

**MAT 6654** *Courbes elliptiques et formes modulaires*  
Hiver 2024, Plan de cours

- Échéancier :** Du 8 janvier au 16 avril (pas de cours le 22 et 23 janvier et 4 et 5 de mars)  
lundi 10h30-12h30 et mardi 9h30 - 11h30  
Pav. André-Aisenstadt 5448
- Professeure :** Matilde N. Lalin  
Pav. André-Aisenstadt 5145  
Disponibilités : lundi 12h30 - 13h30 et mardi 11h30 - 12h30  
Possibilité d'autres périodes de disponibilité sur rendez-vous.  
[matilde.lalin@umontreal.ca](mailto:matilde.lalin@umontreal.ca)
- 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 StudiUM.  
Il faut le remettre en classe les jours: 5 février, 19 février, 11 mars, 25 mars, 8 avril.  
Les devoirs qui seront remis en retard ne seront pas acceptés.
- Barème :** Travaux pratiques (devoir) 80 % (Tous les devoirs seront répartis également.)  
Le devoir le moins bon de chaque étudiant.e sera ignoré.  
Présentation orale 20%
- 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'emballage de sphères, la factorisation d'entiers, etc. Ils sont également liés 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 23 janvier.
- La date limite pour abandonner un cours avec frais : le 15 mars.
- Vous devez motiver, par écrit, toute absence à une évaluation dès que vous êtes en mesure de constater que vous ne pourrez être présent.e à l'évaluation et fournir une justification. Dans les cas de force majeure, vous devez le faire le plus rapidement possible. Il appartiendra à l'autorité compétente de déterminer si le motif est acceptable (Règlement pédagogique - Études supérieures et postdoctorales).
- Il faut bien écrire le nom de famille et la matricule dans les travaux. Cependant, vous n'avez pas l'obligation d'utiliser votre prénom légal, vous pouvez le remplacer par un prénom choisi.
- Le plagiat attention, c'est sérieux! L'étudiant est invité à consulter le site <http://www.integrite.umontreal.ca>
- Il est important de respecter la propriété intellectuelle et le droit à l'image sous peine d'éventuelles sanctions. L'usage de tout document déposé sur StudiUM pour chaque cours (incluant les enregistrements audio et vidéo) est assujéti à l'engagement de chaque étudiant.e à respecter la propriété intellectuelle et le droit à l'image. Il est interdit de faire une captation audio ou vidéo du cours, en tout ou en partie, sans le consentement écrit du professeur. Le non-respect de cette règle peut mener à des sanctions disciplinaires en vertu de l'Article 3 du Règlement disciplinaire concernant les étudiants.

- Pour la disponibilité des livres en bibliothèque, contacter le comptoir de prêt (<http://www.bib.umontreal.ca/nous-joindre/MI.htm>) ou la bibliothécaire Indiana Delsart ([Indiana.delsart@umontreal.ca](mailto:Indiana.delsart@umontreal.ca))
- Si vous éprouvez des difficultés dans votre processus d'apprentissage, et que vous souhaitez recevoir des conseils, vous pouvez contacter Karima Amoura, conseillère à la réussite étudiante, à l'adresse suivante : [cre@dms.umontreal.ca](mailto:cre@dms.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 6654** *Elliptic Curves and Modular Forms*  
Winter 2024, Syllabus

<b>Dates:</b>	January 8 to April 16 (no classes on January 22 and 23 and March 4 and 5) Mondays 10:30AM - 12:30PM and Tuesdays 9:30AM - 11:30AM Pav. André- Aisenstadt 5448
<b>Professor:</b>	Matilde N. Lalin Pav. André- Aisenstadt 5145 Office hours Mondays 12:30PM - 13:30PM and Tuesdays 11:30AM - 12:30PM or by appointment. <code>matilde.lalin@umontreal.ca</code>
<b>Recommended Bibliography:</b>	“Elliptic Curves”, by J. S. Milne, BookSurge Publishers, 2006 “The Arithmetic of Elliptic Curves”, by J. Silverman, Second Edition, Springer, 2009.
<b>Homework:</b>	Homework assignments will be posted in StudiUM. They will be due in class as follows: February 5, February 19, March 11, March 25, April 8. Late assignments will not be accepted.
<b>Grade Weights:</b>	Homework 80 % (Assignments will have the same weight.) The worst of the five assignment marks will be dropped. Oral presentation 20%
<b>Final Mark:</b>	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 conjecture (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 23.
- The deadline for withdrawal of a course without refund at **Université de Montréal** is March 15.
- It is the responsibility of the student to justify, in writing, any foreseeable absence from an exam and to provide supporting documentation as soon as possible. In case of an emergency, the student must contact the corresponding authority 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 (Règlement pédagogique - Études supérieures et postdoctorales).
- It is necessary to write the last name and the student number in submitted work. However, the student is not obliged to use their legal first name, they can replace it with a chosen first name.
- Plagiarism is a serious offence! Students are invited to consult the site <http://www.integrite.umontreal.ca>
- Online material is protected by intellectual property and image rights. It is important to respect these, under penalty of possible sanctions. Every student is expected to respect the intellectual property and image rights of any class material in StudiUM (including audio and video recordings). It is not allowed to make audio or video recordings of the course, in whole or in part, without the written consent of the professor. Failure to comply with this rule may lead to disciplinary sanctions under Article 3 of the Disciplinary Regulations concerning students.
- To check for book availability in the library, contact the circulation desk (<http://www.bib.umontreal.ca/nous-joindre/MI.htm>) or the librarian Indiana Delsart ([Indiana.delsart@umontreal.ca](mailto:Indiana.delsart@umontreal.ca))

- If you experience difficulties in your learning process, and would like to receive advice, you can contact Karima Amoura, the Advisor for Student Success, at [cre@dms.umontreal.ca](mailto:cre@dms.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.