

EXAMEN - 13 DE FEBRERO DE 2015. DURACIÓN: 4 HORAS.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

- Probar que si $1 \leq n \leq 130$ y $n = a \cdot b$, con a, b naturales, entonces $a \leq 11$ o $b \leq 11$.
- Listar todos los primos menores o iguales a 130, explicando brevemente el método utilizado.
- Un coleccionista de discos tiene 3860 dolares que piensa gastar en discos. Los precios de los discos que le interesan de su tienda favorita son de 238 dolares y 178 dolares. ¿Cuántos discos puede comprar el coleccionista utilizando todo el dinero?

Ejercicio 2.

- Hallar $x \equiv 79^{221} \pmod{81}$, con $0 \leq x < 81$.
- Hallar el mínimo x positivo tal que $x \equiv 11^{181} \pmod{595}$.

Ejercicio 3.

- Sea $n = 86$.
 - Hallar el orden de 9 módulo n , es decir el orden de $\bar{9} \in U(n)$.
 - Hallar una raíz primitiva módulo n .
- Para hallar la clave hay que calcular

$$994^{12} \pmod{997} \equiv (-3)^{12} \pmod{997} \equiv 9^6 \pmod{997} \equiv 81^3 \pmod{997}.$$

Calculemos la potencia anterior, $81^2 = 6561 = 6 \cdot 1000 + 561 = 6 \cdot (997 + 3) + 561 \equiv 6 \cdot 3 + 561 \pmod{997} \equiv 18 + 561 \pmod{997} \equiv 579 \pmod{997}$. $81^3 \equiv 81 \cdot 579 \pmod{997} \equiv 46899 \pmod{997} \equiv 46 \cdot (3 + 997) + 899 \pmod{997} \equiv 138 + 899 \pmod{997} \equiv 40 \pmod{997}$

Ejercicio 4.

- Ver teórico.
- Ver teórico.
 - Ver teórico.
- Es falso. Por ejemplo, si $G = U(12)$, con $|G| = \varphi(12) = 4$, se cumple que $\overline{-1}^1 = \overline{-1}^3$ en $U(12)$, pero $1 \not\equiv 3 \pmod{4}$.