CORSO DI GEOMETRIA
ESEMPI DI CAMPI FINITI: CLASSI DI RESTO MODULO n
A.A. 2019/2020
PROF. VALENTINA BEORCHIA

- Consideriamo l'insieme $\mathbb{Z}_2 = \{0, 1\}$. Definiamo due operazioni, la somma $\oplus$, ed il prodotto $\odot$, come segue:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

Si verifica facilmente che $\{0, 1\}$, con queste operazioni è un campo. Osserviamo che $\oplus$ e $\odot$ sono definite come segue: per ogni $a, b \in \{0, 1\}$, $a \oplus b$ (rispettivamente $a \odot b$) è il resto della divisione per 2 della somma usuale $a + b \in \mathbb{Z}$ (rispettivamente il prodotto usuale $a \cdot b \in \mathbb{Z}$). Per tale motivo $\mathbb{Z}_2$ si chiama l'insieme dei resti della divisione per 2.

- Analogamente si può considerare l'insieme $\mathbb{Z}_3 = \{0, 1, 2\}$ e definire due operazioni, la somma $\oplus$ ed il prodotto $\odot$, come segue:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Anche in questo caso si verifica facilmente che $\{0, 1, 2\}$ con queste operazioni è un campo. Osserviamo che $\oplus$ (rispettivamente $\odot$) sono definite come segue: per ogni $a, b \in \{0, 1, 2\}$, $a \oplus b$ (rispettivamente $a \odot b$) è il resto della divisione per 3 della somma usuale $a + b \in \mathbb{Z}$ (rispettivamente il prodotto usuale $a \cdot b \in \mathbb{Z}$). Per tale motivo $\mathbb{Z}_3$ si chiama insieme dei resti della divisione per 3.

- In maniera analoga, definiamo due operazioni $\oplus, \odot$ sull'insieme $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ dei resti della divisione per 4 (scrivere le relative tabelle per esercizio).
  In questo caso, però, non si ottiene un campo (esercizio).

- In generale, per ogni numero naturale $n \neq 0$, si considera l'insieme

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

detto insieme dei resti della divisione per n. Si definiscono due operazioni $\oplus$ e $\odot$ come sopra: se $a, b \in \mathbb{Z}_n$ $a \oplus b$ è il resto della divisione per n di $a + b$; $a \odot b$ è il resto della divisione per n di $a \cdot b$, dove $+$ e $\cdot$ sono le usuali operazioni in $\mathbb{Z}$. Si può dimostrare che $\mathbb{Z}_n$, con le operazioni $\oplus$ e $\odot$ è un campo se e solo se n è un numero primo.