Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2012/2013
AL110 - Algebra 1
Tutorato 6 (8 novembre 2012)

1. Verificare che valgono le seguenti congruenze:

$$22 \equiv -6 \pmod 7; \quad 315 \equiv 23 \pmod 4; \quad 403 \equiv -17 \pmod{10}$$

$$-3 \equiv 74 \pmod{11}; \quad 143 \equiv 0 \pmod{13}; \quad 243 \equiv 63 \pmod{15}$$

2. Per ciascuna delle seguenti classi resto modulo n, $[x]_n$, determinare un rappresentante x' tale che $0 \leq x' \leq n-1$:

   $[-432]_{48}$, $[5678]_{107}$, $[-456]_{35}$, $[209]_{11}$, $[2109]_{12}$, $[2109]_{37}$.

3. Stabilire per quali numeri naturali $n \geqslant 2$ valgono le seguenti congruenze:

$$27 \equiv 5 \pmod n; \quad 1000 \equiv 1 \pmod n; \quad 1331 \equiv 0 \pmod n$$

4. Stabilire quali dei seguenti elementi di $\mathbb{Z}_n$ sono invertibili; per ciascuno degli elementi invertibili trovare l'inverso:

   (a) $[-45]_{12}$, $[29]_{12}$, $[52]_{12}$, $[-30]_{12}$, $[19]_{12}$;

   (b) $[-22]_{18}$, $[41]_{18}$, $[25]_{18}$, $[-47s]_{18}$, $[28]_{18}$.

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

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

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

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

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

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

9. 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 $a \equiv p-1 \pmod p$.

10. Provare che se a è un numero intero pari, allora $a^2 \equiv 0 \pmod 4$ e che se a è un numero intero dispari, allora $a^2 \equiv 1 \pmod 4$.

11. Dimostrare che se a è un numero intero tale $a^2 \equiv 3 \pmod 4$, allora a non può essere la somma dei quadrati di due interi.

12. Provare che:

    (a) se a è un intero pari, allora $a^2 \equiv 0, 4 \pmod 8$;

(b) se a è un intero dispari, allora $a^2 \equiv 1 \pmod 8$.

(c) Dedurne che la somma dei quadrati di tre numeri interi non è mai congrua a 7 (mod 8).

13. Utilizzando il principio di induzione si dimostri se a è un intero *dispari*, allora per ogni $n \geq 1$ si ha che:

$$a^{2^n} \equiv 1 \qquad \bmod\ 2^{n+2}.$$

14. Provare che:

    (a) per ogni numero intero a, si ha che $a^3 \equiv 0, 1, 8 \pmod 9$;

    (b) per ogni numero intero a, si ha che $a^3 \equiv a \pmod 6$.

15. Sia $n \in \mathbb{N}$, $n \geqslant 2$, siano $a,\ b \in \mathbb{Z}$ tali che $a \equiv b \pmod n$. Provare che $\mathrm{MCD}(a, n) = \mathrm{MCD}(b, n)$.

16. Sia $n \in \mathbb{N}$, $n \geqslant 2$, siano $a,\ b$ numeri interi tali che $\mathrm{MCD}(a, n) = 1$. Provare che se $a^k \equiv b^k \pmod n$ e $a^{k+1} \equiv b^{k+1} \pmod n$ con k intero positivo, allora $a \equiv b \pmod n$. Se si toglie l'ipotesi che $\mathrm{MCD}(a, n) = 1$, è ancora vero che $a \equiv b \pmod n$?