Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2005/2006
AL1 - Algebra 1, fondamenti
Tutorato 6 (31 ottobre 2005)
A. Fabbri - G. Fusacchia

1. Utilizzando il metodo delle divisioni successive, trovare il MCD$(3579, 56)$ ed una identità di Bézout.

2. Sia n un numero naturale; trovare MCD$(n, n+1)$.

3. Verificare che se $a \equiv b \pmod{n_1}$ e $a \equiv b \pmod{n_2}$, allora $a \equiv b \pmod{n}$ ove $n =$mcm(n_1, n_2). Quindi se MCD(n_1, n_2)=1, allora $a \equiv b \pmod{n_1 n_2}$.

4. Provare che se $x \equiv a \pmod{n}$, allora $x \equiv a \pmod{2n}$ oppure $x \equiv a + n \pmod{2n}$.

5. Provare che:
   (a) ogni numero primo della forma $3n + 1$ è anche della forma $6m + 1$;
   (b) l'unico numero primo della forma $n^3 - 1$ è 7;
   (c) l'unico numero primo p per cui $3p + 1$ è un quadrato è 5.

6. Per ciascuna delle seguenti classi resto modulo n, $[x]_n$, determinare un rappresentante x' tale che $0 \leq x' \leq n - 1$:
   $[-432]_{48}$, $[5678]_{107}$, $[-456]_{35}$, $[209]_{11}$.

7. Stabilire quali dei seguenti elementi di $\mathbb{Z}_n$ sono zero-divisori e quali sono invertibili; per ciascuno degli elementi invertibili trovare l'inverso:
   (a) $[-45]_{12}$, $[29]_{12}$, $[52]_{12}$, $[-30]_{12}$, $[19]_{12}$;
   (b) $[-22]_{18}$, $[41]_{18}$, $[25]_{18}$, $[-47s]_{18}$, $[28]_{18}$.

8. Provare che:
   (a) se n è un intero pari, allora $n^2 \equiv 0, 4 \pmod{8}$; se n è un intero dispari, allora $n^2 \equiv 1 \pmod{8}$. Dedurne che la somma dei quadrati di tre numeri interi non è mai congrua a 7 (mod 8);
   (b) l'equazione $X^2 + Y^2 - 15Z^2 = 7$ non ha soluzioni intere.

9. Provare che:
   (a) per ogni numero intero n, si ha che $n^3 \equiv 0, 1, 8 \pmod{9}$;
   (b) per ogni numero intero n, si ha che $n^3 \equiv n \pmod{6}$.