CONGRUENZE

I)

Definizione: due numeri naturali a e b si dicono congrui modulo un numero naturale p se hanno lo stesso resto nella divisione intera per p.
Si scrive $a \equiv b \bmod p$ oppure $a \equiv b \ (p)$

proprietà delle congruenze:

la congruenza è una relazione di equivalenza
inoltre:

$$a \equiv b \bmod p \quad c \equiv d \bmod p \quad \textit{allora} \quad \begin{array}{ll} a + c \equiv b + d & (I) \\ a \cdot c \equiv b \cdot d & (II) \end{array}$$

Criteri di divisibilità

- Un numero è congruo modulo 2 alla sua cifra delle unità
- Un numero è congruo modulo 3 alla somma delle sue cifre
- Un numero è congruo modulo 4 al numero intero formato dalle sue due ultime cifre
- Un numero è congruo modulo 5 alla sua cifra delle unità
- Un numero è congruo modulo 8 al numero intero formato dalle sue tre ultime cifre
- Un numero è congruo modulo 9 alla somma delle sue cifre
- Un numero è congruo modulo 10 alla sua cifra delle unità
- Un numero è congruo modulo 11 alla somma a segno alterno delle sue cifre (i segni devono essere messi in modo che la cifra delle unità abbia segno negativo)
- Un numero è divisibile per 7 se e solo se è divisibile per 7 l'intero costruito nel seguente modo: si prende l'intero iniziale privato della cifra delle unità e gli si sottrae due volte la cifra delle unità.

Esempio 1: quanto è il resto nella divisione per tre del numero 2008^{2008}

$$2008^{2008} \equiv \underbrace{2008 \cdot \ 20008 \cdot \ \cdot \ \cdot 20008}_{20008 \ \ volte}$$

$2008 \equiv 1 \quad (3)$

Quindi $2008^{2008} \equiv 1 \pmod 3$

II)

Con le congruenze possiamo caratterizzare i quadrati perfetti:

I.
se un numero a è un quadrato perfetto allora $a \equiv 0$ *oppure* $a \equiv 1$ (4)

dimostrazione: sia $a= n^2$ allora n è pari o dispari.
Se n è pari $n = 2k$ e $n^2 = 4k^2$ quindi $a \equiv 0$ (4)
Se n è dispari allora $n = 2k+1$ e $n^2= 4k^2+4k+1$ e quindi $a \equiv 1$ (4) per e proprietà I e II
Quindi:

- il quadrato di intero pari è sempre congruo a 0 modulo 4
- il quadrato di un intero dispari è sempre congruo a 1 modulo 4

Si può dare una caratterizzazione anche modulo 8 . Se un numero a è un quadrato perfetto allora $a=n^2$ e

n pari $a \equiv \begin{matrix} 0 \\ 4 \end{matrix}$ (8) n dispari $a \equiv 1$ (8)

Si possono caratterizzare nello stesso modo le quarte potenze:

- La quarta potenza di un intero pari è sempre congrua a 0 modulo 16
- La quarta potenza di un intero dispari è sempre congrua a 1 modulo 16

Attenzione! Non sono vere le proprietà inverse, esempio $8 \equiv 0$ mod 4 ma 8 non è un quadrato perfetto.

Esempio 2 : Consideriamo un numero formato concatenando un po' di scritture decimali di 2006. Quante cifre ha il più piccolo quadrato perfetto tra tali numero?

Consideriamo che un numero del tipo 200620002……2006. esso è congruo a 2 mod 4 quindi non può mai essere un quadrato perfetto.

III)
Sistemi di congruenze:

Siano $m_1,\ldots m_k$ k numeri interi e $a_1,\ldots a_k$ altri k numeri interi
Si dice sistema di congruenze un sistema della forma

$x \equiv a_1 \pmod{m_1}$
.
.
.
.
$x \equiv a_n \pmod{m_k}$

Risolvere tale sistema significa trovare gli interi x che verificano contemporaneamente le k congruenze.

Esempio 3

Dati sette numeri interi positivi a,b,c,d,e,f,g tali che i prodotti ab,bc,cd,de,ef, fg, ga sono tutti cubi perfetti. Dimostrare che anche a,b,c,d,e,f,g, sonoi cubi perfetti

Osservazione: se un numero è un cubo perfetto allora ogni esponente che compare nella sua fattorizzazione in fattori primi è multiplo di 3.

Sia p un numero primo e siano $k_a k_b, k_c, \ldots k_g$ gli esponenti con cui compare rispettivamente nella fattorizzazione dei numeri a,b,….g

dalle condizioni iniziali del problema ricaviamo che

k_a+k_b k_b+k_c k_c+k_d k_d+k_e k_e+k_f k_f+k_g k_g+k_a sono tutti multipli di 3

quindi posso scrivere il sistema linerare nel campo dei numeri modulo 3

$k_a+k_b \equiv 0 \pmod 3$
$k_a+k_b \equiv 0 \pmod 3$
$k_c+k_d \equiv 0 \pmod 3$
$k_d+k_e \equiv 0 \pmod 3$
$k_e+k_f \equiv 0 \pmod 3$
$k_f+k_g \equiv 0 \pmod 3$
$k_g+k_a \equiv 0 \pmod 3$

la matrice associata a tale sistema ha determinante diverso da zero e quindi è invertibile. Il sistema ha come soluzione la sola soluzione banale $k_i = 0$ per ogni i quindi ogni esponente è multiplo di 3.

Multipli, sottomultipli, massimo comun divisore minimo comune multiplo.

Teorema di Bézout

Dati due numeri a e b sia d il loro massimo comun divisore (indichiamo d = (a,b))

allora $\exists n.m \in Z \quad tale \quad che \quad ma + nb = d$

esempio sia a = 44 e b= 13 d(44,13) =1
come si calcolano m ed n?

Metodo delle divisioni successive

$44 = [13]\cdot 3 + [5]$
$13 = [5]\cdot 2 + [3]$
$5 = [3]\cdot 1 + [2]$
$[3] = [2]\cdot 1 + 1$

Torno indietro con i resti

$1 = 3 - 2\cdot 1 = 3\text{-}(5\text{-}3\cdot 1)\cdot 1 = 3\cdot 2\text{-}5\cdot 1 = 2(13\text{-}5\cdot 2)\text{-}5 = 5(\text{-}5)+2\cdot 13 = (44\text{-}13\cdot 3)(\text{-}5)+2\cdot 13 =$
$44(\text{-}5)+13(17) =1$

Quindi m= -5 n=17

Esempio 1

Un sottoinsieme A dei numeri naturali compresi tra 1 e 100 è tale che la somma di suoi due elementi qualsiasi è divisibile per 6. Quanti elementi può avere, al massimo, il sottoinsieme A?

Oss. 1 I numeri devono essere tutti pari o dispari e devono essere tutti multipli di 3 ,se in A ci fosse un numero non divisibile per 3 (resto r) allora in A ci potrebbe essere solo un altro elemento (con resto 3-r) quello che sommato con lui sia divisibile per3 , e quindi l'insieme A avrebbe solo due elementi
I multipli pari di tre tra 1 e 100 sono 16
I multipli dispari di 3 tra 1 e 100 sono 17 quindi il numero massimo è 17.

Esempio 2

i) determinare tutte le coppie (m,n) di interi positivi che soddisfano l'equazione $n^2-2^m=1$
ii) determinare tutte le coppie (m,n) di interi positivi che soddisfano l'equazione $2^m-n^2=1$

i) osserviamo che n deve essere dispari quindi poniamo n = 2k+1 l'uguaglianza richiesta si trasforma in $4k(k+1)= 2^m$ perciò l'unico valore è k = 1 (altrimenti 2^m avrebbe un divisore dispari maggiore di 1 da cui n = 3 e m = 3
ii) anche in questo caso n deve essere dispari n = 2k+1 e l'uguaglianza diventa $4k^2+4k+2 = 2^m$ ma il numero a sinistra è congruo a 2 modulo 4 quindi deve essere m = 1 altrimenti 2^m è divisibile per 4.
Otteniamo m = 1 e n = 1

Esempio 3

Quali sono le ultime 4 cifre del numeratore del più piccolo numero razionale $\frac{a}{b}$ con ab= 28! (a,b primi fra loro) e tale che il numero b non sia multiplo di 35

28! è multiplo di 7 e 5 e b non può contenere contemporaneamente il 5 e il 7 quindi il più piccolo numero a è quello dato considerando 5 elevato ad esponente uguale a quante volte compare come fattore in 28! (i multipli di 5 contenuti in 28! sono 5,10,15,29,25 cioè sei volte) o da quello dato considerando il numero di fattori uguali a 7 cioè o 7^4=2401 o
5^6= 15625. la risposta è 2401.

Esempio 4

Determinare il più grande numero di 2 cifre tale che:

a) sia un numero primo
b) scambiando di posto le cifre sia ancora un numero primo
c) il prodotto delle cifre sia un numero primo

il numero deve essere dispari e una e una sola delle due deve essere 1. I possibili numeri sono 13,17,19. Invertendo l'ordine delle cifre sono primi 31 e 71, quindi il numero richiesto è 71.

Forma polinomiale di un numero

Sia b un intero maggiore di 1 la base di un sistema di numerazione

Ogni intero positivo n si può scrivere $n = a_n b^n + a_{n-1} b^{n-1} + \ldots\ldots a_1 b + a_0$ con $0 \leq a_i < b$

Esempio 1

I membri di una tribù hanno 10 dita alle mani e 9 ai piedi e quindi contano indifferentemente in base 10 o 19. Un intero positivo è detto "sacro" se in entrambe le basi si scrive con le stesse due cifre,(comprese tra 1 e 9). Quanti sono i numeri sacri?

Siano a e b le cifre , naturalmente le cifre devono essere presenti in ordine diverso quindi otteniamo che $10a+b=19b+a$ da cui $9a=18b$ cioè $a=2b$
I numeri sono 21 42 63 84.

Esempio 2

Un numero naturale n è detto gradevole se gode delle seguenti proprietà:

- La sua espressione decimale è costituita da 4 cifre
- La prima e la terza cifra di n sono uguali
- La seconda e la quarta cifra di n sono uguali
- Il prodotto delle cifre di n divide n^2
- Si determinino tutti i numeri gradevoli

$n = 1000a+100b+10c+d$ con $a = c$ $b = d$ quindi $n = 1010c+ 101d = 101(10 c + d)$ (i)

con c e d numeri da 1 a 9 (lo 0 è escluso altrimenti il prodotto delle cifre sarebbe 0 e contraddice la quarta condizione)

il prodotto delle cifre è $(cd)^2$ e sappiamo che $(cd)^2 | n^2$ allora $cd|n$ cioè $c|n$ e $d|n$. (ii)

101 è primo quindi $MCD(c,101) = MCD(d,101) = 1$ quindi $c|10c+d$ e $d | 10c+d$ poiché $c |10c$ allora $c|d$ e poiché $d|d$ allora $d|10c$ $c|d|10c$

possiamo avere i seguenti casi :

- d=c
- d=2c
- d=5c

$d = c$ per la (ii) ottengo $c^2|101(11c)$ cioè $c^2|11c$ cioè $c|11$ e quindi $c = 1$ e $d = 1$il numero è 1111
$d = 2c$ ottengo $2c^2|101 (12c)$ cioè $c|6$ per cui $c = 1, 2, 3$ le coppie che ottengo sono (1,2) (2,4) (3,6) i numeri sono 1212 2424 3636
$d = 5c$ ottengo $5c^2|15c$ cioè $c|3$ da cui $c =1,3$ l'unica coppia che ottengo è 1,5 il numero è 1515

Esempio 3

Quanti sono i numeri di due cifre AB tali che $(AB)^2$ = CAAB, con C=B-1 (in notazione decimale)?

Osserviamo intanto che se il quadrato di un numero termina con la stessa cifra del numero tale cifra può essere solo uno dei seguenti numeri 0,1,5,6
Quindi B è uno di questi quattro numeri, dalla condizione che C=B-1 e C positivo (il numero è di quattro cifre) escludiamo che B possa essere 0 o 1.
Analizziamo i due casi

- B= 5 $(A5)^2 = (10A+5)^2 = 100A^2+100A+25$
  $4AA5 = 4000+100A+10A+5$

Uguagliando otteniamo $100A^2 - 10A - 3980 = 0$ $10A^2 - A - 398 = 0$ che non ha soluzioni comprese tra 1 e 9

- B = 6 con lo stesso ragionamento otteniamo $10A^2 + A - 497 = 0$ che ha come unica soluzione intera A = 7

L'unica soluzione per AB è 76.

Equazioni Diofantee

Diofantee di primo grado

Una equazione Diofantea di primo grado in due variabili è del tipo ax+by=c
Se c = 0 l'equazione è omogenea

Teorema 1 Una equazione Diofantea di primo grado omogenea ammette sempre infinite soluzioni
È sufficiente osservare che se d = (a,b) allora a =kd e b=hd allora tutte le soluzioni sono x= .hz e y = -kz al variare di z in Z.

Teorema 2 una equazione Diofantea di primo grado non omogenea ammette almeno una soluzione se e solo se $(a,b) \mid c$ in tal caso le soluzioni sono infinite.

Le soluzioni sono infinite perché:

se (x_1,y_1) (x_2,y_2) sono due soluzioni della non omogenea la coppia (x_1-x_2,y_1-y_2) è soluzione della omogenea. quindi trovate *tutte* le soluzioni (infinite) della omogenea e *una* della non omogenea è sufficiente sommare le prime a questa per ottenere le infinite soluzione della non omogenea.

Per trovare una soluzione della non omogenea è sufficiente considerare d= (a,b) e determinare m ed n del teorema di Bézout cioè tali che am+bn=d. Se è verificata la condizione necessaria e sufficiente) che $d \mid c$ cioè che esiste k tale che c = kd allora x = km e y = kn è una soluzione della non omogenea.

Conclusione: una equazione Diofantea di primo grado ha sempre o 0 soluzioni o infinite soluzioni.

Esempio 1

Determinare tutte le soluzioni (x,y) intere positive dell'equazione 153x-253y=12

calcoliamo il MCD(153 e 253) = 1 allora l'equazione ha soluzione

una soluzione dell'equazione 153 x – 253y = 1 è data dall'applicazione del teorema di Bézout eseguendo il calcolo si ottiene $153 \cdot 43 - 253 \cdot 26 = 1$
da cui $153 \cdot 43 \cdot 12 - 253 \cdot 26 \cdot 12 = 12$ quindi (516,312) è una soluzione dell'equazione.

per il teorema 1 abbiamo che le soluzioni dell'omogenea sono x = 153z e y = 253z essendo MCD = 1 si ha h =253 e k = 153 con $z \in Z$
quindi tutte le soluzioni intere sono
x = 516+253z
y = 312+153z

poiché vogliamo solo le soluzioni positive dobbiamo calcolare la più piccola soluzione positiva e poi considerare $z \in N$.

La più piccola soluzione positiva è x = 10 e y = 6

quindi tutte le soluzioni intere positive sono x = 10 +253z
y = 6 + 153z $\quad z \in N$

Diofantee di grado superiore

Secondo grado

una equazione Diofantea di secondo grado in due variabili è del tipo
$ax^2 + by^2 + cxy + dx + ey + f = 0$

se a = 0 o b = 0 l'equazione è di primo grado in una variabile ed è risolvibile ricavando tale variabile come rapporto di due polinomi.

esempio a = 0 allora $x = -\frac{by^2 + ey + f}{cy + d}$ dividendo i polinomi si riporta sotto la forma

$x = \frac{1}{c^2}\left(a'y + b' + \frac{c'}{cy + d}\right)$ con a',b',c' interi.

un altro modo possibile è scomporre in fattori il polinomio e ricondursi a equazioni di primo grado

Esempio 1

Se a è un numero intero positivo minore di 100, per quanti valori di a il sistema

$$\begin{cases} x^2 = y + a \\ y^2 = x + a \end{cases}$$

ha soluzioni intere?

sottraendo otteniamo (x-y)(x+y) = - (x-y) da cui (x-y) (x+y+1) = 0

- x = y l'equazione diventa x^2-x-a = 0 perché abbia soluzioni intere deve essere 1+4a il quadrato di un numero dispari perciò
  $1+4a = (2n+1)^2$ sviluppando a = n(n+1) essendo a< 100 ho 9 valori per n e quindi 9 valori per a

- x+y+1 = 0 otteniamo x^2+x+1-a = 0 analogamente a prima deve essere 1+4(a-1) il quadrato di un numero dispari $1+4(a-1) = (2n+1)^2$ da cui a = n(n+1)+1 $0 \le n < 10$ perciò 10 valori di a

In totale possiamo avere 19 valori di a.

Esempio 2

Determinare quante sono le soluzioni intere dell'equazione

$x^2-y^2=2007$

l'equazione si trasforma in $(x-y)(x+y) = 3^2 \cdot 223$

quindi dovrei scrivere tutti i possibili sistemi (12) del tipo $\begin{cases} x+y=A \\ x-y=B \end{cases}$ ottengo $x = \frac{A+B}{2}$ e $y = \frac{A-B}{2}$ da queste uguaglianze, sapendo che sto cercando le soluzioni intere deduco che A e B sono o entrambi pari o entrambi dispari e poiché i divisori di 2007 sono tutti dispari ho 12 soluzioni

Esempio 3

Un intero positivo si dice triangolare se si può scrivere nella forma $\frac{n(n+1)}{2}$ per qualche intero positivo n. quante sono le coppie (a,b) di numeri triangolari tali che b-a=2007?

Siano $a= \frac{n(n+1)}{2}$ e $b = \frac{m(m+1)}{2}$

dalla condizione b-a = 2007 otteniamo $(m-n)(m+n+1) = 2 \cdot 3^2 \cdot 223$

osservazione 1 poiché n>0 e m>0 anche m+n+1 >0 ed allora anche m-n >0 .
osservazione 2 m-n < m+n+1

quindi i possibili casi sono (chiamando x = m-n e y = m+n+1)

- $x = 1$ $y = 2 \cdot 3 \cdot 3 \cdot 223$
- $x = 2$ $y = 3 \cdot 3 \cdot 223$
- $x = 3$ $y = 2 \cdot 3 \cdot 223$
- $x = 2 \cdot 3$ $y = 3 \cdot 223$
- $x = 3 \cdot 3$ $y = 2 \cdot 223$
- $x = 2 \cdot 3 \cdot 3$ $y = 223$

risolvendo il sistema $\begin{cases} m-n=x \\ m+n+1=y \end{cases}$ rispetto a m e n otteniamo $\begin{cases} m=\frac{x+y-1}{2} \\ n=\frac{y-x-1}{2} \end{cases}$

sostituendo i valori ottenuti per x e y otteniamo esattamente 6 soluzione intere positive

Bibliografia

Massimo Gobbino Schede olimpiche

Carlo Traverso corso di aritmetica Università di Pisa

testi delle gare provinciali e nazionali e della gara a squadre