# Annexe A: New/Revised Course Content in OBTL+ Format

## Course Overview

| | |
|---|---|
| Expected Implementation in Academic Year (New format) | AY2026-2027 |
| Semester/Trimester/Others (specify approx. Start/End date) | Semester 1 |
| Course Author<br>* Faculty proposing/revising the course | Chan Song Heng |
| Course Author Email | chansh@ntu.edu.sg |
| Course Title | Number Theory |
| Course Code | MH3210 |
| Academic Units | 4 |
| Contact Hours | 51 |
| Research Experience Components | Not Applicable |

## Course Requisites (if applicable)

| | |
|---|---|
| Pre-requisites | MH1300 |
| Co-requisites | |
| Pre-requisite to | |
| Mutually exclusive to | |
| Replacement course to | |
| Remarks (if any) | |

## 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.

## Course's Intended Learning Outcomes (ILOs)

Upon the successful completion of this course, you (student) would be able to:

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

## Course Content

Introduction to basic number theory, including modern applications. Topics include: modular arithmetic; the Chinese remainder theorem, Fermat's little theorem, and Wilson's theorem; number-theoretic functions such as the $\tau$, $\sigma$, Euler's $\varphi$-function; the Möbius inversion formula; applications to cryptography; primitive roots and indices; Legendre's symbols; the quadratic reciprocity law; continued fractions and Pell's equations; primality tests, factorization of integers, and the RSA cryptosystem.

## Reading and References (if applicable)

An introduction to the theory of numbers, by Niven, Ivan, 1915-1999.; Zuckerman, Herbert S.; Montgomery, Hugh L., c1991;

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

NOTE: The above readings comprise the foundational readings for the course and more up-to-date relevant readings will be provided when they are available.

## Planned Schedule

| Week or Session | Topics or Themes | ILO | Delivery Mode | Activities | Readings |
|---|---|---|---|---|---|
| 1 | The Euclid division algorithm, the existence and unicity of writing an integer in a given basis. | 4,7 | In-person | Work on problems in Tutorial 1. Prepare for Weekly Quiz 1. | Theorem 1.10 (Rosen)or Theorem 1.1 (Jones) |
| 2 | Existence of an infinity of primes. Bezout identity. | 4,7 | In-person | Work on problems in Tutorial 2. Prepare for Weekly Quiz 2. | 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 | In-person | Work on problems in Tutorial 2. Prepare for Weekly Quiz 3. | 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 | In-person | Work on problems in Tutorial 4. Prepare for Weekly Quiz 4. | 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 | In-person | Work on problems in Tutorial 5. Prepare for Weekly Quiz 5. | 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 | In-person | Work on problems in Tutorial 6. Prepare for Mid-Semester Quiz 1. | Theorem 5.3 (Jones), Theorem 6.13 (Rosen), Corollary 4.5 (Jones), Theorem 6.1 (Rosen) |

| Week or Session | Topics or Themes | ILO | Delivery Mode | Activities | Readings |
|---|---|---|---|---|---|
| 7 | Applications of Euler's Theorem, e.g. RSA | 4,5 | In-person | Work on problems in Tutorial 7.<br>Prepare for Weekly Quiz 6. | section 8.4 p. 323-324 by Rosen or p.<br>95 by Jones |
| 8 | Existence of primitive roots | 2,5 | In-person | Work on problems in Tutorial 8.<br>Prepare for Weekly Quiz 7. | Theorems 6.5, 6.7, 6.11 (Jones),<br>Theorems 9.1, 9.8, 9.10, 9.15 (Rosen) |
| 9 | Applications of primitive roots | 2,5 | In-person | Work on problems in Tutorial 9.<br>Prepare for Weekly Quiz 8. | section 6.6 (Jones),<br>chapter 10 (Rosen) |
| 10 | Quadratic residues and Legendre symbol | 1,5 | In-person | Work on problems in Tutorial 10.<br>Prepare for Mid-Semester Quiz 2. | chapter 11 (Rosen),<br>chapter 7 (Jones) |
| 11 | Legendre symbol and quadratic reciprocity | 1,4,5 | In-person | Work on problems in Tutorial 11. | chapter 11 (Rosen),<br>chapter 7 (Jones) |
| 12 | Jacobi symbol | 1,5 | In-person | Work on problems in Tutorial 12. | chapter 11 (Rosen),<br>chapter 7 (Jones) |
| 13 | Continued fractions and Pell's equations | 4 | In-person | Prepare for Final Exam. | chapter 11 (Jones),<br>section 13.1 (Rosen) |

## Learning and Teaching Approach

| Approach | How does this approach support you in achieving the learning outcomes? |
|---|---|
| Lectures | 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.<br>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).<br>Whenever possible, plots/animations will be provided to give you a visualization of abstract functions/concepts (e.g. fundamental results in number theory). |
| Tutorials | 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. |

## Assessment Structure

Assessment Components (includes both continuous and summative assessment)

| No. | Component | ILO | Related PLO or Accreditation | Weightage | Description of Assessment Component | Team/Individual | Rubrics | Level of Understanding |
|---|---|---|---|---|---|---|---|---|
| 1 | Continuous Assessment (CA): Test/Quiz(Short Answer Questions 1 ) | 2, 3, 4, 5 | Not Applicable | 15 | | Individual | Analytic | Relational |
| 2 | Continuous Assessment (CA): Test/Quiz(Short Answer Questions 2) | 4, 5, 6, 7 | Not Applicable | 15 | | Individual | Analytic | Relational |
| 3 | Continuous Assessment (CA): Test/Quiz(Short Answer Questions. 6 out of 8 weekly quizzes. 2% each. ) | 1, 2, 3, 4, 5, 6, 7 | Not Applicable | 12 | | Individual | Analytic | Relational |
| 4 | Continuous Assessment (CA): Presentation(Two tutorial presentations) | 1, 2, 3, 4, 5, 6, 7 | Not Applicable | 3 | Two tutorial presentations, 1.5% each, one of which to be conducted individually in the instructor's office, the other may be presented either in class or in the instructor's office. | Individual | Holistic | Relational |

| No. | Component | ILO | Related PLO or Accreditation | Weightage | Description of Assessment Component | Team/Individual | Rubrics | Level of Understanding |
|---|---|---|---|---|---|---|---|---|
| 5 | Summative Assessment (EXAM): Final exam(Short Answer Questions) | 1, 2, 3, 4, 5, 6, 7 | Not Applicable | 55 | | Individual | Analytic | Relational |

Description of Assessment Components (if applicable)

NA

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.

## NTU Graduate Attributes/Competency Mapping

This course intends to develop the following graduate attributes and competencies (maximum 5 most relevant)

| Attributes/Competency | Level |
|---|---|
| Creative Thinking | Basic |
| Curiosity | Basic |
| Problem Solving | Advanced |
| Sense Making | Intermediate |
| Transdisciplinarity | Basic |

# Course Policy

Policy (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. On the use of technological tools (such as Generative AI tools), different courses / assignments have different intended learning outcomes. Students should refer to the specific assignment instructions on their use and requirements and/or consult your instructors on how you can use these tools to help your learning. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Policy (General)

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.

Policy (Absenteeism)

Mid-Semester Quizzes: You are expected to attend the Mid-Semester Quizzes.
- A student who is absent from Mid-Semester Quiz without valid Leave of Absence will be given zero mark.
- No makeup Mid-Semester Quiz will be arranged. In case of valid reason for absence, the total course marks would subsequently be rescaled to a base of 100%.

Weekly Quizzes: You are required to attempt 6 quizzes to satisfy this assessment component.
- The scores for the first 6 attempted quizzes will be used to comptute the total for this component.
- You may miss up to two (2) quizzes for any reason without penalty.
- If you miss more than two quizzes without valid reasons, any additional missed quizzes will be assigned a score of 0%.
- Excused Absences: If you miss N quizzes (where N is between 3 and 8) with valid reasons for absence, then the total course marks would subsequently be rescaled to a base of 100%. No makeup Weekly Quizzes will be arranged.

Policy (Others, if applicable)

Diversity and inclusion policy
Integrating a diverse set of experiences is important for a more comprehensive understanding of science.
It is our goal to create an inclusive and collaborative learning environment that supports a diversity of perspectives and learning experiences, and that honours your identities; including ethnicity, gender, socioeconomic status, sexual orientation, religion or ability.
To help accomplish this:

- If you are neuroatypical or neurodiverse, have dyslexia or ADHD (for example), or have a social anxiety disorder or social phobia;

- If you feel like your performance in the class is being impacted by your experiences outside of class;
- If something was said in class (by anyone, including the instructor) that made you feel uncomfortable;

Please speak to your teaching team, our school pastoral officer or a peer or senior (either in-person or via email) about how we can help facilitate your learning experience.

As a participant in course discussions, you should also strive to honour the diversity of your classmates. You can do this by: using preferred pronouns and names; being respectful of others opinions and actively making sure all voices are being heard; and refraining from the use of derogatory or demeaning speech or actions.

All members of the class are expected to adhere to the NTU anti-harassment policy. if you witness something that goes against this or have any other concerns, please speak to your instructors or a faculty member.

**Appendix 1: Assessment Rubrics**

**Rubric for**

- **Mid-semester Quiz: Short Answer Questions 1 (15%)**
- **Mid-semester Quiz: Short Answer Questions 2 (15%)**
- **Weekly Quizzes: Short Answer Questions, 6 out of 8 weekly quizzes (2% each, 12% total)**
- **Final Examination: Short Answer Questions (55%)**

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 Tutorial Presentation: Two tutorial presentations (1.5% each, 3% total)**

Satisfactory: Awarded 1.5% for the tutorial presentation.

- Student arrives prepared with a clear attempt to solve/discuss the assigned tutorial problem.
- Shows a basic understanding of the concepts, even if minor errors are present.
- Communicates the steps or ideas clearly to the class.

Unsatisfactory: Student to reattempt.

- Student demonstrates a lack of preparation or minimal engagement with the tutorial problem.
- Presentation is incomplete or the student cannot explain his/her thought process when prompted.

Non-Performance: Awarded 0% for the tutorial presentation.

- No-Show: Student agreed to a specific presentation slot but was subsequently absent without a valid reason.
- Opt-Out: Student actively refuses to have any presentation slot assigned to them.