# Algebra (Informatica) — 24 Gennaio 2002

*Si hanno a disposizione 36 punti. Con più di 19 punti si può fare l'orale o accettare il voto dello scritto (30 e lode per chi risolve tutti gli esercizi); con meno di 17 punti si deve rifare lo scritto; con 17, 18 o 19 punti si è ammessi all'orale.*

1. **Risolvere, se possibile, le seguenti congruenze: (3 punti)**

   **a)** $22x = 4 \bmod 5$
   **b)** $2x = -11 \bmod 5$
   **c)** $7x = 1 \bmod 10$

   - Soluzione: **a)** $x = 2 + 5k$ (infatti $2 \times 22 = 44$ e 44 diviso 5 ha resto 4), **b**) $x = 2$ (infatti $2 \times 2 = 4$ e $-11 \bmod 5 = 4$ **c)** $x = 3 + 10k$ (infatti $3 \times 7 = 21$ che diviso per 10 ha resto 1)

2. **Risolvere in numeri interi le seguenti equazioni: (3 punti)**

   **a)** $2x + 7y = 9$
   **b)** $3x - y = 11$

   - Soluzione: **a)** $\{x = 1 - 7N_1, y = 1 + 2N_1\}$ **b)** $\{x = N_1, y = -11 + 3N_1\}$,

3. **Trovare tutti i numeri interi che divisi sia per** 3 **sia per** 7 **danno resto** 2 **(4 punti)**

   - Soluzione:

   $$\begin{cases} x = 2 \bmod 3 \\ x = 2 \bmod 7 \end{cases}$$

   La prima relazione fornisce $x = 2 + 3N$, la seconda $x = 2 + 7M$ (con $N$ e $M$ interi i) per cui si ottiene $3N = 0 \bmod 7$ ovvero $N = 7k$ (con $k$ intero) , cioè $x = 2 + 21k$.

4. **Dimostrare che tutti i numeri della forma** $3n^6 + 4$ **divisi per** 7 **danno resto** 0 **oppure** 4 **(5 punti)**

   - Soluzione: bisogna dimostrare che

   $$3n^6 + 4 = 0 \bmod 7 \text{ oppure } 4 \bmod 7$$

Ci sono due casi da studiare:
**1) Se** $n$ **è multiplo di** 7 non c'è niente da dimostrare, il resto è ovviamente 4.
2) **Se** $n$ **non è divisibile per** 7 **.** Il piccolo teorema di Fermat ci dice in questo caso che $n^6 = 1 \bmod 7$ e quindi:

$$3n^6 + 4 = 7 \bmod 7 = 0 \bmod 7$$

5) **Risolvere, in campo complesso, l'equazione** $x^4 = -16$ **(4 punti)**

Soluzione: $-16 = 2^4(\cos\pi + i\sin\pi)$ per cui le **quattro** radici quarte di $-16$ sono:

$$\alpha_0 = 2\left(\cos\pi/4 + i\sin\pi/4\right) = \sqrt{2} + i\sqrt{2}$$
$$\alpha_1 = 2\left(\cos(\pi/4 + 2\pi/4) + i\sin(\pi/4 + 2\pi/4)\right) = i\sqrt{2} - \sqrt{2}$$
$$\alpha_2 = 2\left(\cos(\pi/4 + 4\pi/4) + i\sin(\pi/4 + 4\pi/4)\right) = -\sqrt{2} - i\sqrt{2}$$
$$\alpha_3 = 2\left(\cos(\pi/4 + 6\pi/4) + i\sin(\pi/4 + 6\pi/4)\right) = \sqrt{2} - i\sqrt{2}$$

6. **Dimostrare che la congruenza $x^2 = 2 \bmod 7$ è risolubile (4 punti)**

   - Soluzione: si deve studiare la risolubilità dell'equazione:

$$x^2 = 2 \bmod 7$$

Si applica il criterio di Gauss: $2^3 \bmod 7 = 1$ e quindi 2 è un residuo quadratico e la congruenza è risolubile. Le soluzioni sono $x = 3$ e $x = 4$.

7. **Nell'ambito della crittografia RSA , sapendo che $(n = 22, e = 7)$ è la chiave pubblica, e $y = 15$ il messaggio cifrato, trovare il messaggio in chiaro. (6 punti)**

   - Soluzione: se $n = 22 = 2 \times 11$,allora $\varphi(n) = (2-1) \times (11-1) = 10$, per cui se $e = 7$ è la chiave pubblica, $d = 1/7 \bmod 10 = 3$ è la chiave privata. Per cui il messaggio in chiaro è $15^3 \bmod 22 = 9$

8. **Calcolare $\sum_{n=0}^{100} u_n$ sapendo che $u_0 = 1$ e che $u_{n+1} + u_n = 0$, (3 punti)**

   - Soluzione: si può porre $u_n = u_0\alpha^n$ (dove $\alpha$ è la soluzione di $\alpha + 1 = 0$). Quindi:

$$\sum_{n=0}^{100} u_n = \sum_{n=0}^{100} (-1)^n = 1$$

9. **Risolvere la seguente relazione di ricorrenza: (4 punti)**

$$u_{n+2} + 2u_{n+1} + u_n = 0$$
$$u_0 = 1$$
$$u_1 = 1$$

   - Soluzione: l'equazione di secondo grado associata è $x^2 + 2x + 1 = 0$, con soluzioni reali e coincidenti.

$$\{\alpha = -1\}, \{\beta = -1\}$$

la soluzione generale è quindi: $u_n = (A + Bn)\alpha^n$. Le costanti $A$ e $B$ si ottengono da:

$$u_0 = A = 1$$
$$u_1 = -A - B = 1$$

Da cui: $A = 1$ e $B = -2$. In definitiva:

$$u_n = (-2n)(-1)^n + (-1)^n$$