SENIOR 2012 – TdN 2 – Medium

Titolo nota 05/09/2012

$p^\alpha \| a-1 \qquad \alpha > 0$

$p \neq 2$ $\qquad v_p(m) = k$ $\qquad (m = p^k s, \text{ con } (s,p)=1)$

$$p^{\alpha+k} \| a^m - 1$$

Remind: $a = 1 + p^\alpha b \qquad (b,p)=1$

$$(1+p^\alpha b)^s = 1 + s p^\alpha b + \binom{s}{2} p^{2\alpha} b^2 + \dots$$

$$p^\alpha \| (a^s - 1)$$

$$(1+p^\alpha b)^p = 1 + \underbrace{p \cdot p^\alpha b}_{p^{\alpha+1}} + \binom{p}{2} p^{2\alpha} b^2 + \dots \qquad p^{\geq 2\alpha+1}$$

$$p^{\alpha+1} \| a^p - 1$$

$p = 2$ $\qquad \alpha \geq 2$ → lo stesso di prima

$$2^\alpha \| a - 1$$

$a - 1 = 2^\alpha b$ $\qquad b$ dispari

$a = 1 + 2^\alpha b$

$m = 2^k s$ $\qquad s$ dispari

$(1+2^\alpha b)^5 = 1 + \underbrace{5\cdot 2^\alpha b}_{\text{divisibile per } 2^\alpha} + \binom{5}{2} 2^{2\alpha} + \dots$

che termini divisibili per più di 2^α

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

esp $= \alpha+1$ $\quad 2\alpha$

$\alpha \geq 2 \quad 2\alpha > \alpha+1 \quad \rightarrow \quad 2^{\alpha+1} \parallel (1+2^\alpha b)^2 - 1$

$\longrightarrow$

$p^\alpha \parallel a+1$

$a = -1 + p^\alpha b$ $\quad$ d dispari

$(-1+p^\alpha b)^d = -1 + d\, p^\alpha b - \binom{d}{2} p^{2\alpha} b^2 + \dots$

$3 \parallel 5+1 \qquad 3 \nmid 5^2+1$

(IMO 1990): Per quali n $\quad n^2 \mid 2^n+1 \quad \left(\frac{2^n+1}{n^2} \in \mathbb{Z}\right)$?

Certamente n deve essere dispari. $\quad (n \neq 1)$

Sia p il più piccolo fattore primo di n

$2^n + 1 \equiv 0 \pmod{p^2} \rightarrow 2^n + 1 \equiv 0 \pmod{p}$

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

$\text{ord}_p(2) \mid 2n \qquad \text{ord}_p(2) \mid p-1 \qquad \text{ord}_p(2) \mid (2n, p-1)$

$\| \quad (2, p-1)$

$\text{ord}_p(2) = 1,2 \rightarrow \boxed{p=3}$ $\quad 2^1-1=1 \quad 2^2-1=3$

$n = 3^k m \quad k \geq 1 \quad (m,3)=1.$

$3 \parallel 2^3+1 = 9$

$3^{a+1} \parallel 2^{3^a}+1 \qquad 3^{2k} \mid n^2 \mid 2^n+1$

$3^{2k} \mid 3^{2k} m^2 \mid 2^{3^k m}+1$

$3^{k+1} \parallel 2^{3^k m}+1$

$2k \leq k+1 \Rightarrow k \leq 1$

Più in generale caso $n = 3m \quad (m,3)=1$

$q \cdot m^2 \mid 2^{3m}+1$

Abbiamo preso il fattore primo di m: q minimo. $(q \neq 3)$

$2^{3m}+1 \equiv 0 \pmod q$

$2^{6m} \equiv 1 \pmod q$

$\text{ord}_q(2) \mid (6m, q-1) = (6, q-1) = \begin{cases} 1 \\ 2 \\ 3 \\ 6 \end{cases}$

$\text{ord}=1 \rightarrow 2^1 \equiv 1 \quad q=1$ NO

$\text{ord}=2 \rightarrow 2^2 \equiv 1 \quad q=3$ NO

$\text{ord}=3 \rightarrow 2^3 \equiv 1 \quad \boxed{q=7}$

$\text{ord}=6 \rightarrow 2^6 \equiv 1 \quad q \mid 63 \quad q=3,7 \rightarrow q=7$

$n = 3m \quad q \mid m \quad 7 \mid m \quad 7^2 \mid m^2$

$49 = 7^2 \mid 2^{3m} + 1 = (2^3+1)(2^{3(m-1)} - 2^{3(m-2)} + \dots + 1)$

modulo 7 $\equiv 2(1 - 1 + \dots + 1) \equiv 2$

ASSURDO

UNICHE SOLUZIONI : $n = 1$, $n = 3$

(IMO 2002) $p_1, p_2, \dots, p_n$ primi dispari distinti > 3.

Dimostrare che $2^{p_1 p_2 \cdots p_n} + 1$ ha $\geq 4^n$ divisori.

$\left(n = q_1^{\alpha_1} \cdots q_s^{\alpha_s} \rightarrow \text{n° div di } n = (\alpha_1+1)\cdots(\alpha_s+1) \right)$

$\left(2^{p_1 \cdots p_{n-1}} + 1 \right) \mid 2^{p_1 p_2 \cdots p_n} + 1 \qquad a+1 \mid a^{p_n} + 1$

$a+1 = \prod q_i^{\alpha_i}$

$a^{p_n} + 1 = \prod q_i^{\beta_i} \prod r_j^{\delta_j} \leq (a+1)^2 \prod r_j^{\delta_j}$

c'è almeno un nuovo primo.

Oss. h, k numeri dispari primi fra loro $(h,k) = 1$.

Allora $(2^h+1, 2^k+1) = 3$.

Dim. oss $3 \mid (2^h+1, 2^k+1)$

$(x^a+1, x^b+1) \leftarrow$ polinomi $= (x^d+1)$ a, b dispari $d = (a,b)$

Se, per assurdo, esistesse $t>3$ $\quad t \mid (2^h+1, 2^k+1)$

allora $\quad 2^h \equiv -1 \pmod t$ $\qquad 2^x \equiv -1 \pmod t \iff x \equiv \frac{r}{2} \pmod r$

$2^k \equiv -1 \pmod t$ $\qquad r = \mathrm{ord}_t(2)$

$\frac{r}{2} \mid (h,k) = 1$ $\quad$ IMPOSSIBILE $\quad (r>2)$

$h = p_1 \cdots p_{n-1} \qquad k = p_n$

$m = \dfrac{(2^h+1)(2^k+1)}{3} \mid 2^{hk}+1$ $\qquad$ ha almeno $2 \cdot 4^{n-1}$ divisori.

$2^{hk+1} \geq m^2 \qquad 2^{hk+1} = am$ con $a>m$

Oss (ovvia): $d(am) \geq 2\,d(m)$ se $a>m$

$\downarrow$ n° divisori

$x, ax \qquad x$

(IMO 2005) Problema: Determinare tutti gli $n>1$ tali che esista un unico a con

$0 < a \leq n!$ tale che $a^n+1 \equiv 0 \pmod{n!}$

(WILSON p primo $\iff (p-1)! \equiv -1 \pmod p$)

Caso banale: $n=2 \qquad 0<a\leq 2!=2 \qquad a^2+1 \equiv 0 \pmod 2$

$a=1$ $\quad$ O.K

Un po' meno banale: n pari $\qquad n=2k>2$

a^2 è sempre un quadrato, $a^2+1 \equiv 1,2 \pmod 4$

$n! \equiv 0 \pmod 4$ IMPOSSIBILE

Supponiamo $n = p$ primo dispari.

$a^p + 1 \equiv 0 \pmod p \Rightarrow a^p + 1 \equiv 0 \pmod p$

$p \mid p!$

$\Rightarrow a^p + 1 \equiv a + 1 \pmod p$

Quindi $\boxed{p \mid a+1}$

Voglio vedere che, se c'è una soluzione $\hat{a}$, allora necessariamente $\underline{a = p! - 1}$ (ossia $p! \mid a+1$)

Mi serve vedere che $\boxed{(p-1)! \mid a+1}$.

Se a è una soluzione, so che

$$(p-1)! \cdot \left| \frac{a^p + 1}{a+1} = (a+1)^{p-1} \right.$$

Voglio dimostrare che, se $q < p$ è primo (un primo che divide $(p-1)!$) allora $q \nmid \frac{a^p+1}{a+1}$

$(a \mid bc, (a,c) = 1 \Rightarrow a \mid b)$

Supponiamo, per assurdo, che $q \mid \frac{a^p+1}{a+1} = a^{p-1} - a^{p-2} + \dots + 1$

(Necessariamente q dovrebbe essere dispari)

Avrei: $a^p + 1 \equiv 0 \pmod q$ $\quad a \equiv -1 \pmod q$

$a^{2p} \equiv 1 \pmod q$

Piccolo FERMAT $\quad a^{q-1} \equiv 1 \pmod q$

Ne segue $a^2 \equiv 1 \pmod q \Rightarrow a \equiv \pm 1 \pmod q$

- Se $a \equiv 1 \pmod q$, allora $\frac{a^p+1}{a+1} \equiv 1 \pmod q$, ASSURDO
- Se $a \equiv -1 \ (q)$ $\frac{a^p+1}{a-1} = a^{p-1} - a^{p-2} + \dots - a + 1$

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

(ma anche $\equiv 0$)

$q \mid p$ ASSURDO $(q < p)$

Concludiamo, se p è primo dispari, l'unica possibilità è $a = p! - 1$ $\quad n = p$

$p! \mid a+1 \mid a^p + 1$

Caso n dispari COMPOSTO

Consideriamo p il più piccolo primo che divide n

$p \mid n!$ $\quad p^\alpha \parallel n!$ $\quad n = p \cdot x$ $\quad x \geq p$ $\quad n \geq p^2$

Quindi $\alpha \geq p > 2$ $\quad n! = p^\alpha m$ $\quad (m, p) = 1$.

$a \equiv -1 \quad (p^{\alpha-1} m) \quad \left(= \frac{n!}{p}\right)$

$p^{\alpha-1} \mid a+1 \Rightarrow p^\alpha \mid a^p + 1 \mid a^n + 1 \Rightarrow n! \mid a^p + 1 \mid a^n + 1$

$m \mid a+1 \mid a^{p+1}$

Conclusione: tutti gli $a \equiv -1 \ (p^{\alpha-1} m)$ sono soluzioni di $a^n + 1 \equiv 0 \pmod{n!}$

INTERI DI GAUSS

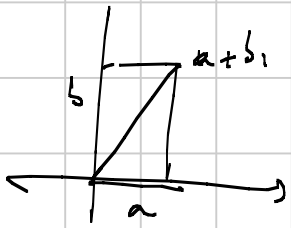
$$\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \} \qquad i^2 = -1.$$

SOMMA E PRODOTTO DI INTERI DI GAUSS SONO INTERI DI GAUSS.

Gli elementi invertibili sono $\pm 1, \pm i$.

$a+bi$ è invertibile $\Rightarrow \exists\ c+di \cdot (a+bi)(c+di) = 1$.

$$|a+bi|^2 |c+di|^2 = 1^2 = 1$$
$$(a^2+b^2)(c^2+d^2) = 1.$$



Per gli interi di Gauss c'è un teorema di fattorizzazione unica analogo a quello degli interi usuali.

Ogni intero di Gauss si scrive in modo unico* come prodotto di elementi primi.

* = a meno dell'ordine (e di elementi invertibili).

p primo : $p \mid ab \Rightarrow p \mid a$ o $p \mid b$

$\mathbb{Z}[\sqrt{5}]$ $\qquad (1+\sqrt{-5})(1-\sqrt{5}) = 1+5 = 2 \cdot 3 = 6$

I fattori primi di $a+bi$ sono divisori di

$(a+bi)(a-bi) = a^2+b^2 \in \mathbb{N}$,

Devo trovare i fattori primi di Gauss degli interi usuali,

ossia devo vedere se i numeri primi usuali si possono scomporre ancora o no.

Esempio: $5 = (2+i)(2-i) = 2^2 + 1^2 = 5$

$p = 2 \qquad 2 = (1+i)(1-i)$ $\quad 1+i,\ 1-i$ NON SONO INVERTIBILI

E SONO PRIMI (cioè IRRIDUCIBILI, cioè NON SI POSSONO SCOMPORRE ULTERIORMENTE)

$$1+i = (a+bi)(c+di)$$
$$|1+i|^2 = |a+bi|^2 |c+di|^2$$
$$2 = (a^2+b^2)(c^2+1^2) \qquad = 2 \cdot 1,\ 1 \cdot 2$$

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

p primo dispari

$$p = (a+bi)(c+di) \qquad p^2 = (a^2+b^2)(c^2+d^2)$$

$p^2 \cdot 1$ → BANALE

$p \cdot p$ → ?

$1 \cdot p^2$ → BANALE

CERCO EVENTUALI FATTORIZZAZIONI DEL TIPO

$$p = (a+bi)(a-bi)$$
con $p = a^2+b^2$

Se $p \equiv 3 \pmod 4$ IMPOSSIBILE

Questi sono primi ANCHE in $\mathbb{Z}[i]$.

Restano i primi $p \equiv 1 \pmod 4$

Supponiamo, per assurdo, che $p \equiv 1 \pmod 4$
RIMANGA PRIMO in $\mathbb{Z}[i]$ $\quad (p \neq (a+bi)(a-bi))$
$a^2+b^2 \neq p$

CONGRUENZA MOD p in $\mathbb{Z}[i]$

$$p \mid ab \Rightarrow p \mid a \text{ o } p \mid b$$
$$\bar{a}\cdot\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0} \text{ o } \bar{b} = \bar{0}$$

A = insieme delle classi di congruenza mod p

$f(x)$ polinomio a coefficienti in A
$\Rightarrow$ n° di radici $\leq \deg f$.

Considero $f(x) = X^2+1$
Sicuramente le classi di i e di $-i$ sono radici.
Osservo che $(\mathbb{Z}/p\mathbb{Z})^*$ ha $p-1$ elementi
e $4 \mid p-1$
C'è un elemento a di ordine 4

$$a^4 \equiv 1 \pmod p \qquad a^2 \equiv 1 \pmod p$$
$$\| \; b$$
$$b^2 \equiv a^4 \equiv 1 \pmod p \qquad a^2 \equiv -1 \pmod p$$

$a, -a$ sono altre due soluzioni.

Conclusione: X^2+1 ha ≥ 4 radici distinte
$\Rightarrow p$ non era primo
$\Rightarrow p = a^2+b^2 = (a+bi)(a-bi)$

SOMME DI DUE QUADRATI

$$m = a^2+b^2 \qquad n = c^2+d^2 \Rightarrow mn = e^2+f^2$$
$$e = ac-bd \quad f = ad+bc$$

$$m = (a+bi)(a-bi) \qquad n = (c+di)(c-di)$$
$$mn = [(a+bi)(c+di)][(a-bi)(c-di)]$$
$$= [(ac-bd)+i(ad+bc)][(ac-bd)-i(ad+bc)]$$

$$2 = 1^2+1^2 \qquad p \equiv 1 \pmod 4 \quad p = a^2+b^2$$
$$q \equiv 3 \pmod 4 \quad q^2 = q^2+0^2$$

$$2^{\alpha} p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{2\gamma_1} \cdots q_s^{2\gamma_s} = s^2+t^2$$
$$p_i \equiv 1 \qquad q_j \equiv 3 \pmod 4$$

D'altra parte, se $n = 2^{\alpha} p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\delta_1} \cdots q_s^{\delta_s}$ $\quad n = s^2+t^2$,
allora necessariamente δ_i è pari $\forall i$.

$$q_1 \mid n = s^2+t^2 = (s+ti)(s-ti)$$
$$q_1 \mid s+ti \qquad s = s_1 q \quad t = t_1 q$$

$$n = q^2(s_1^2+t_1^2) \qquad \frac{n}{q^2} \text{ è somma di due quadrati}$$

TERNE PITAGORICHE PRIMITIVE

$$a^2+b^2 = c^2 \qquad (a+bi)(a-bi) = c^2$$

$$MCD\,(a+bi, a-bi) \mid (2a, 2bi) = 2$$

Il MCD deve essere 1, perché altrimenti

$1+i \mid a+bi$

$2 \mid a^2+b^2$ $\quad a \equiv b \pmod 2$

Ma a, b pari $\to$ terna non primitiva

a, b dispari $\to$ $a^2+b^2 = c^2 \equiv 2 \pmod 4$

IMPOSSIBILE

$a+bi = (m+ni)^2$ $\quad (a-bi) = (m-ni)^2$

$= (m^2-n^2) + 2imn$

$a = m^2-n^2$ $\quad b = 2mn$

---

② Ogni numero naturale n è della forma

$n = x_1^2+x_2^2+x_3^2+x_4^2$

② $n = x_1^2+x_2^2+x_3^2 \iff n \neq 4^a(8k+7)$

$\Rightarrow$ FACILE

$\Leftarrow$ DIFFICILE

$a=0$ $\quad n \equiv 7 \pmod 8$ $\to$ CONSIDERARE LA CONGRUENZA $\quad x^2 \equiv 0, 1, 4 \pmod 8$

$a>0$ $\quad n = x_1^2+x_2^2+x_3^2$ $\quad x_1^2 \equiv 0, 1 \pmod 4$

$n \equiv 0 \pmod 4$ $\quad x_i = 2y_i$

$\frac{n}{4} = y_1^2+y_2^2+y_3^2$