Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Solución Ayudantía 4

Álgebra I - MAT2227

Fecha: 2019/08/27

1) a) Se nota que $18 \mid 4x - 7$, por lo que específicamente $2 \mid 4x - 7$, y por ende $2 \mid -7$, pero eso es una contradicción.

b)

$$\begin{aligned} 10x &\equiv 5 \mod 20 \quad /\text{Se divide por } 5, 20 \\ 2x &\equiv 1 \mod 4 \quad / -1 \\ 2x - 1 &\equiv 0 \mod 4 \quad \text{Se nota que } 2x-1 \text{ es impar, pero } 4 \mid 2x-1 \end{aligned}$$

No tiene solución.

c)

$$\begin{aligned} 5(34x - 24) &\equiv 22 - 4x \mod 76 \\ 170x - 120 &\equiv 22 - 4x \mod 76 \quad / + 4x + 120 \\ 174x &\equiv 144 \mod 76 \quad \text{Reduciendo 174 y 144} \\ 22x &\equiv 68 \mod 76 \quad \text{Dividiendo por } (22, 76) = 2 \\ 11x &\equiv 34 \mod 38 \quad / \cdot 7 \\ 77 &\equiv 238 \mod 38 \quad \text{Reduciendo 77 y 238} \\ x &\equiv 10 \mod 38 \end{aligned}$$

Con lo que se tiene una solución

d)

$$\begin{aligned} 25 - x &\equiv 3(x+2) \quad \text{mód } 27 \\ 25 - x &\equiv 3x + 6 \quad \text{mód } 27 \quad / + x - 6 \\ 19 &\equiv 4x \quad \text{mód } 27 \quad / \cdot 7 \\ 133 &\equiv 28x \quad \text{mód } 27 \quad \text{Reduciendo 133 y 28} \\ 25 &\equiv x \quad \text{mód } 27 \end{aligned}$$

Juntando ambas se tiene $x \equiv 808 \mod (27 * 38)$

2) Se nota que si $a^{16} \equiv 1 \mod 17$ para todo $a \in \mathbb{Z}_{17}$, se tiene lo pedido. Dado un a coprimo con 17, sean $r_1, \ldots, r_{16} \in \mathbb{Z}_{17} \setminus \{0\}$, todos los números coprimos con 17, luego $ar_1, \ldots, ar_{16} \in \mathbb{Z}_{17} \setminus \{0\}$ también son números coprimos con 17, por lo tanto se tiene la siguiente congruencia:

$$r_1 \cdot r_2 \cdot \cdots \cdot r_{15} \cdot r_{16} \equiv ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{15} \cdot ar_{16} \quad \text{mód } 17$$

Reagrupando se ve lo siguiente:

$$r_1 \cdot r_2 \cdot \cdots \cdot r_{15} \cdot r_{16} \equiv a^{16} \cdot (r_1 \cdot r_2 \cdot \cdots \cdot r_{15} \cdot r_{16}) \quad \text{mód } 17$$

Y como cada r_i es coprimo con 17 se tiene que $a^{16} \equiv 1 \mod 17$. Con esto se tiene lo pedido.

3) Como $(a, 68) = (b, 68) = 1$, específicamente $(a, 17) = (b, 17) = 1$, por lo que $a^{16} \equiv b^{16}$ mód 17, o equivalentemente $17 \mid b^{16} - a^{16}$. Como $(a, 68) = 1$ específicamente se tiene $(a, 2) = 1$, por lo que $a \equiv 1 \mod 4$ o $a \equiv 3 \mod 4$, luego viendo cada caso:

$$\begin{aligned} a \equiv 1 \quad \text{mód } 4 &\implies a^2 \equiv 1 \quad \text{mód } 4 \\ a \equiv 3 \quad \text{mód } 4 &\implies a^2 \equiv 3^2 \equiv 9 \equiv 1 \quad \text{mód } 4 \end{aligned}$$

Por lo que si $(a, 2) = 1$ se tiene que $a^2 \equiv 1 \mod 4$, más aún $a^{16} \equiv 1 \mod 4$. Como esto solo dependía de $(a, 2) = 1$, tambien se aplica a b, por lo que $a^{16} \equiv b^{16} \equiv 1 \mod 4$, por lo que $4 \mid b^{16} - a^{16}$. Juntando esto con lo anterior se tiene que $68 \mid b^{16} - a^{16}$.

4) Se generan las siguientes particiones de $\mathbb{Z}_p \setminus \{0\}$:

$$x, x^{-1}$$

Donde x^{-1} es el inverso modular de x[1], para que esto sea una partición se necesita que en cada subconjunto solo estén esos elementos, para eso es suficiente ver que cada elemento tiene un único inverso y es el único inverso de su inverso[2]. Con esto se tiene que cada partición esta bien definida y es a lo más de tamaño dos, las únicas particiones de tamaño menor cumplen que son su propio inverso:

$$\begin{aligned} x^2 &\equiv 1 \mod p \quad / -1 \\ x^2 - 1 &\equiv 0 \mod p \\ (x-1)(x+1) &\equiv 0 \mod p \end{aligned}$$

Como p es primo se tiene que $p \mid (x-1)$ o $p \mid (x+1)$, por lo que $x \equiv \pm 1 \mod p$. Esto implica que las únicas particiones de tamaño 1 son $\{1\}, \{-1\}$. Usando esta información se agrupan los elementos del producto $(p-1)!$ cada uno con su inverso, exceptuando $p-1$ y 1, y se llega a la siguiente expresión:

$$(p-1)! \equiv (p-1) \cdot 1 \equiv -1 \mod p$$

Demostrando lo pedido.

[1] $x \cdot x^{-1} \equiv 1 \mod p$

[2] Aquí x^{-1} es el único elemento en $\mathbb{Z}_p$ tal que $x \cdot x^{-1} \equiv 1 \mod p$, similarmente x es el único que cumple lo mismo para x^{-1}