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

Ayudantía 12 - Teoría de números

14 de junio de 2024

Martín Atria, Paula Grune, Caetano Borges

Resumen

1 Representación de números

Demuestre que todo número $n \in \mathbb{N}$ se puede representar de la forma:

$$n = e_k \cdot 3^k + \cdots + e_1 \cdot 3^1 + e_0$$

donde $e_0, \ldots, e_k \in \{1, 0, -1\}$

2 Divisibilidad

1. Demuestre que si $\gcd(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.
2. Demuestre que si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.
3. En clases se demostró que todo número natural $n > 1$ se puede descomponer como:

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$$

   con $p_1, \ldots, p_k$ primos y $p_1 \leq p_2 \leq \cdots \leq p_k$. Demuestre usando el resultado en el punto anterior que esta descompocición es única.

Solución

1. Por la identidad de Bézout, se tiene que existen $s, t \in \mathbb{Z}$ tal que

$$sa + tb = \gcd(a, b) = 1$$

Por otra parte, como $a \mid bc$, se tiene que existe $k \in \mathbb{Z}$ tal que

$$ka = bc$$

Si multiplicamos por t en ambos lados en esta ecuación obtenemos

$$tka = tbc$$

Reemplazando tb según la identidad de Bézout,

$$\begin{aligned} tka &= (1 - sa)c \\ tk &= \frac{c - csa}{a} \\ tk &= \frac{c}{a} - cs \\ tk - cs &= \frac{c}{a} \end{aligned}$$

Como t, k, c y s son enteros, y los enteros son cerrados bajo suma y multiplicación, entonces $tk - cs$ es entero, y consecuentemente $\frac{c}{a}$ también. Con ello, concluímos que $a \mid c$, que es lo que queríamos demostrar.

2. Hay 4 casos posibles:

   - $\gcd(p, a) = 1$: en este caso, por lo demostrado en el inciso anterior, tenemos que $p \mid b$.
   - $\gcd(p, b) = 1$: análogo al anterior.
   - $\gcd(p, a) \neq 1$: como p es primo, solo tiene dos divisores: 1 y p. Ya que el gcd entre p y a no es 1, la única otra opción es que sea p. Con ello, existe un entero k tal que $a = kp$, por lo que $p \mid a$.
   - $\gcd(p, b) \neq 1$: análogo al anterior.

3. Se demostrará por inducción que la factorización prima de todo número natural $n > 1$ es única.

   BI: Con $n = 2$, es claro que la factorización prima es única.

   HI: Supongamos que la factorización prima de todo natural k tal que $1 < k < n$ es única.

   TI: Demostraremos que la factorización prima de n es única.
   Por contradicción, supongamos que n tiene dos factorizaciones primas distintas. Luego, $n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$, con r, s naturales y $p_, q_i$ primos. Como $p_1 \mid c$, entonces $p_1 \mid q_1 \cdot q_2 \cdot \dots \cdot q_s$. Por lo demostrado en el inciso (2), necesariamente $p_1 \mid q_j$ para algún $j \in \{1, \dots, s\}$. Como p_1 y q_j son ambos primos, nos queda que $p_1 = q_j$. Luego, $p_2 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_s$. Sin embargo, este producto es un número

$k < n$, por lo que, por hipótesis de inducción, no puede tener dos factorizaciones primas distintas, con lo que llegamos a una contradicción.

Concluímos que la factorización prima de todo número natural $n > 1$ es única.

3 Uno cortito

Sean $a, b \in \mathbb{Z}$ tales que $a, b > 0$. Demuestre que $a \mid (a+1)^b - 1$.

Solución
Si $a = 1$ la afirmación se cumple trivialmente. Consideremos el caso en que $a > 1$. Usando propiedades de módulo:

$$\begin{aligned}
&(a+1)^b - 1 \\
\equiv_a\ & (((a+1)^b \bmod a) - (1 \bmod a)) \bmod a \\
\equiv_a\ & \left(\left(\left(\prod_{i=1}^{b}(a+1 \bmod a)\right) \bmod a\right) - 1\right) \bmod a \\
\equiv_a\ & \left(\left(\left(\prod_{i=1}^{b} 1\right) \bmod a\right) - 1\right) \bmod a \\
\equiv_a\ & (1-1) \bmod a \\
\equiv_a\ & 0
\end{aligned}$$

Como $(a-1)^b - 1 \equiv_a 0$, concluímos que $a \mid (a-1)^b - 1$, que es lo que queríamos demostrar.