Compitino di MD
17 dicembre 2015

Cognome e nome: .....

Numero di matricola: ..... Corso e Aula: .....

IMPORTANTE: Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non si può scrivere con il lapis. Motivare in modo chiaro le risposte.

Esercizio 1. Consideriamo l'insieme dei numeri interi

$$A = \{x \in \mathbb{N} \mid 10^6 \leq x < 10^7\}$$

a) Quanti sono i numeri in A nella cui scrittura decimale la cifra 1 compare esattamente quattro volte?
b) Vogliamo suddividere A in due sottoinsiemi, ciascuno di 4500000 elementi. In quanti modi diversi si può fare?

(a) In A ci sono i numeri interi positivi con 7 cifre significative
Quelli con quattro cifre 1 possono essere di 2 tipi

i) 1 _ _ _ _ _ _ 1 al primo posto e 3 cifre 1 nei rimanenti 6 posti.

$\rightarrow \binom{6}{3} \cdot 9^3 \rightarrow$ 9 scelte ~~per~~ ciascuna delle 3 cifre $\neq 1$

$\hookrightarrow$ scelte per le posizioni delle cifre 1

ii) a _ _ _ _ _ _ Per a ho 8 possibili valori ($\neq 0, 1$)
Devo mettere ancora 1 in 6 posti: $\binom{6}{4}$ scelte per la posizione
Le rimanenti 2 cifre possono essere scelte ciascuna in 9 modi $\rightarrow 8\binom{6}{4}9^2$

In Totale $\binom{6}{3}9^3 + \binom{6}{4}9^2 \cdot 8 = \frac{6 \cdot 5 \cdot 4}{3!} 3^6 + \frac{6 \cdot 5}{2} 2^3 3^4 = 2^2 3^5 5^2$

(b) Si chiede di contare le partizioni di A, che ha 9000000 elementi, in 2 sottoinsiemi di cardinalità 4500000. Poiché i 2 sottoins. hanno la stessa cardinalità posso fare bin $\binom{9 \cdot 10^6}{45 \cdot 10^5} \frac{1}{2}$ modi

Esercizio 2. Sia $N = 5000000$.
a) Quanti sono i divisori positivi di N?
b) Quanti sono i divisori positivi di N che sono il quadrato di un numero intero?

$N = 2^6 5^7$ $\quad d \mid N \Leftrightarrow$

$d = 2^a 5^b \quad 0 \leq a \leq 6, \; 0 \leq b \leq 7 \rightarrow 7 \cdot 8 = 56$ divisori

$d = c^2 \Leftrightarrow$ $\quad a$ e b sono pari

$a = 0, 2, 4, 6$ $\quad$ e $\quad b = 0, 2, 4, 6 \Rightarrow 4 \cdot 4 = 16$

Esercizio 3. Avete organizzato una prova didattica del metodo RSA, e avete scelto i primi $p = 11$ e $q = 19$. Avete reso pubblico il prodotto $pq = 209$ e l'esponente di codifica $e = 13$.
Ricevete il messaggio 154.
Qual è il messaggio originale che vi è stato inviato?

Cerco il codice di decodifica d:

$13d \equiv 1 \quad ((11-1)(19-1))$

$13d \equiv 1 \quad (180)$

$180 = 13 \cdot 13 + 11$
$13 = 11 \cdot 1 + 2$
$11 = 2 \cdot 5 + 1$

$1 = 11 - 5 \cdot 2 = 11 - 5(13 - 11) =$
$= -5 \cdot 13 + 6(180 - 13 \cdot 13) =$
$= 6 \cdot 180 - 83 \cdot 13$

$\boxed{d \equiv -83 \equiv 97 \ (180)}$

Il messaggio originale è $x \equiv 154^{97} \ (209)$

Uso il Teorema cinese

$\begin{cases} x \equiv 154^{97} \ (11) \\ x \equiv 154^{97} \ (19) \end{cases}$ $\begin{cases} x \equiv 0 \ (11) \\ x \equiv 2^{97} \ (19) \end{cases}$

$154 \mid 19$
$2 \quad 8$

$97 = 18 \cdot 5 + 7 \qquad 2^{97} \equiv 2^7 \ (19)$
$2^4 = -3 \qquad 2^7 = (-3) \cdot 8 = -24 \equiv -5 \ (19)$

$\begin{cases} x \equiv 0 \ (11) \\ x \equiv -5 \ (19) \end{cases}$

$x = -5 + 19t \qquad -5 + 19t \equiv 0 \ (11)$

$\Rightarrow 8t \equiv 5 \ (11) \qquad t \equiv 5(-4) \ (11) \Rightarrow t \equiv -20 \equiv 2 \ (11)$

$x = -5 + 19(2 + 11k) \Rightarrow \boxed{x \equiv 33 \ (209)}$

Il messaggio originale è $\boxed{x = 33}$

Esercizio 4. Fattorizzare il polinomio x^4-3 come prodotto di polinomi irriducibili in $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_{13}[x]$.

$\mathbb{Q}[x]$

x^4-3 è irriducibile perché lo è in $\mathbb{Z}[x]$ per il criterio di Eisenstein con $p=3$ e quindi lo è anche in $\mathbb{Q}[x]$ per il lemma di Gauß.

Il polinomio è ovviamente riducibile in $\mathbb{C}(x)$ e in $\mathbb{R}[x]$ per il Teorema fondamentale dell'algebra e le sue conseguenze sui polinomi con coeff in $\mathbb{R}$.

$\mathbb{R}[x]$

$x^4-3 = (x^2-\sqrt{3})(x^2+\sqrt{3}) = (x-\sqrt[4]{3})(x+\sqrt[4]{3})(x^2+\sqrt{3})$

↑ è irriducibile perché $\Delta = -\sqrt{3} < 0$

$\mathbb{C}[x]$

$x^4-3 = (x-\sqrt[4]{3})(x+\sqrt[4]{3})(x-i\sqrt[4]{3})(x+i\sqrt[4]{3})$

$\mathbb{Z}_{13}[x]$

Vediamo se il polinomio $f(x)=x^4-3$ ha radici in $\mathbb{Z}_{13}$

$f(0) \neq 0 \quad f(\pm 1) \neq 0 \quad f(\pm 2) = 0 \Rightarrow \nexists\, x-2, x+2 \mid f(x)$

Abbiamo che $2^4-3=0 \Rightarrow 2^4=3$

$f(x) = x^4-2^4 = (x^2-2^2)(x^2+2^2) = (x-2)(x+2)(x^2+4)$

Si tratta ora di valutare se x^2+4 è riducibile o irriducibile in $\mathbb{Z}_{13}[x]$ e poiché ha grado 2 basta vedere se $\Delta = -4$ è o non è un quadrato

x	0	± 1	± 2	± 3	± 4	± 5	± 6

$\Rightarrow -4 = 3^2$

$f(x) = (x-2)(x+2)(x-3)(x+3)$