Nombre de la unidad curricular: Seminario de Curvas Elípticas y Criptografía

Licenciaturas: Matemática

Frecuencia y semestre de la formación al que pertenece: 1 seminario semanal de 1 hora y media de duración.

Créditos asignados: 5

Nombre del/la docente responsable: Claudio Qureshi

E-mail: cqureshi@fing.edu.uy

Requisitos previos: Álgebra lineal. Nociones de teoría de grupos y anillos.

Ejemplos de unidades curriculares de Facultad de Ciencias u otros que aportan dichos conocimientos: \"Álgebra Lineal 1\" y \"Grupos y Teoría de Galois\" (en caso de no haber cursado este curso puede hablar con el docente)

Conocimientos adicionales sugeridos:

Teoría de números. Matemática Discreta. Curvas algebraicas (no imprescindible).

Objetivos de la unidad curricular:

a) Herramientas, conceptos y habilidades que se pretenden desarrollar

Desarrollar la teoría básica de curvas elípticas sobre un cuerpo K. Estudiar especialmente el caso en que K sea un cuerpo finito y discutir varias aplicaciones en criptografia.

b) En el marco del plan de estudios

Temario sintético de la unidad curricular:

1. Puntos racionales en cónicas.
2. La geometría de curvas cúbicas.
3. El grupo de una curva elíptica.
4. Cuerpos finitos.
5. Curvas elípticas sobre cuerpos finitos.
6. Algoritmo de factorización usando curvas elípticas.
7. Criptografía de curvas elípticas.
8. La cota de Hasse-Weil para el números de puntos de una curva elíptica sobre un cuerpo finito.
9. Algoritmos para el cálculo de puntos de una curva elíptica sobre un cuerpo finito.
10. Estructura de grupo de una curva elíptica sobre un cuerpo finito.

Temario desarrollado:

1. Puntos racionales en cónicas (parametrización de puntos racionales, relación con ternas pitagóricas y con el problema de los números congruentes). 2. La geometría de curvas cúbicas (algunos resultados de geometría algebraica de curvas útiles para definir la ley de grupo) 3. El grupo de una curva elíptica (fórmulas explícitas para la ley de grupo, breve discusión de curvas sobre los reales y complejos). 4. Cuerpos finitos (construcción y principales propiedades, el isomorfismo de Frobenius). 5. Curvas elípticas sobre cuerpos finitos (resultados básicos). 6. Algoritmo de factorización usando curvas elípticas (repaso del algoritmo p-1 de Pollard, Algoritmo de Lenstra). 7. Criptografía de curvas elípticas (Diffie-Helman para curvas elípticas, el problema del logaritmo discreto en curvas elípticas). 8. La cota de Hasse-Weil para el números de puntos de una curva elíptica sobre un cuerpo finito. 9. Algoritmos para el cálculo de puntos de una curva elíptica sobre un cuerpo finito (Algoritmo de Schoff y variantes). 10. Estructura de grupo de una curva elíptica sobre un cuerpo finito.

Bibliografía

---

a) Básica:

1. J. H. Silverman, J. T. Tate, \"Rational Points on Elliptic Curves\" 2nd edition, Springer.
2. J.Von zur Gathen, \"CryptoSchool\", Springer.
3. T. R. Shemanske, Modern Cryptography and Elliptic Curves Vol. 83. American Mathematical

Soc.

b) Complementaria:

4. R. Lidl, H. Niederreiter. Finite fields. Cambridge university press.
5. J.H.Silverman, \"The Arithmetic of Elliptic Curves\", Springer.
6. N. Koblitz, \"Algebraic Aspects of Cryptography\", Springer.
7. N. Koblitz, \"A Course on Number Theory and Cryptography\", 2nd edition, Springer.

Modalidad cursada: Seminario

Metodología de enseñanza:

Duración en semanas:

Carga horaria total: 75

Carga horaria detallada:

a) Horas aula de clases teóricas: 19.5

b) Horas aulas de clases prácticas: 0

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: 55.5

Sistema de APROBACIÓN final

Tiene examen final: No

Se exonera el examen final:

Nota de exoneración (del 3 al 12):

Sistema de GANANCIA
a) Características de las evaluaciones:

Exposición oral y entrega de ejercicios.

b) Porcentaje de asistencia requerido para ganar la unidad curricular: 90

c) Puntaje mínimo individual de cada evaluación y total: 5

d) Modo de devolución o corrección de pruebas:

COMENTARIOS o ACLARACIONES:

Por tratarse de un seminario el concepto final es aprobado (sin nota) o reprobado.
Para aprobar el estudiante debe realizar al menos un par de presentaciones orales y obtener al menos un 50 total de puntaje en la lista de ejercicios.
