Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática

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

Solución Ayudantía 5

Álgebra I - MAT2227

Fecha: 2019/08/29

1) 1)

$$\begin{aligned} 3x &\equiv 7 \mod 10 \quad / \cdot 7 \\ 21x &\equiv 49 \mod 10 \quad \text{Reduciendo 21 y 49} \\ x &\equiv 9 \mod 10 \\ x &\equiv 5y \mod 6 \quad / \cdot 5 \\ 5x &\equiv 25y \mod 6 \quad \text{Reduciendo 25} \\ 5x &\equiv y \mod 6 \end{aligned}$$

Entonces se tiene que $y = 6n + 5x$ y $x = 9 + 10k$, por lo que se tienen todas las soluciones.

2) Usando el teorema chino del resto se tiene lo siguiente:

$$x \equiv 2 \cdot \frac{M}{3} \cdot \left(\frac{M}{3}\right)_3^{-1} + 5 \cdot \frac{M}{7} \cdot \left(\frac{M}{7}\right)_7^{-1} + 6 \cdot \frac{M}{8} \cdot \left(\frac{M}{8}\right)_8^{-1} \mod M$$

Donde $M = 3 \cdot 7 \cdot 8$ y $\left(\frac{M}{n}\right)_n^{-1}$ es un entero tal que $\left(\frac{M}{n}\right) \cdot \left(\frac{M}{n}\right)_n^{-1} \equiv 1 \mod n$. Se ven los valores:

$$\begin{aligned} 7 \cdot 8 &\equiv 2 \mod 3 \\ 7 \cdot 8 \cdot 2 &\equiv 1 \mod 3 \end{aligned}$$

Por lo que $\left(\frac{M}{3}\right)_3^{-1} = 2$

$$3 \cdot 8 \equiv 3 \mod 7$$
$$3 \cdot 8 \cdot 5 \equiv 1 \mod 7$$

Por lo que $\left(\frac{M}{7}\right) a_7^{-1} = 5$

$$3 \cdot 7 \equiv 5 \mod 8$$
$$3 \cdot 7 \cdot 5 \equiv 1 \mod 8$$

Por lo que $\left(\frac{M}{8}\right)_8^{-1} = 5$. Con lo que se puede calcular x.

3) Se reescriben las congruencias de la siguiente forma:

$$x \equiv -8 \cdot (4y - 6) \mod 25 \qquad x \equiv -16 \cdot (23y - 8) \mod 49$$

Ahora se juntan ambos cosas y se usa el teorema chino del resto:

$$x \equiv -8 \cdot (4y - 6) \cdot 49 \cdot (-1) - 16 \cdot (23y - 8) \cdot 25 \cdot 2 \mod (25 \cdot 49)$$

Simplificando la congruencia anterior se tienen todas las soluciones.

2) Se recuerda que $\exists n, k \in \mathbb{Z} : an + bk = (a, b)$, por lo que si x tiene inverso modular se tiene lo pedido. Como $x^a \equiv 1 \mod m$ entonces $x \cdot x^{a-1} \equiv 1 \mod m$, por lo que x tiene inverso modular. Ahora $x^a \equiv 1 \mod m$ por lo que $x^{an} \equiv 1 \mod m$, similarmente $x^{bk} \equiv 1 \mod m$, combinando ambos se tiene que $1 \equiv x^{an+bk} \equiv x^{a,b} \mod m$.

3) Se tiene que $a \mid x - y$ y $b \mid x - y$, por lo que escribiendo la descomposición prima de a y de b de las siguientes maneras:

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \qquad b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$$

Donde los p_i están ordenados y $\alpha_i, \beta_i \geq 0$[1]. Luego se ve que:

$$\text{mcm}(a, b) = p_1^{\text{máx}(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\text{máx}(\alpha_n, \beta_n)}$$

Por lo que es suficiente que cada $p_i^{\text{máx}(\alpha_i, \beta_i)}$ dividan $x - y$ para que $\text{mcm}(a, b) \mid x - y$. Ahora, para un i fijo se tiene que o $\alpha_i \geq \beta_i$ con lo que se nota que $p_i^{\alpha_i} \mid x - y$, o $\alpha_i < \beta_i$

[1]Esto garantiza que las factorizaciones de a y de b sean faciles de comparar.

con lo que se nota que $p_i^{\beta_i} \mid x - y$, como en ambos casos $p_i^{\text{máx}(\alpha_i,\beta_i)} \mid x - y$ se tiene lo pedido. Por lo que $x \equiv y \mod \text{mcm}(a, b)$

4) Sean $a = 4$, $b = 6$, $x = 0$ e $y = 12$, se tiene $12 \equiv 0 \mod 4$ y $12 \equiv 0 \mod 6$, pero no se tiene que $0 \equiv 12 \mod 24$

5) Se recuerda que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ por lo que el problema es equivalente a $n(n+1) = 2 \cdot 10^k = 2^{k+1} \cdot 5^k$, como $(n, n+1) = 1$ se tiene que $n = 5^k$ y $n + 1 = 2^{k+1}$, o $n + 1 = 5^k$ y $n = 2^{k+1}$, por lo que el problema es ver para cuales k se tiene $5^k = 2^{k+1} + 1$ o $5^k + 1 = 2^{k+1}$. Y como 5^k crece más rápido que 2^{k+1}, esto tiene a lo más dos soluciones que se pueden encontrar verificando casos: $k = 1 \implies 5^1 = 2^2 + 1$. Por lo que para $k = 1$ y $n = 4$ se tiene lo pedido.