Taller 3 - Teoría de Números

Christian Mauricio Cardenas Baron
20251167009

Carlos Andres Giraldo Hernandez
Facultad de Ciencias Matemáticas y Naturales
Universidad Distrital Francisco José de Caldas

2025-11-06

2. Divisibilidad

2.5. Mínimo Común Múltiplo

Ejercicios:

3) Probar que $(a,b) = (a+b,[a,b])$

Demostración:

Sea $d=(a,b)$, entonces $a=dx$ y $b=dy$, con $(x,y)=1$. Luego

- $a+b = dx+dy = d(x+y)$
- $[a,b] = \frac{ab}{(a,b)} = \frac{dxdy}{d} = dxy$

Entonces $(a+b,[a,b]) = (d(x+y),dxy) = d(x+y,xy)$

Sea p un primo divisor común de $x+y$ y xy

Luego $p|xy$, entonces $p|x$ o $p|y$

Supongamos $p|x$, como $p|(x+y)$ y $p|x$, luego $p|(x+y)+(-x)$, entonces $p|y$

Ahora $p|x$ y $p|y$, pero $(x,y)=1$, esto solo se cumple en caso de $p=1$, por tanto no hay un primo divisor común de $x+y$ y xy, entonces $(x+y,xy)=1$

Retomando

$$(a+b,[a,b]) = d(x+y,xy) = d = (a,b)$$

□

5) Si k es múltiplo de a y b, probar que

$$\frac{|k|}{\left(\frac{k}{a},\frac{k}{b}\right)} = [a,b]$$

Demostración:

Como k es múltiplo de a y b, entonces existen $m,n \in \mathbb{Z}$ tal que $k=am=bn$

$$a=\frac{k}{m} \wedge b=\frac{k}{n} \quad \text{tambien} \quad m=\frac{k}{a} \wedge n=\frac{k}{b}$$

Sabemos que $[a,b] = \frac{|ab|}{(a,b)}$, remplazando a y b

$$[a,b] = \frac{|ab|}{(a,b)} = \frac{\left|\frac{k}{m}\cdot\frac{k}{n}\right|}{\left(\frac{k}{m},\frac{k}{n}\right)} = \frac{\left|k\cdot\frac{k}{mn}\right|}{\left(\frac{k}{m},\frac{k}{n}\right)} = \frac{|k|\left|\frac{k}{mn}\right|}{\left(\frac{k}{m},\frac{k}{n}\right)} = \frac{|k|}{\left|\frac{mn}{k}\right|\left(\frac{k}{m},\frac{k}{n}\right)}$$

Tenemos que $\left(\frac{k}{m},\frac{k}{n}\right) = \left(\left|\frac{k}{m}\right|,\left|\frac{k}{n}\right|\right)$, ademas $\left|\frac{mn}{k}\right|$ es un entero positivo por lo que lo podemos multiplicar dentro

$$\left(\left|\frac{k}{m}\right|\left|\frac{mn}{k}\right|,\left|\frac{k}{n}\right|\left|\frac{mn}{k}\right|\right) = \left(\left|\frac{\cancel{k}\cancel{m}n}{\cancel{m}\cancel{k}}\right|,\left|\frac{\cancel{k}m\cancel{n}}{\cancel{n}\cancel{k}}\right|\right) = (|n|,|m|) = (n,m) = \left(\frac{k}{b},\frac{k}{a}\right)$$

Por lo tanto $[a,b] = \dfrac{|k|}{\left(\frac{k}{a},\frac{k}{b}\right)}$ $\square$

7) Sean d y g enteros positivos. Probar que existen enteros a y b tales que $(a,b) = d$ y $[a,b] = g$ si y solo si $d|g$

Demostración:

- «$\Longrightarrow$» $\quad (d,g \in \mathbb{Z}^+)(\exists a,b \in \mathbb{Z})((a,b) = d \wedge [a,b] = g \Longrightarrow d|g)$

  Como $(a,b) = d$, entonces $d|a$ y $d|b$

  Como $[a,b] = g$, entonces $a|g$ y $b|g$

  Luego $d|a$ y $a|g$, por tanto $d|g$
- «$\Longleftarrow$» $\quad (d,g \in \mathbb{Z}^+)(d|g \Longrightarrow (\exists a,b \in \mathbb{Z})((a,b) = d) \wedge [a,b] = g)$

  Como $d|g$, existe $k \in \mathbb{Z}$ tal que $g = dk$

  Sea $a = d$ y $b = g$

  $$(a,b) = (d,g) = (d,dk)$$

  Como para cualquier $x,n \in \mathbb{Z}$, se tiene que $(x,xn) = x$, luego

  $$(a,b) = (d,dk) = d$$

  Entonces

  $$[a,b] = \frac{|ab|}{(a,b)} = \frac{|dg|}{d} = |g| = g$$

$\square$

10) Hallar enteros a y b tales que $a + b = 216$ y $[a,b] = 480$

Solucion:

Tomemos $a,b \in \mathbb{Z}^+$, ya que $(a,b) = (-a,-b)$

Sea $d = (a,b)$, entonces $d|a$ y $d|b$, luego $d|a+b$

Expresamos $a = dx$ y $b = dy$ con $(x,y) = 1$

Luego
- $a + b = dx + dy = d(x+y) = 216$
- $[a,b] = \frac{|ab|}{(a,b)} = \frac{ab}{(a,b)} = \frac{dxdy}{d} = dxy = 480$

Como $d|216$ y $d|480$, luego $d|(216,480)$, entonces $d \leq (216,480)$, siendo el máximo valor de $d = (216,480)$

Hallamos $(216,480)$

$$\begin{aligned} 480 &= 216 \cdot 2 + 48 \\ 216 &= 48 \cdot 4 + 24 \\ 48 &= 24 \cdot 2 \end{aligned}$$

Entonces $d = (216, 480) = 24$, se sigue que

$$x + y = \frac{216}{d} = \frac{216}{24} = 9 \quad \text{y} \quad xy = \frac{480}{d} = \frac{480}{24} = 20$$

Vemos que los x, y co-primos que cumplen $x + y = 9$ y $xy = 20$, son

$$x = 4 \quad \text{y} \quad y = 5$$

Sustituyendo en $a = dx$ y $b = dy$, tenemos

$$a = 24 \cdot 4 = 96 \quad \text{y} \quad b = 24 \cdot 5 = 120,$$

11) Hallar todos los números a y b que satisfacen $(a, b) = 24$ y $[a, b] = 1440$

Solucion:

Sea la descomposición en factores primeros de a y b

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \quad \text{y} \quad b = \prod_{i=1}^{n} p_i^{\beta_i}$$

Siendo p_i números primos, los exponentes $\alpha_i, \beta_i \in \mathbb{Z}^*$ y n la cantidad de primos en la descomposición que debe ser igual para a y b.

Sabemos que

$$(a, b) = 24 = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)} \quad \text{y} \quad [a, b] = 1440 = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

Por tanto podemos construir diferentes a y b intercambiando los α_i con los β_i en los factores primos, ya que se mantendría los mismos $\min$ y $\max$

Descomponemos 24 y 1440

$$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array} \qquad \begin{array}{r|l} 1440 & 2 \\ 720 & 2 \\ 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r} 24 = 2^3 \cdot 3^1 \cdot 5^0 \\ 1440 = 2^5 \cdot 3^2 \cdot 5^1 \end{array}$$

Ahora construimos los distintos a y b variando los α, β en cada primo

- Para el factor primo $p = 2$ el par de exponentes (α_2, β_2) es $(3, 5)$ o $(5, 3)$
- Para el factor primo $p = 3$ el par de exponentes (α_3, β_3) es $(1, 2)$ o $(2, 1)$
- Para el factor primo $p = 5$ el par de exponentes (α_5, β_5) es $(0, 1)$ o $(1, 0)$

Exponentes (α,β)			a	b
$p=2$	$p=3$	$p=5$		
$(3,5)$	$(1,2)$	$(0,1)$	$a=2^3 3^1 5^0=24$	$b=2^5 3^2 5^1=1440$
$(3,5)$	$(1,2)$	$(1,0)$	$a=2^3 3^1 5^1=120$	$b=2^5 3^2 5^0=288$
$(3,5)$	$(2,1)$	$(0,1)$	$a=2^3 3^2 5^0=72$	$b=2^5 3^1 5^1=480$
$(3,5)$	$(2,1)$	$(1,0)$	$a=2^3 3^2 5^1=360$	$b=2^5 3^1 5^0=96$
$(5,3)$	$(1,2)$	$(0,1)$	$a=2^5 3^1 5^0=96$	$b=2^3 3^2 5^1=360$
$(5,3)$	$(1,2)$	$(1,0)$	$a=2^5 3^1 5^1=480$	$b=2^3 3^2 5^0=72$
$(5,3)$	$(2,1)$	$(0,1)$	$a=2^5 3^2 5^0=288$	$b=2^3 3^1 5^1=120$
$(5,3)$	$(2,1)$	$(1,0)$	$a=2^5 3^2 5^1=1440$	$b=2^3 3^1 5^0=24$

Como $(a,b)=(b,a)$ y $[a,b]=[b,a]$ reduciendo los duplicados tenemos que las parejas a,b tal que $(a,b)=24$ y $[a,b]=1440$ son

$$\{(24,1440),(120,288),(72,480),(360,96)\}$$

4. Congruencias

4.1. Definición y Propiedades Básicas

Ejercicios:

2) Probar que si $ac \equiv_{cn} bc$ entonces $a \equiv_n b$

Demostración:

$$\begin{aligned} ac \equiv_{cn} bc &\Longrightarrow cn \mid ac-bc \\ &\Longrightarrow \cancel{c}n \mid \cancel{c}(a-b) \\ &\Longrightarrow \quad n \mid a-b \quad \Longrightarrow a \equiv_n b \end{aligned}$$

□

4) Probar que $3^{105}+4^{105} \equiv_{13} 0$

Demostración:

Verificamos 3^{105} y 4^{105} modulo 13

$3^{105} \equiv_{13} 3^{3\cdot 35} \equiv_{13} 27^{35} \equiv_{13} 1^{35} \equiv_{13} 1$

$4^{105} \equiv_{13} 4^{2\cdot 52+1} \equiv_{13} 16^{52}(4) \equiv_{13} 3^{3*17+1}(4) \equiv_{13} 27^{17}(3)(4) \equiv_{13} 1^{17}(12) \equiv_{13} -1$

Luego sumando las congruencias

$$3^{105}+4^{105} \equiv_{13} 1+(-1) \equiv_{13} 0$$

□

6) Si p es un primo impar probar que:

a) $1+2+3+\ldots+(p-1) \equiv_p 0$

b) $1^2+2^2+3^2+\ldots+(p-1)^2 \equiv_p 0$

c) $1^3+2^3+3^3+\ldots+(p-1)^3 \equiv_p 0$

Demostración:

a) Sea $S_1 = \sum_{i=1}^{p-1} i$, sabemos que la suma de los n primeros números es

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Luego para $n = p - 1$

$$\sum_{i=1}^{p-1} = \frac{(p-1)((p-1)+1)}{2} = \frac{(p-1)p}{2} = p\frac{(p-1)}{2}$$

Como p es primo y factor de S_1, luego

$$S_1 \equiv_p p\frac{p-1}{2} \equiv_p 0$$

b) Sea $S_2 = \sum_{i=1}^{p-1} i^2$, sabemos que la suma de los n primeros cuadrados es

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Luego para $n = p - 1$

$$\begin{aligned}\sum_{i=1}^{p-1} i^2 &= \frac{(p-1)((p-1)+1)(2(p-1)+1)}{6} \\ &= \frac{(p-1)p(2p-1)}{6} \\ &= p\frac{(p-1)(2p-1)}{6}\end{aligned}$$

Como p es primo y factor de S_2, luego

$$S_2 \equiv_p p\frac{(p-1)(2p-1)}{6} \equiv_p 0$$

c) Sea $S_3 = \sum_{i=1}^{p-1} i^3$, sabemos que la suma de los n primeros cubos es

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Luego para $n = p - 1$

$$\sum_{i=1}^{p-1} i^3 = \left(\frac{(p-1)p}{2}\right)^2 = (S_1)^2$$

De (a) tenemos que $S_1 \equiv_p 0$, luego $(S_1)^2 \equiv_p 0$, y como $(S_1)^2 = S_3$

$$S_3 \equiv_p 0$$

$\square$

8) Si $f(x)$ es un polinomio con coeficientes enteros y $f(a) \equiv_n k$ probar que para todo entero t, $f(a+tn) \equiv_n k$

Demostración:

Sea $f(x) = c_0 + c_1 x + c_2 x^2 + ... + c_m x^m = \sum_{i=0}^{m} c_i x^i$

Por definición $n|tn$, pero $n|(tn + a - a)$, luego $a + tn \equiv_n a$

Para todo $i \in \mathbb{Z}^*$ se tiene que $(a+tn)^i \equiv_n a^i$

Para todo $c_i \in \mathbb{Z}$ se tiene que $c_i(a+tn)^i \equiv_n c_i a^i$

Luego vemos que todo termino i de $f(a+tn)$ es congruente con su correspondiente $f(a)$ modulo n. Por lo tanto su suma también lo es

$$c_i(a+tn)^i \equiv_n c_i a^i$$
$$\sum_{j=0}^{m} c_j(a+tn)^j \equiv_n \sum_{j=0}^{m} c_j a^j$$
$$f(a+tn) \equiv_n f(a)$$

Luego $f(a+tn) \equiv_n f(a) \equiv_n k$, entonces $f(a+tn) \equiv_n k$ □

10) Hallar el dígito de las unidades de los números 13^{13} y $(5)(7)^{29} + (8)(9)^{72}$

Solucion:

a) Calculamos el modulo 10 de 13^{13}

$$13^{13} \equiv_{10} 3^{13} \equiv_{10} 3^{4\cdot3+1} \equiv_{10} 81^3(3) \equiv_{10} 1^3(3) \equiv_{10} 3$$

Por tanto el dígito de las unidades de 13^{13} es 3

b) Calculamos el modulo 10 de $(5)(7)^{29} + (8)(9)^{72}$

Hallamos el ultimo dígito de cada termino por separado

$$\begin{aligned} (5)(7)^{29} &\equiv_{10} 7^{4\cdot7+1}(5) \\ &\equiv_{10} 2401^7(7)(5) \\ &\equiv_{10} 1^7(35) \\ &\equiv_{10} 5 \end{aligned} \qquad \begin{aligned} (8)(9)^{72} &\equiv_{10} 9^{2\cdot36}(8) \\ &\equiv_{10} 81^{36}(8) \\ &\equiv_{10} 1^{36}(8) \\ &\equiv_{10} 8 \end{aligned}$$

Luego sumamos las congruencias

$$(5)(7)^{29} + (8)(9)^{72} \equiv_{10} 5 + 8 \equiv_{10} 13 \equiv_{10} 3$$

Por tanto el ultimo dígito de $(5)(7)^{29} + (8)(9)^{72}$ es 3

4.2. Criterios de Divisibilidad

Ejercicios:

1) Sea $n = a_0 + a_1 10 + a_2 10^2 + \ldots + a_k 10^k$ la representación decimal del entero positivo n. Probar que n es divisible por 11, si y solo si $\sum_{i=0}^{k} (-1)^i a_i$ es divisible por 11

Demostración:

Sea $n = \sum_{i=0}^{k} a_i 10^i, \quad a \in \{0, 1, \ldots, 9\}$

Como $10 \equiv_{11} -1$, luego para todo $i \in \mathbb{Z}^*$ se tiene que $10^i \equiv_{11} (-1)^i$, ademas para todo $a_i \in \{0, 1, \ldots, 9\}$ se tiene que $a_i 10^i \equiv_{11} a_i(-1)^i$

Luego la suma de todos los elementos $a_i 10^i$ va a ser congruente modulo 11 con la suma de todos los elementos $a_i(-1)^i$ de $i = 0, 1, \ldots, k$

$$\sum_{i=0}^{k} a_i 10^i \equiv_{11} \sum_{i=0}^{k} a_i(-1)^i$$

$$n \equiv_{11} \sum_{i=0}^{k} a_i(-1)^i$$

- «$\Longrightarrow$» $\quad 11|n \Longrightarrow 11|\sum_{i=0}^{k} (-1)^i a_i$

  Si $11|n$, entonces $n \equiv_{11} 0$

  Por lo anterior tenemos que $n \equiv_{11} \sum_{i=0}^{k} a_i(-1)^i \equiv_{11} 0$

  Entonces $11|\sum_{i=0}^{k} a_i(-1)^i$
- «$\Longleftarrow$» $\quad 11|\sum_{i=0}^{k} (-1)^i a_i \Longrightarrow 11|n$

  Si $11|\sum_{i=0}^{k} a_i(-1)^i$, entonces $\sum_{i=0}^{k} a_i(-1)^i \equiv_{11} 0$

  Por lo anterior tenemos que $\sum_{i=0}^{k} a_i(-1)^i \equiv_{11} n \equiv_{11} 0$

  Entonces $11|n$

□

2) A partir de la relación $10^3 \equiv_7 -1$, deducir un criterio de Divisibilidad por 7.

Solucion:

Expresamos n en bloques de 3, osea $n = \underbrace{b_m b_{m-1} b_{m-2}}_{a_m} \ldots \underbrace{b_5 b_4 b_3}_{a_1} \underbrace{b_2 b_1 b_0}_{a_0}$

$$n = a_0 + a_1 10^3 + a_2 10^6 + \ldots + a_m 10^{3m} = \sum_{i=0}^{m} a_i 10^{3i}, \quad a_i \in \{0, 1, 2, \ldots, 999\}$$

Como $10^3 \equiv_7 -1$, para todo $i \in \mathbb{Z}^*$ se tiene $\left(10^3\right)^i \equiv_7 (-1)^i$, luego para todo $a_i \in \{0, 1, \ldots, 999\}$ se tiene $a_i 10^{3i} \equiv_7 a_i(-1)^i$, sumando los términos desde $i = 0$ hasta m tenemos que

$$\sum_{i=0}^{m} a_i 10^{3i} \equiv_7 \sum_{i=0}^{m} a_i(-1)^i$$

Luego $n = \sum_{i=0}^{m} a_i 10^{3i}$, y sea $S = \sum_{i=0}^{m} a_i(-1)^i$, remplazando $n \equiv_7 S$

- Supongamos $7|n$, por definición $n \equiv_7 0$, luego $S \equiv_7 0$, entonces $7|S$
- Supongamos $7|S$, por definición $S \equiv_7 0$, luego $n \equiv_7 0$, entonces $7|n$

Por lo tanto $7|n \iff 7|S$, concluyendo

$$7|n \iff 7|\sum_{i=0}^{m} a_i(-1)^i$$

3) Probar que $6|n$ si y solo si $2|n$ y $3|n$.

Demostración:

- «$\Longrightarrow$» $6|n \Longrightarrow 2|n \wedge 3|n$

  Como $6|n$, entonces $n = 6k$, con $k \in \mathbb{Z}$, luego $n = (2)(3)k$, por tanto $2|n$ y $3|n$
- «$\Longleftarrow$» $2|n \wedge 3|n \Longrightarrow 6|n$

  Como $2|n$ y $3|n$, luego $n = 2a = 3b$, con $a, b \in \mathbb{Z}$

  Entonces $2a = 3b$, luego $3b$ debe ser par entonces b es par, sea $b = 2k$

  Luego $n = 2a = 3(2k) = 6k$. Por tanto $6|n$

$\square$

4) Con las notaciones del ejercicio 1, probar que $8|n$ si y solo si $8|(100a_2 + 10a_1 + a_0)$

Demostración:

Sea $n = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + ... + a_k 10^k = \sum_{i=0}^{k} a_i 10^i$

- «$\Longrightarrow$» $8|n \Longrightarrow 8|\left(a_0 + a_1 10 + a_2 10^2\right)$

  Extraemos los 3 primeros términos y factorizamos 10^3

$$\begin{aligned}
n &= a_0 + a_1 10 + a_2 10^2 + \sum_{i=3}^{k} a_i 10^i \\
&= a_0 + a_1 10 + a_2 10^2 + \sum_{i=0}^{k-3} a_{i+3} 10^{i+3} \\
&= a_0 + a_1 10 + a_2 10^2 + \sum_{i=0}^{k-3} a_{i+3} 10^i 10^3 \\
&= \left(a_0 + a_1 10 + a_2 10^2\right) + 10^3 \left(\sum_{i=0}^{k-3} a_{i+3} 10^i\right)
\end{aligned}$$

  Sean $S = a_0 + a_1 10 + a_2 10^2$ y $M = \sum_{i=0}^{k-3} a_{i+3} 10^i$

  Luego $n = S + 10^3 M$

  Por hipótesis $8|\left(S + 10^3 M\right)$, Ademas como $8|10^3$, entonces $8|10^3 M$

  Por lo tanto $8|S$, remplazando

$$8|\left(a_0 + a_1 10 + a_2 10^2\right)$$

- «$\Longleftarrow$» $8|\left(a_0 + a_1 10 + a_2 10^2\right) \Longrightarrow 8|n$

  Por hipótesis $8|\left(a_0 + a_1 10 + a_2 10^2\right)$

  Sabemos que

$$n = a_0 + a_1 10 + a_2 10^2 + 10^3 \sum_{i=0}^{k-3} a_{i+3} 10^i$$

  Y que $8|10^3 \sum_{i=0}^{k-3} a_{i+3} 10^i$, luego

$$8 \mid \left(a_0 + a_1 10 + a_2 10^2\right) + \left(10^3 \sum_{i=0}^{k-3} a_{i+3} 10^i\right)$$

  Por lo tanto $8|n$

$\square$

5) Expresando los enteros positivos en el sistema de numeración con base 100, deducir un criterio de divisibilidad por 101.

Solucion:

Expresamos a n en bloques de 2, osea $n = \underbrace{b_m b_{m-1}}_{a_m} \ldots \underbrace{b_3 b_2}_{a_1} \underbrace{b_1 b_0}_{a_0}$, luego

$$n = a_0 + a_1 10^2 + a_2 10^4 + \ldots + a_m 10^{2m} = \sum_{i=0}^{m} a_i 10^{2i}, \quad a_i \in \{0, 1, 2, \ldots, 99\}$$

Sabemos que $10^2 \equiv_{101} -1$, luego para todo $i \in \mathbb{Z}^*$, se tiene $\left(10^2\right)^i \equiv_{101} (-1)^i$ y para todo $a_i \in \mathbb{Z}$ tenemos $a_i 10^{2i} \equiv_{101} a_i(-1)^i$, sumando los términos desde $i = 0$ hasta m tenemos que

$$\sum_{i=0}^{m} a_i 10^{2i} \equiv_{101} \sum_{i=0}^{m} a_i(-1)^i$$

Luego $n = \sum_{i=0}^{m} a_i 10^{2i}$ y sea $S = \sum_{i=0}^{m} a_i(-1)^i$, remplazando $n \equiv_{101} S$

- Supongamos $101|n$, por definición $n \equiv_{101} 0$, luego $S \equiv_{101} 0$, entonces $101|S$
- Supongamos $101|S$, por definición $S \equiv_{101} 0$, luego $n \equiv_{101} 0$, entonces $101|n$

Concluyendo $101|n \Longleftrightarrow 101|S$