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

Ayudantía 13 - Teoría de números

28 de junio de 2024

Martín Atria, Paula Grune, 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.
- **Teorema:**

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

- **Operacion módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \bmod n$.
- **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 Congruencia módulo

Demuestre que si a es un número impar, entonces $a^2 \equiv 1 \pmod 8$.

Solución

Sea $a \in \mathbb{Z}$ un número impar. Luego sabemos que existe un único par $q, r \in \mathbb{Z}$ tal que

$$a = 8q + r \text{ con } 0 \leq r < 8 \tag{4}$$

Es claro que podemos reescribir 4 como:

$$a \equiv r(\text{mod} 8)$$

Elevando al cuadrado ambos lados de la congruencia obtenemos que $a^2 \equiv r^2 \pmod 8$, por lo que basta con demostrar que $r^2 \equiv 1 \pmod 8$.

Volviendo a 4, como a es impar, realmente existen solo las siguientes posibilidades: $a = 8q+1$, $a = 8q + 3$, $a = 8q + 5$ y $a = 8q + 7$. Es decir:

$$r \in \{1, 3, 5, 7\}$$

Luego notemos que:

- Si $r = 1 : 1^2 = 1 \equiv 1 \pmod 8$
- Si $r = 3 : 3^2 = 9 \equiv 1 \pmod 8$
- Si $r = 5 : 5^2 = 25 \equiv 1 \pmod 8$
- Si $r = 7 : 7^2 = 49 \equiv 1 \pmod 8$

Y así, $a^2 \equiv r^2 \equiv 1 \pmod 8$

3 Números primos

1. Sea p un número primo. Demuestre que para cada $a \in \mathbb{Z}_p$, se tiene que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

   Nota: $\mathbb{Z}_p$ denota al conjunto de las clases de equivalencia de enteros módulo p. Por ejemplo, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

2. Demuestre que si $p > 3$ es un número primo, entonces $p^2 \equiv 1 \pmod{24}$.

Solución

1. Por el pequeño Teorema de Fermat, $a^p \equiv a \pmod p$. Además, como p es primo, $gcd(a, p) = 1$ y por lo tanto existe a^{-1} en $\mathbb{Z}_p$. Multiplicando por a^{-1} a ambos lados, obtenemos $a^{p-1} \equiv 1 \pmod p$. Por definición de congruencia módulo p, se tiene que $\exists k \in \mathbb{Z}$ tal que $a^{p-1} - 1 = kp$. Factorizando en una suma por diferencia,

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = kp$$

   Con lo que obtenemos que $p|(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1)$. Como p es primo, por lo demostrado en la ayudantía pasada, necesariamente $p|(a^{\frac{p-1}{2}} + 1)$ o $p|(a^{\frac{p-1}{2}} - 1)$, lo que implica directamente que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

que es lo que queríamos demostrar.

2. Como $p > 3$ es primo, tenemos que $p-1$ y $p+1$ son números pares. Además, como son dos números pares consecutivos, uno de ellos es múltiplo de 4 y el otro es múltiplo de 2. Además, si consideramos la secuencia $p-1, p, p+1$, como son tres números enteros consecutivos, necesariamente hay un múltiplo de 3 entre ellos. Con todo esto en consideración, el número $k = (p-1) \cdot p \cdot (p+1)$ tiene a $2, 3$ y 4 como factores. Sin embargo, como p es un primo mayor a 3, p no aporta ninguno de esos factores, de lo que concluímos que $k' = (p-1)(p+1)$ también tiene a los factores $2, 3$ y 4, o en otras palabras, es múltiplo de 24, por lo que podemos escribirlo como $24k'' = p^2 - 1$, y como $k'' \in \mathbb{Z}$, esto es equivalente a $p^2 \equiv 1 \pmod{24}$, que es lo que queríamos demostrar.

4 Perros 🐕 y gatos 🐈

1. Sean $a, b, c \in \mathbb{Z}$. Demuestre que la ecuación $ax + by = c$ tiene al menos una solución si y sólo si $gcd(a, b)|c$.
2. Un grupo de perros y gatos gastaron \$100 en una tienda de juguetes para mascotas. Sabiendo que cada perro gastó \$8, y que cada gato gastó \$5, ¿puedes encontrar cuantos perros y cuantos gatos hay en el grupo?

Solución

1. Se demuestran ambas direcciones por separado:
   (a) $\rightarrow$: Se tiene que $ax + by = c$ tiene al menos una solución. Demostraremos que $gcd(a, b)|c$. Al dividir por $gcd(a, b)$ a ambos lados:

$$\begin{aligned} \frac{ax+by}{gcd(a,b)} &= \frac{c}{gcd(a,b)} \\ \frac{ax}{gcd(a,b)} + \frac{by}{gcd(a,b)} &= \frac{c}{gcd(a,b)} \\ \frac{a}{gcd(a,b)} \cdot x + \frac{b}{gcd(a,b)} \cdot y &= \frac{c}{gcd(a,b)} \end{aligned}$$

   Como $gcd(a, b)$ divide a a y a b,

$$k_1 x + k_2 y = \frac{c}{gcd(a,b)}$$

   Y como la ecuación original tiene al menos una solución, x e y son enteros, con lo que $gcd(a, b)|c$, que es lo que queríamos demostrar.

   (b) $\leftarrow$: Se tiene que $gcd(a, b)|c$. Demostraremos que $ax + by = c$ tiene al menos una solución. Por la identidad de Bézout, tenemos que existen $x, y \in \mathbb{Z}$ tal que

$$sa + tb = gcd(a, b)$$

Como $gcd(a,b)|c$, se tiene que $\exists k \in \mathbb{Z}$ tal que $k \cdot gcd(a,b) = c$. Luego, multiplicando a ambos lados por k se obtiene que

$$a(sk) + b(tk) = k \cdot gcd(a,b) = c$$

Podemos decir $x = sk, y = tk$ y llegamos a que

$$ax + by = c$$

Con lo que obtenemos una solución de la forma buscada, y se concluye la demostración.

(a) El problema se puede modelar mediante la siguiente ecuación:

$$8p + 5g = 100$$

Con $a = 8, b = 5$ y $c = 100$, tenemos una ecuación de la misma forma que la del inciso 1. Por lo demostrado en 1.(b), como $gcd(a,b) = gcd(8,5) = 1$, y $1|100$, sabemos que existe una solución para la ecuación. Por la identidad de Bézout, se tiene que

$$8s + 5t = gcd(8,5) = 1$$

Buscando una solución "al ojo", vemos que $s = 2, t = -3$ satisface la identidad. Multiplicando por 100 a ambos lados,

$$8(100s) + 5(100t) = 100$$

Con lo que podemos decir que una solución en los enteros es $p_0 = 100s = 100 \cdot 2 = 200$ y $g_0 = 100t = 100 \cdot -3 = -300$. Sin embargo, buscamos soluciones en los enteros no negativos, por lo que no nos sirve esta solución. Como queremos aumentar la cantidad de gatos (para que sea positiva), una forma de proseguir es quitando perros y añadiendo gatos. Para no romper la igualdad, por cada 5 perros que quitamos debemos agregar 8 gatos. Si hacemos esto k veces, obtenemos el sistema

$$\begin{aligned} p &= p_0 - 5k = 200 - 5k \\ g &= g_0 + 8k = -300 + 8k \\ p &\geq 0 \\ g &\geq 0 \end{aligned}$$

De $p \geq 0$ obtenemos que $k \leq \frac{200}{5} = 40$.
De $g \geq 0$ obtenemos que $k \geq \frac{300}{8} = 37,5$, y como $k \in \mathbb{Z}$, tenemos que $k \geq 38$.
Luego, las soluciones válidas son con $k \in \{38, 39, 40\}$, es decir,

- $p = 10, g = 4$
- $p = 5, g = 12$
- $p = 0, g = 20$