COURSE OUTLINE: MH3210

Course Title	**Number Theory**		
Course Code	**MH3210**		
Offered	Study Year 3, Semester 1		
Course Coordinators	Frederique Elise Oggier (Assoc Prof)	frederique@ntu.edu.sg	6513 2026
	Bernhard Schmidt (Prof)	bernhard@ntu.edu.sg	6513 2009
Pre-requisites	MH1300		
AU	4		
Contact hours	Lectures: 39, Tutorials: 12		
Approved for delivery from	AY 2021/22 semester 1		
Last revised	27 Oct 2021, 14:20		

Course Aims

This course aims to provide a first discovery of number theory using elementary techniques (that is techniques mostly built from scratch during the course). You will learn fundamental results on the divisibility of integers, on prime numbers, on Diophantine equations, and hear about famous conjectures in number theory. You will also practice working with congruences modulo an integer, and solving polynomial congruences and systems of linear congruences. This knowledge will be useful to you if you plan to take a course on abstract algebra, or if you are interested in applications of mathematics to cryptography.

Intended Learning Outcomes

Upon successfully completing this course, you should be able to:

1. State fundamental results in number theory.
2. Compute modulo an integer.
3. Solve linear diophantine equations and linear congruences.
4. Prove results in number theory involving short reasoning.
5. Solve polynomial congruences and systems of linear congruences.
6. Compute primitive roots.
7. Compute Legendre symbol.

Course Content

The Euclid division algorithm and its extended version, and to use them to compute the greatest common divisor of integers.

Bezout identity.

The existence and unicity of writing an integer in a given basis.

Fundamental Theorem of Arithmetic.

Existence of an infinity of primes.

Linear diophantine equations.

Modular arithmetic.

Linear congruences and the Chinese Remainder Theorem.

Primality testing.

Primitive roots.

Legendre symbol.

The law of quadratic reciprocity.

Assessment

Component	Course ILOs tested	SPMS-MAS Graduate Attributes tested	Weighting	Team / Individual	Assessment Rubrics
Continuous Assessment					
Mid-semester Quiz					
Short Answer Questions 1	4, 5, 6, 7	**1.** a, c **3.** a	20	individual	See Appendix for rubric
Short Answer Questions 2	2, 3, 4, 5	**1.** a, c **3.** a	20	individual	See Appendix for rubric
Examination (2.0 hours)					
Short Answer Questions	1, 2, 3, 4, 5, 6, 7	**1.** a, c **2.** c **3.** a	60	individual	See Appendix for rubric
		Total	**100%**		

These are the relevant SPMS-MAS Graduate Attributes.

1. **Competence**

   a. Independently process and interpret mathematical theories and methodologies, and apply them to solve problems

   c. Discover patterns by abstraction from examples

2. **Creativity**

   c. Develop new applications of existing techniques

3. **Communication**

   a. Present mathematics ideas logically and coherently at the appropriate level for the intended audience

Formative Feedback

You will have the opportunity to discuss your understanding of results in number theory, of the techniques taught to execute different types of computations (modulo an integer, solving linear equations) and to prove results (a number of them related to divisibility properties) during lectures via group discussions, during which feedback will be provided by peers and the lecturer.

You will also have the option to present solutions of your exercises during the tutorials, which will receive feedback from the lecturer.

Midterm assessments will be graded and feedback will be provided for each student on the area(s) that should be improved (if any) and those which are already satisfactory.

After the exam period, a feedback on the final exam will be uploaded on NTULearn.

Learning and Teaching Approach

Lectures (39 hours)	Proofs (e.g. for proving divisibility properties of integers) are done on the board, this is to make sure that the pace is appropriate and you get to see how every step is done. Small exercises are provided during the lecture, to be discussed in groups, to make sure that you have understood the new topic/definition before moving on. This also gives you the opportunity to practice computations in class (e.g. modular arithmetic, solving linear equations). Whenever possible, plots/animations will be provided to give you a visualization of abstract functions/concepts (e.g. fundamental results in number theory).
Tutorials (12 hours)	Exercises will belong to typically two categories: small proofs, so you get trained in formulating and proving results in number theory (e.g. for providing divisibility properties of integers), and computations, so you develop the skills to be able to work with modular arithmetic, solve linear integer/congruence equations, systems of congruences.

Reading and References

Elementary Number Theory, by G. A. Jones and M. Jones, Springer Undergraduate Mathematics Series.
This book is recommended and it can be accessed via NTU library.
ISBN-13: 978-3540761976
ISBN-10: 3540761977

Elementary Number Theory, by Rosen. This is book contains broadly the same content, with more exercises, in particular elementary ones, however it is difficult to access it via NTU library (requires the installation of a 3rd party DRM and even after that, only 2 students at a time can access the book).
ISBN-10: 129203954X
ISBN-13: 978-1292039541

Course Policies and Student Responsibilities

As for every course, please try to be as ready as possible before coming to class. This means you should have tried to solve the tutorial exercises, and reminded yourself of the topic taught.

Academic Integrity

Good academic work depends on honesty and ethical behaviour. The quality of your work as a student relies on adhering to the principles of academic integrity and to the NTU Honour Code, a set of values shared by the whole university community. Truth, Trust and Justice are at the core of NTU's shared values.

As a student, it is important that you recognize your responsibilities in understanding and applying the principles of academic integrity in all the work you do at NTU. Not knowing what is involved in maintaining academic integrity does not excuse academic dishonesty. You need to actively equip yourself with strategies to avoid all forms of academic dishonesty, including plagiarism, academic fraud, collusion and cheating. If you are uncertain of the definitions of any of these terms, you should go to the Academic Integrity website for more information. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Course Instructors

Instructor	Office Location	Phone	Email
Frederique Elise Oggier (Assoc Prof)	MAS05-13	6513 2026	frederique@ntu.edu.sg
Bernhard Schmidt (Prof)	SPMS-MAS-05-24	6513 2009	bernhard@ntu.edu.sg

Planned Weekly Schedule

Week	Topic	Course ILO	Readings/ Activities
1	The Euclid division algorithm, the existence and unicity of writing an integer in a given basis.	4, 7	Theorem 1.10 (Rosen)or Theorem 1.1 (Jones)
2	Existence of an infinity of primes. Bezout identity.	4, 7	Theorem 3.1 (Rosen), Theorem 2.6 (Jones), Theorem 3.8 and Corollary 3.8.1 (Rosen), or Theorem 1.7 (Jones)
3	The extended Euclid algorithm, and to use them to compute the greatest common divisor of integers. Fundamental Theorem of arithmetic.	4, 7	Theorem 3.14 (Rosen) or Theorem 1.6 (Jones), Theorem 3.15 (Rosen)or Theorem 2.3 (Jones)
4	Modular arithmetic, modular exponentiation, Linear diophantine equations.	5, 6	Theorem 3.23 and 3.24 (Rosen) or Theorem 3,7 (Jones), Theorem 4.1, 4.2 (Rosen)or Lemma 3.1 (Jones)
5	Linear congruences and the Chinese Remainder Theorem.	3, 5, 6	Theorem 4.11 (Rosen)or Theorem 3.7 (Jones), Theorem 4.12, Theorem 4.13 (Rosen)or Theorem 3.10 (Jones)
6	Euler function, and Euler's and Wilson's theorems	4, 5	Theorem 5.3 (Jones), Theorem 6.13 (Rosen), Corollary 4.5 (Jones), Theorem 6.1 (Rosen)
7	Applications of Euler's Theorem, e.g. RSA	4, 5	section 8.4 p. 323-324 by Rosen or p. 95 by Jones
8	Existence of primitive roots	2, 5	Theorems 6.5, 6.7, 6.11 (Jones), Theorems 9.1, 9.8, 9.10, 9.15 (Rosen)
9	Applications of primitive roots	2, 5	section 6.6 (Jones), chapter 10 (Rosen)
10	Quadratic residues and Legendre symbol	1, 5	chapter 11 (Rosen), chapter 7 (Jones)
11	Legendre symbol and quadratic reciprocity	1, 4, 5	chapter 11 (Rosen), chapter 7 (Jones)
12	Jacobi symbol	1, 5	chapter 11 (Rosen), chapter 7 (Jones)
13	Pythagorean triples	4	chapter 11 (Jones), section 13.1 (Rosen)

Appendix 1: Assessment Rubrics

Rubric for Mid-semester Quiz: Short Answer Questions 1 (20%)

The assessment comprise short answer questions, of two types: short reasoning and computations.

Assessment criteria include:

- right answer,
- proper arguments and justifications,
- details provided.

To score a high mark, it is needed that the right answer is provided with a justification. It is also possible to have a high score while making some small mistake, if the argumentation is clear and the mistake is coming from for example a typo, or an inattention mistake.

A right answer with no justification whatsoever will result in a pass mark, enough evidence of understanding even with a wrong answer will result in a pass mark.

A wrong answer with no argument, or a wrong answer with wrong justification, or no answer will result in a fail mark.

Rubric for Mid-semester Quiz: Short Answer Questions 2 (20%)

The assessment comprise short answer questions, of two types: short reasoning and computations.

Assessment criteria include:

- right answer,
- proper arguments and justifications,
- details provided.

To score a high mark, it is needed that the right answer is provided with a justification. It is also possible to have a high score while making some small mistake, if the argumentation is clear and the mistake is coming from for example a typo, or an inattention mistake.

A right answer with no justification whatsoever will result in a pass mark, enough evidence of understanding even with a wrong answer will result in a pass mark.

A wrong answer with no argument, or a wrong answer with wrong justification, or no answer will result in a fail mark.

Rubric for Examination: Short Answer Questions (60%)

The assessment comprise short answer questions, of two types: short reasoning and computations.

Assessment criteria include:

- right answer,
- proper arguments and justifications,
- details provided.

To score a high mark, it is needed that the right answer is provided with a justification. It is also possible to have a high score while making some small mistake, if the argumentation is clear and the mistake is coming from for example a typo, or an inattention mistake.

A right answer with no justification whatsoever will result in a pass mark, enough evidence of understanding even with a wrong answer will result in a pass mark.

A wrong answer with no argument, or a wrong answer with wrong justification, or no answer will result in a fail mark.