



Nanchang University MATH302: Number Theory

Credit: 4

Contact Hours

This course is composed of 24 lecture sessions, 3 tutorial sessions and 9 office contact hours. Each lecture session takes 2 contact hours in length; each tutorial session takes 3 contact hours in length; There will be a Q-A review session(3 contact hours) and Final Exam (3 contact hours) at the end of this term. This course has 72 contact hours in total.

Course Description

Number theory lies in the core of encryption and authentication process. This course is about number theory, the study of the whole numbers and their properties. Topics include the study of integers, primes, congruence, Euclidean Algorithm, primitive roots, finite fields, law of quadratic reciprocity, Gaussian Integer, and Pell's Equation.

Textbook Information:

A Concrete Introduction to Higher Algebra, By Childs, Lindsay N.

Grading

Participation	10%
Assignment	20%
Quizzes	20%
Midterm	20%
Final Exam	30%

A+ 96-100	A 90-95	A- 85-89
B+ 82-84	B 78-81	B- 75-77
C+ 71-74	C 66-70	C- 62-65
D 60-61	F < 60	

Course Schedule

The course has 24 class sessions in total. All sessions are 2 contact hours in length. At the end of this term, there will be a Q-A review session(3 contact hours) and Final Exam (3 contact hours).

Note: the course outline and required readings are subject to change.



Class 1:

Properties of Integers

Class 2:

Well-Ordering Principle and Euclidean Algorithm

Class 3:

Unique Factorizations

Class 4:

Rational Root Theorem

Class 5:

Pythagorean Triples

Class 6:

Definition and properties of Congruence

Class 7:

Chinese Remainder Theorem

Class 8:

Modular Exponentiation

Class 9:

Primitive Roots

Class 10:

Discrete Logarithm

Class 11:

Algebraic Structure of Congruence

Class 12:

Fermat's Theorem

Class 13:

Midterm

Class 14:

The Euler Totient Function

Class 15:

Application: RSA



Class 16:
Quadratic Residues

Class 17:
Euler's Criterion

Class 18:
Quadratic Reciprocity

Class 19:
Jacobi Symbol

Class 20:
Gaussian Integers

Class 21:
Factorization of $\mathbb{Z}[i]$

Class 22:
Eisenstein Integers

Class 23:
Continued Fractions and Pell's Equation

Class 24:
Fundamental Units

Attending Policy

Regular and prompt attendance is required. Under ordinary circumstances, you may miss two times without penalty. Each absence over this number will lower your course grade by a third of a letter and missing more than five classes may lead to a failing grade in the course. Arriving late and/or leaving before the end of the class period are equivalent to absences.

Policy on "Late Withdrawals"

In accordance with university policy, appeals for late withdrawal will be approved ONLY in case of medical emergency and similar crises.

Academic Honesty

Nanchang University expects all students to do their own work. Instructors will fail assignments that show evidence of plagiarism or other forms of cheating, and will also report the student's name to the University administration. A student reported to the University for



cheating is placed on disciplinary probation; a student reported twice is suspended or expelled.

General Expectations:

Students are expected to:

- Attend all classes and be responsible for all materials covered in class and otherwise assigned;
- Complete the day's required reading and assignments before class;
- Review the previous day's notes before class and make notes about questions you have about the previous class or the day's reading;
- Participate in class discussions and complete required written work on time;
- Refrain from texting, phoning or engaging in computer activities unrelated to class during the class period;
- While class participation is welcome, even required, you are expected to refrain from private conversations during the class period.

Special Needs or Assistance

Please contact the Administrative Office immediately if you have a learning disability, a medical issue, or any other type of problem that prevents professors from seeing you have learned the course material. Our goal is to help you learn, not to penalize you for issues which mask your learning.