

EXAMEN - 15 DE JULIO DE 2022.

Soluciones.

Ejercicio 1. Sea $0 \leq m < 297$ tal que $m \equiv 108^{132} \pmod{297}$. Calcular m .

Solución. El criterio de divisibilidad entre 3 nos sugiere dividir 297 entre 3 repetidas veces, obteniendo $297 = 3^3 \cdot 11 = 27 \cdot 11$. Como 108 es múltiplo de 3, es claro que $108^{132} \equiv 0 \pmod{27}$. Calculemos ahora m módulo 11:

$$m \equiv 108^{132} \equiv 9^{132} \equiv 9^2 \equiv 4 \pmod{11},$$

donde usamos que $\varphi(11) = 10$. Ahora, por el Teorema Chino del resto, sabemos que existe un único $0 \leq m < 297$ que cumple $m \equiv 0 \pmod{27}$ y $m \equiv 4 \pmod{11}$. Casualmente vemos en la cuenta anterior que $9^2 \equiv 4 \pmod{11}$ y claramente $9^2 \equiv 0 \pmod{27}$. Por lo tanto $m = 81$.

Ejercicio 2.

Solución. Sean $n = 341$ y $e = 13$. Para los datos anteriores sea la función de descifrado $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definida por el protocolo RSA. Determinar $D(y)$.

Solución. El criterio de divisibilidad entre 11 nos sugiere dividir 341 entre 11, con lo cual obtenemos $341 = 11 \cdot 31$. Por lo tanto $\varphi(341) = 10 \cdot 30 = 300$. Sabemos que el dato secreto d en el protocolo RSA debe cumplir $e \cdot d \equiv 1 \pmod{300}$. Usando el Algoritmo de Euclides extendido vemos que $300 - 23 \cdot 13 = 1$, entonces $d \equiv -23 \pmod{300}$ cumple lo requerido. Es más conveniente tomar $d = 277$. Por lo tanto $D(y) = y^{277} \pmod{n}$.

Debe decir: $ed \equiv 1 \pmod{300}$

Ejercicio 3.

- a. Dado $n \in \mathbb{N}$, definir congruencia módulo n .

Solución. En las notas de teórico es la Definición 2.2.1.

- b. Sea $n = 10x + y$, probar que $n \equiv 0 \pmod{7}$ si y solo si $x - 2y \equiv 0 \pmod{7}$.

Solución. Multiplicando por -2 vemos que vemos que $10x + y \equiv 0 \pmod{7}$ si y solo si $-20x - 2y \equiv 0 \pmod{7}$, y por otra parte $x - 2y \equiv 0 \pmod{7}$ si y solo si $-20x - 2y \equiv 0 \pmod{7}$.

Concluimos que $10x + y \equiv 0 \pmod{7}$ si y solo si $x - 2y \equiv 0 \pmod{7}$.

- c. Enunciar el Teorema Chino del Resto y demostrarlo solo para el caso de dos ecuaciones.

Solución. En las notas de teórico es el Teorema 2.5.1.

- d. Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 \pmod{5}$ y $3x + 4 \equiv 3 \pmod{7}$.

Solución. La primera congruencia equivale a $2x \equiv 1 \equiv 6 \pmod{5}$, es decir $x \equiv 3 \pmod{5}$. La segunda congruencia equivale a $3x \equiv -1 \equiv 6 \pmod{7}$, es decir $x \equiv 2 \pmod{7}$. Usando el Teorema Chino es fácil ver que $x \equiv 23 \pmod{35}$. Como además queremos que x sea par, debe ser $x \equiv 58 \pmod{70}$.

La menor solución a esta congruencia mayor a 199 es $x = 58 + 3 \cdot 70 = 268$.

Ejercicio 4.

- a. Definir morfismo de grupos.

Solución. En las notas de teórico es la Definición 3.9.1.

- b. Enunciar y demostrar el Teorema de órdenes.

Solución. En las notas de teórico es el Teorema 3.9.8.

c. Dado un número primo impar p se define $f : U(p) \rightarrow U(p)$ la función dada por $f(\bar{x}) = \bar{x}^2$.

I) Probar que f es un morfismo de grupos.

Solución. En efecto $f(\bar{x} \cdot \bar{y}) = (\bar{x}\bar{y})^2 = \bar{x}^2\bar{y}^2 = f(\bar{x}) \cdot f(\bar{y})$.

II) Calcular el núcleo de f para $p = 3, 5$ y 7 .

Solución. Para $p = 3$, tenemos $f(\bar{1}) = \bar{1}$ y $f(\bar{2}) = \bar{1}$ así que el núcleo es $\{\bar{1}, \bar{2}\} = \{\bar{1}, -\bar{1}\}$.

Para $p = 5$, tenemos $f(\bar{1}) = \bar{1}$, $f(\bar{2}) = \bar{4}$, $f(\bar{3}) = \bar{4}$ y $f(\bar{4}) = \bar{1}$ así que el núcleo es $\{\bar{1}, \bar{4}\} = \{\bar{1}, -\bar{1}\}$.

Para $p = 7$, tenemos $f(\bar{1}) = \bar{1}$, $f(\bar{2}) = \bar{4}$, $f(\bar{3}) = \bar{2}$, $f(\bar{4}) = \bar{2}$, $f(\bar{5}) = \bar{4}$ y $f(\bar{6}) = \bar{1}$ así que el núcleo es $\{\bar{1}, \bar{6}\} = \{\bar{1}, -\bar{1}\}$.

III) Calcular el núcleo de f en general y deducir cuantos elementos tiene la imagen de f .

Solución. En los tres casos de la parte anterior, vimos que el núcleo es $\{\bar{1}, -\bar{1}\}$. Veamos que esto vale para cualquier p . Por definición el núcleo de f es

$$\ker f = \{\bar{x} \in U(p) : \bar{x}^2 - 1 = 0\}.$$

El polinomio $X^2 - 1$ tiene grado 2, así que tiene a lo sumo 2 raíces distintas en $U(p)$ (ver Lema 4.1.9 en las notas). Pero $\bar{1}$ y $-\bar{1}$ son claramente dos raíces distintas ya que $p \neq 2$. Concluimos que $\ker f = \{\bar{1}, -\bar{1}\}$.

El Teorema de órdenes implica que $|U(p)| = |\ker f| \cdot |\operatorname{im} f|$, como $|U(p)| = p - 1$ y $|\ker f| = 2$ obtenemos $|\operatorname{im} f| = \frac{p-1}{2}$.