Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Ayudantía 15 - Teoría de números

21 de noviembre de 2025

Manuel Villablanca, Elías Ayaach, Caetano Borges

Resumen

- **Relación divide a:** La relación divide a, denotada por $|$ sobre $\mathbb{Z}\backslash 0$, es tal que $a \mid b$ si y solo si $\exists k \in \mathbb{Z}$ tal que $b = k \cdot a$.
- **Identidad de Bézout:** Esta identidd enuncia que si $a, b \in \mathbb{Z}$ son distintos de 0 y $\gcd(a, b) = d$, entonces existen $x, y \in \mathbb{Z}$ tales que:

$$a \cdot x + b \cdot y = d$$

- **Relación módulo n:** La relación módulo n, denotada por $\equiv_n$ sobre $\mathbb{Z}$, es tal que $a \equiv_n b$ si y solo si $n \mid (b - a)$. Esta relación es de equivalencia.
- **Operacion módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \bmod n$.
- **Teorema:**

$$a \equiv_n b \iff a \bmod n = b \bmod n$$

- **Máximo común divisor:** Dados a y b diremos que su máximo común divisor denotado como $\gcd(a, b)$ es el máximo natural n tal que $n \mid a$ y $n \mid b$.

1 Divisibilidad

Sea $k \in \mathbb{Z}$ tal que $k > 0$, y considere k números enteros consecutivos $x_1, \ldots, x_k$.
Demuestre que $k \left| \prod_{i=1}^{k} x_i \right.$.

Solución
En primer lugar, demostraremos que debe existir un $j \in \{1, \ldots, k\}$ tal que $k | x_j$. Para esto, demostraremos por casos que existe un $j \in \{1, \ldots, k\}$ tal que

$$x_j \equiv_k 0$$

1. $x_1 \equiv_k 0$: en este caso $j = 1$.
2. $x_1 \not\equiv_k 0$: supongamos que $x_1 \equiv_k m$, com $m \in \{1, \ldots, k-1\}$. Sumando $(k-m)$ en ambos lados de la equivalencia:

$$x_1 + k - m \equiv_k m + k - m \tag{1}$$
$$x_1 + k - m \equiv_k k \tag{2}$$
$$x_1 + k - m \equiv_k 0 \tag{3}$$

   Por otro lado, tenemos que $x_1 + k - m = x_{1+k-m}$, ya que los k números son consecutivos y $(k-m) \in \{1, \ldots, k\}$. Tomamos entonces $j = 1 + k - m$.

Utilizando lo anterior tenemos que

$$\prod_{i=0}^{k} x_i = x_j \cdot \prod_{\substack{i=1 \\ i \neq j}}^{k} x_i \equiv_k 0 \cdot \prod_{\substack{i=1 \\ i \neq j}}^{k} x_i \equiv_k 0$$

de donde concluímos que $k \left| \prod_{i=1}^{k} x_i \right.$.

2 MCD

- Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Demuestre que $\text{MCD}(a, b) = |b|$ si y sólo si $b \mid a$.
- Sean $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Demuestre que $\frac{a}{\text{MCD(a,b)}}$, $\frac{b}{\text{MCD(a,b)}}$ son coprimos.

Parte 1)
$\rightarrow$: Supongamos que $\text{MCD}(a, b) = |b|$. Por definición de máximo común divisor, $|b|$ divide tanto a a como a b. En particular, $|b| \mid a$. Eso quiere decir que $a = k|b|$ siendo k un entero arbitrario. Luego, por definición de valor absoluto $|b| = b$ o $|b| = -b$ por lo que la igualdad incial puede ser $a = kb$ (caso uno del valor absoluto) o $a = -kb$ (caso

dos), notamos que $-k$ sigue siendo entero por lo que se cumple que $b|a$ para ambos casos.
$\leftarrow$: Supogamos que se cumple que $b|a$ eso quiere decir que b divide a. Luego, nosotros sabemos que a también es divisible por $|b|$ por lo que podemos concluir que $|b|$ es el natural más grande que divide a b y a a la vez por lo que $MCD(a,b) = |b|$.

Conclusión:

$$\text{MCD}(a,b) = |b| \quad \iff \quad b \mid a.$$

Parte 2)
Sea $d = \text{MCD}(a,b)$. Por definición, $d \mid a$ y $d \mid b$, luego podemos escribir:

$$a = da', \qquad b = db' \qquad \text{con } a', b' \in \mathbb{Z}.$$

Mostremos que $\text{MCD}(a',b') = 1$.
Supongamos por contradicción que existe $c > 1$ tal que c divide simultáneamente a a' y b'. Entonces $c \mid a'$ y $c \mid b'$ implican:

$$c \mid da' = a, \qquad c \mid db' = b.$$

Por lo tanto, cd sería un divisor común de a y b mayor que d, lo que contradice que d es el máximo común divisor.
De aquí concluimos que no existe divisor común mayor a 1 entre a' y b', es decir:

$$\text{MCD}(a',b') = 1.$$

Con $a' = \dfrac{a}{d}$ y $b' = \dfrac{b}{d}$, luego:

$$\frac{a}{\text{MCD}(a,b)} \quad \text{y} \quad \frac{b}{\text{MCD}(a,b)}$$

son coprimos.

Conclusión: Los números a/d y b/d no comparten divisores mayores que 1, por lo que son coprimos.

3 MOD

1. Determine si existe solución para cada una de las siguientes congruencias lineales. En caso que exista, encuentre su solución.
   (a) $8x \equiv 6 \pmod{19}$
   (b) $21x \equiv 12 \pmod{35}$

- Como 19 es un número primo, 8 tiene inverso en $\mathbb{Z}_p$, por lo que la ecuación tiene solución. El inverso de 8 en módulo 19 es 12, ya que $8 \cdot 12 = 96 = 5 \cdot 19 + 1$. Multiplicando por 12 a ambos lados,

$$\begin{aligned} 12 \cdot 8 \cdot x &\equiv_{19} 12 \cdot 6 \\ x &\equiv_{19} 72 \\ x &\equiv_{19} 15 \end{aligned}$$

- 21 y 35 no son coprimos, ya que $7 \,|\, 21$ y $7 \,|\, 35$, por lo que 21 no tiene inverso módulo 35, y la congruencia no tiene solución.

2. Demuestre que todos los elementos de $\mathbb{Z}_p \setminus \{0\}$ tienen inverso multiplicativo en módulo p, si y sólo si p es primo.

Solución

Primero demostraremos que un elemento $a \in \mathbb{Z}_p \setminus \{0\}$ tiene inverso multiplicativo si y solo si $\gcd(a, p) = 1$.

$\rightarrow$: Supongamos que a tiene un inverso multiplicativo a^{-1} en módulo p. Por contradicción, supongamos que $\gcd(a, p) = d > 1$. Como a^{-1} es el inverso de a en módulo p, tenemos que

$$\begin{aligned} & & aa^{-1} &\equiv_p 1 \\ \iff & & \exists k \in \mathbb{Z} : aa^{-1} - 1 &= kp \\ \iff & & aa^{-1} - kp &= 1 \end{aligned}$$

Si dividimos a ambos lados por d, tenemos que

$$a^{-1}\frac{a}{d} - k\frac{p}{d} = \frac{1}{d}$$

y como $\gcd(a, p) = d > 1$, tenemos que $\frac{a}{d}, \frac{p}{d} \in \mathbb{Z}$, sin embargo, $d > 1$ por lo que es imposible que $\frac{1}{d} \in \mathbb{Z}$, con lo que tenemos una contradicción. Concluímos que es imposible que $\gcd(a, p) > 1$, con lo que $\gcd(a, p) = 1$.

$\leftarrow$: Supongamos que $\gcd(a, p) = 1$. Por la identidad de Bézout, existen enteros s, t tales que

$$\begin{aligned} & & sa + tp &= \gcd(a, p) = 1 \\ \iff & & sa - 1 &= (-t)p \\ \iff & & sa &\equiv_p 1 \end{aligned}$$

con lo que s es el inverso de a en módulo p. Ahora, es posible que $s \notin \{0, \ldots, p-1\}$, pero recordemos que $\mathbb{Z}_p$ es el conjunto de las clases de equivalencia módulo p, por lo que $[s]$ siempre existirá en $\mathbb{Z}_p$.