TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

4.4 Congruencias Lineales y el Teorema Chino de Restos

Este es un lugar conveniente en nuestro desarrollo de la teoría de números para investigar la teoría de congruencias lineales: una ecuación de la forma $ax \equiv b \pmod{n}$ se llama una *congruencia lineal*, y por solución referimos a un entero x_0 tal que $ax_0 \equiv b \pmod{n}$. Por la definición, $ax_0 \equiv b \pmod{n}$ si y solo si $n|ax_0 - b$, o lo que es el mismo, si y solo si $ax_0 - b = ny_0$ para algún entero y_0. Entonces el problema de hallar todos los enteros que satisfacen la congruencia lineal $ax \equiv b \pmod{n}$ es idéntico al de obtener todas las soluciones a la ecuación lineal diofántica $ax - ny = b$. Esto nos permite poner en juego los resultados de Capítulo 2.

Es conveniente tratar dos soluciones de $ax \equiv b \pmod{n}$ que son congruentes módulo n como "iguales" aunque no lo sean iguales en el sentido habitual. Por ejemplo, $x = 3$ y $x = -9$ ambos satisfacen la congruencia $3x \equiv 9 \pmod{12}$; como $3 \equiv -9 \pmod{12}$, no son consideradas como soluciones distintas. En breve: cuando referimos al número de soluciones de $ax \equiv b \pmod{n}$, queremos decir el número de enteros incongruentes que satisfacen esta congruencia.

Con estos comentarios en mente, el resultado principal es fácil declarar.

Teorema 4.7. La congruencia lineal $ax \equiv b \pmod{n}$ tiene solución si y solo si $d|b$, en donde $d = \text{mcd}(a, n)$. Si $d|b$, entonces se tiene d soluciones mutualmente incongruentes módulo n.

Demostracion: Ya hemos observado que la congruencia dada es equivalente a la ecuación lineal diofántica $ax - ny = b$. Del Teorema 2.9, se sabe que se puede resolver la última ecuación si y solo si $d|b$; además, si es soluble y x_0, y_0 es una solución específica, entonces cualquier otra solución tiene la forma

$$x = x_0 + \frac{n}{d}t \qquad y = y_0 + \frac{a}{d}t$$

por alguna elección de t.

Entre los varios enteros que satisfacen las primeras de estas fórmulas, consideramos estos que ocurren cuando t toma los valores sucesivos $t = 0, 1, 2, \ldots, d-1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

Afirmamos que estos enteros son incongruentes módulo n, y que todos los demás tales enteros x son congruentes a alguno de ellos. Si sucediera que

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$$

en donde $0 \leq t_1 < t_2 \leq d-1$, entonces tendríamos

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$$

Ahora $\text{mcd}(n/d, n) = n/d$, y entonces por el Teorema 4.3 se puede cancelar el factor n/d para llegar a la congruencia

$$t_1 \equiv t_2 \pmod{d}$$

lo que es decir que $d|t_1 - t_2$. Pero esto es imposible en vista de la desigualdad $0 < t_2 - t_1 < d$.

Queda por argumentar que cualquier otra solución $x_0 + (n/d)t$ es congruente módulo n a uno de los d enteros enumerados anteriormente. El Algoritmo de División nos permite escribir t como $t = dq + r$, en donde $0 \leq r \leq d-1$. Entonces

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n} \end{aligned}$$

siendo $x_0 + (n/d)r$ una de nuestras soluciones seleccionadas. Esto termina la demostración.

El argumento que dimos en la Teorema 4.7 resalta un punto que vale la pena declarar explicitamente: Si x_0 es cualquier solución de $ax \equiv b \pmod{n}$, entonces la $d = \text{mcd}(a, n)$ soluciones incongruentes están dadas por

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

Para la comodidad del lector, registremos también la forma que la Teorema 4.7 toma en el caso especial en el que suponemos que a y n son coprimos.

Corolario. Si $\text{mcd}(a, n) = 1$, entonces la congruencia lineal $ax \equiv b \pmod{n}$ tiene una solución única módulo n.

Dado enteros coprimos a y n, la congruencia $ax \equiv 1 \pmod{n}$ tiene una solución única. Esta solución a veces se llama la inversa (multiplicativa) de a módulo n.

Ahora hacemos una pausa para mirar dos ejemplos concretos.

Ejemplo 4.7. Primero, consideramos la congruencia lineal $18x \equiv 30 \pmod{42}$. Como $\text{mcd}(18, 42) = 6$ y 6 seguramente divide a 30, el Teorema 4.7 garantiza la existencia de exactamente seis soluciones incongruentes módulo 42. Por inspección,

se encuentra una solución $x = 4$. Nuestro análisis nos dice que los seis soluciones son las siguientes:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t \pmod{42} \qquad t = 0, 1, \ldots, 5$$

o, claramente enumerado,

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$$

Ejemplo 4.8. Resolveremos la congruencia lineal $9x \equiv 21 \pmod{30}$. Al principio, como $\text{mcd}(9, 30) = 3$ y $3|21$, sabemos que debe haber tres soluciones incongruentes.

Una manera de hallar estas soluciones es dividir la congruencia dada por 3, reemplazándolo con la congruencia equivalente $3x \equiv 7 \pmod{10}$. La coprimidad de 3 y 10 implica que la última congruencia admite una solución única módulo 10. Aunque no es el método mas eficaz, podríamos probar los enteros $0, 1, 2, \ldots 9$ por turno hasta obtener la solución. Una manera mejor es esta: Multiplica ambos lados de la congruencia $3x \equiv 7 \pmod{10}$ por 7 para obtener

$$21x \equiv 49 \pmod{10}$$

lo que se reduce a $x \equiv 9 \pmod{10}$. (Esta simplificación no es casualidad, como los multiples $0 \cdot 3, 1 \cdot 3, 2 \cdot 3, \ldots, 9 \cdot 3$ forman un conjunto completo de residuos módulo n; entonces, uno de ellos necesariamente es congruente a 1 módulo 10.) Pero la congruencia original fue dado módulo 30, de modo que se busquen sus soluciones incongruentes entre los enteros $0, 1, 2, \ldots, 29$. Tomando $t = 0, 1, 2$, en la fórmula

$$x = 9 + 10t$$

obtenemos $9, 19, 29$, de donde

$$x \equiv 9 \pmod{30} \qquad x \equiv 19 \pmod{30} \qquad x \equiv 29 \pmod{30}$$

son los requeridas tres soluciones de $9x \equiv 21 \pmod{30}$.

Un enfoque diferente al problema es utilizar el método sugerido en la demostración del Teorema 4.7. Como la congruencia $9x \equiv 21 \pmod{30}$ es equivalente a la ecuación lineal diofántica

$$9x - 30y = 21$$

comenzamos expresando $3 = \text{mcd}(9, 30)$ como una combinación lineal de 9 y 30. Se encuentra, o por inspección o por utilizar el Algoritmo de Euclides, que $3 = 9(-3) + 30 \cdot 1$, de modo que

$$21 = 7 \cdot 3 = 9(-21) - 30(-7)$$

Entonces, $x = -21$, $y = -7$ satisface la ecuación diofántica y, en consecuencia, todas las soluciones de la congruencia en cuestión se puede hallar de la fórmula

$$x = -21 + (30/3)t = -21 + 10t$$

Los enteros $x = -21 + 10t$, en donde $t = 0, 1, 2$ son incongruentes módulo 30 (pero todos son congruentes módulo 10); entonces, terminamos con las soluciones incongruentes

$$x \equiv -21 \pmod{30} \qquad x \equiv -11 \pmod{30} \qquad -1 \equiv 29 \pmod{30}$$

o, si uno prefiere los números positivos, $x \equiv 9, 19, 29 \pmod{30}$.

Habiendo considerado una sola congruencia lineal, es natural pasar al problema de resolver un sistema de congruencias lineales simultáneas:

$$a_1x \equiv b_1 \pmod{n_1}, \qquad a_2x \equiv b_2 \pmod{n_2}, \quad \ldots, \quad a_rx \equiv b_r \pmod{n_r}$$

Supondremos que los móduli m_k son coprimos en pares. Evidentemente, el sistema no admitirá una solución a menos que cada congruencia individual es soluble; es decir, a menos que $d_k|b_k$ para cada k, en donde $d_k = \text{mcd}(a_k, m_k)$. Cuando se cumplen estas condiciones, se puede cancelar el factor d_k en el k-ésima congruencia para producer un nuevo sistema con el mismo conjunto de soluciones que el anterior:

$$a_1'x \equiv b_1' \pmod{n_1}, \qquad a_2'x \equiv b_2' \pmod{n_2}, \quad \ldots, \quad a_r'x \equiv b_r' \pmod{n_r}$$

en donde $n_k = m_k/d_k$ y $\text{mcd}(n_i, n_j) = 1$ para $i \neq j$; además, $\text{mcd}(a_i', n_i) = 1$. Las soluciones de las congruencias individuales toman la forma

$$x \equiv c_1 \pmod{n_1}, \quad x \equiv c_2 \pmod{n_2}, \ldots x \equiv c_r \pmod{n_r}$$

Entonces, el problema se reduce a encontrar una solución simultánea de un sistema de congruencias de este tipo más simple.

El tipo de problema que se puede resolver por congruencias simultáneas tiene una larga historia, apareciendo en la literatura china ya en el sigo I d.C. Sun-Tsu preguntó: Hallar un número que deja los restos 2, 3, 2 cuando se divide por 3, 5, 7, respectivamente. (Tales acertijos matemáticos no se limitan en modo alguno a una única esfera cultural; en efecto, el mismo problema ocurre en el *Introductio Arithmeticae* del matemático griego Nichomachus del año 100 d.C.) En honor a sus antiguas contribuciones, la regla para obtener una solución generalmente se llama el Teorema Chino del Resto.

Teorema 4.8. Teorema Chino del Resto. Sean $n_1, n_2, \ldots, n_r$ enteros positivos tales que $\text{mcd}(n_i, n_j) = 1$ para $i \neq j$. Entonces el sistema de congruencias lineales

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

tiene una solución simultánea, lo que es única módulo el entero $n_1n_2 \cdots n_r$.

Demostración: Empezamos por formar el producto $n = n_1 n_2 \cdots n_r$. Para cada $k = 1, 2, \ldots, r$, sea

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$$

En palabras, N_k es el producto de todos los enteros n_i con n_k omitido. Por hipótesis, los n_i son coprimos en pares, de modo que $\text{mcd}(N_k, n_k) = 1$. Según la teoría de una congruencia lineal simple, por lo tanto es posible resolver la congruencia $N_k x \equiv 1 \pmod{n_k}$; denota la solución única x_k. Nuestra objetivo es demostrar que el entero

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

es una solución simultánea del sistema dado.

Primero, observa que $N_i \equiv 0 \pmod{n_k}$ para $i \neq k$, como $n_k | N_i$ en este caso. El resultado es

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

Pero el entero x_k fue elegido para satisfacer la congruencia $N_k x \equiv 1 \pmod{n_k}$, lo que obliga

$$\overline{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$$

Esto muestra que una solución al sistema dado de congruencias existe.

En cuanto a la afirmación de unicidad, supongamos que x' es otro entero que satisface estas congruencias. Entonces

$$\overline{x} \equiv a_k \equiv x' \pmod{n_k} \quad k = 1, 2, \ldots, r$$

y entonces $n_k | \overline{x} - x'$ para cada valor de k. Como $\text{mcd}(n_i, n_j) = 1$, el Corolario 2 al Teorema 2.4 nos proporciona el punto crucial que $n_1 n_2 \cdots n_r | \overline{x} - x'$; entonces $\overline{x} \equiv x' \pmod{n}$. Con esto, el Teorema Chino del Resto está demostrado.

Ejemplo 4.9. El problema planteado por Sun-Tsu corresponde al sistema de tres congruencias

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

En la notación del Teorema 4.8, tenemos $n = 3 \cdot 5 \cdot 7 = 105$ y

$$N_1 = \frac{n}{3} = 35 \quad N_2 = \frac{n}{5} = 21 \quad N_3 = \frac{n}{7} = 15$$

Ahora las congruencias lineales

$$35x_1 \equiv 1 \pmod{3} \quad 21x_2 \equiv 1 \pmod{5} \quad 15x_3 \equiv 1 \pmod{7}$$

están satisfechas por $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectivamente. Por lo tanto, una solución del sistema está dado por

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot +2 \cdot 15 \cdot 1 = 233$$

Módulo 105, obtenemos la solución única $x = 233 \equiv 23 \pmod{105}$.

Ejemplo 4.10. Para una segunda ilustración, resolveremos la congruencia lineal

$$17x \equiv 9 \pmod{276}$$

Como $276 = 3 \cdot 4 \cdot 23$, esto es equivalente a hallar una solución al sistema de congruencias

$$\begin{array}{lll} 17x \equiv 9 \pmod{3} & \text{o} & x \equiv 0 \pmod{3} \\ 17x \equiv 9 \pmod{4} & & x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} & & 17x \equiv 9 \pmod{23} \end{array}$$

Nota que si $x \equiv 0 \pmod{3}$, entonces $x = 3k$ por algún entero k. Substituimos en la segunda congruencia del sistema y obtenemos

$$3k \equiv 1 \pmod{4}$$

Al multiplicar ambos lados por 3, obtenemos

$$k \equiv 9k \equiv 3 \pmod{4}$$

de modo que $k = 3 + 4j$, en donde j es un entero. Entonces

$$x = 3(3 + 4j) = 9 + 12j$$

Para que esto satisfaga la última congruencia, debemos tener

$$17(9 + 12j) \equiv 9 \pmod{23}$$

o $204j \equiv -144 \pmod{23}$, que se reduce a $3j \equiv 6 \pmod{23}$, en consecuencia, $j \equiv 2 \pmod{23}$. Estro produce $j = 2 + 23t$, con t un entero, de dónde

$$x = 9 + 12(2 + 23t) = 33 + 276t$$

Considerándolo todo, $x \equiv 33 \pmod{276}$ provee una solución al sistema de congruencias, y a la vez una solución a $17x \equiv 9 \pmod{276}$.

Deberíamos decir algunas palabras sobre las congruencias lineales en dos variables; es decir, las congruencias de la forma

$$ax + by \equiv c \pmod{n}$$

En analogía con el Teorema 4.7, tal congruencia tiene una solución si y solo si $\text{mcd}(a, b, n)$ divide a c. La condición de solubilidad se cumple si $\text{mcd}(a, n) = 1$ o $\text{mcd}(b, n) = 1$. Digamos $\text{mcd}(a, n) = 1$. Cuando se expresa la congruencia como

$$ax \equiv c - by \pmod{n}$$

el corolario al Teorema garantiza una solución única para cada de los n valores incongruentes de y. Tomemos como simple ejemplo $7x + 4y \equiv 5 \pmod{12}$, que se trataría como $7x \equiv 5 - 4y \pmod{12}$. La sustitución de $y \equiv 5 \pmod{12}$ da $7x \equiv -15 \pmod{12}$, pero esto es equivalente a $-5x \equiv -15 \pmod{12}$, de modo que $x \equiv 3 \pmod{12}$. Resulta que $x \equiv 3 \pmod{12}$, $y \equiv 5 \pmod{12}$ es una de

las 12 soluciones no congruentes de $7x + 4y \equiv 5 \pmod{12}$. Otra solución con el mismo valor de x es $x \equiv 3 \pmod{12}$, $y \equiv 8 \pmod{12}$.

El foco de nuestro atención aquí es cómo resolver un sistema de dos congruencias lineales en dos variables con el mismo módulo. La demostración del siguiente teorema adopta el procedimiento familiar de eliminar uno de los incógnitos.

Teorema 4.9. El sistema de congruencias lineales

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

tiene una solución única módulo n siempre que $\text{mcd}(ad - bc, n) = 1$.

Demostración: Multipliquemos la primera congruencia por d, la segunda congruencia por b, y restar el segundo resultado del primero. Estos cálculos producen

$$(ad - bc)x \equiv dr - bs \pmod{n} \tag{1}$$

La suposición $\text{mcd}(ad - bc, n) = 1$ garantiza que la congruencia

$$(ad - bc)z \equiv 1 \pmod{n}$$

posee una solución única; denotaremos la solución por t. Cuando se multiplica la congruencia (1) por t, obtenemos

$$x \equiv t(dr - bs) \pmod{n}$$

Se encuentra un valor para y por un proceso de eliminación similar. Es decir, multipliquemos la primera congruencia del sistema por c, la segunda por a, y restamos para terminar con

$$(ad - bc)y \equiv as - cr \pmod{n} \tag{2}$$

La multiplicación de esta congruencia por t conduce a

$$y \equiv t(as - cr) \pmod{n}$$

Ya se ha establecido una solución al sistema.

Cerramos esta sección con un ejemplo que ilustra el Teorema 4.9.

Ejemplo 4.11. Consideramos el sistema

$$\begin{aligned} 7x + 3y &\equiv 10 \pmod{16} \\ 2x + 5y &\equiv 9 \pmod{16} \end{aligned}$$

Como $\text{mcd}(7 \cdot 5 - 2 \cdot 3, 16) = \text{mcd}(29, 16) = 1$, existe una solución. Se lo obtiene por el método desarrollado en la demostración del Teorema 4.9. Multiplicando la primera congruencia por 5 y la segunda por 3 y restando, llegamos a

$$29x \equiv 5 \cdot 10 = 3 \cdot 9 \equiv 23 \pmod{16}$$

or, lo que es el mismo, $13x \equiv 7 \pmod{16}$. La multiplicación de esta congruencia por 5 (notando que $5 \cdot 13 \equiv 1 \pmod{16}$) produce $x \equiv 35 \equiv 3 \pmod{16}$. Cuando se elimina el variable x del sistema de congruencias en esta manera, se encuentra que

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \pmod{16}$$

Pero luego $13y \equiv 11 \pmod{16}$, que al multiplicar por 5 da como resultado $y \equiv 55 \equiv 7 \pmod{16}$. Resulta que la solución única de nuestra sistema es

$$x \equiv 3 \pmod{16} \qquad y \equiv 7 \pmod{16}$$

PROBLEMAS 4.4

1. Resolver las siguientes congruencias lineales:
a) $25x \equiv 15 \pmod{29}$.
b) $5x \equiv 2 \pmod{26}$.
c) $6x \equiv 15 \pmod{21}$.
d) $36x \equiv 8 \pmod{102}$.
e) $34x \equiv 60 \pmod{98}$.
f) $140x \equiv 133 \pmod{301}$.
[Consejo: $\text{mcd}(140, 301) = 7$.]

2. Utilizando congruencias, resolver las siguientes ecuaciones diofánticas:
a) $4x + 51y = 9$
[Consejo: $4x \equiv 9 \pmod{51}$ produce $x = 15 + 51t$, mientras $51y \equiv 9 \pmod{4}$ produce $y = 3 + 4s$. Hallar la relación entre s y t.]
b) $12x + 25 = 331$
c) $5x - 53y = 17$

3. Hallar todas las soluciones a la congruencia lineal $3x - 7y \equiv 11 \pmod{13}$.

4. Resolver cada uno de los siguientes conjuntos de congruencias simultáneas:
a) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.
b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$.
c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$.
d) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$.

5. Resolver la congruencia lineal $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ resolviendo

$$17x \equiv 3 \pmod{2} \qquad 17x \equiv 3 \pmod{3}$$
$$17x \equiv 3 \pmod{5} \qquad 17x \equiv 3 \pmod{7}$$

6. Hallar el entero mínimo $a > 2$ tal que

$$2|a, \quad 3|a+1, \quad 4|a+2, \quad 5|a+3, \quad 6|a+4$$

7. a) Obtener tres enteros consecutivos, cada uno teniendo un factor cuadrado. [Consejo: Hallar un entero tal que $2^2|a$, $3^2|a+1$, $5^2|a+2$.]
b) Obtener tres enteros consecutivos, el primero de los cuales es divisible por un cuadrado, el segundo por un cubo, el tercero por una cuarta potencia.

8. (Brahmagupta, Siglo VII d.C.). Cuando se saca huevos de una canasta $2, 3, 4, 5, 6$ a la vez, quedan, respectivamente, $1, 2, 3, 4, 5$ huevos. Cuando se saca 7 a la vez, no quedan ningunos. Hallar el número mínimo de huevos que podría contener la canasta.

9. El problema canasta-de-huevos se expresa a menudo en la siguiente forma: Un huevo queda cuando se saca los huevos $2, 3, 4, 5$, o 6 a la vez, pero ningunos huevos quedan se están sacados 7 a la vez. Hallar el número mínimo de huevos que podría contener la canasta.

10. (Problema Chino Antiguo.) Una banda de 17 piratas robó un saco de monedas de oro. Cuando se trataron de dividir la fortuna en porciones iguales, quedaron 3 monedas. En la pelea que siguió, un pirata murió. La riqueza fue redistribuida, pero esta vez una división igual dejó 10 monedas. Nuevamente se desarrolló otra disputa en la que murió otro pirata. Ahora la fortuna total fue distribuido igualmente entre los sobrevivientes. ¿Cuál fue el número mínimo de monedas que podría haber sido robados?

11. Demostrar que las congruencias

$$x \equiv a \pmod{n} \qquad \text{y} \qquad x \equiv b \pmod{m}$$

admiten una solución simultánea si y solo si $\text{mcd}(n, m)|a - b$; si existe una solución, confirma que es única módulo $\text{mcm}(n, m)$.

12. Utilizar el Problema 11 para demostrar que el siguiente sistema no posee una solución:

$$x \equiv 5 \pmod{6} \qquad \text{y} \qquad x \equiv 7 \pmod{15}$$

13. Si $x \equiv a \pmod{n}$, demostrar que o $x \equiv a \pmod{2n}$ o $x \equiv a + n \pmod{2n}$.

14. Un determinado entero entre 1 y 1200 deja los residuos $1, 2, 6$ cuando se lo divide por $9, 11, 13$ respectivamente. ¿Cuál es el entero?

15. a) Hallar un entero con los residuos $1, 2, 5, 5$ cuando se divide por $2, 3, 6, 12$, respectivamente. (Yih-hing, murió en 717.)
b) Hallar un entero con los residuos $2, 3, 4, 5$ cuando se divide por $3, 4, 5, 6$, respectivamente. (Bhaskara, nació en 1114.)
c) Hallar un entero con los residuos $3, 11, 15$ cuando se divide por $10, 13, 17$, respectivamente. (Regiomontanus, 1436-1476.)

16. Sea t_n el enésimo número triangular. ¿Para cuáles valores de n divide t_n a

$$t_1^2 + t_2^2 + \cdots + t_n^2$$

[Consejo: Como $t_1^2 + t_2^2 + \cdots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$, es suficiente determinar estos n que satisfacen $3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \cdot 3 \cdot 5}$.]

17. Hallar las soluciones al sistema de congruencias:

$$3x + 4y \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 7 \pmod{13}$$

18. Obtener las dos soluciones incongruentes módulo 210 del sistema

$$2x \equiv 3 \pmod{5}$$
$$4x \equiv 2 \pmod{6}$$
$$3x \equiv 2 \pmod{7}$$

19. Obtener las ocho soluciones incongruentes de la congruencia lineal $3x + 4y \equiv 5 \pmod{8}$.

20. Hallar las soluciones de cada de los siguientes sistemas de congruencias:

a) $5x + 3y \equiv 1 \pmod{7}$
$3x + 2y \equiv 4 \pmod{7}$

b) $7x + 3y \equiv 6 \pmod{11}$
$4x + 2y \equiv 9 \pmod{11}$

c) $11x + 5y \equiv 7 \pmod{20}$
$6x + 3y \equiv 8 \pmod{20}$