Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2009/2010
AL110 - Algebra 1
Tutorato 5 (26 ottobre 2009)
E. Di Gloria - D. Menichetti

1. Usando l'Algoritmo Euclideo delle divisioni successive, calcolare il MCD$(2424, 772)$ ed una identità di Bézout.

2. Utilizzando il fatto che il MCD(a, b) divide $a-b$, trovare il MCD$(1962, 1965)$ e il MCD$(1961, 1965)$.

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

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

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

6. Provare che:

   (a) ogni numero primo della forma $3n+1$ con $n \in \mathbb{N}$ è anche della forma $6m+1$;

   (b) l'unico numero primo della forma $n^3 - 1$ con $n \in \mathbb{N}$ è 7;

   (c) l'unico numero primo p per cui $3p+1$ è un quadrato è 5.

7. Per ciascuna delle seguenti classi resto modulo n, $[x]_n$, determinare un rappresentante x' tale che $0 \leq x' \leq n-1$:

   $[-432]_{48}$, $[5678]_{107}$, $[-456]_{35}$, $[209]_{11}$.

8. Utilizzando il principio di induzione si dimostri che:

   (a) per ogni $n \geq 1$ si ha :

   $$(1+i)^n = 2^{\frac{n}{2}}(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4}).$$

   (b) se a è un intero *dispari*, allora per ogni $n \geq 1$ si ha che:

   $$a^{2^n} \equiv 1 \qquad \text{mod } 2^{n+2}.$$

9. 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.

10. 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 $n^3 \equiv n \pmod 6$.

11. Utilizzando il principio di induzione si dimostri che, per ogni $n \geq 1$:

$$2^n + (-1)^{n+1} \equiv 0 \pmod 3$$

12. Dimostrare che se $a, b \in \mathbb{Z}$ ed n un intero ≥ 2 sono tali che $a \equiv b \pmod n$, allora

$$\mathrm{MCD}(a, n) = \mathrm{MCD}(b, n).$$

.