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

Ayudantía 14 - Teoría de números

29 de noviembre de 2024

Martín Atria, José Thomas Caraball, 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 $n \mid b$.
- **Teorema Chino del Resto**: el sistema de ecuaciones

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución única en $\mathbb{Z}_m$ con $m = \prod_{i=1}^{n} m_i$.

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 Números primos

1. 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, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

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.

3 Función φ de Euler

La función $\varphi(n)$ de Euler es una función aritmética[1] que indica la cantidad de enteros positivos menores a n que son coprimos a n, esto es,

$$\varphi(n) = |\{m \in \mathbb{Z} \mid 0 < m < n \wedge \gcd(n,m) = 1\}|$$

1. Una función aritmética f es multiplicativa si cuando n y m son coprimos entonces $f(nm) = f(n)f(m)$, esto es, $\gcd(n,m) = 1 \Rightarrow f(nm) = f(n)f(m)$. Demuestre que φ es multiplicativa.
2. Demuestre que $\varphi(n) = n \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right)$

[1] Una función aritmética es una función cuyo dominio son los enteros positivos y su rango es cualquier subconjunto de los números complejos.

Solución

1. Sean $n, m \in \mathbb{Z}, n, m > 0, \gcd(n, m) = 1$. Consideremos el siguiente sistema de congruencias para $a \in \mathbb{Z}_n, b \in \mathbb{Z}_m$ arbitrarios:

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

   Por el Teorema Chino del Resto, este sistema tiene una única solución en $\mathbb{Z}_{nm}$. Luego, existe una biyección f entre $\mathbb{Z}_n \times \mathbb{Z}_m$ y $\mathbb{Z}_{nm}$.
   Notemos que si x es coprimo a n y también es coprimo a m, entonces necesariamente es coprimo a nm. Como f es una biyección, todo x coprimo a n y m tiene una imagen en $\mathbb{Z}_{nm}$, y particularmente $f(x \mod n, x \mod m)$ es coprimo a nm. Sea S_c con $c \in \mathbb{Z}, c > 0$ el conjunto de los enteros positivos menores a c coprimos a c. Se tiene entonces que $S_n \times S_m \approx S_{nm}$. Además, $S_c = \varphi(c)$. Con ello, concluímos que $\varphi(n) \cdot \varphi(m) = |S_n \times S_m| = |S_{nm}| = \varphi(nm)$, o en otras palabras, que φ es multiplicativa.

2. Por el Teorema Fundamental de la Aritmética, todo número $n \in \mathbb{N}$ puede ser representado como un producto de potencias naturales de primos, o escrito formalmente, $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$. Como el dominio de φ es un subconjunto de los naturales, todo elemento del dominio puede ser representado como un producto de potencias naturales de primos.
   Además, como se demostró en el inciso 1, la función φ es multiplicativa. Como los únicos divisores de un número primo p son 1 y p, entonces si tenemos dos números primos distintos, estos serán coprimos. Similarmente, las potencias de primos distintos también son coprimas, ya que sus únicos divisores son múltiplos de su primo base. Con ello, por un argumento inductivo podemos decir que

$$\varphi(n) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k})$$

   Por definición de φ se tiene que $\varphi(p_i^{e_i})$ es la cantidad de enteros positivos menores a $p_i^{e_i}$ que son coprimos a $p_i^{e_i}$. Los únicos enteros positivos menores o iguales a $p_i^{e_i}$ que son coprimos a $p_i^{e_i}$ son los múltiplos de p_i, esto es, $\text{NoCoprimos}(p_i^{e_i}) = \{p_i, 2p_i, 3p_i, \ldots, p_i^{e_i} - p_i, p_i^{e_i}\}$. Podemos escribir los últimos términos de este conjunto de otra manera para ver más fácilmente su cardinalidad:

$$\text{NoCoprimos}(p_i^{e_i}) = \{p_i, 2p_i, 3p_i, \ldots, (p_i^{e_i-1} - 1) \cdot p_i, p_i^{e_i-1} \cdot p_i\}$$

   Tenemos que $|\text{Divisores}(p_i^{e_i})| = p_i^{e_i-1}$, por lo que la cantidad de números $\leq p_i^{e_i}$ que son coprimos a $p_i^{e_i}$ debe ser $p_i^{e_i} - p_i^{e_i-1}$. Luego,

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{e_1}) \cdot \varphi(p_1^{e_1}) \cdots \varphi(p_k^{e_k}) \\ &= \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdot \left(p_2^{e_1} - p_2^{e_2-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right) \end{aligned}$$

Si factorizamos cada término por $p_i^{e_i}$ obtenemos que

$$\begin{aligned}
&= \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdot \left(p_2^{e_1} - p_2^{e_2-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right) \qquad \square
\end{aligned}$$