PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
INSTITUTO DE INGENIERIA MATEMATICA Y COMPUTACIONAL

Álgebra abstrácta y aplicaciones, Semestre II 2021
Tarea 3
Fecha de entrega: Viernes, Diciembre 5, 2025 (23:59 hora Santiago)

1 Ejercicio de programación [2 puntos]

En el archivo `ecdsa.py` mostrado en clases, y adjunto con esta tarea, terminen la implementación del algoritmo de firma con la curva elíptica secp256k1 especificada en el código. En particular, tienen qué completar la implementación de los métodos `sign` y `verify` en la Figure **??**. Adicionalmente, para poder computar la $e * C$, con e un número natural y C en punto en la curva elíptica, deben implementar esta operación usando el método *double and add*. Para validar su implementación se les deja un ejemplo. *Es importante destacar qué su firma será distinta a la desplegada allá*, dado qué el algoritmo de firma ocupa un parámetro aleatorio.

Puntaje es el siguiente (se evaluará de manera semi-independiente; quiere decir que si no implemntan la multiplicación escalar con el algoritmo double and add, se probará su solución con una implementación correcta de este método):

1. [**2 puntos**] Completar la implementación del método `def __rmul__(self, coefficient)`, la cual nos permite realizar la multiplicación escalar en la clase `Point`. Para que su solución funcione deben implementar este método usando el algoritmo double and add.
2. [**2 puntos**] Implementar el método `sign` de la clase `PrivateKey`.
3. [**2 puntos**] Imeplemntar el método `verify`.