MA-53G Intr. a la Criptografía **Semestre Otoño, 1998**

Cátedra No. 8,9 : 27 abril

Transcriptor: Felipe Saint-jean [1]

1 Más de teoría de números

Teorema 1 *El pequeño teorema de Fermat*

Sea p un primo. Entonces, para todo entero a se cumple que $a^p \equiv a(\text{mod} p)$.

Dem: Separaremos la demostración en dos casos:

Si a y p son primos relativos ($mcd(a,p) = 1$) entonces, por el teorema de Euler visto anteriarmente, se tendrá que $a^{p-1} \equiv 1(\text{mod} p)$ (porque $\phi(p) = p - 1$ y el teorema de Euler nos dice que $a^{\phi}(n) \equiv 1(\text{mod} n)$ si $mcd(a,n) = 1$), multiplicando por a la ecuación obtenemos lo que buscabamos, $a^p \equiv a(\text{mod} p)$.

El otro caso es si p divide a (es decir a y p no son primos relativos $mcd(a,p) > 1$) entonces, por definición de congruencia, se tiene que $a \equiv 0(\text{mod} p)$ y $a^p \equiv 0(\text{mod} p)$ por lo que $a^p \equiv a(\text{mod} p)$. $\square$

Corolario 1 *Si p primo no divide a a y $n \equiv m(\text{mod}(p-1))$, entonces $a^n \equiv a^m(\text{mod} p)$.*

Dem: Si $n \equiv m(\text{mod}(p-1))$, entonces se cumple que existe un entero b tal que $n = m + b(p-1)$. Por lo tanto, $a^n = a^{m+b(p-1)} = a^m \cdot a^{b(p-1)}$ y del teorema de Euler $a^{p-1} \equiv 1(\text{mod} p)$ de donde obtenemos $a^{b(p-1)} \equiv \left(a^{p-1}\right)^b \equiv 1(\text{mod} p)$, y entonces $a^n \equiv a^m(\text{mod} p)$. $\square$

Corolario 2 *Si a es primo relativo con n, y $m \equiv m'(\text{mod}\varphi(n))$, entonces $a^m \equiv a^{m'}(\text{mod} n)$.*

Dem: Del teorema de Euler tenemos que $a^{\varphi(n)} \equiv 1(\text{mod} n)$. Además, $m \equiv m'(\text{mod}\varphi(n))$, o sea que $m = t\varphi(n) + n$, para algún entero t. Entonces, $a^m \equiv a^{t\varphi(n)+m'} \equiv (a^{\varphi(n)})^t \cdot a^{m'} \equiv a^{m'}(\text{mod} n)$. $\square$

Teorema 2 *Teorema Chino del Resto*

Sean $m_1, m_2, ..., m_r$ enteros positivos relativamente primos a pares (es decir $mcd(m_i, m_j) = 1$ para cualquier par i,j distintos). Sea $M = \prod_{i=1}^r m_i$. Dados $a_1, a_2, ..., a_r$ enteros, existe un único (módulo M) entero x que satisface simultaneamente

[1] Estos apuntes están basados en las transcripciones de Jens Hardings(28/8/96) y de Marcos Kiwi(3/9/96)

$$\begin{aligned} x &\equiv a_1(\operatorname{mod} m_1) \\ x &\equiv a_2(\operatorname{mod} m_2) \\ x &\equiv a_3(\operatorname{mod} m_3) \\ &\vdots \\ x &\equiv a_r(\operatorname{mod} m_r) \end{aligned}$$

Nota:Este Teorema nos dice que dada una congruencia, la podemos dividir en un sistema de equivalencias sin ambiguedad.

Dem: Unicidad: Sean x y x' dos soluciones, luego

$$\begin{aligned} x &\equiv a_i(\operatorname{mod} m_i) \\ x' &\equiv a_i(\operatorname{mod} m_i) \end{aligned}$$

donde $i = 1 \ldots r$. Luego $(x - x') \equiv 0(\operatorname{mod} m_i)$, donde $i = 1 \ldots r$. Y como m_i es primo relativo con m_j si $i \neq j$, sigue que $x \equiv x'(\operatorname{mod} M)$

Existencia: Sea $N_i = \frac{M}{m_i} = \prod_{j \neq i} m_i$, luego N_i y m_i no tienen divisores comunes (distintos de uno) por que los m_i son primos relativos a pares, es decir Ni y m_i son primos relativos.

Por lo tanto existe un M_i (inverso de N_i en $\mathcal{Z}_{m_i}$) tal que $N_i M_i \equiv 1(\operatorname{mod} m_i)$. Luego

$$x = \sum_{i=1}^{r} a_i N_i M_i \bmod M.$$

Se tiene que x es solución del sistema de congruencias, puesto que

$$x \equiv \sum_{j=1}^{r} a_j N_j M_j(\operatorname{mod} m_i)$$

pero veamos que

$$N_j M_j(\operatorname{mod} m_i) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

entonces

$$\begin{aligned} x &\equiv a_i N_i M_i(\operatorname{mod} m_i) \\ &\equiv a_i(\operatorname{mod} m_i) \end{aligned}$$

$\square$

Obs: Además de verificar el teorema, la demostración recién vista da un algoritmo eficiente para encontrar las soluciones del sistema de congruencias presentado.

Corolario 3 *Dados $m_1, m_2, ..., m_r$ enteros positivos, relativamente primos a pares, y enteros $a_1, a_2, ..., a_r$ podemos encontrar una solución a las ecuaciones:*

$$\begin{aligned} x &\equiv a_1 (\bmod m_1) \\ x &\equiv a_2 (\bmod m_2) \\ x &\equiv a_3 (\bmod m_3) \\ &\vdots \\ x &\equiv a_r (\bmod m_r) \end{aligned}$$

usando $O((\log m)^2)$ operaciones binarias, donde $m = \prod_{i=1}^{r} m_i$.

Teorema 3 *Enunciado alternativo del Teorema Chino del Resto*

Dados $m_1, m_2, ..., m_r$ enteros positivos, relativamente primos a pares entonces

$$\mathcal{Z}/(m_1 m_2 ... m_r) \cong \mathcal{Z}/(m_1) \oplus \mathcal{Z}/(m_2) \oplus ... \oplus \mathcal{Z}/(m_r)$$

Donde $\oplus$ es la suma directa entre anillos y $\cong$ es isomorfismo de anillos.

Nota:Una versión especial del Teorema Chino del Resto fue dada por Sun Tsu entre los años 280 y 437 d.c, por ello el nombre del teorema.

Es interesante notar que si bien se pueden encontrar soluciones de sistemas de congruencias del tipo $x \equiv a_i (\bmod m_i)$ con $i \epsilon \{1...r\}$ en tiempo polinomial, lo contrario, dada una lista $(x_1, m_1), (x_2, m_2), ..., (x_k, m_k)$ encontrar un x tal que $x \not\equiv x_i (\bmod m_i)$ para todo i, es NP-completo. Este problema es concido como *El Anti-Teorema Chino del Resto*(Bach pp.107).

Teorema 4 *Teorema Chino del Resto Generalizado*

El sistema de congriencias

$$\begin{aligned} x &\equiv a_1 (\bmod m_1) \\ x &\equiv a_2 (\bmod m_2) \\ x &\equiv a_3 (\bmod m_3) \\ &\vdots \\ x &\equiv a_r (\bmod m_r) \end{aligned}$$

tiene solución si y solo si $x_i \equiv x_j (\bmod\ mcd(m_i, m_j))$ para todo $i \neq j$. Si esta solocíón existe, es única (modulo $mcm(m_1, m_2, ..., m_r)$).

Este tororema, en comparación con el Teorema Chino del Resto, nos pide algo más debil, en vez de primos relativos a pares nos pide que los m_i sean congruentes a pares (mod $mcd(m_i, m_j)$). Pero también el resultado es más debil ya que la solución es única *mod* $mcm(m_1, m_2, ..., m_r)$ en vez de ser única *mod* $m_1 m_2 ... mr$ como nos dice el Teorema Chino del Resto.

Ahora que hemos retomado nuestro estudio de Teoría de Números aprovechamos para probar un resultado que habiamos mencionado antes y que concierne a la función φ de Euler.

Lema 1 *La función φ de Euler es multiplicativa, i.e. si m y n son primos relativos*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Dem: La idea de la demostración es identificar cada elemento de $\mathcal{Z}_{mn}^*$ con un único elemento de $\mathcal{Z}_m^* \times \mathcal{Z}_n^*$. Sea $j \in \{1, \ldots, mn\}$ y sean $j_1 = j \bmod n$, $j_2 = j \bmod m$. Notar que j_1 es primo relativo con n si y sólo si j es primo relativo con n. Analogamente, j_2 es primo relativo con n si y sólo si j es primo relativo con n. Luego, por el Teorema Chino del Resto, los $j \in \{1, \ldots, mn\}$ que son primos relativos a mn se pueden asociar 1 a 1 con los pares (j_1, j_2) tales que $j_1 \in \{1, .., n\}$, $j_2 \in \{1, .., m\}$, j_1 es primo relativo con n, y j_2 es primo relativo con m. Sigue que, $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Lema 2 *Para todo n entero positivo, se tiene que $\displaystyle\sum_{d|n} \varphi(d) = n$.*

Dem: Sea $f(n) = \sum_{d|n} \varphi(d)$. Se quiere probar que $f(n) = n$. Notar que la afirmación es evidente si n es primo, pues en este caso $f(n) = \varphi(1) + \varphi(n) = 1 + (n-1)$. Más aun, si $n = p^k$ donde p es primo,

$$f(p^k) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) = p^k.$$

Luego, para concluir que $f(n) = n$ con n arbitrario, bastará aplicar el Teorema Fundamental de la Aritmética y probar que f es una función multiplicativa, i.e. $f(mn) = f(m)f(n)$ si m y n son primos relativos. Sean entonces m y n primos relativos y d un divisor de mn, entonces existen d_1 y d_2 primos relativos (univocamente determinados) tales que $d = d_1 d_2$, $d_1|m$, $d_2|n$. Luego

$$f(mn) = \sum_{d|mn} \varphi(d) = \sum_{d_1|m} \sum_{d_2|n} \varphi(d_1 d_2) = \sum_{d_1|m} \varphi(d_1) \sum_{d_2|n} \varphi(d_2) = f(m)f(n).$$

$\square$