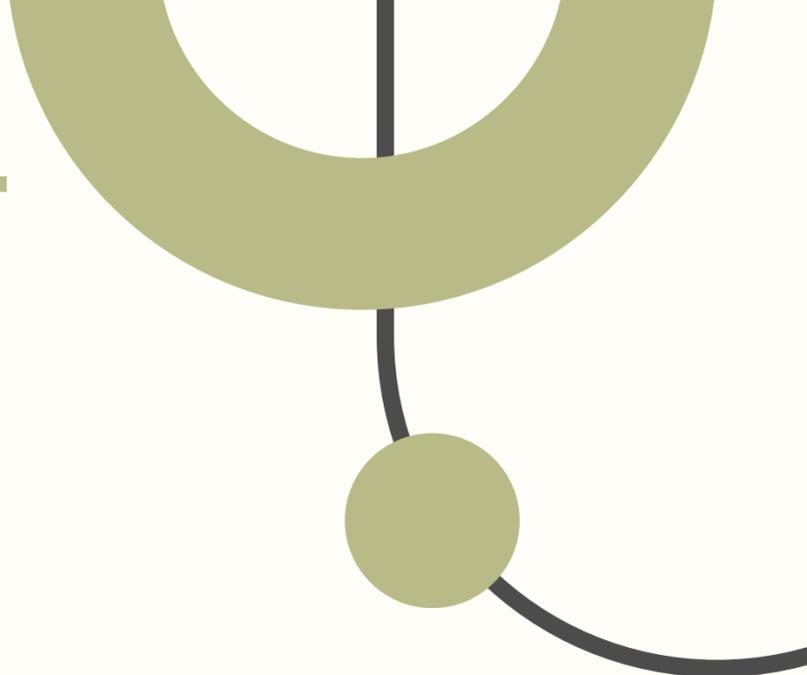


---

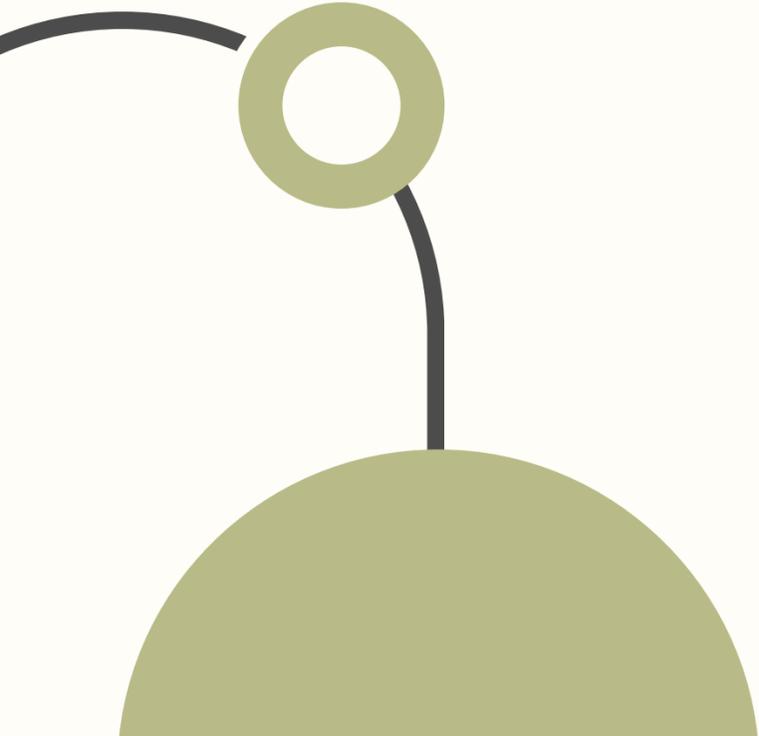


→

# COMPARACIÓN DE SOFTWARES DE TEORÍA DE NÚMEROS

Realizado por:  
Lourdes Saavedra

---



# Índice de CONTENIDOS



---

**01. Introducción**

---

**02. Problemas de Teoría de  
Números**

---

**03. Herramientas y lenguajes  
para Teoría de Números**

---

**04. Problema elegido para la  
comparación**

---

**05. ¿Por qué no usar Python?**

---

# Índice de CONTENIDOS



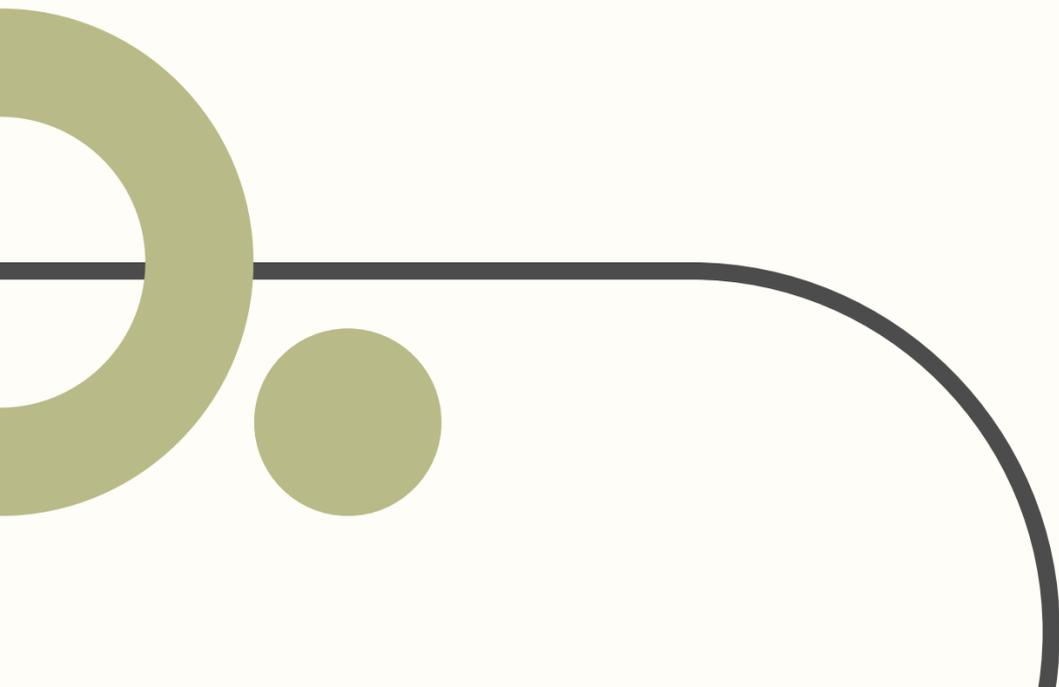
---

**06. Implementación en cada software**

---

**07. Asistentes de pruebas**

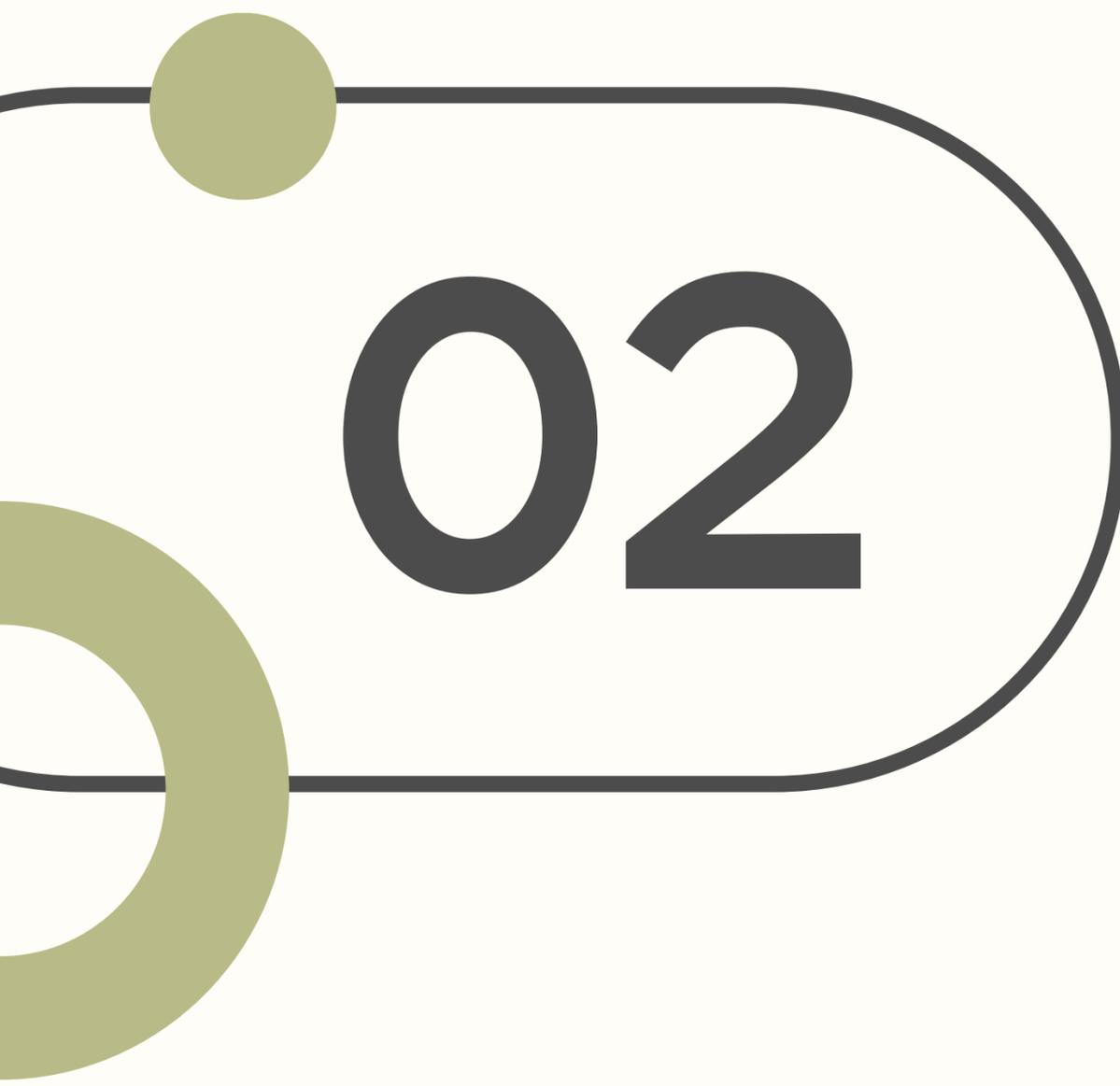
---



- **1950 - 1970**
  - Fortran - John Backus
  - Lisp - John McCarthy
- **1970-1990**
  - PARI/GP - Universidad de Bordeaux
  - Magma
  - Coq - Francia
- **1990-2010**
  - SageMath - Universidad de Washington.
  - Python - SymPy
- **2013 - presente**
  - Lean - Leonardo de Moura

# Un poco de historia

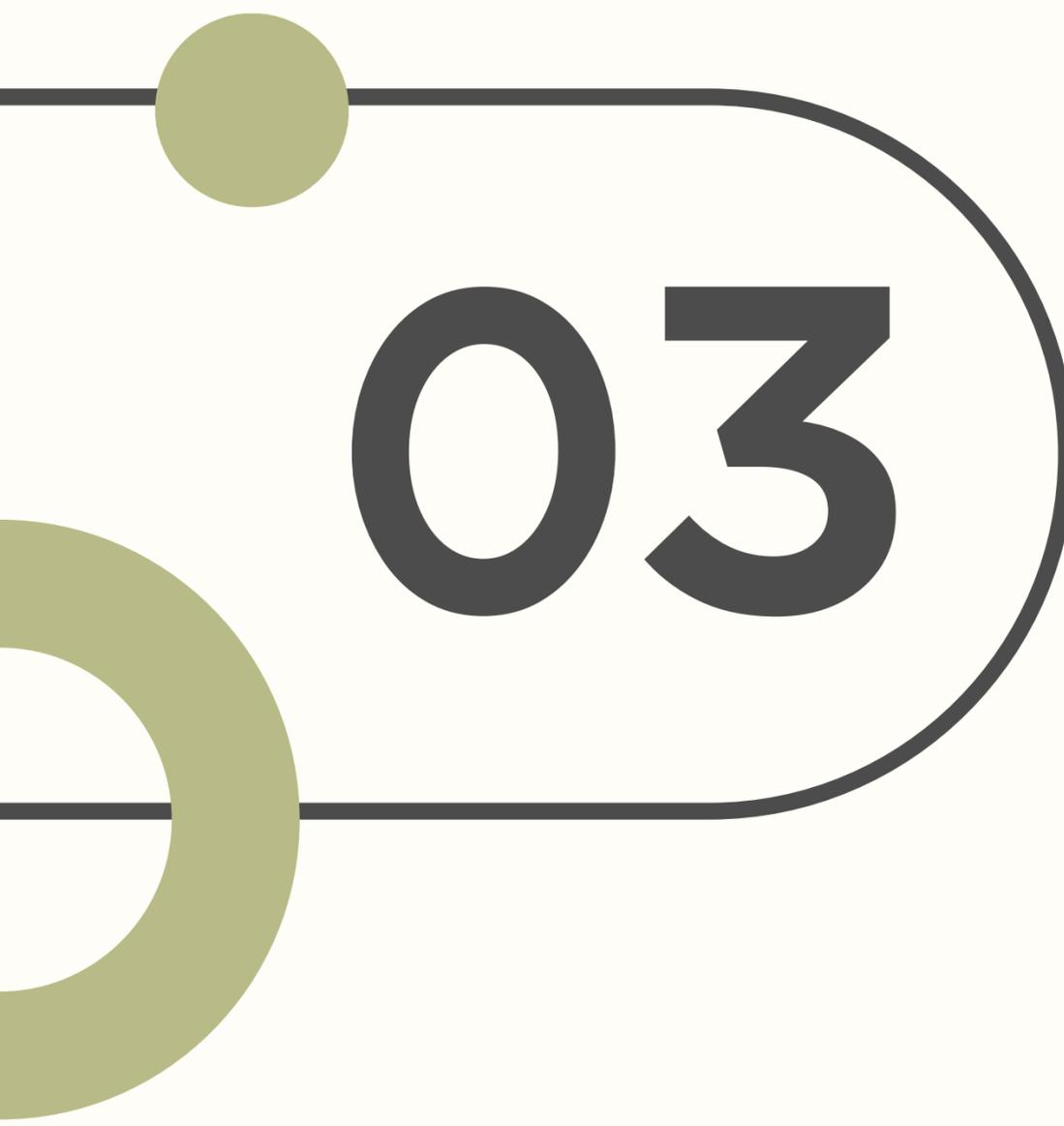




02

*Problemas de*  
**Teoría de**  
**Números**

- 
- 
- 
- **Factorización de números grandes**
  - **Pruebas de primalidad**
  - **Primos gemelos**



03

*Herramientas y lenguajes*

**Teoría de**

**Números**



# SAGEMATH Y PARI/GP



- **SageMath:**

- Sistema de software matemático de código abierto y gratuito.
- Se basa en muchos paquetes de código abierto ya existentes



# SAGEMATH Y PARI/GP



- **PARI/GP:**

- Es un sistema de álgebra computacional muy utilizado, diseñado para cálculos rápidos en Teoría de Números pero que también incluye un gran número de otras funciones útiles para operar con objetos matemáticos.
- Se puede obtener como una colección de rutinas en C para mayor rapidez de cálculo.

# TABLA COMPARATIVA

Aspecto	SageMath	PARI/GP
Licencia	GPL (software libre)	GPL (software libre)
Lenguaje base	Python	GP (lenguaje propio)
Áreas principales de aplicación	Matemáticas generales (álgebra, cálculo, combinatoria, criptografía)	Teoría de números, criptografía, cuerpos numéricos, curvas elípticas
Velocidad en cálculos numéricos	Buena, pero menos eficiente que PARI/GP en cálculos numéricos intensivos	Extremadamente rápida en cálculos numéricos y algebraicos
Capacidades gráficas	Sí, ofrece gráficos 2D y 3D	No, limitado en capacidades gráficas
Integración con otros sistemas	Integra NumPy, SciPy, SymPy, Maxima, GAP, y más	Se puede integrar con C, Python, y otros lenguajes
Facilidad de uso	Fácil para usuarios con experiencia en Python	Fácil para tareas específicas de teoría de números
Optimizado para Teoría de Números	Sí, pero es más generalista	Totalmente optimizado para Teoría de Números
Cálculos algebraicos complejos	Capaz, pero a veces más lento que PARI/GP	Muy eficiente en cálculos algebraicos complejos



04

*Problema elegido para*  
**Comparación**

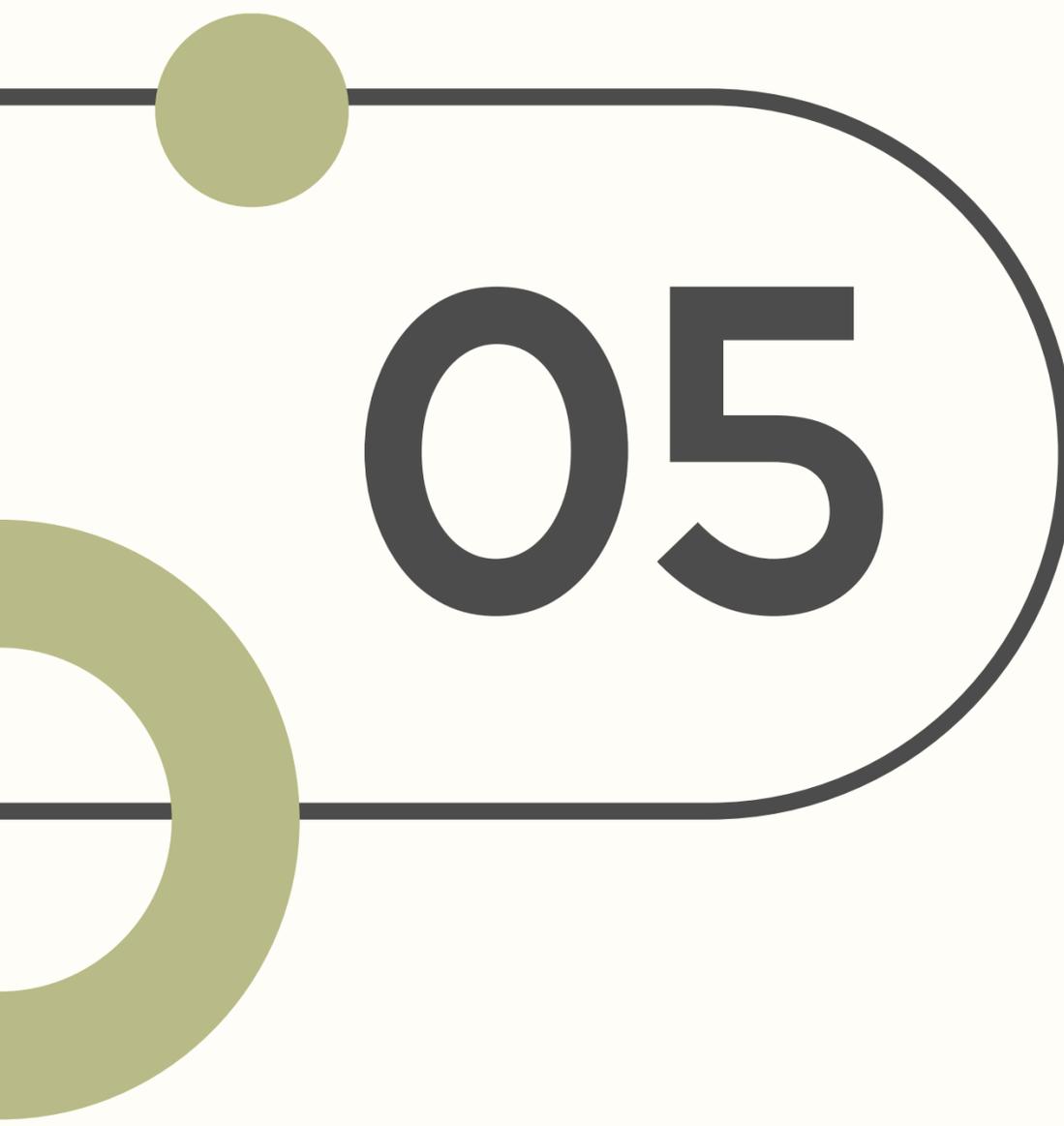
# ¿Qué son los primos gemelos?

## → DEFINICIÓN

Dos números primos  $p$  y  $q$  son primos gemelos si  $p$  y  $q$  difieren en 2. Es decir,  $q = p + 2$

## → PROBLEMA

Dado un  $N$ . encontrar todos los pares de primos gemelos menores que  $N$ .

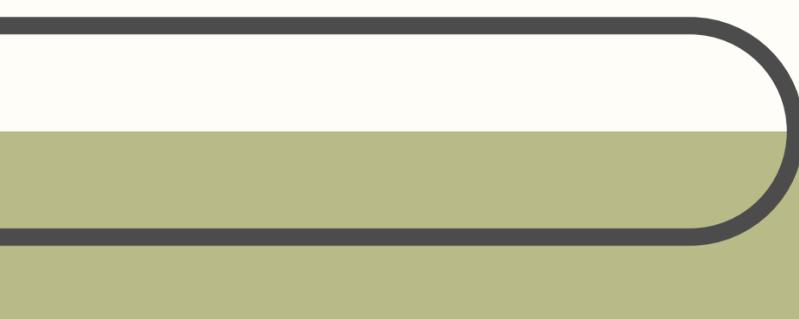


05

*¿Por qué no usar*  
**Python?**

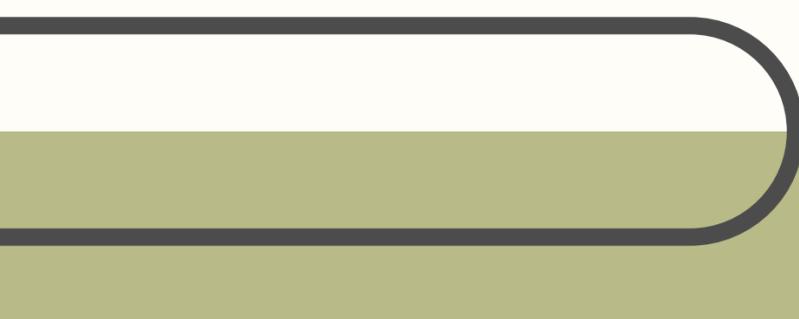


- **Optimización para cálculos matemáticos complejos:**

- SageMath y PARI/GP - diseñados para cálculos avanzados en matemáticas
  - Altamente optimizados para trabajar con números primos y enteros grandes
  - Python - no optimizado para cálculos numéricos a gran escala
- 

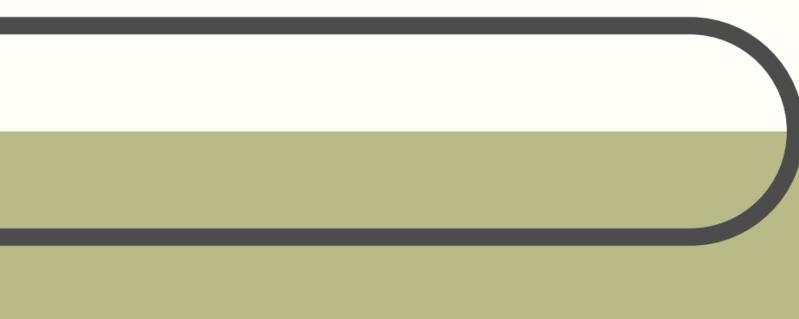


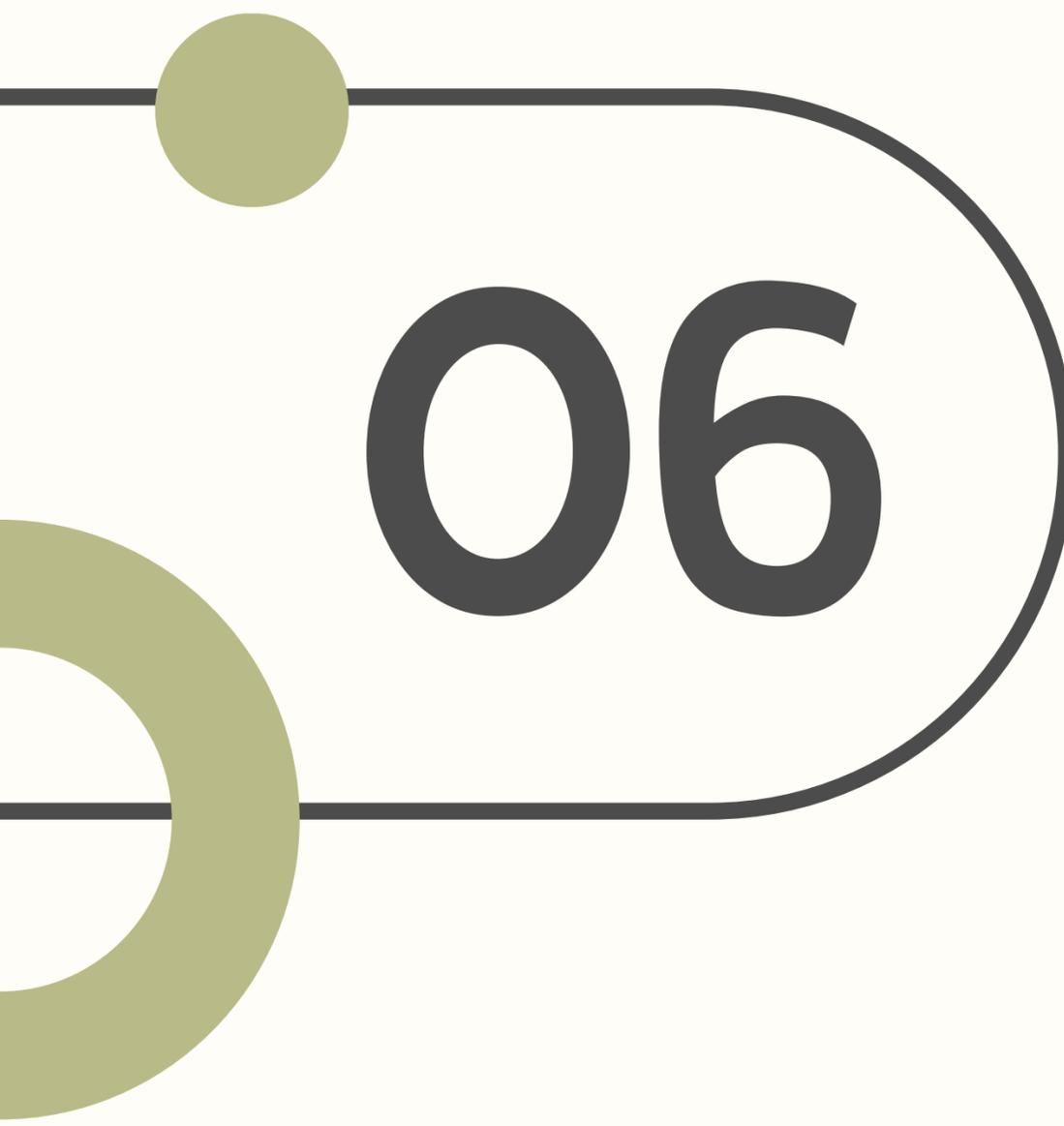
- **Velocidad de cálculo en Teoría de Números:**

- PARI/GP: extremadamente rápido en cálculos con números primos y factorización.
  - PARI/GP supera a SageMath en velocidad
  - PARI/GP se enfoca en cálculos de Teoría de Números
- 



- **Implementación de algoritmos avanzados:**

- SageMath y PARI/GP - algoritmos específicos para la teoría de números y álgebra avanzada.
  - En Python - algoritmos deben ser desarrollados o importados
- 



06

*Implementación en cada*

**Software**



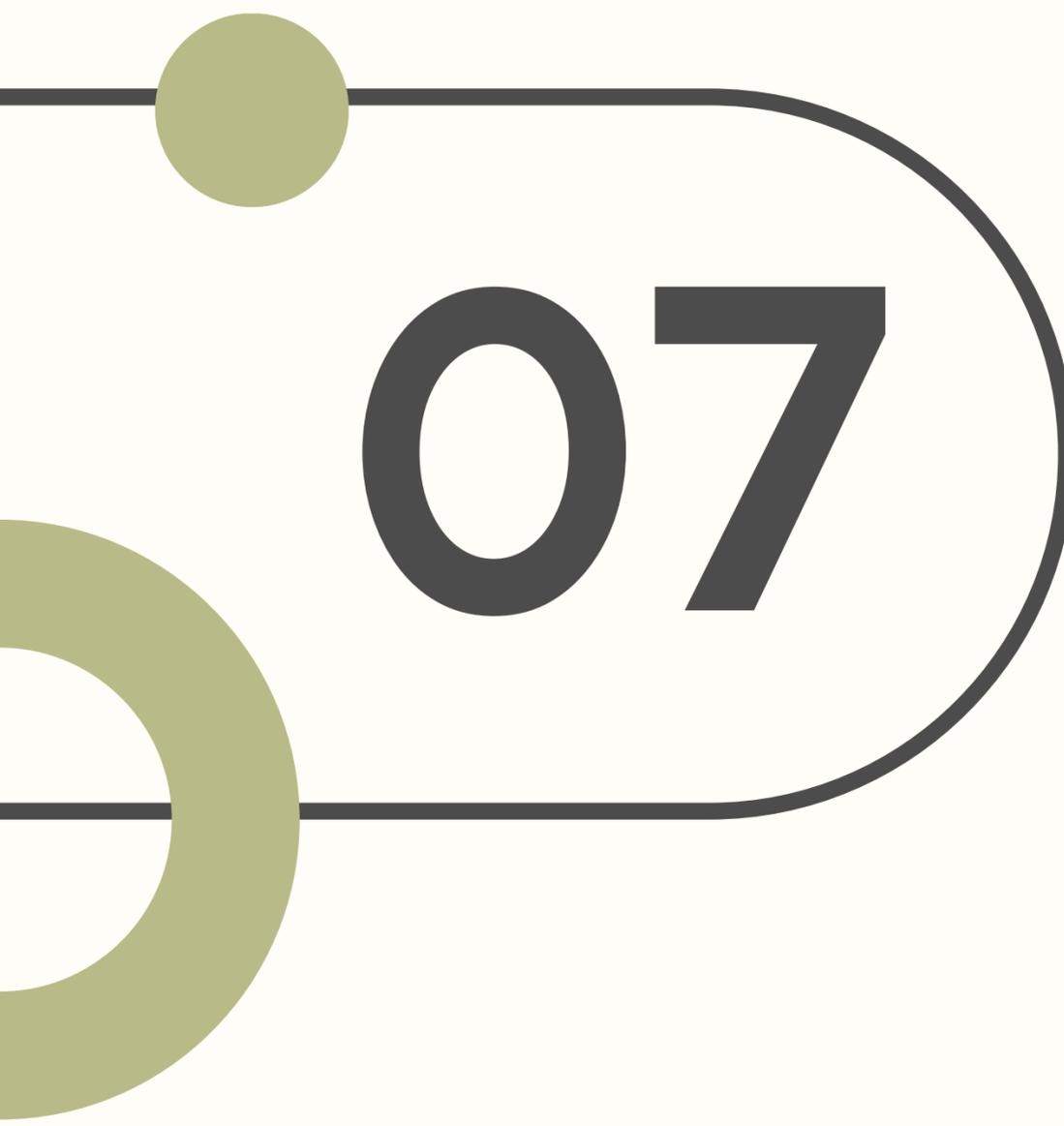
# Código en Python



# Código en SageMath



# Código em PARI/GP



07

*Asistentes de*  
**Pruebas**



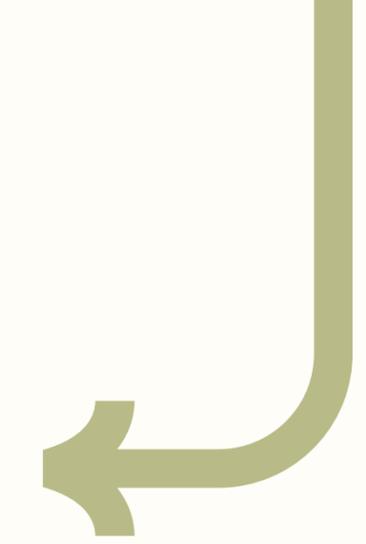
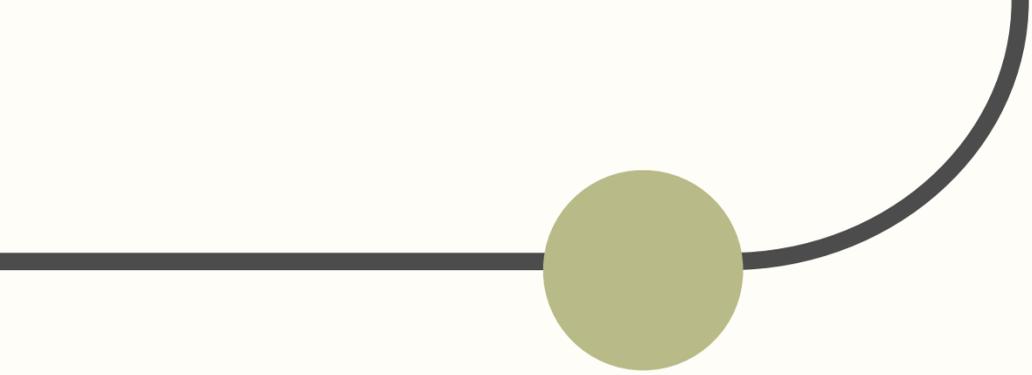
# → LEAN Y COQ ←

## • Lean:

- Biblioteca mathlib
- Verificación rigurosa
- Interactividad
- Curva de aprendizaje

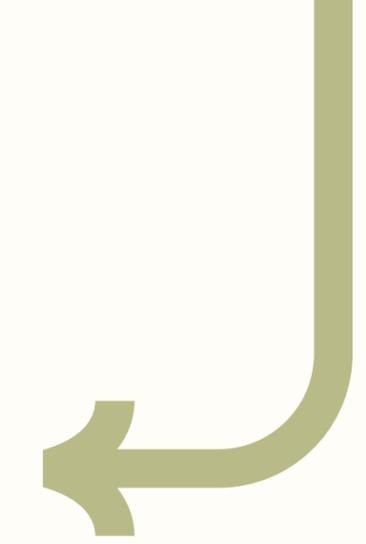
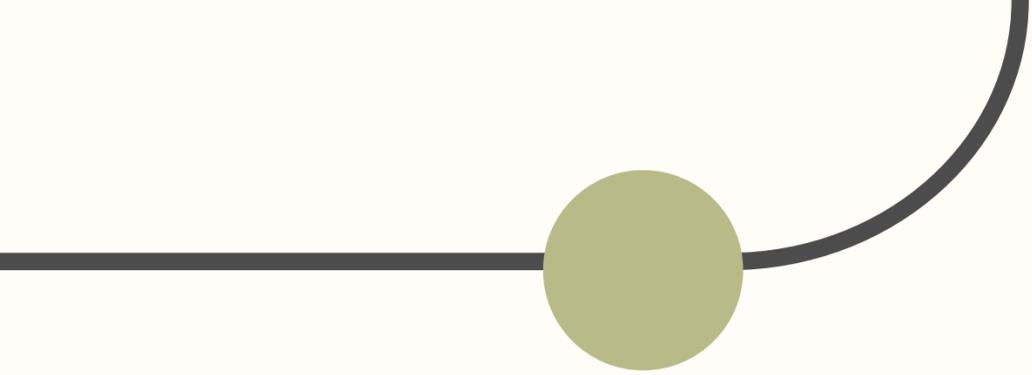
## • Coq:

- Amplia biblioteca de matemáticas
- Soporte para álgebra y teoría de grupos.
- Interfaz y flexibilidad
- Complejidad en pruebas largas



# Demostración en Coq





# Demostración en Lean





# Referencias:

- SageMath. (s.f.). SageMath - Open-Source Mathematics Software. Recuperado de <https://www.sagemath.org/index.html>
  - PARI/GP. (s.f.). PARI/GP Frequently Asked Questions. Recuperado de <https://pari.math.u-bordeaux.fr/faq.html>
  - Universidad Nacional de Colombia. (2013). Análisis y aplicación de algoritmos de teoría de números en problemas criptográficos [Tesis de grado, Universidad Nacional de Colombia]. Repositorio Institucional UNAL. <https://repositorio.unal.edu.co/bitstream/handle/unal/21321/830200.2013.pdf>
  - The Lean Project. (s.f.). About Lean. Recuperado de <https://lean-lang.org/about/>
  - INRIA. (s.f.). The Coq Proof Assistant. Recuperado de <https://coq.inria.fr/>
- 



Muchas  
**GRACIAS**

