Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Matemática

Listado 04: Función de Euler y orden módulo n
Teoría de Números (527288)

1. Sean $n \geq 2$ y a coprimo con n. Mostrar que $n - a$ también es coprimo con n.

2. Sea U_n el grupo de invertibles módulo n. Usando el problema anterior, mostrar que la función $f : U_n \to U_n$ dada por $f(a) = n - a$ es una biyección.

3. Usando el problema anterior, mostrar que si $n > 2$, entonces $\varphi(n)$ es par. *(Indicación: recordar que $\varphi(n)$ tiene varias definiciones: una de ellas es la cardinalidad de U_n.)*

4. Sea $n > 2$. A partir de la expresión

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right)$$

verificar que $\varphi(n)$ es par. *(Indicación: considerar dos casos: cuando n es potencia de 2, y cuando n tiene un factor primo impar.)*

5. Notar: el número 257 es primo. Por lo tanto $\varphi(257) = 256 = 2^8$. Explicar por qué esto significa que para determinar el orden de $a \in U_{257}$ basta mirar el conjunto

$$\{a, a^2, a^4, a^8, a^{16}, a^{32}, a^{64}, a^{128}\}$$

6. Usar el ejercicio anterior para determinar el orden de 2 módulo 257 y el orden de 5 módulo 257. ¿Es alguno de ellos raíz primitiva?

Mini-proyecto: teorema de Wilson

El teorema de Wilson describe los números primos en función del cálculo de factoriales.

7. Para $n \in \{2, 3, \ldots, 12\}$, calcular $(n-1)! \pmod{n}$. Describir algún patrón encontrado. *(Observación: hay un número que se comporta diferente a los demás.)*

8. Si $n = a \cdot b$, con $a \neq b$, explicar por qué $(n-1)! \equiv 0 \pmod{n}$.

9. Si $n = a^2$, con $a > 2$, explicar por qué $(n-1)! \equiv 0 \pmod{n}$.*(Indicación: $2a < n$.)*

10. Si n es primo, sea g una raíz primitiva módulo n. Escribir $(n-1)!$ como una potencia de g módulo n. ¿Cuál es el exponente de dicha potencia?

11. Verificar que el exponente del ejercicio anterior no es múltiplo de $\varphi(n)$. Explicar por qué esto significa que $(n-1)! \not\equiv 1 \pmod{n}$.

12. Usando el ejercicio anterior: si n es primo, mostrar que $(n-1)!^2 \equiv 1 \pmod{n}$. *(Indicación: mostrar que el nuevo exponente de g es múltiplo de $\varphi(n)$.)*

13. De los dos puntos anteriores concluir que, si n es primo, entonces $(n-1)! \equiv -1 \pmod{n}$.