❖科目名Course Title			
数論アルゴリズム			
❖担当教員Instructor			
長谷川 雄之			
❖開講学期Semester	前期	❖対象学年Year	3年
❖履修可能人数Capacity	5名	❖単位数Number of Credits	2
❖授業形態Type of Class	遠隔		

❖キーワードKey Words

整数、ユークリッド互除法、合同式、繰り返し自乗法、孫子の定理、オイラー関数、原始根、ＲＳＡ暗号

❖授業の目的Course Objectives

今の社会は情報技術抜きには成り立たない。数論はその根幹部分と深く関わっており、そのことを理解してもらうために数論アルゴリズムの基礎について講義する。

❖授業概要Course Description

試験日を除き、教員からの講義による授業を行う。また、講義を行う週のうちの４つ以上の週で、成績評価に関係する演習を事前通告なく行う。

❖到達目標Course Goals

(1) 拡張ユークリッド互除法の意味を理解し、かつ計算ができる。
(2) 合同式の計算、特に繰り返し自乗法を用いた計算ができる。
(3) １次合同式が解ける。
(4) 孫子の定理の意味を理解し、かつ連立合同式が解ける。
(5) オイラー関数の意味を理解し、かつ計算ができる。
(6) フェルマーの小定理、オイラーの公式を用いた計算ができる。
(7) 原始根に関する計算ができる。
(8) 暗号理論の基礎を理解し、一定の計算ができる。

❖授業計画Course Schedule

1. 整数に関する基礎事項
2. ユークリッド互除法
3. 拡張ユークリッド互除法
4. 合同式（定義と基本性質）
5. 合同式（繰り返し自乗法）
6. １次合同式
7. １次合同式の解法
8. 孫子の定理
9. 連立合同式の解法
10. 中間試験
11. フェルマーの小定理、オイラーの公式
12. オイラー関数の性質
13. 原始根と離散対数
14. ＲＳＡ暗号（暗号化と復号のしくみ）
15. ＲＳＡ暗号（復号の演習）
16. 期末試験

❖成績評価Grading System

成績は、２回の試験（いずれも100点満点）および演習をもって評価する。
合格基準は次の(1)、(2)をともに満たすこととする。
(1) (a)+(b)+(c)≧60　（左辺の合計の小数点以下は切捨て）
　(a) 中間試験の得点×0.4
　(b) 期末試験の得点×0.4
　(c) 演習点（20点満点）
(2) 期末試験の得点≧45

❖テキストTextbooks

市販のものは特に指定しない。講義内容に関連するプリントを適宜作成し配付する。

❖参考書Reading List

必要に応じて講義中に紹介する。

❖準備学習Homework

❖オフィスアワーOffice Hour

火曜日14:35～16:05

❖連絡先（E-mail）E-mail

yuji(at)mmm.muroran-it.ac.jp

❖質問・相談への対応方法Contact Information

Eメールにて受付(件名には所属大学名と氏名を明記して下さい。)

❖履修上の注意Notes

１．試験をひとつでも欠席した場合は不合格である。
２．中間試験前の演習がすべて未提出の場合は、中間試験の受験資格を喪失する（したがって、自動的に不合格となる）。
３．病気・事故等やむを得ない事情により中間試験・期末試験を欠席した場合、追試験を行う。同様に、病気・事故等やむを得ない事情により演習を行った週を欠席した場合、演習の事後提出を認める。ただし、どちらも以下の【 】内の条件を満たしている場合に限る。
【シラバス記載の連絡先に直ちに連絡すること。欠席理由を証明する書類の提出を求めることがある。その上で、欠席日より１週間以内に所属大学の担当事務に欠席届を提出・受理されていること。】
４．演習課題が未提出の場合、成績判定において著しく不利となる。演習を実施した週に正当な理由なく欠席した場合は未提出として取り扱う。
５．再試験は行わない。
６．学生からの申し出による合格の取消は認めない。

❖備考Other Information

※「対象学年」と「単位数」は，科目提供大学における数字であり，受講大学に応じて異なるので，所属大学で確認してください。
※「履修可能人数」は，科目提供大学以外の人数であり，遠隔と対面それぞれの受講形態で履修できる人数を示しています。(例.5(遠隔)，5(対面):遠隔授業で5名，対面授業で5名まで履修可能。)
※北海道大学の対面授業は，教室の収容人数によって履修できない場合があります。