TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

4.2 Propiedades Básicas de Congruencias

En el primer capítulo de *Disquisitiones Arithmeticae*, Gauss introduce el concepto de congruencia y la notación que lo hace una técnica tan poderosa (el explica que fue inducido a adoptar el símbolo $\equiv$ debido a su estrecha analogía con igualdad algebraica). Según Gauss, "Si un número mide la diferencia entre dos números a y b, entonces se dice que a y b son congruentes con respeto a n; si no, incongruentes." Poniendo esto en la forma de definición,

Definición 4.1. Sea n un entero fijo. Se dice que dos enteros a y b son *congruentes módulo n*, simbolizado por

$$a \equiv b \pmod{n}$$

si n divide a la diferencia $a - b$; es decir, que $a - b = kn$ por algún entero k.

Para fijar la idea, consideramos $n = 7$. Es rutinario comprobar que

$$3 \equiv 24 \pmod{7} \qquad -31 \equiv 11 \pmod{7} \qquad -15 \equiv -64 \pmod{7}$$

como $3-24 = (-3)7$, $-31-11 = (-6)7$, y $-15-(-64) = 7\cdot 7$. Cuando $n \nmid (a-b)$, se dice que a es *incongruente a b módulo n*, y en este caso escribimos $a \not\equiv b \pmod{n}$. Por un ejemplo simple, $25 \not\equiv 12 \pmod{7}$, como 7 no divide $25 - 12 = 13$.

Es de notar que cualquier dos enteros son congruentes módulo 1, mientras dos enteros son congruentes módulo 2 cuando son ambos pares o ambos impares. Ya que la congruencia módulo 1 no es particularmente interesante, la práctica habitual es suponer que $n > 1$.

Dado un entero a, sea q y r su cociente y resto al dividir por n, de modo que

$$a = qn + r \qquad 0 \leq r < n$$

Luego, por la definición de congruencia, $a \equiv r \pmod{n}$. Como hay n opciones para r, veamos que cada entero es congruente módulo n a exactamente uno de los valores $0, 1, 2, \ldots, n-1$; en particular, $a \equiv 0 \pmod{n}$ si y solo si $n|a$. El conjunto de n enteros $0, 1, 2, \ldots, n-1$ se llama el conjunto de *mínimos residuos no negativos módulo n.*

En general, de dice que una colección de enteros $a_1, a_2, \ldots, a_n$ forma un *conjunto completo de residuos módulo n* si cada entero es equivalente módulo n a uno y solo uno de los a_k. Para decirlo de otra manera, $a_1, a_2, \ldots, a_n$ son congruentes módulo

n a $0, 1, 2, \ldots, n-1$, tomado en algún orden. Por ejemplo,

$$-12, -4, 11, 13, 22, 82, 91$$

constituyen un conjunto completo de residuos módulo 7; aquí, tenemos

$$-12 \equiv 2 \qquad -4 \equiv 3 \qquad 11 \equiv 4 \qquad 13 \equiv 6 \qquad 22 \equiv 1 \qquad 82 \equiv 5 \qquad 91 \equiv 0$$

todos módulo 7. Una observación de cierta importancia es que cualquier n enteros forman un conjunto completo de residuos módulo n si y solo si no hay dos de ellos congruentes módulo n. Este hecho necesitaremos más tarde.

Nuestro primer teorema provee una caracterización útil de congruencia módulo n en términos de restos al dividir por n.

Teorema 4.1. Para enteros arbitrarios a y b, $a \equiv b \pmod{n}$ si y solo si a y b tienen el mismo resto no negativo al dividir por n.

Demostración: Primero, tomemos $a \equiv b \pmod{n}$, de modo que $a = b + kn$ por algún entero k. Al dividir por n, b tiene un cierto resto r; es decir, $b = qn + r$, en donde $0 \leq r < n$. Entonces,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

lo cual indica que a tiene el mismo resto que b.

Por otro lado, suponemos que podemos escribir $a = q_1 n + r$ y $b = q_2 n + r$, con el mismo resto r $(0 \leq r < n)$. Entonces

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

de donde $n|a - b$. En el lenguaje de congruencia, tenemos $a \equiv b \pmod{n}$.

Ejemplo 4.1. Como se puede expresar los enteros -56 y -11 en la forma

$$-56 = (-7)9 + 7 \qquad -11 = (-2)9 + 7$$

con el mismo resto 7, el Teorema 4.1 nos dice que $-56 \equiv -11 \pmod{9}$. En la otra dirección, la congruencia $-31 \equiv 11 \pmod{7}$ implica que -31 y 11 tienen el mismo resto al dividir por 7; esto es claro de las relaciones

$$-31 = (-5)7 + 4 \qquad 11 = 1 \cdot 7 + 4$$

Se puede ver congruencia como una forma generalizada de igualdad, en el sentido que su comportamiento con respeto a la adición y la sustracción recorda a la igualdad ordinaria. Algunas de las propiedades que se transfieren aparecen en el siguiente teorema.

Teorema 4.2. Sea $n > 1$ fijo y a, b, c enteros arbitrarios. Entonces las siguientes propiedades son ciertas:

a) $a \equiv a \pmod{n}$.

b) Si $a \equiv b \pmod{n}$, entonces $b \equiv a \pmod{n}$.

c) Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.

d) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{n}$ y $ac \equiv bd \pmod{n}$.
e) Si $a \equiv b \pmod{n}$, entonces $a + c \equiv b + c \pmod{n}$ y $ac \equiv bc \pmod{n}$.
f) Si $a \equiv b \pmod{n}$, entonces $a^k \equiv b^k \pmod{n}$ para todo entero positivo k.

Demostración: Para cualquier entero a, tenemos $a - a = 0 \cdot n$, de modo que $a \equiv a \pmod{n}$. Ahora si $a \equiv b \pmod{n}$, entonces $a - b = kn$ por algún entero k. Entonces, $b - a = -(kn) = (-k)n$ y como $-k$ es un entero, esto produce la propiedad b).

La propiedad c) es ligeramente menos obvia: Supongamos que $a \equiv b \pmod{n}$ y también $b \equiv c \pmod{n}$. Entonces existen enteros h y k que satisfacen $a - b = hn$ y $b - c = kn$. Resulta que

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

lo cual es $a \equiv c \pmod{n}$ en la notación de equivalencia.

En la misma manera, si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces estamos seguros de que $a - b = k_1 n$ y $c - d = k_2 n$ para alguna elección de k_1 y k_2. Sumando estas ecuaciones, obtenemos

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 = k_2)n\end{aligned}$$

o, como una declaración de congruencia, $a + c \equiv b + d \pmod{n}$. En cuanto a la segunda afirmación de la propiedad d), nota que

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Como $bk_2 + dk_1 + k_1 k_2 n$ es un entero, esta dice que $ac - bd$ es divisible por n, de donde $ac \equiv bd \pmod{n}$.

La demostración de e) está cubierto por d) y el hecho que $c \equiv c \pmod{n}$. En fin, obtenemos la propiedad f) al hacer un argumento de inducción. La afirmación ciertamente es válida para $k = 1$, y supondremos es cierta para algún k fijo. De d), sabemos que $a \equiv b \pmod{n}$ y $a^k \equiv b^k \pmod{n}$ juntos implican que $aa^k \equiv bb^k \pmod{n}$, o equivalentemente $a^{k+1} \equiv b^{k+1} \pmod{n}$. Esto es la forma la afirmación debería tomar para $k + 1$, y entonces el paso de inducción está completo.

Antes de ir más lejos, deberíamos ilustrar que las congruencias pueden ayudar mucho en realizar ciertos tipos de computaciones.

Ejemplo 4.2. Esforcémonos a mostrar que 41 divide a $2^{20} - 1$. Empezamos notando que $2^5 \equiv -9 \pmod{41}$, de donde $(2^5)^4 \equiv (-9)^4 \pmod{41}$ por el Teorema 4.2f); en otras palabras, $2^{20} \equiv 81 \cdot 81 \pmod{41}$. Pero $81 \equiv -1 \pmod{41}$, y entonces $81 \cdot 81 \equiv 1 \pmod{41}$. Utilizando los partes b) y e) del Teorema 4.2, en fin llegamos a

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$$

Por lo tanto, $41|2^{20} - 1$, como se desee.

Ejemplo 4.3. Para otro ejemplo en el mismo espíritu, supongamos que se nos pide que hallar el resto obtenido al dividir la suma

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

por 12. Si la ayuda de las congruencias, este sería un cálculo asombroso. La observación que nos pone en marcha es que $4! \equiv 24 \equiv 0 \pmod{12}$; entonces, para $k \geq 4$,

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$$

De esta manera, encontramos que

$$\begin{aligned} 1! + 2! + 3! &+ 4! + \cdot + 100! \\ &\equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12} \end{aligned}$$

En consecuencia, la suma en cuestión deja un resto de 9 al dividir por 12.

En el Teorema 4.1 vimos que si $a \equiv b \pmod{n}$, entonces $ca \equiv cb \pmod{n}$ para cualquier entero c. El reciproco, sin embargo, no se cumple. Por ejemplo, tal vez tan simple como cualquier, nota que $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, mientras $4 \not\equiv 1 \pmod{6}$. En resumen, no se puede cancelar un factor común sin restricciones en la aritmética de las congruencias.

Con las precauciones adecuadas, se puede permitir la cancelación; un paso en esta dirección, y uno importante, lo proporciona el siguiente teorema.

Teorema 4.3. Si $ca \equiv cb \pmod{n}$, entonces $a \equiv b \pmod{n/d}$, en donde $d = \text{mcd}(c, n)$.

Demostración: Por hipótesis, podemos escribir

$$c(a - b) = ca - cb = kn$$

por algún entero k. Al saber que $\text{mcd}(c, n) = d$, existen enteros coprimos r y s que satisfacen $c = dr$, $n = ds$. Cuando se sustituye estas valores en la ecuación mostrada y se cancela el factor común d, el resultado es

$$r(a - b) = ks$$

Entonces $s|r(a - b)$ y $\text{mcd}(r, s) = 1$. El Lema de Euclides produce $s|a - b$, que se puede escribir como $a \equiv b \pmod{s}$; en otras palabras, $a \equiv b \pmod{n/d}$.

El teorema obtiene su fuerza máxima cuando se suma el requisito que $\text{mcd}(c, n) = 1$, pues entonces se puede realizar la cancelación sin cambiar el módulo.

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

Tomamos un momento para registrar un caso especial del Corolario 1 que tendremos ocasión de utilizar con frecuencia, a saber, el Corolario 2.

Corolario 2. Si $ca \equiv cb \pmod{p}$ y $p \nmid c$, entonces $a \equiv b \pmod{p}$.

Demostración: Las condiciones $p \nmid c$ y p un primo implican que $\text{mcd}(c, p) = 1$.

Ejemplo 4.4. Consideramos la congruencia $33 \equiv 15 \pmod{9}$ o, si se prefiere, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Como $\text{mcd}(3, 9) = 3$, el Teorema 4.3 nos conduce a la conclusión que $11 \equiv 5 \pmod{3}$. Una ilustración más está dada por la congruencia $-35 \equiv 45 \pmod{8}$, que es lo mismo que $5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}$. Los enteros 5 y 8 siendo coprimos, podemos cancelar el factor 5 para obtener la congruencia correcta $-7 \equiv 9 \pmod{8}$.

Llamemos la atención sobre el hecho que, en el Teorema 4.3, no es necesario estipular que $c \not\equiv 0 \pmod{n}$. De hecho, si $c \equiv 0 \pmod{n}$, entonces $\text{mcd}(c, n) = n$ y la conclusión del teorema declararía que $a \equiv b \pmod{1}$; pero como observamos antes, esto es trivialmente cierto para todos enteros a y b.

Hay otra situación curiosa que puede surgir con las congruencias. El producto de dos enteros, ninguno de los cuales es congruente a cero, puede resultar ser cero. Por ejemplo, $4 \cdot 3 \equiv 0 \pmod{12}$, pero $4 \not\equiv 0 \pmod{12}$ y $3 \not\equiv 0 \pmod{12}$. Es un asunto sencillo de mostrar que si $ab \equiv 0 \pmod{n}$ y $\text{mcd}(a, n) = 1$, entonces $b \equiv 0 \pmod{n}$: el Corolario 1 nos permite legítimamente cancelar el factor a de ambos lados de la congruencia $ab \equiv a \cdot 0 \pmod{n}$. Una variación de esto es cuando $ab \equiv 0 \pmod{p}$, con p un primo, entonces o $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$.

PROBLEMAS 4.2

1. Demostrar cada uno de los siguientes afirmaciones:
a) Si $a \equiv b \pmod{n}$ y $m|n$, entonces $a \equiv b \pmod{m}$.
b) Si $a \equiv b \pmod{n}$ y $c > 0$, entonces $ca \equiv cb \pmod{cn}$.
b) Si $a \equiv b \pmod{n}$ y los enteros a, b, n todos son divisibles por $d > 0$, entonces $a/d \equiv b/d \pmod{n/d}$.

2. Dar un ejemplo para mostrar que $a^2 \equiv b^2 \pmod{n}$ no tiene por qué implicar que $a \equiv b \pmod{n}$.

3. Si $a \equiv b \pmod{n}$, demostrar que $\text{mcd}(a, n) = \text{mcd}(b, n)$.

4. a) Hallar los restos cuando se dividen 2^{50} y 41^{65} por 7.
b) ¿Cual es el resto cuando se divide la siguiente suma por 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

5. Demostrar que el entero $53^{103} + 103^{53}$ es divisible por 39, y que $111^{333} + 333^{111}$ es divisible por 7.

6. Para $n \geq 1$, utilizar la teoría de congruencias para establecer cada uno de los

siguientes declaraciones de divisibilidad:
a) $7|5^{2n} + 3 \cdot 2^{5n-2}$.
b) $13|3^{n+2} + 4^{2n+1}$.
c) $27|5^{2n+1} + 5^{n+2}$.
d) $43|6^{n+2} + 7^{2n+1}$.

7. Para $n \geq 1$, demostrar que

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

[Consejo: Nota que $(-13)^2 \equiv -13 + 1 \pmod{181}$; usar inducción en n.]

8. Demostrar las siguientes afirmaciones:
a) Si a es un entero impar, entonces $a^2 \equiv 1 \pmod 8$.
b) Para cualquier entero a, $a^3 \equiv 0, 1, \text{ o } 6 \pmod 7$.
c) Para cualquier entero a, $a^4 \equiv 0 \text{ o } 1 \pmod 5$.
d) Si el entero a no es divisible por 2 o 3, entonces $a^2 \equiv 1 \pmod{24}$.

9. Si p es un primo que satisface $n < p < 2n$, demostrar que

$$\binom{2n}{n} \equiv 0 \pmod p.$$

10. Si $a_1, a_2, \ldots, a_n$ es un conjunto completo de residuos módulo n y $\text{mcd}(a, n) = 1$, demostrar que $aa_1, aa_2, \ldots aa_n$ también es un conjunto completo de residuos módulo n.
[Consejo: Es suficiente mostrar que los números en cuestión son incongruentes módulo n.]

11. Verificar que $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ forman un conjunto completo de residuos módulo 11, pero $0, 1^2, 2^2, 3^2, \ldots, 10^2$ no.

12. Demostrar los siguientes declaraciones:
a) Si $\text{mcd}(a, n) = 1$, entonces los enteros

$$c, c + a, c + 2a, c + 3a, \ldots, c + (n - 1)a.$$

forman un conjunto completo de residuos módulo n para cualquier c.
b) Cualquier n enteros consecutivos forman un conjunto completo de residuos módulo n.
[Consejo: Utilizar parte a).]
c) El producto de cualquier conjunto de n enteros consecutivos es divisible por n.

13. Verificar que si $a \equiv b \pmod{n_1}$ y $a \equiv b \pmod{n_2}$, entonces $a \equiv b \pmod n$, en donde $n = \text{mcm}(n_1, n_2)$. Por lo tanto, cuando n_1 y n_2 son coprimos, $a \equiv b \pmod{n_1 n_2}$.

14. Dar un ejemplo para mostrar que $a^k \equiv b^k \pmod{n}$ y $k \equiv j \pmod{n}$ no implican necesariamente que $a^j \equiv b^j \pmod{n}$.

15. Establecer que si a es un entero impar, entonces para cualquier $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

[Consejo: Proceder por inducción en n.]

16. Utilizar la teoría de congruencias para verificar que

$$89|2^{44} - 1 \qquad \text{y} \qquad 97|2^{48} - 1$$

17. Demostrar que siempre que $ab \equiv cd \pmod{n}$ y $b \equiv d \pmod{n}$, con $\text{mcd}(b, n) = 1$, entonces $a \equiv c \pmod{n}$.

18. Si $a \equiv b \pmod{n_1}$ y $a \equiv c \pmod{n_2}$, demostrar que $b \equiv c \pmod{n}$, en donde el entero $n = \text{mcd}(n_1, n_2)$.