Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
TN1 - Introduzione alla teoria dei numeri
Tutorato 1 (5 marzo 2009)
Giacomo Milizia

1. Provare che se p è un numero primo maggiore di 3 tale che $p + 2$ è un numero primo, allora 12 divide $p + (p + 2)$.

   (Sugg. $12 = 2^2 \cdot 3$)

2. Provare che se 2 non divide n e 3 non divide n, allora 24 divide $n^2 + 23$.

3. Provare che 3 è l'unico numero primo p tale che anche $p^2 + 2$ è primo.

4. (a) Verificare che l'insieme $\{0, 1, 2, 2^2, 2^3, \cdots, 2^9\}$ è un sistema completo di residui modulo 11.

   (b) Stabilire se l'insieme $\{0, 1^2, 2^2, 3^2, \cdots, 10^2\}$ è un sistema completo di residui modulo 11.

   (c) Stabilire se l'insieme $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ è un sistema ridotto di residui modulo 7.

5. Utilizzando il principio di induzione matematica, provare che se m è un intero positivo, allora:

   (a) $4^m \equiv 1 + 3m \pmod 9$;

   (b) $5^m \equiv 1 + 4m \pmod{16}$.

6. Sia p un numero primo.
   Provare che un numero intero a è un inverso aritmetico di se stesso se e solo se $a \equiv 1 \pmod p$ oppure $a \equiv p - 1 \pmod p$.

7. (a) Provare che se m è un intero dispari, allora $m^2 \equiv 1 \pmod 8$. Dedurne che la somma dei quadrati di tre numeri interi non è mai congruente a 7 (mod 8).

   (b) Provare che l'equazione $X^2 + Y^2 - 15Z^2 = 7$ non ha soluzioni intere.

8. Provare che le seguenti equazioni diofantee non hanno soluzioni intere:

   (a) $X^3 - X + 1 = 0$

   (b) $X^3 + X^2 - X + 1 = 0$

   (c) $X^3 + X^2 - X + 3 = 0$.

9. Per ciascuna delle seguenti equazioni diofantee lineari, stabilire la risolubilità e nei casi positivi determinare tutte le soluzioni:

   (a) $2X + 7Y = 3$
   (b) $5X - 4Y = 7$
   (c) $4X + 2Y = 1001$
   (d) $58X - 134Y = 10$.

10. Determinare tutte le eventuali soluzioni incongruenti delle seguenti congruenze lineari:

    (a) $5X \equiv 4 \pmod{16}$;
    (b) $6X \equiv 11 \pmod{9}$;
    (c) $20X \equiv 0 \pmod{60}$;
    (d) $8X \equiv 24 \pmod{28}$;
    (e) $10X \equiv 25 \pmod{45}$.

11. Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze lineari:

$$\begin{cases} 4X \equiv 5 & \pmod{9} \\ 6X \equiv 10 & \pmod{13} \\ 7X \equiv 6 & \pmod{10} \end{cases}$$

$$\begin{cases} 2X \equiv 4 & \pmod{5} \\ 10X \equiv 6 & \pmod{7} \\ 11X \equiv 14 & \pmod{16} \\ 3X \equiv 3 & \pmod{9} \end{cases}$$

12. Provare che il sistema di congruenze lineari

$$\begin{cases} X \equiv 5 & \pmod{6} \\ X \equiv 7 & \pmod{15} \end{cases}$$

    non possiede soluzioni.

13. Provare che il sistema di congruenze lineari

$$\begin{cases} X \equiv a & \pmod{n} \\ X \equiv b & \pmod{m} \end{cases}$$

    ammette una soluzione se e solo se $\mathrm{MCD}(n, m) \mid a - b$. Se una soluzione esiste, verificare che essa è unica modulo $\mathrm{mcm}(n, m)$.

14. Trovare il più piccolo intero $a > 2$ tale che

$$2 \mid a, \quad 3 \mid a+1, \quad 4 \mid a+2, \quad 5 \mid a+3, \quad 6 \mid a+4.$$