Teoria dei numeri

ma_go

Titolo nota 03/09/2014

divisibilità: a, b interi — a **divide** b — $a \mid b$

esiste **intero** k t.c. $ak = b$.

se $a \mid b \Rightarrow |a| \leq |b|$

a meno che $b = 0$

primi: { p è un **primo** se è divisibile $\Leftrightarrow$ **Gioca** per se stesso e per 1.

def "vera": $p > 1$ è **primo** se $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

def MCD (massimo comun divisore) di a, b interi:

è il massimo dei divisori comuni.

a intero positivo ha una fattorizzazione in primi e questa fattorizzazione è unica (a meno dell'ordine).

es Dimostrare il teorema fondam. dell'aritmetica.

MCD si calcola bene dalle fattorizzazioni.

---

n intero positivo, $d(n) = \#\{$ divisori positivi di $n\}$ ← numero di

es Per quali n, $d(n)^2 = n$? ← n è ☐

⇓

α_i pari $\forall i$

Calcolare $d(n)$!

Se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_2^{\alpha_2}$, allora

(*) $d(n) = (\alpha_1+1) \cdot \ldots \cdot (\alpha_2+1)$.

es $\iff$ $\left[(\alpha_1+1) \cdot \ldots \cdot (\alpha_2+1)\right]^2 = n = p_1^{\alpha_1} \cdot \ldots \cdot p_2^{\alpha_2}$.

$\Rightarrow$ n è dispari (*) (n è $\square$ $\Leftrightarrow$ $d(n)$ è dispari)

$p_1 < p_2 < \ldots < p_2 \Rightarrow p_1 \geq 3$.

Se n ha un solo fattore primo p, $d(p^\alpha)^2 = p^\alpha$

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

es Dimostrare per induzione che $p^\alpha \geq (\alpha+1)^2$ per $\alpha \gg 0$.

$p=3$: $p^\alpha = (\alpha+1)^2$ 2 è una sol.
(col è l'unica! es)

$p \geq 5$ $p^\alpha = (\alpha+1)^2$

$(\alpha+1)^2 \leq 3^\alpha < 5^\alpha$ non ci sono sol.

trovate 1 sol: $n=9$; $n=1$ unica sol.

MCD $(1227, 4721)$

$4721 = 1227 \cdot 3 + 1040$

$1227 = 1040 \cdot 1 + 187$

$1040 = 187 \cdot 5 + 105$

$$187 = 105 \cdot 1 + 82$$
$$105 = 82 \cdot 1 + 23$$
$$82 = 23 \cdot 3 + 13$$

$23 =$	$13 \cdot 1$	10	$(*_3)$
$13 =$	$10 \cdot 1$	3	$(*_2)$
$10 =$	$3 \cdot 3$	1 → MCD!	$(*_1)$
$3 =$	$1 \cdot 3$	0	$(*_0)$

thm (Bézout) L'algoritmo di Euclide produce l'MCD

Come otteniamo tornando indietro?

$10 = 3 \cdot 3 + 1$

$13 = (3 \cdot 3 + 1) \cdot 1 + 3 = 13 = 3 \cdot$

Andiamo a provare vero Bézout (quello vero)

thm (Bézout) Se $d = MCD(a,b)$, esistono due interi h, k t.c. $h \cdot a + k \cdot b = d$.

in part. se a e b sono **coprimi**, $h \cdot a + k \cdot b = 1$.

idea Prendo 3 dalla $(*_2)$ e lo sostituisco nella $(*_1)$

$(*_2) \quad 13 = 10 \cdot 1 + 3 \Rightarrow 3 = 13 - 10$

$(*_1) \quad 10 = 3 \cdot 3 + 1$

$$10 = (13 - 10) \cdot 3 + 1 \Rightarrow$$
$$1 = (-3) \cdot 13 + 4 \cdot 10$$

($1 = d$, $-3 = h$, $13 = a$, $4 = k$, $10 = b$)

IMO 59/1 $\quad \dfrac{21n+4}{14n+3}$ è irriducibile?

Alg. di Euclide

$$21n+4 = (14n+3)\cdot 1 + (7n+1)$$

$$14n+3 = (7n+1)\cdot 2 + (1) \leftarrow \text{non c'è } n!$$

la frazione è irrid, sempre!

Variazioni: $\dfrac{21n+4}{14n+9}$

$$21n+4 = (14n+9) + 7n-5$$
$$14n+9 = (7n-5)\cdot 2 + (7) \quad [?]$$
$$7n-5 = 7\cdot n - 5$$

$$m^2+(m+1)^2 = n^4+(n+1)^4$$

$$2m^2+2m+1 = 2n^4+4n^3+6n^2+4n+1$$

$$m^2+m = n^4+2n^3+3n^2+2n$$
$$m^2+m+1 = \underbrace{n^4+2n^3+3n^2+2n+1}_{(n^2+n+1)^2}$$
$$\boxed{m^2+m+1} = x^2$$

$m \lneq \sqrt{m^2+m+1} \lneq m+1$, se $m>0$, non ci sono lol!

$m=0 \rightarrow n=0$!

IMO 06/4 $\quad 1+2^x+2^{2x+1} = y^2$

x, y interi.

$x < -1$, LHS non è intero

$x = -1$, $LHS = 2 \neq y^2$.

$x \geq 0$, $x = 0$ $\quad 1 + 1 + 2 = 4 = 2^2$.

$(0, \pm 2) \rightsquigarrow$ bl.

$x > 0$, y è dispari.

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

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

$MCD(y-1, y+1) \mid (y+1) - (y-1) = 2 \Rightarrow MCD = 2$.

$d \mid a, \; d \mid b \Rightarrow d \mid a \pm b$. $\quad (d \mid a + kb)$

$$1 + 2^x + 2 \cdot 2^{2x} \qquad 2^{x-1} = a$$

$$1 + 2 \cdot a + 2 \cdot a^2 \cdot 4 = 1 + 2a + 8a^2 =$$

$$= (a+1)^2 + 7a^2$$

$$y^2 = (a+1)^2 + \underbrace{7a^2}_{\text{pochi fattori primi!}}$$

$$(y - a - 1)(y + a + 1) = 7a^2$$

$$M \qquad N$$

$MCD(M, N) \mid 2y \rightsquigarrow y$ dispari

(Se un po' di att., non hanno alcun fatt. in comune)

$$MCD = 2$$

$$M \cdot N = 7 \cdot 2^{2(x-1)} \qquad M < N$$

Un paio di possibilità:

$2, 2^{2x-3}, 7$ da distribuire

$2 \cdot 7, 2^{2x-3}$

$2, 7 \cdot 2^{2x-3}$

$M = 14, \quad N = 2^{2x-3}$ --- (es)

$M = 2, \quad N = 7 \cdot 2^{2x-3}$?

$\parallel$

$$\begin{cases} y - 2^{x-1} - 1 = 2 \\ y + 2^{x-1} + 1 = 7 \cdot 2^{2x-3} \end{cases}$$

$$2^x + 2 = 7 \cdot 2^{2x-3} - 2$$

$$\underbrace{2^x}_{\text{div. per } 8} + 4 = \underbrace{7 \cdot 2^{2x-3}}_{\text{divisibile per } 8} \qquad \text{se } x \geq 3$$

CONGRUENZE:

def $a \equiv b \pmod m$ se

- $m \mid (a-b)$
- $a = b + km$ per qualche $k \in \mathbb{Z}$
- il resto della div. di a per m $\parallel$ " " " b " " .

non si dovrebbe scrivere $5 \bmod 3 = 2$.

Classi di congruenza $\mathbb{Z}/m\mathbb{Z}$.

Ricordiamo: $a = b \Rightarrow a \equiv b \pmod m$

\pmod{m}.

$$a \equiv b \pmod m, \quad c \equiv d \pmod m$$

$$\Rightarrow \quad a + kc \equiv b + kd \pmod m$$
$$a \cdot c \equiv b \cdot d \pmod m$$

La divisione si comporta bene con i modi "coprimi" col divisore.

Bézout entra in scena:

Ø intero, cerco h inverso di a mod m,

dove $MCD(a, m) = 1$.

ovvero cerco h intero tale che $h \cdot a \equiv 1 \pmod m$.

Dalla seconda def. di $\equiv$, $h \cdot a = 1 + km$ per qualche k.

$$h \cdot a - k \cdot m = 1$$

Posso trovare h e k interi e solo se $MCD(a, m) = 1$.

(li trovo esplicitamente con Euclide).

Quante sono le soluzioni?

Prendo un'altra soluzione (h', k')

$$h' \cdot a - k' m = 1 \quad -$$
$$h \cdot a - k \cdot m = 1$$

$$(h - h') \cdot a - (k - k') \cdot m = 0$$
$$(h - h') \cdot a = (k - k') \cdot m$$

$h - h' = \ell \cdot m$ per qualche ℓ.

$h \equiv h' \pmod m$

h, h' inversi mod m

$h \cdot a \equiv h' \cdot a \Rightarrow (h' - h) \cdot a \equiv 0$

$\Rightarrow (h' - h) \cdot \cancel{a \cdot h} \equiv 0 \pmod m$

<u>oss</u> se m è primo, l'unica classe di resto non invertibile è 0.

a è invertibile mod $p \iff p \nmid a$. (p primo)

- $x^2 + y^2 = 2015$

<u>modulo 4</u>

$x^2 + y^2 \equiv 2015 \equiv 3 \equiv -1 \pmod 4$

se x è pari $\Rightarrow 4 \mid x^2 \Rightarrow x^2 \equiv 0 \pmod 4$

se x è dispari $\Rightarrow (2y+1)^2 = \underbrace{4y^2 + 4y}_{\text{div. per } 4} + 1 \equiv 1 \pmod 4$

$x \equiv \begin{cases} +1 \\ -1 \end{cases} \pmod 4 \Rightarrow x^2 = (\pm 1)^2 = 1 \equiv 1 \pmod 4$

$x^2 + y^2 \quad \begin{cases} 0 \\ 1 \\ 2 \end{cases} \pmod 4$ <u>no</u>

$x^2 + y^2 = 2208$

mod 3: $x^2 \begin{cases} 0 \equiv 0 \\ (\pm 1)^2 \equiv 1 \end{cases}$

x^2+y^2 $\left\{\begin{matrix}0\\1\\2\end{matrix}\right.$ $\longrightarrow$ sob $\iff x\equiv y\equiv 0$ (3)

$$x^2+y^2 \equiv 0 \pmod 7$$

IMO 2009/1 k, n interi positivi $2 \le k \le n$.
$a_1, \dots, a_k$ interi distinti in $\{1, \dots, n\}$.
Supponiamo che $n \mid a_j(a_{j+1}-1)$ per $j=1,\dots,k-1$.

Dimostrare che $n \nmid a_k(a_1-1)$.

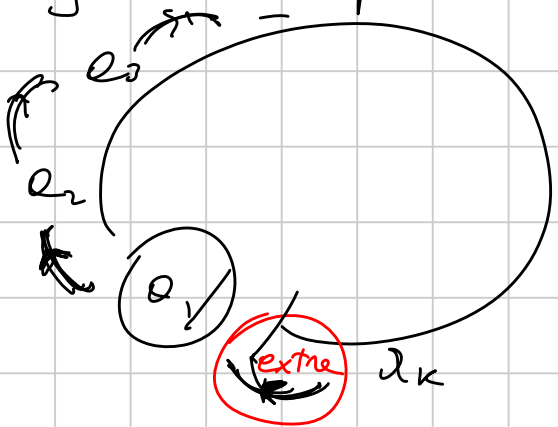
$$a_j(a_{j+1}-1) \equiv 0 \pmod n$$

$$a_j \cdot a_{j+1} \equiv a_j \pmod n$$

$$a_1 \cdot a_2 \equiv a_1 \pmod n$$
$$a_2 \cdot a_3 \equiv a_2 \pmod n$$
$$\Downarrow$$
$$a_1 \cdot a_2 \cdot a_3 \equiv a_1 \cdot a_2 \equiv a_1 \pmod n$$

$\Rightarrow$ per induzione, $\underbrace{a_1 \cdot \dots \cdot a_k} \equiv a_1 \pmod n$

e fossi fatto le ipotesi, $a_k \cdot a_1 \equiv a_1 \pmod n$
$\Rightarrow$ ogni prodotto di k consecutivi è congruo al primo:



$a_1 \cdot \ldots \cdot a_k \equiv a_1$,

$a_2 \cdot \ldots \cdot a_k \cdot a_1 \equiv a_2 \pmod n$ □

$p^2 - 2q^2 = 1$ cu p, q prime

p dispar. $\Rightarrow p-1, p+1$ pari

$(p-1)(p+1) = p^2 - 1 = 2q^2 \Rightarrow q = 2 \Rightarrow p = 3$.

$\not\exists$ $p, q > 2 \Rightarrow$ sunt dispari $\Rightarrow p^2, q^2 \equiv 1 \pmod 4$

$\Rightarrow 1 - 2 \equiv 1 \pmod 4$ imposibil.

Pe rând: n $4n+9$ & $9n+1$ sunt entrambi □?

$$\begin{cases} 4n+9 = x^2 \\ 9n+1 = y^2 \end{cases} \quad \begin{cases} x^2 - y^2 = -5n + 8 \\ (x-y)(x+y) = 8 - 5n \end{cases} \ddot\smile$$

mod 3 $\quad x^2 \equiv n \pmod 3$

$y^2 \equiv 1 \pmod 3$

n par: $\quad$ n dispar, $4n \equiv 4 \pmod 8$

$\Rightarrow 4n + 9 \equiv 4 + 1 \equiv 5 \pmod 8$

$4y(y+1) + 1 \equiv 1 \pmod 8$

$\Rightarrow n$ par.

$9x^2 - 4y^2 = \cancel{36n} + 81 - \cancel{36n} - 4$ ☺

$(3x - 2y)(3x + 2y) = 77 = 7 \cdot 11$

1 $\quad$ 77 $\Rightarrow x = 13, y = 19 \Rightarrow n = 40$

7 $\quad$ 11 $\Rightarrow x = 3, y = 1 \Rightarrow n = 0$

$$4n+9 = 13^2 \Rightarrow n = \frac{169-9}{4} = 40$$

$a_1, \dots, a_{37}$ interi $\Rightarrow \exists 1 \le i \le j \le 37$ t.c.

$S(i,j) = a_i + a_{i+1} + \dots + a_{j-1} + a_j$ è div. per 37.

$$S(i,j) = \underbrace{S(j,1)}_{S_j} - \underbrace{S(i-1,1)}_{S_{i-1}}$$

$S_1, \dots, S_{37}$

$a_1, \; a_1+a_2, \dots, \; a_1+\dots+a_{37}$

ORA, CASSETTI: o ben due diversi $\Rightarrow \exists j$ t.c. $S(j,1) \equiv 0$.

o a me ben 2 uguali $\Rightarrow S_j - S_i \equiv 0$.

FINE.

Esercizi:

- es. 36, 39, 45, pp. 9-11
- es. 2 p. 38
- per quali m $m^4 + 4^m$ è primo?
- risolvere $\frac{1}{m} + \frac{1}{n} = \frac{1}{3}$ $(m, n > 0)$
- $p^3 + q^2 = 2^4$ $(p, q, 2$ primi$)$

es 21 Per quali valori del primo p l'equazione

$$x^2 + px - 444p = 0$$

ha radici intere?

$\triangle = \square$. ∴

$\triangle = p^2 + 4 \cdot 444p = n^2$

$p \mid n \Rightarrow p^2 \mid n^2 \qquad p^2 \mid p^2$

$p^2 \mid n^2 - p^2 \Rightarrow p^2 \mid 4 \cdot 444 \cdot p$

$\Rightarrow p \mid 4 \cdot 444 = 2^4 \cdot 3 \cdot 37$

$p = 2 \qquad 4 + 1776 \cdot 2 = 3556 \quad \cdot < 60^2$

$\uparrow$

59^2

$p = 3 \qquad 9 + 1776 \cdot 3 = 5337$ ✗ non □

$p = 37 \qquad 37^2 + 37 \cdot 37 \cdot 16 \cdot 3 =$

$37^2 (1 + 48) = (7 \cdot 37)^2 .$

□!

es 3| $m^4 + 4^m .$

0 $m = 1$ funziona

1 m dev'esser dispari oppure $0 \Rightarrow$ dispari

2 $m = 2n+1$

$m^4 + 4^{2m+1} = m^4 + 4 \cdot 4^{2m} =$

$= m^4 + 4 \cdot (2^n)^4$

$m = x, \; 2^n = y \qquad x^4 + 4y^4$

□ □

$\underbrace{\left(x^4 + 4x^2y^2 + 4y^4\right)}_{\square} - \underbrace{4x^2y^2}_{\square} =$

(Sophie Germaine) $(x^2 + 2y^2 - 2xy)(x^2 + 2y^2 + 2xy)$

$$x^2+2y^2-2xy=1$$

$$m^2+2\cdot 2^{2n}-2^n\cdot m$$

$$2\cdot 2^{2n}-2^n\cdot(2n+1)+(2n+1)^2$$

$$2^{2n+1} > 2^n\cdot(2n+1)+(2n+1)^2$$

per induzione es

□

$$\frac{1}{m}+\frac{1}{n}=\frac{1}{p} \qquad p \text{ primo}$$

$$pn+pm=m\cdot n$$

$$mn-p\cdot m-p\cdot n=0$$

$$(m-p)(n-p)=mn-pm-pn+p^2=p^2$$

WLOG $m \geq n$

$m-p \geq n-p$

- $n-p = 1 \Rightarrow m-p=p^2$
- $n-p = p \Rightarrow m-p=p \Rightarrow \frac{1}{2p}+\frac{1}{2p}=\frac{1}{p}$

$$\begin{cases} n-p=1 \\ m-p=p^2 \end{cases} \Rightarrow \begin{matrix} n=1+p \\ m=p^2+p \end{matrix}$$

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

$$=\frac{1}{p+1}\cdot\frac{p+1}{p}=\frac{1}{p}$$

$$S=\{(2p,p),(p+1,p^2+p),(p^2+p,p+1)\} \Leftarrow$$

es 5 $\quad p^3 + q^2 = r^4$

$$p^3 = r^4 - q^2 = (r^2 - q)(r^2 + q)$$

2 casi: $\begin{cases} r^2 - q = 1 \\ r^2 + q = p^3 \end{cases}$ oppure $\begin{cases} r^2 - q = p \\ r^2 + q = p^2 \end{cases}$

1) ~~$2r^2 = 1 + p^3$~~ $\quad q = r^2 - 1 = (r-1)(r+1)$

~~$2q = p^3 - 1$~~ $\Downarrow$

$r = 2$

$\Downarrow$

$q = 3, \; p = \underline{\text{no}}.$

$p^2 - r^2 = q \Rightarrow (p-r)(p+r) = q \Rightarrow p - r = 1$

$p = 3, \; r = 2$ che non funziona.

(Forse) Abbiamo trovato le sol. con q ed r primi. □

Seconda soluzione $\quad p, q, r = 2$ $\underline{\text{no}}$ (non va)

$p^3 + q^2 = r^4 \Rightarrow$ ce n'è ~~almeno~~ (poi

$p = 2$ non funziona: $\quad 8 = (r^2 - q)(r^2 + q)$

$\begin{cases} r^2 - q = 2 \\ r^2 + q = 4 \end{cases}$

$q = 2$ non funziona

$r = 2 \quad p^3 + q^2 = 16$ non funziona. □