SEMINARIOS DE MATEMÁTICA PARA ESTUDIANTES DE GRADO

DESCRIPCIÓN DE LAS UNIDADES CURRICULARES

1. Nombre y descripción de las unidades curriculares

El *Seminario "Curvas Elípticas y Criptografía"* (MA217) es una actividad tipo seminario en donde se pretende un acercamiento a las actividades de investigación y comunicación de un trabajo científico de matemática para estudiantes de grado.

2. Licenciaturas en las que se enmarcan las unidades curriculares

Licenciatura en Matemática, Licenciatura en Física.

3. Frecuencia y semestre de la formación al que pertenece

Reuniones con duración de 1 hora y media, una vez por semana, durante el segundo semestre de 2020. Para poder inscribirse al seminario, el estudiante deberá tener validado al menos 90 créditos de la carrera.

4. Créditos asignados

5 créditos.

5. Ubicación dentro del plan de estudios

Es una actividad de tipo seminario, área A (matemática).

6. Nombre del/la docente responsable

Claudio Michael Qureshi Valdez

7. Correo electrónico

cqureshi@fing.edu.uy

8. Requisitos previos

Para poder inscribirse al seminario, el estudiante deberá tener validado al menos 90 créditos de la carrera.

Previas: Conocimiento de álgebra lineal, anillos y módulos y teoría elemental de números.

Date: November 18, 2020.

9. Objetivos de la unidad curricular

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

El objetivo del seminario es aproximar al estudiante a la investigación en matemática, integrándolo en la creación y desarrollo de un abordaje científico concreto, vinculado a amplios aspectos de la actividad de investigación en matemática. Se pretende además que el estudiante adquiera experiencia en la transmisión de conocimientos adquiridos a un público de pares, en un ámbito de discusión académica.

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

El seminario constituye, junto con la actividad "Trabajo monográfico", parte de la currícula en la Licenciatura en Matemática destinada a la aproximación al trabajo de investigación y difusión de los conocimientos.

10. Temario sintético de las unidades curriculares

Desarrollar la teoría básica de curvas elípticas. Estudiar especialmente el caso de curvas elípticas sobre cuerpos finitos y discutir aplicaciones en criptografía.

11. Temario desarrollado

- Curvas afines y proyectivas (ref. [Fulton]).
- Curvas elípticas, ley de grupo y forma normal de Weierstrass (ref. [SilvermanTate]).
- Diffie-Helmann y El-Gamal clásicos y la versión con curvas elípticas (refs. cap. 8.2 de [Shemanske] y cap 6.2 de [KoblitzNT]).
- Cuerpos finitos: existencia, unicidad, construcción, extensiones y el automorfismo de Frobenius (ref. [LidlNiederreiter]).
- Algoritmo de Factorización de Lenstra y de primalidad basado en curvas elípticas (ref. cap. 6.3 y 6.4 de [KoblitzCrypto]).
- Algoritmo de Schoof para calcular el número de puntos de una curva elíptica sobre un cuerpo finito (ref. [Schoof]).
- Algoritmo de Harvey para calcular el número de puntos de una curva elíptica sobre un cuerpo finito.
- Isogenias de curvas elípticas y aplicación al PLD (refs. [Silverman] y [Qureshi]).
- Puntos de l-torsión y pairing de Weil (refs. [Silverman] y [Dias]).
- Computación eficiente del pairing de Weil (ref. [Dias]).
- Ataque MOV: reducción del PLD de curvas elípticas a cuerpos finitos (ref. [Dias]).

12. Bibliografía

(a) *Básica*

i. [SilvermanTate] 1. J. H. Silverman, J. T. Tate, "Rational Points on Elliptic Curves" 2nd ed., Springer.
ii. [Silverman] J.H.Silverman, "The Arithmetic of Elliptic Curves", Springer.
iii. [Shemanske] T. R. Shemanske, "Modern Cryptography and Elliptic Curves" Vol. 83. American Mathematical Soc.
iv. [KoblitzNT] N. Koblitz, "A Course on Number Theory and Cryptography", 2nd ed., Springer.

v. [KoblitzCrypto] Koblitz, Neal. Algebraic aspects of cryptography. Vol. 3. Springer Science & Business Media, 2012.

(b) *Complementaria*

vi. [Gathen] 2. J.Von zur Gathen, "CryptoSchool", Springer.
vii. [AshGrossGross] Ash, Avner, Robert Gross, and Robert Gross. Elliptic tales: curves, counting, and number theory. Princeton University Press, 2012.
viii. [Fulton] Fulton, William. "Algebraic curves." An Introduction to Algebraic Geom (2008): 54.
ix. [LidlNiederreiter] R. Lidl, H. Niederreiter. "Finite fields". Cambridge university press.
x. [Schoof] Schoof, René. "Counting points on elliptic curves over finite fields." Journal de théorie des nombres de Bordeaux 7.1 (1995): 219-254.
xi. [Qureshi] Qureshi, Claudio. "Criptografía de Curvas Elípticas y Logaritmo Discreto". Tesis de maestría, UdelaR.
xii. [Dias] Dias da Cruz, Steve. "Elliptic Curve Cryptography and the Weil pairing". bachelor Thesis, Université du Luxembourg.

13. Modalidad de la actividad

La actividad se desarrolla en modalidad mixta. Con reuniones semanales presenciales que se transmiten en directo a través de Zoom para quienes opten no acudir a clases.

14. Metodología de enseñanza

Presentación por parte de los participantes de conferencias abordando parte de la temática. Los estudiantes deberán realizar al menos una exposición oral y elaborar unas notas con un resumen del tema de su exposición.

15. Duración en semanas

La actividad abarcará todo el semestre, por lo que espera una duración de 15 semanas.

16. Carga horaria total

Las actividades tendrán una carga horaria total de trabajo por parte de los estudiantes de 75 horas, correspondientes a 5 créditos.

17. Carga horaria detallada

Se harán 15 x 1.5 = 22.5 horas de conferencias, el resto de la carga horaria está destinada al trabajo individual del estudiante.

18. Sistema de aprobación

El seminario se aprueba con nota APROBADO/NO APROBADO; para aprobar el seminario, el estudiante deberá realizar al menos una exposición y la elaboración de unas notas con resumen de su exposición. Se espera que el estudiante participe activamente en las sesiones del seminario.

19. Comentarios o aclaraciones

El cronograma específico del seminario varía en función del desarrollo del seminario.