$

SE $x = 3$ $\quad 3 < 2^3$

SE $x > 3$ $\quad x < 2^{\frac{x(x-1)}{2}}$

$x = 2, 1, 0$

$x < 0, \; y \geq 0 \qquad a = |x|$

$$2^{a^2 - y} = y^2 + a$$

$$a = \left(2^{\frac{a^2-y}{2}} + y\right)\left(2^{\frac{a^2-y}{2}} - y\right)$$

$$a < 2^{\frac{a^2-y}{2}} + y \qquad a \geq 3$$

Si $y < x \Rightarrow \quad 2^{\frac{x^2-y}{2}} + y > 2^{\frac{x(x-1)}{2}} > x \qquad \forall\, x \geq 3$

$x \geq 0, \; y < 0 \qquad b = |y|$

$$2^{x^2+b} = b^2 - x$$

$$x = \left(b + 2^{\frac{x^2+b}{2}}\right)\left(b - 2^{\frac{x^2+b}{2}}\right)$$

$x > 0$

$$b + 2^{\frac{x^2+b}{2}} \geq 2^{\frac{x^2}{2}} > x \qquad \forall\, x$$

$x = 0 \qquad b = 2^{\frac{x+b}{2}}$

$b = 2^{\frac{b}{2}}$

$b = 2$

$b = 4$

$(0; -2)$

$(0; -4)$

Si: $x < 0$, $y < 0$, $a = |x|$, $b = |y|$

$$2^{a^2+b} = b^2 + a$$

$$a = \left(2^{\frac{a^2+b}{2}} + b\right)\left(2^{\frac{a^2+b}{2}} - b\right)$$

$$2^{\frac{a^2+b}{2}} + b \geq 2^{\frac{a^2}{2}} > a$$

$$2^n + 5^n = x^2 + 65$$

$$x^2 = 2^n + 5^n - 65$$

n PARI

Se n DISPARI

$$2^n + 5^n = 7 \cdot \text{NOSA}$$

$x^2 + 65 \equiv 0 \pmod 7$

$x^2 \equiv 5 \pmod 7$

ASSURD!

$\therefore$

$$2^{2n} + 5^{2n} - 65 = x^2$$

$n > 3$

5^n $\qquad$ $5^n + 1$

$$(5^n)^2 < 2^{2n} + 5^{2n} - 65$$

$$\Rightarrow$$

$$65 < 2^{2n}$$

$$(5^n + 1)^2 > 2^{2n} + 5^{2n} - 65$$

$$5^{2n} + 1 + 2 \cdot 5^n > 4^n + 5^{2n} - 65$$

$$2 \cdot 5^n + 66 > 4^n \quad \text{VERO}$$

$n = 2$

$x = 24$

$(n, x) = (4, 24)$

① $p^2 + qr = (p+r)^s$

② $p^2 + qt = r^4$

$qt = (r^2 - p)(r^2 + p)$

$r^2 - p = 1 \Rightarrow r^2 = 3$ IMPO

$r = 2 \quad p = 3$

$\left(q = r^2 - p \wedge t = r^2 + p\right) \vee \left(q = r^2 + p \wedge t = r^2 - p\right)$

$r^2 + p = 7$

$q \leq r^2 + p$

① $s \geq 3 \quad (p+r)^s \geq (p+r)^3 = p^3 + 3p^2r + 3pr^2 + r^3$

$> p^2 + pr + r^3 = p^2 + r(r^2 + p)$

$\geq p^2 + rq$

$s = 2 \quad (p+r)^2 = p^2 + qr \Rightarrow p^2 + 2pr + r^2 = p^2 + qr$

$q = 2p + r$

$q = r^2 - p \Rightarrow r(r-1) = 3p \Rightarrow$ **$p=2,\ r=3,\ q=7,\ t=11$** $s=2$

$q = r^2 + p \Rightarrow r(r-1) = p \Rightarrow p = 2 = r \quad q = 6$ NO

---

① $p^2 + qr = (p+r)^s$

② $p^2 + qt = r^4$

$qt = (r^2-p)(r^2+p)$ Se r e p fossero dispari

$p \cdot p \rightarrow$ impossibile

↗ $r = 2$ $\quad (4-p)(4+p) = qt \quad \Rightarrow p = 3$ ... NULLA

↘ $p = 2$ $\quad qt = (r^2-2)(r^2+2)$

q $\quad t$

t $\quad q$

2 generatore mod 5^a

FATTO ogni generatore di p^2 è un generatore di p^a

FATTO 2: g è un generatore mod p, allora g V $(g+p)$ è un generatore mod p^2

J $\quad \ell(J)$ $\quad J \geq K + \ell(J)$ $\quad J \geq \dfrac{K}{1 - \log_{10} 2}$

$2^{\phi(5^{K+\ell(J)}) + J}$ ABBIA ESATTAMENTE

K 0 CONSECUTIVI

$5^{k+\ell(J)} \mid \boxed{2^{\phi(5^{k+\ell(J)})+J} - 2^J}$ $\quad k+\ell(J) \in \mathbb{N}$

$2^{k+\ell(J)} \mid 2^{\phi(5^{k+\ell(J)})+J} - 2^J$

— o — o —

$\frac{2^\alpha}{10^\beta} \overset{\text{Hope!}}{=} 1{,}000\ldots\_9\ldots$

$\frac{2^\alpha}{10^\beta}$ sia >1 e molto vicino a 1

$\frac{2^\alpha}{10^\beta}$ per opportuni α e β

$1+\varepsilon > \boxed{\frac{2^\alpha}{10^\beta} > 1}$

$$\log_{10} \frac{2^\alpha}{10^\beta} \rightsquigarrow 0$$

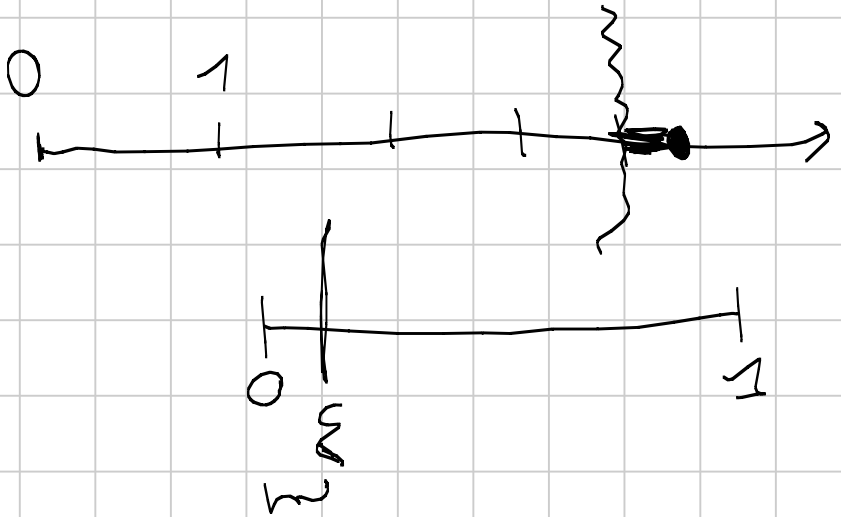
$$\alpha \log_{10} 2 - \beta \rightsquigarrow 0$$

$$0 < \alpha \log_{10} 2 - \beta < \varepsilon$$

$$\alpha \log 2 - \beta$$

$$\{\alpha \log 2\}$$

$$\beta = \lfloor \alpha \log 2 \rfloor$$



$\log 2$ = irrazionale

$10^{\log 2} = 2$

$10^{\beta/9} = 2$

$10^\beta = 2^9$ NO

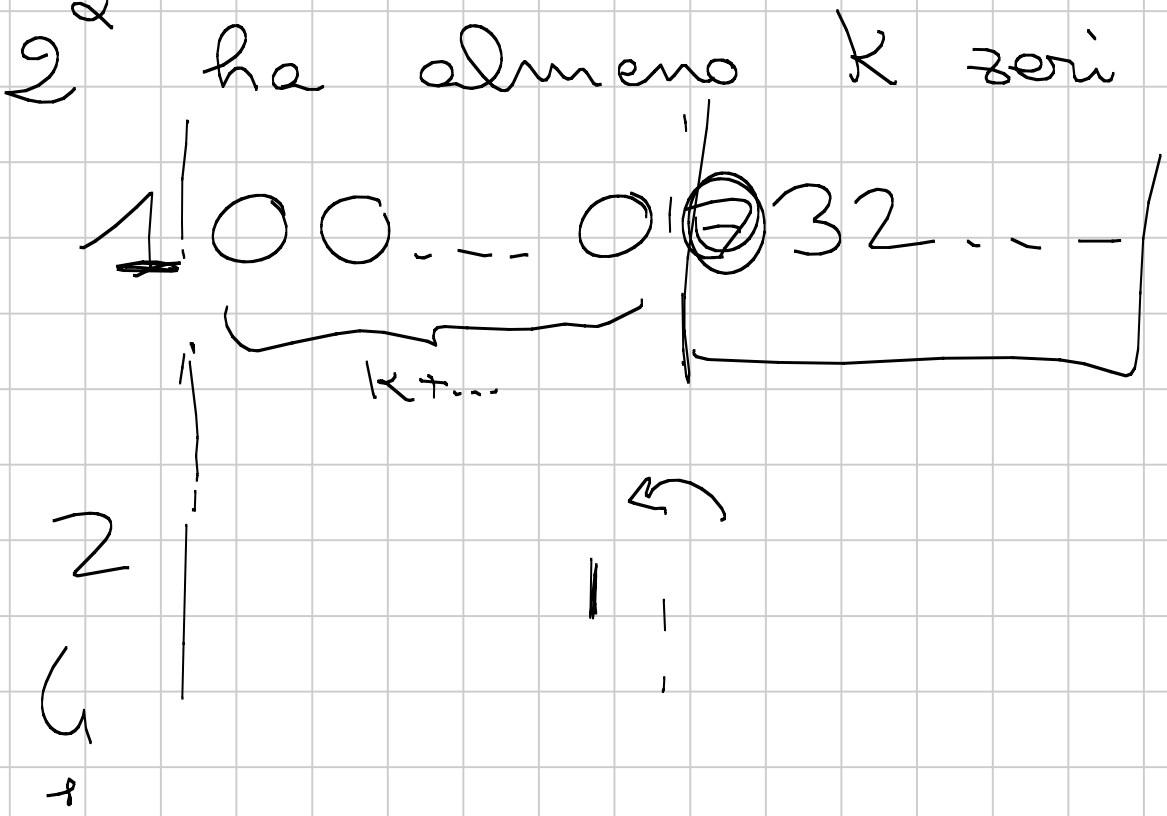
$\{\alpha \log 2\}$

$\alpha_1 \geq \alpha_2$

$\{\alpha_1 \log 2\} - \{\alpha_2 \log 2\}$

$= \{(\alpha_1 - \alpha_2) \log 2\}$

2^α ha almeno k zeri



Basta ottenere almeno k zeri e poi se ne ottengono esattamente k.

1000 zeri $\qquad 2^{7000} = \underbrace{A \ldots\ldots Z}$

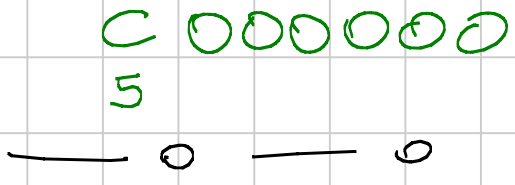
Domanda: esiste m t.c.

$$2^m = \ldots\ldots \underbrace{A \ldots Z}_{2^{7000}}$$

basta fare in modo che $2^m \equiv 2^{7000} \mod (10^{7000})$

$$2^m = \text{ROBA} \,|\, \overbrace{00000\,\underbrace{A \ldots Z}_{2^{7000}}}^{7000 \text{ cifre}}$$

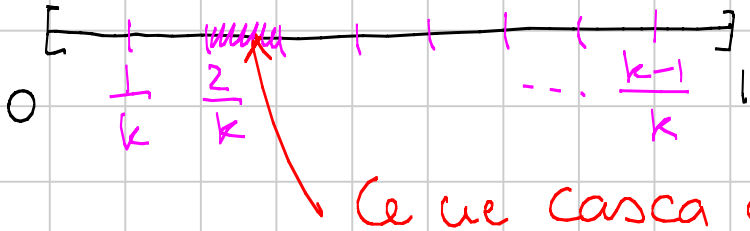
$7000 - 7000 \log_{10} 2$



Consideriamo la successione $\{n \log 2\}$ ← parte frazionaria

↑ >0 ; ↑ irrazionale

Questa è densa in $[0,1]$



Se ne casca almeno uno

1° passo Trovare n_1 ed n_2 t.c. $\{n_1 \log 2\}, \{n_2 \log 2\}$

siano abbastanza vicini

Fissato k $\quad \{0 \log 2\}, \{1 \cdot \log 2\}, \ldots, \{k \cdot \log 2\}$

$k+1$

$\Rightarrow$ ne esistono almeno 2 che cascano nello stesso pezzo

$$\{n \log 2\} - \{m \log 2\} < \frac{1}{k}$$

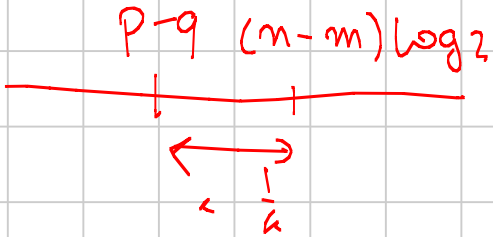
$$(n \log 2 - p) - (m \log 2 - q) < \frac{1}{k}$$

$$(n-m)\log 2 - (p-q) < \frac{1}{k}$$

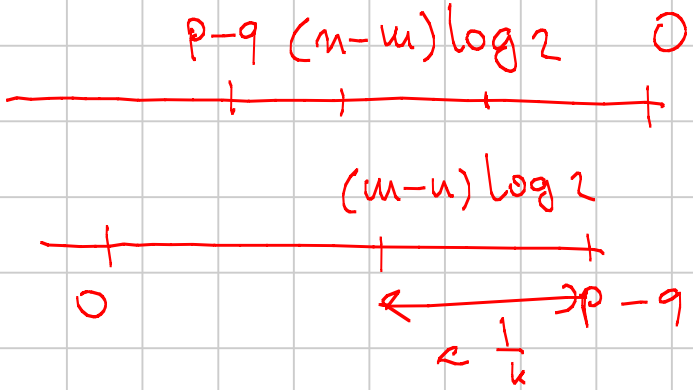
$$\{(n-m)\log 2\}$$

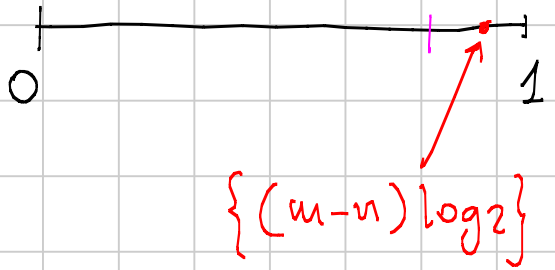
$\{(n-m)\log 2\}$

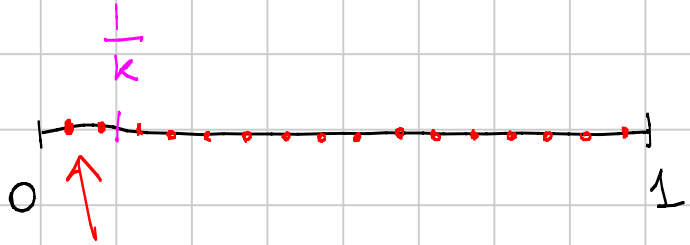
Se $n > m$

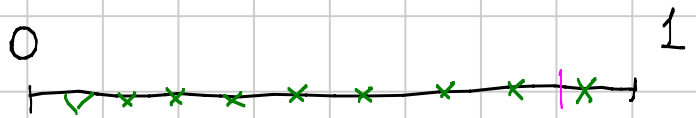


Se $n < m$









$\{n \log 2\}$ $\{2n \log 2\} = 2\{n \log 2\}$

(sinistra)

Conseguenza: fissato un qualunque "inizio"

$\exists\, n$ t.c. 2^n inizia in quel modo

a generatore modulo p^2 $\quad p$ primo $\neq 2$

$\Rightarrow$ a generatore modulo p^n $\quad \forall n \geq 2$

$(\mathbb{Z}/p^n\mathbb{Z})^*$ classi resto prime con p.

(

ciclico se $p \neq 2$ $\forall n$.

$= \{a, a^2, a^3, \ldots, a^{\phi(p^n)} = 1\}$

$a^{\phi(p^2)} = a^{p(p-1)} \equiv 1 \pmod{p^2}$

$a^{p-1} \not\equiv 1 \pmod{p^2}$

$a^{p-1} \equiv 1 + kp \pmod{p^2}$ $\quad k \not\equiv 0 \pmod{p}$

$$(a^{p-1})^n = (1 + kp + \dots)^n = 1 + nkp + \dots$$

$\Downarrow$

n multiple de p ou de p^2

$$\equiv 1 \mod p^2 \iff n \equiv 0 \ (p)$$

$n = p$ $\quad (1 + kp + sp^2)^p = 1 + kp^2 + \dots$

$$a^x \equiv 1 \ (\mod p^n) \qquad a^x \not\equiv 1 \ (\mod p^{n+1})$$

$\Downarrow$

$$a^{xp} \equiv 1 \ (\mod p^{n+1}) \qquad a^x \not\equiv 1 \ (\mod p^{n+1})$$

$$a^x = 1 + kp^n \qquad p \nmid k$$

$$a^{xp} = 1 + kp^{n+1} + \dots$$

$$a^{p-1} = 1 + kp \qquad k \not\equiv 0 \pmod{p}$$

$$a^{(p-1)x} \equiv 1 \pmod{p^2} \quad \Rightarrow \quad p \mid x$$

$$\operatorname{ord} a = p(p-1)$$

$$\downarrow \mod p^2$$

$$\not\equiv 1 \pmod{p^3}$$

$$a^{p(p-1)y} \equiv 1 \pmod{p^3} \qquad p \mid y$$

$$\operatorname{ord}_{p^3} a = p^2(p-1) = \phi(p^3)$$