香 港 資 優 教 育 學 苑
The Hong Kong Academy for Gifted Education

FROM NUMBER THEORY TO NETWORK COMMUNICATION SERIES:

BASIC NUMBER THEORY

(MATS2440)

Introduction

- How do QR codes work? Why are damaged QR codes still decodable?
- How does Bitcoin work? How to protect your Bitcoins against hackers?
- What is the theory behind e-signature? How to verify its authenticity? How to prevent the receiver from reusing it without the sender's authorisation?

With the rapid development of computers and the internet, there is a great demand on security and accuracy in electronic transmission of information, which has stimulated the great development of coding theory and cryptography over the past few decades. At heart, these theories rely heavily on number theory and abstract algebra, which are two important, classical branches of pure mathematics. In this series of courses, we will appreciate the interaction of pure and applied mathematics and explore some of their real-world applications.

The "From Number Theory to Network Communication Series" programmes offered by the **Department of Mathematics, The Chinese University of Hong Kong**, are designated for students to learn Cryptography progressively.

From Number Theory to Network Communication Series consists of the following programmes:

Programme	Code	Application	Programme held
Basic Number Theory	**MATS2440**	**Jul-19**	**Oct 2019**
Introduction to Abstract Algebra	**MATS3270**	**Oct-19**	**Dec 2019**
Foundations of Coding Theory	**MATS3430**	**Jan-20**	**Mar 2020**
Introduction to Cryptography	**MATS3440**	**Apr-20**	**Jun - Jul 2020**

Here comes the first programme in the series, Basic Number Theory.

"Mathematics is the queen of the sciences, and number theory is the queen of mathematics" – by German mathematician Carl Friedrich Gauss (1777–1855)

Number Theory is a branch of pure mathematics which originated from the study of integers. Integer, which is the essential tool to do counting, is one of the major discoveries in human civilization. Despite of the early discovery of the integer system, its mathematical structures and properties are so rich that related researches are still being carried out even now. That makes number theory to be a long lasting queen of mathematics.

In this course, we will discuss some fundamental results in basic number theory including Euclidean algorithm, linear Diophantine equations, modular arithmetic, Chinese Remainder Theorem, Fermat's Little Theorem, Euler's Theorem…

Programme Type / Level

Numbers and Arithmetic Course (Level 3) (Token-required)

Instructor(s)

Dr Liu Chun Lung Kelvin

Pre-requisites

Student should

1) have basic knowledge in secondary school algebra, including algebraic expressions, polynomials, factorization, simultaneous equations in two unknowns, quadratic equations and functions;
2) have great passion in studying deeper mathematical theories and rigor.

Target Participants

- S1 – S6 HKAGE student members
- Class size: 30

All applicants **MUST** attend the screening test held on **17 Aug 2019** in **CUHK**

Medium of Instruction

Cantonese with English handouts

Certificate

E-Certificate will be awarded to participants who have:

- Attending **at least 3 sessions AND**
- Satisfactory performance in all assignments and assessments

Intended Learning Outcomes

Upon completion of the programme, participants should be able to:

1. apply basic knowledge and concepts of number theory in problem solving;
2. solve simple computational problems with knowledge in number theory;
3. provide rigorous proofs for simple mathematical statements with knowledge in number theory;
4. appreciate the beauty of number theory.

Application Deadline

12 Aug 2019 12:00 n.n.

Application Result Release Date

30 Aug 2019

If student members withdraw from the programme after the Application Deadline, the token will be deducted.

Schedule

Session	Date	Time	Venue	Content
	17 Aug 2019	**2:30 p.m. – 3:30 p.m.**	**LT8 YIA CUHK**	**Screening Test**
~~Cancelled~~	~~5 Oct~~	2:00 p.m. – 5:00 p.m.	ARC 211 CUHK	
1	12 Oct			Basic Concepts Euclidean Algorithm
2	19 Oct			Linear Diophantine Equations Modular Arithmetic
3	26 Oct			Chinese Remainder Theorem Modular Exponentiation
4	2 Nov			Fermat's Little Theorem and Euler's Theorem Primitive Roots

Remarks: For any assessment to be held in the programme, no make-up will be arranged, including Screening Test.

Direction to ARC from the University Station (Map)

ARC: Lee Shau Kee Architecture Building

Sample Examples for the Programme

1) Let a and b be integers and let p be a prime. Prove that if $p|ab$, then $p|a$ or $p|b$.
2) Find $17^{-1} \pmod{101}$.
3) Solve $x \equiv 5 \pmod{12345}$, $x \equiv 7 \pmod{11111}$.

Enquiries

For enquiries, please contact us at 3940 0101 after language selection, press "1".