Math 261 - Number theory
Fall 2018–2019

Professor: Nicolas Mascot
Contact: nm116@aub.edu.lb
Office: Bliss Hall 206C
Classes: Monday, Wednesday, and Friday, 11:00 – 11:50 AM, Nicely 324.
Office hours: Monday, Wednesday, and Friday, 2:00 – 3:00 PM; or by appointment.
Textbook: *The higher arithmetic*, 8th edition, by H. Davenport.

Number theory is the study of the property of the integers, mainly in view of attempting to solve *diophantine equations*, that is to say equations whose unknown are required to assume integer values. Such equations are often extremely difficult to solve, and the goal of this course is to introduce the basic techniques needed to tackle such equations.

For instance, by the end of this course, you will easily be able to show that the equation

$$x^3 + y^3 + z^3 = 31$$

has no solutions in integers, and that 2018 and 2017 can be expressed as a sum of two squares, whereas 2016 can be expressed as a sum of three squares but not as a sum of two, and 2015 can be expressed as a sum of four squares but not three.

Topics to be covered (if time permits):

1. Divisibility and factorization of the integers

   Prime numbers, gcd, Euclid's algorithm, Bézout's theorem, ideals of $\mathbb{Z}$, multiplicative functions.

2. Congruences

   Arithmetic in the ring $\mathbb{Z}/n\mathbb{Z}$ and in the field $\mathbb{Z}/p\mathbb{Z}$, Euler's function $\phi(n)$, Chinese remainders, multiplicative order and primitive roots, polynomial equations mod n.

3. Quadratic residues

   Legendre symbol, quadratic reciprocity, quadratic equations mod p.

4. Sums of squares

   Integers that are the sum of 2 or 3 squares, every integer is the sum of 4 squares.

5. Quadratic forms

   Equivalence of quadratic forms, discriminant, integers represented by quadratic forms.

6. Continued fractions

   Continued fraction expansion of rationals and of quadratic irrationals, Lagrange's theorem, diophantine approximation, Pell-Fermat equations.

7. Further topics

   More diophantine equations, number theory and cryptography, elliptic curves, elliptic curves mod p (to be selected based on the audience's interests).

Homework: Weekly exercise sheets will be handed on every Monday at the beginning of the class (starting Monday September 10), to be returned on the next Monday at the beginning of the class.

Exams dates: The exams are tentatively scheduled as follows:

- Exam 1: Wednesday October 3, 18:30PM–19:30PM, room to be announced later.
- Exam 2: Wednesday October 31, 18:30PM-19:30PM, room to be announced later.
- Final exam: to be announced later.

Grading scheme:

- Weekly homework: 15%
- Better of exam 1 and exam 2: 25%
- Worse of exam 1 and exam 2: 20%
- Final exam: 40 %

Important: Final grades will be assigned with a curve that will not be determined before the final exam.

Accessibility: AUB strives to make learning experiences accessible for all. If you anticipate or experience academic barriers due to a disability (such as ADHD, learning difficulties, mental health conditions, chronic or temporary medical conditions), please do not hesitate to inform the Accessible Education Office. In order to ensure that you receive the support you need and to facilitate a smooth accommodations process, you must register with the Accessible Education Office (AEO) as soon as possible: `accessibility@aub.edu.lb`; +961-1-350000, x3246; West Hall, 314.

Further Help: The Department of Mathematics has a free drop-in tutorial service, the Math Clinic, that runs every weekday.