湖北工業大學
HUBEI UNIVERSITY OF TECHNOLOGY

Course Title	Introduction to Number Theory
Course Code	MATH 3101
Semester	Summer 2026
Course Length	4 Weeks, 60 Contact Hours
Credits	4
Instructor	TBA
Office	TBA
Email	TBA
Prerequisite	MATH 1112 Calculus II MATH 2151 Linear Algebra I

Course Description:

This course offers a systematic introduction to the classical and modern foundations of number theory. Starting from the fundamental properties of integers, the curriculum advances through congruences, multiplicative functions, and the elegant structures of quadratic residues. Students will explore the distribution of primes and the computational foundations of modern cryptography. The course concludes with an introduction to diophantine approximations via continued fractions and the arithmetic of elliptic curves, bridging the gap between classical methods and modern algebraic geometry.

Course Goals:

Students who successfully complete this course will demonstrate competency in the following general education core goals:

- **Critical Thinking Skills** – Students will engage in analytical thinking, demonstrating the ability to critically evaluate, synthesize, and apply knowledge to complex problems, and construct well-reasoned solutions and arguments.
- **Independent Research and Inquiry** – Students will conduct independent research, utilizing academic resources to explore relevant topics, formulating research questions, analyzing data, and presenting findings in a coherent, scholarly manner.
- **Problem-Solving and Application** – Students will apply theoretical concepts and methodologies learned in the course to real-world problems, demonstrating the ability to develop practical solutions informed by academic inquiry.
- **Global and Cultural Awareness** – Students will gain awareness of the global and cultural contexts relevant to the course, appreciating diverse perspectives and considering the implications of their studies in a broader, international context.

Student Learning Outcomes:

Upon completion of this course, students will be able to:

- Master the foundational proofs regarding divisibility and the distribution of prime numbers;
- Develop computational fluency in modular arithmetic and its application to primality testing;
- Analyze and solve polynomial congruences and primitive roots;
- Apply number-theoretic algorithms to secure communication protocols (RSA, Diffie-Hellman);
- Understand the theory of quadratic forms and the geometry of elliptic curves.

Textbooks/Supplies/Materials/Equipment/ Technology or Technical Requirements:

Primary: David M. Burton. *Elementary Number Theory, 7th Edition*. McGraw-Hill Higher Education.

Supplemental:

- Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery. *An Introduction to the Theory of Numbers, 5th Edition.* Wiley, 1991.
- Neal Koblitz. *A Course in Number Theory and Cryptography, 2nd Edition.* Springer, 1994.
- Joseph H. Silverman. *A Friendly Introduction to Number Theory, 4th edition*. Pearson.

Course Requirements:

Homework Assignments (25%)

Four written homework sets will be distributed throughout the semester, one at the end of each major thematic block. Each set contains approximately 8-12 problems of varying difficulty, ranging from direct computations to proof-writing exercises.

Research Essay (15%)

Each student will produce an expository essay (approximately 1500 words) on a topic in number theory that extends or contextualizes course material. Suitable topics include the history of the prime number theorem, modern primality testing algorithms (e.g., AKS), lattice-based cryptography as an alternative to RSA, Fermat's Last Theorem and connections to elliptic curves, or the Birch and Swinnerton-Dyer conjecture. Grading emphasizes mathematical accuracy, clarity of exposition, appropriate engagement with sources, and the student's ability to connect the chosen topic to the theoretical content of the course.

Midterm Examination (25%)

The closed-book written examination covers all material from Lectures 1 through 11, encompassing divisibility theory, prime distribution, congruence arithmetic, Fermat's and Euler's theorems, primitive roots, and an introduction to cryptographic applications. The format includes a combination of computational problems, short-answer theoretical questions, and one or two proof questions.

Final Examination (35%)

A comprehensive closed-book examination administered during the examination period at the end of the semester. The final examination covers all 25 lectures and all four thematic blocks, with an emphasis on the latter half of the course. Students can expect a mix of computational problems (approximately 40%), proof-writing tasks (approximately 40%), and conceptual short-answer questions (approximately 20%).

Assessments: Activity	**Percent Contribution**
Homework Assignments (4 sets)	25%
Research Essay	15%
Midterm Examination	25%
Final Examination	35%

Grading:

Final grades will be based on the sum of all possible course points as noted above.

Grade	**Percentage of available points**
A	94-100
A-	90-93
B+	87-89
B	84-86
B-	80-83
C+	77-79
C	74-76
C-	70-73
D	64-69
D-	60-63
F	0-59

Course Schedule:
The schedule of activities is subject to change at the reasonable discretion of the instructor. Minor changes will be announced in class, major ones provided in writing.

MATH 3101 Schedule		
Lecture	Topic	Readings
L1	Divisibility and the Division Algorithm; Mathematical Induction	*Burton* §1.1-1.2, §2.1-2.2
L2	Greatest Common Divisor; Euclidean Algorithm and Bezout's Identity	*Burton* §2.3-2.4
L3	Prime Numbers; Unique Factorization (Fundamental Theorem of Arithmetic)	*Burton* §3.1
L4	Sieve of Eratosthenes; Goldbach's Conjecture; Introduction to Prime Distribution	*Burton* §3.2-3.3
L5	Introduction to Congruences; Basic Properties and Linear Congruences	*Burton* §4.2, §4.4
L6	Systems of Linear Congruences; Chinese Remainder Theorem; **HW 1 Due**	*Burton* §4.4
L7	Fermat's Little Theorem and Applications; Wilson's Theorem	*Burton* §5.2-5.3
L8	Arithmetic Functions: Sum and Number of Divisors (sigma, tau); Mobius Function	*Burton* §6.1-6.2

L9	Euler's Phi-Function; Euler's Theorem; Applications to Modular Exponentiation	*Burton* §7.2-7.3
L10	Order of an Integer Modulo n; Primitive Roots for Primes	*Burton* §8.1-8.2
L11	Primitive Roots for Composite Moduli; Theory of Indices	*Burton* §8.3-8.4
L12	Introduction to Cryptography: From Caesar Cipher to Public-Key Systems	*Burton* §10.1; *Koblitz* Ch. 3
---	**Midterm Examination**	Covers L1-11
L13	RSA Public-Key Encryption: Setup, Encoding, and Decoding; **Research Essay (Draft) Due**	*Koblitz* Ch. 4 §4.2; *Burton* §10.3
L14	RSA Security Analysis; Primality Testing and Factorization Concepts	*Koblitz* Ch. 5 §5.1; *Burton* §16.2
L15	Quadratic Residues; Euler's Criterion; Legendre Symbol and Properties; **HW 2 Due**	*Burton* §9.1-9.2
L16	Gauss's Lemma; Further Properties of the Legendre Symbol	*Burton* §9.2
L17	Law of Quadratic Reciprocity: Statement and Proof	*Burton* §9.3
L18	Applications of Quadratic Reciprocity; Quadratic Congruences with Composite Moduli (Jacobi Symbol)	*Burton* §9.4
L19	Quadratic Forms: Definitions, Equivalence, and Discriminant	*Niven, Zuckerman & Montgomery* Ch. 3; Instructor Notes
L20	Representation of Integers by Quadratic Forms; Sums of Two Squares; **HW 3 Due**	*Niven, Zuckerman & Montgomery* Ch. 3; *Burton* §13.1-13.2
L21	Continued Fractions: Finite Continued Fractions; Convergents	*Burton* §15.2
L22	Infinite and Periodic Continued Fractions; Farey Fractions	*Burton* §15.3-15.4; *Silverman* Ch. 47
L23	Pell's Equation: Formulation and Solutions via Continued Fractions	*Burton* §15.5; *Silverman* Ch. 32, 34
L24	Introduction to Elliptic Curves: Weierstrass Form, Group Law, and Basic Theory; **Research Essay (Final) Due**	*Koblitz* Ch. 6 §6.1; *Silverman* Ch. 41-42
L25	Rational Points on Elliptic Curves; Applications and Course Review; **HW 4 Due**	*Koblitz* Ch. 6 §6.1-6.2; *Silverman* Ch. 43
	Final Examination	Cumulative

Accommodation Statement:

Academic accommodations may be made for any student who notifies the instructor of the need for an accommodation. It is imperative that you take the initiative to bring such needs to the instructor’s attention, as he/she is not legally permitted to inquire. Students who may require assistance in emergency evacuations should contact the instructor as to the most appropriate procedures to follow.

Academic Integrity Statement

Each student is expected to maintain the highest standards of honesty and integrity in academic and professional matters. The University reserves the right to take disciplinary action, up to and including dismissal, against any student who is found guilty of academic dishonesty or otherwise fails to meet the standards. Any student judged to have engaged in academic dishonesty in coursework may receive a reduced or failing grade for the work in question and/or for the course.

Academic dishonesty includes, but is not limited to, dishonesty in quizzes, tests, or assignments; claiming credit for work not done or done by others; hindering the academic work of other students; misrepresenting academic or professional qualifications within or without the University; and nondisclosure or misrepresentation in filling out applications or other University records.

Other Items:

Attendance and Expectations
All students are required to attend every class, except in cases of illness, serious family concerns, or other major problems. We expect that students will arrive on time, be prepared to listen and participate as appropriate, and stay for the duration of a meeting rather than drift in or out casually. In short, we anticipate that students will show professors and fellow students maximum consideration by minimizing the disturbances that cause interruptions in the learning process. This means that punctuality is a must, that cellular phones be turned off, and that courtesy is the guiding principle in all exchanges among students and faculty. You will be responsible for the materials and ideas presented in the lecture.

Assignment Due Dates
All written assignments must be turned in at the time specified. Late assignments will not be accepted unless prior information has been obtained from the instructor. If you believe you have extenuating circumstances, please contact the instructor as soon as possible.

Make-Up Work
The instructor will not provide students with class information or make-up assignments/quizzes/exams missed due to an unexcused absence. Absences will be excused and assignments/quizzes/exams may be made up only with written documentation of an authorized absence. Every effort should be made to avoid scheduling appointments during class. An excused student is responsible for requesting any missed information from the instructor and setting up any necessary appointments outside of class.

Access, Special Needs, and Disabilities
Please notify the instructor at the start of the semester if you have any documented disabilities, a medical issue, or any special circumstances that require attention, and the school will be happy to assist.