# PREIMO 2011 - TEORIA DEI NUMERI - M

Titolo nota 26/05/2011

## Esercizio 1

$$pq \mid 5^p + 5^q$$

1° caso: $p = 2$

$$q \mid 2q \mid 5^2 + 5^q$$

$$q \mid 5^q - 5 \quad \Rightarrow \quad q \mid 5^2 + 5 = 30$$

$q = 2, 3, 5$

↓

NO

2° caso: $p = 5$

$$q \mid 5q \mid 5^5 + 5^q \quad \Rightarrow \quad q \mid 5^5 + 5 = 3130$$

$$= 2 \cdot 5 \cdot 313$$

| | | |
|---|---|---|
| ok | ok | ok |

$$p, q \notin \{2, 5\}$$

$$pq \mid 5^p + 5^q = 5\left(5^{p-1} + 5^{q-1}\right)$$

$$pq \mid 5^{p-1} + 5^{q-1}$$

mod $p$ $\quad 5^{p-1} \equiv 1 \quad 5^{q-1} \equiv -1$

mod $q$ $\quad 5^{p-1} \equiv -1 \quad 5^{q-1} \equiv 1$

$p - 1 = 2^a d$, dispari

$q-1 = 2^b d'$, $d'$ dispari

Supponiamo $a \le b$

$$5^{2^b d'} \begin{cases} = 5^{k(p-1)} \equiv 1 & (\text{mod } p) \\ \equiv (-1)^d \equiv -1 & (\text{mod } p) \end{cases}$$

## Esercizio 2

$2^n \equiv n \pmod m$ si risolve

Induzione su $m$

$n = 2^k$ $\qquad 2^{2^k} \equiv 2^k \pmod m$

- $m$ dispari $\qquad 2^k \equiv k \pmod{\varphi(m)}$

$$2^k = a\varphi(m) + r, \quad k = b\varphi(m) + r$$

$$2^{2^k} \equiv 2^{a\varphi(m)+r} \equiv 2^r \equiv 2^{b\varphi(m)+r} \pmod m$$

- $m$ pari $\quad m = 2^e \cdot d$

$$2^{2^k} \equiv 2^k \pmod{d}$$

$$(0 \equiv)\ 2^{2^k} \equiv 2^k \pmod{2^e} \qquad \text{(TCR)}$$

$$2^k > k \geq e$$

$$k \rightsquigarrow k + m\varphi(m)$$

---

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

$$2,\ 2^2,\ \underbrace{2^{2^2}},\ \underbrace{2^{2^{2^2}}},\ \ldots \qquad \left[k^{k^{k}} \ldots\right]$$

$$\equiv \pmod{m}$$

$m = 2^e \cdot d$ Induzione su $m$

$2^{2^{\cdots}}$ si stabilizza mod $\varphi(m)$

$$2^{\left(2^{\cdots}\right)} \equiv 2^{\cdots} \pmod{m}$$

2ª SOLUZIONE

$\forall m\ \exists n$ t.c. $2^n \equiv n \pmod{m}$

$n$ primo $\neq 2$

$$2^{(n-1)^2} \equiv (n-1)^2 \pmod{n}$$

$n = p^2$ con $p$ primo

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

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

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

$$-kp(p-1)$$

---

Prendo $n$ generico

definisco $M = \text{n.c.m}\{n, \varphi(n), \varphi\varphi(n), \varphi\varphi\varphi(n) \dots\}$

$M = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ $\quad p_1 < p_2 < \dots < p_k$

definisco $b_1, b_2, \dots, b_{\Sigma \alpha_i}$

$b_1 = p_1 \quad b_2 = p_1^2 \quad b_3 = p_1^3, \dots, b_{\alpha_1} = p_1^{\alpha_1} \quad b_{\alpha_1+1} = p_1^{\alpha_1} p_2$

ogni volta aggiungo un primo.

Per $b_1 = p_1$ già fatto. P.B.

P.I. esiste $n$ per $b_j \Rightarrow$ esiste $n$ per $b_{j+1}$

$\varphi(b_{j+1}) \mid b_j$ perché?

2 CASI: $b_{j+1} = b_j \cdot p_h$ e $p_h \nmid b_j$

$b_j = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_{h-1}^{\alpha_{h-1}}$

$b_{j+1} = b_j \cdot p_h$

$\varphi(b_{j+1}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \dots \cdot \varphi(p_{h-1}^{\alpha_{h-1}}) \cdot \varphi(p_h)$

$\varphi(b_{j+1})$ contiene solo primi $< p_h$

quindi $\varphi(b_{j+n}) \mid b_j \iff \varphi(b_{j+1}) \mid M$

$\varphi(M) \mid M \longrightarrow \varphi(b_{j+n}) \mid M$

$\varphi(M) \mid M$ se $p^k \| \varphi(M)$.

PURTROPPO È FALSO E LA DIMOSTRAZIONE SALTA.

$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}$

$0 < a < 1 \qquad a \in \mathbb{R}$

$a^x = x \qquad a^{a^x} = x \qquad a^{a^{a^x}} = x$

$x = \lim a^{a^{a^{\dots}}}$

PROBL 3

PER QUALI $n$ $\exists x, y$ disp:

$$x^2 + 7y^2 = 2^n$$

$$\mathbb{Z}[\sqrt{-7}] = \{ a + b\sqrt{-7} \mid a, b \text{ INTERI} \}$$

$$(x + \sqrt{-7}\, y)(x - \sqrt{-7}\, y) = 2^n$$

$$(1 + \sqrt{-7})(1 - \sqrt{-7}) = 8$$

$$(1 + \sqrt{-7})^2 = 1 - 7 + 2\sqrt{-7} = 2(-3 + \sqrt{-7})$$

$$\mathbb{Z}\left[\frac{1 + \sqrt{-7}}{2}\right] = \left\{ a + b\,\frac{1+\sqrt{-7}}{2} \;\middle|\; a, b \text{ INT.} \right\}$$

$$\jmath = \frac{1 + \sqrt{-7}}{2} \qquad (2\jmath - 1)^2 + 7 = 0$$

$$4\jmath^2 - 4\jmath + 8 = 0$$

$$\bar{\jmath} = \frac{1 - \sqrt{-7}}{2} \qquad \jmath^2 - \jmath + 2 = 0 \qquad \jmath^2 = \jmath - 2$$

$$(a + b\jmath)(c + d\jmath) = ac + (bc + da)\jmath + bd\jmath^2 =$$

$$= ac + (bc + da)\jmath + bd(\jmath - 2)$$

$$\jmath\bar{\jmath} = 2$$

$$\jmath^n \bar{\jmath}^n = 2^n$$

$\varepsilon^n = a + b\varepsilon \qquad \bar{\varepsilon}^n = a + b\bar{\varepsilon}$

$(a+b\varepsilon)(a+b\bar{\varepsilon}) = 2^n$

$\left(a + b\,\frac{1+\sqrt{-7}}{2}\right)\left(a + b\,\frac{1-\sqrt{-7}}{2}\right) = 2^n$

$\left(a + \frac{b}{2} + \frac{b}{2}\sqrt{-7}\right)\left(a + \frac{b}{2} - \frac{b}{2}\sqrt{-7}\right) = 2^n$

$\left(2a + b + b\sqrt{-7}\right)\cdot\left(2a + b - b\sqrt{-7}\right) = 2^{n+2}$

$\varepsilon^n = a + b\varepsilon$

$\mathbb{Z}[\varepsilon]$ È EUCL. $\Rightarrow$ UFD

$\varepsilon \mid a+b\varepsilon \Rightarrow \varepsilon \mid a \qquad \bar{\varepsilon} \mid a \qquad 2 \mid a.$

$2 \mid b\,?$ $\qquad 2 \mid a+b\varepsilon \qquad 2 \mid \varepsilon^n \Rightarrow \bar{\varepsilon} \mid \varepsilon^n$

ASSURDO.

$\varepsilon + \bar{\varepsilon} = 1 \qquad (\varepsilon, \bar{\varepsilon}) = 1$

$2^{n+2} \qquad n > 0$ $\qquad$ ABBIAMO VINTO

$a + b\varepsilon = \varepsilon^n \qquad a + b\bar{\varepsilon} = \bar{\varepsilon}^n$

$\underbrace{2a + b}_{x_n} = \varepsilon^n + \bar{\varepsilon}^n \qquad b(\varepsilon - \bar{\varepsilon}) = \varepsilon^n - \bar{\varepsilon}^n$

$\underbrace{b}_{y_n} = \frac{\varepsilon^n - \bar{\varepsilon}^n}{\varepsilon - \bar{\varepsilon}}.$

$$(1+\sqrt{-7})^n (1-\sqrt{-7})^n = 8^n = 2^{3n}$$

$$x_n + y_n\sqrt{-7} = (1+\sqrt{-7})^n$$

$$x_n = 2^{n-1} a_n \qquad y_n = 2^{n-1} b_n$$

$a_n, b_n$ dispari $\qquad a_n \equiv b_n \pmod 4$

$$x_{n+1} + y_{n+1}\sqrt{-7} = (x_n + y_n\sqrt{-7})(1+\sqrt{-7})$$

$$x_{n+1} = x_n - 7y_n \qquad y_{n+1} = x_n + y_n$$

$$= 2^{n-1} a_n - 2^{n-1} \cdot 7 b_n$$

$$\frac{(1+\sqrt{-7})^n}{2^{n-1}} \cdot \frac{(1-\sqrt{-7})^n}{2^{n-1}} = \frac{2^{3n}}{2^{2n-2}} = 2^{n+2}$$

## Esercizio 4

$$5^n - 3^m = a^2$$

$5^n \equiv a^2 \pmod 3 \quad \Rightarrow \quad n = 2k$ è pari

$$5^{2k} - a^2 = 3^m$$

$$(5^k + a)(5^k - a) = 3^m$$

$d \mid 5^k + a \quad d \mid 5^k - a \quad \Rightarrow \quad d \mid 2 \cdot 5^k \quad d \mid 2a$

$$5^k + a = 3^m \qquad 5^k - a = 1$$

$$2 \cdot 5^k = 3^m + 1$$

Congruenza mod 5 $\quad m \equiv 2 \pmod 4$

$m = 2d$ $d$ dispari

dimostro per 10 $\quad 5^{k-1} = \dfrac{g^d + 1}{g+1} = g^{d-1} - g^{d-2} + g^{d-3} \ldots + 1$

$\downarrow$

$0 \quad \equiv 1 + 1 + \ldots + 1 = d$

$\dfrac{g^{5d'} + 1}{g+1}$ è divisibile per $\dfrac{g^5+1}{g+1} = 5$ per

$= 5 \cdot 1181$

$$2 \cdot 5^k = 3^m + 1$$

$5 \| 3^2 + 1 \qquad m = 2s$

$3^{2s} + 1 \qquad 3^2 = 2 \cdot 5 - 1$

$3^{2s} = 2^{2s} 5^{2s} \quad 5^2 5^2 + 2s \cdot 5 - 1$

$4$

$3^m \geq 3^{2 \cdot 5^{k-1}}$