ALGEBRA I: ESERCITAZIONE IN CLASSE del 12 Aprile 2011. Sketch delle soluzioni.

Esercizio 1.
Ieri abbiamo visto che il resto della divisione per 7 di 3^{302} è uguale a 2. Analogamente si può dimostrare che il resto della divisione per 5 e per 11 di 3^{302} è uguale a 4 e 9 rispettivamente.
Determinare il resto della divisione per 385 di 3^{302}. (Suggerimento: $385 = 5 \cdot 7 \cdot 11$...)
Soluzione.
Dobbiamo determinare la classe resto modulo 385 di 3^{302} Utilizzando l'isomorfismo $F : \mathbb{Z}_{385} \to \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$ ed il testo dell'esercizio capiamo che è equivalente determinare la soluzione x_0 del sistema cinese

$$\begin{cases} X \equiv 4 \mod 5 \\ X \equiv 3 \mod 7 \\ X \equiv 9 \mod 11 \end{cases}$$

con $0 \leq x_0 \leq 385$. Si risolve con il ben noto metodo e si trova $x_0 = 9$.

Esercizio 2.
(2.1) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbb{Z}_p : x^2 = 1\} = \{\pm\overline{1}\}$
(2.2) Sia $n = pq$ prodotto di due primi p, q entrambi maggiori di due. Determinare il numero di elementi in $\mathcal{U}(\mathbb{Z}_{pq})$ tali che $x^2 = \overline{1}$.
Soluzione.
(2.1) Sia x un intero. $x^2 \equiv 1(p) \Leftrightarrow x^2 - 1 \equiv 0(p) \Leftrightarrow (x-1)(x+1) \equiv 0(p)$. Ma p è primo, quindi p divide $(x-1)$ oppure p divide $(x+1)$ e quindi $x \equiv 1(p)$ oppure $x \equiv -1(p)$. Segue subito la tesi.
(2.2) Procedendo come sopra ed utilizzando l'isomorfismo $F : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$ vediamo che $x^2 \equiv 1(pq)$ se e solo se

$$\begin{cases} (x+1)(x-1) \equiv 0 \mod p \\ (x-1)(x+1) \equiv 0 \mod q \end{cases}$$

Applicando il ragionamento di (2.1) vediamo che le soluzioni di questo sistema sono l'unione delle soluzioni dei quattro sistemi

$$\begin{cases} (x+1) \equiv 0 \mod p \\ (x+1) \equiv 0 \mod q \end{cases}, \quad \begin{cases} (x+1) \equiv 0 \mod p \\ (x-1) \equiv 0 \mod q \end{cases}$$

$$\begin{cases} (x-1) \equiv 0 \mod p \\ (x-1) \equiv 0 \mod q \end{cases}, \quad \begin{cases} (x-1) \equiv 0 \mod p \\ (x+1) \equiv 0 \mod q \end{cases}$$

Gli elementi in $\mathcal{U}(\mathbb{Z}_{pq})$ tali che $x^2 = \overline{1}$ sono quindi quattro.

Esercizio 3.
Utilizzando l'esercizio precedente determinare gli elementi in $\mathcal{U}(\mathbb{Z}_{15})$ tali che $x^2 = \overline{1}$.
Soluzione.
Applichiamo (2.2) con $p = 3$, $q = 5$. Risolviamo i quattro sistemi e troviamo $\overline{x} = 14, \overline{x} = 11, \overline{x} = 1, \overline{x} = 4$.

Esercizio 4.
Calcolare le ultime due cifre del numero 123^{123}.
Soluzione.
Vedere `http://www.mat.uniroma1.it/ incitti/algebra/pdf/foglio6sol.pdf`, Esercizio 0.

Esercizio 5.
Un elemento a in un anello A è detto *nilpotente* se $\exists n \in \mathbb{N}$, $n > 0$, tale che $a^n = 0$.
(5.1) Sia A un anello commutativo. Verificare che la somma di due elementi nilpotenti è nilpotente.
(5.2) Determinare i nilpotenti di $\mathbb{Z}_{60}$. (Suggerimento $\overline{x}$ è nilpotente se e solo se x è multiplo di....).
Soluzione.
Vedere `http://www.mat.uniroma1.it/ incitti/algebra/pdf/foglio6sol.pdf`, Esercizio 3.

Esercizio 6.
Determinare il resto della divisione per 7 di $19^{19^{19}}$.

Soluzione.
Dobbiamo calcolare la classe resto modulo 7 di $19^{19^{19}}$. Ma 19 e 5 sono congrui modulo 7. Quindi dobbiamo calcolare $5^{19^{19}}$. Dato che $\phi(7) = 6$ vediamo che $5^6 \equiv 1(7)$. Ora, 19 è congruo a 1 modulo 6; quindi $19^{19} \equiv 1(6)$; esiste quindi N tale che $19^{19} = 1 + 6N$. Mettendo tutto insieme:

$$19^{19^{19}} \equiv 5^{19^{19}} \equiv 5^{1+6N} \equiv 5(5^6)^N \equiv 5 \bmod 7$$

.