Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2007/2008
TN1 - Introduzione alla teoria dei numeri
Tutorato 1 (29 febbraio 2007)
Micaela De Santis

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. $12 = 2^2 3$)

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

3. (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.

4. Siano $a, r \in \mathbb{Z}$, con $r \neq 1$; provare che per ogni intero positivo n si ha che:
$$a + ar + \cdots + ar^n = \frac{a(r^{n+1}-1)}{r-1}$$
   Un intero $n > 1$ si dice *perfetto* se n è uguale alla somma di tutti i suoi divisori positivi diversi da se stesso.
   (a) Provare che nessuna potenza di un numero primo è un numero perfetto.
   (b) Provare che se $2^k - 1$ è un numero primo con $k \in \mathbb{Z}$, $k \geqslant 2$, allora
      i. k è un numero primo;
      ii. $2^{k-1}(2^k-1)$ è un numero perfetto;
      (Sugg. : per ogni $n \geqslant 1$, $b^n - 1 = (b-1)(b^{n-1}+b^{n-2}+\cdots+b+1)$)
      iii. Provare che se $2^h + 1$ con $h \in \mathbb{Z}$, $h \geqslant 1$, è un numero primo, allora h è una potenza di 2.
      (Sugg.: sia $h = 2^l m$ con m dispari; inoltre il polinomio $X^m + 1 \in \mathbb{Z}[X]$ha come radice -1)

5. (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.

6. Provare che l'equazione diofantea
$$7Y^2 - 2 = X^2$$
   non ha soluzioni.

7. Determinare tutte le eventuali soluzioni incongruenti delle seguenti congruenze lineari:
   (a) $X \equiv 1 \pmod 8$;
   (b) $6X \equiv 12 \pmod 9$;
   (c) $20X \equiv 0 \pmod{100}$;
   (d) $10X \equiv 24 \pmod{45}$;
   (e) $10X \equiv 325 \pmod{4115}$.

8. Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze lineari:
$$\begin{cases} 5X \equiv 7 \pmod 9 \\ 9X \equiv 8 \pmod{13} \\ 11X \equiv 15 \pmod{20} \end{cases}$$
$$\begin{cases} 2X \equiv 4 \pmod 5 \\ 10X \equiv 6 \pmod 7 \\ 11X \equiv 14 \pmod{16} \\ 3X \equiv 6 \pmod 9 \end{cases}$$

9. Provare che il sistema di congruenze lineari
$$\begin{cases} X \equiv 5 \pmod 6 \\ X \equiv 7 \pmod{15} \end{cases}$$
non possiede soluzioni.

10. 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 $\mathrm{mcm}(n, m)$.

11. Trovare il più piccolo intero $a > 2$ tale che
$$2 \mid a, \quad 3 \mid a + 1, \quad 4 \mid a + 2, \quad 5 \mid a + 3, \quad 6 \mid a + 4.$$

12. Utilizzando il teorema di Wilson, provare che per ogni numero primo dispari p si ha che:
$$1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$
Sugg. : $k \equiv -(p-k)) \pmod p$

13. Calcolare le seguenti potenze:
$$6^{15} \pmod{13}; \qquad 7^{67} \pmod{45}; \qquad 128^{10} \pmod{33}.$$