Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
TN410 - Introduzione alla teoria dei numeri
Tutorato 3 (31 marzo 2011)
Giacomo Milizia

1. Trovare le soluzioni di ciascuno dei seguenti sistemi di congruenze lineari:

$$\begin{cases} 8X + 5Y \equiv 3 \pmod{13} \\ 3X + 7Y \equiv 6 \pmod{13} \end{cases}$$

$$\begin{cases} 3X + 2Y \equiv 2 \pmod{7} \\ X + 6Y \equiv 5 \pmod{7} \end{cases}$$

2. Studiare la risolubilità del seguente sistema di congruenze lineari al variare del parametro λ:

$$\begin{cases} Y + \lambda Z \equiv \lambda + 1 \pmod{5} \\ X + Y + Z \equiv 2 \pmod{5} \\ \lambda X + Y \equiv \lambda + 1 \pmod{5} \end{cases}$$

3. Risolvere il seguente sistema di congruenze lineari:

$$\begin{cases} 2X + 3Y + 6Z \equiv -1 \pmod{7} \\ 2X - Y \equiv -3 \pmod{7} \end{cases}$$

4. Provare che $\varphi(n) = \frac{n}{2}$ se e soltanto se $n = 2^k$ per qualche $k \geqslant 1$.

5. Provare che se ogni numero primo che divide n divide anche m, allora

$$\varphi(nm) = n\varphi(m);$$

in particolare per ogni intero positivo n si ha:

$$\varphi(n^2) = n\varphi(n).$$

6. Trovare gli ordini degli elementi di U_{21} e di U_{24}.

7. Verificare che 2 è una radice primitiva modulo 13; trovare tutte le radici primitive modulo 13.

8. Verificare che 2 è una radice primitiva modulo 25.

9. Trovare tutte le radici primitive modulo n per $n = 29$ e 31.

10. Sapendo che 2 è una radice primitiva modulo 37, trovare:
    (a) tutti gli interi positivi minori di 37 di ordine 9 modulo 37;
    (b) tutti gli interi positivi minori di 43 di ordine 18 modulo 37.

11. Sia p un numero primo dispari. Sia r una radice primitiva modulo p. Provare che:
    (a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
    (b) Se r' è un'altra radice primitiva modulo p, allora rr' non è una radice primitiva modulo p.
    (c) Se r' è un numero intero tale che $rr' \equiv 1 \pmod{p}$, allora r' è una radice primitiva modulo p.

12. Provare che se $p > 3$ è un numero primo, allora le radici primitive mod p si possono raggruppare in coppie r, r' tali che $rr' \equiv 1 \pmod{p}$.

13. Sia r una radice primitiva modulo un numero primo dispari p. Provare che:
    (a) Se $p \equiv 1 \pmod{4}$, allora anche $-r$ è una radice primitiva modulo p.
    (b) Se $p \equiv 3 \pmod{4}$, allora $-r$ ha ordine $\frac{p-1}{2}$ modulo p.