Titolo nota 30/05/2007

$$2^a = 3^b \cdot 5^c + 7^d$$

$$2^a \equiv 7^d \quad (3)$$

$$2^a \equiv 1 \quad (3)$$

$$2^a \equiv 2^d \quad (5)$$

$a \equiv 0 \quad (2)$

$\| \|$

d

$a = 2a'$

$d = 2d'$

$$(2^{a'} - 7^{d'})(2^{a'} + 7^{d'}) = 3^b \cdot 5^c$$

$$MCD\left(2^{a'} - 7^{d'}, 2^{a'} + 7^{d'}\right) = \left(2^{a'} + 7^{d'}, 2 \cdot 7^{d'}\right) = 1$$

$$2^{a'} = 7^{d'} + 1$$

$$2^{a'} \equiv \underline{1} \quad (7)$$

2

$$8^m = (7+1)\left(7^{d'-1} - 7^{d'-2} + \dots + 1\right)$$

d' = 1 4 1

$e' = 3$

$$\begin{cases} 2^{e'} - 7^{d'} = 3^b \\ 2^{e'} + 7^{d'} = 5^c \end{cases}$$

$$\begin{cases} 2^{e'} - 7^{d'} = 5^e \\ 2^{e'} + 7^{d'} = 3^e \end{cases}$$

$$2^{e'+1} = 5^{\cancel{e}} + 3^b$$

$$2 = 2^c \quad (3)$$

$\operatorname{ord}_7(2) = 3$

$e = 6$
$d = 2$

$$2^{e'} - 1 \equiv 0 \quad (3)$$

e' pari
d' pari

$$2^{e'} + 1 \equiv 0 \quad (3)$$

e' dispari
$e'+1$ pari

$$(2^k - 5^c)(2^k + 5^c) = 3^b$$

$$2^k - 5^c = \underline{1}$$

$$16^l - 1 = 5^e$$

$$(2^l - 1)(2^l + 1)(4^l + 1) = 5^c$$

$$\frac{2^m a^m - (a+b)^m - (a-b)^m}{3a^2+b^2}$$

intero $\forall a,b \in \mathbb{Z} \neq (0,0)$

$\boxed{a=1}$

$$\frac{2^m - (1+b)^m - (1-b)^m}{3+b^2}$$

intero $\forall b$

Fatto generale: $\frac{P(x)}{q(x)} \in \mathbb{Z}$ per infiniti valori di x

$\Updownarrow$

$P(x) = q(x) \cdot r(x)$

$P(x)$ è divisibile per $q(x)$ $\Leftrightarrow$ le radici di $q(x)$ sono radici di $P(x)$ con almeno stessa molteplicità

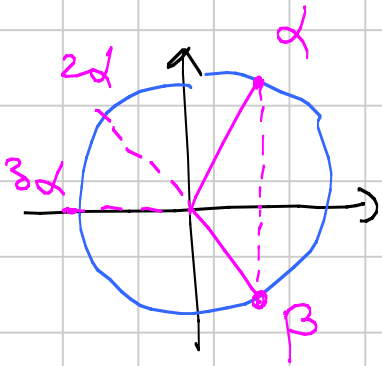
Nel nostro caso $\sqrt{3}\,i$ deve essere radice del num.

$$\frac{2^m - (1+b)^m - (1-b)^m}{3+b^2}$$

$$2^m - (1+\sqrt{3}\,i)^m - (1-\sqrt{3}\,i)^m = 0$$

$$\left(\frac{1+\sqrt{3}\,i}{2}\right)^m + \left(\frac{1-\sqrt{3}\,i}{2}\right)^m = 1$$

α $\qquad$ β



$\searrow$ periodica di periodo 6

$m = 1 \Rightarrow$ vero

$m = 1$
$m = 5$

$m \equiv 1 \pmod 6$
$m \equiv 5 \pmod 6$

Idea per il viceversa (che va fatto)

$p(x)$ è multiplo di $q(x)$

$p\left(\frac{a}{b}\right)$ è multiplo di $q\left(\frac{a}{b}\right)$

— o — o —

$$\frac{x^7-1}{x-1} = y^5 - 1$$

No soluzioni intere

Idea: trovare un primo p t.c.

$p \mid$ RHS e $p \nmid$ LHS (o viceversa)

FATTO GENERALE: come sono fatti i primi che dividono il LHS: $\longrightarrow 7$

$\searrow p \equiv 1 \pmod 7$

Supponiamo che $7 \mid LHS \Rightarrow 7 \mid RHS$

$\Downarrow$

$y^5 - 1 = (y-1)(y^4+y^3+y^2+y+1) \Leftarrow y \equiv 1 \pmod 7$

$\equiv 0 \ (7)$

$\equiv 5 \pmod 7$

ma i primi che lo dividono, dividono pure il LHS, quindi sono o 7 o $\equiv 1 \ (7)$

ASSURDO

La potenza 5^a è iniettiva mod 7

$x^5 \equiv x^{-1} \pmod 7$

Supponiamo che $7 \nmid LHS \Rightarrow LHS \equiv 1 \ (7)$

$\Downarrow$

$$RHS \equiv 1 \quad (7)$$

$$\Downarrow$$

$$y^{-1} \equiv y^5 \equiv 2 \ (7) \quad \Leftarrow \quad y^5 - 1 \equiv 1 \quad (7)$$

$$\Downarrow$$

$$y \equiv 4 \ (7)$$

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

$3 \bmod 7 \Rightarrow$ contiene un primo $\not\equiv 1 \ (7)$

ASSURDO

$$p \mid \frac{x^7-1}{x-1} \implies p \mid x^7-1 \implies x^7 \equiv 1 \quad (p)$$

$$\Downarrow$$

$$\mathrm{ord}_p(x) \mid 7$$

$$\Downarrow$$

$$\mathrm{ord}_p(x) = \begin{cases} 1 \implies x \equiv 1 \ (p) \\ 7 \implies 7 \mid p-1 \implies p \equiv 1 \ (7) \end{cases}$$

$$x^7-1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1) \implies p=7$$

qui c'è p

questo è multiplo di p

$1+1+1+\cdots+1 = 7 \equiv 0 \ (p)$

Se $7 \mid \frac{x^7-1}{x-1}$, allora $\frac{x^7-1}{x-1} \equiv 7 \quad (49)$

$\Downarrow$

$x \equiv 1 \quad (7) \implies x = 1+7k$

$x^6 + x^5 + \dots x^2 + x + 1 =$

$\uparrow \qquad \uparrow \qquad \uparrow$

$1+14k+49k^2 \quad 1+7k \quad 1$

$\Downarrow$

$7 + 7k\,(1+2+3+\dots+6) + 49k^2 \cdot \text{roba}$

$\uparrow \quad \frac{7 \cdot 6}{2}$

$\equiv 0 \quad (49)$

$$\frac{a^2+b^2+1}{ab} \in \mathbb{Z} \quad \Rightarrow \quad m=3$$

$$a^2 - mab + b^2 + 1 = 0$$

$a = b$ $\qquad 2a^2 - ma^2 + 1 = 0$

$$3 - m + 1 = 0 \qquad m = 3$$

(a_0, b_0) $\qquad a_0$ e sol. de

$$X^2 - mXb_0 + b_0^2 + 1 = 0$$

$a_0 > b_0$ $\qquad (a_1, b_0)$

$$a_1 + a_0 = mb_0 \qquad a_1 a_0 = b_0^2 + 1$$

$$a_1 = mb_0 - a_0$$

$$a_1 < b_0$$

$(a_0, b_0) \to (a_1, b_1) \to (a_2, b_2)$

$a_0 > b_0$ $\quad a_1 < b_0$ $\quad a_2 > b_1$

$$a^2 + 0 + b^2 + 1 = 0$$

$(a, b) = (1, 1)$

$$a^2 - 3a + 2 = 0$$

$a = 1, \quad a = 2$

$$a^2 - 3ab + b^2 + 1 = 0$$

$(2, 1) \to (2, b') \to (a', b')$

$$a^m b^n = (a+b)^2 + 1 = a^2 + b^2 + 1 + 2ab$$

$$a^2 + b^2 + 1 = ab(\underbrace{a^{m-1} b^{n-1}}_{\| \; 3} - 2)$$

$a^{m-1} b^{n-1} = 5$

$a^{m-1} = 1$ $\quad b^{n-1} = 5$ $\quad b = 5 \quad n = 2$

$m - 1 = 0$

$a = 1 \quad m = 1$

$25a = (a+5)^2 + 1$

$a^2 - 15a + 26 = 0$

$a = 2 \quad a = 13$

$$a^m = (a+b)^2 + 1$$

$a^m = x^2 + 1$ $\quad x = pori$ $\quad 2 \mid\mid a^m$

$a^m = (x+i)(x-i)$

$(x+i, x-i) \mid 2$ $\quad x = 2y$ $\quad (2y+i, 2) = i = 1$

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

$|1+i| = 2 \;/\; |x+i| = x^2+1$

$$x+i = (b+ic)^m \qquad x-i = (b-ic)^m$$

$c = \pm 1$

b è pari perché altrimenti $1+i \mid x+i$ NO

Considero la parte immaginaria

$$1 = \pm m \pm \binom{m}{2} b^2 \pm \binom{m}{4} b^4 \pm \dots \pm \binom{m}{m-1} b^{m-1}$$

$\mod 4 \quad 1 \equiv 1$

$2^a \| b$

$$v_2\left(\binom{m}{2} b^2\right) < v_2\left(\binom{m}{2k} b^{2k}\right)$$