Corso di Algebra per Informatica

Lezione 24: Esercizi

- (1) Utilizzare l'algoritmo delle divisioni successive per trovare, in \mathbb{Z} , MCD(72, 402), MCD(141, 39), MCD(182, 104), MCD(1111231, 111123).
- (2) Per ogni coppia (a, b) di numeri dell'esercizio precedente scegliere un $d \in MCD(a, b)$ ed utilizzare la dimostrazione del Teorema di Bézout per trovare due interi u e v tali che d = au + bv. [Si tratta del cosiddetto "Algoritmo delle divisioni successive esteso"]
- (3) Esiste un numero u tale che 2u 1 è multiplo di 3? Trovarlo.
- (4) Esiste un numero u tale che 79u 1 è multiplo di 23?
- (5) Trovare $a.b, c \in \mathbb{Z}$ per cui non valga il Lemma di Euclide.
- (6) Dimostrare che 2 è un numero primo.
- (7) Dimostrare che -2 è irriducibile.

Sia $s \neq \emptyset$ e * un'operazione binaria interna su s. Una relazione di equivalenza \sim su s si dice *compatibile a sinistra* con * se $(\forall a, b, c \in s)(a \sim b \rightarrow c * a \sim c * b)$. Rispettivamente *a destra*.

Sia $s \neq \emptyset$ e siano $*_1, \ldots, *_n$ n operazioni binarie interne su s. Una relazione di equivalenza \sim su s si dice una *congruenza* in $(s, *_1, \ldots, *_n)$ se $(\forall a, b, c, d \in s)((\forall i \in \{1, \ldots, n\})((a \sim b \land c \sim d) \rightarrow a *_i c \sim b *_i d))$.

- (8) Sia $s \neq \emptyset$, siano $*_1, \ldots, *_n n$ operazioni binarie interne su s e sia \sim una relazione di equivalenza su s. Dimostrare che \sim è una congruenza in $(s, *_1, \ldots, *_n)$ se e solo se è compatibile a destra e a sinistra con ogni operazione di $(s, *_1, \ldots, *_n)$.
- (9) Sia m un elemento di \mathbb{Z} . Dimostrare che \equiv_m è una congruenza rispetto a + e a \cdot .
- (10) Sia * l'operazione binaria di $\mathbb Z$ definita da

$$(\forall a, b \in \mathbb{Z})((2 / b \to a * b = a + b) \land (2 | b \to a * b = a + b/2)).$$

Dimostrare che \equiv_2 non è una congruenza rispetto a *.