MCD = Massimo Comun divisore.

per brevità: $(a,b) = MCD(a,b)$.

Teorema (Bezout): $\exists x, y \in \mathbb{Z}$ $MCD(a,b) = ax + by$ (combinazione lineare di a, b a coefficienti in $\mathbb{Z}$)

Esempio $MCD(1020, 351) = 3 =_{\text{visto}} 1020 \cdot \boxed{-32} + 351 \cdot \boxed{93}$

Lo rifaccio.

1° metodo per trovare l'MCD è la scomposizione sui primi

$1020 = 5 \cdot 204 = 5 \cdot 2^2 \cdot 51 = 5 \cdot 2^2 \cdot 3 \cdot 17$

$351 = 3 \cdot 117 = 3 \cdot 3 \cdot 39 = 3 \cdot 3 \cdot 3 \cdot 13$

$\Rightarrow 3 = MCD(1020, 351)$

nov 24-13:53

2° Metodo per Trovare MCD(1020,351). Fornisce anche X, Y

$MCD = 1020X + 351Y$.

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

Regola $(a,b) = (a - kb, b)$

1020	351
318	2

$1020 = 351 \cdot 2 + 318$

$351 - 318 = 33$ ←

$318 - 33 \cdot 9 = 21$ ←

318	33
21	9

$\Rightarrow 3 = MCD(1020, 351) = 1020 \cdot (-32) + 351 \cdot 93$

nov 24-14:17

Risolvere $12 = 1020\,u + 351\,v$ | Trovare $u, v \in \mathbb{Z}$.

esistono u, v ?

Sì perché 12 è multiplo del $MCD(1020, 351) = 3$ | Se u, v fossero in $\mathbb{R}$ sarebbe facile: $u = 0$, $v = \frac{12}{351} \in \mathbb{Z}$

Sappiamo risolvere $3 = 1020\,(-32) + 351\,(93)$ (*)

Voglio 12 anziché 3. Moltiplico per 4 la (*):

$12 = 1020\,(-32 \cdot 4) + 351\,(93 \cdot 4)$

$-32 \cdot 4 = -128$

$93 \cdot 4 = 372$

quindi $u = -32 \cdot 4$, $v = 93 \cdot 4$.

Risolvere $11 = 1020X + 351Y$ | Non si può: perché $3 \nmid 11$. $3 = MCD(1020, 351)$

perché non si può? Se esistessero X, Y.

$\Rightarrow$ $1020X$ è multiplo di 3, $351Y$ multiplo di 3. Somma di multipli di 3 è multiplo di 3. $\Rightarrow 3 \mid 11$ ASSURDO.

Teo $n = aX + bY$ $(n, a, b \in \mathbb{Z}$ dati$)$ $X, Y \in \mathbb{Z}$ da trovare

è risolubile $\Leftrightarrow$

n è multiplo di $MCD(a, b)$

ovvero $MCD(a, b) \mid n$.

Per trovare X, Y uso **Bezout**:

Prima trovo x', y' tali che $MCD(a, b) = ax' + by'$.

Controllo se $MCD(a, b) \mid n$. Se lo divide trovo k tale che

$n = MCD(a, b) \cdot k$.

$\Rightarrow$ $n = a(x' \cdot k) + b(y' \cdot k)$. $\Rightarrow \begin{cases} X = x'k \\ Y = y'k \end{cases}$.

nov 24-14:29

Congruenze

$ax \equiv b \mod(c)$. $\quad a, b, c \in \mathbb{Z}$, $x \in \mathbb{Z}$ da trovare

$\updownarrow$

$ax - b = cy$

$\exists y \in \mathbb{Z}$

$ax + c(-y) = b$ ← Equazione Lineare Diofantea.

$\updownarrow$

$\exists z \in \mathbb{Z}$

$ax + cz = b$

QUINDI la sapete già fare!

ES $351(v) \equiv 12 \mod(1020)$. Trovare $v \in \mathbb{Z}$ se esiste.

equivale a trovare v, e k

$\rightarrow 351v = 12 + 1020k$. Separiamo $12 = 1020[-128] + 351[372]$

$12 = 1020(-k) + 351(v)$

$k = 128$, $v = 372$

del k non mi importa, trovo $v = 372$ che risolve

$351v \equiv 12 \ (1020)$.

La congruenza mi dà meno informazioni.

Però ci sono modi più facili per le congruenze.

ES Trovare $x \in \mathbb{Z}$

$195 \equiv 27 \ (42)$

$195 = 42 \cdot 4 + 27$

$195 \equiv 42 \cdot 4 + 27 \equiv 27 \ (42)$

$195x \equiv 6 \ (42)$

$\exists y \quad 195x = 6 + 42y$ inutile

$195x \equiv 6 \ (42)$ ha le stesse soluzioni di $27x \equiv 6 \ (42)$

dividi tutto per 3 incluso il modulo

$9x \equiv 2 \ (14)$

Perché lo posso fare?

Passando alla diofantea si vede subito

$\frac{1}{3} \updownarrow \quad \begin{cases} 27x = 6 + 42y \quad (\exists y) \\ 9x = 6 + 14y \end{cases}$

?

a occhio $3 \cdot 9 \equiv 27 \equiv -1 \ (14)$

$\times 3$

$(3 \cdot 9)x \equiv (3 \cdot 2) \ (14)$

$-x \equiv 6 \ (14) \iff x \equiv -6 \ (14) \iff$

$\iff x = -6 + k14$

es. $\begin{cases} x = -6 \\ x = 14 - 6 = 8 \text{ etc} \\ x \equiv \dots \end{cases}$

nov 24-14:52

Giustificare:

$A \equiv B \ (C)$ $\Rightarrow$ sempre $k \cdot A \equiv k \cdot B \ (C)$

$\Leftarrow$ solo se k ha un inverso modulo C

infatti se $k \cdot r \equiv 1 \ (C)$ per passare da $kA \equiv kB \ (C)$ a $A \equiv B \ (C)$ moltiplico per r:

$kA \equiv kB \ (C)$

$\Downarrow$

$rkA \equiv rkB \ (C)$

$\Downarrow$

$1 \cdot A \equiv 1 \cdot B \ (C)$

$A \equiv B \ (C)$

Sempre

Quando è che k ha inverso mod C ?

nov 24-15:05

Inversi mod c :

Esempio $2 \cdot 3 \equiv 1 \mod 5$.
2 e 3 sono inversi modulo 5.
2 è l'inverso di 3 e 3 è l'inverso di 2 mod (5).

Def k e r sono inversi mod c se $k \cdot r \equiv 1 \ (c)$.

Teo k ha un inverso mod c $\iff$ MCD(k,c) = 1

Dim facile. MCD(k,c) = 1. $\Rightarrow$ Bezout $1 = kX + cY$

X è l'inverso di k. $\boxtimes$ $1 \equiv kX + cY \ (c)$

Prima ero passato da $9x \equiv 2 \ (14)$

$3 \cdot 9x \equiv 2 \cdot 3 \ (14)$

↓ sempre. ↑ la posso fare perché 3 ha un inverso mod 14 essendo $MCD(3,14) = 1$.

quindi potevo fare ↑. Non c'è bisogno di trovare l'inverso.

Ma se lo voglio trovare, chi è?

$3 \cdot \square \equiv 1 \ (14)$ $\quad \square = ?$

Bezout $\quad 1 = 14x + 3y$

	14	3
14	$= 1 \cdot 14 + 0 \cdot 3$	
3	0	1
(-4) 2	1	-4
(-1) 1	-1	5

$1 = 14 \cdot \boxed{(-1)} + 3 \cdot \boxed{5}$

$1 \underset{(14)}{\equiv} 14 \cdot (-1) + 3 \cdot 5$

l'inverso di 3 mod 14 è 5.

$3 \cdot 5 \equiv 1 \ (14)$.

Teorema $\exists x \; ax \equiv b \; (c)$ $\iff$ $MDC(a,c) \mid b$.

$a, b, c \in \mathbb{Z}$ dati
x da trovare.

Es $3x \equiv 5 \; (12)$

non esiste x perché $MCD(3,12) = 3 \nmid 5$.

Es esiste x $3x \equiv 5 \; (11)$ perché $MCD(3,11) = 1 \mid 5$.

Dim teo $\exists x (ax \equiv b \; (c))$

$\iff \exists x \; \exists y \quad ax = b + cy$

$ax + c(-y) = b$

$a\square + c\square = 6$

b deve essere multiplo di $MCD(a,c)$ .. cioè $MCD(a,c) \mid b$.

nov 24-15:32

Q. $a \mid bc \longrightarrow a \mid b \vee a \mid c$? no in generale.

$4 \mid 6 \cdot 10$ ma $4 \nmid 6$, $4 \nmid 10$

Teo $\left[a \mid bc \wedge MCD(a,b) = 1 \Rightarrow a \mid c \right]$

Dim Bezout $1 = MCD(a,b) = ax + by$ $\exists x, y$.

$\times(c)$ $c = acx + bcy$

acx: multiplo di a; bcy: multiplo di a perché $a \mid bc$ per ipotesi.

Somma di multipli di a è multiplo di a

$\Rightarrow c$ multiplo di a

cioè $a \mid c$

nov 24-15:36

Con p primo, $p \mid bc \longrightarrow \underbrace{p \mid b}_{A} \vee \underbrace{p \mid c}_{B}$? Sì

Dim Suppongo $p \mid bc$.

Basta mostrare che $p \nmid b \Rightarrow p \mid c$.

$A \vee B \equiv \neg A \to B$

Se $p \nmid b \Rightarrow MCD(p,b) = 1$ perché p è primo.

Quindi visto che $MCD(p,b) = 1$ siamo nella situazione del teo precedente

$p \mid bc$, $MCD(p,b) = 1 \Rightarrow p \mid c$. ☒

dovendo dividere p è 1 o p. Non è p perché $p \nmid b$.

$p \mid a_1 a_2 a_3 \longrightarrow p \mid a_1 \vee p \mid a_2 \vee p \mid a_3$

idem per n fattori (induzione).

$p \mid (a_1 \cdots a_{n-1}) a_n \Rightarrow p \mid (a_1 \cdots a_{n-1}) \vee p \mid a_n$

$\Rightarrow$ ind. $p \mid a_1 \vee \cdots \vee p \mid a_{n-1} \vee p \mid a_n$.

Teo $17 \mid \binom{17}{5}$ $\qquad \binom{17}{5} = \frac{17!}{12!\ 5!} \in \mathbb{Z}$!

Teo $p \mid \binom{p}{i}$ se p primo e $i \neq 0, p$.

$\binom{p}{0} = 1 = \binom{p}{p}$

Teo $i \neq 0, p$ p primo $\Rightarrow p \mid \binom{p}{i}$. $\boxed{0 < i < p}$

Dim. $\binom{p}{i} = \dfrac{p!}{(p-i)!\, i!} \Rightarrow \binom{p}{i} \cdot (p-i)!\, i! = p!$

(1) $p \mid p!$ ovvio.

Quindi $p \mid \binom{p}{i} (p-i)!\, i!$. p primo.

$\Rightarrow p \mid \binom{p}{i}$ $\vee$ $\underbrace{p \mid (p-i)!}_{\text{Assurdo}}$ $\vee$ $\underbrace{p \mid i!}_{\text{Assurdo (perché } i \neq 0,p)}$

$p \mid i! \Rightarrow p \mid i \cdot (i-1) \cdot (i-2) \cdot (i-3) \cdots 1$

$\Rightarrow p \mid i \vee p \mid (i-1) \vee p \mid (i-2) \vee \cdots \vee p \mid 1$

perché è assurdo? $\boxed{i < p} \Rightarrow p \nmid i \quad p \nmid i-1$ etc.

$p \mid (p-1)! \Rightarrow$ Assurdo stesso motivo. $p - i < p$ perché $i \neq 0$.

$(p-i)! = (p-i)(p-i-1)(\cdots)\cdots 1$

prodotto di numeri $< p$.

bernardo@dm.unipi.it

nov 24-15:57