Matemáticas Avanzadas (Grado en Ingeniería de Computadores) **Curso 2021-2022**

Práctica 5
EJERCICIOS BÁSICOS

1. Sin usar ordenador, calcula cuál es el resto de dividir 20! entre 23. (**Pista:** busca la manera de utilizar el Teorema de Wilson).

2. Utiliza el algoritmo de exponenciación binaria para calcular:

   (a) $4^{171} (\mathrm{mod}\, 38)$ (b) $2^{142} (\mathrm{mod}\, 96)$.

3. Con los datos del ejercicio anterior, toma cada base y su exponente y aplica el test del Pequeño Teorema de Fermat (el módulo tendrás que cambiarlo). Tienes que escribir los pasos pero puedes usar `SAGE` para hacer los cálculos.

4. Decide si los siguientes números pasan, para la base dada, el test de primalidad de Miller (puedes usar `SAGE` para hacer los cálculos):

   (a) Número 1453 para la base 2.

   (b) Número 937 para la base 3.

`SAGE` 1. Implementa una función que utilice el Teorema de Wilson para decidir si un número dado es primo o no. Prueba con números grandes y utiliza `walltime` para comparar el tiempo que tarda tu función y el que tarda el comando `is_prime`. ¿Qué conclusiones sacas?

- Los ejercicios básicos son obligatorios y determinarán la calificación de las actividades semanales.
- Los ejercicios de refuerzo se proponen para adquirir mayor destreza. Tienen carácter opcional, por lo que podrán incrementar la calificación pero no disminuirla.
- Los ejercicios de profundización plantean cuestiones relacionadas fuera del temario de la asignatura. Son opcionales y el estudio de alguno de ellos proporcionará puntos extra.

EJERCICIOS DE REFUERZO

1. Sin usar ordenador, calcula cuál es el resto de dividir 16! entre 19. (**Pista:** busca la manera de utilizar el Teorema de Wilson).

2. Usa el Pequeño Teorema de Fermat para calcular:

   (a) $7^{2156} \pmod{11}$ (b) $14^{27354} \pmod{19}$.

3. Calcula, utilizando el algoritmo de exponenciación binaria:

   (a) $3^{134} \pmod{65}$ (b) $4^{205} \pmod{100}$ (c) $3^{215} \pmod{68}$ (d) $5^{83} \pmod{28}$.

4. Decide si los siguientes números pasan, para la base dada, el test de primalidad de Miller (tienes que escribir los pasos pero puedes usar `SAGE` para hacer los cálculos):

Número	1457	933	577
Base	2	3	4

5. Comprueba que 1729 es un pseudoprimo fuerte para la base 9 pero no para la base 2 (por tanto, no es primo).

`SAGE` 1. Implementa el algoritmo de exponenciación binaria para números enteros.

`SAGE` 2. Implementa el test de primalidad de Miller.

EJERCICIOS DE PROFUNDIZACIÓN

1. Sea $n \in \mathbb{N}$ y sea a coprimo con n. Se dice que a es un *residuo cuadrático* módulo n si la ecuación $x^2 \equiv a \pmod{n}$ tiene solución.

   (a) Encontrar los residuos cuadráticos módulo 11.

   (b) Demostrar que si $p \geq 3$ es primo y a no es divisible por p, entonces la ecuación $x^2 \equiv a \pmod{p}$ o bien no tiene soluciones, o bien tiene exactamente dos soluciones módulo p.

   (c) Demostrar que si $p \geq 3$ es primo entre los enteros $1, 2, \ldots, p-1$ hay exactamente $\frac{p-1}{2}$ residuos cuadráticos.

`SAGE` 1. Implementa un método que, dado un $n \in \mathbb{N}$, determine los elementos de $\mathbb{Z}_n^*$.

`SAGE` 2. Implementa el sistema criptográfico RSA.