Universidad Autónoma Metropolitana
Unidad Iztapalapa
División de Ciencias Básicas e Ingeniería
Departamento de Matemáticas

Matemáticas Discretas I
Resoluciones de ecuaciones con congruencias

Trimestre 2019I

Problema. En caso de que tenga solución, resuelve la ecuación

$$8x \equiv 3 \mod 45. \tag{1}$$

Solución. Para poder despejar la x, primero debemos buscar un número para multiplicar por ambos lados de forma tal que obtengamos un número congruente con uno módulo 45 como coeficiente de la x, es decir, buscamos un **inverso módulo** 45 de 8. ¿Cuándo existe dicho inverso? Existe cuando 8 y 45 son primos relativos, es decir, cuando $\mathrm{mcd}(8, 45) = 1$. Utilicemos el algoritmo de Euclides para obtener su máximo común divisor.

$$45 = 5 \cdot 8 + 5 \tag{2}$$
$$8 = 1 \cdot 5 + 3 \tag{3}$$
$$5 = 1 \cdot 3 + 2 \tag{4}$$
$$3 = 1 \cdot 2 + \boxed{1} \tag{5}$$
$$2 = 2 \cdot 1 + 0 \tag{6}$$

De la última fórmula donde $b = 1$ y $r = 0$, se sigue que $\mathrm{mcd}(b, r) = \mathrm{mcd}(1, 0) = \mathrm{mcd}(8, 45) = 1$. Por lo tanto, como 8 y 45 sí son primos relativos, se sigue que 8 **sí tiene** inverso módulo 45.

Para encontrar un inverso, utilizaremos las ecuaciones previas para expresar 1 como combinación líneal de 8 y 45. Primero, despejamos los residuos en las ecuaciones 2–6:

$$1 = 3 - 1 \cdot 2 \tag{7}$$
$$2 = 5 - 1 \cdot 3 \tag{8}$$
$$3 = 8 - 1 \cdot 5 \tag{9}$$
$$5 = 45 - 5 \cdot 8 \tag{10}$$

Finalmente, substituimos «para atrás»:

$$
\begin{aligned}
1 &= \boxed{3 - 1 \cdot 2} && \text{Por la ecuación 7} \\
&= 5 - 1(\boxed{5 - 1 \cdot 3}) && \text{Por la ecuación 8} \\
&= 3 - 5 + 1 \cdot 3 \\
&= 2 \cdot 3 - 5 \\
&= 2(\boxed{8 - 1 \cdot 5}) - 5 && \text{Por la ecuación 9} \\
&= 2 \cdot 8 - 2 \cdot 5 - 5 \\
&= 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (\boxed{45 - 5 \cdot 8}) && \text{Por la ecuación 10} \\
&= 2 \cdot 8 - 3 \cdot 45 + 15 \cdot 8 \\
&= 17 \cdot 8 - 3 \cdot 45
\end{aligned}
$$

Verificamos que $17 \cdot 8 - 3 \cdot 45 = 136 - 135 = 1$.

Ya tenemos que

$$1 = 17 \cdot 8 - 3 \cdot 45$$

y despejamos el sumando que tiene a 8 por factor (porque queremos su inverso)

$$17 \cdot 8 = 1 + 3 \cdot 45.$$

Por lo tanto, tenemos que

$$17 \cdot 8 \equiv 1 \text{ mód } 45. \tag{11}$$

Al combinar las ecuaciones 1 y 11, tenemos que

$$17 \cdot 8x \equiv 17 \cdot 3 \text{ mód } 45. \tag{12}$$

Luego,

$$136x \equiv 51 \text{ mód } 45. \tag{13}$$

Pero tenemos que $136 \text{ mód } 45 = 1$ y $51 \text{ mód } 45 = 6$. Por lo tanto,

$$x \equiv 6 \text{ mód } 45. \tag{14}$$

Se sigue que $x = 6$ es una solución de la ecuación 1:

$$
\begin{aligned}
8x &\equiv 3 \text{ mód } 45 \\
8 \cdot 6 &\equiv 3 \text{ mód } 45 \\
48 &\equiv 3 \text{ mód } 45,
\end{aligned}
$$

pero claramente $48 \text{ mód } 45 = 3$.

Ya que la ecuación solución $x \equiv 6 \text{ mód } 45$, de hecho todos los números que sean congruentes con seis módulo 45 serán soluciones de la ecuación 1, como por ejemplo: 51, 96 y -39. Es decir, las soluciones de ese tipo de ecuaciones no son únicas.