



PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE  
ESCUELA DE INGENIERIA  
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

**Criptografía y Seguridad Computacional - IIC3253**  
**Ayudantía 8**  
**Alexander Pinto**

## Test de primalidad

1. Realice una demostración práctica del test de primalidad visto en clases para el número  $n = 137$ , con una probabilidad de error menor a 0.02.
2. Como parte del enunciado para el desarrollo de la Tarea 2, usted cuenta con el código de algunas funciones auxiliares. Explique en detalle las funciones `_is_probably_prime` y `es_potencia`.

3. Realice una demostración práctica del test de primalidad para los números:

$P = 1138635978041936386847462333038662758629597993511163194549328390767284389468$   
961478610140452303820384766400302879858094555412195493316565144895475971007768664  
63781814271673557022247941312150642379569909302715887114574430158983100551787005  
26009643888726738585998120562566732806649886086397912653034050178893859

$Q = 1158389097919437489229877538510503345601933436088389431674657627218724842389$   
072833056092604521954331322479352180330249249815794050512733603717539838857536549  
572347220644465877544459460806219430881604975789561518670631269886523216721614484  
39688550488904372167035366626051841175064590746743483812434310620662793

Reporte el tiempo de ejecución.