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

Ayudantía 14 - Teoría de números

Héctor Núñez, Paula Grune, Manuel Irarrázaval

Ejercicio 1: Aritmética Modular

Sean a, b, c y $m \in \mathbb{Z}$ tales que $m \geq 2$.

1. Demuestre que si $a \equiv b (\text{mód} m)$, entonces $MCD(a, m) = MCD(b, m)$.
2. Demuestre que si $ac \equiv bc (\text{mód} m)$, entonces $a \equiv b \left(\text{mód} \frac{m}{MCD(c,m)} \right)$.

Solución

1. Supongamos que $a \equiv b (\text{mód} m) (1)$. Primero demostraremos que para cualquier $c \in \mathbb{Z}$ tal que $c \mid m$, se cumple que $c \mid a$ si, y solo si, $c \mid b$.

   Sea c tal que $c \mid m$ y $c \mid a$ (2). Por definición de (1), sabemos que existe un $k \in \mathbb{Z}$ tal que

   $$b = a + k \cdot m$$

   Por (2), sabemos que c divide a ambos sumandos del lado derecho de esta igualdad. En consecuencia, concluimos que c divide al lado izquierdo de tal igualdad: $c \mid b$.

   Análogamente podemos demostrar la dirección contraria, vale decidr que si $c \mid m$ y $c \mid b$, entonces $c \mid a$.

   Esto implica que los factores en común de a y m son los mismos que los de b y m. En particular, podemos concluir que el máximo de estos factores debe ser el mismo, y por lo tanto:

   $$MCD(a, m) = MCD(b, m)$$

2. Supongamos que $ac \equiv bc (\text{mód} m)$. Por definición sabemos que existe $k \in \mathbb{Z}$ tal que:

$$
\begin{aligned}
ac - bc &= k \cdot m \\
(a-b) \cdot c &= k \cdot m \\
a - b &= \frac{k \cdot m}{c}
\end{aligned}
$$

Por otro lado, sea $c' \in \mathbb{Z}$ tal que $c = c' \cdot MCD(c,m)$. Reemplazando esto en (1):

$$a - b = \frac{k \cdot m}{c' \cdot MCD(c,m)}$$

Notemos que $a - b$ es un entero y por definición $\frac{m}{MCD(c,m)}$ también lo es. Luego, $\frac{k}{c'}$ también debe ser un entero. Sea este último entero k', entonces tenemos que:

$$a - b = k' \cdot \frac{m}{MCD(c,m)}$$

Lo cual por definición implica que:

$$a \equiv b \left(\text{mód} \frac{m}{MCD(c,m)} \right)$$

Ejercicio 2: Pequeño teorema de Fermat

1. Demuestre que $13 | (7^{121} + 6)$

   Veamos que esto es equivalente a:

   $$7^{121} + 6 \bmod 13 = 0$$

   Descomponiendo $121 = 12 \cdot 10 + 1$ y ocupando el pequeño teorema de Fermat:

   $$7^{120} \cdot 7 + 6 \bmod 13 = (7^{10})^{(13-1)} \cdot 7 + 6 \bmod 13 = 1 \cdot 7 + 6 \bmod 13 = 0$$

2. Un googleplex es equivalente $10^{10^{100}}$. ¿Que dia de la semana va a ser en un googleplex dias? (Hoy dia es miércoles).

   Para encontrar el cambio neto en dias de semana, debemos encontrar cuantos dias han pasado módulo 7, es decir:

   $$10^{10^{100}} \bmod 7$$

   Notemos que como 7 es primo y no divide a ninguna potencia de 10, entonces $10^{(7-1)c} \bmod 7 = 1$. Si descomponemos $10^{100} = 6q + r$:

   $$10^{10^{100}} \bmod 7 = 10^{6q} \cdot 10^{r} \bmod 7 = 10^{r} \bmod 7$$

Vemos que $r = (10^{100} \bmod 6)$ y notemos lo siguiente:

$$10 \bmod 6 = 4$$

Y si $10^k \bmod 6 = 4$, entonces:

$$10^k \cdot 10 \bmod 6 = 4 \cdot 4 \bmod 6 = 16 \bmod 6 = 4$$

$$10^{k+1} \bmod 6 = 4$$

Por lo que por inducción $10^n \bmod 6 = 4$ para todo n.. Especificamente, $10^{100} \bmod 6 = 4 = r$

Finalmente llegamos a lo siguiente:

$$10^r \bmod 7 = 10^4 \bmod 7 = 4$$

Por lo tanto, en un googleplex días va a ser domingo.

Ejercicio 3: Máximo común divisor y algoritmo euclidiano

Considere el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Demuestre que el sistema tiene solución si y solo si $\mathrm{MCD}(m_1, m_2) \mid (a_1 - a_2)$.

Solución:

($\Rightarrow$) Sea $d = \mathrm{MCD}(m_1, m_2)$. Si el sistema tiene solución, entonces existe $x \in \mathbb{Z}$ tal que

$$x = a_1 + m_1k_1 = a_2 + m_2k_2$$

para algunos $k_1, k_2 \in \mathbb{Z}$. De lo anterior, tenemos que

$$a_1 - a_2 = m_2k_2 - m_1k_1.$$

Finalmente, como d divide a m_1 y a m_2 (por ser el máximo común divisor entre ambos), obtenemos que

$$\mathrm{MCD}(m_1, m_2) \mid (a_1 - a_2).$$

($\Leftarrow$) Suponemos $d \mid (a_1 - a_2)$, en otras palabras, existe $k \in \mathbb{Z}$ tal que $a_1 - a_2 = dk$. Utilizando el algoritmo extendido de Euclides, sabemos que existen enteros s y t tales que $d = sm_1 + tm_2$. Si juntamos lo anterior, obtenemos

$$a_1 - a_2 = dk = (sm_1 + tm_2)k.$$

Luego podemos obtener $a_1 + (sk)m_1 = a_2 + (tk)m_2$, lo que significa que existe un entero z tal que $z \equiv a_1 \pmod{m_1}$ y $z \equiv a_2 \pmod{m_2}$.