Tutorato 6 di Algebra 1 (AL110)

a cura di Andrea Cattaneo e Simone Mastrodonato

Università degli studi Roma Tre, Corso di Laurea in Matematica
Anno Accademico 2011/2012

Esercizio 1.

Sia p un numero primo e $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ l'insieme delle classi d'equivalenza della relazione congruenza modulo p.

(I) Si definisca l'indicatore di Eulero φ e si calcoli, motivando la risposta, $\varphi(p)$.

(II) Sia $[i]_p \in \mathbb{Z}_p$. Si calcoli:
$$\prod_{i=1}^{p-1} [i]_p;$$

(III) Si provi che $(p-2)! \equiv_p 1$;

(IV) Nel caso in cui p e' un primo ≥ 3 si dimostri:
$$(p-3)! \equiv_p \frac{p-1}{2}.$$

Esercizio 2.

Sia $\varphi(n)$ l'indicatore di Eulero calcolato in n.
Si provi che :

(I) $\varphi(n) = \frac{n}{2}$ se e solo se $n = 2^k$ per qualche $k \in \mathbb{N}$.

(II) Se ogni primo che divide n divide anche m allora:
$$\varphi(nm) = n\varphi(m);$$
e quindi per ogni $n \in \mathbb{N}$
$$\varphi(n^2) = n\varphi(n).$$

Esercizio 3.

Si risolvano, quando possibile, le seguenti equazioni congruenziali:

(I) $4x \equiv_{17} -3$;

(II) $29x + 12 \equiv_4 3$;

(III) $18x \equiv_{52} 27$.

Esercizio 4.

(I) Si diano delle condizioni sufficienti affinché un sistema di equazioni congruenziali lineare nella variabile X sia risolubile.

(II) Si discuta la risolubilità dei seguenti sistemi e, quando esistono, se ne determinino le soluzioni:

$$\begin{cases} x \equiv_5 2 \\ x \equiv_6 2 \\ x \equiv_4 0 \end{cases} \qquad \begin{cases} x \equiv_5 2 \\ x \equiv_6 2 \\ x \equiv_4 0 \end{cases} \qquad \begin{cases} 5x \equiv_{13} 27 \\ 4x \equiv_3 10 \\ 7x \equiv_{11} 23 \end{cases}$$

Esercizio 5.

(I) Sia p primo dispari. Si dimostri che $x^2 \equiv_p 1$ ha esattamente due soluzioni non congrue modulo p.

(II) Si dica quante e quali soluzioni non congrue modulo 35 ha $x^2 \equiv_{35} 1$.

Esercizio 6.

Provare che per ogni numero p tale che $n \leq p \leq 2n$ si ha:

$$\binom{2n}{n} \equiv_p 0 \qquad \text{e} \qquad \binom{2n}{n} \not\equiv_{p^2} 0$$