

Andrew Granville. Bureau: 6153 André Aisenstadt, 343-6583, andrew@dms.umontreal.ca

Nous emploierons **Number theory revealed: An Introduction** de Andrew Granville: Devoir sera pris de ce livre. (Vous pouvez utiliser **Number theory revealed: A masterclass** de Andrew Granville pour un version avec beaucoup plus d'étudier.)

Ou un livre en français (supplémentaire): **Introduction à la théorie des nombres** de Jean-Marie de Koninck et Armel Mercier.

Horaires: Lundi 15h30-16h30; Mercredi 9h30-11h30, Local: En ligne

Périodes de disponibilité: Être déterminé. Si vous avez besoin de parler, envoyez-moi un email et nous trouverons un moment pour une réunion

Objectifs: La théorie des nombres a été appelée "la reine des mathématiques" par plusieurs des grands mathématiciens d'histoire. Le sujet est plein des questions, qui semblent accessibles, dont beaucoup restent égales sans réponse aujourd'hui. C'est un sujet qui a fasciné s'enquérir des esprits pendant des siècles. et j'espère partager avec vous certains de ces plaisirs!

Dans une veine plus pratique nous discuterons un application moderne et importante — la cryptographie qui est utilisé pendant chaque jour, par chaque personne par des machines de banque, des téléphones de cellules, et le web, et nous apprendrons ces idées fondamentales.

Contour de cours:

0. (prérequis) Le principe de l'induction. Le théorème du binôme.

1. Notions fondamentales: la divisibilité, l'algorithme d'Euclid, le pgcd et ppcm, combinaisons linéaires des entiers.

2. Les congruences: propriétés élémentaires, la difficulté de division, les testes pour divisibilité.

3. L'algèbre de base de la théorie des nombres: Théorème fondamental de l'arithmétique, division en congruences, les nombres irrationnels, le théorème du reste chinois, les racines carrées de $1 \pmod{n}$.

4. Fonctions multiplicatives: $\phi(n), \tau(n), \sigma(n)$; les nombres parfaits, l'inversion de Möbius.

5. La distribution des nombres premiers: des preuves qu'il y a une infinitude, les inégalités de Tchebychev, les grandes questions, le postulat de Bertrand, la fonction zêta de Riemann.

6. Les équations diophantiennes: L'arithmétique et la géométrie de l'équation $x^2 + y^2 = z^2$, pas de solution par descente, le dernier théorème de Fermat.

7. Résidus de puissance: Ordres, le petit théorème de Fermat, racines primitives, pseudo-premiers et les nombres de Carmichael. Les expansion décimale des fractions.

8. Les résidus quadratiques: le symbole de Legendre, critère d'Euler, lemme de Gauss, la loi de la réciprocité quadratique, le symbole de Jacobi.

9. Equations quadratiques: somme de deux carrés, les formes quadratiques binaires, principe local-global.

10. Questions d'informatiques: les racines carrés mod n . le codage des messages secrets (RSA), les testes de primalité (AKS), P et NP, les méthodes de factorization.

11. Les nombres rationnelles et irrationnelles: principe du casier, approximation de nombres irrationnels, le théorème de Dirichlet, l'équation de Pell, les nombres transcendants, conjecture *abc*.

12. Formes quadratiques binaires: représentations, classes d'équivalence, nombre des classes, groupe des classes.

Nous ferons ces matières et suivrons également des questions de la classe pour voir où ils mènent.

Devoir: C'est important de faire cette travail, chaque semaine. Je donnerai plusieurs questions chaque fois, et vous avez besoin de me donner les solutions le lundi avant le début du cours. Chaque étudiant doit me donner un devoir de soi-même. Si vous manquez une classe puis vous êtes responsable d'obtenir les notes pour cette classe, et de n'importe quel devoir donné, d'un autre étudiant. J'essayerai de placer le travail sur la page Web chaque semaine, mais il n'y a aucune garantie.

La page Web du cours:

<http://www.dms.umontreal.ca/~andrew/Courses/2020.Aut.3632/MAT3632.A20.html>

Barème: Travaux pratiques (devoir) 20% . Examen intra (1 novembre) 30% . Examen final (20 décembre) 50% .

Habitudes d'études: Les études ont prouvé que les étudiants typiquement améliorent dans les cours s'ils étudient ainsi que d'autres étudiants. Le plus réussite si de telles sessions d'étude sont regardées, par les étudiants, en tant qu'élément de leur vie sociale. La plupart des personnes travaillent mieux discutent le nouveau matériel avec d'autres et le construisant sur des idées de chacun, et je vous encourage fortement à faire ainsi.

Parfois il y a une tentation pour faire la moitié chacune, et pour ne pas regarder vraiment ce que l'autre personne a fait. Ce n'est pas une bonne idée, puisque vous devez comprendre tout le matériel. Ainsi veuillez, faites-vous une faveur et travaillez avec d'autres, et employez cette expérience pour apprendre plus par des idées des autres.

Dans la classe: Veuillez poser les questions, svp? Beaucoup des personnes se sentent intimidées au sujet de poser des questions: habituellement cependant, si vous ne comprenez pas quelque chose, il y a au moins un autre dans la classe qui ne comprends pas aussi! Ainsi il nous bénéficie tous si vous demandez.

Les jours du cours: 2, 9, 14, 16, 21, 23, 28, 30 septembre;

5, 7, 14, 26, 28 octobre; 2, 4, 9, 11, 16, 18, 23, 25, 30 novembre; 2, 7, 16 décembre.

Examen intra: Mercredi le 28 octobre, 10h30–12h30. En ligne.

Examen finale: Mercredi le 16 décembre, 9h00–12h00. En ligne.