# TEORIA DEI NUMERI (WC 2014)

Titolo nota 29/01/2014

N4. Trovare $k$ t.c.

$$p_1 p_2 \cdots p_k = a^b + 1 \qquad b \geq 2$$

* Se $b$ è pari, RHS è una somma di quadrati. Ma $3 \mid c^2 + d^2 \iff 3 \mid c,\ 3 \mid d$; siccome nel nostro caso $d = 1$ non ci sono soluzioni

* I fattori primi di $a$ sono $> p_k$ (oppure 2)

* Escludiamo 2: per $k \geq 3$ abbiamo che $7 \mid a^b + 1$; se $a$ fosse una potenza di 2, e siccome $2 = 3^2 \pmod 7$, abbiamo che

$$7 \mid \square + 1 \qquad \text{ASSURDO}$$

* Sia $q$ un divisore primo di $b$, $b = qn$

$$p_1 \cdots p_k = a^{qn} + 1$$

Supponiamo che $q \leq p_k$. Allora $\text{LHS} \equiv 0 \pmod q$, quindi $0 \equiv 1 + (a^n)^q \equiv 1 + a^n \pmod q$

* In particolare, $v_q(1 + a^b) = v_q(a^n + 1) + v_q(q) \geq 2$

e questo contraddice il fatto che LHS è prodotto di primi distinti

* Quindi: $\begin{cases} a \text{ non è una potenza di } 2 \\ \text{i fattori primi dispari di } a \geq p_k \end{cases}$

$\Rightarrow a \geq p_k$

$b \geq p_k$

$RHS \geq p_k^{p_k} + 1 \geq p_k^{k} + 1 > LHS$ (ASSURDO)

LEMMA LTE $p$ primo dispari, $p \mid x-1$

Allora $v_p(x^n - 1) = v_p(x-1) + v_p(n)$

⚠ $p=2$

N5. $(a + b\sqrt{2})^{2n} = a_n + b_n\sqrt{2}$

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

$p=2$: a mano.

Lavoriamo con $b_n$ modulo $p$, anzi: con l'espressione a numeratore (stiamo cercando $b_n \equiv 0 \ (p)$)

Supponiamo che esista un $m$ : $m^2 \equiv 2 \pmod p$

$$(a+b\sqrt{2})^{2n} \equiv (a-b\sqrt{2})^{2n} \quad (p)$$

**Speranza:** per $n = \frac{p-1}{2}$ entrambi i membri fanno 1 (o zero, se la base era zero)

1° caso: esattamente uno dei due è zero modulo $p$, diciamo $a - b\sqrt{2} \equiv 0 \ (p)$

$$\Rightarrow \quad a \equiv b\sqrt{2} \quad (p)$$

$$\Rightarrow \quad a^2 \equiv 2b^2 \quad (p)$$

2° caso: entrambi zero mod $p$

$$a + b\sqrt{2} \equiv 0 \quad (p)$$
$$\cdot \ a - b\sqrt{2} \equiv 0 \quad (p)$$

$$2a \equiv 0 \ (p) \qquad 2b\sqrt{2} \equiv 0 \ (p)$$

$$\Rightarrow \quad a \equiv b \equiv 0 \pmod p$$

(contraddice l'ipotesi)

3° caso: $a \pm b\sqrt{2} \not\equiv 0 \ (p) \Rightarrow$ posso prendere $n = \frac{p-1}{2}$ (entrambi i membri fanno 1)

**Senza barare:**

$$2 \cdot \sum_{k \equiv 1 (2)} \binom{2n}{k} a^k (\sqrt{2}b)^{2n-k} = 2\sqrt{2}\, b_n$$

$$\frac{1}{\sqrt{2}} \sum_{j=0}^{n-1} \binom{2n}{2j+1} a^{2j+1} b^{2n-2j-1} \sqrt{2}^{2n-2j-1} = \sqrt{2} b_n$$

$$\sum_{j} \binom{2n}{2j+1} a^{2j+1} b^{2n-2j-1} 2^{n-j-1} = b_n$$

Questa espressione la posso guardare mod p, sostituire $2 \equiv m^2$ e finire come sopra

**Soluzione:** $n = \frac{p-1}{2}$

Supponiamo adesso che $m^2 \equiv 2 \pmod p$ non abbia soluzioni.

$$(a+b\sqrt{2})^{2n} \equiv (a-b\sqrt{2})^{2n} \pmod p$$

**Euristica:** voglio $n$ piccolo

$$n \mid (p+1)(p-1)$$

$p-1$ non funzionerà

Proviamo $n = \frac{p+1}{2}$.

$$\begin{aligned}(a+b\sqrt{2})^{p+1} &= (a+b\sqrt{2})^{p}(a+b\sqrt{2}) \\ &= (a^p + b^p \sqrt{2}^{p-1} \cdot \sqrt{2})(a+b\sqrt{2}) \\ &= (a + b \cdot 2^{\frac{p-1}{2}} \cdot \sqrt{2})(a+b\sqrt{2})\end{aligned}$$

$2^{\frac{p-1}{2}} \equiv -1 \ (p)$ Eulero $\longrightarrow \equiv (a - b\sqrt{2})(a+b\sqrt{2})$

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

Per fare il conto, si usa che $\binom{p+1}{k} \equiv 0 \ (p)$

per $2 \le k \le p-1$

N6. $m^6 = n^{n+1} + n - 1$

Prime osservazioni
- $m^6 = a^2 +$ cose piccole
  lo so risolvere
- lo stesso per $m^6 = b^3 +$ c.p.

Se $n$ è dispari, voglio stringere RHS tra due quadrati:

$RHS > \left(n^{\frac{n+1}{2}}\right)^2$

$RHS < \left(n^{\frac{n+1}{2}} + 1\right)^2$

$n$ dispari $(n \neq 1) \Rightarrow$ no soluzioni

Stessa conclusione se $n \equiv 2 \mod 3$

stringendo RHS tra due cubi

Se $n \equiv 0 \ (3)$, $RHS \equiv -1 \ (3)$, il che è assurdo perché dà $m^6 \equiv -1 \ (3)$

Se esistono soluzioni con $n \neq 1$, $n \equiv 4 \ (6)$

$$m^6 \equiv n^{n+1} + n - 1 \pmod{(n+1)}$$

$$\equiv (-1)^{n+1} - 1 - 1 \equiv -3 \pmod{(n+1)}$$

$n+1 \equiv 5 \pmod 6 \Rightarrow$ $n+1$ ha un fattore primo $\equiv 2 \bmod 3$ e $\neq 2$. Chiamando $p$.

Sappiamo $1 = \left(\frac{-3}{p}\right) = \left(\frac{p}{-3}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$

(Rec. Quadr)

## Reciprocità quadratica

$p, q$ primi dispari $\Rightarrow$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} -1 & p \equiv 3, 5 \pmod 8 \\ 1 & p \equiv 1, 7 \pmod 8 \end{cases}$$

## Calcolare $\left(\frac{-3}{p}\right)$ senza rec. quadratica

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2} \qquad \zeta_3^2 + \zeta_3 + 1 = 0$$

$-3$ è un quadrato $\hookrightarrow$ ho $\zeta_3 \bmod p$

In particolare $\zeta_3^3 \equiv 1 \pmod p$

$\zeta_3 \not\equiv 1 \pmod p$

$\Leftrightarrow$ ho un elemento di ordine 3

$\Leftrightarrow$ $3 \mid p-1$

**Soluzione 2** $n \equiv 4 \pmod 6$

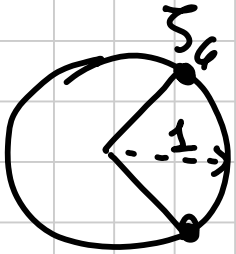
Speranza: RHS si fattorizza, e un fattore è $\Phi_6(x)$

La speranza funziona perché

$$RHS(\zeta_6) = 0$$

$$\zeta_6^{n+1} + \zeta_6 - 1 = \zeta_6^5 + \zeta_6 - 1$$

$$= \overline{\zeta_6} + \zeta_6 - 1 = 0$$




$$n^6 = (n^2 - n + 1)\left(\frac{n^{n+1} + n - 1}{n^2 - n + 1}\right)$$

$p(x)$

Calcolo l'MCD (...) e viene 1.

Conclusione: $n^2 - n + 1 = \square$ **no**

$$p(x) = \frac{X^{n+1} + X - 1}{X^2 - X + 1} = (X^{n-1} + X^{n-2} - X^{n-4} - X^{n-5}) + (X^{n-7} + X^{n-8} - X^{n-10} - X^{n-11}) + \dots + (X^3 + X^2 - 1)$$

e l'MCD si calcola...

N7. $P_n(x) = (x^2+x+1)^n - (x+1)^n - (x^2+x)^n$

$- (x^2+1)^n + x^{2n} + x^n + 1$

$P_n(x)$ sia il polinomio nullo mod 7

Termine noto: $P_n(0) = 0$

$x = 0$

$x^2 = 0$

$n > 3$ $\quad x^3 : \binom{n}{1,1,n-2} + \binom{n}{0,3,n-3} - \binom{n}{3}$

$$n(n-1) \equiv 0 \pmod 7$$

Sviluppo multinomiale $\quad (a+b+c)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} a^i b^j c^k$

$$\binom{n}{i,j,k} = \frac{n!}{i!\,j!\,k!}$$

Osservazione: $q(x^p) \equiv q(x)^p \pmod p$

Quindi, se $n$ è multiplo di 7 ho

$$P_n(x) \equiv P_{n/7}(x^7) \pmod 7$$

Questo dice che $n$ funziona $\Leftrightarrow$ $7n$ funziona

In particolare, wlog $7 \nmid n$

Dal calcolo del coeff. $x^3$, $n \equiv 1 \ (7)$

$$n = 1 + 7^a b \qquad \text{con} \quad 7 \nmid b$$

Calcoliamo il coeff. di $x^{7^a+2}$ : è $b$ $\left(\begin{smallmatrix}\text{se}\\ b \geq 2\end{smallmatrix}\right)$

$$P_n(x) = (x^2+x+1)^n - (x+1)^n - (x^2+x)^n - (x^2+1)^n + x^{2n} + x^n + 1$$

$$n = 1 + 7^a b$$

$$P_n(x) = (x^2+x+1)\left(x^{2\cdot 7^a} + x^{7^a} + 1\right)^b + \cdots$$

quindi $n = 1 + 7^k$

Due casi: $n = 7^a$

$n = 7^a (1 + 7^k)$