Teoria dei numeri n+1

Titolo nota 06/09/2007

(dove n è intero della forma $\frac{x^2+y^2+1}{xy}$ con $x,y \in \mathbb{Z}$)

- Reciprocità quadratica
- Interi di Gauss, Pell
- Nullstellensatz (?)
- funzioni moltiplicative
- Esponenti "scendenti"

Simbolo di Legendre: p primo

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è residuo quadratico (mod } p) \\ -1 & \text{se } a \text{ non è } \text{“ } \text{“ } \text{“ } \\ 0 & \text{se } p \mid a \end{cases}$$

a è residuo quadratico $\iff \exists\, x \in \mathbb{Z}/p\mathbb{Z}$ t.c. $x^2 \equiv a \ (p)$

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \ (p)$$

se $\nexists\, x$ t.c. $x^2 \equiv a \ (p)$ $\quad a = g^k$

g è un generatore e k è dispari

supp. per assurdo che $a = g^{2r}$ $\quad a = (g^r)^2$

$$a = g^k \qquad a^{\frac{p-1}{2}} = g^{k\left(\frac{p-1}{2}\right)} \equiv g^{\frac{p-1}{2}}$$

$k \equiv 1 \quad (2)$

$k\left(\frac{p-1}{2}\right) \equiv \left(\frac{p-1}{2}\right) \qquad (p-1)$

$$\left(g^{\frac{p-1}{2}} + 1\right)\left(g^{\frac{p-1}{2}} - 1\right) = g^{p-1} - 1 \equiv 0 \qquad (p)$$

$\not{1}\not{1}\not{1}$
0

$\not{0}$
$p-1 = ord_p(g) \mid \frac{p-1}{2}$

$a^{\frac{p-1}{2}} \equiv (-1) \quad (p)$ se a non è residuo quadratico

per p dispari: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

$$a^{\frac{p-1}{2}} \; b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}}$$

$a = 48$

$$\left(\frac{a}{p}\right) = \left(\frac{a + k_p}{p}\right)$$

$$\left(\frac{a}{p}\right) = \left(\frac{48}{p}\right) = \left(\frac{3 \cdot 16}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{16}{p}\right) =$$

$$= \left(\frac{3}{p}\right)\left(\frac{4}{p}\right)^2 = \left(\frac{3}{p}\right)$$

2. almeno uno tra $3, 2, 6$ è residuo quadratico mod p.

$$\left(\frac{3}{p}\right)\left(\frac{2}{p}\right)\left(\frac{6}{p}\right) = (-1)^3 = (-1)$$

$$\left(\frac{6}{p}\right)\left(\frac{6}{p}\right) = \left(\frac{6}{p}\right)^2 \neq (-1)$$

Legge di reciprocità quadratica:

p, q sono dispari primi allora

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

$$\left(\frac{234}{101}\right) = \left(\frac{117 \cdot 2}{101}\right) = \left(\frac{16}{101}\right)\left(\frac{2}{101}\right) = \left(\frac{2}{101}\right)$$

$$\left(\frac{2}{p}\right) = ?$$

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

i) $p \equiv 1 \quad (4)$

ii) $p \equiv 3 \quad (4)$

$\rightarrow \frac{p-1}{4}, \frac{p+3}{4}$

i) $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdot 6 \cdot \ldots \cdot p-1 =$

$= 2 \cdot 4 \cdot 8 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+3}{2} \cdot \ldots \cdot p-1 =$

$\equiv 2 \cdot 4 \cdot 8 \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-3}{2}\right)\left(-\frac{p-5}{2}\right) \cdot \ldots (-1) =$

$= \left(\frac{p-1}{2}\right)! \, (-1)^{\frac{p-1}{4}}$

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \quad (p)$$

ii) $p \equiv 3 \ (4)$ stessa cosa $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$

Raggruppando $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p+1)(p-1)}{8}}$

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

Riassunto

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è r.q. } \mod p \\ -1 & \text{se } a \text{ non è } \text{“ } \text{“ } \\ 0 & \text{se } p \mid a \end{cases}$$

i) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$

ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

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

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

Se a, b hanno la stessa parità allora

$$2^a - 1 \nmid 3^b - 1$$

1) a è pari allora $2^a - 1 \equiv 0 \ (3)$

$$3 \mid 2^a - 1 \mid 3^b - 1$$ Assurdo

2) a è dispari

$$2^a - 1 \mid 3^{b+1} - 3$$

$b+1$ è pari.

3 è residuo quadratico modulo $2^a - 1$

Simbolo di Jacobi

$$\left(\frac{ab}{cd}\right) = \left(\frac{a}{c}\right)\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left(\frac{b}{d}\right) = \left(\frac{ab}{c}\right)\left(\frac{ab}{d}\right)$$

$\left(\frac{a}{b}\right) = -1$ $\left(\frac{a}{b}\right) = 1$ → nessuna informazione (se b non primo)

↓ sicuramente a non è r.q. (mod b)

$$\left(\frac{ab}{pq}\right) = 1 \quad \not\Leftarrow \quad \left(\frac{ab}{p}\right) = 1$$

$$\left(\frac{ab}{q}\right) = 1$$

$$\left(\frac{3}{2^a-1}\right) = \left(\frac{2^a-1}{3}\right)(-1)^{\left(\frac{2^a-2}{2}\right)\left(\frac{3-1}{2}\right)} =$$

$$= \left(\frac{1}{3}\right)(-1)^{(2^{a-1}-1)\cdot 1} = \left(\frac{1}{3}\right)\cdot(-1) = (-1)$$

$$2^a - 1 \equiv 3 \quad (4)$$

$\exists \quad p \mid 2^a - 1 \qquad p \equiv 3 \quad (4)$

vorremo $p \equiv 1 \quad (3)$!

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

$\uparrow$ 1

tutti i prim. de $|\ 2^a - 1$

sono $\begin{cases} \equiv 1 \ (4) & \equiv 1 \ (3) \\ \equiv 3 \ (4) & \equiv 2 \ (3) \end{cases}$ $\qquad p \equiv \pm 1 \ \ (12)$

$2^a - 1 \equiv 2^{2k+1} - 1 \qquad \begin{cases} \equiv 1 \ (3) \\ \equiv 3 \ (4) \end{cases} \qquad \equiv 7 \ \ (12)$

Assurdo c'è almeno un primo della forma $\begin{cases} \equiv 1 \ (4) & \equiv 2 \ (3) \\ \equiv 3 \ (4) & \equiv 1 \ (3) \end{cases}$

Equazione di Pell

$d \neq a^2$

studiare le soluzioni di

$$x^2 - dy^2 = 1$$

al variare di $x, y \in \mathbb{N}$

$$= (x - \sqrt{d}\,y)(x + \sqrt{d}\,y)$$

$$(x_0, y_0) \qquad (x_0 \pm \sqrt{d}\,y_0)^n = x_{n-1} \pm \sqrt{d}\,y_{n-1}$$

$\Rightarrow (x_{n-1}, y_{n-1})$ è soluzione.

$$(x_0 + \sqrt{d}\, y_0)^n = x_{n-1} + \sqrt{d}\, y_{n-1}$$

$$(x_0 - \sqrt{d}\, y_0)^n = x_{n-1} - \sqrt{d}\, y_{n-1}$$

$$(x_0^2 - d y_0^2)^n = x_{n-1}^2 - d y_{n-1}^2$$

$$\| \quad 1^n = 1$$

tutte e sole le soluzioni sono della forma precedente, cioè sono tutte generate da una sola soluzione

2° fatto (x_0, y_0) è soluzione allora

$x_0 + \sqrt{d}\, y_0 > 1$ $\quad x_0 - \sqrt{d}\, y_0 < 1$ $\quad$ se $x_0 + \sqrt{d} y_0 \neq x_0 - \sqrt{d} y_0$

$y_0 \neq 0$

$\pm(x, y) = (\pm 1, 0)$

$$S = \left\{ (x, y) \in \mathbb{N}_{>0}^2 \;\middle|\; x^2 - d y^2 = 1 \right\}$$

$$\min_{(x,y) \in S} \; x + \sqrt{d}\, y$$

(x_0, y_0)

$x_0 + \sqrt{d}\, y_0 = x_1 + \sqrt{d}\, y_1$

$\Leftarrow$ $\Rightarrow$ $\quad y_1 = y_0$ $\Rightarrow$ $x_0 = x_1$

$x_0 - x_1 = \sqrt{d}\,(y_1 - y_0)$

Supp. per assurdo $\exists$ z, t tali che

$$z^2 - dt^2 = 1 \qquad (x_0+\sqrt{d}y_0)^n < z + \sqrt{d}t < (x_0+\sqrt{d}y_0)^{n+1}$$

$$(x_0+\sqrt{d}y_0)^n(x_0-\sqrt{d}y_0)^n < (z+\sqrt{d}t)(x_0-\sqrt{d}y_0)^n < (x_0+\sqrt{d}y_0)^{n+1}(x_0-\sqrt{d}y_0)^n$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$1 < z' + \sqrt{d}t' < x_0+\sqrt{d}y_0$$

$t', z' > 0 \qquad (z', t') \in S$

$$z' - \sqrt{d}t' = (z-\sqrt{d}t)(x_0+\sqrt{d}y_0)^n$$

$$z'^2 - dt'^2 = (z'-\sqrt{d}t')(z'+\sqrt{d}t') = (x_0^2-dy_0^2)^n(z^2-dt^2) = 1$$

$(z', t') \in S$ ma $z' + \sqrt{d}\, t' < x_0 + \sqrt{d}\, y_0$

ASSURDO

per la minimalità

di $x_0 + \sqrt{d}\, y_0$.

$x^2 \pm d y^2$ $x, d, y \in \mathbb{Z}$

$\forall\, x, y, z, t \;\; \exists\, a, b$ t.c.

$$(x^2 + d y^2)(z^2 + d t^2) = a^2 + d b^2$$

$$(x + i\sqrt{d}\, y)(x - i\sqrt{d}\, y)(z + i\sqrt{d}\, t)(\ldots)$$

$$((xz - d y t) + i\sqrt{d}\,(yz + tx))((xz - dyt - i\sqrt{d}\,(yz + tx)) =$$

$$= (\underbrace{xz - dyt}_{A})^2 + d(\underbrace{yz + tx}_{B})^2 = A^2 + dB^2$$

Ritorno a Pell:

$x^2 - dy^2 = m$ con (a,b) sol. minimale per $m = 1$

minimale

(x_0, y_0) sol $^{\text{r}}$ di $x^2 - dy^2 = m$

(x, y) sol $\iff \exists k \; (x_0 + \sqrt{d}\, y_0)(a + \sqrt{d}\, b)^k = x + \sqrt{d}\, y$

$1 < x_0 + \sqrt{d}\, y_0 < x + \sqrt{d}\, y$

$$1 < x_0 + \sqrt{d}\, y_0 < x + \sqrt{d}\, y$$

$$\Downarrow$$

$$(x + \sqrt{d}y)(a + \sqrt{d}b)^k < x_0 + \sqrt{d}\, y_0 < (x + \sqrt{d}y)(a + \sqrt{d}b)^{k+1}$$

$$(x + \sqrt{d}y) < x_1 + \sqrt{d}y_1 < (x + \sqrt{d}y)(a + \sqrt{d}b)$$

Lasciamo in sospeso ----

$P(x) \geq 0 \quad \forall \quad x \geq 0$ allora

$P(x) = A(x)^2 + x\,B(x)^2$ per qualche polinomio $A(x), B(x)$

$P(x) = ax+b$ è positivo per $x \geq 0 \iff a \geq 0$, $b \geq 0$

$P(x) = a^2 x + b^2$

$P(x) = ax^2 + bx + c$ i) $\Delta \geq 0$, $a \geq 0$

ii) $x_1, x_2 \leq 0 \Rightarrow a \geq 0 \quad b \geq 0 \quad c \geq 0$

$(\Delta \geq 0)$

$$a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}\right] \qquad -\frac{b}{a} = x_1 + x_2 \leq 0$$

$$x_1 x_2 \geq 0$$

$$a(x+\alpha)^2 + xr^2 = ax^2 + 2a\alpha x + \alpha^2 a + xr^2$$

$$\alpha^2 = \frac{c}{a}$$

$$ax^2 + \left(2a\sqrt{\frac{c}{a}} + r^2\right)x + \frac{c}{a}a$$

$$b \geq 2\sqrt{ca}$$ cond. nec. e suff. affinché $\exists\ r$

$$b^2 - 4ac \geq 0$$

$$\Delta \geq 0$$

(1) $P(x) \geq 0 \quad \forall x \in \mathbb{R}$

$$P(x) = A^2(x) + B^2(x) \qquad \text{con } A(x), B(x) \in \mathbb{R}[x]$$

- $P \neq$ di 0-esimo grado $\quad P(x) = a^2 + 0^2$

- P è di 2° grado $\quad P(x) = a\left[\left(x + \frac{b}{2a}\right)^2 - \underbrace{\frac{\Delta}{4a^2}}_{\geq 0}\right] =$

$$= \left[A^2\left(x + \frac{b}{2a}\right)^2 + C^2\right]$$

Voglio dimostrare x induzione che se $P(x)$ è di $2n$-esimo grado allora se è soddisfatta la (1) allora $P(x) = A^2(x) + B^2(x)$ per qualche A, B

i) $p(x)$ ha almeno una radice complessa non reale

$\Rightarrow p(a+ib)=0 \quad , \quad p(a-ib)=0$

$\overline{p(a+ib)} = \overline{0}$

$\overline{p}\left(\overline{(a+ib)}\right) = \overline{0} \qquad p(a-ib)=0$

$p(x) = \left(x-(a+ib)\right)\left(x-(a-ib)\right) R(x) = \left((x-a)^2+b^2\right) R(x)$

$p(x)$: grado $2n$; $R(x)$: grado $2n-2$

$$R(x) = \frac{p(x)}{(x-a)^2+b^2} \geq 0 \qquad \forall \; x \in \mathbb{R}$$

≥ 0 (numeratore) ; > 0 (denominatore)

$$\left((x-a)^2+b^2\right) R(x) = \left[A^2(x)+B^2(x)\right]\left((x-a)^2+b^2\right) = C^2(x) + D^2(x)$$

a) $P(x)$ ha solo radici reali

$$P(x) = A\,(x-x_1)^{\alpha_1}(x-x_2)^{\alpha_2}\cdots(x-x_n)^{\alpha_n}$$

Supp ce ne sia uno dispari

ordiniamoli e facciamo in modo

che $\cdots \le x_3 \le x_1 \le x_2 \le \cdots$

$x > x_1 \qquad P(x) \geq 0$

$x < x_1 \qquad P(x) \geq 0$

$$P(x) = A(x-x_1)^{\alpha_1}(x-x_2)^{\alpha_2}\cdots(x-x_n)^{\alpha_n}$$

α_i è più $\forall i \Rightarrow A = B^2$

$f(x) = (AQ(x))^2$

Interi di Gauss

Bobo ha torto ... a volte

$a+ib \qquad a, b \in \mathbb{Z}$

negli interi di Gauss c'è la fattorizzazione unica e i primi sono o primi negli interi con $p \equiv 3 \ (4)$ oppure $x+iy$ con x^2+y^2 numero primo

$p \equiv 3 \ (4)$ $\quad \exists \ x+iy$ primo $x+iy \mid p$

$$p = (x+iy)(a+ib) = xa - yb + i(ya + xb)$$

$$ya = -xb \Rightarrow \frac{x}{a} = -\frac{y}{b} = \frac{1}{c}$$

$$a+ib = (x-iy)c = (x+iy)\frac{p}{y}$$

$$p = c(x^2+y^2) = x^2+y^2$$

$$x^2 \equiv -y^2 \ (p)$$

$p \equiv 3 \ (4) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$

$$\left(\frac{x}{y}\right)^2 \equiv -1 \ (p)$$

Se p primo $\quad p \equiv 1 \pmod 4 \Rightarrow$

$\exists \; x, y$ t.c. $\quad x^2 + y^2 = p$

$$p \mid a^2 + 1$$

$$p \mid (a+i)(a-i) \qquad p \mid a+i$$

$$(x+iy)p = (a+i)$$

p non è primo negli interi di Gauss

$$(x+iy)(a+ib) = p$$

$$x+iy \neq \pm 1, \pm i$$

$$(a, b) = (x, -y)$$

$$yb + ax = 0$$

$$p = (x+iy)(x-iy) = x^2 + y^2$$

Altri anelli in cui vale la fattorizzazione unica: per $\mathbb{Z}[\sqrt{d}]$ con $d = -1, -2, -3, -7, -11$

$-19, -43, -67, -163$

Attenzione! $\mathbb{Z}[\sqrt{d}]$ $\mathbb{Q}[\sqrt{d}]$

$$\{ a + \sqrt{d}\, b \;,\; a, b \in \mathbb{Q} \}$$

$\mathbb{Z}[\sqrt{d}]$ sono le soluzioni $\in \mathbb{Q}[\sqrt{d}]$

di polinomi monici in $\mathbb{Z}[x]$

$$\mathbb{Z}[\sqrt{d}] = \left\{ a + \frac{1+\sqrt{d}}{2} b \right\} \qquad (d \text{ dispari})$$

$$\| $$

$$\left\{ \frac{c + \sqrt{d}\, b}{2} \text{ con } c \equiv d \pmod 2 \right\}$$

$$2 = \left(\frac{1+\sqrt{3}}{2}\right)\left(-\frac{\sqrt{3}+1}{2}\right) \qquad 2 \text{ non è primo}$$

$$\left(\frac{-163}{p}\right) = 1 \quad \Rightarrow \quad \exists\ x, y \ \text{t.c.}\ 4p = x^2 + 163y^2$$

$$y^2 + 2 = x^3 \quad \longrightarrow \quad y^2 + 1 = x^3 - 1$$

$$y^2 + 1 = (-1)(x^2 + x + 1)$$

$$x \equiv 3 \pmod 8 \quad (8)^2 \equiv 1 \pmod 8 \quad \not\equiv 5 \pmod 8$$

$$\downarrow$$

$$(y + i\sqrt{2})(y - i\sqrt{2}) = x^3$$

$y + i\sqrt{2}$, $y - i\sqrt{2}$ coprimi

$$p \mid y + i\sqrt{2}$$

$$p \mid y - i\sqrt{2}$$

$$p \mid i\sqrt{2} \cdot 2 \qquad p \mid 2$$

$$|p| \mid 8 \qquad |p| \mid x^6$$

$$|x+i\sqrt{2}y| = x^2+2y^2$$

$$(y+i\sqrt{2}) = (a+i\sqrt{2}b)^3 =$$

$$= a^3 - 3\cdot 2\cdot b^2 a + i\sqrt{2}(3a^2b - 2b^3)$$

$$3a^2b - 2b^3 = 1$$

$$(3a^2 - 2b^2)b = 1 \qquad b = \pm 1$$

$b=1$ $\quad 3a^2 - 2 = 1 \quad \Rightarrow \quad a = 1$

$3a^2 + 2 = 1 \quad \Rightarrow$ ↯

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

$5^2 + 2 = 3^3$

$$x^2+1=y^n$$

$$(x+i)(x-i)=y^n$$

$n \geq 2$

$n \geq 3$

n Ajaran

$p \mid x+i$

$p \mid x-i$

$p \mid 2i$

$|p| \mid 4$

$|p| \mid y^{2n}$

$|p|=1$

x dipari $\quad x^2+1 \equiv 2 \pmod 8$

$2 \mid y^n$

$\Rightarrow 4 \mid y^n$

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

$$(x+i)=(a+ib)^n$$

$$x+i = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} a^{n-2j} b^{2j} (-1)^j + i \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2j+1} a^{n-2j-1} b^{2j+1} (-1)^j$$

$$= X$$

multiplo di b $= Y$

$$X + iY = x + i$$

$$\rightarrow Y = 1 \qquad b \mid Y \qquad b = \pm 1$$

$$\rightarrow \sum_{j=0}^{n} \binom{2n+1}{2j} a^{2j} (-1)^{n-j} = \pm 1$$

$$2 \mid a$$

$$(x+i) = (a \pm i)^n$$

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

$$x^2+1 = (a^2+1)^n$$

$$2 \mid a$$

$$\left(\sum_{j=1}^{n} \binom{2n+1}{2j} a^{2j} \right) + (-1)^n = \pm 1$$

a^2 to divide

⇓

4 to divide $\rightsquigarrow$ $\pm 1 - (-1)^n \equiv 0 \ (4)$

supposto tacitamente $a^2 \neq 0$

$$\sum_{s=1}^{n} (-1)^{n-s} \binom{2n+1}{2s} a^{2s-2} = 0$$

$$(-1)^{n-1}\binom{2n+1}{2} + (-1)^{n-2}\binom{2n+1}{4} a^2 + \cdots = 0$$

$$\underbrace{\qquad\qquad}_{11} \qquad\qquad \underbrace{\qquad\qquad\qquad\qquad}_{a = 2a'}$$

$$\frac{(2n+1)(2n)}{2} + \cdots \binom{2n+1}{2k} 2^{2k-2} \cdot a'^{2k-2}$$

$$v_2\left(\frac{(2n+1)(2n)(2n-1)(2n-2)\cdots \cdot 2^{2k-2}}{(2k)!} \right) > v_2\left(\binom{2n+1}{2}\right)$$

$(2k)!$ ← Al più $2k-1$ fattori 2

Almeno un fattore 2

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots <$$

$$= \frac{n}{2} + \frac{n}{4} + \frac{n}{8} + \qquad = n$$

$$v_2(\text{SKIFO}) \geq v_2(2n) + (-1) + v_2(2n-2)$$

$$\geq v_2(2n) > v_2\left(\binom{2n+1}{2}\right) = v_2(2n) - 1$$

Assumo $(e = 0)$

$$e^2 + 1 = 1^n$$

Fine!

$p = x^2 + y^2$ se $p \equiv 1 \quad (4)$

$$A = \{ x \in \mathbb{N}^+ \text{ t.c. } 0 \le x \le \lfloor \sqrt{p} \rfloor \}$$

$\exists \ a \ \text{t.c.} \quad a^2 \equiv -1 \quad (p)$

$(x, y) \in A \times A \quad (x - ay)$

N° coppie $= (\lfloor \sqrt{p} \rfloor + 1)^2 > p$

$\sqrt{p}$

$\exists \ (x_1, y_1), (x_2, y_2)$ distinti!

$x_1 - a y_1 = x_2 - a y_2$

$$(x_1 \pm x_2) \equiv a\,(y_1 - y_2)$$

$$0 \le x_1 - x_2 \;,\; y_1 - y_2 < \sqrt{p}$$

$$(x_1 - x_2)^2 \equiv a^2 (y_1 - y_2)^2 \equiv -(y_1 - y_2)^2 \quad (p)$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad \| \; -1$$

$$x^2 + y^2 \equiv 0 \quad (p)$$

$$0 \le x^2 < p \qquad 0 \le y^2 < p \qquad\qquad 0 \le x^2 + y^2 < 2p$$

$$x^2 + y^2 = p$$

$(a,b) = 1$

$\{ ax + by \quad x, y \in \mathbb{N} \} = S$

max n° che non e' in S

$ab - a - b$

i) $ab - a - b = ax + by$

$ab = a(x+1) + b(y+1) \geq 2ab$

$a \mid y+1$
$b \mid x+1$

ii) $ab - a - b + k = ax + by$ per qualche (x, y)

$\forall\ k > 0$

$k \equiv 0 \pmod a$

$$\begin{cases} ab - a + k \equiv 0 \pmod a \\ ab - a - b + k \qquad b > a \\ ab - a - 2b + k \\ ab - a - 3b + k \\ \\ ab - a - (a-1)b + k = b - a + k \end{cases}$$

$a-1$ sono tutti diversi e div.

$a \mid k$

$ab - a - 5b + k = 5a$

$ab - a - b + k = 5a + (5-1)b$

$$ab - a - b + ka = (k-1)a + (k-1)b$$

$$k > 1 \qquad a > 1$$

* $2abc - ab - bc - ca$ è il massimo intero non rappresentabile nella forma

$$abx + bcy + caz \qquad \text{con} \quad x, y, z \in \mathbb{N}$$

$$(a,b) = 1 \qquad (b,c) = 1 \qquad (c,a) = 1$$

IMO 1983/3

$p \mid x - y$ $\qquad$ $p \parallel \dfrac{x^p - y^p}{x - y}$

$x = y + kp$

$$x^p = (y+kp)^p = y^p + \underbrace{kp^2 y^{p-1}}_{v_p(kp)=1} + \underbrace{k^2 p^3 \left(\cdots\right)}_{v_p(\cdot) \geq 2}$$

$$v_p\left(x^p - y^p\right) = v_p\left(kp^2\right) = v_p(kp) + 1$$

$$p^k \parallel \frac{x^{p^k} - y^{p^k}}{x^{p^{k-1}} - y^{p^{k-1}}} \cdot \frac{x^{p^{k-1}} - y^{p^{k-1}}}{x - y} \qquad p^{v_p(n)} \parallel \frac{x^n - y^n}{x - y}$$

$x \equiv y \ (p)$

$$\frac{x^n - y^n}{x-y} = \underbrace{x^{n-1} + yx^{n-2} + \cdots + y^{n-1}}_{n} \equiv$$

$$\equiv n x^{n-1} \not\equiv 0 \ (p)$$

$$\frac{2^n + 1}{h^2} \in \mathbb{Z} \qquad n \text{ dispari}$$

$$n^2 \mid 2^n - (-1)^n$$

P.P.P. $\mid n$ $\qquad p \mid n$ $\qquad \mathrm{ord}_p(2)$ $\qquad p^2 \mid 2^n - (-1)^n$

$p \mid 2^n + 1$ $\qquad$ $2^{2n} \equiv 1 \ (p)$ $\qquad$ $2^n \equiv 1$

$\text{ord}_p(2) \mid 2n \rightarrow$ ha solo fattori $\geq p$

$2^2 \equiv 1 \ (p) \Leftarrow \text{ord}_p(2) \mid p-1$

$3 \equiv 0 \ (p)$

$p = 3$

$p \quad 3^2 \mid 2^3 + 1$

$3^{2k} \mid 2^{3^k} + 1$ $\qquad$ (per quali k?)

$$3^2 \| 2^3 - (-1)$$

$$3^{k-1} \| \frac{2^{3^k} - (-1)^{3^k}}{2^3 - (-1)}$$

$$3^{k+1} \| 2^{3^k} + 1$$

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

$$2k \leq k+1$$

$$k \leq 1$$

$p = 3 \cdot n'$ p il $p.p.$ di n'

$$p \mid 2^{3 \cdot n'} + 1$$

$$2^{6n'} \equiv 1 \quad (p)$$

$ord_p(2) \mid 6n'$ -> 有 a Ho... $\geq p$

$ord_p(2) \mid p-1$

$ord_p(2) \mid 6$

~~2~~, ~~3~~, ~~1~~, 6

$$2^{3n'} + 1 \equiv 0$$

3 NO

1 NO

$$2^6 - 1 \equiv 0$$

$$(2^3+1)(2^3-1) \equiv 0 \quad (p)$$

9 11

IMO 2000/5

IMO 1999/4

NULLSTELLENSATZ
(combinatorial)

ho un campo $\mathbb{K}$ allora se ho un polinomio $p(x_1, x_2, \dots, x_n)$ che ha grado massimo d e ho che il coeff. di $x_1^{d_1} x_2^{d_2} x_3^{d_3} \cdots x_n^{d_n}$ con $d_1 + d_2 + \dots + d_n = d$ è nonnullo allora se ho $S_1, S_2, \dots, S_n$ insieme con $|S_i| \geq d_i + 1$ allora $\exists\ y_1, y_2, \dots, y_n$ con $S_i \subset \mathbb{K}$ $\forall_i$

$y_1 \in S_1$, $y_2 \in S_2$ - , $y_n \in S_n$ t.c.

$p(y_1, y_2, \dots, y_n) \neq 0$

Dim. supp. per assurdo che si annulli per tutti i valori di $(y_1, y_2, y_n) \in S_1 \times S_2 \times S_n \times \mathbb{K}$

$p(x_1, x_2, \dots, x_n)$

caso 1) l'unico termine di grado massimo è proprio $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$

e inoltre che tutti i monomi che contengono un $x_i^{\alpha_i}$ hanno $\alpha_i \leq d_i$

$$p(x_1, x_2, -, x_n)$$

fisso $(x_2, -, x_n) \in S_2 \times S_3 \times \cdots \times S_n$

faccio variare x_1 - questo è un polinomio di grado d_1 e ho $d_1 + 1$ soluzioni

$$p(x_1, x_2, -, x_n) = x_1^{d_1} q(x_2, -, x_n) + x_1^{d_1 - 1} (\ ) + \\ + \cdots + c$$

$\forall$ $(x_2, -, x_n) \in S_2 \times S_3 \times - S_n$

(abbiamo $d \in \rho_{(x_2, \ldots, x_n)}(x_1) \equiv 0$

$q(x_2, \ldots, x_n) = 0$

2° passo) $p(x_1, x_2, \ldots, x_n)$ generico

$Q_{x_1} (x_1 - \alpha_1)(x_1 - \alpha_2) \cdots = (x_1 - \alpha_{d_1+1})$

$S_1 = \{\alpha_1, \ldots, \alpha_{d_1+1}\}$

$S_1 \times S_2 \times \ldots \times S_n$

$q(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n) +$

$$+ A_1(x_1 \dots x_n) Q_{x_1} + A_2(x_1 \dots x_n) Q_{x_2}$$

$$+ A_3(x_1 \dots x_n) Q_{x_3}$$

$q = p$ sull'iperrettangolo $S_1 \times S_2 \dots \times S_n$

$$X_1^{d_1+k} \qquad x^{d_1+1} \longrightarrow \underbrace{x^{d_1+1} - Q_{x_1}}_{\deg \le d_1} \qquad \deg(Q_{x_1}) = d_1+1$$

$$x_1^{d_1+2} \; x_2^{d_2-2} \dots x_n^{1}$$

ai tuoi $x_1 \; x_2 \dots x_n$

$$\left(x^{d_1+1} - Q_{x_1}\right) x_1 x_2^{d_2-2} \cdots x_n$$

$$x^{d_1+2} x_2^{d_2-2} \cdots x_n - Q_{x_1}\left(x_1 x_2^{d_2-2} \cdots x_n\right)$$

Alla Fine mi ritrovo un $q(x) = p(x)$ in $S_1 \times S_2 \cdots \times S_n$ ma $q(x)$ rispetta il caso 1

A, B $\quad |A+B| = \{ a+b : a \in A, b \in B \}$

$A \subset K \quad B \subset K$

$$|A+B| \geq \min(|K|, |A|+|B|-1)$$

Thesi

Supp. per assurdo che esistano al più $|A|+|B|-2$ valori in $A+B = \{a_1, a_2, \dots a_{|A|+|B|-2}\}$

$$P(x,y) = (x+y-a_1)(x+y-a_2)\cdots(x+y-a_{|A|+|B|-2})$$

Vedo che il numero $x^{|A|-1}\, y^{|B|-1}$

ha come coeff. $\binom{|A|+|B|-2}{|A|-1} \neq 0$

ma abbiamo che $(x,y) \in A \times B$

$$p(x,y) = 0$$

$$|A \dot{+} A| \geq \min(|K|, 2|A|-3)$$

Supp. per assurdo vino al più $2|A|-4$

$$p(x,y) = (x+y-a_1)(x+y-a_2)\cdots(x+y-a_{2|A|-4})(x-y)$$

$$x^{|A|-1}\, y^{|A|-2}$$

qvzl el il coeff d $x^{|A|-1} y^{|A|-2}$?

$$\binom{2|A|-4}{|A|-2} x^{|A|-2} y^{|A|-2} \cdot x - x^{|A|-1} y^{|A|-3} \cdot y \binom{2|A|-4}{|A|-1}$$

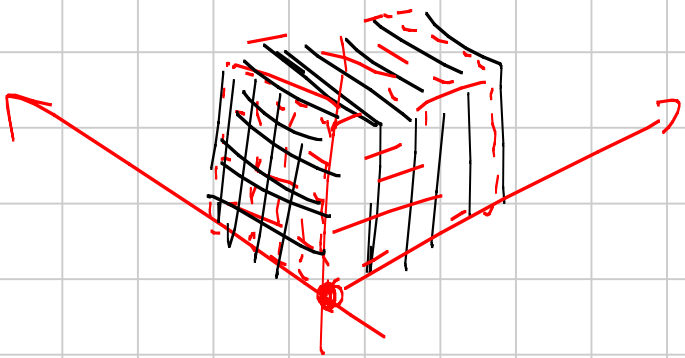
$$x^{|A|-1} y^{|A|-2} \left(\quad \right) \neq 0$$

$$\{x_1, x_2 - - , x_{|A|}\} = A$$

$$\{x_2 - - , x_{|A|}\} = A/x,$$

$$\{(x, y, z) = \{0, 1, \dots, n\}^3\} / \{(0, 0, 0)\} = A$$

Io voglio ricoprire tutti i punti di A con dei piani ma senza ricoprire $(0, 0, 0)$



3n ce la faccio

Supponiamo per assurdo che ce la faccio con meno di 3n piani

k piani ce la faccio

piano $ax + by + cz = d$

$d_i \neq 0 \ \forall i$

$$p(x,y,z) = \prod_{i=1}^{3n} (a_i x + b_i y + c_i z - d_i) - \alpha \prod_{i=1}^{n} (x-i)(y-i)(z-i)$$

Scelgo α t.c. $p(0,0,0) = 0$ con $\alpha \neq 0$

$\alpha x^n y^n z^n$ quindi posso applicare

il [illegible]

$x_i \in \{0, -, -, n\}$

$y_i \in \{0, -, -, n\}$

$z_i \in \{0, -, -, n\}$