Alcuni esercizi risolti di **MATEMATICA DISCRETA**
C.L. **Informatica e tecnologie per la produzione del software**
Informatica - Brindisi

1. Determinare il resto della divisione di 190^{597} per 17.

   Soluzione Bisogna "semplicemente" esprimere 190^{597} $(\texttt{mod}\ 17)$. Si osserva prima che
   $$190 \equiv 3 (\texttt{mod}\ 17).$$
   Inoltre, è noto che $a^{p-1} \equiv 1 (\texttt{mod}\ p)$, se $M.C.D.(a,p) = 1$. Quindi nel caso in esame
   $$3^{16} \equiv 1 (\texttt{mod}\ 17).$$
   Allora
   $$3^{597} = (3^{16})^{37} \cdot 3^5 \equiv 1^{37} \cdot 3^5 = 3^5 (\texttt{mod}\ 17).$$
   Si vede facilmente che $3^5 = 238 \equiv 5 (\texttt{mod}\ 17)$, e quindi il resto è 5.

2. Determinare le ultime due cifre del numero 523^{321}.

   Soluzione Si deve ridurre 523^{321} $(\texttt{mod}\ 100)$. Si osserva che
   $$523 \equiv 23 (\texttt{mod}\ 100)$$
   e quindi
   $$523^{321} \equiv 23^{321} (\texttt{mod}\ 100).$$
   Poichè $M.C.D.(23, 100) = 1$, si può usare il teorema di Eulero, secondo il quale
   $$23^{\varphi(100)} \equiv 1 (\texttt{mod}\ 100). \tag{1}$$
   Per le proprietà della funzione di Eulero si ha
   $$\varphi(100) = \varphi(5^2)\varphi(2^2) = (5^2 - 5) \cdot (2^2 - 2) = 20 \cdot 2 = 40$$
   pertanto (1) diventa
   $$23^{40} \equiv 1 (\texttt{mod}\ 100).$$
   D'altra parte $321 = 40 \cdot 8 + 1$ e quindi
   $$23^{321} = (23^{40})^8 \cdot 23 \equiv 1^8 \cdot 23 = 23 (\texttt{mod}\ 100)$$
   In conclusione $523^{321} \equiv 23 (\texttt{mod}\ 100)$.

3. Determinare le ultime 3 cifre del numero 173^{31}.

   Soluzione Per determinare le ultime 3 cifre del numero 173^{31}, bisogna ridurlo $(\texttt{mod}\ 1000)$. Si può osservare che $\varphi(1000) = 400$ e che l'esponente è $31 < 400$, per cui non si può usare il teorema di Eulero. Potrebbe essere conveniente trovare la quarta potenza di 173, in modo da avere:

$173^{31} = 173^{28+3} = 173^{28} \cdot 173^3 = (173^4)^7 \cdot 173^3 = (895.745.041)^7 \cdot 5.177.717.$

Ma $895.745.041 \equiv 41 (\mathtt{mod}\ 1000)$, $5.177.717 \equiv 717\ (\mathtt{mod}\ 1000)$ per cui, usando compatibilità delle congruenze $(\mathtt{mod}\ n)$ $(n \in \mathbb{N}^*)$ con il prodotto e la proprietà seguente:

$$\forall a, a', b \in \mathbb{Z},\ a \equiv a'\ (\mathtt{mod}\ n)\ \Rightarrow ab \equiv a'b\ (\mathtt{mod}\ n)$$

si ottiene $(895.745.041)^7 \cdot 5.177.717 \equiv (41)^7 \cdot 717\ (\mathtt{mod}\ 1000)$. D'altra parte, $41^6 = 4.750.104.241 \equiv 241\ (\mathtt{mod}\ 1000)$, per cui

$$173^{31} \equiv (41)^7 \cdot 717 \equiv 241 \cdot 41 \cdot 717\ (\mathtt{mod} 1000).$$

A questo punto, poichè $241 \cdot 41 \cdot 717 = 7.084.677 \equiv 677\ (\mathtt{mod}\ 1000)$, le ultime 3 cifre di 173^{31} sono 677. Si osservi che, naturalmente, si può procedere in modo diverso, per esempio partendo dalla terza potenza di 173; si consiglia di rifare l'esercizio seguendo questa strada.