Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2003/2004
ALGEBRA 1 - Prof. M. Fontana
Tutorato 7 – 18 novembre 2003

1. (a) Sia p un numero primo, allora mostrare che:

$$(p-1)! + 1 \equiv 0 \pmod{p}$$ (**Teorema di Wilson**).

(b) Sia $n \geq 2$. Mostrare che:

$$n \text{ è primo} \Leftrightarrow (n-1)! + 1 \equiv 0 \pmod{n}.$$

2. Risolvere i seguenti sistemi di congruenze:

(a) $X \equiv 1 \pmod 3$, $X \equiv 2 \pmod 5$, $X \equiv 3 \pmod 7$

(b) $X \equiv 5 \pmod 6$, $X \equiv 2 \pmod 5$, $X \equiv 1 \pmod{11}$

3. Risolvere i seguenti sistemi di congruenze:

(a) $3X \equiv 1 \pmod{10}$, $4X \equiv 2 \pmod 7$

(b) $3X \equiv 2 \pmod 4$, $2X \equiv 7 \pmod{15}$, $4X \equiv 6 \pmod 7$

4. Si chiama **sistema completo di residui** (mod n) un insieme $S \subset \mathbf{Z}$ tale che ogni $a \in \mathbf{Z}$ è congruo (mod n) ad uno ed un solo elemento di S.

Ad esempio, $S = \{0, 1, \dots, n-1\}$ è un sistema completo di residui (mod n).

Mostrare che:

(a) $S := \{r_1, \dots, r_n\}$è un sistema completo di residui (mod n), se e soltanto se:

$$Z / \equiv_n = \{[r_1]_n, \dots, [r_n]_n\};$$

(b) se $S := \{r_1, \dots, r_n\}$è un sistema completo di residui (mod n), presi comunque $a, b \in \mathbf{Z}$ con MCD(a,n) = 1, allora:

$$S' := \{a r_1 + b, \dots, a r_n + b\}$$

è ancora un sistema completo di residui (mod n);

(c) se $S := \{x_1, \dots, x_n\}$ (risp., $T := \{y_1, \dots, y_m\}$) è un sistema completo di residui (mod n), (risp., (mod m)) e se MCD(n, m) = 1, allora

$$\{m x_i + n y_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

è un sistema completo di residui (mod nm);

(d) se $n > m > 1$, con MCD(n, m) = 1, sia:

$r_1 := n$, $r_2 := n - m$, e, per induzione,

$$r_{k+1} := \begin{cases} r_k - m, & \text{se } r_k \geq m \\ r_k + n, & \text{se } r_k < m \end{cases}$$

per $k \geq 2$, allora $\{r_1, r_2, \dots, r_{n+m}\}$ è un sistema completo di residui (mod n + m).

5. (a) Verificare se $\{1, 23, 38, -17, 12, -204, 35\}$ forma un sistema completo di residui (mod 7).

(b) Dati $S := \{1, -3, 8, -1, -20\}$, sistema completo di residui (mod 5), e $T := \{-5, 8, -18\}$, sistema completo di residui (mod 3), determinare un sistema completo di residui (mod 15), utilizzando la tecnica dell'esercizio 4(c).

(c) Sia n = 7, m = 5, determinare un sistema completo di residui (mod 12) utilizzando la tecnica dell'esercizio 4(d).

6. Si chiama **sistema ridotto di residui** (mod n) un insieme $S^* \subset \mathbf{Z}$ tale che, per ogni $a \in \mathbf{Z}$ con MCD(a, n) = 1, esiste uno ed un solo elemento di S^* congruo ad a (mod n). Ad esempio, $S^* := \{k : 1 \leq k \leq n-1$ con MCD(k, n) = 1$\}$ è un sistema ridotto di residui (mod n).

Mostrare che:

(a) $S^* := \{k_1, \dots, k_t\}$ è un sistema ridotto di residui (mod n) se e soltanto se $\{[k_1]_n, \dots, [k_t]_n\}$ coincide con il sottoinsieme di $Z/\equiv_n$ formato dagli elementi invertibili;

(b) Se si denota con $\varphi(n)$ il **numero di elementi dell'insieme degli invertibili di $Z/\equiv n$,** allora per ogni sistema ridotto di residui (mod n) S^*, si ha: $\text{Card}(S^*) = \varphi(n)$;
inoltre, se MCD(n, m) = 1, allora: $\varphi(nm) = \varphi(n)\,\varphi(m)$;

(c) se $S^* := \{k_1, \dots, k_{\varphi(n)}\}$ è un sistema ridotto di residui (mod n) e se $a \in \mathbf{Z}$ con MCD(a, n) = 1, allora $\{a k_1, \dots, a k_{\varphi(n)}\}$ è ancora un sistema ridotto di residui (mod n);

(d) con le stesse notazioni del punto (c), se $b \in \mathbf{Z}$ allora non è vero, in generale, che $\{k_1 + b, \dots, k_{\varphi(n)} + b\}$ sia un sistema ridotto di residui (mod n) (dare un esempio);

(e) se $S^* := \{k_1, \dots, k_{\varphi(n)}\}$ è un sistema ridotto di residui (mod n) e $T^* := \{k_1, \dots, k_{\varphi(m)}\}$ è un sistema ridotto di residui (mod m), con MCD(n, m) = 1, allora: $\{m ki + n hj : 1 \leq i \leq \varphi(n), 1 \leq j \leq \varphi(m)\}$ è un sistema ridotto di residui (mod nm).

7. (a) Per n = 2, 3, 4, 5, 6, 10, determinare il sottoinsieme S^* di $S = \{0, 1, \dots, n-1\}$ che forma un sistema ridotto di residui (mod n).

(b) Noti un sistema ridotto di residui (mod 3) ed uno (mod 7), determinare un sistema ridotto di residui (mod 21), utilizzando l'esercizio 6(e).