Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2006/2007
AL1 - Tutorato 9 (11 Dicembre 2006)

1. Mostrare che, se p è un numero primo, allora $\binom{p}{k} \equiv 0 \pmod{p}$ per $1 \leq k \leq p$.
2. Mostrare che, per ogni $n \in \mathbb{N}$,
$$\begin{cases} n^2 \equiv 0, 4 & \mod 8 \quad \text{se } n \text{ è pari} \\ n^2 \equiv 1 & \mod 8 \quad \text{se } n \text{ è dispari} \end{cases}$$
3. Stabilire quanti sono gli elementi invertibili di $\mathbb{Z}_n$ per $n = 30, 75, 187, 3969$.
4. Mostrare che se la congruenza lineare $aX \equiv b \mod n$ è risolubile, allora $d := MCD(a, n)$ divide b.
5. Stabilire se le seguenti equazioni lineari in due indeterminate hanno soluzioni intere e, in caso affermativo, determinare tali soluzioni:
$$3X + 5Y = 1; \quad 10X + 2Y = 15; \quad 10X + 55Y = 4115.$$
6. Mostrare che, se $a \equiv b \mod n$ e $a \equiv b \mod m$, allora
$$a \equiv b \mod mcm(m, n).$$
7. Siano p, q due primi distinti. Mostrare che, se $a^p \equiv a \mod q$ e $a^q \equiv a \mod p$, allora
$$a^{pq} \equiv a \mod pq.$$
8. Mostrare che, se $MCD(m, n) = 1$, una soluzione del sistema
$$\begin{cases} X \equiv a & \mod m \\ X \equiv b & \mod n \end{cases}$$
è $x = an^{\varphi(m)} + bm^{\varphi(n)}$, dove φ è la funzione di Eulero. Determinare una simile formula per il caso di più equazioni.
9. Mostrare che, se $MCD(m, n) = 1$, la corrispondenza
$$\mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_{mn}; \quad ([a]_m, [b]_n) \mapsto [an^{\varphi(m)} + bm^{\varphi(n)}]_{mn}$$
è una corrispondenza biunivoca.
10. Mostrare che se $d_i := MCD(a_i, n_i)$ divide b_i, $i = 1, \ldots, s$, il sistema di congruenze lineari
$$\begin{cases} a_1 X \equiv b_1 & \mod n_1 \\ \ldots & \\ a_s X \equiv b_s & \mod n_s \end{cases}$$
ha esattamente $d_1 d_2 \ldots d_s$ soluzioni distinte $\mod n_1 n_2 \ldots n_s$.
11. Risolvere i seguenti sistemi di congruenze lineari:
$$\begin{cases} 20X \equiv 6 & \mod 42 \\ 18X \equiv 3 & \mod 33 \end{cases} \qquad \begin{cases} 6X \equiv 4 & \mod 14 \\ 10X \equiv 15 & \mod 65 \\ 8X \equiv 10 & \mod 34 \end{cases}$$