A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
ESERCITAZIONI. FOGLIO 5.

Esercizio 5.1. Determinare le ultime tre cifre di $n = 13^{1625}$. (*Suggerimento. Sfruttare il Teorema di Eulero-Fermat*)

Esercizio 5.2. Risolvere il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 13\,X \equiv 2 \quad (mod\, 21) \\ 9\,X \equiv 3 \quad (mod\, 10) \\ 23\,X \equiv 12 \quad (mod\, 43) \end{cases}$$

Risolvere lo stesso sistema sostituendo alla prima equazione la seguente:

$$7\,X \equiv 2 \quad (mod\, 21)$$

Esercizio 5. 3. Stabilire per quali valori del parametro a il sistema è compatibile; per tali valori determinare la generica soluzione:

$$\begin{cases} 11\,X \equiv 4a \quad (mod\, 9) \\ 4\,X \equiv a \quad (mod\, 5) \\ 106\,X \equiv a+1 \quad (mod\, 26) \end{cases}$$

Esercizio 5.4. Determinare le soluzioni $(mod\, 315)$ del seguente sistema:

$$\begin{cases} 14\,X \equiv 21 \quad (mod\, 63) \\ 3\,X \equiv 4 \quad (mod\, 5) \end{cases}$$

Esercizio 5.5. Sia $\{a_1, ..., a_n\}$ una collezione di numeri interi:
(A) Mostrare che $(a_1 + \cdots + a_n)^3 \equiv a_1^3 + \cdots + a_n^3 \quad (mod\, 3)$;
(B) Trovare un'espressione modulo 4 per $(a_1 + \cdots + a_n)^4$ come funzione dei soli quadrati degli a_i.

Esercizio 5.6. [1] Sia φ la funzione di Eulero. Per ogni intero positivo n, sia $\omega(n)$ il numero dei fattori primi distinti di n. Dimostrare che:

$$\frac{\varphi(n)}{n} \geq \frac{1}{\omega(n)+1}$$

(*Suggerimento. Procedere per induzione su* $\omega(n)$. *Può essere utile ricordare che dati* m *interi distinti* $n_1, .., n_m$ *strettamente maggiori di* 1 *allora* $n_m \geq m+1$)

[1] Esercizio tratto da un compito del Prof. R. Dvornicich — Università di Pisa — A.A. 2005-2006.

ESERCIZI PER CASA

Esercizio 5.7. [2] Determinare le soluzioni di $x^{27} \equiv x^{15} \pmod{77}$. (*Suggerimento. Tradurre la precedente equazione in un sistema — sfruttare la scomposizione in primi di* 77 *— e risolverlo*)

Esercizio 5.8. [3] Siano $a, b, c \in \mathbb{N}^*$ e supponiamo che valgano le seguenti:

$$\begin{cases} a \equiv b \pmod{c} \\ b \equiv c \pmod{a} \\ c \equiv a \pmod{b} \end{cases}$$

(A) Cosa possiamo dedurre sugli MCD delle tre coppie?
(B) Quale relazione sussiste tra a, b e c?

[2] Esercizio tratto da un compito del Prof. R. Dvornicich — Università di Pisa — A.A. 2005-2006.
[3] Esercizio tratto da *A concrete introduction to Higher Algebra* di L. N. Childs