

---

**Nombre de la unidad curricular:** Teoría de Números

---

**Licenciaturas:** Matemática

---

**Frecuencia y semestre de la formación al que pertenece:** Bianual - segundo semestre

---

**Créditos asignados:** 12 - Área A, A6 intermedio

---

**Nombre del/la docente responsable:** Gustavo Rama

---

**E-mail:** gusrama@cmat.edu.uy

---

**Requisitos previos:** Conocimientos básicos de Álgebra

---

**Ejemplos de unidades curriculares de Facultad de Ciencias u otros que aportan dichos conocimientos:** Álgebra lineal 2

---

**Conocimientos adicionales sugeridos:**

---

**Objetivos de la unidad curricular:**

**a) Herramientas, conceptos y habilidades que se pretenden desarrollar**

**b) En el marco del plan de estudios**

**Temario sintético de la unidad curricular:**

- Números primos
- Congruencias
- Criptografía de clave pública
- Reciprocidad cuadrática
- Fracciones continuas
- Formas cuadráticas
- Curvas elípticas y criptografía

**Temario desarrollado:**

- Números primos (Dos semanas)
  1. División entera, algoritmo de Euclides, factorización única.
  2. Infinitud de los números primos.
- Congruencias (Dos semanas)
  1. Ecuaciones lineales.
  2. Teoremas de Fermat y de Euler.
  3. Teorema chino de los restos.
  4. Cálculo de inversos y potencias, raíces primitivas.
- Criptografía de clave pública (Dos semanas)
  1. Intercambio de clave Diffie-Hellman, criptosistema RSA.
  2. Ataques al RSA y factorización.
- Reciprocidad cuadrática (Tres semanas)
  1. Residuos cuadráticos, criterio de Euler.
  2. Demostración de la ley.
  3. Sumas de Gauss, otra demostración.
  4. Cálculo de raíces módulo  $p$ .
- Fracciones continuas (Dos semanas)
  1. Fracciones continuas finitas, convergencia de fracciones continuas infinitas.
  2. Irracionales cuadráticos y fracciones continuas periódicas.
  3. Reconocimiento de racionales.
- Formas cuadráticas (Dos semanas)
  1. Sumas de dos cuadrados, algunos teoremas de Fermat.
  2. Representación de números por formas cuadráticas.
  3. Clases de formas cuadráticas, reducción.
  4. Representación por discriminante y número de clases 1.
- Curvas elípticas y criptografía (Dos semanas)
  1. Definición, ley de grupo geométrica.

2. Factorización usando curvas elípticas.
  3. Criptografía usando curvas elípticas, ElGamal, problema del logaritmo discreto.
- 

## **Bibliografía**

---

### **a) Básica:**

Stein, William - Elementary number theory: primes, congruences, and Secrets.

### **b) Complementaria:**

Serre, J. P. - A course in arithmetic

---

**Modalidad cursada:** Presencial

---

**Metodología de enseñanza:**

---

**Duración en semanas:** 15

---

**Carga horaria total:** 180

---

**Carga horaria detallada:**

**a) Horas aula de clases teóricas:** 3

**b) Horas aulas de clases prácticas:** 1.5

**c) Horas de seminarios:**

**d) Horas de talleres:**

**e) Horas de salida de campo:**

**f) Horas sugeridas de estudio domiciliario durante el período de clase:** 112.5

---

**Sistema de APROBACIÓN final**

**Tiene examen final:** Si

**Se exonera el examen final:** No

**Nota de exoneración (del 3 al 12):**

**Sistema de GANANCIA**

**a) Características de las evaluaciones:**

Exoneración de examen práctico.

Entrega de ejercicios por práctico, más una lista de ejercicios final.

**b) Porcentaje de asistencia requerido para ganar la unidad curricular:** 0

**c) Puntaje mínimo individual de cada evaluación y total:** El curso se gana con 50 de los puntos. El examen práctico se exonera con 70.

**d) Modo de devolución o corrección de pruebas:**

**COMENTARIOS o ACLARACIONES:**

---

Iguá 4225 esq. Matajojo • 11.400 Montevideo – Uruguay  
Tel. (598) 2525 0378 • (598) 2522 947 • (598) 2525 8618 al 23 ext. 7 110 y 7 168 • Fax (598)  
2525 8617