

Conferencia 3 - Congruencia

December 1, 2024

Definición. Sea $n \in \mathbb{Z}_+$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, se dice que a es congruente con b módulo n si a y b tienen el mismo resto al ser divididos por n y esto se denota $a \equiv b \pmod{n}$ o $a \equiv b(n)$

Teorema. Sea $n \in \mathbb{Z}_+$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, se dice que $a \equiv b(n)$ si y solo si $n|a - b$

Demostración

Como $a \equiv b(n)$, por definición, $a = kn + r$ y $b = qn + r$ luego

$$a - kn = b - qn$$

$$a - b = kn - qn$$

$$a - b = (k - q)n$$

por lo que $n|a - b$

Teorema. La relación de congruencia módulo n es una relación de equivalencia

Propiedades básicas de la congruencia

1. Para todo a , $a \equiv a(n)$

Demostración

Como $a - a = 0 = n * 0$ entonces $n|a - a$

2. Si $a \equiv b(n)$ si y solo si $b \equiv a(n)$

Demostración

Si $a - b = kn$ para algún k luego $b - a = -kn$

3. Si $a \equiv b(n)$ y $b \equiv c(n)$ entonces $a \equiv c(n)$

Demostración

Si $a - b = kn$ y $b - c = ln$ para k, l enteros entonces $a - c = (k + l)n$

4. Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a \pm b \equiv c \pm d(n)$

Demostración

Si $a - b = kn$ y $c - d = ln$ para k, l enteros entonces

$$(a + c) - (b + d) = (k + l)n \text{ y } (a - c) - (b - d) = (k - l)n$$

5. Si $a \equiv b(n)$ y $k \in \mathbb{Z}_+$ entonces Si $ak \equiv bk(n)$

Demostración

Se suma k veces $a \equiv b(n)$

6. Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $ab \equiv cd(n)$

Demostración

Para ello se debe demostrar que $ab - cd$ es múltiplo de n . Entonces

$$ac - bd = ac - bc + bc - cd = c(a - b) + c(b - d)$$

y $a - b$ y $c - d$ son múltiplos de n entonces $ab - cd$ también lo es

7. Si $a \equiv b(n)$ y $k \in \mathbb{Z}_+$ entonces $a^k \equiv b^k(n)$

Demostración

Se multiplica k veces $a \equiv b(n)$

8. Si $a \equiv b(n)$ entonces $a + c \equiv b + c(n)$ y $ac \equiv bc(n)$

Demostración

Se tiene que $a \equiv b(n)$ y también que $c \equiv c(n)$ luego $a + c \equiv b + c(n)$

Se suma c veces $a \equiv b(n)$ y se tiene entonces $ac \equiv bc(n)$

9. Si c es divisor común de a, b, n luego, si $a \equiv b(n)$ entonces $\frac{a}{c} \equiv \frac{b}{c}(\frac{n}{c})$

Demostración

Como c es divisor común de a, b, n entonces para a_1, b_1, n_1 enteros se tiene que $a = ca_1$, $b = cb_1$ y $n = cn_1$ y, entonces, $ca_1 \equiv cb_1(cn_1)$ luego $ca_1 - cb_1 = kcn_1$ para k entero, lo que es lo mismo que $a_1 - b_1 = kn_1$, por lo que $a_1 \equiv b_1(n_1)$ por tanto $\frac{a}{c} \equiv \frac{b}{c}(\frac{n}{c})$

10. Si $c|n$ y $a \equiv b(n)$ entonces $a \equiv b(c)$

Demostración

Como $c|n$ entonces $n = qc$ con q entero y como $a \equiv b(n)$ entonces $a - b = kn$ con k entero, luego $a - b = kqc$ y como kq es un entero entonces $a \equiv b(c)$

Teorema. Si $ca \equiv cb(n)$ entonces $a \equiv b(\frac{n}{d})$ donde $d = \text{mcd}(c, n)$

Demostración

Como $ca \equiv cb(n)$ entonces $ca - cb = c(a - b) = kn$, ahora si se tiene que $d = \text{mcd}(c, n)$ entonces existen s y r , $(r, s) = 1$ tales que $c = dr$ y $n = ds$, si se sustituye en la igualdad previa se tiene que $dr(a - b) = kds$ y si se simplifica queda que $r(a - b) = ks$.

A partir de esto se tiene que $s|r(a - b)$ y, como r y s son primos relativos, entonces por el Lema de Euclides $s|a - b$ y, por tanto $a \equiv b(s)$ lo que es lo mismo que $a \equiv b(\frac{n}{d})$

Corolario. Si $ca \equiv cb(n)$ y $\text{mcd}(c, n) = 1$ entonces $a \equiv b(n)$

Demostración

Para $d = 1$ se tiene entonces, a partir del teorema anterior que $a \equiv b(\frac{n}{1})$

Corolario. Si $ca \equiv cb(p)$ y $p \nmid c$ donde p es primo, entonces $a \equiv b(p)$

Demostración

Como $p \nmid c$ y p es primo, entonces $\text{mcd}(c, p) = 1$, y entonces se tienen el corolario anterior

Propiedades fuertes de la congruencia

1. Si $a \equiv b(m)$ y $a \equiv b(n)$ entonces $a \equiv b(\text{mcm}(m, n))$

Demostración

Por el **Teorema Fundamental de la Aritmética**

$$m = \prod_p p^{m_p}, n = \prod_p p^{n_p} \text{ y } \text{mcm}(m, n) = \prod_p p^{\max(m_p, n_p)}$$

donde p son números primos, $m_p \geq 0$ y $n_p \geq 0$.

Entonces, si $a \equiv b(m)$ y $a \equiv b(n)$ esto significa que $p^{m_p} | a - b$ y que $p^{n_p} | a - b$ y, por tanto, $p^{\max(m_p, n_p)} | a - b$.

Ahora como $a - b = \prod_p p^{c_p}$ donde $c_p \geq \max(m_p, n_p)$ entonces $\text{mcm}(m, n) | a - b$ y, por tanto, $a \equiv b(\text{mcm}(m, n))$

2. Si $a \equiv b(n)$ entonces $\text{mcd}(a, n) = \text{mcd}(b, n)$

Demostración

Si $a \equiv b(n)$ entonces $a - b = kn$ para k entero, luego $a = k * n + b$ y por tanto $\text{mcd}(a, n) = \text{mcd}(n, b)$

3. Si $ac \equiv bd(n)$, $c \equiv d(n)$ y $\text{mcd}(c, n) = 1$ entonces $a \equiv b(n)$

Demostración

Como $c \equiv d(n)$ entonces $\text{mcd}(d, n) = \text{mcd}(c, n) = 1$ y $c - d = qn$, lo que es lo mismo que $c = qn + d$

Ahora, como $ac \equiv bd(n)$ entonces $ac - bd = kn$ y sustituyendo c se tiene que

$$a(qn + d) - bd = kn$$

$$aqn + ad - bd = kn$$

$$ad - bd = kn - aqn$$

$$ad - bd = (k - aq)n$$

entonces $da \equiv db(n)$ y como $\text{mcd}(d, n) = 1$ entonces $a \equiv b(n)$

4. Sea $f(x)$ un polinomio con coeficientes enteros $a \equiv b(n)$ entonces $f(a) \equiv f(b)(n)$

Demostración

$f(x)$ de manera general se puede definir como $f(x) = \sum_{k=0}^m c_k x^k$

Como $a \equiv b(n)$ entonces se puede tener $a^k \equiv b^k(n)$ luego se pueden multiplicar por un entero tal que $c_k a^k \equiv c_k b^k(n)$ y estas se pueden sumar varias veces de modo que $\sum_{k=0}^m c_k a^k \equiv \sum_{k=0}^m c_k b^k(n)$ y como $f(a) = \sum_{k=0}^m c_k a^k$ y $f(b) = \sum_{k=0}^m c_k b^k$ entonces $f(a) \equiv f(b)(n)$

Definición. Si $f(x)$ es un polinomio con coeficientes enteros se dice que a es solución de $f(x) \equiv 0(n)$ si $f(a) \equiv 0(n)$

Teorema. Sea $f(x)$ un polinomio con coeficientes enteros tal que a es solución de $f(x) \equiv 0(n)$ y $a \equiv b(n)$, entonces b también es solución

Demostración

Por el teorema anterior se tiene que $f(a) \equiv f(b)(n)$ entonces se tiene que $f(b) \equiv f(a) \equiv 0(n)$ y, por tanto, b es solución

Teorema. Pequeño Teorema de Fermat. Sea p primo y $a \in \mathbb{Z}$, luego si $p \nmid a$ entonces $a^{p-1} \equiv 1(p)$

Demostración

Si se tienen los primeros $n - 1$ múltiplos positivos de a , que serían $a, 2a, 3a, \dots, (p - 1)a$, ninguno de ellos es congruente con otro módulo p pues si eso pasara entonces se tendría $ra \equiv sa(n)$, $1 \leq r < s \leq p - 1$, lo que resultaría en que $r \equiv s(n)$ lo que es falso.

Entonces el conjunto de múltiplos debe ser congruente módulo p con $1, 2, 3, \dots, p - 1$, en algún orden. Luego, si multiplicamos todas estas congruencias se tiene:

$$a * 2a * 3a * \dots * (p - 1)a \equiv 1 * 2 * 3 * \dots * (p - 1)(p)$$

Lo que es lo mismo que:

$$(p - 1)! a^{p-1} \equiv (p - 1)!(p)$$

$$\text{luego } a^{p-1} \equiv 1(p)$$