Sostituisco Ilaria. Abbiate pazienza....

Congruenze: lavoro in $\mathbb{Z}$.

$a \equiv b \pmod c \iff c \mid a-b$

$\overset{\text{def}}{\iff}$ a e b danno lo stesso resto divisi per c.

Es Che giorno era della settimana 100 giorni fa? Oggi è Lunedì

100 | 7
30 | 14
2

$100 = 7 \cdot 14 + 2$

$-100 = 7(-14) - 2$

$-100 \equiv -2 \pmod 7$. Era Sabato.

$-100 = 7 \cdot (-14) - 2$

$= (7(-14) - 7 + 7 - 2)$

$= 7(-15) + 5$

$-100 \mid 7$

$5 \quad -15$

Il resto di -100 diviso 7 è 5

Il resto di a diviso b è

$0 \leq r < b$

MCD = massimo comun divisore

Ci aiutiamo con la congruenza.

$MCD(252, 198) = ?$

1° Metodo Scompongo in primi.

$252 = 2^2 \cdot 3^2 \cdot 7$, $198 = 2 \cdot 3^2 \cdot 11$

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

Si prendono i fattori primi p massima potenza m tale che $p^m \mid a \wedge p^m \mid b$.

$MCD(a,b)$ è il più grande intero positivo d che divide sia a che b.

$MCD(0,0) = ?$ $5 \mid 0$? Si $5 \cdot 0 = 0$

$6 \mid 0$? Si $6 \cdot 0 = 0$

il massimo non c'è.

$MCD(0,0)$ non è definito.

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

$MCD(252, 0) = 252$ ← esempio

$MCD(-252, 0) = 252$ $252 \mid -252$? Si : $252 \cdot (-1) = 252$.

Si lavora in $\mathbb{Z}$ ma l'MCD lo voglio positivo.

Osserva che $MCD(a,b) = MCD(|a|,|b|)$

es. $MCD(-5,10) = MCD(5,10) = 5$.

oss. $d = MCD(a,b)$ e $a \neq 0 \Rightarrow d \leq |a|$.

Proposizione: Se a e b sono multipli di d, anche $a+b$ e $a-b$ lo sono.

Dim. $a = kd$, $b = td \Rightarrow$

$(a+b) = (kd + td) = (k+t)d$.

Anche $(a-b)$ è multiplo di d:

$a - b = kd - td = (k-t)d$. □

Corollario.

$MCD(a,b) = MCD(a-b, b)$ (1)

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

Perché? Il numeri che dividono sia a che b sono gli stessi che dividono sia a che $a-b$ (1) e quindi anche il massimo è uguale.

Usando il corollario, per calcolare $MCD(a,b)$ mi riduco al MCD di numeri più piccoli.

$MCD(a,b) = MCD(a-b,b) = MCD(a-2b,b) = MCD(a-3b,b) = \text{etc.}$ (applico ripetutamente la (1))

Teo $(a \equiv a' \bmod b) \Rightarrow MCD(a,b) = MCD(a',b)$.

1 Dim. $a \equiv a' \bmod b \Rightarrow a - a'$ multiplo di b

$\Rightarrow a = a' + kb$ (esiste k).

$MCD(a,b) = MCD(a-b,b) = MCD(a-2b,b) = \dots = MCD(a-kb,b)$

$= MCD(a',b)$. □

2 Dim Se un numero divide a e b divide anche $\underbrace{a-kb}_{=a'}$ e b

Se divide a' e b divide anche $a'+kb$ e b

$\Rightarrow$ i numeri x che dividono a,b sono gli stessi che dividono a',b

$\Rightarrow MCD(a,b) = MCD(a',b)$.

Esempio Ricalcolo $MCD(252, 198)$ senza scomporre in primi.

$MDC(252, 198) = MCD(252 - 198, 198) = MCD(54, 198)$ ci siamo ricondotti a numeri più piccoli.

ora sottraggo da 198 multipli di 54

$= MCD(54, \underbrace{198 - 3 \cdot 54}_{\text{resto di 198 diviso 54}}) = MCD(54, 36)$

Cambio di nuovo modi: Dal 54 sottraggo multipli di 36

$= MCD(54 - 36, 36) = MCD(18, 36)$ $(= 18$ "a occhio", ma continuo$)$

$= MCD(18, 36 - 18) = MCD(18, 18) = MCD(18, 18 - 18) = MCD(18, 0) = 18$

Se non lo vedo a occhio prima continuo finché uno dei due diventa zero.

Se a, b sono grandi, conviene questo procedimento piuttosto che scomporre in primi. È più veloce.

PAUSA !

Ricapitoliamo: Scrivo per brevità (a,b) invece

- Se $a \equiv a' \ (b)$, allora $(a,b) = (a',b)$.
- Se a' è il resto di a diviso b allora $a' \equiv a \ (b)$ e posso applicare la regola.

$(a,b) = (\text{resto di } a \text{ diviso } b, b)$ (se b è il più grande faccio $(a, \text{resto di } b \text{ diviso } a)$

Es $100 \ \ 7$
$\ \ 2 \ \ 14$

$100 = 7 \cdot 14 + 2$
$\Downarrow$
$100 \equiv 2 \ (7)$

Quindi
$(100,7) = (\text{resto di } 100 \text{ diviso } 7, 7)$
$= (100 - 7 \cdot 14, 7)$
$= (2,7) = 1$ (a occhio).
$= (2, \text{resto di } 7 \text{ diviso } 2)$
$= (2,1) = (2-1-1, 1) = (0,1)$
$= 1.$

Torniamo alle congruenze.

Le congruenze $a \equiv b \ (c)$ si comportano per molti aspetti come uguaglianze:

Regole:
- posso moltiplicare: $a \equiv b \ (c) \Rightarrow a \cdot k \equiv b \cdot k \ (c)$
- posso sommare $a \equiv b \ (c) \Leftrightarrow a + k \equiv b + k \ (c)$
- sottrarre $a \equiv b \ (c) \Leftrightarrow a - k \equiv b - k \ (c)$
- però non sempre posso dividere. Se $ka \equiv kb \ (c)$ non è detto che $a \equiv b \ (c)$

Giustifichiamo la regola del sommare:

$a \equiv b \ (c)$ significa che la differenza $a - b$ è multiplo di c.

Ma la differenza tra $a+k$ e $b+k$ è la stessa.

$(a+k) - (b+k) = a - b$

Quindi anche $(a+k) - (b+k)$ è multiplo di c. Cioè

$a + k \equiv b + k \ (c)$.

Esercizio Giustificate la regola
$a \equiv b\ (c) \Rightarrow ak \equiv bk\ (c)$.

Dim $a - b = c \cdot t \Rightarrow ak - bk = (a-b)k$
$= ct \cdot k$
multiplo di c. □

Per giustificare serve parlare degli inversi di un numero k modulo c.

Quando è che posso dividere modulo c?

REGOLA Se $ka \equiv kb\ (c)$
e Se $MCD(k,c) = 1$, allora
$a \equiv b\ (c)$.

$\frac{1}{k}$ non si può fare perché lavoro in $\mathbb{Z}$ però c'è qualcosa che può giocare il ruolo di $\frac{1}{k}$ modulo c.
se $MCD(k,c) = 1$.

ES $2 \cdot 3 \equiv 6 \equiv 1 \ (5)$

$2 \cdot 3 \equiv 1 \ (5)$. Il 3 gioca il ruolo di $\frac{1}{2}$ modulo 5.

non ha senso in $\mathbb{Z}$.

DEF Un inverso di K modulo (c) è un numero $S \in \mathbb{Z}$ tale che

$K \cdot S \equiv 1 \ (c)$.

Se ragiono in settimane l'inverso del martedì è il giovedì

$2 \cdot 4 \equiv 8 \equiv 1 \ (7)$.

.... SCHERZO ....

Esistono sempre gli inversi? Purtroppo NO.

modulo 5 ogni numero ha un inverso eccetto 0 e i numeri congrui a zero mod(5).

Oss $X \equiv 0\ (5) \iff 5 \mid X$

$\iff X = 0, 5, 10, 15, -5, -10, -15$ etc.

Se $X \equiv 0\ (5) \Rightarrow X$ non ha inverso mod (5). Se K fosse un suo inverso $KX \equiv 1\ (5)$??

Ma se $X \equiv 0\ (5)$

$\Rightarrow KX \equiv K0 \equiv 0\ (5)$

Assurdo.

I numeri congrui a zero modulo 5 (o qualunque altro modulo) sicuramente non hanno inverso.

Gli altri?

Modulo 5 siamo fortunati perché 5 è primo.

Teo p è primo $\Rightarrow$ tutti i numeri non congrui a zero modulo p hanno inverso mod. p.

Dim posporta.

Con i numeri composti le cose vanno peggio.

Invertibili modulo 6. Chi ce li ha?

2 ha inverso? NO.

il 5! Sì

$5 \cdot 1 \equiv 5 \ (6)$

$5 \cdot 2 \equiv 10 \equiv 4 \ (6)$

$5 \cdot 3 \equiv 15 \equiv 3 \ (6)$

$5 \cdot 4 \equiv 20 \equiv 2 \ (6)$

$5 \cdot 5 \equiv (5 \cdot 4 + 5) \equiv (2 + 5) \equiv 7 \equiv 1 \ (6)$

5 è l'inverso di 5 modulo 6

il 2 non ha inverso mod 6
perchè ~~se per assurdo~~ se per assurdo

$$2 \cdot K \equiv 1 \quad (6) \qquad \Big\| \times 3$$

$$(2 \cdot 3) \cdot K \equiv 3 \quad (6)$$

$$\Big\|$$

$$0 \cdot K \equiv 3 \quad (6)$$

$$\Big\|$$

$$0 \equiv 3 \quad (6)$$ Assurdo.

La regola generale è che
K ha inverso mod. C
se $MCD(K, C) = 1$.

Se C è primo

$$MCD(K,C) = \begin{cases} 1 & \text{se } C \nmid K \\ C & \text{se } C \mid K \end{cases}$$

$$MCD(K,C) = \begin{cases} 1 & \text{se } K \not\equiv 0 \ (C) \\ C & \text{se } K \equiv 0 \ (C) \end{cases}$$

ES $14 \equiv 8 \ (c) \overset{?}{\Rightarrow} 7 \equiv 4 \ (c)$

con $c = 6$ non funziona.

$14 \equiv 8 \ (6)$ sì

ma $7 \not\equiv 4 \ (6)$.

Il problema è che ho diviso per 2 ma 2 non aveva un inverso modulo 6. (non potevo dividere!)

Una congruenza modulo (c) la posso dividere per k solo se k ha un inverso mod (c).

(Perché se ha un inverso, dividere per k equivale a moltiplicare per l'inverso di k, e moltiplicare preserva la congruenza).

ES $14 \equiv 8 \ (3)$ sì.

Posso dividere per 2? sì perché $MCD(?,3)=1$

$\Rightarrow 7 \equiv 4 \ (3)$ giusto!

posso farlo anche senza calcolare

... l'inverso.

Ma chi era?

l'inverso di 2 mod 3 è 2 stesso:

$2 \cdot 2 \equiv 4 \equiv 1 \ (3)$.

Avevo $14 \equiv 8 \ (3)$

Dividerla per 2 è come moltiplicarla per l'inverso di 2, che è 2.

Controllate che $14 \cdot 2 \underset{(3)}{\equiv} 7$, $8 \cdot 2 \underset{(3)}{\equiv} 4$.

$14 \cdot 2 = 7(2 \cdot 2) \equiv 7 \ (3)$ $\quad$ $8 \cdot 2 \equiv 8 \cdot (2 \cdot 2) \equiv 4 \ (3)$.

FINE