WC 2012 - Teoria dei Numeri

Titolo nota 25/01/2012

4) $a^2 + 1 \equiv 0 \ (p)$

$0 < a_1, a_2 < p \qquad a_1 = p - a_2$

$(p-1)^2 + 1 \geq a^2 + 1 = p \cdot q \cdot b \qquad q > p$

$\downarrow$

p^2

c $P(c^2+1) = p, \qquad c > p$

$c^2 + 1 = 2y^2 \geq 2q^2 \Rightarrow \quad c > q$

$q \mid c^2 + 1 \Rightarrow q^2 \mid y^2$

$P(c^2+1) = p \qquad a = c \mod p$

$b = p - a$

$$x^2 + 1 = 2y^2 \qquad x^2 - 2y^2 = -1$$

$$x^2 - 2y^2 = 1 \qquad (3, 2)$$

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

$$(1 + \sqrt{2})^2 \qquad 1^2 - 2 \cdot 1^2 = -1$$

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

$$\frac{(1 + \sqrt{2})^{2k+1} - (1 - \sqrt{2})^{2k+1}}{2\sqrt{2}} = y_k$$

$p \equiv 5 \pmod 8$

$$(1 + \sqrt{2})^{2k+1} \equiv (1 - \sqrt{2})^{2k+1} \quad (p)$$

$$(1 + \sqrt{2})^{4k+2} \equiv (-1)^{2k+1} \equiv -1 \quad (p)$$

$4k + 2 = p + 1$

$$(1 + \sqrt{2})^{p+1} \equiv (1 + \sqrt{2})^p (1 + \sqrt{2})$$

$$\equiv \left(1 + (\sqrt{2})^p\right)(1 + \sqrt{2})$$

$$\equiv \left(1 + (\sqrt{2})^{p+1}\right) + \sqrt{2}\left(1 + \sqrt{2}^{p-1}\right)$$

$$\equiv \left(1 + 2^{\frac{p+1}{2}}\right) + \sqrt{2}\left(1 + 2^{\frac{p-1}{2}}\right) \equiv \star$$

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{se } a \text{ è quadr. mod } p \\ -1 & \text{" " non " " " } \end{cases}$$

$$\not{*} \equiv \left(1 + 2^{\frac{p-1}{2}} \cdot 2\right) \equiv -1 \pmod{p}$$

4) $(n^2+1)\left((n-1)^2+1\right) =$

$$= \left(n^2-n+1\right)^2+1$$

$$\max\{P(n),\ P((n-1))\} = P\left(n^2-n+1\right)$$

Non è possibile che valga $P(n+1) > P(n)\ \forall n$

$\Rightarrow$ esistono m per cui

$$P(m-1) \leq P(m),\quad P(m+1) \leq P(m)$$

$$P(m) = \max\{P(m), P(m-1)\} = P\left(m^2-m+1\right)$$

$$P(m) = \max\{P(m+1), P(m)\} = P\left((m+1)^2-(m+1)+1\right)$$

5) • $F_n = 7^m + 117$

Mod 8 : RHS $\equiv 6 \pmod 8$

$4 \pmod 8$

0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1

- $9^m + 18 = F_n$

$9 \mid F_n$ $\qquad F_n = \dfrac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n \cdot \sqrt{5}}$

$0 \equiv F_n \pmod 9 \iff$

$(1+\sqrt{5})^n \equiv (1-\sqrt{5})^n \pmod 9$

$(1+\sqrt{5})^{2n} \equiv (-4)^n \pmod 9$

$\|\|$

$(6+2\sqrt{5})^n \equiv (2\sqrt{5})^n + n \cdot 6 \cdot (2\sqrt{5})^{n-1}$

$(-1)^n \equiv (-\sqrt{5})^n \pmod 3 \Rightarrow n$ pari

$\rightarrow n \equiv 0 \pmod 3$

$0, 1, 1, 0, 1, \ldots$

F_{3k} é par

$$\boxed{F_{n+1} = F_n + F_{n-1}} \qquad x^2 = x+1$$

$a, b, a+b$

$(a, b) \to (b, a+b)$

Successione modulo p (p primo)

$a + bx \qquad b + (a+b)x$

$(a+bx)x = ax + bx^2$

MODULO $x^2 - (x+1)$

$\equiv ax + bx + b = b + (a+b)x$

$x = \frac{1+\sqrt{5}}{2}$ Se $5 = \square \bmod p$ *

$\frac{1+\sqrt{5}}{2} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$

$\left(\frac{1+\sqrt{5}}{2}\right)^n \equiv 1$ sicuramente per $n = p-1$

(in generale può venire un divisore)

* $p \equiv \pm 1 \pmod 5$

Caso $5 \neq \square \pmod p$ $(p \equiv 2, 3 \pmod 5)$

$\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}_p$

$\downarrow$

$\in$ campo che ha p^2 elementi

$\neq 0$ $\{a+b\sqrt{5} \mid a, b \in \mathbb{Z}/p\mathbb{Z}\}$

tra cui p^2-1 sono $\neq 0$

$(a+b\sqrt{5})^{p^2-1} \equiv 1$

$\alpha^{p+1} = -1$

$\alpha^{2(p+1)} = 1$

$X^2 - X - 1$

$(X-\alpha)(X-\alpha^p)$

$\alpha^{\frac{2(p+1)}{2}} = 1$

d dispari

$X^3 + aX^2 + bX + c$ coeff in $\mathbb{Z}/p\mathbb{Z}$

IRRIDUCIBILE

non ha radici in $\mathbb{Z}/p\mathbb{Z}$

Le radici sono del tipo $h + l\xi + m\xi^2$

$\alpha, \alpha^p, \alpha^{p^2}$

p^3

N6) $a+b \mid a \cdot m^a + b \cdot n^b, \quad (a,b)=1$

$a+b=p \qquad m=n=1 \quad$ ok

$$a \cdot m^a + (p-a) \cdot n^{p-a} \mod p$$

Trovare $a<p$ con $p \mid a\left(m^a - n^{1-a}\right)$

Cerchiamo $(p, mn)=1$

$$p \mid (mn)^a - n$$

Male SE $(mn)^a - n = p_1^{\beta_1} \cdots p_k^{\beta_k}$

$$(mn)^2 - n = p_1^{e_1} \cdots p_k^{e_k}$$

$$(mn)^{2+kb} - n \equiv (mn)^2 - n \left(p_1^{f_1} \cdots p_k^{f_k}\right)$$

$$b = \varphi\left(p_1^{f_1} \cdot \cdots \cdot p_k^{f_k}\right)$$

$$f_1 > e_1, \ \ldots, \ f_k > e_k$$

Se $p_1^{\beta_1} \mid (mn)^{2+kb} - n$ e $\beta_1 > e_1$

ASSURDO, perché $p_1^{e_1} \| \text{RHS}$ ma

$p_1^{e_1+1} \mid \text{LHS}$

$p \mid n$ per k grande la massima pot. di p che divide $\left((mn)^{2+kb} - n\right)$

$$v_p\left((mn)^{2+kb} - n\right) = v_p(n)$$

$$p \mid (mn)^{\alpha} - n$$

Quindi se $p \nmid n \Rightarrow p \nmid m$

(Voglio $\alpha < p$: se $\alpha \geq p$ considero

$$\alpha - (p-1))$$