CONGRUENCIAS ENTRE NUMEROS Y MODULOS NO ENTEROS

José Oliver S.
Luis Balbuena C.

1. Introducción

La teoría de números es una inagotable fuente de situaciones y problemas interesantes. Los que somos del "plan antiguo" echamos de menos en los contenidos actuales ciertos temas de teoría de números que resultaban de gran riqueza formativa. Algunas cuestiones que estudian los alumnos hoy en la enseñanza no universitaria, quedan sin explicación porque no se desarrollan los fundamentos que permiten razonar el por qué. Pensemos, por ejemplo, en los criterios de divisibilidad. Se enseñan y se comprueba que, por ejemplo, un número es múltiplo de 3 "si la suma de los valores absolutos de sus cifras es múltiplo de 3" y ahí queda eso... Algunos podrán pensar -y tal vez así lo pensaron quienes planificaron los contenidos- que basta con saber aplicar el criterio. Si ese criterio de selección de contenidos se aplicara de forma estricta, las matemáticas deberían reducirse a un recetario que el alumno aprenderá a utilizar y no es necesario dar ningún tipo de explicación ni de demostración, ¿para qué?. Desgraciadamente algo de eso hay ...

Las congruencias es uno de los temas que pasó al olvido. Se sacrificó ¿a cambio de qué? ¿Es más interesante que un alumno acabe sabiendo la Fórmula de Taylor que conocer toda la riqueza numérica que se desprende de las congruencias? Como casi todo, es opinable y habrá quien opine que sí y quien opine que no. No es este el foro adecuado para la polémica. Nosotros, sin pretender abrirla, creemos que este tema nunca debió ser sustituido.

En el presente trabajo, después

de recordar la definición clásica de congruencia, expondremos algunas ampliaciones de la congruencia entera que pueda servir de apoyo a aquellos que deseen profundizar. No es un campo excesivamente estudiado. De hecho, en la bibliografía habitual no se recogen esas congruencias.

2. Definiciones y notaciones.

Si un número entero **a** lo dividimos por otro **m**, se obtiene un resto único:

$$\begin{array}{l|l} a & m \\ \cline{2-2} r & c \end{array}$$

c = cociente ; r = resto

Dos números a y b se dice que son congruentes módulo m, y lo representamos $a \equiv b(m)$, si al dividir a y b entre m se obtiene en ambos casos el mismo resto.

Así, pues: si , $a \equiv b(m)$ entonces:

$$\left.\begin{array}{ll} \begin{array}{l|l} a & m \\ \cline{2-2} r_1 & c_1 \end{array} \Rightarrow & a = c_1 \cdot m + r_1 \\ \begin{array}{l|l} b & m \\ \cline{2-2} r_2 & c_2 \end{array} \Rightarrow & b = c_2 \cdot m + r_2 \end{array}\right\} \quad r_1 = r_2$$

Si restamos miembro a miembro, se obtiene

$$a\text{-}b = c_1m\text{-}c_2m = (c_1\text{-}c_2)m = \dot{m}$$

Esta es otra caracterización de la congruencia

$$\boxed{a \equiv b\,(\,m\,) \Leftrightarrow a - b = \dot{m}}$$

Algunas propiedades de las congruencias:

* Si $a \equiv b(m)$ y $b \equiv c(m)$, entonces $a \equiv c(m)$

* Si $a_1 \equiv b_1(m), a_2 \equiv b_2(m), ..., a_n \equiv b_n(m)$, entonces

1°) $a_1+a_2+...+a_n \equiv b_1+b_2+...+b_n(m)$

2° $a_1 \cdot a_2 \cdot a_3 ... \cdot a_n \equiv b_1 \cdot b_2 \cdot b_3 \cdot ... \cdot b_n(m)$

* Si $a \equiv b(m)$, entonces $k\,a \equiv k\,b(km)$, $k \in Z$

3. Otras congruencias

3.1 **Números enteros congruentes respecto a un módulo fraccionario**

$$\boxed{a \equiv b(m/n) \Leftrightarrow a \equiv b(m)}$$

Ejemplos:

- $41 \equiv 55\left(\frac{7}{9}\right) \Rightarrow 55\text{-}41 = \frac{\dot{7}}{9} = K \cdot \frac{7}{9} \Rightarrow 14 = K \cdot \frac{7}{9} \Rightarrow K = 18$

  Por tanto, $41 \equiv 55(7)$

- $73 \equiv 67\left(\frac{7}{9}\right) \Rightarrow 73\text{-}67 = K \cdot \frac{7}{9} \Rightarrow 6 = K \cdot \frac{7}{9} \Rightarrow 54 = K \cdot 7 \Rightarrow K \notin Z$

  Por tanto, $73 \not\equiv 67\left(\frac{7}{9}\right)$

3.2 **Fracciones congruentes respecto a un módulo entero**

$$\frac{m}{r} \equiv \frac{r}{s}(a) \Leftrightarrow ms - nr = \dot{a} \qquad \text{(I)}$$

En efecto:

$$\frac{m}{n} = \frac{r}{s}\,(a) \iff \frac{m}{n} - \frac{r}{s} = \dot{a} \Rightarrow \frac{ms - rn}{ns} = \dot{a} \Rightarrow$$

$$ms\text{-}rn = n\,s\,\dot{a} = \dot{a}$$

Teniendo en cuenta que, dadas dos fracciones cualesquiera, se puede conseguir el mismo denominador con fracciones equivalentes, (I) se puede expresar también así:

$$\frac{m}{n} = \frac{r}{n}\ (a) \iff ms - nr = \dot{a}$$

Ejemplo: ¿Es $\frac{1}{3} \equiv \frac{24}{7}$ (5) ?

$$\frac{1}{3} \equiv \frac{24}{7}(5) \iff \frac{7}{21} \equiv \frac{72}{21}\ (5) \iff 72 \equiv 7\ (5)$$

y como $72\text{-}7 = 5$, entonces la respuesta es afirmativa.

3.3 Fracciones congruentes respecto a un módulo fraccionario

Teniendo en cuenta lo indicado en el apartado anterior:

$$\boxed{\frac{m}{n} \equiv \frac{r}{n}\left(\frac{p}{q}\right) \iff m \equiv r\ (np)}$$

En efecto:

$$\frac{m}{n} \equiv \frac{r}{n}\left(\frac{p}{q}\right) \iff \frac{m}{n} - \frac{m}{n} = K\cdot\frac{p}{q} \Rightarrow\quad m\text{-}r = K\cdot m\frac{p}{q} \Rightarrow$$

$$\Rightarrow q\,(m - r) = Kmp = n\dot{p} \Rightarrow \qquad m \equiv r\ (np)$$

Ejemplos: • ¿Es $\frac{703}{20} \equiv \frac{843}{20} \left(\frac{7}{9}\right)$?

$$843\text{-}703 = 140 = \overline{7 \cdot 20}^{\bullet}$$

Por tanto, si son congruentes.

• ¿Es $\frac{175}{8} \equiv \frac{242}{8} \left(\frac{3}{5}\right)$?

$$242\text{-}175 = 67 \neq \overline{3 \cdot 8}^{\bullet}$$

Por tanto, no son congruentes.

3.4 **Números complejos congruentes respecto a un módulo entero**

$$a+bi \equiv m+ni(h) \Rightarrow \left\{ \begin{array}{l} a+bi = hc+R \\ m+ni = hc'+R \end{array} \right\} \Rightarrow$$

$$\Rightarrow (a+bi)\text{-}(m+ni) = (a\text{-}m)+(b\text{-}n)i = h(c\text{-}c') = \dot{h} \Leftrightarrow$$

$$\Leftrightarrow \left\{ \begin{array}{l} a\text{-}m = \dot{h} \\ b\text{-}n = 0 \end{array} \right. \quad \left\{ \begin{array}{l} a \equiv m(h) \\ b = n \end{array} \right.$$

Por tanto,

$$\boxed{a+bi \equiv m+ni(h) \Leftrightarrow \left\{ \begin{array}{l} a \equiv m(h) \\ b = n \end{array} \right.}$$

Ejemplos:

- $4+5i \not\equiv 8\text{-}7i(3)$, ya que sus partes imaginarias no son iguales.

¿Es $10+4i \equiv 24+4i(7)$?

Lo será si sus partes reales son congruentes con ese módulo.
Como 24-10 = 14 = 7, sí son congruentes.

3.5 Números complejos congruentes respecto de módulo fraccionario

$$a + bi \equiv m + ni \left(\frac{h}{k}\right) \Rightarrow \begin{cases} a + bi = \dfrac{h}{k} \cdot C + R \\ m + ni = \dfrac{h}{k} \cdot C^1 + R \end{cases} \Rightarrow$$

$$\Rightarrow (a+bi)-(m+ni) = (a-m)+(b-n)i = \frac{h}{k}\,(C - C^1)(\dot{\frac{h}{k}}) \Rightarrow$$

$$\Rightarrow \begin{cases} a - m = (\dot{\frac{h}{k}}) \\ b - m = o \end{cases} \Rightarrow \begin{cases} a \equiv m \left(\frac{h}{k}\right) \\ b = n \end{cases}$$

Por tanto:

$$\boxed{a + bi \equiv m + ni \left(\frac{h}{k}\right) \Leftrightarrow \begin{cases} a \equiv m \left(\frac{h}{k}\right) \\ b = n \end{cases}}$$

Ejemplo: Se comprueba que 48+4i ≡ 55+4i(7/9)

3.6 Números enteros congruentes respecto a un módulo complejo

$$\boxed{m \equiv n\ (a + bi) \ \Leftrightarrow\ m \equiv n \left(\frac{a^2 + b^2}{a + bi}\right)}$$

(Se sabe que $(a+bi)(a-bi) = a^2+b^2 \Rightarrow a + bi = \dfrac{a^2 + b^2}{a - bi}$)

Por lo que, teniendo en cuenta lo expresado en el apartado 3.1, se concluye:

$$m \equiv n(a+bi) \iff m \equiv n(a^2+b^2)$$

Ejemplo:

$$123 \equiv 13(1+2i), \text{ pues } 123 \equiv 13(5)$$

3.7 **Fracciones congruentes respecto a módulo complejo**

$$\boxed{\frac{a}{b} \equiv \frac{c}{d}(m+ni) \iff ad \equiv bc\left((m^2+n^2)\,bd\right)}$$

Es una consecuencia de 3.3 y 3.6

Ejemplo:

$$¿\text{Es } \frac{2}{3} \equiv \frac{24}{5}(1+2i)?$$

Hemos de comprobar si:

$$2 \cdot 5 \equiv 24 \cdot 3(5 \cdot 3 \cdot 5), \text{ es decir, } 10 \equiv 72(30)$$

Por tanto, se verifica la congruencia.

3.8 **Número complejo congruente respecto a un módulo complejo.**

Supongamos $a+bi \equiv m+ni(p+qi)$

$$(a+bi)-(m+ni) = k(p+qi) \Rightarrow \begin{cases} a - m = \dot{p} \\ b - n = \dot{q} \end{cases} \Rightarrow \begin{cases} a \equiv m\ (p) \\ b \equiv n\ (p) \end{cases}$$

Por tanto:

$$\boxed{a+bi \equiv m+ni(p+qi) \iff \begin{cases} a \equiv m(p) \\ b \equiv n(q) \end{cases}}$$

Ejemplos:
Veamos si $48+32i \equiv 55+41i(7+9i)$

Hemos de comprobar si $48 \equiv 55(7) \Rightarrow 55-48 = \dot{7}$ y si $32 \equiv 41(9) \Rightarrow 41-32 = \dot{9}$

Como se verifican ambas congruencias, afirmamos que la congruencia es cierta.
Veamos que los restos de dividir $48+32i$ y $55+41i$ entre $7+9i$ son iguales:

$$\begin{array}{r|l} 32\,i + 48 & 9i + 7 \\ \hline -32i - \frac{32\cdot 7}{9} & \frac{32}{9} \end{array} \qquad \begin{array}{r|l} 41i + 55 & 9i + 7 \\ \hline -41i - \frac{41\cdot 7}{9} & \frac{41}{9} \end{array}$$

$$R_1 = 48 - \frac{32\cdot 7}{9} = \frac{9\cdot 48 - 32\cdot 7}{9} = \frac{208}{9}$$

$$R_2 = 55 - \frac{41\cdot 7}{9} = \frac{9\cdot 55 - 41\cdot 7}{9} = \frac{208}{9}$$

Las conocidas propiedades de las congruencias de números enteros se mantienen.
Veamos mediante un ejemplo que:

Si $a+bi \equiv m+ni(p+qi)$, entonces $(a+bi)^2 \equiv (m+ni)^2(p+qi)$

Puede comprobarse fácilmente que

$$8+10i \equiv 15+9i(7+9i)$$

$(8+10i)^2 = 64-100+160i = -36+160i$

$(15+9i)^2 = 225-361+570i = -136+570i$

Estudiemos si $(8+10i)^2 \equiv (15+9i)^2(7+9i)$, es decir,

$-36+160i \equiv -136+570i(7+9i)$,

o lo que es igual:

$36-160i \equiv 136-570i(7+9i)$

Resulta que:

$$\frac{36-160i}{7+9i} = \frac{(36-160i)(7-9i)}{130} = -9-11i + \frac{-9-7i}{65} = -9-11i + R_1$$

$$\frac{136-570i}{7+9i} = \frac{(136-570i)(7-9i)}{130} = -32-40i + \frac{-9-7i}{65} = -32-40i + R_2$$

$R_1 = R_2$, por lo que se verifica la congruencia.

4. Bibliografía:

* I. Vinogradov. "Fundamentos de la teoría de los números". Editorial Mir-1977.
* J. Rey Pastor, Pi Calleja, C.A. Trejo. "Análisis Matemático. Vol. I. Editorial Kapeluz.