Proposizione 1. *Sia $n \in \mathbb{N} - \{0,1\}$. La relazione $\mathcal{R}_n = \{(a,b) \in \mathbb{Z} \times Z : n \mid a-b\}$ è una relazione di equivalenza su $\mathbb{Z}$.*

La dimostrazione viene lasciata per esercizio.

Definizione 1. La relazione di equivalenza $\mathcal{R}_n$ si dice *congruenza modulo n*.

Notazione Per ogni $a, b \in \mathbb{Z}$, invece che $(a,b) \in \mathcal{R}_n$ si scrive

$$a \equiv b \ (\mathtt{mod} n)$$

e si legge "a congruo b modulo n".

Teorema 1. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ ha esattamente n elementi, cioè:

$$\mathbb{Z}/\mathcal{R}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

dove $[x]_n$ indica la classe di equivalenza di $x \in \mathbb{Z}$.

Dimostrazione. Si dimostra prima che le classi di equivalenza $[0]_n, [1]_n, \ldots, [n-1]_n$ sono distinte fra loro. Siano $a, b \in \mathbb{N}$, con $a \neq b$, $0 \leq a \leq n-1$, $0 \leq b \leq n-1$, e si può supporre che sia $a < b$. Se fosse $[a]_n = [b]_n$ allora sarebbe $b \equiv a \ (\mathtt{mod} n)$ cioè $n \mid b-a$. Però $b - a \leq n-1$ e quindi n potrebbe essere un divisore di $b-a$ solo se $b-a = 0$, il che contraddice l'ipotesi $a \neq b$.
Resta da provare che non ci sono classi di equivalenza diverse da $[0]_n, [1]_n, \ldots, [n-1]_n$ in $\mathbb{Z}/\mathcal{R}_n$. A tale scopo, sia $m \in \mathbb{Z}$. Per il teorema sulla divisione, esistono $q, r \in \mathbb{Z}$, con $0 \leq r < n$ tali che $m = nq + r$. Allora $m - r = nq$, per cui $n \mid m - r$, ovvero $m \equiv r \ (\mathtt{mod} n)$ e quindi $[m]_n = [r]_n$. Segue che:

$$\forall [m]_n \in \mathbb{Z}/\mathcal{R}_n \ \exists r \in \mathbb{N}, \text{ con } 0 \leq r \leq n-1 \text{ tale che } [m]_n = [r]_n$$

e ciò conclude la dimostrazione.

Definizione 2. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ si chiama *insieme dei resti modulo n* e si indica con il simbolo $\mathbb{Z}_n$.

Definizione 3. Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0,1\}$. Si dice *congruenza lineare* l'espressione

$$ax \equiv b \ (\mathtt{mod}\ n). \tag{1}$$

Si dice soluzione di (1) ogni intero x_0 tale che $ax_0 \equiv b \ (\mathtt{mod}\ n)$.

Teorema 2. *Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0,1\}$ e sia $d = M.C.D.(a,n)$. Allora*

1. *la congruenza lineare (1) ammette soluzioni se e solo se $d \mid b$.*
2. *se x_0 è una soluzione di (1), posto $\bar{n} = \frac{n}{d}$, tutte le altre soluzioni di (1) sono $x_0 + k\bar{n}$, al variare di $k \in \mathbb{Z}$*
3. *ci sono esattamente d soluzioni non congrue tra loro $\mathtt{mod}\ n$, cioè $x_0, x_0+\bar{n}, \ldots, x_0+(d-1)\bar{n}$.*

Dimostrazione. Per provare 1., si osserva che, affermare che la congruenza lineare (1) ha soluzioni equivale a dire che esiste $x_0 \in \mathbb{Z}$ tale che

$$n \mid ax_0 - b,$$

ovvero che esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0 - b = ny_0,$$

ossia

$$ax_0 + n(-y_0) = b. \tag{2}$$

Questo vuol dire che l'equazione diofantea $ax + ny = b$ ammette soluzione $(x_0, -y_0)$. Dal teorema sulle equazioni diofantee è noto che 2 ha soluzioni se e solo se $M.C.M.(a,n)|b$.

Anche la 2. segue subito dal teorema sulle equazioni diofantee. La dimostrazione della 3. si tralascia.