Esercizio 3.

a. Fattorizzare il polinomio $x^3 + 2x^2 + x + 2$ in $\mathbb{R}$, in $\mathbb{C}$ e in $\mathbb{Z}/13\mathbb{Z}$.

b. Quanti sono i polinomi di grado 3 (non necessariamente monici) in $\mathbb{Z}/13\mathbb{Z}$ con tre radici distinte?

a) $p(x) = x^3+2x^2+x+2 = x^2(x+2)+(x+2) = (x^2+1)(x+2)$

$\mathbb{R}[x]$ $\quad x^2+1$ è irriducibile perché $\Delta = -4 < 0$

$\Rightarrow p(x) = (x^2+1)(x+2)$

$p(x) = (x+i)(x-i)(x+2)$ è la fattorizza[zione]

$\mathbb{C}[x]$

(i polinomi di grado 1 sono sempre irriducibi[li] in ogni campo, e sono gli unici pol irridu[cibili] di $\mathbb{C}$)

$\mathbb{Z}/_{13\mathbb{Z}}[x]$ $\quad p(x) = (x+2)(x^2+1)$ Occorre vedere se x^2+1 è irriducibile o no. Poiché un[...] grado 2 è riducibile $\Leftrightarrow$ ha radici $\Leftrightarrow \exists \alpha \in \mathbb{Z}/_{13\mathbb{Z}}$ t.c. $\alpha^2+1=0$ $(\alpha^2=-1)$

Calcolo i quadrati degli el di $\mathbb{Z}/_{13\mathbb{Z}}$

0	±1	±2	±3	±4	±5	±6
0	1	4	-4	3	-1	-3

$\Rightarrow p(x) = (x+2)(x-5)(x+5)$

b) Dobbiamo contare i polinomi del tipo

$c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ $\quad c \in \mathbb{Z}/_{13\mathbb{Z}}$ $c \neq 0$, $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$[...] distinti

quindi 12 scelte per c, $\binom{13}{3}$ per gli α_i

Esercizio 4.
Trovare la minima soluzione positiva $d \in \mathbb{Z}$ della congruenza $7d \equiv 1 \mod (60)$.
Una volta determinato d, si calcoli il resto di 40^{7d} modulo 77.

$60 = 2^2 \cdot 3 \cdot 5$

$$7d \equiv 1 \ (60) \iff \begin{cases} 7d \equiv 1 \ (4) \\ 7d \equiv 1 \ (3) \\ 7d \equiv 1 \ (5) \end{cases} \qquad \begin{cases} d \equiv -1 & (4) \\ d \equiv 1 & (3) \\ 2d \equiv 1 & (5) \end{cases}$$

$$\begin{cases} d \equiv 7 & (12) \\ d \equiv 3 & (5) \end{cases} \qquad \begin{cases} d = 7+12k \\ 7+12k \equiv 3 & (5) \end{cases}$$

$2+2k \equiv 3 \ (5)$ $\quad 2k \equiv 1 \ (5)$ $\quad k \equiv 3 \ (5)$

$d = 7 + 12 \cdot 3 \ (60)$

$d = 43 \ (60)$ $\quad \boxed{d = 43}$

$[40^{7d}]_{77}$ $\qquad x \equiv 40^{7d} \ (77)$

$\Downarrow$

~~Sappiamo~~

$$\begin{cases} x \equiv 40^{7d} & (7) \\ x \equiv 40^{7d} & (11) \end{cases}$$

$7d \equiv 1 \ (60) \Rightarrow 7d \equiv 1 \ (6)$ $\quad 7d = 1 + 6k$

Per il piccolo Teorema di Fermat, poichè $(40,7)=1$

$40^6 \equiv 1 \ (7)$ $\quad \Rightarrow 40^{7d} = 40^{6k+1} = (40^6)^k 40 = 1 \cdot 40 \equiv 40$

$7d \equiv 1 \ (60) \Rightarrow 7d \equiv 1 \ (10)$ $\quad 7d = 1 + 10h$

Per il piccolo Teorema di Fermat poichè $(40,11)=1$
si ha $40^{7d} \equiv 40^{6h+1} \equiv (40^6)^h 40 \equiv 40 \ (11)$

$$\Rightarrow \begin{cases} x \equiv 40 & (7) \\ x \equiv 40 & (11) \end{cases} \iff x \equiv 40 \ (77)$$