PRACTICO 4:

CONGRUENCIAS:

Definición Dos numeros a y $b \in \mathbb{Z}$ se dicen congruentes modulo n con $n \in \mathbb{Z}$, si $a-b$ es un multiplo de n, es decir $n \mid a-b$ y se denota $\boxed{a \equiv b \bmod n}$ siendo b el representante de la clase

Lema Son equivalentes:

1) $a \equiv b \pmod n$
2) $a = b + kn$, $k \in \mathbb{Z}$
3) a y b tienen el mismo resto cuando se divide entre n

Proposición

1) Si $a \in \mathbb{Z}$ y $n \in \mathbb{N} \Rightarrow \exists!$ resto $\in \mathbb{Z}^+$: r: $a \equiv r \pmod n$ y $0 \leq r < n$
2) La congruencia modulo n es una relación de equivalencia

Observaciones:

- $a \equiv a \pmod n$ $\forall a \in \mathbb{Z}$, $\forall n \in \mathbb{N}$
- $a \equiv b \pmod 1$ $\forall a, b \in \mathbb{Z}$
- $a \equiv b \pmod 0 \leftrightarrow a = b$
- $a \equiv 0 \pmod n \leftrightarrow n \mid a$
- a es par $\leftrightarrow a \equiv 0 \pmod 2$
  a es impar $\leftrightarrow a \equiv 1 \pmod 2$
- $a \equiv b \pmod n \leftrightarrow a \equiv b \pmod{(-n)}$
- Todo numero mod 10, es congruente con su digito de unidad

Propiedades: Sean $a, b, c, n, m \in \mathbb{Z}$

1) $a \equiv b \pmod n$ y $c \equiv d \pmod n$
   $\Rightarrow a + c \equiv b + d \pmod n$ y $ac \equiv bd \pmod n$
2) $b \equiv c \pmod n \Rightarrow a + b \equiv a + c \pmod n$
3) $a \equiv b \pmod n$ y $m \mid n \Rightarrow a \equiv b \pmod m$
4) $a \equiv b \pmod m \Rightarrow n \cdot a \equiv n \cdot b \pmod m$
5) $a \equiv b \pmod m$ y $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod m$

Propiedades cancelativas

Sea $a, b, c, n \in \mathbb{Z}$ con $c \neq 0$

1) Si $ca \equiv cb \pmod n$ y $\operatorname{mcd}(c, n) = 1$
   $\Rightarrow a \equiv b \pmod n$
2) Si $c \mid n$ y $ca \equiv cb \pmod n$
   $\Rightarrow a \equiv b \pmod{n/c}$
3) Si $ca \equiv cb \pmod n$
   $\Rightarrow a \equiv b \pmod{n/d}$ con $d = \operatorname{mcd}(c, n)$

Propiedades practico

1) $a, b \in \mathbb{Z}$ y p es primo
   $\Rightarrow (a+b)^p \equiv a^p + b^p \pmod p$
2) Teorema de Fermat: $a^p \equiv a \pmod p$
   $\forall a \in \mathbb{Z}$ y p primo
3) Sea $n \in \mathbb{N}$ cuya representación en base 10 es $a_k \cdot a_{k-1} \dots a_1 \cdot a_0$
   $\Rightarrow n \equiv \sum_{i=0}^{q-1} 2^i \cdot a_i \pmod{2^q}$
4) $4^n \equiv 4 \pmod 6$ $\forall n \geq 1$
5) $\forall a \in \mathbb{Z}$, se cumple que:
   $a^2 \equiv 0 \pmod 4$ o $a^2 \equiv 1 \pmod 4$

Criterios de divisibilidad

- Prop: $3 \mid n \leftrightarrow 3 \mid$ la suma de los digitos de n
- Prop: $4 \mid n \leftrightarrow 4 \mid$ las ultimas dos cifras de n
- Prop: $6 \mid n \leftrightarrow 2 \mid n$ y $3 \mid n$
- Prop: $7 \mid n \leftrightarrow 7 \mid a_n$ sin la unidad menos dos veces la unidad
- Prop: $9 \mid n \leftrightarrow 9 \mid$ la suma de los digitos de n
- Prop: $11 \mid n \leftrightarrow 11 \mid$ suma de los digitos en un lugar impar menos la suma de los digitos en un lugar par