# Teoría de números

## Hoja de ejercicios 6

Docente: Gabriel Chicas Reyes, MSc.
Alumno: Kevin López Aquino

Jueves 17 de octubre de 2019

El siguiente lema será de utilidad para los ejercicios 15 y 16.

**Lema 1.** Sean $m_1, \ldots, m_r$ enteros positivos. Entonces, para todo $1 \leq i \leq r$

$$x \equiv y \pmod{m_i}$$

si y solo si

$$x \equiv y \pmod{\operatorname{mcm}(m_1, \ldots, m_r)}.$$

*Demostración.* ($\Rightarrow$) Si se tiene $x \equiv y \pmod{m_i}$ para $1 \leq i \leq r$, se sigue que para cada $m_i$, $m_i \mid x - y$, de forma que $x - y$ es un múltiplo común de todos los módulos y, por tanto,

$$\operatorname{mcm}(m_1, \ldots, m_r) \mid x - y,$$

o de forma equivalente,

$$x \equiv y \pmod{\operatorname{mcm}(m_1, \ldots, m_r)}.$$

($\Leftarrow$) Supongamos que

$$x \equiv y \pmod{\operatorname{mcm}(m_1, \ldots, m_r)}.$$

Entonces podemos deducir cada congruencia $x \equiv y \pmod{m_i}$, para $1 \leq i \leq r$, debilitando la congruencia original, puesto que $m_i \mid \operatorname{mcm}(m_1, \ldots, m_r)$. $\square$

**15.** Sea $m = p_1 \cdot \ldots \cdot p_r$ un entero libre de cuadrados. Determine el número de soluciones de la congruencia

$$x^2 \equiv x \pmod{m}.$$

• Comenzamos con el siguiente lema.

**Lema 2.** Sea $p$ primo. Entonces,

$$x^2 \equiv x \pmod{p}$$

si y solo si $x \equiv 0 \pmod{p}$ o $x \equiv 1 \pmod{p}$.

*Demostración.* ($\Rightarrow$) Supongamos que

$$x^2 \equiv x \pmod{p}.$$

De esto se sigue que $p \mid x(x-1)$. Por el lema de Euclides, o bien $p \mid x$, de forma que $x \equiv 0 \pmod{p}$, o bien $p \mid x - 1$, de forma que $x \equiv 1 \pmod{p}$.

($\Leftarrow$) Si $x$ es congruente con 0 o con 1 módulo $p$, se sigue que $x^2 \equiv x \pmod{p}$. $\square$

Procedemos al resultado principal.

**Proposición.** Sea $m = p_1 \cdot \ldots \cdot p_r$ un entero libre de cuadrados. Entonces, la congruencia

$$x^2 \equiv x \pmod{m}$$

tiene $2^r$ soluciones distintas módulo $m$.

*Demostración.* Por el lema anterior, sabemos que para cada primo $p_i$ en la factorización de $m$, la congruencia

$$x^2 \equiv x \pmod{p_i}$$

implica y es implicada por las dos alternativas

$$x \equiv 0 \pmod{p_i} \quad \text{o} \quad x \equiv 1 \pmod{p_i}.$$

Así, para cada $p_i$ en la factorización de $m$, hay 2 posibilidades. Puesto que hay $r$ primos distintos en la factorización de $m$, se sigue que hay $2^r$ formas de construir un sistema de $r$ congruencias.
Notando que los módulos en los sistemas de congruencias son coprimos dos a dos, podemos aplicar el teorema chino del resto y deducir que cada sistema de congruencias produce una solución única módulo $p_1 \cdot \ldots \cdot p_r = m$.

$\square$

**16.** Encontrar todos los idempotentes módulo 2019.

• Aplicamos la idea de la demostración anterior a este caso concreto. Primero notamos que $2019 = 3 \cdot 673$ y que 3 y 673 son primos. Podemos formar los siguientes sistemas de congruencias:

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 0 \pmod{673} \end{cases} \tag{1}$$

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{673} \end{cases} \tag{2}$$

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{673} \end{cases} \tag{3}$$

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{673} \end{cases} \tag{4}$$

Por el teorema chino del resto, cada uno de estos sistemas tiene una única solución módulo 2019. Por los **lemas 1** y **2**, si $x$ es la solución de alguno de estos sistemas, se sigue que $x^2 \equiv x \pmod{2019}$. Además, estos 4 sistemas representan todas las soluciones.

La solución al sistema (1) es $x \equiv 0 \pmod{2019}$. De manera similar, la solución al sistema (2) es $x \equiv 1 \pmod{2019}$. Para el sistema (3), construimos la siguiente tabla, donde 449 corresponde al inverso multiplicativo de 3 módulo 673, encontrado haciendo uso del algoritmo de Euclides.

| $m_j$ | $a_j$ | $m/m_j$ | $b_j$ |
|---|---|---|---|
| 3 | 1 | 673 | 1 |
| 673 | 0 | 3 | 449 |

Por la fórmula del teorema chino del resto, la solución en este caso es,

$$x \equiv 673 \pmod{2019}.$$

Para el sistema (4), la tabla es casi igual:

| $m_j$ | $a_j$ | $m/m_j$ | $b_j$ |
|---|---|---|---|
| 3 | 0 | 673 | 1 |
| 673 | 1 | 3 | 449 |

De nuevo, por el teorema chino del resto, la solución es

$$x \equiv 3 \cdot 449 \equiv 1347 \pmod{2019}. \quad \blacksquare$$

**20.** Sean $m$ y $n$ enteros positivos cualesquiera. Sea $d = \text{mcd}(m, n)$. Demuestre la identiddad
$$\varphi(mn) = \frac{d\varphi(m)\varphi(n)}{\varphi(d)}.$$
¿Qué sucede si $m$ y $n$ son coprimos?

• Notamos que si $m$ y $n$ son coprimos

$$\text{mcd}(m, n) = 1$$
$$\varphi(\text{mcd}(m, n)) = \varphi(1) = 1$$

de forma que lo anterior se reduce al hecho que $\varphi(mn) = \varphi(m)\varphi(n)$ cuando $m$ y $n$ son coprimos. De forma más interesante, supongamos que $\varphi(m)\varphi(n) = \varphi(mn)$. Entonces, de la fórmula a demostrar se sigue que

$$1 = \frac{d}{\varphi(d)}$$

$$\varphi(d) = d.$$

El único número que satisface esta ecuación es $d = 1$. En efecto, si $d \geq 2$, se tiene que $d > \varphi(d)$. De esto se sigue que $m$ y $n$ deben ser coprimos.

Veamos un ejemplo. Consideremos 2 y 10 y notemos que $\text{mcd}(10, 2) = 2$. Entonces,

$$\varphi(10 \cdot 2) = 10 \cdot 2 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$\varphi(10)\varphi(2) = 10 \cdot 2 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$\varphi(d) = \varphi(2) = 2 \cdot \left(1 - \frac{1}{2}\right)$$

Así, se cumple que

$$\varphi(10 \cdot 2) = \frac{2 \cdot \varphi(10) \cdot \varphi(2)}{\varphi(2)}.$$

En general,

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1 - \frac{1}{p}\right) = \frac{\frac{1}{m}\prod_{p|m}\left(1 - \frac{1}{p}\right) \cdot \frac{1}{n}\prod_{p|n}\left(1 - \frac{1}{p}\right)}{\frac{1}{\text{mcd}(m,n)}\prod_{p|\text{mcd}(m,n)}\left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}}.$$

Así, $\varphi(mn) = \frac{d\varphi(m)\varphi(n)}{\varphi(d)}$. ■

**21.** Sea $n \geq 2$. Demuestre que la suma de todos los enteros positivos $1 \leq k \leq n$ coprimos con $n$ vale

$$\frac{1}{2} n\varphi(n).$$

• Primero notamos que para todo $1 \leq k \leq n$,

$$-k \equiv n - k \pmod{n}$$

Esto implica que $\operatorname{mcd}(k, n) = \operatorname{mcd}(-k, n) = \operatorname{mcd}(n - k, n)$. De forma que si $k$ es coprimo con $n$, entonces $n - k$ también será coprimo con $n$.

Si $n = 2$, la proposición se cumple. Por otro lado, si $n > 2$, en la suma de los coprimos positivos menores que $n$, podemos formar parejas de enteros de la forma

$$k \quad \text{y} \quad n - k.$$

Cada pareja suma $n$ y hay $\frac{\varphi(n)}{2}$ parejas, por lo que suma total es

$$\frac{1}{2} n\varphi(n). \quad \blacksquare$$