M DAL

ARITMETICA

Criteri di divisibilità.

$$\sum_{i=0}^{m} a_i 10^i \underset{(3)}{\equiv} \sum_{i=0}^{m} a_i$$

Es. $1234564 \equiv 1+2+3+4+5+6+4 \equiv 1 \quad (3)$

$$\sum_{i=0}^{m} a_i 10^i \underset{(9)}{\equiv} \sum_{i=0}^{m} a_i$$

$$\sum_{i=0}^{m} a_i \cdot 10^i \underset{(4)}{\equiv} a_0 + a_1 10 \qquad \text{perché } 100 = 25 \cdot 4 \equiv 0 \, (4)$$

Es $1234 \underset{(4)}{\equiv} 34 \underset{(4)}{\equiv} 2$.

$1000 \equiv 7 \cdot 143 - 1 \equiv -1 \, (7)$

$$\sum_{i=0}^{m} a_i 10^i \equiv (a_0 + a_1 10 + a_2 100) + 1000 (a_3 + a_4 \cdot 10 + a_5 \cdot 100) + \dots$$
$$\equiv (a_0 + a_1 10 + a_2 100) - (a_3 + a_4 \cdot 10 + a_5 \cdot 100) + \dots$$

Es $1234567 = 567 - 234 + 1 \equiv 234 \equiv 5 \, (7)$

Es $\sqrt{1234567} \notin \mathbb{N}$

$x^2 = 1234567 \Rightarrow x^2 \equiv 67 \equiv 3 \, (4)$

ma x è congruo a $0,1,2$ o 3 mod(4) e in ogni caso $x^2 \not\equiv 3 \, (4)$

in quanto $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$, $3^2 \equiv 1 \, (4)$.

Cambio di base

Scrivere 12345 in base 8.

$1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \equiv \sum_i a_i 8^i \quad$ con $0 \le a_i < 8$

$12345 = a_0 + a_1 8 + a_2 8^2 + \dots + a_n 8^m \equiv a_0 + 8(a_1 + a_2 8 + \dots + a_n 8^{n-1})$

$\equiv a_0 \mod 8$

$12345 = 8 \cdot 1543 + 1 \Rightarrow a_0 = 1$

$a_1 + a_2 8 + \dots + a_n 8^{n-1} = 1543$

$1543 = 8 \cdot 192 + 7 \Rightarrow a_1 = 7$

$192 = 8 \cdot 24 + 0 \Rightarrow a_2 = 0$

$24 = 8 \cdot 3 + 0 \Rightarrow a_3 = 0$

$3 = 8 \cdot 0 + 3 \Rightarrow a_4 = 3 \qquad (12345)_{10} = (30071)_8$.

MCD = massimo comun divisore

Esempio: MCD(252, 198)

$252 = 2^2 \cdot 3^2 \cdot 7$

$198 = 2 \cdot 3^2 \cdot 11$

$\Rightarrow \text{MCD}(252, 198) = 2 \cdot 3^2 = 18$

<u>Def</u> MCD(a,b) è il più grande intero positivo che divide sia a che b

MCD(0,0) = ? non è definito. $5 \mid 0$? <u>sì</u> $5 \cdot 0 = 0$.

MCD(a,b) esiste se $a \neq 0 \vee b \neq 0$.

ALGORITMO DI EUCLIDE PER IL MASSIMO COMUN DIVISORE

<u>OSS</u>: Se a, b sono multipli di c anche $a+b$ e $a-b$ lo sono.

<u>Corollario</u>:

$$MCD(a,b) = MCD(a-b,b) \quad (*)$$

Ricordiamo che $a \equiv a' \ (b) \iff b \mid a-a'$

$\iff \exists k \in \mathbb{Z} \quad bk = a-a'$

$\iff a = a' + kb$

$\iff a$ e a' differiscono per un multiplo di b.

<u>Teo</u>

Se $a \equiv a' \ (b)$, $MCD(a,b) = MCD(a',b)$

<u>Dim</u>: $a' = a+kb$ $\quad MCD(a+kb,b) = MCD(a,b)$ applicando k volte la $(*)$.

Questo può accelerare il calcolo del MDC.

Per brevità scrivo (a,b) invece di $MCD(a,b)$.

$(252,198) = (252-198, 198) = (54, 198) = (198, 54) =$

↑ Algoritmo di Euclide per il MCD

<u>Esempio</u> $(1048, 10) = ?$

non c'è bisogno di scomporre in primi 1048.

Osservo che $1048 \equiv 8 \pmod{10}$

Quindi $(1048, 10) = (8, 10) = 2$.

Teorema di Bezout

Dati $a, b \in \mathbb{Z}$ sia (a,b) il MCD di a, b.
Allora $\exists x, y \in \mathbb{Z}$

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

Corollario:
$ax + by = n$ ha soluzione se e solo se n è multiplo di $MCD(a,b)$.

Corollario:
Supponiamo $a \mid bc$ e $(a,b) = 1$.
Allora $a \mid c$.

Dim: Per Bezout $\exists x, y$ $ax + by = 1$.
Moltiplico per c: $acx + bcy = c$.
Osservo che acx e bcy sono entrambi multipli di a (siccome a divide bc).
La somma di due multipli di a è un multiplo di a. Quindi $a \mid c$. $\boxtimes$

Corollario:
nel senso che è divisibile solo per $\pm 1, \pm p$.
Se p è primo e $p \mid ab$, allora $p \mid a$ o $p \mid b$

Dim: $p \mid ab$. Due casi:

1. $(p, a) = 1 \Rightarrow p \mid b$
2. $(p, a) \neq 1 \Rightarrow p \mid a$ (perché se $d = (p,a) \neq 1$, $d = \pm p$ essendo p primo).

ALTRE CONSEGUENZE DI BEZOUT

Teorema: Supponiamo $(a,b)=1$, $a|c$, $b|c$.
Allora $ab|c$.

Dim: Poiché $a|c$, esiste $k \in \mathbb{Z}$ tale che $ak=c$.
Poiché $b|c$ e $c=ak$ ottengo $b|ak$.
Ma $(b,a)=1$, quindi $b|k$.
Esiste dunque $l \in \mathbb{Z}$ $bl=k$.
Dunque $c=ak=abl$ e concludo che $ab|c$.

Quindi se $(a,b)=1$

$$\begin{cases} x \equiv 0 \mod (a) \\ x \equiv 0 \mod (b) \end{cases} \iff x \equiv 0 \mod (ab)$$

Teorema: $a|c$ e $b|c \implies \frac{ab}{(a,b)} \,\Big|\, c$.

Dim: Sia $d=(a,b)$.

$$a|c \text{ e } b|c \implies \frac{a}{d} \Big| \frac{c}{d} \text{ e } \frac{b}{d} \Big| \frac{c}{d}.$$

(se $ak=c \rightarrow \frac{a}{d}k=\frac{c}{d}$)

Poichè $\left(\frac{a}{d}, \frac{b}{d}\right)=1$, per il teorema precedente $\frac{a}{d} \cdot \frac{b}{d} \,\Big|\, \frac{c}{d}$,
e quindi $\frac{ab}{d} \,\Big|\, c$. $\square$

MINIMO COMUNE MULTIPLO

Il mcm di a, b è il più piccolo intero ≥ 0 che è multiplo sia di a sia di b.

Per il teorema precedente,

c è multiplo comune di a e b se e solo se $\frac{ab}{(a,b)} \mid c$. Quindi $\frac{ab}{(a,b)}$ è il minimo comune multiplo di a e b (se $a, b > 0$, se no bisogna mettere un segno ± 1)

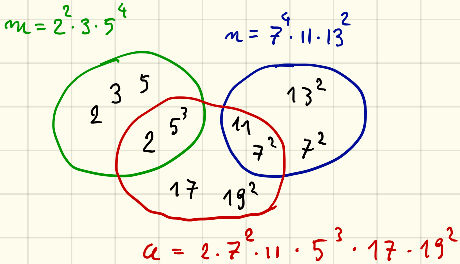
CONCLUSIONE:

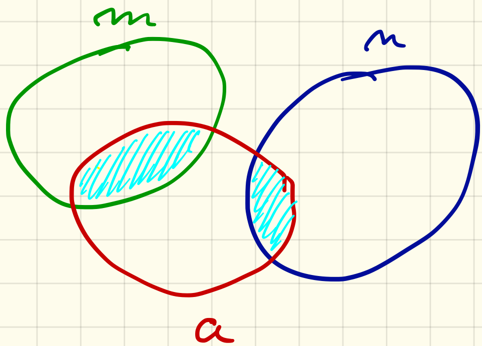
$$\boxed{MCM(a,b) = \frac{\pm ab}{MCD(ab)}}$$

Teo $(m,n)=1 \Rightarrow (a,mn)=(a,m)(a,n)$.

Dim. (a,m) e (a,n) sono relativamente primi perché un loro divisore comune sarebbe anche un divisore comune di m ed n.
Inoltre entrambi dividono $m\cdot n$, quindi anche il loro prodotto $(a,m)(b,n)$ divide $m\cdot n$ (per un risultato precedente).
Similmente $(a,m)(b,n)$ divide a.
Quindi $(a,m)\cdot(b,n) \mid (a,m\cdot n)$.

Vale anche il viceversa, guardate le figure e provate a dimostrarlo.





$(a,m) =$

Gli ovali rappresentano i divisori primi di a, m, n contati con le molteplicità.

$= (a, mn)$.

Esempio di MCD e Bezout.

Teorema di Bezout

Dati $a, b \in \mathbb{Z}$ sia (a,b) il MCD di a, b.
Allora $\exists x, y \in \mathbb{Z}$

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

Esempio con $a = 1020$, $b = 351$

		1020	351
	1020	1	0
	351	0	1
(-2)	318	1	-2
(-1)	33	-1	3
(-9)	21	10	-29
(-1)	12	-11	32
(-1)	9	21	-61
(-1)	3	-32	93

← cioè $318 = 1 \cdot 1020 + (-2) \cdot 351$

$MDC(1020, 351) = 3$

$$\boxed{3 = 1020(-32) + 351(93)}$$

Trovare tutte le soluzioni del sistema di congruenze

$$\begin{cases} 3x \equiv 1 \quad (14) \\ x \equiv 1 \quad (8) \\ 3x \equiv 9 \quad (5) \end{cases}$$

Soluzione: Mi riduco al sistema equivalente

$$\begin{cases} x \equiv 5 \quad (14) \\ x \equiv 1 \quad (8) \\ x \equiv 3 \quad (5) \end{cases}$$

Considero le prime due congruenze:

$$\rightarrow \begin{cases} x = 5 + 14k \\ 5 + 14k \equiv 1 \quad (8) \end{cases}$$

$14k \equiv 4 \quad (8)$

$7k \equiv 2 \quad (4)$

$21k \equiv 6 \quad (4)$

$k \equiv 2 \quad (4)$

$k = 2 + 4\ell$

Sostituisco $k = 2 + 4\ell$ in $x = 5 + 14k$

$x = 5 + 14(2 + 4\ell)$

$x = 5 + 28 + 56\ell$

$x \equiv 33 \quad (56)$ ← soluzione delle prime due congruenze

Il sistema equivale a $\begin{cases} x \equiv 33 \ (56) \\ x \equiv 3 \ (5) \end{cases}$

Svolgo i calcoli

$$\rightarrow \begin{cases} x = 33 + 56\ell \\ 33 + 56\ell \equiv 3 \quad (5) \end{cases}$$

$3 + \ell \equiv 3 \quad (5)$

$\ell \equiv 0 \quad (5)$

$\ell = 5i$

$\rightarrow$ $x = 33 + 56(5i)$

$= 33 + 280i$

$\boxed{x \equiv 33 \quad (280)}$ ← Soluzione finale.

Funzione ϕ di Eulero.

$\phi(n)$ = numero degli elementi tra 0 e $n-1$ invertibile modulo n.

Teo $\quad$ p primo $\Rightarrow$ $\phi(p) = p-1$

$1, 2, 3, \ldots, p-1$ sono invertibili modulo p.

$\phi(p^2) = p^2 - p$

Tutti gli interi tra 1 e p^2 sono invertibili tranne i multipli di p, che sono $p, 2p, 3p, \ldots, p \cdot p$.

$\phi(p^n) = p^n - p^{n-1}$

Tutti gli interi tra 1 e p^n sono invertibili tranne i multipli di p che sono p^{n-1}

Teo La Φ di Eulero è moltiplicativa
ovvero $\Phi(ab) = \Phi(a) \cdot \Phi(b)$ se $(a,b) = 1$.

Dim:

Per il teorema Cinese dei resti esiste una biiezione F

$$F: \mathbb{Z}/(ab) \longrightarrow \mathbb{Z}/(a) \times \mathbb{Z}/(b)$$
$$[x]_{ab} \longmapsto \langle [x]_a , [x]_b \rangle$$

Ad esempio con $a=3, b=5$

$$F: [7]_{15} \mapsto \langle [7]_3, [7]_5 \rangle = \langle [1]_3, [2]_5 \rangle$$

La F è surgettiva perché dati $[u]_a \in \mathbb{Z}/(a)$ e $[v]_b \in \mathbb{Z}/(b)$ per ottenere $[x]_{ab} \in \mathbb{Z}/(ab)$ tale che $F([x]_{ab}) = \langle [u]_a, [v]_b \rangle$ basta che risolvere il sistema

$$\begin{cases} x \equiv u \ (a) \\ x \equiv v \ (b) \end{cases}.$$

È anche iniettiva perché se x_0, x_1 sono due soluzioni del sistema, $x_0 \equiv x_1 \ (ab)$ e quindi $[x_0]_{ab} = [x_1]_{ab}$.

Cor: Se $(a,b)=1$ allora $\phi(ab)=\phi(a)\phi(b)$.

Teo: $a^{\phi(n)} \equiv 1 \ (n)$ se $(a,n)=1$.

Dim.

Lo dimostro solo nel caso $n = p_1 \cdot p_2 \cdots p_k$ (*)
con $p_1, \dots, p_k$ primi distinti.

$a^{\phi(n)} = a^{(p_1-1)\dots(p_k-1)} \equiv 1 \ (p_i)$ per ogni i
per il piccolo teorema di Fermat.

Quindi $a^{\phi(n)} \equiv 1 \ (p_1 \cdot p_2 \cdots p_k)$ per il teorema dei resti cinese. $\square$

A lezione lo abbiamo visto in generale
(con $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$)

Trovare tutte le soluzioni intere di:

ES $54 = 252x + 198y$ $\qquad MCD(252, 198) = 18$

$\Updownarrow$

$3 = 14x + 11y$ $\qquad (14, 11) = 1$

$3 = 14(1) + 11(-1)$

omogenea

$$\boxed{0 = 14(K11) + 11(-K14)}$$

Soluzione

$3 = 14(1 + K11) + 11(-1 - K14)$

Verifico che non ci siano altre soluzioni:

$x = 1 + K11$

$y = -1 - K14$

Sono tutte? sì:

$3 = 14x + 11y$

$\Rightarrow 3 \equiv 14x \ (11)$

$3 \equiv 3x \ (11)$ $\qquad 3 \cdot 4 \equiv 12 \equiv 1 \ (11)$ $\qquad$ 3 ha inverso mod 11.

$1 \equiv x \ (11)$

$x = 1 + 11K$ $\qquad$ Quindi le x sono tutte.