室蘭工業大学　前期提供科目

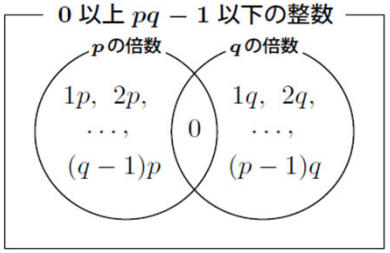
数論アルゴリズム

担当教員 *teacher in charge*

長谷川 雄之

室蘭工業大学
ひと文化系領域
准教授

$$\begin{aligned}\varphi(pq) &= pq - p - q + 1\\ &= (p-1)(q-1)\\ &= \varphi(p)\varphi(q)\end{aligned}$$



授業の目的

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。

到達目標

(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。

成績評価

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

授業計画

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