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

Ayudantía 16 - Teoría de números

28 de noviembre de 2025

Elías Ayaach, Manuel Villablanca, Caetano Borges

Resumen

- **Relación divide a:** La relación divide a, denotada por $|$ sobre $\mathbb{Z}\backslash 0$, es tal que $a \,|\, b$ 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 $n \,|\, (b - a)$. 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:**

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

- **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 $n \,|\, a$ y $n \,|\, b$.
- Pequeño Teorema de Fermat: Sea p un número primo. Para todo $a \in \mathbb{Z}$ se tiene que $a^p \equiv_p a$.
- Teorema Fundamental de la Aritmética: Cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

1 Pequeño Teorema de Fermat

Demuestre el Pequeño Teorema de Fermat:

Sea p un número primo. Si $a \in \mathbb{Z}_p = \{0, \ldots, p-1\}$, entonces $a^p \bmod p = a$

Demostración. Sea p un número primo y sea $a \in \{0, \ldots, p-1\}$. Demostraremos que

$$a^p \equiv a \pmod{p}.$$

Procedemos por inducción en a. Para $a = 0$ y $a = 1$ el resultado es trivial. Supongamos que para cierto a con $2 \leq a < p$ se cumple que

$$a^p \equiv a \pmod{p}.$$

Consideremos $a + 1$. Usamos el binomio de Newton:

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k.$$

Entonces:

$$(a+1)^p - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k.$$

Lema. Para todo $k \in \{1, \ldots, p-1\}$ se cumple $p \mid \binom{p}{k}$.
Demostración del lema. Como p es primo:

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k!} = p \cdot \frac{(p-1) \cdots (p-k+1)}{k!},$$

y el factor entre paréntesis es un entero. Luego $p \mid \binom{p}{k}$.

□

Por hipótesis inductiva se tiene $p \mid (a^p - a)$, y por el lema

$$p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k.$$

Por lo tanto

$$p \mid \left((a+1)^p - (a+1)\right),$$

lo que implica

$$(a+1)^p \equiv a + 1 \pmod{p}.$$

Con esto la inducción se completa y concluimos que, para todo $a \in \{0, \ldots, p-1\}$,

$$a^p \equiv a \pmod{p}.$$

■

2 Teorema Fundamental de la Aritmética

1. Demuestre que si p es un número primo y $p \mid (a \cdot b)$, entonces $p \mid a$ o $p \mid b$.
2. Demuestre el Teorema Fundamental de la Aritmética: cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

Solución

1. Supongamos que $p \nmid a$. Demostraremos que $p \mid b$.
   Como $p \nmid a$, tenemos que $\gcd(a, p) = 1$. Por la Identidad de Bézout, existen $s, t \in \mathbb{Z}$ tales que $sa + tp = 1$. Multiplicando por b a ambos lados,

   $$sab + tpb = b$$

   Como $p \mid ab$, y $p \mid p$, necesariamente $p \mid b$.
2. La existencia ya ha sido demostrada antes. Demostraremos unicidad.
   Sea $n \in \mathbb{N}$. Supongamos que $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot \ldots \cdot q_\ell^{\beta_\ell}$.
   Usando el Lema en su versión contrapositivo, como $p \nmid q$ para cualquier par p, q de primos distintos, tendremos que $p \nmid q^r$ para cualquier r. Concluímos que $k = \ell$ y $p_i = q_i$ para $i \in \{1, \ldots, k\}$.
   Por contradicción, supongamos que $\alpha_i > \beta_i$ para algún i. Tenemos entonces que

   $$p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$$
   $$p_1^{\alpha_1} \cdot \ldots \cdot p_{i-1}^{\alpha_{i-1}} \cdot p_{i+1}^{\alpha_{i+1}} \cdot \ldots \cdot p_k^{\alpha_k} = p_1^{\beta_1} \cdot \ldots \cdot p_{i-1}^{\beta_{i-1}} \cdot p_i^{\beta_i - \alpha_i} \cdot p_{i+1}^{\beta_{i+1}} \cdot \ldots \cdot p_k^{\beta_k}$$

   Como $\beta_i - \alpha_i > 0$, se tiene que p_i divide al lado derecho de la ecuación, sin embargo, por el Lema no divide al lado izquierdo, por lo que tenemos una contradicción. Obtenemos una contradicción de manera análoga si $\beta_i > \alpha_i$ para algún i. Concluímos que $\alpha_i = \beta_i$ para todo i, con lo que la factorización prima es única.

3 Números primos

Sea p un número primo > 2. Demuestre que para cada $a \in \mathbb{Z}_p, a \neq 0$, 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, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

Solución

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.

4 Un último esfuerzo

1. Para $m > 1$ demuestre que si $a \equiv b \pmod m$, entonces $\gcd(a,m) = \gcd(b,m)$.

Solución
Por contrapositivo, supongamos que $\gcd(a,m) \neq \gcd(b,m)$. Sin pérdida de generalidad, supongamos que $\gcd(a,m) > \gcd(b,m)$. Supongamos que $a \equiv_m b$. Esto quiere decir que existe un $k \in \mathbb{Z}$ tal que

$$a - b = km \qquad / \cdot \frac{1}{\gcd(a,m)}$$
$$\frac{a}{\gcd(a,m)} - \frac{b}{\gcd(a,m)} = \frac{km}{\gcd(a,m)}$$

Tenemos que $\frac{a}{\gcd(a,m)}, \frac{km}{\gcd(a,m)} \in \mathbb{Z}$. Sin embargo, $\frac{b}{\gcd(a,m)} \in \mathbb{Z}$ implica que $\gcd(a,m) \mid b$, y como $\gcd(a,m) > \gcd(b,m)$, existe un divisor común de b y m mayor a $\gcd(b,m)$, lo que es una contradicción. Concluímos que $a \not\equiv_m b$.

2. Para $m > 1$ demuestre que si $ac \equiv bc \pmod m$, entonces $a \equiv b \pmod{\frac{m}{\gcd(m,c)}}$.

Solución
Supongamos que $ac \equiv_m bc$. Esto quiere decir que $\exists k \in \mathbb{Z}$ tal que

$$ac - bc = km \qquad / \cdot \frac{1}{c}$$
$$a - b = \frac{km}{c}$$

Sea $d \in \mathbb{N}$ tal que $c = d \cdot \gcd(c, m)$. Luego,

$$a - b = \frac{km}{d \cdot gcd(c, m)}$$

Además, por el Teorema Fundamental de la Aritmética tenemos que $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Con ello,

$$a - b = \frac{k \cdot \frac{m}{\gcd(c,m)}}{p_1^{\alpha_1} \cdots p_n^{\alpha_n}}$$

Por el Lema del ejercicio 1.1, para cada p_i tendremos que $p_i \mid k$ o $p_i \mid \frac{m}{\gcd(c,m)}$. Pero $p_1 \mid \gcd(c, m)$ es imposible, porque implicaría que $\gcd(c, m)$ no es divisor común maximal de c y m. Luego, necesariamente $d \mid k$. Podemos asignar $k' := \frac{k}{d} \in \mathbb{Z}$, con lo que llegamos a

$$\begin{aligned} & a - b = k' \left(\frac{m}{\gcd(c, m)} \right) \\ \iff \quad & a \equiv b \pmod{\frac{m}{\gcd(c, m)}} \end{aligned}$$