Universidad del Valle de Guatemala
Departamento de Matemática
Licenciatura en Matemática Aplicada

Estudiante: Rudik Roberto Rompich
E-mail: rom19857@uvg.edu.gt
Carné: 19857

MM2015 - Matemática Discreta - Catedrático: Mario Castillo
31 de mayo de 2021

Tarea 7

1. Problema 1

Teorema 1 - Sección 4.4 de Rosen and Krithivasan (2012)

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer a less than m that is an inverse of a modulo $m$and every other inverse of a modulo m is congruent to a modulo m.)

Utilice el algoritmo euclidiano para encontrar un entero a^{-1} en $\mathbb{Z}_n$ tal que $a^{-1} \cdot a \equiv 1 \pmod{n}$, en donde:

1. $a \equiv 5 \pmod{13}$

   Solución. Procedemos a calcular el mcd(13,5) con el algoritmo de Euclides:

   $$\begin{aligned} 13 &= 2 * 5 + 3 \\ 5 &= 1 * 3 + 2 \\ 3 &= 1 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

   Por lo tanto, el mdc(13,5) = 1. Entonces, el **teorema 1** nos afirma que existe un inverso de 5 en módulo 13. Nótese que por el procedimiento anterior, se propone encontrar los coeficientes de Bézout, yendo hacia atrás:

   $$\begin{aligned} 1 &= (1 * 3) + (-1 * 2) \\ &= (-1 * 5) + (2 * 3) \\ &= (2 * 13) + (-5 * 5) \\ &= (-5 * 5) + (2 * 13). \end{aligned}$$

Por lo tanto, los coeficientes son -5 y 13. Es decir que $a^{-1} \equiv -5 \bmod (13)$. Comprobando:

$$a^{-1} \cdot a = -5 \cdot 5 = -25 \equiv 1, \pmod{13}.$$

□

2. $a \equiv 13 \pmod{19}$

Solución. Procedemos a calcular el mcd(19,13) con el algoritmo de Euclides:

$$\begin{aligned} 19 &= 1 * 13 + 6 \\ 13 &= 2 * 6 + 1 \\ 6 &= 6 * 1 + 0 \end{aligned}$$

Por lo tanto, el mdc(19,13) = 1. Entonces, el **teorema 1** nos afirma que existe un inverso de 13 en módulo 19. Nótese que por el procedimiento anterior, se propone encontrar los coeficientes de Bézout, yendo hacia atrás:

$$\begin{aligned} 1 &= (1 * 13) + (-2 * 6) \\ &= (-2 * 19) + (3 * 13) \\ &= (3 * 13) + (-2 * 19) \end{aligned}$$

Por lo tanto, los coeficientes son 3 y -2. Es decir que $a^{-1} \equiv 3 \bmod (19)$. Comprobando:

$$a^{-1} \cdot a = 3 \cdot 13 = 39 \equiv 1, \pmod{19}.$$

□

El entero a^{-1} se conoce como el *inverso multiplicativo* de $a \pmod{n}$.

2. Problema 2

¿Para qué valores de $m > 0$ tiene solución la ecuación $30x + 14y = m$?

Solución. Procedemos a encontrar el mcd(30,14):

$$\begin{aligned} 30 &= 2 * 14 + 2 \\ 14 &= 7 * 2 + 0 \end{aligned}$$

Es decir que el mcd(30,14) = 2. Por lo tanto, cualquier valor $2m>0$, tendrá solución la ecuación. □

3. Problema 3

Resuelva las siguientes congruencias:

1. $66x \equiv 42 \pmod{168}$

Solución. Procedemos a encontrar la inversa de $a \equiv 66 \pmod{168}$. Es neceario calcular el mcd(168,66):

$$\begin{aligned} 168 &= 2 * 66 + 36 \\ 66 &= 1 * 36 + 30 \\ 36 &= 1 * 30 + 6 \\ 30 &= 5 * 6 + 0 \end{aligned}$$

Entonces, el mdc(168,66)=6. Por lo tanto, 6 es múltiplo de 42; por lo que la ecuación sí tiene solución. Ahora tenemos la ecuación diofántica:

$$168x + 66y = 42$$

Nótese que por el procedimiento anterior, se propone encontrar los coeficientes de Bézout, yendo hacia atrás:

$$\begin{aligned} 6 &= (1 * 36) + (-1 * 30) \\ &= (-1 * 66) + (2 * 36) \\ &= (2 * 168) + (-5 * 66) \\ &= (-5 * 66) + (2 * 168) \end{aligned}$$

Nótese que sí multiplcamos por 7, entonces tenemos 2 soluciones:

$$x_0 = 14 \qquad y \qquad y_0 = -35.$$

Para encontar las soluciones generales, tenemos las siguientes ecuaciones demostradas en clase:

$$\boxed{s = -\frac{(\lambda a)}{\text{mcd}(a,b)} \text{ y } t = \frac{(\lambda b)}{\text{mcd}(a,b)}}$$

Por lo tanto:

$$s = -\frac{\lambda 168}{6} = -28\lambda \qquad y \qquad t = \frac{\lambda 66}{6} = 11\lambda.$$

Por lo tanto, la solución:

$$x = 14 + 11\lambda \qquad y \qquad y = -35 - 28\lambda.$$

Las soluciones particulares son triviales. □

2. $21x \equiv 18 \pmod{30}$

Solución. Procedemos a encontrar la inversa de $a \equiv 21 \pmod{30}$. Es necesario calcular el mcd(30,21):

$$\begin{aligned} 30 &= 1 * 21 + 9 \\ 21 &= 2 * 9 + 3 \\ 9 &= 3 * 3 + 0 \end{aligned}$$

Entonces, el mdc(30,21)=3. Por lo tanto, 3 es múltiplo de 18; por lo que la ecuación sí tiene solución. Ahora tenemos la ecuación diofántica:

$$30x + 21y = 18.$$

Nótese que por el procedimiento anterior, se propone encontrar los coeficientes de Bézout, yendo hacia atrás:

$$\begin{aligned} 3 &= (1 * 21) + (-2 * 9) \\ &= (-2 * 30) + (3 * 21) \\ &= (3 * 21) + (-2 * 30) \end{aligned}$$

Nótese que sí multiplcamos por 6, entonces tenemos 2 soluciones:

$$x_0 = -12 \qquad y \qquad y_0 = 18$$

Para encontar las soluciones generales, tenemos las siguientes ecuaciones demostradas en clase:

$$\boxed{s = -\frac{(\lambda a)}{\text{mcd}(a,b)} \text{ y } t = \frac{(\lambda b)}{\text{mcd}(a,b)}}$$

Por lo tanto:

$$s = -\frac{\lambda 30}{3} = -10\lambda \qquad y \qquad t = \frac{\lambda 21}{3} = 7\lambda.$$

Por lo tanto, la solución:

$$x = -12 + 7\lambda \qquad y \qquad y = 18 - 10\lambda.$$

Las soluciones particulares son triviales. □

3. $35x \equiv 42 \pmod{49}$

Solución. Procedemos a encontrar la inversa de $a \equiv 35 \pmod{49}$. Es necesario calcular el mcd(49,35):

$$\begin{aligned} 49 &= 1 * 35 + 14 \\ 35 &= 2 * 14 + 7 \\ 14 &= 2 * 7 + 0 \end{aligned}$$

Entonces, el mdc(49,35)=7. Por lo tanto, 7 es múltiplo de 42; por lo que la ecuación sí tiene solución. Ahora tenemos la ecuación diofántica:

$$49x + 35y = 42.$$

Nótese que por el procedimiento anterior, se propone encontrar los coeficientes de Bézout, yendo hacia atrás:

$$\begin{aligned} 7 &= (1 * 35) + (-2 * 14) \\ &= (-2 * 49) + (3 * 35) \\ &= (3 * 35) + (-2 * 49) \end{aligned}$$

Nótese que sí multiplcamos por 6, entonces tenemos 2 soluciones:

$$x_0 = -12 \qquad y \qquad y_0 = 18.$$

Para encontar las soluciones generales, tenemos las siguientes ecuaciones demostradas en clase:

$$\boxed{s = -\frac{(\lambda a)}{\text{mcd}(a,b)} \text{ y } t = \frac{(\lambda b)}{\text{mcd}(a,b)}}$$

Por lo tanto:

$$s = -\frac{\lambda 49}{7} = -7\lambda \qquad y \qquad t = \frac{\lambda 35}{7} = 5\lambda.$$

Por lo tanto, la solución:

$$x = -12 + 5\lambda \qquad y \qquad y = 18 - 7\lambda.$$

Las soluciones particulares son triviales. □

4. Problema 4

Teorema 2 (Teorema chino del resto) de Rosen and Krithivasan (2012) de la sección 4.4

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x \equiv & a_1 \pmod{m_1}, \\ x \equiv & a_2 \pmod{m_2}, \\ & \vdots \\ x \equiv & a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Una banda de 17 piratas se reúne para repartirse un cofre con más de 100 monedas de oro, sobrando 1 moneda después del reparto. En la consiguiente pelea, muere un pirata y vuelve a hacerse el reparto sobrando de nuevo 1 moneda. ¿Cuál es el menor número de monedas que puede contener el cofre?

Solución. Sea x el número de monedas del cofre. De la primera y segunda condición, tenemos

$$\begin{cases} x \equiv 1 \pmod{17} \\ x \equiv 1 \pmod{16} \end{cases}$$

Entonces, aplicando el **teorema chino del resto**:

$$m = m_1 \cdot m_2 = 17 * 16 = 272{+}1 = 273.$$

Se le suma $+1$, para que la condición tenga sentido y obtengamos el número menor de monedas que puede contener el cofre. □

Supongamos que la solución anterior es el número real de monedas en el cofre y que la historia continúa: siempre que sobran monedas en el reparto, hay una pelea y muere un pirata. ¿Cuántos piratas quedarán vivos cuando en el reparto no sobre ninguna moneda?

Solución. Trivial. Usando la función la función mód, tenemos, para el número menor de monedas (273):

$$\begin{aligned} 273 &\equiv 1 \ (\text{mód} 17) \\ 273 &\equiv 1 \ (\text{mód} 16) \\ 273 &\equiv 3 \ (\text{mód} 15) \\ 273 &\equiv 7 \ (\text{mód} 14) \\ 273 &\equiv 0 \ (\text{mód} 13) \end{aligned}$$

Por lo tanto, quedarán vivos 13 piratas cuando ya no sobre ninguna moneda. □

Referencias

Rosen, K. H. and Krithivasan, K. (2012). *Discrete mathematics and its applications: with combinatorics and graph theory*. Tata McGraw-Hill Education.