Algebra B — 30 Giugno 2009

1. Sia $\mathbb{Z}_2[x]$ l'anello dei polinomi in x a coefficienti in $\mathbb{Z}_2$.

   - Mostrare che non ha divisori dello zero. E' un campo?
   - Fattorizzare in polinomi di primo grado il polinomio $x^2 + 1$.
   - Mostrare che il polinomio $x^2 + x + 1$ non ha radici in $\mathbb{Z}_2$.
   - Sia ε una radice complessa di $x^2 + x + 1$ e si consideri l'insieme:

   $$\mathbb{F} = \left\{ a + \varepsilon b \text{ con } a, b \in \mathbb{Z}_2 \text{ , } \varepsilon^2 + \varepsilon + 1 = 0 \right\} \tag{1}$$

   con le due operazioni:

   $$(a + \varepsilon b) + (c + \varepsilon d) = (a + c) + \varepsilon (b + d) \tag{2}$$
   $$(a + \varepsilon b)(c + \varepsilon d) = (ac + bd) + \varepsilon (ad + bc + bd) \tag{3}$$

   - Scrivere le tavole delle due operazioni e concludere che è un campo.
   - Mostrare che rispetto alla somma $\mathbb{F}$ non è un gruppo ciclico.
   - Mostrare che invece rispetto alla moltiplicazione $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ è un gruppo ciclico e darne un generatore.
   - Mostrare che $\mathbb{F} = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ dove $(x^2 + x + 1)$ è l'ideale generato dal polinomio irriducibile
   $$x^2 + x + 1$$

2. Mostrare che nessun numero intero congruo a 3 modulo 4 può essere scritto come somma di due quadrati.

3. Dimostrare che l'espressione $\frac{1}{11}(n^{111} + 10n)$ rappresenta un numero intero per ogni n intero.

SOLUZIONI

Esercizio n.1

- $\mathbb{Z}_2[x]$ non ha divisori dello zero perchè i coefficienti sono in un campo. Non è un campo perchè l'unico elemento invertibile è 1
- $x^2+1=(x+1)(x+1)$.
- La funzione x^2+x+1 assume solo il valore 1.
- Gli elementi dell'insieme sono $0,1,\varepsilon,1+\varepsilon$ e le tavole delle operazioni sono:

$+$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\varepsilon}$	$\mathbf{1+\boldsymbol{\varepsilon}}$
$\mathbf{0}$	0	1	ε	$1+\varepsilon$
$\mathbf{1}$	1	0	$1+\varepsilon$	ε
$\boldsymbol{\varepsilon}$	ε	$1+\varepsilon$	0	1
$\mathbf{1+\boldsymbol{\varepsilon}}$	$1+\varepsilon$	ε	1	0

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\varepsilon}$	$\mathbf{1+\boldsymbol{\varepsilon}}$
$\mathbf{0}$	0	0	0	0
$\mathbf{1}$	0	1	ε	$1+\varepsilon$
$\boldsymbol{\varepsilon}$	0	ε	$1+\varepsilon$	1
$\mathbf{1+\boldsymbol{\varepsilon}}$	0	$1+\varepsilon$	1	ε

- E' un campo perchè è un anello commutativo con unità ed inoltre ogni elemento diverso da zero ha un *inverso.*
- $\mathbb{F}$ ha ordine 4, ma non ha elementi di ordine 4, infatti tutti i suoi elementi hanno ordine 2 rispetto alla somma.
- $\mathbb{F}^*=\mathbb{F}\setminus\{0\}$ ha ordine 3, un generatore è ad esempio, ε che ha ordine 3 rispetto al prodotto.
- In $\mathbb{F}=\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ ogni classe è rappresentata da $\overline{a+bx}$, essendo $a+bx$ il resto della divisione di qualsiasi polinomio per x^2+x+1. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$\begin{aligned}(a+\varepsilon b)+(c+\varepsilon d) &= (a+c)+\varepsilon(b+d) &(4)\\ (a+\varepsilon b)(c+\varepsilon d) &= (ac+bd)+\varepsilon(ad+bc+bd) &(5)\end{aligned}$$

Per la somma è ovvio, per il prodotto si ha:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right)=\overline{(a+bx)(c+dx)}=\overline{ac+(ad+bc)x+bdx^2} \tag{6}$$

ma essendo (ricordando che in $\mathbb{Z}_2$ ogni elemento ha ordine 2 ripetto alla somma):

$$ac+(ad+bc)x+bdx^2=ac+bd+(ad+bc+bd)x+bd\left(x^2+x+1\right) \tag{7}$$

si ottiene il risultato voluto:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right)=\overline{ac+bd+x(ad+bc+bd)} \tag{8}$$

Un isomorfismo tra $\mathbb{F}$ e $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ è dato da $(a+\varepsilon b)\rightarrow\left(\overline{a+bx}\right)$.

Esercizio n.2

- Un quadrato diviso per 4 può avere come resti solo 0 oppure 1, quindi la somma di due quadrati non può mai avere resto 3

Esercizio n.3

- Bisogna dimostrare che
$$n^{111} + 10n = 0 \bmod 11$$

Ci sono due casi da studiare:
1) se n è multiplo di 11 non c'è niente da dimostrare, il resto è ovviamente 0.
2) se n non è divisibile per 11, il piccolo teorema di Fermat ci dice in questo caso che $n^{10} = 1 \bmod 11$ e quindi, ragionando $\bmod 11$,

$$n^{111} + 10n = n(n^{110} + 10) = n\left[\left(n^{10}\right)^{11} + 10\right] = n(1 + 10) = 11n = 0$$