A LA CAZA DE LOS NÚMEROS PRIMOS CON PYTHON

XVII Seminario Nacional ESTALMAT - Castro Urdiales

Marc Munar Covas, Juan Vicente Riera Clapés

Universitat de les Illes Balears

Govern de les Illes Balears
Conselleria d'Educació i Universitats

Real Academia de Ciencias Exactas, Físicas y Naturales de España

Purposeful Ventures

CIEM

Centro Internacional de Encuentros Matemáticos

Excmo. Ayuntamiento de Castro Urdiales

Financiado por la Unión Europea
NextGenerationEU

¿Cómo hemos llegado aquí?

SESIONES DE ESTALMAT

- Sesión *¿cómo hablamos a los ordenadores?*, segundo curso.
- Impartida desde el curso 2017-18.
  - Hasta el curso 2020-2021, programación con Python y aplicaciones generales.
  - Desde el curso 2021-2022, programación con Python y su aplicación al estudio de números primos.

SESIONES DE ESTALMAT

- Sesión *¿cómo hablamos a los ordenadores?*, segundo curso.
- Contenido:
  - Declaración de variables.
  - Python como calculadora.
  - Bucles `for` y `while`.
  - Funciones.
  - Estructuras de datos básicas (listas).

SESIONES DE ESTALMAT

- Sesión *¿cómo hablamos a los ordenadores?*, segundo curso.
- Aplicaciones:
  - Encontrar el mínimo/máximo dentro de una lista.
  - Revertir el orden de una secuencia (lista, suma, etc).

SESIONES DE ESTALMAT

- Sesión *¿cómo hablamos a los ordenadores?*, segundo curso.
- Aplicaciones:
  - Encontrar el mínimo/máximo dentro de una lista.
  - Revertir el orden de una secuencia (lista, suma, etc).
  - Test básico de primalidad y sucesivas mejoras.
  - Números primos de Mersenne.
  - Números de Fibonacci y comprobación de propiedades.
  - Cálculo del factorial y algunas propiedades.

- Sesión *Explorando algunos test de primalidad de números naturales*, veteranos.
- Objetivo: abordar el **Problema del Test de Primalidad**.

SESIONES DE ESTALMAT

- Sesión *Explorando algunos test de primalidad de números naturales*, veteranos.
- Contenido:
  - Introducción al problema de la primalidad. Evolución histórica.
  - Repaso básico de Python.
  - Test de división por tentativa.
  - Test de Wilson.
  - Test probabilístico de Miller-Rabin.
  - Test determinista polinomial de AKS.

Parte I - ¿Cómo hablamos a los ordenadores?

MATERIAL DE LA SESIÓN

MATERIAL DE LA SESIÓN

https://tinyurl.com/estalmatPython

EXPERIENCIA DE LA SESIÓN

- Valoración positiva del temario.
- Atracción del cálculo intenso.

EXPERIENCIA DE LA SESIÓN

- Valoración positiva del temario.
- Atracción del cálculo intenso.
- Dificultad inicial en la sintaxis.
- Dificultad en el razonamiento secuencial.

EXPERIENCIA DE LA SESIÓN

- Valoración positiva del temario.
- Atracción del cálculo intenso.
- Dificultad inicial en la sintaxis.
- Dificultad en el razonamiento secuencial.
- Alumnos con conocimiento previo, sesión a dos velocidades.
- Google Colab, imprescindible.

EXPERIENCIA DE LA SESIÓN

- Valoración positiva del temario.
- Atracción del cálculo intenso.
- Dificultad inicial en la sintaxis.
- Dificultad en el razonamiento secuencial.
- Alumnos con conocimiento previo, sesión a dos velocidades.
- Google Colab, imprescindible.
- **Pregunta del alumnado:** ¿no hay algo *mejor* para la primalidad?

PARTE II - TEST DE PRIMALIDAD

¿ES PRIMO?

999999 9999999999 9999999999 9999999841

Contenido de la sesión - Test básicos

- Resultados básicos de primalidad, con demostraciones.
  - Hay un número infinito de números primos.
  - Si p es primo, entonces $p = 6k + 1$ o $p = 6k - 1$, para algún entero k.

Contenido de la sesión - Test básicos

- Test básico de la división por tentativa, con demostraciones.
  - Primera mejora: límite superior $\lceil \frac{n}{2} \rceil$.
  - Segunda mejora: límite superior $\lfloor \sqrt{n} \rfloor$.

CONTENIDO DE LA SESIÓN - TEST BÁSICOS

- Test de Wilson, sin demostraciones.
  - Basado en el teorema de Wilson: n primo si, y solo si, $(n-1)! + 1$ divisible entre n.

- Test de Wilson, sin demostraciones.
  - Basado en el teorema de Wilson: n primo si, y solo si, $(n-1)! + 1$ divisible entre n.
  - Desventaja: $(1009-1)! + 1 \approx 4,17 \cdot 10^{2591}$.

- Test de Miller-Rabin, sin demostraciones pero con deducciones.

Teorema

Sea $n > 2$ un número primo, con $n = 1 + 2^j d$ y d impar. Entonces, la b-secuencia definida por

$$\{b^d, b^{2d}, b^{4d}, b^{8d}, \ldots, b^{2^{j-1}d}, b^{2^j d}\} \pmod{n}$$

tiene una de las dos formas siguientes:

$$(1, 1, \ldots, 1, 1, 1, \ldots, 1),$$

$$(?, ?, \ldots, ?, -1, 1, \ldots, 1),$$

reducida módulo n, para cualquier $2 \leq b \leq n - 1$. (Se ha denotado por ? un número diferente de ± 1).

CONTENIDO DE LA SESIÓN - MILLER RABIN

- Si n es primo, la b-secuencia de n será de una de las dos formas del teorema.

CONTENIDO DE LA SESIÓN - MILLER RABIN

- Si n es primo, la b-secuencia de n será de una de las dos formas del teorema.
- Si la b-secuencia es una de las dos formas del teorema, **no es cierto en general** que n sea primo, pero **es probable** que n sea primo.

- Si n es primo, la b-secuencia de n será de una de las dos formas del teorema.
- Si la b-secuencia es una de las dos formas del teorema, **no es cierto en general** que n sea primo, pero **es probable** que n sea primo.
- En otro caso, si la b-secuencia de n tiene una de las siguientes tres formas:

$$(?, \ldots, ?, 1, 1, \ldots, 1),$$

$$(?, \ldots, ?, ?, ?, \ldots, -1),$$

$$(?, \ldots, ?, ?, ?, \ldots, ?),$$

entonces n es compuesto.

Ejemplo

Apliquemos el test de Miller-Rabin a $n = 13$.

- $n - 1 = 12 = 2^2 \cdot 3$, así que $j = 2$ y $d = 3$.
- Consideremos $b = 4$, elegido aleatoriamente.
- La b-secuencia es $\left(4^3, (4^3)^2, (4^3)^4\right)$, y módulo n queda $(12, 1, 1)$. Ahora bien, $12 = 0 \cdot 13 + 1 = 1 \cdot 13 - 1$, así que $12 \equiv -1 \pmod{13}$.
- Concluimos que $n = 13$ es probablemente primo.

CONTENIDO DE LA SESIÓN - TEST AKS

- Test AKS, sin demostraciones pero con deducciones.
  - Test basado en operaciones de polinomios. Se requiere introducir aspectos previos.
  - Enteros módulo n: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
  - $\mathbb{Z}_n[X]$ polinomios (de cualquier grado) con coeficientes de $\mathbb{Z}_n$. Por ejemplo:
    - El polinomio $p(X) = X^2 + 3X + 2$ es un polinomio de $\mathbb{Z}_5[X]$.
    - Visto dentro de $\mathbb{Z}_3[X]$ sería $p(X) = X^2 + 0X + 2 = X^2 + 2$.

- Caracterización de un número primo $n \in \mathbb{N}$ usando polinomios.

Proposición

Sea $n \in \mathbb{N}$ con $n > 2$, y $a < n$ un entero coprimo con n. Entonces:

$$n \text{ primo} \Leftrightarrow \text{En } \mathbb{Z}_n[X], \text{ se tiene que } (X + a)^n = X^n + a.$$

Ejemplo

¿Es $n = 3$ primo con este criterio?

Podemos coger $a = 2$, que es un entero menor estricto y coprimo con n. Entonces,

$$(X + 2)^3 = X^3 + 6X^2 + 12X + 8,$$

pero lo tenemos que calcular en $\mathbb{Z}_3[X]$. Haciendo los cálculos, llegamos a la igualdad pedida.

- Puede parecer que el problema está resuelto, pero no.
- **Inconveniente:** Calcular $(X + a)^n$ es costoso, ya que

$$(X + a)^n = X^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i X^{n-i} + a^n.$$

- Puede parecer que el problema está resuelto, pero no.
- **Inconveniente:** Calcular $(X+a)^n$ es costoso, ya que

$$(X+a)^n = X^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i X^{n-i} + a^n.$$

- **Solución:**
  - No hay que comparar $(X+a)^n$ con $X^n + a$ de forma absoluta en $\mathbb{Z}_n[X]$.
  - Basta hacerlo módulo un polinomio $X^r - 1$, donde r se elige de forma técnica.

MATERIAL DE LA SESIÓN

https://tinyurl.com/estalmatTest