MAT 6630 *Courbes elliptiques et formes modulaires*
Hiver 2017, Plan de cours

Langage:	À déterminer en classe. Français/Anglais au bureau.
Échéancier :	Du 10 janvier au 12 avril (pas de cours le 28 février et le 1er mars) mardi 11h-13h et mercredi 13h30 - 14h30 Pav. ANDRE-AISENSTADT 4186

Professeure :	Matilde N. Lalín
	Pav. ANDRE-AISENSTADT 5145
	Disponibilités mardi 13 - 14 et mercredi 11h30 - 12h30
	Possibilité d'autres périodes de disponibilité sur rendez-vous.
	`mlalin@dms.umontreal.ca`
	`www.dms.umontreal.ca/~mlalin/mat6630`

Manuels recommandés :	"Elliptic Curves", de J. S. Milne, BookSurge Publishers, 2006 "The Arithmetic of Elliptic Curves", de J. Silverman, Second Edition, Springer, 2009.
Devoir:	Le devoir sera placé sur la page web du cours. Il faut le remettre en classe les jours: 31 janvier, 14 février, 7 mars, 21 mars, 4 avril. Les devoirs qui seront remis en retard ne seront pas acceptés.
Barème :	Travaux pratiques (devoir) 100 % (Tous les devoirs seront répartis également.) Le devoir le moins bon de chaque étudiant sera ignoré.
Note final :	Combinaison des mesures absolues et de distribution.

Objectifs et généralités : L'une des grandes questions de la théorie des nombres concerne la résolution des équations polynomiales en nombres entiers ou rationnels (équations diophantiennes). Les polynômes de degré 1 ou 2 sont bien compris. La prochaine étape consiste à étudier les équations de degré 3. Essentiellement une courbe elliptique est définie par une équation de la forme

$$y^2 = x^3 + ax + b.$$

Il s'avère que les solutions rationnelles de cette équation forment un groupe, abélien et de type fini (théorème de Mordell). La connaissance du rang de ce groupe implique une conjecture célèbre (Birch – Swinnerton-Dyer) dont la résolution vaut un million de dollars.

Les courbes elliptiques apparaissent dans de nombreuses aires (qui ne sont pas a priori liées), comme les nombres congruents, l'empaquetage de sphères, la factorisation d'entiers, etc. Ils sont également liées aux formes modulaires qui est le point de départ de la preuve du dernier théorème de Fermat.

Matière : Le but de ce cours est d'étudier les fondements des courbes elliptiques et, si le temps le permet, leur relation avec les formes modulaires.

Nous envisageons de discuter des sujets suivants.

1. Courbes planes, cubiques, la structure de groupe en cubiques.
2. La définition de courbes elliptiques, l'équation de Weierstrass, les courbes elliptiques modulo p, les points de torsion.
3. La structure complexe des courbes elliptiques.
4. L'arithmétique des courbes elliptiques. Les groupes de Selmer et de Tate–Shafarevich, le théorème de Mordell, les courbes elliptiques sur des corps finis, la conjecture de Birch–Swinnerton-Dyer.
5. Les courbes elliptiques et les formes modulaires. Les formes modulaires, la fonction L d'une courbe elliptique.

Quelques rappels :

- La date limite pour modifier un choix de cours et pour abandonner un cours sans frais : le 20 janvier.
- La date limite pour abandonner un cours avec frais : le 10 mars.
- Il est fait obligation à l'étudiant de motiver une absence prévisible à une évaluation dès qu'il est en mesure de constater qu'il ne pourra être présent, il appartiendra à l'autorité compétente de déterminer si le motif est acceptable (règlement des études de premier cycle `http://www.etudes.umontreal.ca/reglements/reglements.html`).

  Les examens intra-trimestriels n'ont pas de reprise. En cas d'absence motivée (voir la procédure prévue par le règlement pédagogique), la note de l'examen final sera attribuée à l'intra manqué. Pour les étudiants ayant été absents au final et ayant motivé leur absence, un examen différé sera tenu.
- Le plagiat attention, c'est sérieux! L'étudiant est invité à consulter le site `http://www.integrite.umontreal.ca`
- Pour la disponibilité des livres en bibliothèque, contacter le comptoir de prêt (`http://www.bib.umontreal.ca/nous-joindre/MI.htm`) ou la bibliothécaire Ferroudja Nazef (`f.nazef@umontreal.ca`)

Clause de non-responsabilité : Les erreurs typographiques dans ce plan de cours sont sujettes à des changements qui seront annoncés en classe.

MAT 6630 *Elliptic Curves and Modular Forms*
Winter 2017, Syllabus

Language:	To be determined (lectures). French and English (office hours).
Dates:	January 10 to April 12 (no classes on February 28 and March 1st) Tuesdays 11AM - 1PM and Wednesdays 1:30PM - 2:30PM Pav. ANDRE-AISENSTADT 4186

Professor:	Matilde N. Lalín
	Pav. ANDRE-AISENSTADT 5145
	Office hours Tuesdays 1PM - 2PM and
	Wednesdays 11:30AM - 12:30PM or by appointment.
	`mlalin@dms.umontreal.ca`
	`www.dms.umontreal.ca/~mlalin/mat6630`

Recommended Bibliography:	"Elliptic Curves", by J. S. Milne, BookSurge Publishers, 2006 "The Arithmetic of Elliptic Curves", by J. Silverman, Second Edition, Springer, 2009.
Homework:	Homework assignments will be posted in the course website. They will be due in class as follows: January 31, February 14, March 7, March 21, April 4. Late assignments will not be accepted.
Grade Weights:	Homework 100 % (Assignments will have the same weight.) The worst of the five assignment marks will be dropped.
Final Mark:	Based on a combination of absolute measures and distribution.

Objectives and General Description: One of the big questions in number theory concerns the resolution of polynomial equations in integers or rational numbers (Diophantine equations). Polynomials of degree 1 or 2 are well-understood. The next natural step is to look at equations of degree 3. Essentially an elliptic curve is defined by an equation of the form

$$y^2 = x^3 + ax + b.$$

It turns out that the rational solutions to this equation form a group, which is abelian and finitely generated (Mordell's theorem). Understanding the rank of this group involves a famous conjecure (Birch–Swinnerton-Dyer) whose resolution is worth a million dollars.

Elliptic curves show up in many areas (that look unrelated), such as congruent numbers, sphere packing, factorization of integers, etc. They are also related to modular forms which is the starting point for the proof of Fermat's Last Theorem.

Topics: The goal of this class is to study the basics of elliptic curves and, time permitting, their relationship with modular forms.

We plan to discuss the following topics.

1. Plane curves, Cubics, group structure in cubics.

2. Definition of elliptic curves, Weierstrass equation, elliptic curves modulo p, torsion points
3. Complex structure of elliptic curves.
4. Arithmetic of elliptic curves. Groups of Selmer and Tate–Shafarevich, Mordell theorem, elliptic curves over finite fields, Birch–Swinnerton-Dyer conjecture.
5. Elliptic Curves and modular forms. Modular forms, L-function of elliptic curves.

Some Reminders:

- The deadline for adding/dropping or withdrawal of a course with refund at **Université de Montréal** is January 20.
- The deadline for withdrawal of a course without refund at **Université de Montréal** is March 10.
- It is the responsability of the student to notify the instructor of a previsible absence from an exam as soon as possible. The supporting documentation will be evaluated by the correspondent authority who will determine if the reasons for the absence are properly justified. (As per the regulations in `http://www.etudes.umontreal.ca/reglements/reglements.html`.)

  Midterm exams can not be taken in alternate dates. In the case of a justified absence (according to the pedagogical regulations at the Université de Montréal), the mark from the final exam will be assigned to the midterm exam. Students with justified abscence from the final exam will write a deferred final exam.
- Plagiarism is a serious offence! Students are invited to consult the site `http://www.integrite.umontreal.ca`
- To check for book availability in the library, contact the circulation desk (`http://www.bib.umontreal.ca/nous-joindre/MI.htm`) or the librarian Ferroudja Nazef (`f.nazef@umontreal.ca`)

Disclaimer: Any typographical errors in this Course Outline are subject to change and will be announced in class. When in doubt, the French version of this document takes precedence.