Semana 8: Congruencias

1. Definición de congruencia

Comenzaremos describiendo una forma de presentar algunos resultados relacionados con la divisibilidad a través de definir una relación sobre los enteros.

Definición 8.1. Sea $m > 1$ un número natural . Para dos enteros a y b, diremos que *a es congruente con b módulo m* si y sólo si $a - b$ es un múltiplo de m. En símbolos, escribiremos

$$a \equiv b \mod m.$$

Vamos a establecer una convención respecto a las posibles relaciones que resultan para la elección de m. Primero notamos que cualquier número es divisible por 1, por lo que la relación módulo 1 no es muy interesante, ni tampoco la de los números negativos, pues con su parte positiva se puede conseguir el mismo resultado. Es por esta razón que, cuando no se especifique, el número m se asumirá $m > 1$ cuando se hable de congruencias.

Es importante plantearse la razón de ser de este nuevo concepto, pues uno puede pensar de manera poco acertada que es sólo una nueva forma de hablar acerca de la divisibilidad, pues $a \equiv 0$ mód m si y sólo si $m \mid a$. En su lugar, su intención es proveer una notación bastante sugestiva para

$$m \mid a - b.$$

Esta expresión de no debe parecer ajena pues el teorema de la división nos da un caso de esta forma. Veamos cómo.

Proposición 8.1. *Para cada entero $a > 1$, existe un único entero $0 \leq r < m$ tal que*

$$a \equiv r \mod m.$$

Demostración. Como se comentó, esto será resultado del teorema de la división. Dicho teorema, garantiza la existencia de un único par de números q y $0 \leq r < m$ de forma que

$$a = qm + r,$$

en otras palabras $m \mid a - r$ y en consecuencia $a \equiv r \mod m$. Este número debe ser único pues cualquier otro número con la propiedad que buscamos resulta ser simplemente el residuo de la misma división. Esto es lo que afirma el resultado. ■

Esta última proposición es provocativa: a, de alguna forma, está representado por el residuo de dividirlo entre m. Al menos parece contener toda la información necesaria para definir la relación módulo m. De hecho, la proposición nos permite decir que cualquier entero $r + (\text{múltiplo de } m)$ debe ser equivalente con a módulo m. Esta apariencia se confirma en el siguiente resultado.

Proposición 8.2. *Sean a y b enteros y sean también r_1 y r_2 los residuos de dividir a entre m y b entre m, respectivamente. Entonces $a \equiv b \mod m$ si y sólo si $r_1 = r_2$.*

Demostración. Muy parecido al caso anterior, escribimos $a = q_1 m + r_1$ y $b = q_2 m + r_2$ donde los residuos satisfacen $0 \leq r_1, r_2 < m$. Ahora, si $r_1 = r_2$, entonces

$$a - q_1 m = b - q_2 m$$

o en otras palabras

$$a - b = (q_1 - q_2)m$$

por lo que $a \equiv b \mod m$.

Si por el contrario $a \equiv b \mod m$, entonces $a - b = km$ para algún k. En ese caso

$$a = km + b = km + q_2 m + r_2 = (k + q_1)m + r_2,$$

como $r_2 < m$, éste debe ser el residuo indicado por el algoritmo de la división, luego $r_1 = r_2$. ■

La proposición anterior puede resultar increíblemente sencilla de probar si se sabe de antemano que la relación módulo resulta una relación de equivalencia lo cual ya hemos tenido oportunidad de probar con anterioridad.

2. Propiedades principales

Teorema 8.3. *Para cualesquiera enteros a, b, c y d se verifica:*

1. *Si $a \equiv b \mod m$, entonces $ca \equiv cb \mod m$, para todo entero c.*
2. *Si $a \equiv b$ y $c \equiv d \mod m$, entonces $a + c \equiv b + d$ y $ac \equiv bd \mod m$.*

Demostración. Estos resultados son inmediatos de las definiciones y se probará solamente 1. Supongamos con este objetivo que $a \equiv b \mod m$; en ese caso, existe un número k de forma que $a - b = km$. Entonces,

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

por lo que $m \mid ca - cb$ y como consecuencia de la definición, $ca \equiv cb \mod m$. ■

Hay muchas propiedades que nos permiten cambiar el módulo y dar afirmaciones sin esfuerzo alguno. Una muy interesante está contenida en el siguiente lema.

Lema 8.4. *Para un natural $n > 1$ se tiene que*

1. *Si $n \mid m$ y $a \equiv b \mod m$, entonces $a \equiv b \mod n$.*
2. *Si $a \equiv b \mod m$ y $a \equiv b \mod n$, entonces $a \equiv b \mod [m, n]$.*

Demostración. Para probar 1, sólo es necesario seguir las propiedades de la divisibilidad: Por hipótesis $n \mid m$ y $m \mid a - b$, como la divisibilidad es transitiva, entonces $n \mid a - b$ y en consecuencia $a \equiv b \mod n$.

La prueba de 2, es una simple observación de la definición del mínimo común múltiplo: Por hipótesis $a - b$ es un múltiplo de m y de n, entonces $a - b$ es también múltiplo de $[m, n]$ por lo que $a \equiv b \mod [m, n]$. ■

La siguiente definición es sólo una conveniencia, es importante notar que no es una operación nueva, ni refiere de forma alguna a los inversos multiplicativos, es sólo una manera de hacer referencia al cociente de una división cuando ésta no presenta residuo. La única razón por la que se introduce es para simplificar algunas expresiones y se debe tratar con sumo cuidado hasta que se comprenda la diferencia.

Definición 8.2. Si $a \mid b$, al único número q tal que $b = qa$ se le denotará por b/a o $\frac{b}{a}$.

Proposición 8.5. *Para un natural $n > 1$ se tiene que:*

1. *Si $na \equiv nb \mod nm$, entonces $a \equiv b \mod m$.*
2. *Si $na \equiv nb \mod m$ y $(m,n) = 1$, entonces $a \equiv b \mod m$.*
3. *Si $na \equiv nb \mod m$, entonces $a \equiv b \mod \frac{m}{(m,n)}$.*

Demostración. Para probar 1, suponemos que $na \equiv nb \mod nm$, lo que por definición significa que $nm \mid na - nb$ o en otras palabras,

$$n(a-b) = n(qm),$$

lo que por ley de cancelación implica que $m \mid a - b$ y consecuencia $a \equiv b \mod m$.

Para probar 2, aparte de suponer que $na \equiv nb \mod m$, debemos notar que $na \equiv nb \mod n$; de acuerdo al lema 8.4, se debe tener que

$$na \equiv nb \mod [m,n],$$

pero como $(m,n) = 1$ debemos tener que $mn = [m,n]$; esto nos lleva directamente a la congruencia

$$na \equiv nb \mod mn$$

y por 1, debemos concluir que

$$a \equiv b \mod m.$$

Para probar 3, usamos la congruencia que se obtuvo en el primer paso del párrafo anterior, i.e.,

$$na \equiv nb \mod [m,n]$$

Ahora, tomamos q como el único entero tal que $m = q(m,n)$, en ese caso tenemos

$$[m,n](m,n) = mn = nq(m,n)$$

y como m y n son enteros > 1, la ley de cancelación garantiza que

$$nq = [m,n],$$

esto se traduce en tener

$$na \equiv nb \mod nq;$$

de nueva cuenta por 1, y como $q = m/(m,n)$,

$$a \equiv b \mod \frac{m}{(m,n)}.$$ ∎

3. El teorema chino del residuo

Hemos desenredado algunas de las propiedades de las congruencias. Sin embargo, hemos de notar que sólo son reformulaciones de los resultados que hemos presentado sobre divisibilidad, que resulta en un lenguaje nuevo para hablar de lo mismo. Entonces, ¿cuál es la ventaja de presentarlo de esta manera? Se podrá notar que el símbolo para la congruencia $\equiv$ guarda similitud con el de igualdad, esto por supuesto no es una coincidencia. La ventaja de presentar los conceptos de divisibilidad a través de congruencias resulta en que podemos plantear ecuaciones usando esta nueva "igualdad". Por ejemplo, al preguntar si podemos encontrar un número x de forma que

$$x + 2 \equiv 3 \mod 5.$$

En este caso basta notar que estamos buscando números $x \equiv 1 \mod 5$ los cuales, por la proposición 8.1 son aquellos números que tienen residuo 1 al dividir por 5, de manera explícita, las soluciones son el conjunto

$$\{q \cdot 5 + 1 \mid q \in \mathbb{Z}\}.$$

Como podemos ver, las propiedades de congruencia nos permiten resolver de manera sencilla las ecuaciones del tipo $x + a \equiv b \mod m$. Podemos preguntarnos qué sucede con las congruencias del tipo

$$ax \equiv b \mod m.$$

Si éstas fueran una igualdad, lo que debemos encontrar es un entero x de forma que $ax = b$, en otras palabras buscamos responder si $a \mid b$. Pero al ser congruencias, lo que buscamos es un entero x de forma que $b = ax + n$, donde n es un múltiplo de m, o de manera equivalente si podemos encontrar enteros x y y de forma que $b = ax + my$. Si traemos de vuelta los conceptos de divisibilidad, sabemos como resolver esas ecuaciones: Como b es una combinación lineal de a y m, entonces las soluciones se pueden garantizar a condición que (a, m) divida a b. Si este es el caso, la identidad de Bézout nos dice como proceder. Ilustremos esto con un par de ejemplos.

Ejemplo. Consideremos primero la congruencia

$$3x \equiv 4 \mod 12.$$

En ese caso $(3, 12) = 3$, sin embargo, si suponemos que la congruencia tiene solución, entonces podemos expresar

$$3x - 4 = 12q$$

para algunos x y q enteros. Esto quiere decir que 4 es una combinación lineal de 3 y 12 por lo que debería ser divisible por cualquier divisor común de estos, en particular de 3, pero $3 \nmid 4$ por lo que asumir que tiene solución deriva en contradicción. Debemos entonces suponer que la congruencia no tiene solución.

Ejemplo. Supongamos ahora la congruencia

$$20x \equiv 5 \mod 15,$$

en ese caso $(15, 20) = 5$ el cual es múltiplo de 5 y ocupando la identidad de Bézout podemos expresar $5 = 1 \cdot 20 + (-1) \cdot 15$ y en consecuencia $x = 1$ es una solución para la congruencia que buscamos. Además no es difícil verificar que $x = 4$ es otra posible solución, en realidad cualquier suma de 1 con un múltiplo de 3 es una solución (¡compruébalo!).

Por particulares que parezcan los ejemplos, son lo suficimiente ilustrativos para plantear un método general. Maravilloso. Para estructura dicho método, seguiremos los pasos que hemos realizado ya en los ejemplos pero de manera abstracta.

Definición 8.3. Dos enteros a y b que satisfacen $(a, b) = 1$ se dicen *primos entre sí.*

Teorema 8.6. *Si a y b son primos entre sí, entonces tiene solución la congruencia*

$$ax + b \equiv 0 \mod m.$$

Además, cualesquiera dos soluciones x_1 y x_2 satisfacen

$$x_1 \equiv x_2 \mod m.$$

Demostración. Comencemos notando que al ser $(a, m) = 1$, la identidad de Bézout garantiza la existencia de enteros s y t de forma que

$$sa + tm = 1$$

por lo que debemos tener

$$bsa + btm = b$$

y en consecuencia

$$(-bs)a + b = btm$$

o en términos de congruencias

$$(-bs)a + b \equiv 0 \mod m$$

por lo que elegir $x = -bs$ resulta una solución de la congruencia.

Para probar la segunda parte supongamos que dos números x_1 y x_2 son soluciones de la congruencia, i.e.,

$$ax_1 \equiv -b \mod m$$
$$ax_2 \equiv -b \mod m$$

Por ser la relación transitiva y simétrica, debemos tener que

$$ax_1 \equiv ax_2 \mod m$$

y como $(a, m) = 1$, el lema 8.5 implica que

$$x_1 \equiv x_2 \mod m.$$ ■

Teorema 8.7. *La congruencia*

$$ax + b \equiv 0 \mod m$$

tiene solución si b es un múltiplo de (a, m). Además, cualesquiera dos soluciones x_1 y x_2 satisfacen

$$x_1 \equiv x_2 \mod \frac{m}{(m, a)}$$

Demostración. La prueba es semejante al caso anterior. Describimos primero $b = q(m, a)$ para algún entero q, enseguida usamos la identidad de Bézout para encontrar los enteros r y s de forma que

$$sa + tm = (a, m)$$

con lo que tenemos

$$qsa + qtm = q(a, m) = b$$

y en consecuencia

$$(-qs)a + b \equiv 0 \mod m.$$

por lo que la congruencia tiene solución en $x = -qs$, garantizando la existencia. La prueba de la segunda parte es muy similar a la del teorema anterior y se obtiene en el ejercicio 8.7. ■

Corolario 8.8. *La congruencia* $ax \equiv 1 \mod m$ *tiene solución si y sólo si* $(a, m) = 1$.

Por último, notamos que podemos tener de igual forma sistemas de congruencias y mientras sean lineales, éstas siempre tienen solución. De hecho, problemas que involucran congruencias simultaneas con módulos primos relativos aparecen en antiguos manuscritos Chinos y el método para resolverlos que aparece en éstos, es el que motiva, tras siglos de refinamiento, la prueba del siguiente teorema.

Teorema 8.9 (Teorema chino del residuo)**.** *Si m y n son primos entre sí, entonces las siguientes congruencias tienen una solución común:*

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

Demostración. Comenzamos notando que el teorema 8.6 garantiza que la primer congruencia tiene al menos una solución y cualquier número se podrá expresar como

$$x = a + ym$$

para algún entero y, será de igual forma una solución. Esto quiere decir que si podemos encontrar un entero y de forma que

$$a + ym \equiv b \mod n$$

podremos concluir el resultado que buscamos. Pero podemos escribir la congruencia anterior como

$$my + (a - b) \equiv 0 \mod n$$

y como $(m, n) = 1$, de nueva cuenta el teorema 8.6 garantiza la existencia de un entero con esa propiedad. Así, $x = a + ym$ es una solución común las congruencias. ■

4. Usos y deusos: Dos pruebas de sanidad

El principal interés del lema 8.4 se encuentra en la expresión decimal de los enteros. Con un poco de observación podemos ver que nuestra forma de escribir cualquier número es una combinación lineal de las potencias de 10, e.g.,

$$134 = 1 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

$$7245 = 7 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0,$$

estas combinaciones lineales por supuesto, no admiten más que *dígitos*, i.e., los números $0, 1, \ldots, 8$ y 9. En general, para cualquier entero positivo a, podemos expresarlo como

$$a = a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$$

donde los números $a_0, \ldots a_{n-1}$ y a_n se les llama los dígitos de a. Presentamos ahora un teorema, como mera curiosidad, a través del cual observaremos cómo es que el concepto de congruencia se logra transmitir a los dígitos. Vamos a relacionar estas observaciones con la teoría de congruencias que hemos desarrollado hasta ahora.

Teorema 8.10. *Un entero a es múltiplo de 9 si y sólo si 9 divide a la suma de sus dígitos.*

Demostración. En efecto, debemos notar primero que $10 \equiv 1 \mod 9$, y según el teorema 8.3, debemos tener $10^n \equiv 1 \mod 9$; bajo el mismo teorema, también podemos expresar

$$\begin{aligned} a &= a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n \\ &\equiv a_1 + \cdots + a_n \mod 9. \end{aligned}$$

Esto quiere decir que a y la suma de sus dígitos $a_1 + \cdots + a_n$ tienen en mismo residuo al dividirlos entre 9. En consecuencia, a es divisible por 9 si y sólo si 9 divide a la suma de sus dígitos. ■

Teorema 8.11. *Un entero a es un múltiplo de 2 si y sólo si a_0 es un múltiplo de 2.*

Demostración. Debemos notar que $10^n \equiv 0 \mod 2$ y en consecuencia

$$\begin{aligned} a &= a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n \\ &\equiv a_0 \mod 2. \end{aligned}$$

Lo que implica que a es múltiplo de 2 si y sólo a_0 es múltiplo de 2. ■

Un par de casos derivado de estos ejemplos están presentes en los ejercicio 8.4. Estos ejemplos constituyen parte de un interesante grupo de problemas conocidos como *pruebas de sanidad* y una discusión mucho más elaborada puede encontrarse en el capítulo 5 sección C de [Chi95].

Ejercicios

Ejercicio 8.1. Verifica las siguientes congruencias

1. $1329 \equiv 2 \mod 9$.
2. $182 \equiv 119 \mod 9$.
3. $-3 \equiv 27 \mod 6$.
4. $145 \equiv 2 \mod 13$.

Ejercicio 8.2. Prueba que la relación $\cdot \equiv \cdot \mod m$ es una relación de equivalencia.

Ejercicio 8.3. Termina la demostración del teorema 8.3

Ejercicio 8.4 (Otras pruebas de sanidad). Demuestra que:

1. Un entero a es múltiplo de 3 si y sólo si 3 divide a la suma de sus dígitos.
2. Un entero a es un múltiplo de 5 si y sólo si a_0 es un múltiplo de 5.

Ejercicio 8.5. Muestra que $x \equiv y \mod m$, implica $(x, m) = (y, m)$.

Ejercicio 8.6. Encuentra el menor entero positivo x, si existe, que satisfaga:

1. $16x - 9 \equiv 0 \mod 35$.
2. $200x + 315 \equiv 0 \mod 411$.
3. $6x + 3 \equiv 4 \mod 10$.
4. $(2n+1)x + 7 \equiv 0 \mod 4n$, para $n > 1$.

Ejercicio 8.7. Termina la prueba del teorema 8.7.

Ejercicio 8.8 (El otro teorema chino del residuo). Sean $m_1, \ldots, m_{k-1}$ y m_k primos relativos en pares, i.e., siempre que $i \neq j$, se tiene $(m_i, m_j) = 1$. Demuestra que las congruencias

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

tienen una solución común.

Ejercicio 8.9. Encuentra una solución común para las siguientes colecciones de congruencias.

1. $x \equiv 0 \mod 7$ y $x \equiv 0 \mod 8$.
2. $x \equiv 3 \mod 17$, $x \equiv 4 \mod 21$. y $x \equiv 5 \mod 25$

Ejercicio 8.10. Tomando los números $a = p_1^{e_1} \ldots p_k^{e_k}$ y $b = p_1^{f_1} \ldots p_k^{f_k}$, permitiendo la posibilidad que los exponentes sean cero, demuestra que a divide a b si y sólo si $e_i \leq f_i$ para todo $1 \leq i \leq k$.

Ejercicio 8.11. Tomando los números a y b como en el ejercicio anterior, demuestra que, tomando $s_i = \text{mín}(e_i, f_i)$ y $r_i = \text{máx}(e_i, f_i)$, se deben cumplir las igualdades

$$(a, b) = p_1^{s_1} \ldots p_k^{s_k}$$

y

$$[a, b] = p_1^{r_1} \ldots p_k^{r_k}.$$

Ejercicio 8.12. Usando los dos ejercicios anteriores, concluye que se debe tener $ab = (a, b)[a, b]$.

Para entregar: Ejercicio 8.4

Referencias

[Chi95] Childs, Lindsay N.: *A concrete introduction to higher algebra*. Springer, 2ª edición, 1995.

[CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: *Álgebra Superior*. Editorial Trillas, 1990.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.