情報数学

第14回
補遺

久保田 匠
情報システム学科

今日の内容

- 授業の重要な部分はすべて終わった。
- 今日はシラバスで消化しきれていない内容を補充する。
- 試験範囲外なので気楽に聞いてもらって良い。

除法定理（除法の原理）

- 以下は高校で習っている。

a を整数, b を自然数とする。このとき

$$a = qb + r \quad (0 \leqq r < b)$$

を満たす整数 q, r がただひとつ存在する。

- a = 13, b = 5 とすると 13 = 2*5 + 3 より q = 2, r = 3

素数と素因数分解

- 素数と素因数分解は中学で習っている。
- 2以上の自然数p が、1とp自身しか正の約数をもたないとき、pを素数という。
  - *13*の正の約数は *1* と *13* のみ。よって *13* は素数。
  - *12* の正の約数は *1, 2, 3, 4, 6, 12*。よって *12* は素数ではない。
- 任意の自然数は素数の積の形で表すことができる。
- これを素因数分解という。
- 12 を素因数分解すると $12 = 2^2 \cdot 3$
- 大きなふたつの素数の積（10進数で300～1000桁程度）の素因数分解は現在でも困難。
- RSA暗号はこの素因数分解の困難性を利用した暗号。

ユークリッドの互除法

- ユークリッドの互除法も高校で習っている。
- a, bを自然数とする。a, bに共通な約数のうち最大の数を最大公約数という。
  - *12と18の約数はそれぞれ*
  - *12の約数 → 1, 2, 3, 4, 6, 12*
  - *18の約数 → 1, 2, 3, 6, 9, 18*
  - だから *12と18*の最大公約数は *6* である。
- ふたつの自然数の最大公約数を gcd(a,b)で表す。
- aをbで割った商をq、余りを r とすると、除法の原理より a = qb + r が成り立つ。
- このとき gcd(a, b) = gcd(b, r) が成り立つ。
- 上記の等式を繰り返し適用することで a, b の最大公約数が求まる（ユークリッドの互除法）。

オイラー関数

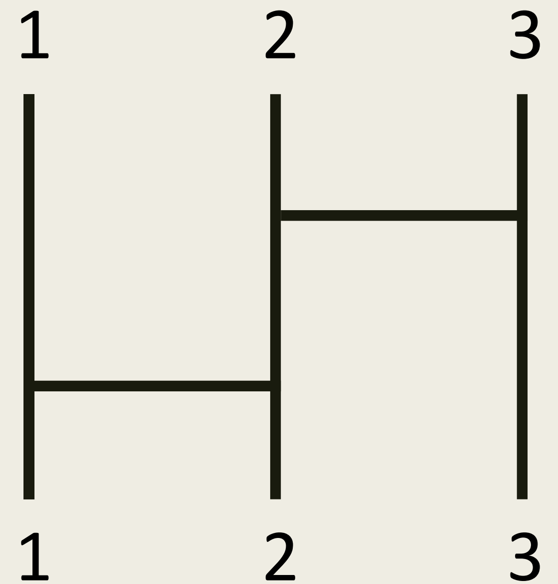
- gcd(a,b) = 1 のとき、aとbは互いに素であるという。
- 自然数nに対して n と互いに素である1以上n以下の自然数の個数をϕ(n)で表す。関数ϕをオイラー関数と呼ぶ。
- ϕ(6) を求めてみよう。
  - *1*から*6*のうち*6*と互いに素な数は *1,5* の*2*個。
  - よって*φ(6) = 2.*
- ϕ(7) を求めてみよう。
  - *1*から*7*のうち*7*と互いに素な数は *1,2,3,4,5,6* の*6*個。
  - よって *φ(7) = 6.*
- 一般に、素数p に対してϕ(p) = p-1.

置換

- f: A → B が全射かつ単射であるとき**全単射**という。
- 特に A = B であるとき、つまり全単射 f: A → A を A 上の**置換**という。

例.
A = {1,2,3} とする。f: A → A を f(1) = 2, f(2) = 3, f(3) = 1 と定めると f は A上の置換である。

- 置換はいわば「あみだくじ」。
- ふたつの置換の合成はあみだくじの「合体」に対応する。
- [発展的な話題] 置換は方程式の可解性を議論をする上で本質的に重要であり、ガロア理論と密接に関連している。



[発展] 方程式の可解性

n次方程式は複素数の範囲で
(重複込みで)n個の解が存在する。
「存在する」と「表せる」は違う。

- 2次方程式 $ax^2+bx+c = 0$ の解は

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- 解 x が四則演算と冪根（k乗根）で表せる（代数的に解ける）。
- 3次以上の方程式はどうか？

ここで初めて
虚数が登場

k次方程式	代数的に解ける？	誰によっていつ示された？
3次方程式	Yes	カルダノ（タルタリア）, 1545年
4次方程式	Yes	フェラリ, 1545年
5次以上	No	アーベルとルフィニ, 1824年

[発展] 方程式の可解性

k次方程式	代数的に解ける？	誰によっていつ示された？
3次方程式	Yes	カルダノ（タルタリア）, 1545年
4次方程式	Yes	フェラリ, 1545年
5次以上	No	アーベルとルフィニ, 1824年

- ガロアも 1829年 に5次以上の方程式が(一般には)代数的に解けないことを証明した。
- ガロアは「どのような方程式がなぜ代数的に可解なのか」にまで踏み込んだ。
- ガロアはその研究で「群」と呼ばれる概念に到達。
- 群とは、演算がひとつ入った集合で、置換（あみだくじ）のように、「単位元（何もしない元）」と「逆元」があり、必ずしも交換法則が成り立たないもの。

オイラーの定理（数論）

- オイラーは偉い数学者なので「オイラーの定理」だけだとどの定理か定まらない。
- 「数論とか初等整数論のオイラーの定理」といえば数学者は「ああ、あの定理ね」と伝わる。

オイラー（1707-1783）

定理（オイラーの定理（数論））.
a, nを自然数とし、aとnは互いに素とする。
このとき以下が成立。

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

オイラーの定理（数論）

- オイラーの定理はフェルマーの小定理の一般化。
- 素数pに対してφ(p) = p-1 を思い出そう。

定理（オイラーの定理（数論））.
a, nを自然数とし、aとnは互いに素とする。
このとき以下が成立。

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

定理（フェルマーの小定理）.
pを素数とし、aを自然数する。aとpが互いに素ならば以下が成立。

$$a^{p-1} \equiv 1 \pmod{p}$$

情報数学の試験について

★到達目標

- (a) 集合，写像，関係について，
  - *1)* 集合/論理 演算ができ，
  - ~~*2)* 写像，関係を説明できる。~~
- (b) 帰納法について，
  - *1)* 帰納的定義/帰納的アルゴリズムに従って処理ができ，
  - ~~*2)* その性質を求められる。~~
- (c) 整数演算について，
  - *1)* 不定方程式または合同方程式の解法ができ，
  - *2)* ベキ乗の剰余演算ができる

★成績評価

- A: 到達目標(a1), (b1), (c1)を達成し, 6つの到達目標を総合的に90%以上達成。
- B: 到達目標(a1), (b1), (c1)を達成し, 6つの到達目標を総合的に80~89%達成。
- C: 到達目標(a1), (b1), (c1)を達成し, 6つの到達目標を総合的に70~79%達成。
- D: 到達目標(a1), (b1), (c1)を達成。

演習

- 残った時間は演習。
- 授業評価アンケートにまだ答えていない学生は答えてください。
- 授業評価アンケートに答えた学生から期末試験の勉強。
- 何か質問があれば遠慮なく聞いてください。