Teoria Dei Numeri 1 - BASIC

Titolo nota 04/09/2018

ert-uricksen

$x^2 = 7 + y^2 \qquad x, y \in \mathbb{Z}$

$(x-y)(x+y) = 7$

$3a + 2b = 5$

$a^n + b^n = c^n$

$n^2 - 6n = m^2 + m - 12$

$n^2 - 6n + 9 = m^2 + m - 3$ $\qquad (n-3)^2 = \underline{m^2+m-3} > m^2$

$\uparrow$

$m^2 + m - 3 \overset{?}{<} (m+1)^2$ $\qquad m - 3 < 2m + 1$ $\qquad m > -4$

$(m+1)^2 > (n-3)^2 > m^2$ $\qquad (n-3)^2 = 9$

$x, y \in \mathbb{N} \qquad x^5 - xy^2 + y^2 - 1 = 0$

$x^5 - 1 = y^2(x-1) \qquad x^4 + x^3 + x^2 + x + 1 = y^2$

$(x^2 + ax + b)^2 \qquad \left(x^2 + \frac{1}{2}x\right)^2 = x^4 + x^3 + \frac{1}{4}x^2 < LHS$

$\left(x^2 + \frac{1}{2}x + 1\right)^2 = x^4 + x^3 + 2x^2 + \frac{1}{4}x^2 + x + 1 > LHS$

$\left(x^2 + \frac{1}{2}x\right)^2 < y^2 < \left(x^2 + \frac{1}{2}x + 1\right)^2$

$x^4 + x^3 + x^2 + x + 1 = y^2 = \left(x^2 + \frac{1}{2}x + \frac{1}{2}\right)^2 = x^4 + x^3 + \frac{1}{4}x^2 + x^2 + \frac{1}{2}x + \frac{1}{4}$

$\frac{1}{4}x^2 - \frac{1}{2}x - \frac{3}{4} = 0 \qquad x^2 - 2x - 3 = 0 \qquad (x-3)(x+1) = 0$

CONGRUENZE

$a|b \iff \exists k \in \mathbb{Z}$ t.c. $b = ak$ $\quad a, b \in \mathbb{Z}$ $a \neq 0$

$b \equiv c \ (a) \iff a \mid b-c \iff$ resto di $\frac{b}{a}$ è = a resto $\frac{c}{a}$

$\{0, 1, 2, \dots, a-1\}$ $\quad \left\{\frac{-a+1}{2}, \frac{-a+3}{2}, \dots, \frac{a-1}{2}\right\}$

$a = 5$ $\quad \{-2, -1, 0, 1, 2\}$ $\quad \{0, 1, 2, 3, 4\}$

$[a]$ = classe di resto di a mod b

$[a+c] = [a]+[c]$ $\quad [a \cdot c] = [a] \cdot [c]$ $\quad \Leftarrow$

~~$\frac{[a]}{[c]} = [\frac{a}{c}]$~~ No!

MCD: $a, b \in \mathbb{Z}$ $\quad d = (a,b) = MCD(a,b)$ è t.c.

$d|a$, $d|b$ e $\forall c \in \mathbb{Z}, c \neq 0$ t.c. $c|a$ e $c|b \Rightarrow$

$\Rightarrow c|d$.

$(a,b) = (a, a+b) = (a+b, b)$

dati $x, y \in \mathbb{Z}$ NON vale che $(a,b) = (a, xa+yb)$

è vero però che $(a,b) = (a, b+xa)$

$(2,3) \neq (2, 1 \cdot 2 + 2 \cdot 3)$

dati $a, b, c \in \mathbb{Z}$ voglio determinare $x, y \in \mathbb{Z}$ t.c.

$ax + by = c$.

$d = (a,b)$ e $d \nmid c \Rightarrow$ no soluzioni

$(a,b)=1$ $\quad ax+by=c \quad ax'+by'=1 \quad x=cx' \quad y=cy'$

$ax+by=1 \quad (a,b)=1$.

$77x+127y=1$

$127 = 1\cdot 77 + 50$

$77 = 1\cdot 50 + 27$

$50 = 1\cdot 27 + 23$

$27 = 1\cdot 23 + 4$

$23 = 5\cdot 4 + 3$

$4 = 1\cdot 3 + 1$

$1 = 4 - 1\cdot 3 = 4 - 1\cdot(23 - 5\cdot 4) =$

$= 6\cdot 4 - 1\cdot 23 = 6\cdot(27-23) - 1\cdot 23$

$= 6\cdot 27 - 7\cdot 23 = 6\cdot 27 - 7\cdot(50-27) =$

$= -7\cdot 50 + 13\cdot 27 =$

$= -7\cdot 50 + 13(77-50) = -20\cdot 50 + 13\cdot 77$

$= \boxed{-20}\,127\,\boxed{+33}\,77$

$(-20)\cdot 127 + (33)\cdot 77 = 1 \qquad (x,y) = (-20, 33)$

$(-20+77k,\ 33-127k) \quad k\in\mathbb{Z}$

$(a,b) = d \neq 1 \quad e \quad d \mid c \qquad a' = \frac{a}{d} \quad b' = \frac{b}{d} \quad c' = \frac{c}{d}$

$(a',b') = 1$ siamo nel caso di prima

IDENTITÀ DI BEZOUT : Se $(a,b)=d$, $\exists x,y\in\mathbb{Z}$ t.c. $ax+by=d$

Torniamo alle congruenze ...

Se so che $(a,b)=1$ e un certo $c \in \mathbb{Z}$,

$c\,(b)$ $\quad \frac{c}{a}\,(b)$ $\quad c \cdot \frac{1}{a}$ cercare a' t.c. $a' \cdot a \equiv 1 (b)$

$\Rightarrow \frac{c}{a} := c \cdot a' \,(b)$

$\exists x, y$ t.c. $\quad ax + by = 1 \Rightarrow ax \equiv 1\,(b) \quad a' := x$.

questo è detto inverso moltiplicativo

mod 7 $\quad 2\,(\text{mod } 7)$ $\quad$ 4 funziona perché $4 \cdot 2 \equiv 1 (7)$

$2\,(\text{mod } 10)$ non ha inverso!

Se cerco a t.c. $2a \equiv 3\,(10)$ $\quad 2a = 3 + 10k$

$2a - 10k = 3$

↑ pari ↑ dispari

$2a \equiv 3\,(7)$ $\quad 4 \cdot 2 \cdot a \equiv 4 \cdot 3\,(7)$

$a \equiv 5\,(7)$ $\quad a \equiv \frac{3}{2}\,(7) = 3 \cdot \frac{1}{2}\,(7)$

$2a \equiv 4\,(10)$ $\quad$ ~~$a \equiv 2\,(10)$~~ No!

$\Rightarrow$ può $\quad a \equiv 2\,(5)$ $\quad 2a = 4 + 10b \quad a = 2 + 5b$

2, 7.

p si dice primo se dati $a, b \in \mathbb{Z}$ t.c. $p \mid ab \Rightarrow$

$\Rightarrow p \mid a \vee p \mid b$.

TEOREMA DI WILSON

Se p è un primo allora $(p-1)! \equiv -1\,(p)$

DIM: $\{1, \dots, p-1\}$

$ax + by = 1$ date (x_0, y_0) sol. $(x_0 + bk, y_0 - ak)$

$\Rightarrow a(x_0 + bk) \equiv a x_0 \ (b)$

$\{1, \dots, p-1\}$ $\quad x^2 \equiv 1 \ (p)$ $\quad (x-1)(x+1) \equiv 0 \ (p)$

si accoppiano

$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv -1 \ (p)$

$p = 7$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 6 \equiv -1 \ (7)$

RESIDUI QUADRATICI

a si dice residuo quadratico mod n se $\exists\, b$ t.c.

$b^2 \equiv a \ (n)$

Per $n = 3$ $\quad 0$ è R.Q. $0^2 \equiv 0$, 1 è R.Q. $1^2 \equiv 1$

$2^2 \equiv 1 \ (3) \Rightarrow$ 2 non è R.Q.

$n = 4$ $\quad 0, 2 \to 0$ $\quad 0^2 \equiv 0$ $\quad 2^2 \equiv 0$

$1, 3 \to 1$ $\quad 1^2 \equiv 1$ $\quad 3^2 \equiv 1$

$n = 5$ $\quad 0 \to 0$ $\quad 1, -1 \to 1$ $\quad 2, -2 \to -1$

Determinare al variare di $n \in \mathbb{N}$ il max di

$(100 + n^2, 100 + (n+1)^2)$

$(100 + n^2, 100 + n^2 + 2n + 1) = (100 + n^2, 100 + n^2 + 2n + 1 - 100 - n^2) =$

perché $2n+1$ è dispari

$= (100+n^2, 2n+1) = (200+2n^2, 2n+1) = (200+2n^2-2n^2-n, 2n+1) =$

$= (200-n, 2n+1) = (400-2n, 2n+1) = (401, 2n+1)$

per $n = 200$ $\quad (100+200^2, 100+(201)^2) =$

$= (100(1+400), 100\cdot 401 + 401) = 401$.

Sia p primo, determinare per quali p $x^2+px-444p$ ha soluzioni intere

$x = \frac{-p \pm \sqrt{\Delta}}{2}$ deve valere $\Delta = \square$

$\Delta = p^2 + 4\cdot 444\, p = p(p+4\cdot 444)$

$\Rightarrow \quad p \mid p+4\cdot 444 \qquad p \mid 4\cdot 444$

IMO 2016 # 4

Un insieme A si dice profumato se $A \subseteq \mathbb{N}$ e $\forall x \in A$ $\exists\, y \in A$ t.c. $(x,y) \neq 1$. $P(x) = x^2+x+1$, vogliamo determinare (se esiste) il più piccolo $b \in \mathbb{N}^+$ t.c. $\exists a \in \mathbb{N}$ $\{P(a+1), \dots, P(a+b)\}$ è profumato.

$P(n+1) - P(n) = n^2+2n+1+n+2-n^2-n-1 = 2n+2$

Se $d \mid n^2+n+1$ e $d \mid 2n+2 \Rightarrow d \mid n+1$

n^2+n+1 sempre dispari

$d \mid n^2+n+1 - n(n+1) = 1 \quad \Rightarrow \quad d = 1$

Vogliamo vedere più in generale vogliamo vedere quanto può valere $(P(n), P(n+k)) = d$

$P(n+k) - P(n) = n^2 + 2nk + k^2 + n + k + 1 - n^2 - n - 1 =$

$= k(2n+k+1)$

Abbiamo detto che se $k=1 \Rightarrow d=1$

Se $k=2$ $\quad d \mid 2\cdot(2n+3)$ $\quad d \mid n^2+n+1$ Come prima

$d \mid 2n+3$ ← anche lui è dispari

$(P(n), P(n+2)) = (P(n), 2(2n+3)) = (P(n), 2n+3) = (2P(n), 2n+3) =$

$= (2n^2+2n+2, 2n+3) = (2n^2+2n+2-2n^2-3n, 2n+3) =$

$= (-n+2, 2n+3) = (-n+2, 7) \quad \Rightarrow \quad d \mid 7$

perché $d=7$ deve valere che $7 \mid -n+2 \Rightarrow n \equiv 2(7)$

Quindi in sostanza $(P(n), P(n+2)) \neq 1 \iff n \equiv 2(7)$

$b \neq 1$. $b \neq 2$ (caso $k=1$). $b \neq 3$ (per caso $k=1$).

$b \neq 4$ perché avremmo $\{P(a+1), P(a+2), P(a+3), P(a+4)\}$

assurdo perché dovremmo avere $a+1 \equiv a+2 \equiv 2(7)$.

Se $k=3$ $\quad k(2n+k+1) = 3(2n+4)$

$(P(n), P(n+3)) = (P(n), 3(2n+4)) = (P(n), 3(n+2))$

se $3 \nmid d$ allora $(P(n), P(n+3)) = (P(n), n+2) =$

$= (n^2+n+1, n+2) = (n^2+n+1 - n^2-2n, n+2) = (-n+1, n+2) =$

$= (-n+1, 3) \Rightarrow d \mid 3 \Rightarrow d = 1$.

se $3 \mid d \Rightarrow 3 \mid n^2+n+1 \quad n(n+1) \equiv -1 \,(3) \Rightarrow n \equiv 1 \,(3)$.

$\Rightarrow n = 3m+1$. $(P(n), P(n+3)) = (P(n), 3n+6) = d$

$d \mid (3P(n), 3n+6) = (3n^2+3n+3, 3n+6) = (-3n+3, 3n+6) =$

$= (-3n+3, 9) \Rightarrow d \mid 9$. Tuttavia $n = 3m+1 \Rightarrow$

$P(n) = 9m^2+6m+1+3m+1+1 = 9m^2+9m+3 \equiv 3 \,(9)$

$\Rightarrow d = 3$. Inoltre $d = 3 \iff n \equiv 1 \,(3)$

se $k = 4 \quad k(2n+k+1) = 4 \cdot (2n+5)$

$(P(n), P(n+4)) = (P(n), 2n+5) = (2P(n), 2n+5) =$

$= (2n^2+2n+2 - 2n^2-5n, 2n+5) = (-3n+2, 2n+5) =$

$= (-n+7, 2n+5) = (-2n+14, 2n+5) = (19, 2n+5)$

$\Rightarrow d \mid 19$ affinché $d \mid 19$ deve valere $2n \equiv -5 \,(19)$

$n \equiv -50 \,(19) \quad n \equiv 7 \,(19)$. (è un se e solo se).

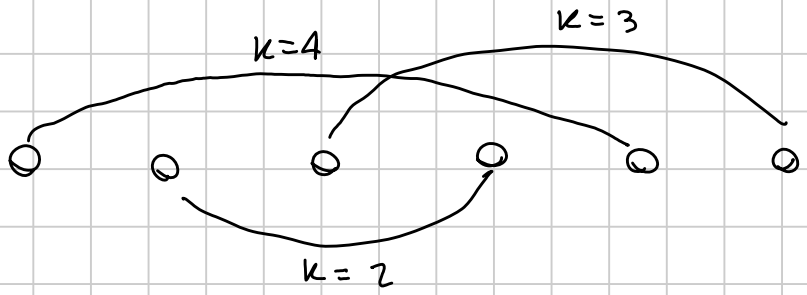
se $b = 5 \quad 2+1 \quad 2+2 \quad 2+3 \quad 2+4 \quad 2+5$

per 3, 7, 19 c'è al più una coppia con MCD $\neq 1$.

$\Rightarrow$ un tizio rimane da solo

infatti $k=4$ serve solo per $(x+1) \sim (x+5)$, $k=3$ esclude $x+3 \Rightarrow k=2$ deve essere usato per $x+3$.
Ma allora $k=3$ deve scegliere se lasciare da solo $x+2$ o $x+4$. $\Rightarrow b \neq 5$

$b=6$?



Ci riusciamo se $x+1 \equiv 7 \ (19)$, $x+2 \equiv 2 \ (7)$,

$x+3 \equiv 1 \ (3)$

$$\begin{cases} x \equiv 6 \ (19) \\ x \equiv 0 \ (7) \\ x \equiv 1 \ (3) \end{cases}$$

ESERCIZI:

PAG 10: 40 - (41) - (42) - 43 - (49) - 50 - 54 - 55 - (56)

PAG: 42 : 3 - 5

BONUS:

- Siano p, q primi tali che $\exists n \in \mathbb{N}$ per cui $\frac{p}{p+1} + \frac{q+1}{q} = \frac{2n}{n+2}$; trovare tutti i possibili valori di $p-q$

- Mostrare che la successione 5, 12, 19, 26, 33 ... non ha elementi nella forma $2^n - 1$ per un certo n.

- $mn + 2m - n - 8 = 0$

$m(n+2) - (n+2) - 6 = 0$ $\qquad (n+2)(m-1) = 6$

- p primo $\qquad 5p + 49 = a^2 \qquad 5p = (a-7)(a+7)$

- $n^2 + 5n + 16 = 169\,y \qquad n^2 + 5n + 16 \equiv 0\ (13)$

$n^2 - 8n + 16 \equiv 0\ (13) \qquad (n-4)^2 \equiv 0\ (13) \Rightarrow$

$\Rightarrow 13 \mid (n-4)^2 \Rightarrow 13 \mid n-4 \Rightarrow n \equiv 4\ (13)$

$\Rightarrow 13^2 \mid n^2 - 8n + 16$

$n^2 + 5n + 16 = n^2 - 8n + 16 + 13n = \underline{169 \cdot m^2} + 13(4 + 13m) \not\equiv 0\ (169)$

$n = \dfrac{-5 \pm \sqrt{25 - 64}}{2} \leftarrow \sqrt{-39} \equiv 0$

$n^2 + 5n + 16 \equiv \underbrace{n^2 + 5n + 3}_{(n-4)^2 + 13} \underbrace{-3 + 16}_{\equiv (n-4)^2}$

$\sqrt{-1} = x \qquad x^2 \equiv -1\ (13)$

$x \equiv 5\ (13)$

- $x^2 + 3y = 2 \qquad x^2 \equiv 2\ (3)$ NO!

- $3^y - x^2 = 41$

$3^y \equiv 1 + x^2 \equiv 1\ (4) \Rightarrow y$ pari $\qquad y = 2k$

$(3^k - x)(3^k + x) = 41 \qquad 3^k - x = 1 \qquad 3^k + x = 41$

$2 \cdot 3^k = 42 \qquad 3^k = 21$ no!

- $abc \mid (a+b+c)^n \quad \forall a,b,c$ t.c. $a \mid b^3,\ b \mid c^3,\ c \mid a^3$.

$a \mid b^3 \mid c^9 \qquad (c^9, c^3, c) = (a, b, c)$

$c^{13} \mid (a+b+c)^n = c^n(\dots)^n \qquad n = 13$.

$(a+b+c)^{13} = \sum a^i b^j c^k \qquad i+j+k = 13$

$abc \mid a^i b^j c^k \qquad c \mid a^{i-1} b^{j-1} \qquad i+j = 13$

se $i \geq 4 \quad c \mid a^3 \mid a^{i-1}$, altrimenti $j > 9 \Rightarrow c \mid b^9 \mid b^{j-1}$.

$abc \mid a^{13} \qquad bc \mid a^{12} = a^3 \cdot a^9 \Rightarrow n = 13$ funziona.

$a = 2^9 \quad b = 2^3 \quad c = 2 \qquad 2^{13} \mid (2^9 + 2^3 + 2)^n$ per $n \overset{?}{<} 13$

$(2^9 + 2^3 + 2)^n = 2^n (2^8 + 2^2 + 1)^n$.

- EGMO 2012 # 5

$$\frac{p}{p+1} + \frac{q+1}{q} = \frac{2n}{n+2}$$

$$\frac{p}{p+1} - 1 + \frac{q+1}{q} - 1 = \frac{2n}{n+2} - 2$$

$$-\frac{1}{p+1} + \frac{1}{q} = \frac{-4}{n+2} \qquad \frac{p+1-q}{(p+1)q} = \frac{-4}{n+2}$$

$(q - p - 1)(n+2) = 4q(p+1) \qquad q > p+1$

$\uparrow \quad \uparrow \quad \uparrow$

$q \mid q-p-1 \qquad q \mid p+1$, impossibile $\Rightarrow q \mid n+2$.

$(q-p-1, p+1) = (q, p+1) = 1 \Rightarrow p+1 \mid n+2$.

$q-p-1 \mid 4$

- IMO LONGLIST 1992

  prese $5+7k$, mostrare che non ci sono 2^n-1 .

$5+7k = 2^n-1 \qquad 6+7k = 2^n$ a meno di cambiare k scrivo $7k = 2^n+1 \qquad 7 \mid 2^n+1$

$1 \to 1 \quad 2 \to 4 \quad 3 \to 2 \quad -3 \to 2 \quad -2 \to 4 \quad -1 \to 1$

1, 2, 4 sono gli unici R.Q. mod 7 .

Se n è pari $2^n+1 \equiv 2, 3, 5 \ (7) \Rightarrow 7 \nmid 2^n+1$

Se n è dispari $n = 1+2m \qquad 7 \mid 2 \cdot 2^{2m} + 1 \qquad 2 \cdot 2^{2m} + 1 \equiv 0 \ (7)$

$2^{2m} \equiv -\frac{1}{2} \ (7) \equiv 3 \ (7)$ che non è R.Q.