CN Basic

Titolo nota 26/09/2024

Terne pitagoriche

Tutte le terne pitagoriche primitive ($MCD(a,b,c)=1$) sono della forma $a^2+b^2=c^2$ $a=m^2-n^2$, $b=2mn$ $c=m^2+n^2$. con $(m,n)=1$

1) è vero che $\forall m,n$ interi queste sono terne pitagoriche:

$$(m^2+n^2)^2 = m^4+2m^2n^2+n^4 = (m^2-n^2)^2+4m^2n^2 = (m^2-n^2)^2+(2mn)^2.$$

2) • monstri pari, anzi per forza 2 disp. e 1 pari. a, b disp e 2 pari? no mod 4.

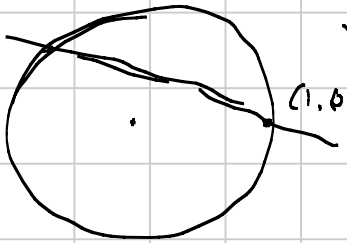
supp. a disp., b pari, c disp.

$b^2 = c^2-a^2 = (c-a)(c+a)$ $MCD(c+a, c-a) = (2c, c-a) = 2$

(nota: primitiva $\to (a,b)=(a,c)=(b,c)=1$).

$b=2h$ $h^2 = \frac{c-a}{2}\cdot\frac{c+a}{2}$ analizzando le potenze dei primi, vediamo che $\frac{c-a}{2}=n^2$ $\frac{c+a}{2}=m^2$ per certi $m,n\in\mathbb{N}$ e allora $b=2mn$ $a=m^2-n^2$ $c=m^2+n^2$. □

2ª dim.



$x^2+y^2=1$ in $\mathbb{R}^2$

mi accorgo che $a^2+b^2=c^2$

$\iff \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$ (e viceversa)

Dico che pp. a coord. razionali corrisp. a rette per $(-1,0)$ a coeff. angolare razionale.

$(x+1)=my$ $x=my+1$ $(my+1)^2+y^2=1$ $(1+m^2)y^2+2my=0$.

$y=0$ $y=\frac{-2m}{1+m^2}$ $x=\frac{-2m^2}{1+m^2}+1=\frac{1-m^2}{1+m^2}$ $m=\frac{s}{t}$ $(s,t)=1$

$y=\frac{-2\frac{s}{t}}{1+\frac{s^2}{t^2}}$ $x=\frac{1-\frac{s^2}{t^2}}{1+\frac{s^2}{t^2}}$

$\frac{-2st}{s^2+t^2}$ $\frac{t^2-s^2}{s^2+t^2}$

la terna viene $-2st$ $(o\ 2st)$, t^2-s^2, t^2+s^2

Teorema di approssimazione di Dirichlet

Sia $\alpha \in \mathbb{R}$ irrazionale. Fissiamo $n \in \mathbb{N}$

Esistono p, q interi con $q \in \{1, \dots, n\}$ t.c.

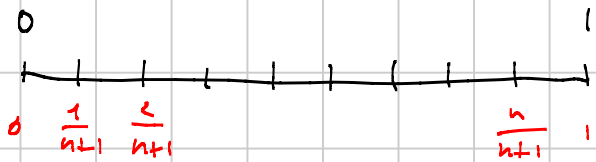
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q(n+1)}.$$

Dim. Tesi $\Leftrightarrow \left|q\alpha - p\right| < \frac{1}{n+1}$ Consideriamo allora tutti i

$q\alpha$ $\quad q \in \{0, \dots n\}$ Consideriamo $F = \{ \{q\alpha\} \mid q = 0, \dots n \} \subset [0,1]$

↳ parte frazionaria

$|F| = n+1$



$F \cup \{1\}$ ha $n+2$ elementi,

per il principio dei cassetti,

$\exists\, q_1, q_2$ nello stesso intervallino.

Questo significa che $\left|\{q_1\alpha\} - \{q_2\alpha\}\right| < \frac{1}{n+1}$ supp. $q_1 > q_2$

$[q_1\alpha] = p_1, \quad [q_2\alpha] = p_2$ $\qquad (q_1 - q_2)\alpha = [q_1\alpha] + \{q_1\alpha\} - [q_2\alpha] - \{q_2\alpha\}$

$q_1 - q_2$ e $p_1 - p_2$ sono interi $\quad q_1 - q_2 \leq n$ e

$$\alpha = \frac{p_1 - p_2 + \{q_1\alpha\} - \{q_2\alpha\}}{q_1 - q_2} = \frac{p_1 - p_2}{q_1 - q_2} + \frac{\{q_1\alpha\} - \{q_2\alpha\}}{q_1 - q_2}$$

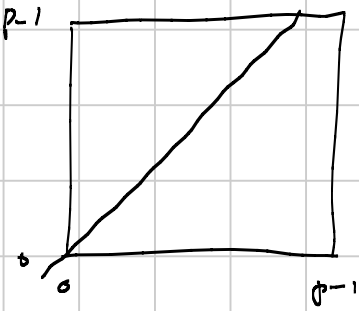
$\{q_1\alpha\} - \{q_2\alpha\} < \frac{1}{n+1}$, $\quad q_1 - q_2 \geq 1$, $\quad q_1 - q_2 \leq q$

$$\left|\alpha - \frac{p_1 - p_2}{q_1 - q_2}\right| < \frac{1}{(n+1)(q_1 - q_2)}$$

Lemma di Thue:

p primo. Esistono $|x|, |y| \leq [\sqrt{p}]$ t.c. $x \equiv my \pmod p$.

m intero $\qquad (x, y) \neq (0,0)$



$$F : (x, y) \longrightarrow \frac{x}{y} \pmod p$$

se ho che $\frac{x_1}{y_1} \equiv \frac{x_2}{y_2} \pmod p$

(dal principio dei cassetti)

$x_1, y_1 = 0, \dots [\sqrt{p}]$

$x_1 y_2 \equiv y_1 x_2$ Hmm... Oppure $G: (x,y) \longmapsto x - my \pmod p$

Abbiamo $[\sqrt{p}]^2$ coppie e p cassetti. se $x - my \equiv 0$ esiste, ok altrimenti, $p-1$ cassetti, Con un conto accurato, si vuole che abbiamo più coppie che cassetti e se $x_1 - m y_1 \equiv x_2 - m y_2 \pmod p$

allora $(x_1 - x_2) - m(y_1 - y_2) \equiv 0 \mod p$.

□

Es. Consideriamo per $n \in \mathbb{N}$ $\dfrac{2^n + 1}{n}$. Quando è intera?

1) per quali p primi?
2) per quali p^k con p primo?
3) dim. che n è sempre multiplo di 3.

1) p primo $2^p + 1 \equiv 0 \mod p$? $a \not\equiv 0 \mod p$ $a^{p-1} \equiv 1 \mod p$ (piccolo teorema di Fermat)

$2^p \equiv 2 \cdot 2^{p-1} \equiv 2 \mod p$.

$2^p + 1 \equiv 3 \mod p$. $\longrightarrow$ unica sol. $p = 3$

2) $n = p^k$? $2^{p^k} + 1 \equiv 0 \mod p^k$ picc. teor. Fermat: $2^{\varphi(p^k)} \equiv 1$

$\varphi(p^k) = p^{k-1} \cdot (p-1) = p^k - p^{k-1}$

$2^{p^k} \equiv 2^{p^k (p-1)} \cdot 2^{p^{k-1}} \equiv 2^{p^{k-1}} \mod p^k$.

$\equiv 1$

Ah, ma se $2^{p^k} + 1 \equiv 0 \mod p^k \Rightarrow 2^{p^k} + 1 \equiv 0 \mod p$. e allora

$2^{p^k} \equiv \left(2^{p^{(k-1)}}\right)^p \equiv 2^{p^{k-1}} \equiv 2^{p^{k-2}} \equiv \dots \equiv 2^p \equiv 2 \mod p$.

quindi $2^{p^k} + 1 \equiv 3 \mod p$. $\longrightarrow p = 3$ unica sol.

e k? $2^{3^k} + 1 \equiv 0 \pmod{3^k}$ $\swarrow k = 1$ ok.

$k = 2$? ok $\quad k = 3$?

$513 = 57 \cdot 9 = 19 \cdot 3^3$

posso guadagnare sempre un fattore 3??

$2^{3^k} + 1 = \left(2^{3^{k-1}}\right)^3 + 1^3 = \underbrace{\left(2^{3^{k-1}} + 1\right)}_{k \text{ fattori } 3} \left(\left(2^{3^{k-1}}\right)^2 - 2^{3^{k-1}} + 1\right)$

$\equiv 2^2 - 2 + 1 \mod 3$ ok

Quindi in $2^{3^k} + 1$ ci sono $k+1$ fattori 3 $\Rightarrow$ è divis. per 3^k

3) Supp. che $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_h^{\alpha_h}$ $\underbrace{p_1 < p_2 < \cdots < p_h}_{\text{dispari}}$ primi e $\alpha_i \geq 1$

e supp. che $2^n + 1 \equiv 0 \pmod n$

$2^n \equiv -1 \pmod n \Rightarrow 2^{2n} \equiv 1 \pmod n$ e $2^{2n} \equiv 1 \bmod p_1$

però se $p_1 \mid 2^n + 1$ so che $2^{p_1 - 1} \equiv 1 \bmod p_1$

$\Rightarrow \operatorname{ord}_{p_1}(2) \mid 2n$ e $\operatorname{ord}_{p_1}(2) \mid p_1 - 1$ quindi

$\operatorname{ord}_{p_1}(2) \mid (2n, p_1 - 1)$ ma p_1 è il più piccolo $\Rightarrow (n, p_1 - 1) = 1$

$\Rightarrow (2n, p_1 - 1) = 2 \Rightarrow \operatorname{ord}_{p_1}(2) = 2$

$2^2 \equiv 1 \bmod p_1 \Rightarrow p_1 = 3$