Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2006/2007
AL1 - Algebra 1, fondamenti
Tutorato 8 (4 Dicembre 2006)
A cura di **Chiara Valenti**

1. Sia A un anello commutativo unitario. Un elemento $a \in A$ si dice *idempotente* se $a^2 = a$ e A si dice *booleano* se ogni suo elemento è idempotente.

   Mostrare che:

   (1) Se a è idempotente e $a \neq 0, 1$, allora a è uno zero-divisore;

   (2) Se A è booleano, allora $2a = 0$, per ogni $a \in A$;

   (3) L'anello $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ n volte, con le operazioni di addizione e moltiplicazione definiti componenete per componente, è un anello booleano, per ogni ≥ 1.

   Conoscete altri anelli booleani?

2. Dimostrare che l'insieme degli zero-divisori di un anello commutativo unitario non è mai un gruppo moltiplicativo. Includendo lo zero, può essere un gruppo additivo?

3. Dimostrare che, per ogni coppia (a, b) di numeri interi dispari, risulta
$$a^2 \equiv b^2 \pmod 4 .$$

4. Sia p un numero primo e sia $\overline{a} \in \mathbb{Z}_p$. Dimostrare che
$$(\overline{a})^{-1} = \overline{a} \Leftrightarrow \overline{a} = \overline{1} \quad \text{oppure} \quad \overline{a} = \overline{(p-1)} .$$
   Mostrare con un esempio che l'ipotesi che p sia primo è necessaria.

5. Determinare gli elementi invertibili e gli zero-divisori degli anelli:
$$\mathbb{Z}_7 ; \quad \mathbb{Z}_8 ; \quad \mathbb{Z}_9 ; \quad \mathbb{Z}_{12} ; \quad \mathbb{Z}_{15} .$$
   In ognuno di questi casi, scrivere inoltre la tabella moltiplicativa del gruppo degli elementi invertibili.

6. Calcolare la funzione di Eulero di 21, 41, 49.

7. Siano $a, b \in \mathbb{Z}$, $d := MCD(a, b)$ e $d = xa + yb$ un'identità di Bezout. Mostrare che $MCD(x, y) = 1$.

8. Determinare un inverso aritmetico di 32 modulo 625 e di 59 modulo 997.

9. Risolvere, quando è possibile, le seguenti congruenze lineari:

   $9X \equiv 27 \mod 20$; $9X \equiv 27 \mod 18$;

   $9X \equiv 12 \mod 18$; $9X \equiv 18 \mod 12$;

   $150X \equiv 1 \mod 727$; $150X \equiv 11 \mod 727$;

   $150X \equiv 11 \mod 39275$; $150X \equiv 39 \mod 231$.

10. Risolvere il seguente sistema di congruenze lineari:
$$\begin{cases} 15X \equiv -3 \mod 6 \\ 20X \equiv 5 \mod 9 \end{cases}$$