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

Listado 05: Raíces primitivas módulo n
Teoría de Números (527288)

1. Sean g una raíz primitiva módulo n y k un número coprimo con $\varphi(n)$. Mostrar: g^k también es raíz primitiva módulo n.

2. Sean g una raíz primitiva módulo n y $k \geq 1$. Si g^k también es raíz primitiva módulo n, mostrar: k y $\varphi(n)$ son coprimos.

3. Sabiendo que 2 es raíz primitiva módulo 19, usar los ejercicios anteriores para determinar todas las raíces primitivas módulo 19.

4. Si $n \mid m$, mostrar: el orden de un elemento módulo n divide a su orden módulo m.

5. Encontrar una raíz primitiva módulo 5. A partir de ella, encontrar raíces primitivas módulo 25 y 125.

Mini-proyecto: existencia de raíces primitivas módulo $2p^\alpha$

En lo que sigue, sea $n > 2$ un número impar. Se demostrará lo siguiente: si g es raíz primitiva módulo n, entonces un elemento de $\{g, g+n\}$ es raíz primitiva módulo $2n$. Asumir que g es raíz primitiva módulo n.

6. Mostrar: $\varphi(n) = \varphi(2n)$.

7. Combinando el item anterior con el problema 4 de este listado, mostrar que si g tiene orden módulo $2n$, entonces es raíz primitiva módulo $2n$.

8. En relación a la expresión *si g tiene orden*: verificar que $g = 2$ es raíz primitiva módulo 5, pero no tiene orden módulo $2 \cdot 5 = 10$.

9. Si g no tiene orden módulo $2n$, mostrar que $g + n$ sí lo tiene.

10. Mostrar que $g + n$ es raíz primitiva módulo n.

11. Usando el problema 7 y el item anterior, concluir la demostración de la propiedad.