PROBLEMA 1

Sia X l'insieme dei numeri da 0 a 9 (compresi),

e A = {0, 1, 3, 5, 6, 8}

a) (Punti 4) Contare le stringhe di 10 cifre in X aventi 4 come prima cifra e non contenenti cifre in A.

il gruppo X è così composto X={0 1 2 3 4 5 6 7 8 9 }

X-A={2 4 7 9}

abbiamo quindi 4 scelte e 10 caselle disponibili sapendo che la prima sarà sempre 4 le altre 9 saranno casualmente composte dalle 4 cifre

quindi la soluzione è 49 in modo da avere tutte le possibili combinazioni

b) (Punti 4) Contare le stringhe di 10 cifre in X tali che la prima cifra è in A e l'ultima cifra è congrua modulo 5 alla somma delle prime cinque cifre.

la prima cifra sarà sicuramente in A quindi abbiamo: 6 alternative

le rimanenti cifre libere sono 8 dato che l’ultima ha una condizione quindi le combinazioni sono 108

l'ultima cifra la otteniamo creando 2 sottogruppi di 5 elementi

B={0 1 2 3 4}

C={5 6 7 8 9}

che sono le possibili classi di resto mod 5

quindi ci sono esattamente 2 scelte possibili per l’ultima cifra in base alla somma delle precedenti cifre

quindi in conclusione le possibili stringhe sono 2\*6\*108

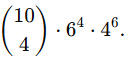
c)(Punti 3) Contare le stringhe di 10 cifre in X contenenti esattamente 4 cifre in A

quindi abbiamo 4 scelte su 10 possibilità che sono

quindi la risposta è (10! /4! \*(10-4)! o 10 su 4 coefficiente binomiale

Ogni posizione scelta per una cifra in A può essere occupata da una qualsiasi delle 6 cifre in A={0,1,3,5,6,8} quindi dato che le cifre sono 4 abbiamo 64 combinazioni

utilizzando X-A={2 4 7 9} calcolato nel punto A sappiamo che X-A ha cardinalità 4 quindi le combinazioni per le restanti 6 cifre sono 46

la formula completa quindi sarà:

PROBLEMA 2

a) (Punti 4) Dire se la congruenza:

34x ≡ 6 mod 38

ammette soluzioni e in questo caso risolverla

mcd(34 38)=2

6/2=3

la congruenza ammette soluzione

semplifichiamo dividendo tutto per il mcd ovvero due e viene:

17x≡3 mod 19

ora bisogna trovare l’inverso moltiplicativo di 17

euclide( 19 17 )

19=17\*1+2

17=2\*8+1

2=1\*2+0

bezout

1=17-2\*8

1=17-(19-17)\*8=

1=17\*9-19\*8

9 è l’inverso moltiplicativo di 17 mod 19

ora moltiplichiamo ad entrambi i lati per 9

9⋅17x≡9⋅3 mod 19

dato che 9 è l’inverso di 17 esso scompare e rimane

x≡27 mod 19 ovvero x≡8 mod 19

b) (Punti 4) dire se 7 sta in Z☆32; in caso affermativo determinarne il periodo

per determinarlo dobbiamo dare l’mcd tra 7 e 32

mcd(7 32)=1 quindi si sta in Z☆32

il periodo è il più piccolo intero positivo k tale che: ak≡1 mod n

nel nostro caso quindi 7k≡1 mod 32

procediamo calando le varie potenze di 7 e troviamo che la più piccola che è congrua ad 1 mod 32 è : 74

quindi il periodo è 4

c) (Punti 3) Sia N = 7919 e si dia per noto che N è primo. Calcolare:

215839 + N11 mod 3N

calcoliamo i 2 termini

215839 mod 3N e N11 mod 3N

n=7919 (sappiamo che è primo)

quindi il mod sarà 3\*7919

calcoliamo il ᵠ del modulo ᵠ(3\*7919)=2\*7918=15836

sapendo che 15836 è id

215839 mod 15836 ≡ a 23 mod 15836

quindi 215839 ≡ 8 mod 15836

Poiché mcd (N, 3) = 1 e φ(3) = 2, si ha per il teorema di Eulero N11 = (N 2)5 · N ≡ N mod 3.

N11 mod 3N ≡ N quindi N=7919

8+N=7927 mod 3N