Repaso de Aritmética Modular

Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 13) 23.septiembre.2021

Congruencias

Hacen su aparición en la obra de Gauss, *Disquisitiones Arithmeticae* (1801).

Definición

Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, *con* $n > 1$. *Definimos* $a \equiv b \pmod{n}$ *si, y sólo si,* $n \mid a - b$. *En ese caso, decimos que* a ***es congruente con*** b ***módulo*** n, *o que* a *y* b ***son congruentes módulo*** n.
En caso contrario, escribirmos $a \not\equiv b \pmod{n}$, *y decimos que* a *y* n *no son congruentes módulo* n.

Ejemplo: $17 \equiv 3 \pmod{7}$, $\quad 11 \equiv -4 \pmod{3}$.

Basta calcular que la diferencia entre 17 y 3 es un múltiplo de 7:
$17 - 3 = 14 = 2(7) \qquad \Longrightarrow \qquad 7 \mid 17 - 3.$
Otra forma de verlo es vía el residuo de la división:

$$\tfrac{17}{7} = 2 + \tfrac{3}{7} \qquad \Longrightarrow \qquad 17 \equiv 3 \pmod{7}.$$

Propiedades (Propiedades de las Congruencias)

Para cualesquiera enteros $a, b, c, d, k, n \in \mathbb{Z}$, $n > 1$. *se tiene.*

1. *(Reflexividad)* $a \equiv a \pmod{n}$,
2. *(Simetría) si* $a \equiv b \pmod{n}$, *entonces* $b \equiv a \pmod{n}$,
3. *(Transitividad) Si* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$,
4. *(Compatibilidad con suma y resta)*
$$\begin{cases} a \equiv b & \pmod{n} \\ c \equiv d & \pmod{n} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d & \pmod{n}, \\ a - c \equiv b - d & \pmod{n}, \end{cases}$$
5. *(Compatibilidad con producto)*
$$\begin{cases} a \equiv b & \pmod{n} \\ c \equiv d & \pmod{n} \end{cases} \Rightarrow ac \equiv bd \pmod{n},$$
6. *Si* $a \equiv b \pmod{n}$, *entonces* $ka \equiv kb \pmod{n}$, *para todo* $k \in \mathbb{Z}$,
7. *Si* $a \equiv b \pmod{n}$, *entonces* $a^k \equiv b^k \pmod{n}$, *para* $k \geq 0$.

8. (Cancelación) Si $(n, c) = 1$, entonces $ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n}$.

Prueba: (1.) Para todo $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \mid 0 = a - a \Rightarrow a \equiv a \pmod{n}$.

(2.) $a \equiv b \pmod{n} \Rightarrow n \mid b - a \Rightarrow n \mid a - b \;\; b \equiv a \pmod{n}$.

(3.) $n \mid b - a$, $n \mid c - b \Rightarrow n \mid (b - a) + (c - b) = c - a \Rightarrow a \equiv c \pmod{n}$.

(4.) $n \mid b - a$, $n \mid d - c \Rightarrow n \mid (b - a) \pm (d - c) = (b \pm d) - (a \pm c) \Rightarrow a \pm c \equiv b \pm d \pmod{n}$.

(5.) $n \mid b - a$, $n \mid d - c \Rightarrow n \mid (b - a)c$ y $n \mid a(d - c)$. Luego, $n \mid (b - a)c - a(d - c) = bc - ad \Rightarrow ad \equiv bc \pmod{n}$.

(6.) Aplicando (4.) k-veces consecutivas, con $c = a$, $d = b$, se obtiene, $ka \equiv kb \pmod{n}$.

(7.) Aplicando (5.) k-veces consecutivas, con $c = a$, $d = b$, se obtiene, $a^k \equiv b^k \pmod{n}$. Otra alternativa es ver que si $a \equiv b \pmod{n}$, entonces $n \mid b - a$ $\Rightarrow n \mid (b - a)(b^{k-1} + ab^{k-1} + \ldots + a^{k-2}b + a^{k-1}) = b^k - a^k$. Así, $a^k \equiv b^k \pmod{n}$.

(8.) Suponga que $ac \equiv bc \pmod{n}$, con $(n, c) = 1$. Entonces $n \mid bc - ac = (b - a)c$. Por el lema de Eulices, como $(n, c) = 1$, entonces $n \mid b - a \Rightarrow a \equiv b \pmod{n}$. $\square$

Congruencias

Obs! Dados $a \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$, por el Algoritmo de la División, existen $q, r \in \mathbb{Z}$ tales que $a = qn + r$, con $0 \leq r < n$. Entonces, por definición de congruencia, $n \mid -qn = r - a$ $\Rightarrow \; a \equiv r \pmod{n}$. Porque hay n opciones para r, vemos que todo entero es congruente módulo n exactamente con uno de los valores residuos $0, 1, 2, \ldots n-1$; en particular, $a \equiv 0 \pmod{n}$ si, y sólo si, $n \mid a$.

Definición

*El conjunto de n enteros $0, 1, 2, \ldots, n-1$ se denomina el **conjunto de residuos mínimos no negativos** o **residuos canónicos**, módulo n.*
*En general, una colección de n números enteros $a_1, a_2, \ldots, a_n$ forman un **conjunto completo de residuos** (o un **sistema completo de residuos**) módulo n si cada a_i es congruente a alguno de los números $0, 1, 2, \ldots, n-1$, módulo n.*

Ejemplo: $-12, -4, 11, 13, 22, 82, 91$ constituyen un sistema completo de residuos módulo 7.

Obs! $S = \{a_i\}_{i=1}^{n} \subset \mathbb{Z}$ es un sistema de residuos módulo $n \iff a_i \not\equiv a_j \pmod{n}$, para $i \neq j$.

Teorema

Para enteros arbitrarios $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n} \Leftrightarrow$ a y b dejan el mismo residuo cuando se divide por n.

Prueba: $(\Rightarrow)$ Si $a \equiv b \pmod{n}$, de modo que $n \mid b - a$ y $b = a + kn$ para algún entero k. Suponga que en la división entre n, a deja un cierto residuo r; es decir, $ab = qn + r$, con $0 \leq r < n$. Por lo tanto, $b = a + kn = (qn + r) + kn = (q + k)n + r$, por lo que b tiene el mismo residuo que a.
$(\Leftarrow)$ Por otro lado, suponga que podemos escribir $b = q_1 n + r$ y $b = q_2 n + r$, con el mismo residuo $0 \leq r < n$ Entonces,

$$b - a = (q_2 n + r) - (q_1 n + r) = (q_2 - q_1)n,$$

de modo que $n \mid b - a$. Esto es $a \equiv b \pmod{n}$. $\square$

Ejemplo: -56 y -11 pueden escribirse como $-56 = (-7)9 + 7$, $-11 = (-2)9 + 7$. Esto muestra que $-56 \equiv -11 \pmod{9}$.

Vimos que una de las propiedades básicas de congruencias es que si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \pmod{n}$, siempre que $(c, n) = 1$. Cuando $(c, n) \neq 1$ la cancelación en general no vale. Por ejemplo, $2(4) \equiv 2(1) \pmod{6}$, pero $4 \not\equiv 1 \pmod{6}$.

Con las precauciones adecuadas, se puede permitir la cancelación

Teorema

Si $ca \equiv cb \pmod{n}$, entonces $a \equiv b \pmod{\frac{n}{d}}$, donde $d = (c, n)$.

Prueba: Por hipótesis, $n \mid cb - ca$ y podemos escribir $c(b-a) = cb - ca = kn$, para algún $k \in \mathbb{Z}$. Como $(c, n) = d$, existen enteros primos relativos r, s que satisfacen $c = dr$, $n = ds$. Sustituyendo en la ecuación anterior,

$$dr(b-a) = kds \qquad \Rightarrow \qquad r(b-a) = ks,$$

de modo que $s \mid r(b-a)$. Como $(r, s) = 1$, el Lema de Euclides garantiza que $s \mid b - a$. Portanto, $a \equiv b \pmod{s}$; en otras palabras, $a \equiv b \pmod{\frac{n}{d}}$. $\square$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Corolario

Si $ca \equiv cb \pmod{n}$, *y* $(c, n) = 1$, *entonces* $a \equiv b \pmod{n}$. $\square$

Corolario

Si $ca \equiv cb \pmod{p}$, *y* $p \nmid c$, *con* p *primo, entonces* $a \equiv b \pmod{p}$.

<u>Prueba</u>: Las condiciones p primo y $p \nmid c$ implican que $(c, p) = 1$. $\square$

Ejemplo: Considere la congruencia $42 \equiv 15 \pmod{27}$. Como $(3, 27) = 3$, debido al teorema anterior podemos "cancelar" el factor 3 en la congruencia. Así $14 =\equiv 5 \pmod{9}$. Una ilustración adicional es la congruencia $-35 \equiv 45 \pmod{8}$. Aquí, 5 y 8 son primos relativos, y podemos cancelar el factor 5 para obtener $-7 \equiv 9 \pmod{8}$.

Obs! En el teorema, no es necesario que $c \not\equiv 0 \pmod{n}$, pues en ese caso tendríamos $c \equiv 0 \pmod{n} \Rightarrow (c, n) = n$, y la conclusión sería $a \equiv b \pmod{1}$, se mantiene automáticamente para todos entero a y b.

Ejemplos

Ejemplo: Hallar el residuo de la división $5^{3^{20}}$ entre 13.

Solución:
$5^4 \equiv 1 \pmod{13}$. Además, los residuos de dividir 5^n por 13 se repiten en ciclos de 4:

$$\begin{aligned} 5^0 &\equiv 1 \pmod{13}, & 5^4 &\equiv 1 \pmod{13},\\ 5^1 &\equiv 5 \pmod{13}, & 5^5 &\equiv 5 \pmod{13},\\ 5^2 &\equiv -1 \pmod{13}, & 5^6 &\equiv -1 \pmod{13},\\ 5^3 &\equiv -5 \pmod{13}, & 5^7 &\equiv -5 \pmod{13}, \ \ldots \end{aligned}$$

Por otro lado, tenemos que $3 \equiv -1 \pmod{4}$, de modo que $3^{20} \equiv (-1)^{20} \equiv 1 \pmod{4}$. Esto es, 3^{20} deja residuo 1 al dividirse por 4. Así, $5^{3^{20}} \equiv 5^1 \equiv 5 \pmod{13}$.

Ejercicio: Hallar el residuo de la división de 3^{1000} entre 101.

Potenciación Binaria

Aplicación: Cálculo de potencias grandes módulo n.

Con frecuencia deseamos calcular el valor de una potencia $a^k \pmod n$, cuando k es grande. ¿Existe una forma eficiente de obtener este cálculo?

Uno de esos procedimientos, es llamado el **algoritmo exponencial binario**, y se basa en elevar al cuadrado de forma sucesiva, módulo n.
Más específicamente, el exponente k se escribe en forma binaria, como

$$k = (a_m a_{m-1} \cdots a_2 a_1 a_0)_2 = \sum_{k=0}^{m} a_k d^k,$$

y los valores $a^{2^j} \pmod n$ se calculan para las potencias de 2, que corresponden a los 1's en la representación binaria de k. Estos resultados parciales luego se multiplican para dar la respuesta final.

Potenciación Binaria

Ejemplo: Calcular $5^{110} \pmod{131}$.

Primero, expresamos el exonente 110 en base 2 como

$$110 = 64 + 32 + 8 + 4 + 2 = 2^6 + 2^5 + 2^3 + 2^2 + 2^1 = (1101110)_2.$$

Obtenemos ahora las potencias de $5^{2^j} \pmod{131}$, correspondientes a los 1's en la representación anterior:

$$\begin{aligned}
5^2 &\equiv 25 \pmod{131}, \\
5^4 &\equiv 25^2 \equiv 625 \equiv 101 \pmod{131}, \\
5^8 &\equiv 101^2 \equiv 10201 \equiv 114 \pmod{131}, \\
5^{16} &\equiv 114^2 \equiv 12996 \equiv 27 \pmod{131}, \\
5^{32} &\equiv 27^2 \equiv 729 \equiv 74 \pmod{131}, \\
5^{64} &\equiv 74^2 \equiv 5476 \equiv 105 \pmod{131}.
\end{aligned}$$

Potenciación Binaria

Multiplicamos ahora los resultados parciales, correspondientes a los 1's en la expansión binaria del exponente

$$5^{110} = 5^{64} \cdot 5^{32} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131}.$$

Como una variación del procedimiento anterior, se podrían calcular módulo 131, las potencias $5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ para llegar al resultado

$$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^{2} \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131},$$

lo que requeriría menos multiplicaciones.

Potenciación Binaria

Algoritmo: (Potenciación Binaria).
Inputs: $x, k, n \in \mathbb{N}$ números naturales, $k \geq 0$, $n > 1$, donde x es la base, k es la potencia, y n es el módulo.
Outputs: $\texttt{result} = x^k \pmod{n}$,

```
Initialize answer result = 1,
# repeat until k becomes 0
while (y > 0):
    If (y % 2 == 1):
        result = (result * x) % n,
    # binary shift to half y (y = y//2
    y = y » 1,
    # change x to x^2
    x = (x*x) % n,
return result.
```


UNIVERSIDAD DEL VALLE DE GUATEMALA