“Essere congruo modulo n significa che la differenza tra ciò che sta al primo e ciò che sta al secondo membro è multiplo di n.”

* **CONGRUENZE LINEARI**

DEFINIZIONE: Una CONGRUEZA LINEARE è ogni equazione del tipo: incongita.

Risolvere una congruenza lineare significa trovare un intero

BEZOUT

PROPOSIZIONE: La congruenza \*) ammette soluzione

LEMMA

DIMOSTRAZIONE:

o)

Se \*) ammette soluzione,

Detto o).

Siccome

è una soluzione di \*).

ES. Siccome la congruenza non ammette soluzioni;

Siccome la congruenza ammette soluzioni;

Le divisioni successive permettono di risolvere questa equazione.

TEOREMA: Sia una congruenza lineare tale che (a,n)\b.

Detto una soluzione, tutte e sole le soluzioni sono del tipo dove . Tra queste le soluzioni , sono tutte NON CONGRUE modulo n e ogni altra soluzione è CONGRUA modulo n a una di queste.

Abbiamo infinite soluzioni, ma ne scegliamo d interessanti perché appartengono a d classi distinte di congruenza.

d è il numero massimo che esaurisce le non congruenze

DIMOSTRAZIONE:

Proviamo che ogni è soluzione.

che è multiplo di n.

Proviamo che ogni soluzione è del tipo

Sia una soluzione, allora sappiamo che Sappiamo anche che

LEMMA

Sottraggo dalla prima la seconda membro a membro:

Dividiamo per d

Proviamo che sono a due a due non congruenti mod n.

Siano soluzioni, h, k < d.

Supponiamo per assurdo il che è assurdo perché sono entrambi < d, avremmo quindi che , ASSURDO!

Proviamo che ogni soluzione è congrua mod n a una delle d precedenti.

Sia una soluzione.

Dividiamo per h e per d (divisione euclidea) 🡪

Allora

Così siamo in grado di calcolare tutte le soluzioni dell’equazione diofantea.

Es. Trovare tutte le soluzioni della congruenza

Ris: la congruenza ha soluzione.

Una soluzione è Le soluzioni sono non congrue modulo 9 ed ogni altra soluzione è congrua modulo 9 a una di queste.

Es. Trovare tutte le soluzioni della congruenza

Ris: la congruenza ha una soluzione che è

Le soluzioni sono non congrue mod 5 ed ogni altra soluzione è congrua modulo 5 a una di queste.

* **SISTEMA DI CONGRUENZA**

LEMMA: Si consideri il SISTEMA DI CONGRUENZE \*) tale che ogni congruenza ammetta soluzione e

Allora \*) è equivalente a un sistema dove

DIMOSTRAZIONE: Siccome Detti il sistema \*) è equivalente al sistema \*\*) dove e ciascuna congruenza ammette un’unica soluzione ck modulo n’k per il teorema precedente.

Quindi \*\*) è equivalente a \*\*\*) dove

TOEREMA (CINESE DEL RESTO):

Dato un sistema del tipo \*), il sistema \*) ammette un’unica soluzione modulo

DIMOSTRAZIONE: Sia . Definisco .

Considero le seguenti conseguenze:

Osserviamo che

la congruenza k) ammette almeno una soluzione che sarà chiamata

Si consideri Allora è soluzione di \*).

Infatti,

È multiplo di rk perché è soluzione della congruenza k)

0)

Osserviamo che e quindi è un multiplo di rk o) è un multiplo di rk.

Se è soluzione del sistema, allora

LEMMA: Si consideri il SISTEMA DI CONGRUENZE \*) tale che ogni congruenza ammetta soluzione e

Allora \*) è equivalente a un sistema dove

ESERCIZIO: trovare le soluzioni, se esistono, del seguente sistema \*)

RISPOSTA: Dobbiamo ricordarci di un lemma, essendo i moduli tutti coprimi tra loro

Siccome , le 2 congruenze ammettono soluzione.

Quindi \*) è equivalente al sistema

che è equivalente al sistema o)

Grazie al TeoremaCinesedelResto e si considera la congruenza

cioè 1)

2)

1) ammette come soluzione 2) ammette come soluzione

Sia

Allora 13 è la soluzione di \*) unica modulo 10.

PROBLEMA: Un Sacchetto contiene delle caramelle, se le tolgo a 2 a 2, a 3 a3, a 4 a 4, a 5 a 5, a 6 a 6, ottengo sempre una caramella nel sacchetto. Se le tolgo a 7 a 7 non ne rimane nessuna.

Qual è il numero minimo di caramelle che deve contenere il sacchetto?

RISPOSTA: Detto x il numero di caramelle nel sacchetto, si ha \*)

Il sistema \*) è equivalente al sistema \*\*) che soddisfa le ipotesi del TCR.

Sia

Sia

Sia

Sia

Sia

Consideriamo le congruenze



SI consideri che è soluzione unica di \*) mod 420, quindi il numero minimo di caramelle è dato dal più piccolo positivo della forma che è 301.

ESERCIZIO: In aula ci sono x studenti,

siamo nell’ipotesi del TCR, sia

Consideriamo le congruenze:



Quindi . È la sola e unica soluzione mod 30 🡪 il numero di studenti in aula oggi è 18!

ESERCIZIO: Trovare il resto della divisione di

RISPOSTA: Osserviamo che \*). Adesso \*) Il resto cercato è 1.

ESERCIZIO: Trovare il resto della divisione per 10 di

RISPOSTA: Osserviamo che Osserviamo che

che è il resto ricercato.

ESERCIZIO: Si provi che è divisibile per 5.

RISPOSTA: Sia

Osservo che se z è multiplo di 5

Se , allora . Se allora z è multiplo di 5. Se allora .

Quindi anche quando , allora z è multiplo di 5.

Le potenze pari sono congrue a 1, quelle dispari a 4.