SENIOR 2015 - N1

Titolo nota 23/08/2015

- NUMERI PRIMI

  $p > 1$ divisibili solo per sè stessi e per 1

  2, 3, 5, 7, ...

- FATTORIZZAZIONE UNICA

  Ogni numero intero positivo ammette un'unica fattorizzazione come prodotto di primi

  1 = prodotto di nessun numero primo
  $= 2^0 \cdot 3^0 \cdot 5^0 \cdots$

  $12 = 2^2 \cdot 3 \cdot 5^0 \cdot 7^0 \cdots$

  $2^{\cdots} \cdot 3^{\cdots} \cdot 5^{\cdots} \cdots$

- DIVISIBILITÀ

  $a \mid b$ "a divide b" se b è un multiplo di a, ovvero $b = K \cdot a$ con K intero

  $a \neq 0$

  Oss: $\pm 1 \mid b$ per ogni b intero
  $a \mid 0$ per ogni $a \neq 0$ intero

Fatto: $a \mid b$ se e solo se per ogni primo p che divide a (p compare nella fattoriz. di a con esponente K)
$p^K \mid b$

$a \mid b$ e $b \mid c \Rightarrow a \mid c$

Quindi $p^k \mid a$ e $a \mid b \Rightarrow p^k \mid b$

Viceversa: $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$b = p_1^{\beta_1} \cdots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \cdots p_{r+s}^{\beta_{r+s}}$

Se $\alpha_1 \le \beta_1$

$\alpha_2 \le \beta_2$

$\vdots$

$\frac{b}{a} = p_1^{(\beta_1 - \alpha_1)} \cdot p_2^{\beta_2 - \alpha_2} \cdots p_{r+1}^{\beta_{r+1}} \cdots$ intero

($\beta_1 - \alpha_1 \ge 0$, $\beta_2 - \alpha_2 \ge 0$)

$\Rightarrow a \mid b$

- MCD a, b interi non entrambi nulli

(a, b) è il più grande divisore comune tra a e b

Es: $(12, 15) = 3$

PROPRIETÀ: se $d \mid a$ e $d \mid b$, allora $d \mid (a, b)$

$p \mid d$ p primo

VALUTAZIONE p-ADICA $v_p(x)$ (x intero)

è il massimo esponente k tale che $p^k \mid x$

$v_2(12) = 2$

$v_p(d) \le v_p(a)$ perché $d \mid a$

$v_p(d) \le v_p(b)$ perché $d \mid b$

$v_p(d) \le \min\left(v_p(a), v_p(b)\right) = v_p((a,b))$

$(12, 15) = 3$

$2^2 \cdot 3 \quad 3 \cdot 5$

- ALGORITMO DI EUCLIDE

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

DIM: Vogliamo dimostrare che $d = (a,b)$ è il MCD tra $a+b$ e b

- $d \mid a+b$ e $d \mid b$

  ok perché $d \mid a$ e $d \mid b \Rightarrow d \mid a+b$

- Quindi $d \mid (a+b, b)$

Sia $d' = (a+b, b)$. $\quad d' \mid b$

$d' \mid a = (a+b) - b$

$\Downarrow$

$d' \mid (a,b) = d$

Conclusione: $d \mid d'$ e $d' \mid d \Rightarrow d = d'$

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

$(a,b) = (a-b, b)$]

Più in generale: $(a,b) = (a+kb, b)$ per qualsiasi k intero.

ES: $k=2 \quad (a,b) = (a+b, b) = (a+b+b, b) = (a+2b, b)$

INDUZIONE

$(123, 36) = 3$ $\qquad (a,b) = (a+kb, b)$

$123 = 36 \cdot 3 + 15$

$$(123, 36) = (123 - \overbrace{36 \cdot 3}^{108}, 36) = (15, 36)$$

$$
\begin{aligned}
&= (36, 15) \\
&= (36 - 15\cdot 2, 15) \\
&= (36 - 30, 15) \\
&= (6, 15) \\
&= (15, 6) \\
&= (15 - 6\cdot 2, 6) \\
&= (3, 6) \\
&= (6 - 3\cdot 2, 3) \\
&= (0, 3)
\end{aligned}
$$

$(a, 0) = |a| \quad a \neq 0$

$123 = \boxed{36}\cdot 3 + \boxed{15}$

$36 = \boxed{15}\cdot 2 + \boxed{6}$

$15 = \boxed{6}\cdot 2 + \boxed{3}$ ← MCD (l'ultimo resto $\neq 0$)

$6 = 3\cdot 2 + \boxed{0}$

- COMBINAZIONI LINEARI DI NUMERI INTERI

123, 36

Quali numeri potete scrivere nella forma $123x + 36y$? (con x, y interi)

$123 - 36$

> a, b si dicono "coprimi" o "primi tra loro" se $(a, b) = 1$

$a, b \quad (a,b) \mid ax + by$ per ogni x, y

Oss 1:

$(123, 36) = 3$ $\qquad$ $123x + 36y = 9$

$41x + 12y = 3$

Oss 2: si può ottenere (a,b) come combinazione lineare

$$123 = 36 \cdot 3 + 15$$
$$36 = 15 \cdot 2 + 6$$
$$15 = 6 \cdot 2 + 3 \quad \leftarrow \text{MCD}$$
$$6 = 3 \cdot 2 + 0$$

$$\begin{aligned} 3 &= 15 - 6 \cdot 2 \\ &= 15 - (36 - 15 \cdot 2) \cdot 2 \\ &= 15 \cdot 5 - 36 \cdot 2 \\ &= (123 - 36 \cdot 3) \cdot 5 - 36 \cdot 2 \\ &= 123 \cdot 5 - 36 \cdot 17 \end{aligned}$$

$3 = 123x + 36y$ $\qquad$ $x = 5$, $y = -17$

Oss 3 Per ottenere un multiplo di (a,b) come comb. lineare di a e b ...?

$$(a,b) = a \cdot x_0 + b \cdot y_0$$

$$k \cdot (a,b) = a \cdot \underbrace{(kx_0)}_{x} + b \cdot \underbrace{(ky_0)}_{y}$$

$3 = 123x + 36y$ $\qquad$ $x_0 = 5$, $y_0 = -17$

$$3 = 123x + 36y \qquad x, y \text{ interi}$$

$$3 = 123 \cdot \underbrace{5}_{x_0} + 36 \cdot \underbrace{(-17)}_{y_0}$$

$$0 = 123(x - \underbrace{x_0}_{5}) + 36(y - \underbrace{y_0}_{-17})$$

$$123(x - x_0) = -36 \cdot (y - y_0)$$

$$41(x - x_0) = -12 \cdot (y - y_0)$$

$$12 \mid x - x_0 \qquad x - x_0 = 12k \quad k \text{ intero}$$

$$41 \cdot 12k = -12 \cdot (y - y_0)$$

$$y - y_0 = -41k$$

$$x = x_0 + 12k = 5 + 12k$$

$$y = y_0 - 41k = -17 - 41k$$

$(5 + 12k, \; -17 - 41k)$ al variare di k intero sono tutte le soluzioni intere dell'equazione

$$123x + 36y = 3$$

$\Rightarrow ax + by = t \cdot (a, b)$ $\quad a, b, t$ fissati

Cercate le soluzioni (x, y)

- Trovate una coppia x_0, y_0 particolare

$\Rightarrow ax_0 + by_0 = t(a, b)$

$$a(x - x_0) + b(y - y_0) = 0$$

$$\frac{a}{(a,b)}(x-x_0) = -\frac{b}{(a,b)}(y-y_0) \qquad \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

$$x - x_0 = \frac{b}{(a,b)} k$$

$$y - y_0 = -\frac{a}{(a,b)} k$$

Conclusione: le soluzioni sono $\begin{cases} x = \frac{b}{(a,b)} k + x_0 \\ y = -\frac{a}{(a,b)} k + y_0 \end{cases}$

al variare di k intero

$k = 0 \rightarrow \begin{matrix} x = x_0 \\ y = y_0 \end{matrix}$

- EQUAZIONI DIOFANTEE

0) $ax + by = c$ "equazione diofantea lineare"

$3^x + 5 \cdot y^7 + z^4 = 9$

1) $xy = 15$

$3 \cdot 5$

x	y
1	15
3	5
5	.
15	.
-1	
-3	
-5	
-15	

2) $x^2 - y^2 = 9$

$(x+y)(x-y) = 3^2$

$x+y$	$x-y$
1	9
3	3
9	1
-1	-9
-3	-3
-9	-1

$\begin{cases} x+y=1 \\ x-y=9 \end{cases}$

$2x = 10 \quad x = 5$

$2y = -8 \quad y = -4$

$\begin{cases} x+y = d \\ x-y = \frac{9}{d} \end{cases} \quad d \mid 9$

$2x = d + \frac{9}{d}$

$\left[\begin{array}{l} x = \frac{d + \frac{9}{d}}{2} \\ y = \frac{d - 9/d}{2} \end{array} \right.$ (a = d, b = 9/d)

2bis) $x^2 - y^2 = 14$

$\begin{cases} x+y = a \\ x-y = b \end{cases} \quad ab = 14$

$x = \frac{a+b}{2}$

$y = \frac{a-b}{2}$

non sono mai interi!

3) $xy + x + y = 11$

$xy + x + y + 1 = 12$

$(x+1)(y+1) = 12$

$x+1$	$y+1$
1	
2	
3	
⋮	⋮

4) $5xy + 3x + y = 3$

$+a$

$5xy + 3x + y + a = (5x + \alpha)(y + \beta)$

$5xy + 5\beta \cdot x + \alpha \cdot y + \alpha\beta$

$\alpha = 1$

$\beta = 3/5$

$$5xy + 3x + y + 3/5 = (5x+1)(y+3/5)$$

$$= 3 + a = 3 + 3/5$$

$$(5x+1)(y+3/5) = 3 + 3/5$$

$$(5x+1)(5y+3) = 18$$

$$18 = ab \qquad \begin{cases} 5x+1 = a \\ 5y+3 = b \end{cases} \qquad \begin{matrix} a = 18 \\ b = 1 \end{matrix} \text{ no!}$$

$$\begin{matrix} a = 1 \\ b = 18 \end{matrix} \qquad \begin{matrix} x = 0 \\ y = 3 \end{matrix}$$

$$\begin{matrix} a = 6 \\ b = 3 \end{matrix} \qquad \begin{matrix} x = 1 \\ y = 0 \end{matrix}$$

3) $xy + x + y = 11$

Ricaviamo x

$$x(y+1) = 11 - y$$

$$x = \frac{11-y}{y+1} = \frac{12-(y+1)}{y+1} = \frac{12}{y+1} - 1$$

$$x = \underbrace{\frac{12}{y+1} - 1}$$

Quando $\frac{12}{y+1} - 1$ è intero?

$$y+1 \mid 12$$

5) $\dfrac{3x^2 - 4x + 7}{x-3}$ per quali interi x è intero?

$3x(x-3)$

~~$3x^2 - 9x +$~~

$$\frac{3x^2-4x+7}{x-3} = \frac{r}{x-3} + \text{quoziente}$$

$r = 1$

$r = 3\cdot 3^2 - 4\cdot 3 + 7 = 22$

$\frac{22}{x-3}$ intero $\quad x-3$ divisore di 22

...

6) $\frac{x^3+5}{x^2-1}$ per quali x interi è intero?

$$= \frac{x+5}{x^2-1} + \frac{x}{\quad}$$

$|x+5| \geq |x^2-1|$ ←

oppure $x+5=0$

CONGRUENZE

Domanda: che giorno sarà il 3/9/2016 ?

sabato (giovedì + 2)

$$365 = \underline{52} \cdot 7 + \underline{1}$$

"modulo 7"

Qual è il resto della divisione di 365 per 7 ?

a, b interi $\quad m$ intero ≥ 2

$a \equiv b \ (m)$ "a è congruo a b modulo m"

se $m \mid a-b$

equiv: $a = b + km$ per qualche k intero

equiv: a e b hanno lo stesso resto nella divisione per m.

$m = 7$

		...	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	...				

7 colonne

- 365
- 365 + 15

Proprietà:

se $a \equiv a' \ (m)$

e $b \equiv b' \ (m)$

allora $a+b \equiv a'+b' \ (m)$

$365 \equiv 1 \ (7)$

$15 \equiv 1 \ (7)$

$365+15 = 1+1 \ (7)$

$a = a' + km$

$b = b' + hm$

$a+b = a' + km + b' + hm = a'+b' + (k+h)m$

$a \equiv a' \ (m)$ & $b \equiv b' \ (m)$

$\Rightarrow ab \equiv a'b' \ (m)$

$ab = (a'+km)(b'+hm) = a'b' + m(kb' + ha' + khm)$

$365 \cdot 365 \equiv 1 \cdot 1 \equiv 1 \quad (7)$

$365^3 \equiv 365 \cdot 365 \cdot 365 \equiv 1 \cdot 1 \cdot 1 \equiv 1 \quad (7)$

$m = 2$ Lavorare modulo 2 è come ragionare con le parità

$P + D = D$

$0 + 1 \equiv 1 \quad (2)$

$P \cdot D = P$

$0 \cdot 1 \equiv 0 \quad (2)$

Come si comportano le potenze?

$m = 6$

$2015 \equiv 5 \equiv -1 \quad (6)$

$2015^2 \equiv (-1)^2 \equiv 1 \quad (6)$

$2015^3 \equiv (-1)^3 \equiv -1 \quad (6)$

$m = 5$

$333 \equiv 3 \quad (5)$

$333^2 \equiv 3^2 = 9 \equiv 4 \quad (5)$

$333^3 \equiv 333^2 \cdot 333 \equiv 4 \cdot 3 = 12 \equiv 2 \quad (5)$

$333^4 \equiv 2 \cdot 3 = 6 \equiv 1 \quad (5)$

$333^5 \equiv 1 \cdot 3 \equiv 3$

4

2

1

$333^{2015} \equiv 333^{3} \equiv 2 \quad (5)$ (4)

ATTENZIONE: GLI ESPONENTI NON SI DEVONO RIDURRE MODULO m

$m = 12 \qquad 10^k$

$10 \equiv 10 \equiv -2 \quad (12)$] ANTIPERIODO 1

$10^2 \equiv (-2)^2 = 4 \quad (12)$ } PERIODO 1

$10^3 \equiv -8 \equiv 4 \quad (12)$

$10^4 \equiv 4 \quad (12)$

$10^{2015} \equiv \cancel{8}\ 4$

In generale: a^k modulo m al variare di k c'è un antiperiodo + periodo

PROBLEMA: Un multiplo di 5 può essere $\equiv 4 \ (7)$?

Sì. Es: $25 \equiv 4 \ (7)$

- $5x \equiv 4 \ (7)$
- $5x = 4 + 7k$ Equazione diofantea lineare

Risolvere congruenze del tipo $ax \equiv b \ (m)$
è come risolvere equazioni del tipo $ax - m \cdot k = b$
incognite: x, k.

$5 \equiv -2 \ (7)$

$\begin{cases} -2x \equiv 4 \ (7) \\ x \equiv -2 \ (7) \end{cases}$ ⚠

Si può dividere per 2 a destra e a sinistra perché $2 \nmid 7$

$\begin{cases} -2x \equiv 4 \ (6) & x = 1 \ \checkmark \\ -x \equiv 2 \ (6) & x = 1 \ \text{NO!} \end{cases}$

Dividere entrambi i membri di una congruenza per a si può fare a patto che $(a, m) = 1$

Es $-2 \equiv 4 \ (6)$ VERO
$-1 \equiv 2 \ (6)$ FALSO

$ab \equiv ac \ (m) \overset{?}{\Rightarrow} b \equiv c \ (m)$

$m \mid ab - ac = a(b-c) \Rightarrow m \mid b - c$

Se a ha fattori in comune con m, può venire che siano importanti perché $a(b-c)$ sia multiplo di m.

$ax \equiv b \ (m) \qquad ax - km = b$

$x = x_0 + \frac{m}{(a,m)} \cdot t$ al variare di t intero

Es: $2x \equiv 1 \ (4)$ NO. $\quad 2x - 4k = 1$

MORALE:
- per avere soluzioni $(a,m) \mid b$
- se c'è almeno una soluzione x_0
  tutte le soluzioni sono: $x = x_0 + \frac{m}{(a,m)} \cdot t$

CASO PARTICOLARE $(a,m) = 1$

$ax \equiv b \ (m)$
- c'è soluzione
- soluzioni: $x_0 + m \cdot t$

Se ci interessa x mod m, c'è un'unica soluzione!
La congruenza $ax \equiv b \ (m)$ ha <u>esattamente</u> una soluzione

se $b = 1$
"inverso moltiplicativo di a mod m"

ES: $2x \equiv 1 \ (5) \longrightarrow x \equiv 3 \ (5)$
3 è l'inverso di 2 mod 5
$3 \cdot 2 \equiv 1 \ (5)$

ESERCIZI:

BREVI (pagg. 9, 10, 11) | 38, 39, 40, 41
43, 44, 45

LUNGHI (pag 39) | 6, 8, 9

- Dimostrare che $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$ non è mai intero per alcun valore di n.

CORREZIONE

38) $p^2 \mid a^3 \Rightarrow p^6 \mid a^6$? SI

$\Rightarrow p \mid a \Rightarrow$

40) (a) $= \frac{n+7}{2n+1} = \frac{13/2}{2n+1} + \frac{1}{2}$

$n+7 \mid 2n+1$

$-n-\frac{1}{2} \mid \frac{1}{2}$

$\frac{13}{2}$

(2a) $= \frac{13}{2n+1} + 1$ $\quad 2n+1 \mid 13$

41) $x^3 - y^3 = 7004$

- mod 7 : $x^3 - y^3 \equiv 4 \ (7)$

$x^3 \equiv \begin{cases} 0 \\ 1 \\ -1 \end{cases}$

$0^3 = 0$
$1^3 = 1$
$2^3 = 8 \equiv 1$
$3^3 \equiv 27 \equiv -1$

- $\underbrace{(x-y)}_{a}\underbrace{(x^2+xy+y^2)}_{b} = 2^2 \cdot 17 \cdot 103$

$\begin{cases} x-y = a \\ x^2+xy+y^2 = b \end{cases}$ $\quad ab = 2^2 \cdot 17 \cdot 103$

- $x^2+xy+y^2 > 0 \quad a, b > 0$
- $x > y$

$|x-y| \leq \max(x, y)$

$x^2+xy+y^2 = (x-y)^2 + 3xy$

$\begin{cases} x-y = a \\ (x-y)^2 + 3xy = b \end{cases}$ $\quad \begin{cases} x-y = a \\ 3xy = b-a^2 \end{cases}$

$$\begin{cases} x-y=a \\ xy=\underbrace{\frac{b-a^2}{3}} \end{cases}$$

$ab = 7ax$

$a^2 \equiv 1 \ (3)$

$a \equiv 1 \ (3)$

$a \equiv 2 \ (3)$

$b \equiv 1 \ (3)$

$x-y \le x^2+xy+y^2$

$y=-z$ $\qquad x+z \le x^2+z^2-xz$

$x \le z$ $\qquad x^2+z(\underbrace{z-x}_{\ge 0})$

$x=z$ a parte

$z-x \ge 1$ $\qquad x^2+z(z-x) \ge x^2+z \ge x+z$

⑥ $d = MCD$ $\qquad p^4-q^4$ $\qquad p,q$ numeri primi di ≥ 2 cifre

$p=13$
$q=11$ $\qquad p^4-q^4 = 2^5 \cdot 3 \cdot 5 \cdot 29$ ←

$d \mid 2^5 \cdot 3 \cdot 5 \cdot 29$

- fattore 2 $\qquad p^4-q^4 = \underbrace{(p^2+q^2)}(\underbrace{p+q}_{A})(\underbrace{p-q}_{B})$

mod 4
p,q dispari
$p \equiv 1 \ (4) \searrow$
$p \equiv 3 \ (4) \nearrow \quad p^2 \equiv 1 \ (4)$

$p^2+q^2 \equiv 2 \ (4)$

$v_2(p^2+q^2) = 1$

$A+B = 2p \equiv 2 \ (4)$

Uno dei due è $\equiv 2 \ (4)$ e l'altro $\equiv 0 \ (4)$

$2^4 \mid p^4-q^4$

$(p+q)(p-q)$ mod 8

$p+q \equiv 2 \ (8)$
$p-q \equiv 4 \ (8)$

$p \equiv 3 (8)$
$q \equiv -1 (8)$] $p = 19$, $q = 23$

$v_2(d) = 4$

- fattore 3 $\quad p^4 - q^4$ $\quad p \equiv 1 (3)$, $p \equiv 2 (3)$ $\rightarrow p^2 \equiv 1 (3) \rightarrow p^4 \equiv 1 (3)$

$p^4 - q^4 \equiv 1 - 1 \equiv 0 (3)$

$v_3(d) = 1$

- fattore 5 $\quad p^4 - q^4$ $\quad p \equiv 1 (5) \rightarrow p^2 \equiv 1 (5)$, $p \equiv 2 (5)$, $p \equiv 3 (5)$, $p \equiv 4 (5) \rightarrow p^2 \equiv 4 (5)$ $\rightarrow p^4 \equiv 1 (5)$

$p^4 - q^4 \equiv 1 - 1 \equiv 0 (5)$

$v_5(d) = 1$

- fattore 29 $\quad p = 29 \quad q \neq 29$

$29 \nmid p^4 - q^4$

$d = 2^4 \cdot 3 \cdot 5$

(8) $d_n = (100 + n^2, 100 + (n+1)^2)$ $\quad (a, b) = (a + kb, b)$

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

$= (100 + n^2, 2n + 1)$ $\leftarrow$ $\quad 2n + 1 = d \cdot k$ $\quad n = \frac{dk - 1}{2}$

$= (200 + 2n^2, 2n + 1)$ $\quad 100 + n^2 = d \cdot h$

$= (200 + 2n^2 - n(2n+1), 2n + 1)$ $\quad 100 + \left(\frac{dk-1}{2}\right)^2 = dh$

$= (200 - n, 2n + 1)$ $\quad 401 + d^2k^2 - 2dk = 4dh$

$= (200 - n, 2n + 1 + 2(200 - n))$ $\quad 401 \equiv 0 (d)$ $\quad d \mid 401$

$= (200-n, 401) \;/\; 1$

$\setminus 401$ se $401 \mid 200-n$

$n \equiv 200 \ (401)$

$n = 200$

601

⑨ $f(0) = 0 \quad \rightarrow \boxed{f(2n) = 2f(n) + 1}$.

$f(1) = 0 \qquad f(2n+1) = 2f(n)$

$f(10) = 1$

$f(11) = 0$

$f(100) = 11$

$\rightarrow f(101) = 10$

$f(1010) = 2 \cdot f(101) + 1 = f(101)$ con aggiunto un ① alla fine

($1010 = 2n$, $101 = n$)

$101 \rightarrow 010 = 10$

Per induzione:

	BASE 10	BASE 2	
passo base	0	[]	$\longrightarrow$ []
	1	1	$\longrightarrow$ 0

Passo induttivo: n implica $2n$

$f(2n) = 2f(n) + 1 =$ $f(n)$ con un 1 alla fine

$\uparrow$ BASE 2

$=$ n con cifre scambiate & un 1 alla fine

$\swarrow$

$f($ n con uno 0 alla fine $)$

n implica $2n+1$: uguale.

(a) $f(n) < n$ per $n \neq 0$

(b) 1010 ... 1010

2002

- Servono almeno 2002 cifre
- Devo perdere solo una cifra alla volta

11
00 NO

$$2 \cdot \left(1 + 4 + 4^2 + \dots + 4^{1000}\right) = 2 \cdot \frac{4^{1001} - 1}{3}$$

(P) $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n} = \frac{p}{q}$ $\quad q = mcm(2, 3, \dots, n)$

q pari

$p = q/2 + q/3 + q/4 + \dots + q/n =$ dispari

$2^k \leq n$ k massimo

$q/2^k$ è dispari

PARI

$v_2(q) = k$ Tutti gli altri sono pari!

$2^k \to q/m$ $\quad m \leq n$

2^k $\quad m = 2^k$

$m \geq 2^k \cdot 2 = 2^{k+1} > n$