Congruencias módulo n.

Sobre $\mathbb{Z}$ definimos la siguiente relación: tomando un $n \in \mathbb{N}$ fijo.
$\forall\, a,b \in \mathbb{Z}$, decimos que:

$$a \equiv b \bmod n \iff n \mid a-b$$

Ya se probó que $\equiv \bmod n$ es una relación de equivalencia, por lo cual las clases de equivalencia inducen una partición en $\mathbb{Z}$.
Si $a \in \mathbb{Z}$:

$$[a] := \bar{a} = \{ b \in \mathbb{Z} \mid a \equiv b \bmod n \} = a + n\mathbb{Z}$$

donde $n\mathbb{Z} = \{ nq \mid q \in \mathbb{Z} \}$ y $a + n\mathbb{Z} = \{ a + nq \mid q \in \mathbb{Z} \}$, la igualdad se da, pues:

$$b \in [a] \iff a \equiv b \bmod n \iff n \mid a-b \iff n \mid b-a \iff \exists!\, q \in \mathbb{Z} \ \text{m}\ nq = b-a$$
$$\iff \exists!\, q \in \mathbb{Z} \ \text{m}\ b = a + nq$$

Luego $[a] = a + n\mathbb{Z}$.
Denotamos al conjunto cociente de clases de equivalencia bajo la congruencia módulo n, como $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, i.e:

$$\mathbb{Z}/n\mathbb{Z} = \{ a + n\mathbb{Z} \mid a \in \mathbb{Z} \}$$

Si $a \in \mathbb{Z}$, por el algoritmo de la división, $\exists!\ q, r \in \mathbb{Z}$ m

$$a = nq + r,\ 0 \leq r < n$$

luego:

$$a - r = nq \Rightarrow n \mid a-r \Rightarrow a \equiv r \bmod n$$

por tanto: $[a] = [r]$, donde $0 \leq r < n$, así:

$$\mathbb{Z}/n\mathbb{Z} = \{ n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, n-1 + n\mathbb{Z} \}$$

y cada clase es diferente, en efecto: si $0 \leq i < j < n$, entonces

$$i \not\equiv j \bmod n,\ \text{pues de otra forma, si}$$

$$
\begin{aligned}
i \equiv j \bmod n &\Rightarrow n \mid j-i \\
&\Rightarrow \exists\ q \in \mathbb{Z} \ \text{m}\ nq = j-i \\
&\Rightarrow q \in \mathbb{Z}^{+},\ \text{pues } j-i > 0 \\
&\Rightarrow j-i = nq > 0 \\
&\Rightarrow j-i = nq > n \\
&\Rightarrow j-i > n \ \#_c
\end{aligned}
$$

luego, $i \not\equiv j \bmod n \Rightarrow i+n\mathbb{Z} \neq j+n\mathbb{Z}$. En resumen:

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

Con todo lo anterior, definimos una suma y un producto en $\mathbb{Z}/n\mathbb{Z}$:

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad y \quad \cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

$$[a]+[b] \longmapsto [a+b] \qquad\qquad [a]\cdot[b] \longmapsto [ab]$$

$\forall\ a,b \in \mathbb{Z}$. Con la definición anterior, tenemos problemas, pues las definicion es dependen del representante de clase, pues puede que $a \neq a'$, $b \neq b'$ y $[a] = [a']$ y $[b]=[b']$, veremos que en tal caso: $[a]+[b] = [a']+[b']$, y $[a]\cdot[b] = [a']\cdot[b']$. En efecto, probaremos que $+$ y $\cdot$ son funciones:

Sean $a,b \in \mathbb{Z}$ y $a' \in [a]$, $b' \in [b]$. Entonces:

$$a' = a + nq_1 \quad y \quad b' = b + nq_2$$

$$\Rightarrow a'+b' = a+b+nq_1+nq_2 \quad y \quad a'b' = ab + naq_2 + nbq_1 + n^2q_1q_2$$

$$\Rightarrow a'+b' = a+b+n(q_1+q_2), \quad y \quad a'b' = ab + n(aq_2+bq_1+nq_1q_2)$$

$\Rightarrow a'+b' \in [a+b]$, y $a'b' \in [ab]$, luego

$$[a'+b'] = [a+b], \ y \quad [a'b'] = [ab]$$

por tanto, $+$ y $\cdot$ están bien definidas, i.e, son funciones.

Con lo anterior, tenemos que $\mathbb{Z}/n\mathbb{Z}$ con $+$ es un grupo abeliano finito de orden n, con elemento identidad $[0]$, y $\forall\ [a] \in \mathbb{Z}/n\mathbb{Z}\ \exists\ -[a] = [-a]$ tal que:

$$[a]+(-[a])=[0]$$

En efecto:

Claramente, por lo que se probó anteriormente, $|\mathbb{Z}/n\mathbb{Z}|=n$, además:

(i) Sean $[a],[b]$ y $[c]\in\mathbb{Z}/n\mathbb{Z}$, entonces:

$$[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]=[(a+b)+c]=[a+b]+[c]$$
$$=([a]+[b])+[c]$$

(ii) $\exists\ [0]\in\mathbb{Z}/n\mathbb{Z}$ tal que, $\forall\ [a]\in\mathbb{Z}/n\mathbb{Z}$:

$$[a]+[0]=[a+0]=[0+a]=[0]+[a]=[0+a]=[a]$$

luego, $[0]$ es el elemento identidad.

(iii) $\forall\ [a]\in\mathbb{Z}/n\mathbb{Z}\ \ \exists -[a]=[-a]$ tal que

$$[a]+(-[a])=[a]+[-a]=[a-a]=[0]=[-a+a]=[-a]+[a]=(-[a])+[a]$$

(iv) $\forall\ [a],[b]\in\mathbb{Z}/n\mathbb{Z}$:

$$[a]+[b]=[a+b]=[b+a]=[b]+[a]$$

Por (i)-(iv), $\mathbb{Z}/n\mathbb{Z}$ es un grupo conmutativo de orden n.

q.e.d

$(\mathbb{Z}/n\mathbb{Z},\cdot)$ es un monoide abeliano, donde $e=[1]$, con $n\geqslant 2$, pues si $n=1$: $[0]=[1]$, este no es un grupo, pues $[0]$ no es invertible. Para que sea grupo, hacemos lo siguiente:

Def. Definimos

$$\mathbb{Z}/n\mathbb{Z}^*=\{[m]\in\mathbb{Z}/n\mathbb{Z}\mid (m,n)=1\}$$

Probaremos que $(\mathbb{Z}/n\mathbb{Z}^*,\cdot)$ es un grupo, en efecto:

a) $\cdot|_{\mathbb{Z}/n\mathbb{Z}^*\times\mathbb{Z}/n\mathbb{Z}^*}$ es cerrada en $\mathbb{Z}/n\mathbb{Z}^*$, en efecto, sean $[a],[b]\in\mathbb{Z}/n\mathbb{Z}^*$, entonces:

$1 \leqslant a, b < n$, y con $(a,n) = 1 = (b,n)$, se sigue que $(ab,n) = 1$. Si $ab < n$, entonces $[ab] = [a]\cdot[b] \in \mathbb{Z}/n\mathbb{Z}^*$, si $n \leqslant ab$, por el algoritmo de la división $\exists!\ q, r \in \mathbb{Z}$ ∍

$$ab = nq + r,\ 0 \leqslant r < n$$

Claramente $[ab] = [r]$, y $(r,n) = 1$. Suponga que $(r,n) = d$, $d > 1$, luego $\exists$ p primo tal que $p \mid n$ y $p \mid r$, luego $p \mid ab$ y $p \mid n \Rightarrow p \mid (ab,n) = 1 \Rightarrow p \mid 1$ #c luego $(r,n) = 1$, así $[r] \in \mathbb{Z}/n\mathbb{Z}^*$, y $[ab] = [r]$, por tanto $\cdot$ es cerrada en $\mathbb{Z}/n\mathbb{Z}^*$.

De momento, $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ es un monoide abeliano. Probaremos que éste es un grupo.

Sea $[m] \in \mathbb{Z}/n\mathbb{Z}^*$, entonces $1 \leqslant m < n$ y $(m,n) = 1$. Como $(m,n) = 1$, entonces $\exists!\ s, t \in \mathbb{Z}$ ∍ $ms + nt = 1 \Rightarrow nt = 1 - ms \Rightarrow n \mid 1 - ms \Rightarrow 1 \equiv ms \bmod n$, así $[ms] = [1]$. Como $ms + nt = 1$, entonces $(s,n) = 1$.

Ahora, por el algoritmo de la división $\exists!\ q, r \in \mathbb{Z}$ ∍

$$\begin{aligned} s &= nq + r,\ 0 \leqslant r < n \\ &\Rightarrow s - r = nq \\ &\Rightarrow s \equiv r \bmod n \\ &\Rightarrow [s] = [r] \end{aligned}$$

Claramente $(r,n) = 1$, como $0 \leqslant r < n$ se sigue que $[r] \in \mathbb{Z}/n\mathbb{Z}^*$. Por tanto para $[m]$ $\exists\ [m]^{-1} = [r]$ tal que:

$$[r][m] = [m][r] = [m][s] = [ms] = [1]$$

Luego $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ es un grupo abeliano multiplicativo.

q.e.d

Se denota a la cantidad de elementos de $\mathbb{Z}/n\mathbb{Z}^*$ como $\varphi(n)$, i.e:

$$|\mathbb{Z}/n\mathbb{Z}^*| = \varphi(n),\ \forall\ n \in \mathbb{N}$$

Donde φ es la función de Euler dada como sigue:

$$\varphi : \mathbb{N} \to \mathbb{N}$$

$$1 \mapsto 1$$

$$m \mapsto \varphi(m) = \{ n \in \mathbb{N} \text{ m } 1 \leq n < m \text{ y } (m,n) = 1 \}$$