代数学序論のノート

SHINGO TAKI

Abstract. ２年生の代数学序論のノートである.

Contents

Date: May 23, 2022.
Key words and phrases. Euclid の互除法，合同式，平方剰余の相互法則.
Version 0.32.

1. はじめに

東海大学理学部数学科 2 年生向けの授業「代数学序論」の講義ノート[1]である．大学生の向けの講義ではあるが，高度な微分積分を駆使しているような箇所は全くなく,「数学の議論」にさえ付いて来られれば中学生や高校生でも読み終えることが可能だと思う．話題は初等整数論であり，Euclid の互除法から始めて，一次不定方程式，合同式，Euler の定理（Euler の名前が付いている定理は沢山あるが）に触れ，平方剰余の相互法則が一つの目標である．

「代数学序論」はカリキュラムの性質上，今後学ぶと期待されている抽象代数（群，環，体）学への入門の役割を担っているハズである．しかし実のところあまりそれらを意識してノートを用意していない．また初等整数論に付き物（？）の暗号理論などの応用も全く意識していない．個人的に面白そうだと思う初等整数論の話題を扱い，結果的にその後の話に繋がればその都度コメントを少しする，という具合で講義ノートを準備した.（後日「意識的に」記述を変えるかもしれない.）

[1]2016 年度と 2017 年度は大体このノート通りに講義を行った.

前半部分は Euclid の互除法が物を言う世界であり，具体的な計算を実行できることが大切である．中盤以降は多少抽象論がでてくる．「同値関係」や「商集合」などは大体の若者（？）が一度は足を止めてしまう概念である．このあたりまでの原稿を書く上で [1], [2] を参考にしている．後半は初等整数論の花形「平方剰余の相互法則」である．[1], [4] を参考にした．初等整数論の話とは言えないが，付録として高次方程式論の話がある．個人的には割と好きな話である．Galois 理論を表に出さず 5 次（以上の）方程式の代数的可解性の議論をしている．ただし一つだけ「仮定」をして議論している．普通ここの議論を省いてはダメなのだが，講義の時間上省略した．[3] にちゃんとした解説があるので，長期の休みの時に埋めていただけるとありがたい．また人によっては「卒業研究」のネタにしてしまう事も悪くないと思う．（ただし私以外の先生のところで取り組んでいただく事を強く勧める．）ここでは [3] や [5] を参考にした．

1.1. **カリキュラムの覚書．** この授業は「半期に 90 分授業が 30 コマ」という形式で行われる．このノートで扱っている分量だと，試験を授業期間中に行ったとしても 13 週（26 コマ）くらいでなんとか終えられる[2]と思う．

カリキュラム的に，この授業を受講している学生さんは「線形代数は学習済み」という事になっている．ただし対角化くらいまでで，Jordan 標準形はやっていない．集合論は触れているが，写像の単射性や全射性くらいまでで，濃度や同値関係はやっていない．対角線論法は当然やってない．（集合論をやっていないと同値な気もする …．）距離空間や位相空間論も既に学習しているようであるが，ϵ-δ はこの授業と平行して学習している．この辺はちょっと謎な現象である．代数学序論の後に，群論を勉強し，環論と体論を勉強する．

[2]とは言うものの，演習の時間を設けなくてはならないので，案外「相場」かもしれない．

2018 年度の新入生からカリキュラムが変わる.「半期に 100 分授業が 28 コマ」になる．よくわからないが，予備知識は大差ないと思われる．もしかしたら対角線論法は学習済みになるかもしれない.

2. 数学的帰納法と除法の定理

数学的帰納はよく使う証明方法の一つである．まず最初に復習しておく.

数学的帰納法

自然数 n に対し，P_n を n に関する命題とする．P_n が
- P_1 は真（P_1 が成り立つ）.
- 任意の自然数 k に対して P_k が真ならば P_{k+1} も真.

をみたすとき，すべての n に対して P_n は真である.

おそらくこの枠を何度眺めても帰納法を使いこなせるようにはならない．実際に使ってみることである.

例 2.1. $P_n : 1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ 数学的帰納法を用いて示す.

- $n = 1$ のとき，左辺は 1^2 であり，右辺は $1(1+1)(2\times 1+1)/6$ であり，ともに 1 である．従って P_1 は真である.
- $n = k$ のとき P_k が真，つまり
$$1^2 + 2^2 + \ldots k^2 = \frac{k(k+1)(2k+1)}{6}$$
が成り立つと仮定する．このとき両辺に $(k+1)^2$ を加えると
$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\ &= (k+1) \times \frac{2k^2+7k+6}{6} \\ &= (k+1) \times \frac{(k+2)(2k+3)}{6} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \end{aligned}$$

である．従って P_{k+1} も真である．

例 2.2. n を自然数とする．このとき，n^3+5n は 6 の倍数であることを数学的帰納法を用いて次を示す.

$n=1$ のとき $1^3+5\times 1=6$ なので 6 の倍数である．k^3+5k が 6 の倍数であるとする.

$$\begin{aligned}(k+1)^3+5(k+1) &= k^3+3k^2+3k+1+5k+5\\ &= k^3+5k+3k(k+1)+6\end{aligned}$$

であるが，k か $k+1$ のどちらかは偶数なので $3k(k+1)$ は 6 の倍数である．従って $(k+1)^3+5(k+1)$ は 6 の倍数である.

例 2.3. n を自然数とする．このとき，$2^{2n}-1$ は 3 で割り切れることを数学的帰納法を用いて次を示す.

$n=1$ のとき $2^{2\times 1}-1=2^2-1=3$ なので 3 で割り切れる．$n=k$ のとき $2^{2k}-1$ が 3 で割り切れると仮定する．$2^{2(k+1)}-1=2^{2k+2}-1=2^{2k}\times 2^2-4+4-1=4(2^{2k}-1)+3$ であるが，仮定より $2^{2k}-1$ は 3 で割り切れるので，$4(2^{2k}-1)+3$ も 3 で割り切れる．以上より，$2^{2n}-1$ は 3 で割り切れる.

帰納法を用いて次の定理を示す．この定理は次節で示す Euclid の互除法の鍵となるものである.

定理 2.4 (除法の定理)**.** a,b を整数，特に b を正とする．このとき $a=bq+r$ $(0\leq r<b)$ をみたす整数 q,r が唯一つ存在する.

除法の定理とは言え，話は小学生の時にやった「余りのある割り算」である．$a=309, b=25$ とすると $309=25\times 12+9$ なので $q=12, r=9$ である.

証明の前に微妙な例を見ておく．$a<0$ のときに注意が必要である.

例 2.5. $a=-720, b=23$ とする．このとき

(1) $-720=23\times(-31)-7$ より $q=-31, r=-7$ である.

(2) $-720 = 23 \times (-32) + 16$ より $q = -32, r = 16$ である．

などが考えられる．計算そのものとしてはどちらも間違いではないのだが，除法の定理の主張に $0 \leq r < b$ とあるので，我々の立場からは (1) の考え方は却下する．

除法の定理を証明していくが，示すべきことは「q と r が一意的に存在する」である．ここでは「存在」と「一意性」を 2 つに分けて示す．

Proof. まずは存在から示す．$a = 0$ のときは $q = r = 0$ とすれば良い．$a > 0$ とする．もし $a < b$ であれば，$q = 0, r = a$ とすれば良い．そこで $a \geq b$ として a に関する帰納法を用いる．

$a = 1$ ならば $b = 1$ であり，$q = 1, r = 0$ である．任意の自然数 k に対し，除法の定理が成り立つとする．つまり $a = 2, 3, \ldots, k$ のとき $a = bq + r,\ (0 \leq r < b)$ をみたす整数 q と r が存在すると仮定する．このとき $k + 1 = bq + r,\ (0 \leq r < b)$ をみたす整数 q と r が存在すれば良い．

さて，$k + 1 - b$ は k 以下の自然数であることに注意する．すなわち $k+1-b = bq_1+r_1,\ (0 \leq r_1 < b)$ をみたす整数 q_1, r_1 が（一意的に）存在する．従って $k+1 = (q_1+1)b+r_1$ であり，$q = q_1+1, r = r_1$ とすれば良い．$a < 0$ であれば，$-a > 0$ なので $-a = bq' + r',\ (0 \leq r' < b)$ をみたす整数 q' と r' が（一意的に）存在する．すなわち $a = b(-q') + (-r')$ である．もし $r' = 0$ であれば $q = -q', r = 0$ とすれば良い．もし $r' > 0$ であれば $a = -q'b - r' = b(-q' - 1) + b - r'$ なので，$q = -q' - 1, r = b - r'$ とすれば良い．今 $0 < r' < b$ より $0 < b - r' < b$ であることに注意する．

次に一意性を示す．方針は「除法の定理の主張をみたす q と r が 2 つあるとする．すると，いろいろな議論の末，結局はその 2 つは一致する」というものである．これは一意性を示す時の定石と言えるほどのものである．

$a = bq + r = bq_0 + r_0\ (0 \leq r, r_0 < b)$ と 2 通りの表し方ができたとする．このとき $b(q - q_0) = r_0 - r$ と $|r_0 - r| < b$ に注意する．また $q - q_0$

は整数であるから，$b(q-q_0)=r_0-r=0$ を得る．つまり $q=q_0, r=r_0$ である． □

注意 2.6. 前半の「存在」に関する証明で,「一意性も同時に示せているのでは?」と思うかもしれないが，$a=b=1$ の場合に少し問題がある．$q=1, r=0$ だが，この 1 や 0 の一意性を示していないことに注意する．実際，有理整数環 $\mathbb{Z}$ 内で 1 や 0 は一意的である．(おそらく環論の授業の最初にもやるハズである.）この辺りの議論を終えておけば，後半の一意性に関する議論は前半部の存在証明のところへ押し付けることができる．

定義 2.7. 定理 2.4 の q と r をそれぞれ a を b で割った時の**商**と**余り**という．

3. 最大公約数と Euclid の互除法

Euclid の互除法は初等整数論において最も重要な定理である．このノートのほとんどの命題はこれから導かれると言って過言ではない．幾つか記号の定義をする．

定義 3.1. a, b を整数とする．$b=aq$ をみたす整数 q が存在するとき $a|b$ と記す．これは「a が b を割り切る」や「a（と q）は b の約数」を意味する．

注意 3.2. $a|b$ であれば $\pm a|\pm b$ であるので，整数の符号は「割り切る」「割り切らない」などの整除関係に影響を与えない．整数の約数は正のものだけを考える，という姿勢もあろうが,「負の数の約数は定義しない」という姿勢だと後でやる一次不定方程式や合同式を考えるときに困る．また 0 の約数は 0 以外の整数すべてである．

本稿を手にする人は既に知っていることであろうが，上で定義した記号を使って次を定義する．

定義 3.3. a, b を整数とする．

- 整数 d が $d|a$ かつ $d|b$ をみたすとき，d を a と b の**公約数**と言う．
- d を a と b の正公約数とする．a と b の任意の公約数 d' に対し，$d'|d$ のとき d は a と b の**最大公約数**という．

例 3.4. $a = 24, b = 18$ のとき，公約数は $\pm 1, \pm 2, \pm 3, \pm 6$ であり，このうち全ての数で割り切られる数は ± 6 である．-6 は負の数なので，最大公約数は 6 である．

補題 3.5. 最大公約数 d は任意の公約数 d' に対し $d' \leq d$ である．特に最大公約数は一意的に定まる．

Proof. 約数は正の数であるから，$d'|d$ であれば $d = d'q$ をみたす正の整数 q が存在する．つまり $d' \leq d$ である．また d と e を最大公約数とすると，$d \leq e$ と $e \leq d$ が成り立つ．従って $d = e$ である． □

注意 3.6. 代数（特に環論）の勉強を進めてから，このあたりを振り返る[3]と，$d > 0$ としている仮定を不満に思うかもしれない．「d を a と b の公約数として，a と b の任意の公約数 d' に対し，$d'|d$ のとき $\cdots$ 」とするのである．そうすると，最大公約数は複数（ほとんどの場合 2 つ）現れることになる．その場合でも特に理論的には困らないのだが，説明文の中にイチイチ「正の最大公約数を $\cdots$ 」というというフレーズが現れてしまい，何かとメンド臭いので $d > 0$ としている仮定を付けている．

定義 3.7. a, b を整数とする．

- a と b の最大公約数を (a, b) や $\mathrm{GCD}(a, b)$ と記す．
- $(a, b) = 1$ のとき a と b は**互いに素**という．

例 3.8. 最大公約数を求めるときの一つの手段は素因数分解である．

- $132 = 2^2 \times 3 \times 11$ であり，$60 = 2^2 \times 3 \times 5$ なので 132 と 60 の公約数は $1, 2, 2^2, 3, 2 \times 3, 2^2 \times 3$ である．このうち最大のものは $2^2 \times 3 = 12$ である．つまり $(132, 60) = 12$ である．

[3]そういう機会があるかどうかは知らないが．

- $196 = 2^2 \times 7^2$ であり $54 = 2 \times 3^3$ なので 196 と 54 の公約数は 1 と 2 のみ．従って $(196, 54) = 2$ である．

素因数分解が簡単な場合には上のように最大公約数を求めることができるが，一般に大きな数の素因数分解は難しい.（実はこれがある種の「暗号」の基礎になっている.）素因数分解をしなくても最大公約数を求めることは可能である．それが **Euclid の互除法**である．鍵となるのは定理 2.4 の除法の定理である．それを今から使う形に書き換えて置くと，

除法の定理（変形版）

自然数 a, b が $a > b$ をみたすとする．このとき $a = bq + r$ $(0 \leq r < b)$ をみたす自然数 q, r が唯一つ存在する．

である．

もし $r = 0$ であれば，$a = bq$ であり，最大公約数が求まった．もちろん $(a, b) = b$ である．もし $r \neq 0$ であれば，b と r に関して除法の定理を用いる．つまり $b = rq_1 + r_1$ $(0 \leq r_1 < r)$ をみたす自然数 q_1, r_1 を唯一つ得ることができる．もし $r_1 = 0$ であれば，$b = rq_1$ であり，$a = bq + r = rq_1q + r = r(q_1q + 1)$ である．つまり r は a と b の公約数である．実はこれが公約数の中で最大である．すなわち次が成り立つ.

主張 3.9. $(a, b) = r$.

Proof. $(a, b) = d \neq r$ とすると自然数 a_1, b_1 が存在し，$a = a_1d, b = b_1d$ と表せる．$a = bq + r$ であるから $r = a - bq = (a_1 - b_1q)d$ となる．すなわち d は r の約数である．これは d が最大公約数であることに反する．従って $(a, b) = r$ である． □

さて，もし $r_1 \neq 0$ であれば r と r_1 に関して除法の定理を用いて，上と同じ議論を繰り返す．この議論では非負の整数のみを扱っているので，この議論は有限回で終了する．この「余りが 0 になるまで除法の定理を繰り返す」というのが Euclid の互除法のカラクリである.

注意 3.10. 定理 2.4 は整数の範囲で成り立っていた．それを自然数に制限してる理由は大した話ではない．話の見やすさ，つまり「割り算」を繰り返すと扱う数がだんだんと「小さくなる」という雰囲気を残すためと次が理由である．今 a と b の最大公約数 $(a,b)=d$ を求めようとしている．以前言及したように約数の話に正負を持ち込んでいない．すなわち $(-a,b)=(a,b)$ だからである．

実際のところ，Euclid の互除法は最大公約数を求めるだけに使われるわけではない.（たとえば次の節で扱う一次不定方程式である.）もし $a<0$ であっても，除法の定理を一度使ってやれば全て非負の世界になる．つまり $a=bQ+R$ $(0\leq R<b)$ となるので，$R>0$ と b に対して議論を行えば良い.

命題 3.11 (Euclid の互除法)**.** a,b を整数，特に b を正とする．除法の定理を有限回行うことで

$$\begin{aligned}
a &= bq + r \ (0<r<b)\\
b &= rq_1 + r_1 \ (0<r_1<r)\\
r &= r_1q_2 + r_2 \ (0<r_2<r_1)\\
r_1 &= r_2q_3 + r_3 \ (0<r_3<r_2)\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n \ (0<r_n<r_{n-1})\\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}$$

を得る．このとき $(a,b)=r_n$ である．

Euclid の互除法に現れる式は上の式から下の式を得ているわけだが，全体ができあがると，下から見ていくことが多い．証明そのものもそうである.

Proof. 下 2 つの式に注目すると $r_{n-2}=r_{n-1}q_n+r_n=(q_{n+1}q_n+1)r_n$ であるから r_n は r_{n-2} の約数である．さらに下から 3 つ目にある（はず

の）式を用いると

$$\begin{aligned} r_{n-3} &= (q_{n+1}q_n + 1)r_n q_{n-1} + r_n q_{n+1} \\ &= ((q_{n+1}q_n + 1)q_{n-1} + q_{n+1})r_n \end{aligned}$$

なので r_n は r_{n-3} の約数である．同様にすれば r_n は $r_{n-2}, r_{n-3}, \ldots, r_1, r, b, a$ の約数であることがわかる．つまり r_n は a と b の公約数である．

また，$(a, b) = d$ とすると最大公約数の定義から r_n は d の約数である．一方，主張 3.9 と同様の議論を繰り返すと，d は r_n の約数であることがわかる．すなわち $d = r_n$ である． □

これより直ちに次がわかる．

系 3.12. 整数 a, q と自然数 b に対し $(a, b) = (a - qb, b)$ が成り立つ．

例 3.13. Euclid 互除法を用いて最大公約数を求める．最大公約数そのものは 2 つの数を素因数分解すれば求められるのだが，一般に素因数分解は簡単ではない．また後ほど，最大公約数を求める過程に表れる式が大事になる．

(1) 527 と 341 の最大公約数を求める．

$$\begin{aligned} 527 &= 341 \times 1 + 186 \\ 341 &= 186 \times 1 + 155 \\ 186 &= 155 \times 1 + 31 \\ 155 &= 31 \times 5 + 0 \end{aligned}$$

ゆえに $(527, 341) = 31$ である．

(2) 925 と 1980 の最大公約数を求める．

$$1980 = 925 \times 2 + 130$$
$$925 = 130 \times 7 + 15$$
$$130 = 15 \times 8 + 10$$
$$15 = 10 \times 1 + 5$$
$$10 = 5 \times 2 + 0$$

ゆえに $(925, 1980) = 5$ である．

(3) -7935 と 5796 の最大公約数を求める．

$$-7935 = 5796 \times (-2) + 3657$$
$$5796 = 3657 \times 1 + 2139$$
$$3657 = 2139 \times 1 + 1518$$
$$2139 = 1518 \times 1 + 621$$
$$1518 = 621 \times 2 + 276$$
$$621 = 276 \times 2 + 69$$
$$276 = 69 \times 4 + 0$$

ゆえに $(-7935, 5796) = 69$ である．もちろん $(7935, 5796) = 69$ である．

例 3.14. 整数 x に対し $0 = x \times 0$ であり，$7 = 1 \times 7$ なので $(0, 7) = 7$ である．Euclid 互除法を用いると，$0 = 7 \times 0 + 0$ である．

4. 一次不定方程式

この節の目的は次である．

目的

a, b, c を整数とするとき**一次不定方程式** $ax + by = c$ の整数解を求める．（これは Diophantus 方程式の一種であり，Bézout の等式とも呼ばれる．）

命題 4.1. 整数 a, b の最大公約数を d とする．このとき一次不定方程式 $ax + by = d$ の整数解が存在する．

Proof. $a = 0$ または $b = 0$ ならば $d = b$ 又は a であり，扱う方程式は一次方程式なので解は $x = a/a = 1$ または $y = b/b = 1$ である．

$a, b > 0$ とする．Euclid 互除法を用いて $r_{n-1} = q_{n+1}r_n + 0$ となれば，$r_n = d, (r_{n+1} = 0)$ である．このとき直前の式が $r_{n-2} = q_n r_{n-1} + r_n$ であるので，

$$d = r_{n-2} - q_n r_{n-1} \dots (1)$$

を得る．さらにこの一つ前の式は $r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}$ であり，r_{n-1} について解いて (1) に代入すれば

$$\begin{aligned} d &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= -q_n r_{n-3} + (1 + q_n q_{n-1})r_{n-2} \dots (2) \end{aligned}$$

である．さらに一つ前の式から $r_{n-2} = r_{n-4} - q_{n-2}r_{n-3}$ を得るので，これを (2) に代入して整理すると

$$d = (1 + q_n q_{n-1})r_{n-4} - (q_n + (1 + q_n q_{n-1})q_{n-2})r_{n-3}$$

を得る．このように Euclid 互除法によって得られた式を下から見ていけば良い．つまり $r_{-1} = a, r_0 = b$ とみなせば，$i = 0, 1, \dots, n-1$ について $r_{i+1} = r_{i-1} - q_{i+1}r_i$ であるので，上と同じ変形を繰り返すと d はある整数 c_{i-1}, c_i を用いて $d = c_{i-1}r_{i-1} + c_i r_i$ と表せる．特に $i = 0$ のとき $ac_{-1} + bc_0 = d$ である．つまり $x = c_{-1}$ と $y = c_0$ が解（の一つ）である．

$a < 0, b > 0$ のときは $-a > 0, b > 0$ であるので，一次不定方程式 $(-a)X + bY = d$ は解を持つ．その解を $X = c_{-1}$, $Y = c_0$ とすると $ax + by = d$ の解として $x = -c_{-1}$, $y = c_0$ を得る．

$a > 0, b < 0$ や $a < 0, b < 0$ も同様で，それぞれ $ax + (-b)y = d$ と $(-a)x + (-b)y = d$ を考えれば良い． □

例 4.2. 一次不定方程式 $24x + 136y = 8$ を考える．Euclid 互除法を用いると

$$136 = 24 \times 5 + 16$$
$$24 = 16 \times 1 + 8$$
$$16 = 8 \times 2 + 0$$

を得る．上 2 つの式より

$$\begin{aligned} 8 &= 24 - 16 \times 1 \\ &= 24 - (136 - 24 \times 5) \times 1 \\ &= 24 \times 6 + 136 \times (-1) \end{aligned}$$

である．つまり $x = 6$ と $y = -1$ が $24x + 136y = 8$ の解の一つである．

問題 4.3. 東海道新幹線の座席配置は，だいたいの場合通路を挟んで 2 人席と 3 人席がある．（つまり横 1 列に 5 人の席がある．）この座席配置には何か意味があるか？$d(> 1)$ 人の団体旅行客を上手く座らせる問題と不定方程式 $2x + 3y = d$ を解くということの対応を考え，いろいろと邪推（？）せよ．

命題 4.4. 一次不定方程式 $ax + by = c$ が解を持つための必要十分条件は $(a, b)|c$，すなわち (a, b) は c の約数である．

Proof. 整数 x_0, y_0 を $ax + by = c$ の解とする．$d := (a, b)$ とすると，$a = a'd, b = b'd$ をみたす整数 a', b' が存在する．従って

$$\begin{aligned} c = ax_0 + by_0 &= a'dx_0 + b'dy_0 \\ &= d(a'x_0 + b'y_0) \end{aligned}$$

である．つまり d は c の約数である．

逆に $d = (a, b)$ が c の約数であるとする．命題 4.1 より一次不定方程式 $ax + by = d$ は解を持つので，その一つを $x = x_0, y = y_0$ とする．すなわち $ax_0 + by_0 = d$ である．この両辺を $c' = c/d$ 倍すると

$$a(c'x_0) + b(c'y_0) = c'd = c$$

である．従って $x = c'x_0$ と $y = c'y_0$ は $ax + by = c$ の解である． □

例 4.5. 例 4.2 より，一次不定方程式 $24x + 136y = 16 (= 8 \times 2)$ の解として $x = 6 \times 2 = 12$ と $y = (-1) \times 2 = -2$ がある．

系 4.6. 整数 a, b が互いに素であるとき，任意の整数 c に対し，一次不定方程式 $ax + by = c$ は解を持つ．

Proof. a と b が互いに素であれば $(a, b) = 1$ である． □

次は今までの一次不定方程式論を用いた一つの応用[4]である．

命題 4.7. 整数 a, b, c に対し $(a, bc) = 1$ の必要十分条件は $(a, b) = 1$ かつ $(a, c) = 1$ である．

Proof. 系 4.6 より $(a, b) = 1$ かつ $(a, c) = 1$ であれば，一次不定方程式 $ax_1 + by_1 = 1$ と $ax_2 + cy_2 = 1$ をみたす整数 x_1, y_1, x_2, y_2 が存在する．また

$$\begin{aligned} 1 &= (ax_1 + by_1)(ax_2 + cy_2) \\ &= ax_1(ax_2 + cy_2) + aby_1x_2 + bcy_1y_2 \\ &= a(ax_1x_2 + cx_1y_2 + by_1x_2) + bc(y_1y_2) \end{aligned}$$

が成り立つ．$X = ax_1x_2 + cx_1y_2 + by_1x_2, Y = y_1y_2$ とすれば，これらは一次不定方程式 $aX + bcY = 1$ の解である．従って，命題 4.4 より $(a, bc) = 1$ である．

逆に $(a, bc) = 1$ であれば，系 4.6 より一次不定方程式 $ax + bcy = 1$ の解は存在するが，$ax + bcy = ax + b(cy) = ax + c(by)$ とみなすことにより，一次不定方程式 $ax + by = 1$ も $ax + cy = 1$ も解は存在する．従って，命題 4.4 より $(a, b) = (a, c) = 1$ である． □

さて，一次不定方程式の解の型を調べて行く．線形代数で学んだ連立一次方程式の理論，すなわち（拡大）係数行列の階数や未知数の数の話をここで利用すると，$ax + by = d$ の解が存在するならば，それは

[4]もちろん直接示すこともできる．

無限個存在する．次の命題は一次不定方程式の解が存在すれば，そのすべてを記述するものである．

命題 4.8. 一次不定方程式 $ax+by=c \ldots (*)$ において $d=(a,b)$ が c の約数とする．このとき解の一組を $x=x_1, y=y_1$ とし，$a'=a/d, b'=b/d$ とおくと，$(*)$ の解の全体は

$$x = x_1 + b'k,\ y = y_1 - a'k \quad (k \in \mathbb{Z})$$

である．

Proof. $ax_1+by_1=c$ なので $(*)$ と辺々引くと

$$a(x-x_1)+b(y-y_1)=0$$

である．$a=a'd, b=b'd$ であることに注意し，両辺を d で割ると

$$a'(x-x_1)=-b'(y-y_1)$$

を得る．この右辺は b' を約数に持つが，a' と b' は互いに素なので b' は $(x-x_1)$ を割り切る．故に $x=x_1+b'k\ (k\in\mathbb{Z})$ である．同様に a' は $-(y-y_1)$ を割り切るので $y=y_1-a'k$ である． □

例 4.9. $24x+136y=16$ の全ての解を調べる．$(24,136)=8$ なので，命題 4.8 の記号で，$a'=24/8=3, b'=136/8=17$ である．また，例 4.5 より $24x+136y=16$ の解の一つとして $x=12, y=-2$ があった．従って $24x+136y=16$ の解は $x=12+17k, y=-2-3k$ と書ける．

一次不定方程式の解き方

一次不定方程式 $ax+by=c$ は次の手順で解く.

(1) Euclid の互除法で $d=(a,b)$ を求める.
(2) c を d で割る.
  (2-1) $d \not| c$ ならば解なし.(終了)
  (2-2) $d|c$ ならば $c'=c/d$ として (3) へ.
(3) (1) に現れた式を用いて一次不定方程式 $ax+by=d$ の解を一組み求める. それを $x=x_1, y=y_1$ とする.
(4) $x=c'x_1, y=c'y_1$ は一次不定方程式 $ax+by=c$ の解である.
(5) $a'=a/d, b'=b/d$ とすると一次不定方程式 $ax+by=c$ の全ての解は, $k\in\mathbb{Z}$ を用いて $x=c'x_1+b'k$ と $y=c'y_1-a'k$ の型で書ける.

問題 4.10. 例 3.13 を参考に一次不定方程式 $1980x+925y=30$ の解を求めよ.

5. 素因数分解の一意性

主張そのものは有名である.

定理 5.1 (素因数分解の一意性). 0 と 1 以外の整数は -1 及び幾つかの素数の積として, 積の順序の違いを除いて一意的に表せる.

この定理は二つの主張を含んでいる.「整数は素数の積(と $\pm$)で表すことが可能」という事と「表し方の一意性」である. ある程度素数に馴染みがあると当然のように思うが, この手の話が成り立たない代数系も存在する.(そのうち環論の授業で素元や既約元や UFD などの言葉を耳にするであろう.)以下, この証明をしていくが, 次の補題が大切である.

補題 5.2. p を素数, a,b を整数とする. このとき $p|ab$ であれば $p|a$ または $p|b$ が成り立つ.

Proof. $p|ab$ かつ $p \not| a$ とする．このとき $p|b$ を示せば良い．

$(p, a) = 1$ なので系 4.6 より一次不定方程式 $ax + py = 1$ の整数解が存在する．この両辺に b を掛ければ $abx + bpy = b$ であり，$p|ab$ なので左辺は p で割り切れる．従って $p|b$ である． □

定理 5.1 を示す．n を 2 以上の整数として定理の主張を示せば，$-n$ を考えることによって負の整数に関しても定理の主張を示すことができる．したがって以下では n は 2 以上の整数とする．

Proof. n に関する帰納法を用いる．

まず n が素数の積に分解できることを示す．もし n が素数であれば，当然ながら素数（一つだけ）の積である．そこで n は合成数とする．2 と 3 は素数であるから，最初の合成数は 4 である．この場合は $4 = 2 \times 2$ と素数の積に分解できる．$n > 4$ として $4 < k < n$ をみたす合成数 k は素数の積に分解できると仮定する．今 n は合成数であるから，$1 < a < n$ と $1 < b < n$ をみたす自然数 a, b を用いて $n = ab$ と表すことができる．帰納法の仮定より a と b は素数の積で表せるので，$n = ab$ も素数の積で表せる．

次に一意性を示す．もし n が

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

と 2 通りの素数の積への分解の仕方を持っているとする．素数 p_1 は $n = q_1 q_2 \dots q_s$ を割り切るので補題 5.2 より，ある番号 $j \in \{1, 2, \dots, s\}$ に対して $p_1|q_j$ である．今 q_j も素数であるから $p_1 = q_j$ である．$q_1, q_2, \dots, q_s$ の添字を適当に付け替えることで $p_1 = q_1$ として良い．つまりこのとき

$$n = p_1 p_2 \dots p_r = p_1 q_2 \dots q_s$$

である．$k = n/p_1$ とすれば $1 \leq k < n$ であることに注意する．もし $k = 1$ ならば $n = p_1 = q_1$ であるから，一意性は成り立つ．$k > 1$ ならば $k = p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$ であるが，帰納法の仮定より k の素因数分解は一意的である．つまり $r = s$ であり適当に添字を適当に付け替

えることで

$$p_2 = q_2, p_3 = q_3, \dots, p_r = q_r$$

が成り立つ．$p_1 = q_1$ と合わせれば n の素因数分解の一意性が成り立つ．□

6. 合同式

今まで「余りのある割り算」を考えて来たが，ここでは「余りだけ」で代数をする．

定義 6.1. 整数 a, b と自然数 m に対し $m|(a-b)$ のとき $a \equiv b \mod m$ と記し，a と b は m を法として**合同**という．

例 6.2. m の倍数全体の集合を $m\mathbb{Z}$ とする．すなわち $m\mathbb{Z} = \{0, \pm m, \pm 2m, \dots\}$ である．このとき $a \equiv b \mod m \Leftrightarrow a - b \in m\mathbb{Z}$ である．

(1) $5 - 2 = 3 \in 3\mathbb{Z}$ なので $5 \equiv 2 \mod 3$ である．
(2) $5 - (-1) = 6 \in 3\mathbb{Z}$ なので $5 \equiv -1 \mod 3$ である．
(3) $121 - 0 = 11^2 \in 11\mathbb{Z}$ なので $121 \equiv 0 \mod 11$ である．

補題 6.3. a と b を m で割った時の余りが等しくなるための必要十分条件は $a \equiv b \mod m$ が成り立つことである．

Proof. 定理 2.4（除法の定理）を用いて $a = mq_1 + r_1,\ b = mq_2 + r_2$ と表す．このとき $0 \leq r_1, r_2 < m$ なので $|r_1 - r_2| < m$ に注意する．$a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$ なので，$a - b \in m\mathbb{Z} \Leftrightarrow r_1 = r_2$ である．□

次の補題を見ても「だから何だ？」という気がするのはある意味自然である．しばらくするとアリガタミが分かってくる．必要になったときにもう一度見直すべし．整数を「余りの世界」で考えることには意味がある，という保証をしてくれている．

補題 6.4. a, b, c を整数とし，m を自然数とする．このとき

(1) $a \equiv a \mod m$

(2) $a \equiv b \mod m$ ならば $b \equiv a \mod m$

(3) $a \equiv b \mod m,\ b \equiv c \mod m$ ならば $a \equiv c \mod m$

が成り立つ.

Proof. (1) $a - a = 0 \in m\mathbb{Z}$ より従う. (2) $a \equiv b \mod m$ は $a - b \in m\mathbb{Z}$ の意味であるが, $-(a-b) \in m\mathbb{Z}$ が成り立つので $b-a = -(a-b) \in m\mathbb{Z}$ である. 従って $b \equiv a \mod m$ が成り立つ. (3) $a \equiv b \mod m,\ b \equiv c \mod m$ ならば $a-b, b-c \in m\mathbb{Z}$ であり, $(a-b)+(b-c) = a-c \in m\mathbb{Z}$ が成り立つ. つまり $a \equiv c \mod m$ である. □

注意 6.5. 上の証明だけでなく, 今後も $a - b$ が $m\mathbb{Z}$ に入るかどうか? という議論を多く行う. つまり $a - b$ は m の整数倍になり得るか? という話である. 基本的には次を認識していないと今後の議論を追っていくことは難しいかもしれない.

- $a, b \in m\mathbb{Z}$ ならば $a \pm b \in m\mathbb{Z}$ である.
- $a \in m\mathbb{Z}$ かつ $k \in \mathbb{Z}$ ならば $ka \in m\mathbb{Z}$ である.

これは是非自分でチェックしておくべきである.「$a \in m\mathbb{Z}$ ならば $a = ma'$ をみたす整数 a' が存在するので $\cdots$ 」という具合にやっていけば良い. ピンとこなければ m を 3 や 5 などの具体的な数を入れてみよ.

6.1. **合同式の演算.** この節の初めに「「余りだけ」で代数をする」と宣言したが, そのココロが次の命題である. 整数全体には加法(足し算)と乗法(掛け算)を定めることができるが, 余りだけを考えていても同様の加法と乗法を矛盾なく定める(well-defined)ことができる.

命題 6.6 (合同式の計算則). $a_1 \equiv a_2 \mod m$, $b_1 \equiv b_2 \mod m$ とする. このとき次が成り立つ.

(1) $a_1 + b_1 \equiv a_2 + b_2 \mod m$

(2) $a_1 b_1 \equiv a_2 b_2 \mod m$

Proof. (1) $a_1 \equiv a_2 \mod m$, $b_1 \equiv b_2 \mod m$ ならば $a_1 - a_2,\ b_1 - b_2 \in m\mathbb{Z}$ であり, $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2) \in m\mathbb{Z}$ が成り立

つ．すなわち $a_1 + b_1 \equiv a_2 + b_2 \mod m$ である．(2) $a_1b_1 - a_2b_2 \in m\mathbb{Z}$ を言えば良い．

$$\begin{aligned} a_1b_1 - a_2b_2 &= a_1b_1 - b_1a_2 + b_1a_2 - a_2b_2 \\ &= (a_1 - a_2)b_1 + (b_1 - b_2)a_2 \end{aligned}$$

であるが，$a_1 - a_2,\ b_1 - b_2 \in m\mathbb{Z}$ なので $(a_1 - a_2)b_1 + (b_1 - b_2)a_2 \in m\mathbb{Z}$ である． □

注意 6.7. $a_1 = a_2 = -1$ として (2) を用いると $-b_1 \equiv -b_2 \mod m$ である．ここで (1) を用いると減法（引き算）も矛盾なく定義できる．すなわち $a_1 - b_1 \equiv a_2 - b_2 \mod m$ が成り立つ．

繰り返すが，合同式では加法，減法，乗法が自由にできる．

例 6.8. $0 \leq x \leq 9$ のとき $7 + x \equiv 1 \mod 9$ をみたす x を求める．$7 \equiv 7 \mod 9$ なので問題の合同式から辺々引くと $7 + x - 7 \equiv 1 - 7 \mod 9$ である．故に $x \equiv -6 \equiv 3 \mod 9$ である．$0 \leq x \leq 9$ なので $x = 3$ である．

例 6.9. $273 \times 36 + 478 \times 142$ を 13 で割った余りを求める．

$$\begin{aligned} 273 &\equiv 0 \mod 13 \\ 36 &\equiv -3 \mod 13 \text{（実はこれは計算しなくても良い）} \\ 478 &\equiv 10 \mod 13 \\ 142 &\equiv -1 \mod 13 \end{aligned}$$

なので

$$\begin{aligned} 273 \times 36 + 478 \times 142 \mod 13 &\equiv 0 \times (-3) + 10 \times (-1) \mod 13 \\ &\equiv -10 \mod 13 \\ &\equiv 3 \mod 13 \end{aligned}$$

である．従って求める余りは 3 である．（もちろん $273 \times 36 + 478 \times 142 = 77704 = 13 \times 5977 + 3$ と計算できる．）

命題 6.10. $a \equiv b \mod m$ のとき任意の自然数 k に対し，$a^k \equiv b^k \mod m$ が成り立つ．

Proof. $a^k - b^k \equiv (a-b)\sum_{i=0}^{k-1} a^{k-1-i}b^i$ に注意すれば，仮定より $a-b \in m\mathbb{Z}$ なので $a^k - b^k \in m\mathbb{Z}$ である． □

注意 6.11. 命題 6.6 (2) を k 回用いても良い．

例 6.12. 整数のベキを割った時の話は Fermat 小定理や Euler の定理などもあるが，基本は上の命題である．それを使ってみる．

(1) 24^{100} を 25 で割った余りを求める．
$24 \equiv -1 \mod 25$ なので $24^{100} \equiv (-1)^{100} = 1 \mod 25$ である．
故に 24^{100} を 25 で割った余りは 1 である．

(2) 2010^{10001} を 101 で割った余りを求める．
$2020 = 2^2 \times 5 \times 101$ なので，$2010 \equiv -10 \mod 101$ 及び $2010^2 \equiv 100 \equiv -1 \mod 101$ が成り立つことに注意する．

$$\begin{aligned} 2010^{10001} &= 2010^{2\times 5000+1} \\ &= (2010^2)^{5000} \times 2010 \\ &\equiv (-1)^{5000} \times (-10) \mod 101 \\ &\equiv -10 \mod 101 \\ &\equiv 91 \mod 101 \end{aligned}$$

である．従って 2010^{10001} を 101 で割った余りは 91 である．

合同式において加法（と減法）と乗法の様子は分かった．当然次に気になるのは除法（割り算）である．

疑問 6.13. 整数 a, b と自然数 m に対し $b \equiv aq \mod m$ のとき”商”q は a, b により m を法として唯一に定まるか？また $c \not\equiv 0 \mod m$ のとき，$ac \equiv bc \mod m$ であれば $a \equiv b \mod m$ か？

例 6.14. $39 - 15 = 24 \in 6\mathbb{Z}$ なので $39 = 13 \times 3 \equiv 15 = 5 \times 3 \mod 6$ である．しかし $13 - 5 = 8 \notin 6\mathbb{Z}$ であるから $13 \not\equiv 5 \mod 6$ である．

整数の世界では $c \neq 0$ であり $(a-b)c = 0$ ならば $a - b = 0$ である．合同式はここが上手くいかない．つまり「$xy \equiv 0$ ならば $x \equiv 0$ または $y \equiv 0$」が必ずしも成り立たない．実際上の例で，$(13-5) \times 3 \equiv 0 \mod 6$ であるが $13 - 5 = 8 \not\equiv 0 \mod 6$ かつ $3 \not\equiv 0 \mod 6$ である．

合同式の「除法（割り算）」に相当するものは次である．

命題 6.15. 整数 a, b, c と自然数 m に対して次が成り立つ．

(1) $(c, m) = 1$ のとき $ac \equiv bc \mod m$ ならば $a \equiv b \mod m$ である．
(2) $(c, m) = d > 1$ のとき $m' = m/d$ とすると，$ac \equiv bc \mod m$ ならば $a \equiv b \mod m'$ である．

Proof. (1) $ac \equiv bc \mod m$ ならば $(a-b)c \in m\mathbb{Z}$ であるが，今 $(c, m) = 1$ であるから c は m の倍数ではない．故に $a - b \in m\mathbb{Z}$ である．(2) $c' = c/d$ とするとき $(c', m') = 1$ に注意する．$ac - bc \in m\mathbb{Z}$ であれば $(a-b)(dc') \in dm'\mathbb{Z}$ なので $(a-b)c' \in m'\mathbb{Z}$ である．(1) と同様に $a - b \in m'\mathbb{Z}$ が成り立つ． □

系 6.16. a, b を整数，p を素数とする．このとき $a \equiv 0 \mod p$ または $b \equiv 0 \mod p$ の必要十分条件は $ab \equiv 0 \mod p$ である．($\mathbb{Z}/p\mathbb{Z}$ は**整域**である．)

Proof. $b \not\equiv 0 \mod p$ とする．このとき $ab \equiv 0 = 0 \times b \mod p$ と $(b, p) = 1$ なので，命題 6.15 (1) を用いれば $a \equiv 0 \mod p$ である．逆は合同式の積の演算そのもの． □

6.2. **一次合同式.** 整数 a, b と自然数 m に対し，$ax \equiv b \mod m$ をみたす整数 x を求めたい．しかし我々はそれを得るための術を持っている．少し問題の言い換えをしてみたい．今更強調するまでもないが $ax \equiv b \mod m$ は $ax - b \in m\mathbb{Z}$ の意味である．すなわち $ax \equiv b \mod m$ が成り立つということは $ax - b = my$ をみたす整数 y が存在することである．実際に求めたいものは y ではなくて x であるが，扱っているものは一次不定方程式 $ax - my = b$ である．従って一次不定方程式の理論より次がわかる．

命題 6.17. $d := (a, m)$ とする．このとき次が成り立つ．

(1) 一次合同式 $ax \equiv b \mod m$ が解を持つことの必要十分条件は d が b の約数である．
(2) $ax_1 \equiv b \mod m$ とし，$m' = m/d$ とすると $ax \equiv b \mod m$ の解の全体は $x = x_1 + m'k,\ (k \in \mathbb{Z})$ である．
(3) $ax \equiv b \mod m$ の（m を法とした）解は d 個存在する．つまり $x \equiv x_1, x_1+m', x_1+2m', \ldots, x_1+(d-1)m'$ が一次合同式 $ax \equiv b \mod m$ の全ての解である．

Proof. 命題 4.4 から (1) が，命題 4.8 から (2) が従う．(3) $k, k' \in \mathbb{Z}$ とする．$x_1 + m'k \equiv x_1 + m'k' \mod m$ であれば $m'k \equiv m'k' \mod m$ であるが，$(m, m') = m'$ なので命題 6.15 (2) より $k \equiv k' \mod d$ である．故に異なる k の取り方は d を法として d 通り存在する．すなわち $x = x_1 + m'k$ の取り方は m を法として d 通り存在する． □

命題 6.17 (3) の補足を与える．実際に解いてみれば分かるが，一次合同式 $18x \equiv 30 \mod 48$ の解は $x \equiv 7 \mod 8$ の形である．（例 6.20 を見よ．）言い換えれば $x = 7 + 8k$ であり，具体的な整数として書き下すと $x = 7, 15, 23, 31, 39, 47, 55, \ldots$ となる．しかし今は「48 を法として」考えているので $55 \equiv 7 \mod 48$，つまり 7 と 55 は同一視される．他も同様である．従って一次合同式 $18x \equiv 30 \mod 48$ の具体的な解は $x = 7, 15, 23, 31, 39, 47$ の 6 個ある．

系 6.18. p を素数，$a \not\equiv 0 \mod p$ とする．このとき $ax \equiv 1 \mod p$ となる x が p を法として唯一つ存在する．（$\mathbb{Z}/p\mathbb{Z}$ は**体**である．）

Proof. $(a, p) = 1$ と命題 6.17 から従う． □

一次合同式の解き方

一次合同式 $ax \equiv b \mod m$ は次の手順で解く．

(1) Euclid の互除法で $d = (a, m)$ を求める．

(2) b を d で割る．

(2-1) $d \not| b$ ならば解なし．（終了）

(2-2) $d|b$ ならば $b' = b/d$ として (3) へ．

(3) (1) に現れた式を用いて一次合同式 $ax \equiv d \mod m$ の解を一つ求める．それを $x = x_1$ とする．

(4) $x = b'x_1$ は一次合同式 $ax \equiv b \mod m$ の解である．

(5) $m' = m/d$ とすると一次合同式 $ax \equiv b \mod m$ の全ての解は $x = b'x_1 + m'k$ $(k \in \mathbb{Z})$ と書ける．

(6) 解の個数は d 個，すなわち $x = b'x_1 + m'k$ に対して $k = 0, 1, 2, \ldots, (d-1)$ が異なる解を与える．

注意 6.19. 多少記号の差があるが,「一次不定方程式の解き方」と見比べると Step 6 を除いて本質的に同じである．一次不定方程式の解として x だけ求めて，Step 6 の作業を追加しているだけである．

命題 6.6 と命題 6.15 にあるような合同式の演算を駆使すれば別の解法もある．

例 6.20. 一次合同式 $18x \equiv 30 \mod 48$ をみたす x を求める．

（解１）Euclid の互除法を用いて $(18, 48)$ を求める：

$$48 = 18 \times 2 + 12$$
$$18 = 12 \times 1 + 6$$
$$12 = 6 \times 2 + 0$$

なので $(18, 48) = 6$ であり，$30/6 = 5$ なので一次合同式 $18x \equiv 30 \mod 48$ に解は存在する．次に一次合同式 $18X \equiv 6 \mod 48$ の

解を一つ求める．

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (48 - 18 \times 2) \\ &= 18 \times 3 + 48 \times (-1) \end{aligned}$$

なので $18 \times 3 - 6 = 48 \in 48\mathbb{Z}$，すなわち $X = 3$ は $18X \equiv 6 \mod 48$ をみたす．故に $18x \equiv 30 \mod 48$ の解として $x = 5 \times 3 = 15$ がある．故に $18x \equiv 30 \mod 48$ の全ての解は

$$\begin{aligned} x &= 15 + \frac{48}{6}k \\ &= 15 + 8k \end{aligned}$$

で与えられる ($k \in \mathbb{Z}$)．$18x \equiv 30 \mod 48$ の解は 6 個存在し，具体的に表すと $k = -1, 0, 1, 2, 3, 4$ のときの $x = 7, 15, 23, 31, 39, 47$ である．

（解２）$(18, 48) = 6$ なので命題 6.15 より $18x \equiv 30 \mod 48$ ならば $3x \equiv 5 \mod 8$ である．$8x \equiv 0 \mod 8$ なので，これらの辺々引くと $5x \equiv -5 \mod 8$ である．再び命題 6.15 と $(5, 8) = 1$ を用いれば，$x \equiv -1 \equiv 7 \mod 8$ を得る．つまり $18x \equiv 30 \mod 48$ の解は $x = 7 + 8k$ の型をしており，$k = 0, 1, 2, 3, 4, 5$ が異なる 6 個の解 $x = 7, 15, 23, 31, 39, 47$ を与える．

例 6.21. 一次合同式 $7x \equiv -2 \mod 24 \ldots (1)$ の解を求める．

まず，$(7, 24) = 1$ なので解は 1 つだけであることに注意する．$24x \equiv 0 \mod 24$ であるから，(1) の両辺を 3 倍したものこれから引くと $3x \equiv 6 \mod 24 \ldots (2)$ を得る．[5]最後に (1) と (2) の辺々を引くと $4x \equiv -8 \mod 24 \ldots (3)$ であり，(3) と (2) の辺々を引いて $x \equiv -14 \equiv 10 \mod 24$ を得る．

[5]ここで一番やってはイケナイのが「この両辺を 3 で割って，$x \equiv 2 \mod 24$」である．実際に (1) に $x \equiv 2$ を代入すると $14 \equiv -2 \mod 24$ となってオカシイ．

6.3. **連立一次合同式（中国式剰余定理）.** 合同式に関する四則演算の事がわかり，一次合同式の事も触れた．次にくるのはやはり（？）連立一次合同式であろう．

定理 6.22 (中国式剰余定理, 孫子の定理). それぞれ互いに素な自然数 $m_1, m_2, \ldots, m_k$ （つまり $i \neq j$ であれば $(m_i, m_j) = 1$）と整数 $a_1, a_2, \ldots, a_k$ に対し，連立一次合同式

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \qquad \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

をみたす解は $M := m_1 m_2 \ldots m_k$ を法として唯一つ存在する．

Proof. （解の存在について） $M_i = M/m_i$ とすると，各 i に対して $(m_i, M_i) = 1$ に注意する．命題 6.17 より一次合同式 $M_i t_i \equiv 1 \mod m_i$ をみたす t_i は m_i を法として唯一つ存在する．また $i \neq j$ であれば M_j には m_i が約数として含まれているので $M_j \equiv 0 \mod m_i$ である．そこで $X := \sum_{i=1}^{k} M_i t_i a_i$ とすると，

$$\begin{aligned} X &\equiv 0 + 0 + \cdots + 0 + 1 \times a_i + 0 + \cdots + 0 \mod m_i \\ &\equiv a_i \mod m_i \end{aligned}$$

である．つまりこの X は連立一次合同式の解の一つである．

（解の一意性について）与えられた連立一次合同式の解として Y も存在したとする．すなわち $Y \equiv a_i \mod m_i$ をみたす．$X \equiv a_i \mod m_i$ でもあるから $X \equiv Y \mod m_i$ が成り立つ．すなわち各 i について $m_i | (X - Y)$，つまり $M | (X - Y)$ である．故に $X \equiv Y \mod M$ である． □

この証明は連立一次合同式の解き方まで示唆している．

連立一次合同式の解き方

連立一次合同式 $x \equiv a_i \mod m_i \quad (i = 1, 2, \ldots, k)$ は次の手順で解く．

(1) $M = m_1 m_2 \ldots m_k$ とおき，各 i について $M_i = M/m_i$ とおく．
(2) 各 i について一次合同式 $M_i t_i \equiv 1 \mod m_i$ を解く．
(3) 求める解は M を法として唯一つで，$x = \sum_{i=1}^{k} M_i t_i a_i$ である．

例 6.23. 連立一次合同式[6]

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$$

を解く．

$M = 3 \times 5 \times 7 = 105$，$M_1 = M/3 = 35$，$M_2 = M/5 = 21$，$M_3 = M/7 = 15$ とし，3 つの一次合同式

$$35t_1 \equiv 1 \mod 3 \ldots (1)$$
$$21t_2 \equiv 1 \mod 5 \ldots (2)$$
$$15t_3 \equiv 1 \mod 7 \ldots (3)$$

を解く．$35 \equiv -1 \mod 3$ なので (1) は $-t_1 \equiv 1 \mod 3$，すなわち $t_1 \equiv -1 \mod 3$ となる．また $21 \equiv 1 \mod 5$ なので (2) は $t_2 \equiv 1 \mod 5$ である．(3) も同様に $t_3 \equiv 1 \mod 5$ である．以上より $X = 35 \times (-1) \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 = -70 + 63 + 30 = 23$ が 105 を法としたときの解である．つまり求める解は $x \equiv 23 \mod 105$ である．

問題 6.24. 連立一次合同式：$x \equiv 1 \bmod 5$，$x \equiv 2 \bmod 7$ の解を求めよ．

[6]余談だが，実はこの問題は連立一次合同式の問題で一番有名と言える．定理 6.22 の名前の由来である『孫子算経』という古い書物に「3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 2 余る数は何か？」という問題がある（らしい）．これを定式化すれば上の連立一次合同式そのものである．
なお，兵法書の『孫子』の孫子さんとは別人のようである．

7. 同値関係と剰余集合

この節では少し話が変わって，今までよりも抽象的である．初等整数論の話の一つ，というよりは「数学全体における基本的な概念で，それを初等整数論の場合を例にして扱う」という感じである．次節以降への準備である．

定義 7.1. 集合 S の元 x, y に対して $x \sim y$ または $x \not\sim y$ のいずれか一方が成り立つ（二項）関係[7]$\sim$ が

- $x \sim x$ （反射律）
- $x \sim y$ ならば $y \sim x$ （対称律）
- $x \sim y$ かつ $y \sim z$ ならば $x \sim z$ （推移律）

をみたすとき**同値関係**という．

例 7.2. $\mathbb{Z}$ 上の関係 $\sim$ を次のように定める．

(1) $x \sim y \Leftrightarrow |x - y| \leq 2$ とすると，この関係は同値関係ではない．実際 $|1-3| = 2 \leq 2$ かつ $|3-5| = 2 \leq 2$ なので $1 \sim 3$ かつ $3 \sim 5$ であるが $|1-5| = 4 > 2$ なので $1 \not\sim 5$ である．つまり推移律が成り立たない．

(2) $x \sim y \Leftrightarrow x = y$ とすると，この関係は同値関係である．つまり $x = x$ が成り立ち， $x = y$ ならば $y = x$ も成り立ち，$x = y$ かつ $y = z$ ならば $x = z$ も成り立つ．従ってこの $\mathbb{Z}$ 上の関係 $\sim$ は同値関係である．

例 7.3. $\mathbb{C}^2 \setminus \{(0,0)\}$ 上の関係を次で定める：$(a_0, a_1) = c(b_0, b_1)$ となる $c \in \mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ が存在するとき[8]$(a_0, a_1) \sim (b_0, b_1)$ と記す．このとき関係 $\sim$ は同値関係である事を示す．

（反射律）：$c = 1$ とすれば，$(a_0, a_1) = c(a_0, a_1)$ であり，$c \in \mathbb{C}^\times$ であるから $(a_0, a_1) \sim (a_0, a_1)$ が成り立つ．

---

[7] x と y を定めれば真偽が確定する命題と思っても良い．

[8] 平たく言えば，比 $a_0 : a_1$ と $b_0 : b_1$ が等しいとき．

（対称律）: $(a_0, a_1) \sim (b_0, b_1)$ とすると，$(a_0, a_1) = c(b_0, b_1)$ となる $c \in \mathbb{C}^\times$ が存在するが，このとき $(b_0, b_1) = \frac{1}{c}(a_0, a_1)$ が成り立つ．$1/c \in \mathbb{C}^\times$ なので $(b_0, b_1) \sim (a_0, a_1)$ である．

（推移律）: $(a_0, a_1) \sim (b_0, b_1)$，$(b_0, b_1) \sim (d_0, d_1)$ とする．つまり $(a_0, a_1) = c(b_0, b_1)$ となる $c \in \mathbb{C}^\times$ と $(b_0, b_1) = c'(d_0, d_1)$ となる $c' \in \mathbb{C}^\times$ が存在したとする．このとき $(a_0, a_1) = cc'(d_0, d_1)$ であり，$cc' \in \mathbb{C}^\times$ なので $(a_0, a_1) \sim (d_0, d_1)$ が成り立つ．

補題 6.4 により，次が成り立つ．

命題 7.4. $\mathbb{Z}$ 上の合同 $\equiv$ は同値関係である．

定義 7.5 (同値類)**.** S を集合とし，$\sim$ を S 上の同値関係とする．$a \in S$ に対し $[a] := \{x \in S | x \sim a\}$ を $\sim$ による a の**同値類**という．また a を $[a]$ の**代表元**という．

注意 7.6. $[a]$ 以外に $C(a)$ や $\bar{a}$ という記号が用いられることも多い．個人的には $\bar{a}$ をよく使うのだが，TEX の事情でここでは $[a]$ を使う事にする．

例 7.7. $\mathbb{Z}$ 上の関係として「3 を法とした合同」を考える．つまり $x \sim y$ を $x \equiv y \mod 3$ とする．このとき同値類は 1 の同値類，2 の同値類，0 の同値類の 3 つである．具体的には

$$\begin{aligned}[1] &= \{x \in \mathbb{Z} | x \sim 1\} \\ &= \{x \in \mathbb{Z} | x \equiv 1 \mod 3\} \\ &= \{x \in \mathbb{Z} | x \text{ は } 3 \text{ で割って } 1 \text{ 余る }\}\end{aligned}$$

と

$$\begin{aligned}[2] &= \{x \in \mathbb{Z} | x \sim 2\} \\ &= \{x \in \mathbb{Z} | x \equiv 2 \mod 3\} \\ &= \{x \in \mathbb{Z} | x \text{ は } 3 \text{ で割って } 2 \text{ 余る }\}\end{aligned}$$

と

$$\begin{aligned}[0] &= \{x \in \mathbb{Z} | x \sim 0\} \\ &= \{x \in \mathbb{Z} | x \equiv 0 \mod 3\} \\ &= \{x \in \mathbb{Z} | x \text{ は } 3 \text{ で割って } 0 \text{ 余る }\}\end{aligned}$$

である．

また $3 \equiv 0 \mod 3$ なので $[0] = [3] = \cdots = [3k]$ である．同様に $[1] = [4] = \cdots = [3k+1]$ や $[2] = [-1] = [5] = \cdots = [3k+2]$ である．これは整数を 3 で割ったときの余りで「類別」している．実際，整数を 3 で割ったときの余りは 0 か 1 か 2 である．(しかし商を調整してやって「余りは 3 か -2 か 5 である」と言っても間違ってはいない.)

今の場合，$[1] \neq [2]$ や $[1] \cap [2] = \emptyset$ などは直ぐに確認できる．実際には次が成り立つ．

命題 7.8. S を集合，$\sim$ を S 上の同値関係とする．このとき $a, b \in S$ に対し，同値類 $[a], [b]$ は $[a] \cap [b] = \emptyset$ または $[a] = [b]$ のいずれか一方が成り立つ．

Proof. $[a] \cap [b] \neq \emptyset$ とする．$x \in [a] \cap [b]$ とすれば $x \sim a$ かつ $x \sim b$ をみたす．$\sim$ は同値関係であるから対称律と推移律を用いれば $a \sim b$ である．すなわち $[a] = [b]$. □

系 7.9. S を集合，$\sim$ を S 上の同値関係とする．このとき S は同値類の直和[9] $S = \coprod_{x \in S} [x]$ として表せる．

例 7.10. $\mathbb{Z}$ 上の同値関係として $x \sim y$ を $x - y \in 3\mathbb{Z}$ と定める．このとき

$$\mathbb{Z} = [0] \coprod [1] \coprod [2]$$

[9]集合 A と B が $A \cap B = \emptyset$ をみたすとき，$A \cup B$ を A と B の**直和**といい，$A \coprod B$ で表す.

が成り立つ．これは整数を 3 で割った時の余りは 0 か 1 か 2 のみであり，3 で割った時の余りを 2 種類以上もつような整数は存在しない事を意味する．

定義 7.11. S を集合，$\sim$ を S 上の同値関係とする．このとき S の $\sim$ による同値類全体を $S/\sim$ と記す．つまり $S/\sim := \{[x] | x \in S\}$ であり，これを $\sim$ による S の**商集合**という．

注意 7.12. $\mathbb{Z}$ 上の同値関係 $x \sim y$ として $x - y \in m\mathbb{Z}$ を考えるとき，$\mathbb{Z}/\sim$ を $\mathbb{Z}/m\mathbb{Z}$ と記す．例えば $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ である．また，$a \in \mathbb{Z}$ の同値類 $[a] \in \mathbb{Z}/m\mathbb{Z}$ を特に，m を法とした a の**剰余類**と言う（ことが多い）．

定義 7.13. S を集合，$\sim$ を S 上の同値関係とするとき，$x \in S$ を $[x]$ へ移す写像 $p : S \to S/\sim\ (x \mapsto [x])$ を**自然な写像**と言う．また K を S の部分集合とするとき，自然な写像を K に制限した写像 $p_{|K} : K \to S/\sim$ が全単射のとき，K を $S/\sim$ の**完全代表系**という．

各剰余類から一つずつ代表元を取ってきて作った集合が完全代表系ということである．

例 7.14. 集合 $\{0, 1, 2\}$，$\{0, 1, -1\}$，$\{111, 10, 5\}$ はどれも $\mathbb{Z}/3\mathbb{Z}$ の完全代表系である．このように，法を一つ定めても完全代表系は唯一には定まらない．

次に $\mathbb{Z}/m\mathbb{Z}$ に「演算」を定義できる[10]ことを見る．整数 a, b に対し，

$$[a] + [b] := [a + b], \quad [a][b] := [ab]$$

によって $\mathbb{Z}/m\mathbb{Z}$ 上の和と積を定める．左辺が $\mathbb{Z}/m\mathbb{Z}$ の演算である．その演算は右辺で定義される，ということである．つまり $\mathbb{Z}$ の演算で $a + b$（または ab）を計算して，それが定める同値類をとれ，ということである．

[10] $\mathbb{Z}/m\mathbb{Z}$ に環の構造を入れる．

この $\mathbb{Z}/m\mathbb{Z}$ の演算は $\mathbb{Z}$ の演算から自然に定めているので問題ないように思うかもしれないが，これは我々が「勝手に定めている」わけである．すなわち，この演算の定義に何か不具合があるとも限らない．それはチェックする必要がある．

命題 7.15. 上で定めた演算は代表元の取り方に依存しない．つまり矛盾なく定義されている（well-defined である）．

Proof. $[a] = [a'], [b] = [b']$ のとき，$[a+b] = [a'+b'], [ab] = [a'b']$ を示す．

（和に関して）$[a] = [a'], [b] = [b']$ ならば $a - a' \in m\mathbb{Z}$ かつ $b - b' \in m\mathbb{Z}$ であり，$(a - a') + (b - b') \in m\mathbb{Z}$ が成り立つ．$(a - a') + (b - b') = (a + b) - (a' + b')$ なので $[a + b] = [a' + b']$ である．

（積に関して）$[a] = [a'], [b] = [b']$ ならば $a - a' \in m\mathbb{Z}$ かつ $b - b' \in m\mathbb{Z}$ であり，$(a - a')b \in m\mathbb{Z}$ かつ $a'(b - b') \in m\mathbb{Z}$ が成り立つ．つまり $(a - a')b + a'(b - b') \in m\mathbb{Z}$ である．$(a - a')b + a'(b - b') = ab - a'b'$ なので $[ab] = [a'b']$ である． □

例 7.16. $\mathbb{Z}/5\mathbb{Z}$ 上の加法を考える．$[1] + [3] = [1 + 3] = [4]$ であるが，これは「5 で割って余りが 1 の整数と 5 で割って余りが 3 の整数を足した時，その数を 5 で割れば余りは 4 である」という意味である．たとえば 6 は 5 で割って余りが 1 の数，8 は 5 で割って余りが 3 の数である．それらの和は 14 で 5 で割れば余りは 4 である．しかしこの結果は 6 と 8 と 14 という代表元限定の話である．上の命題は代表元の取り方に依存しないと言っている．

例 7.17. $\mathbb{Z}/5\mathbb{Z}$ 上の加法に対して，$[3] + [3] = [3 + 3] = [6] = [1]$ が成り立つ．また $\mathbb{Z}/4\mathbb{Z}$ 上の乗法に対して，$[2][2] = [2 \times 2] = [4] = [0]$ である．もちろん $[2] \neq [0]$ である．整数の演算と違って，零でない元を掛けても答えが零になることがある．

8. 既約剰余類と Euler 関数

8.1. 既約剰余類.

定義 8.1. a を整数，m を自然数とする．$(a,m)=1$ のとき a の m を法とした同値類 $[a]\in\mathbb{Z}/m\mathbb{Z}$ を**既約剰余類**という．また既約剰余類の集合を $(\mathbb{Z}/m\mathbb{Z})^\times$ で表す．つまり

$$(\mathbb{Z}/m\mathbb{Z})^\times=\{[a]\in\mathbb{Z}/m\mathbb{Z}|(a,m)=1\}$$

である．

例 8.2. $(\mathbb{Z}/5\mathbb{Z})^\times$ を調べる．$(\mathbb{Z}/5\mathbb{Z})^\times=\{[a]\in\mathbb{Z}/m\mathbb{Z}|(a,5)=1\}$ であるが，$(a,5)=1$ すなわち 5 と互いに素な数は $1,2,3,4$ である．従って $(\mathbb{Z}/5\mathbb{Z})^\times=\{[1],[2],[3],[4]\}$ である．

同様に $(a,6)=1$ をみたす整数を調べることによって $(\mathbb{Z}/6\mathbb{Z})^\times=\{[1],[5]\}$ を得る．

定義 8.3. Λ を $\mathbb{Z}$ の部分集合とする．自然な写像 $p:\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ に対し，制限写像 $p_{|\Lambda}:\Lambda\to(\mathbb{Z}/m\mathbb{Z})^\times$ が全単射のとき，Λ を $(\mathbb{Z}/m\mathbb{Z})^\times$ の**既約剰余系**という．すなわち，各既約剰余類の中から一つずつ代表元を取ってきて作った集合が既約剰余系である．

例 8.4. $(\mathbb{Z}/6\mathbb{Z})^\times=\{[1],[5]\}$ であるが，$\{1,5\}$ も $\{1,-1\}$ も $\{37,605\}$ も既約剰余系である．完全代表系と同様で，法を一つ定めても既約剰余系は唯一には定まらない．

補題 8.5. a,b を整数，m を自然数とする．$[a],[b]\in\mathbb{Z}/m\mathbb{Z}$ に対し，$[a]=[b]$ が成り立つならば $(a,m)=(b,m)$ も成り立つ．

Proof. 定理 2.4（除法の定理）より，$a=mq_1+r_1$ と $b=mq_2+r_2$ とできる．ここで $0\le r_1,r_2<m$ なので $|r_1-r_2|<m$ に注意する．$[a]=[b]$ より $a-b\in m\mathbb{Z}$ なので

$$r_1-r_2=(a-b)-m(q_1-q_2)\in m\mathbb{Z}$$

が成り立つ．これは $|r_1-r_2|\ge m$ または $r_1-r_2=0$ を意味する．従って $r_1=r_2$ である．これと系 3.12 より，$(a,m)=(r_1,m)=(r_2,m)=(b,m)$ を得る． □

既約剰余類の立場から捉えると，この補題は $(a,m)=1$ をみたす $[a]$ を定めると，$[a]$ に含まれる全ての元は m と互いに素である，と主張している．つまり $[a]$ が既約剰余類であるということは代表元の取り方に依存しない．

次に $(\mathbb{Z}/m\mathbb{Z})^\times$ の元の個数を調べる．それは実質，Euler 関数を調べることで分かる．そのために次の補題を示しておく．

補題 8.6. m と n を互いに素な自然数とする．このとき全単射

$$\Phi : (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/mn\mathbb{Z})^\times$$

が存在する．

Proof. まずは全単射 $\Phi' : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/mn\mathbb{Z}$ （とその逆写像）を構成する．その後でこの写像を $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ に制限し，それが全単射である事を示す．

最初に写像 $\Phi' : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/mn\mathbb{Z}$ を構成する．$[a] \in \mathbb{Z}/m\mathbb{Z}$ と $[b] \in \mathbb{Z}/n\mathbb{Z}$ に対し，定理 6.22（中国式剰余定理）を用いれば，連立一次合同式

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

をみたす x は mn を法として唯一に定まる．従って写像 Φ' が $\Phi'([a],[b]) = [x]$ として定まる．

次に逆向きの写像 $\Psi' : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ を構成する．$[x] \in \mathbb{Z}/mn\mathbb{Z}$ に対し，定理 2.4（除法の定理）より $x = mq_1 + r_1$ $(0 \le r_1 < m)$ と $x = nq_2 + r_2$ $(0 \le r_2 < n)$ をみたす整数 r_1, r_2 （と q_1, q_2）が唯一つ存在する．従って写像 Ψ' が $\Psi'([x]) = ([r_1],[r_2])$ として定まる．また，Φ' と Ψ' の構成法から $\Phi' \circ \Psi' = id_{\mathbb{Z}/mn\mathbb{Z}}$ と $\Psi' \circ \Phi' = id_{(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})}$ は明らかである．つまり Φ' と Ψ' は全単射である．

さて，本題である写像 Φ を調べる．Φ' を $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ へ制限した写像を Φ とする．今の段階では

$$\Phi = \Phi'_{|(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times} : (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{Z}/mn\mathbb{Z}$$

に過ぎないことに注意する．$([a],[b]) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ とすると $\Phi([a],[b]) = \Phi'([a],[b]) = [x]$ であるが，$[a]$ と $[b]$ は既約剰余類なので $(a,m) = (b,n) = 1$ である．また補題 8.5 を用いれば，$x \equiv a \mod m$ なので $(x,m) = 1$ を得る．同様に $x \equiv b \mod m$ なので $(x,n) = 1$ である．従って命題 4.7 より $(x,mn) = 1$，つまり $[x] \in (\mathbb{Z}/mn\mathbb{Z})^\times$ が成り立つ．以上により写像

$$\Phi : (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/mn\mathbb{Z})^\times, \quad ([a],[b]) \mapsto [x])$$

が定まる．

同様に Ψ' を $(\mathbb{Z}/mn\mathbb{Z})^\times$ へ制限した写像 Ψ を考える．$[x] \in (\mathbb{Z}/mn\mathbb{Z})^\times$ に対し，再び定理 2.4 より $x = mq_1 + r_1$ $(0 \leq r_1 < m)$ と $x = mq_2 + r_2$ $(0 \leq r_2 < n)$ をみたす整数 r_1, r_2 が唯一つ存在する．今 $(x,mn) = 1$ であるが，命題 4.7 より $(x,m) = 1$ かつ $(x,n) = 1$ なので $r_1, r_2 \neq 0$ である．さらに系 3.12 より $(r_1,m) = 1$ かつ $(r_2,n) = 1$ である．以上により

$$\Psi : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times, \quad ([x] \mapsto ([r_1],[r_2]))$$

が定まる．

また Φ と Ψ が全単射であることは Φ' と Ψ' が全単射であることから従う． □

これより次が従う．

命題 8.7. 集合 $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ と集合 $(\mathbb{Z}/mn\mathbb{Z})^\times$ は対等である．すなわち

$$\sharp\left((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times\right) = \sharp(\mathbb{Z}/mn\mathbb{Z})^\times$$

である．

8.2. **Euler 関数.**

定義 8.8. n を自然数とし，集合 $\{1,2,\ldots,n\}$ のなかで n と互いに素となる数の個数を $\varphi(n)$ と表す．特にこの φ を **Euler 関数**という．

$\varphi(n)$ の値は $\{1/n, 2/n, \ldots, n/n\}$ のうち，約分できない分数の個数とも言える．

具体的に幾つかの例を見る．

例 8.9. φ を Euler 関数とする．

(1) $\varphi(5) = \sharp\{x \in \{1,2,3,4,5\} | (x,5) = 1\} = \sharp\{1,2,3,4\} = 4$
(2) $\varphi(6) = \sharp\{x \in \{1,2,3,4,5,6\} | (x,6) = 1\} = \sharp\{1,5\} = 2$
(3) $\varphi(8) = \sharp\{x \in \{1,2,3,4,5,6,7,8\} | (x,8) = 1\} = \sharp\{1,3,5,7\} = 4$

(3) で別の計算をしてみる．8 個の数字のうち $(x,8) = 1$ とならない整数 x の個数を計算して，全体 $8 = 2^3$ から引けば良い．$(x,8) = 1$ とならない整数 x は 2 の倍数であり，それは $2,4,6,8$ の $4 = 2^2$ 個である．従って $\varphi(8) = 2^3 - 2^2 = 4$ である．

このように p を素数としたとき $\varphi(p^k)$ の値を求めるためには 1 から p^k までのうち，p の倍数の個数を調べることが有力である．

補題 8.10. m, n を自然数とする．1 から n までのうち，m の倍数の個数は n を m で割った時の商に等しい．

Proof. 定理 2.4 を用いて $n = mq + r$ $(0 \leq r < m)$ と表したとき，1 から n までのうち m の倍数は $1m, 2m, \ldots, qm$ である． □

$n = p^k, m = p$ とすることで次を得る．

系 8.11. 1 から p^k のうち，p の倍数は p^{k-1} 個存在する．

命題 8.12. φ を Euler 関数，p を素数，k を自然数とする．このとき $\varphi(p) = p - 1$ 及び $\varphi(p^k) = p^k - p^{k-1}$ が成り立つ．

Proof. p は素数なので，$\{1,2,\ldots,p\}$ のなかで p と互いに素とならない数は p だけである．また $\{1,2,\ldots,p^k\}$ のなかで p^k と互いに素でない数は p の倍数であり，系 8.11 よりその数は p^{k-1} である． □

定義から察することができるが，Euler 関数と既約剰余類の集合には次の関係がある．

補題 8.13. φ を Euler 関数，m を自然数とする．このとき $\varphi(m) = \sharp(\mathbb{Z}/m\mathbb{Z})^\times$ が成り立つ．

Proof. $[0] = [m]$ なので $\mathbb{Z}/m\mathbb{Z} = \{[1], [2], \ldots, [m]\}$ である．これに含まれる既約剰余類の個数は $\{1, 2, \ldots, m\}$ のうち m と互いに素な数の個数である． □

素数と素数のべきの場合は Euler 関数の値は計算できた．それ以外の場合は次の命題が本質的である．

命題 8.14. m と n を互いに素な自然数とする．このとき $\varphi(mn) = \varphi(m)\varphi(n)$ が成り立つ．

Proof. 命題 8.7 と補題 8.13 から従う． □

例 8.15. 素数同士は互いに素なので，素因数分解を用いれば次のように計算できる．

(1) $\varphi(6) = \varphi(2 \times 3) = \varphi(2)\varphi(3) = (2-1)(3-1) = 2$.
(2) $\varphi(60) = \varphi(2^2 \times 3 \times 5)$ だが 2^2 と 3×5 は互いに素なので $\varphi(2^2 \times 3 \times 5) = \varphi(2^2)\varphi(3 \times 5)$ である．もう一度上の命題を用いれば $\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5) = (2^2-2)(3-1)(5-1) = 16$ である．

Euler 関数の値を計算するだけならば命題 8.14 で十分であろうが，一般には次の形で表すことができる．

定理 8.16. n を自然数とし，n の素因数分解を $n = \prod_{k=1}^{m} p_k^{\alpha_k}$ (ただし $i \neq j$ であれば $p_i \neq p_j$) とする．このとき

$$\varphi(n) = n \prod_{k=1}^{m} \left(1 - \frac{1}{p_k}\right)$$

である．

Proof. 命題 8.14 より，

$$\varphi(n) = \varphi\left(\prod_{k=1}^{m} p_k^{\alpha_k}\right) = \prod_{k=1}^{m} \varphi(p_k^{\alpha_k})$$

に注意する．命題 8.12 を用いれば,

$$\begin{aligned}\varphi(n) &= \prod_{k=1}^{m}(p_k^{\alpha_k} - p_k^{\alpha_{k-1}}) \\ &= \prod_{k=1}^{m}\left(p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)\right) \\ &= \prod_{k=1}^{m} p_k^{\alpha_k} \times \prod_{k=1}^{m}\left(1-\frac{1}{p_k}\right) \\ &= n\prod_{k=1}^{m}\left(1-\frac{1}{p_k}\right)\end{aligned}$$

である． □

例 8.17. $\varphi(n) = 10$ をみたす自然数 n を全て求める．

$n = \prod_{k=1}^{m} p_k^{\alpha_k}$ と素因数分解する．

$$\varphi(n) = \prod_{k=1}^{m} p_k^{\alpha_k - 1}(p_k - 1) = \prod_{k=1}^{m} p_k^{\alpha_k - 1}\varphi(p_k)$$

なので，$\varphi(n)$ は $\varphi(p_k)$ で割り切れる[11]．従って n の素因数の候補は $2, 3, 11$ である．また $\varphi(3\times 11) = \varphi(3)\times\varphi(11) = 2\times 10 = 20$ なので，3 と 11 は同時に n の素因数に表れない．つまり n は $2^a, 3^b, 11^c, 2^a3^b, 2^a11^c$（$a, b, c$ は自然数）のうちいずれかの形をしている．

もし $n = 2^a$ であれば，$\varphi(n) = n(1-1/2) = 2^{a-1} \neq 10$ なので $n = 2^a$ にはなり得ない．$n = 3^b$ であれば，$\varphi(n) = n(1-1/3) = 2\times 3^{b-1} \neq 10$ なので $n = 3^b$ にもなり得ない．$n = 11^c$ ならば $\varphi(n) = n(1-1/11) = 10\times 11^{c-1}$ なので $c = 1$ のときに $\varphi(n) = 10$ である．$n = 2^a3^b$ であれば，$\varphi(n) = n(1-1/2)(1-1/3) = 2^a\times 3^{b-1} \neq 10$ なので $n = 2^a3^b$ にはなり得ない．$n = 2^a11^c$ ならば $\varphi(n) = n(1-1/2)(1-1/11) = 10\times 2^{a-1}\times 11^{c-1}$ なので $a = c = 1$ のときに $\varphi(n) = 10$ である．以上により $\varphi(n) = 10$ をみたす自然数は 11 と 22 のみである．

命題 8.18. φ を Euler 関数とする．このとき次が成り立つ．

[11] もし $p_k = 7$ ならば $\varphi(n) = 10$ は $\varphi(7) = 6$ で割り切れることになる．

(1) n が 3 以上の自然数であれば $\varphi(n)$ は偶数である．

(2) 任意の自然数 n に対し，$\varphi(n) \neq 14$ である．

Proof. (1) $n = \prod_{k=1}^{m} p_k^{\alpha_k}$ と素因数分解する．$\varphi(n) = \prod_{k=1}^{m} p_k^{\alpha_k - 1}(p_k - 1)$ であるが，p_k が 3 以上の素数ならば $(p_k - 1)$ は偶数である．もし p_k に 3 以上の素数が含まれないならば，$n = 2^\alpha$ なので $\varphi(n) = 2^{\alpha-1}$ である．従って $\varphi(n)$ は偶数である．

(2) $\varphi(n) = 14 = 2 \times 7$ とする．例 8.17 と同様に $\varphi(n)$ は n の素因数の Euler 関数の値 $\varphi(p_k)$ で割り切れなくてはならないので，n の素因数の候補は 2 と 3 である．($\varphi(p) = p - 1 = 7$ となる素数 p は存在しない.) つまり $n = 2^a 3^b, 2^a, 3^b$ である．

$n = 2^a 3^b$ ならば $\varphi(n) = n(1 - 1/2)(1 - 1/3) = 2^a \times 3^{b-1} \neq 14$ であり，$n = 2^a$ ならば $\varphi(n) = n(1 - 1/2) = 2^{a-1} \neq 14$ であり，$n = 3^b$ ならば $\varphi(n) = n(1 - 1/3) = 2 \times 3^{b-1} \neq 14$ である．つまりいずれの場合も $\varphi(n) \neq 14$ である． □

以上のことより，原理的には次の表を得ることができる．

注意 8.19. $\varphi(n) \leq 21$ をみたす自然数 n は次の表にあるものだけである．

$\varphi(n)$	20	18	16	12	10	8	6	4	2	1
	66	54	60	42	22	30	18	12	6	2
	50	38	48	36	11	24	14	10	4	1
n	44	27	40	28		20	9	8	3	
	33	19	34	26		16	7	5		
	25		32	21		15				
			17	13						

命題 8.20. n を自然数，φ を Euler 関数とする．このとき

$$\sum_{d|n} \varphi(d) = n$$

が成り立つ．

Proof. $n=\prod_{k=1}^{m}p_k^{\alpha_k}$ と素因数分解すると $d|n$ をみたす d は $d=\prod_{k=1}^{m}p_k^{\beta_k}$ と表せる．ただし $0\leq\beta_k\leq\alpha_k$ である．命題 8.12 により，素数 p に対し，

$$\begin{aligned}\varphi(p^0)+\varphi(p^1)+\varphi(p^2)+\cdots+\varphi(p^\gamma)&=1+(p-1)+(p^2-p)+\cdots+(p^\gamma-p^{\gamma-1})\\&=p^\gamma\end{aligned}$$

が成り立つ事に注意する．これと命題 8.14 より，

$$\begin{aligned}\sum_{d|n}\varphi(d)&=\sum_{0\leq\beta_k\leq\alpha_k}\varphi\left(\prod_{k=1}^{m}p_k^{\beta_k}\right)\\&=\sum_{0\leq\beta_k\leq\alpha_k}\left(\prod_{k=1}^{m}\varphi\left(p_k^{\beta_k}\right)\right)\\&=\prod_{k=1}^{m}\left(\sum_{0\leq\beta_k\leq\alpha_k}\varphi\left(p_k^{\beta_k}\right)\right)\\&=\prod_{k=1}^{m}\left(\varphi(p_k^0)+\varphi(p_k^1)+\cdots+\varphi(p_k^{\alpha_k})\right)\\&=\left(\varphi(p_1^0)+\varphi(p_1^1)+\cdots+\varphi(p_1^{\alpha_1})\right)\ldots\left(\varphi(p_m^0)+\varphi(p_m^1)+\cdots+\varphi(p_m^{\alpha_m})\right)\\&=p_1^{\alpha_1}\ldots p_m^{\alpha_m}\\&=n\end{aligned}$$

を得る． □

注意 8.21. 3 つ目の等号に関しては微積分の授業で色々言われたと思うが，ここでは有限和と有限積の交換である．

例 8.22. 18 の約数は $1,2,3,6,9,18$ であるので，

$$\begin{aligned}\sum_{d|18}\varphi(d)&=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)+\varphi(9)+\varphi(18)\\&=1+1+2+2+6+6\\&=18\end{aligned}$$

である．

問題 8.23. 上の例で $(k,18)=d$ をみたす k を各 $d=1,2,3,6,9,18$ 毎にリストアップせよ．

9. Fermat の小定理と Euler の定理

補題 9.1. p を素数，r を $0 < r < p$ をみたす整数とする．このとき

$$\binom{p}{r} := \frac{p!}{r!(p-r)!} \equiv 0 \mod p$$

が成り立つ．

Proof. 分子は p で割り切れるので，分母が p で割り切れない事を見れば良い．$r!(p-r)!$ が p で割り切れたとすると，この積のいずれかの項は p で割り切れる．しかしそれは $0 < r < p$ に反する． □

注意 9.2. 定義から明らかだが $\binom{p}{r}$ は二項係数である．中学か高校のときにやった「組合せ」の ${}_p\mathrm{C}_r$ と同じ意味である．大学に入学する前まではC を使う方が多数派だと思うが，$\binom{p}{r}$ の方が一般的である．

例 9.3. $p = 7, r = 3$ とする．

$$\begin{aligned}\binom{7}{3} &= \frac{7!}{3!(7-3)!} \\ &= \frac{7\times6\times5\times4\times3\times2\times1}{3\times2\times1\times4\times3\times2\times1} \\ &= 7\times5 \\ &\equiv 0 \mod 7\end{aligned}$$

命題 9.4. p を素数，a, b を整数とする．このとき $(a+b)^p \equiv a^p + b^p \mod p$ が成り立つ．

Proof. 二項定理：$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k$ を用いる．補題 9.1 より

$$(a+b)^p \equiv \binom{p}{0}a^p + \binom{p}{p}b^p \mod p$$

なので $(a+b)^p \equiv a^p + b^p \mod p$ が成り立つ． □

定理 9.5 (Fermat の小定理)**.** p を素数，a を整数とする．このとき次が成り立つ．

(1) $a^p \equiv a \mod p$
(2) $(a, p) = 1$ ならば $a^{p-1} \equiv 1 \mod p$

Proof. (1) が成り立てば命題 6.15 より (2) が従うので (1) を示す.

$a > 0$ とする．a に関する帰納法を用いる．$a = 1$ ならば $1^p = 1$ なので $a^p \equiv a \mod p$ である．$a = k$ のとき $k^p \equiv k \mod p$ が成り立つとする．命題 9.4 と帰納法の仮定より

$$\begin{aligned}(k+1)^p &\equiv k^p + 1^p \mod p \\ &\equiv k+1 \mod p\end{aligned}$$

が成り立つので $a^p \equiv a \mod p$ が示される.

また $a < 0$ のとき $-a > 0$ であるから $(-1)^p a^p = (-a)^p \equiv -a \mod p \ldots (*)$ が成り立つ．$p = 2$ ならば $-1 \equiv 1 \mod 2$ より $(-1)^p a^p \equiv a^p, -a \equiv a \mod 2$ である．また $p \neq 2$ ならば $(-1)^p \equiv -1 \mod p$ なので，$(*)$ の両辺を -1 倍すれば良い．いずれにせよ $a^p \equiv a \mod p$ が成り立つ.

$a = 0$ のときは明らかである． □

例 9.6. 10^{100} を 17 で割ったときの余りを求める.

$p = 17$ として定理 9.5 を用いると $(10, 17) = 1$ なので $10^{16} \equiv 1 \mod 17$ である．また $100 = 6 \times 16 + 4$ なので $10^{100} = (10^{16})^6 \times 10^4 \equiv 1 \times 10^4 \mod 17$．さらに $102 = 6 \times 17$ なので $100 = 10^2 \equiv -2 \mod 17$ である．故に $10^4 = (10^2)^2 \equiv (-2)^2 = 4 \mod 17$，すなわち 10^{100} を 17 で割ったときの余りは 4 である.

Fermat の小定理の一般化が次の Euler の定理である.

注意 9.7. Fermat と Euler の活躍した時代はちょうど 100 年くらいずれている．Fermat が生まれた頃は「関ヶ原の戦い」と「大坂冬の陣」の間くらいである．一方の Euler が生まれた頃には「生類憐れみの令」でお馴染みの五代将軍徳川綱吉がまだ生きている．囲碁で言えば五世本因坊道知の時代である．味わい深い歴史である.

定理 9.8 (Euler の定理). φ を Euler 関数，m を自然数，a を m と互いに素な整数とする．このとき $a^{\varphi(m)} \equiv 1 \mod m$ が成り立つ.

注意 9.9. m が素数であれば $\varphi(m) = m - 1$ なので Fermat の小定理そのものである.

Proof. $\sharp(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$ なので $(\mathbb{Z}/m\mathbb{Z})^\times = \{[x_1], [x_2], \ldots, [x_{\varphi(m)}]\}$ とする. このとき $(a, m) = 1$ かつ $(x_i, m) = 1$ なので, 命題 4.7 より $(ax_i, m) = 1$ である. また命題 6.15 より $[ax_i] = [ax_j]$ であることの必要十分条件は $[x_i] = [x_j]$ であることが分かる. すなわち $[ax_i]$ も既約剰余類である. つまり $\{[x_1], [x_2], \ldots, [x_{\varphi(m)}]\}$ と $\{[ax_1], [ax_2], \ldots, [ax_{\varphi(m)}]\}$ は元の並んでいる順番が異なるだけであって, それらを全てを掛けると等しい:

$$\begin{aligned}[x_1 x_2 \ldots x_{\varphi(m)}] &= [x_1][x_2] \ldots [x_{\varphi(m)}] \\ &= [ax_1][ax_2] \ldots [ax_{\varphi(m)}] \\ &= [a^{\varphi(m)} x_1 x_2 \ldots x_{\varphi(m)}]\end{aligned}$$

従って $a^{\varphi(m)} x_1 x_2 \ldots x_{\varphi(m)} \equiv x_1 x_2 \ldots x_{\varphi(m)} \mod m$ である. 各 i に対して $(x_i, m) = 1$ なので $\varphi(m)$ 回 命題 6.15 (1) を用いると $a^{\varphi(m)} \equiv 1 \mod m$ が成り立つ. □

例 9.10. 7^{500} を 44 で割った時の余りを求める.

$(7, 44) = 1$ であり, $\varphi(44) = \varphi(2^2)\varphi(11) = (2^2 - 2) \times 10 = 20$ である. 定理 9.8 より $7^{20} \equiv 1 \mod 44$ なので, $7^{500} = 7^{20 \times 25} = (7^{20})^{25} \equiv 1^{25} \mod 44$ である. 従って 7^{500} を 44 で割った時の余りは 1 である.

系 9.11 (一次合同式の解の公式)**.** m を自然数, a, b を整数とする. $(a, m) = 1$ のとき一次合同式 $ax \equiv b \mod m$ は m を法として唯一つの解を持ち, それは $x \equiv a^{\varphi(m)-1} b \mod m$ である.

Proof. 命題 6.17 (3) より m を法として解は唯一つ存在する．$ax \equiv b \mod m$ の左辺に $x = a^{\varphi(m)-1}b$ を代入すると，定理 9.8 より

$$\begin{aligned} ax &\equiv a(a^{\varphi(m)-1}b) \mod m \\ &\equiv a^{\varphi(m)}b \mod m \\ &\equiv 1 \times b \mod m \end{aligned}$$

である．すなわち $x \equiv a^{\varphi(m)-1}b$ が唯一つの解である． □

例 9.12. 一次合同式 $15x \equiv 1 \mod 22$ を解く．$(15, 22) = 1$ なので，系 9.11 より $x \equiv 15^{\varphi(22)-1} \times 1 \mod 22$ が解である．$\varphi(22) = 10$ と $15^9 = (15^2)^4 \times 15$ より，

$$\begin{aligned} x &\equiv ((-7)^2)^4 \times (-7) \mod 22 \\ &\equiv 5^4 \times (-7) \mod 22 \\ &\equiv 25^2 \times (-7) \mod 22 \\ &\equiv 3^2 \times (-7) \mod 22 \end{aligned}$$

を得る．従って解は $x \equiv -63 \equiv 3 \mod 22$ である．

問題 9.13. この例を複数の解き方で解け.（例 6.20 も見よ.）

10. 原始根

次節からは二次合同式を扱う．それへの準備である．

命題 10.1. p を素数とする．整数係数 n 次合同式

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \mod p$$

（ただし $a_n \not\equiv 0 \mod p$ とする）の整数解は p を法として高々 n 個である．

Proof. n に関する帰納法で示す．$n = 1$ のときは命題 6.17 から従う．$n > 1$ とする．$x_1, x_2, \ldots, x_k$ を p を法として相異なる $f(x)$ の解とする．ここで $k \leq n$ を示せば良い．

$f(x)$ を $x - x_1$ で割ると余りは $f(x_1)$ に等しい．つまりある整数係数多項式 $f_1(x)$ が存在[12]し，$f(x) = (x - x_1)f_1(x) + f(x_1)$ が成り立つ．$f_1(x)$ は $n-1$ 次式で，最高次の係数は $a_n \not\equiv 0 \mod p$ なので $f_1(x) \equiv 0 \mod p$ は $n-1$ 次合同式である．ここで $f(x) \equiv 0 \mod p$ の解の一つである x_i $(i \neq 1)$ を代入すると，

$$(x_i - x_1)f_1(x_i) \equiv 0 \mod p$$

が成り立つ．今 $x_i - x_1 \not\equiv 0 \mod p$ なので，系 6.16 より $f_1(x_i) \equiv 0 \mod p$ である．つまり $x_2, x_3, \ldots, x_k$ は $n-1$ 次合同式 $f_1(x) \equiv 0 \mod p$ の解であるが，その個数は帰納法の仮定より p を法として高々 $n-1$ 個である．つまり $k - 1 \leq n - 1$ である．故に $k \leq n$ を得る． □

注意 10.2. 素数を法とする，というのは本質的である．例えば $x^2 \equiv 1 \mod 8$ の解は $x = 1, 3, 5, 7$ の 4 つである．

上の命題は解が存在すれば，その個数は …，という話である．もちろん，いつ解が存在するか？という問題は残っている．二次合同式に関してそれを調べるのが次節である．

話は少し変わる．

定義 10.3. m を自然数，a を $(a, m) = 1$ をみたす整数とする．このとき $a^n \equiv 1 \mod m$ となる最小の自然数 n を $\mathrm{ord}_m(a)$ と記し，法 m に関する a の**位数**という．また，素数 p に対し，$\mathrm{ord}_p(a) = p - 1$ となる $a \in \mathbb{Z}$ を p を法とする**原始根**という．

例 10.4. 7 を法とする原始根を求めるために，$a = 1, 2, \ldots, 6$ に対して a^i $(i = 1, 2, \ldots, 6)$ を 7 で割った余りを調べる．

$a = 1$ のとき，$1^1 = 1^2 = \cdots = 1^6 = 1$ なので $i = 1, 2, \ldots, 6$ に対し，$a^i \equiv 1 \mod 7$ である．つまり $\mathrm{ord}_7(1) = 1$ なので，1 は 7 を法とする原始根ではない．

[12] これはちゃんと示すべきことかもしれない．

$a = 2$ のとき，$2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 1, 2^4 = 16 \equiv 2, 2^5 = 32 \equiv 4, 2^6 \equiv 1 \mod 7$ であるから，$\mathrm{ord}_7(2) = 3$ である．従って 2 は 7 を法とする原始根ではない．なお $2^6 \equiv 1 \mod 7$ は Fermat の小定理（定理 9.5）の例である．

$a = 3$ のとき，$3^1 = 3, 3^2 = 9 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \mod 7$ であるから，$\mathrm{ord}_7(3) = 6$ である．従って 3 は 7 を法とする原始根である．

以下同様に $\mathrm{ord}_7(4) = 3$，$\mathrm{ord}_7(5) = 6$，$\mathrm{ord}_7(6) = 2$ となる．以上より 7 を法とする原始根は 3 と 5 である．

問題 10.5. 11 を法とする原始根を求めよ．

補題 10.6. m を自然数，a を $(a, m) = 1$ をみたす整数とする．$n = \mathrm{ord}_m(a)$ のとき，次が成り立つ．

(1) $a^i \equiv a^j \mod m$ の必要十分条件は $i \equiv j \mod n$ である．
(2) 整数 k に対して $\mathrm{ord}_m(a^k) = \dfrac{n}{(n, k)}$ が成り立つ．

Proof. (1) $(a, m) = 1$ なので，$a^i \equiv a^j \mod m$ の両辺を a で j 回割ると $a^{i-j} \equiv 1 \mod m$ を得る．さらに $i - j$ を n で割ると，除法の定理（定理 2.4）より $i - j = n \times q + r$ $(0 \leq r < n)$ をみたす整数 q, r が存在する．今 $a^n \equiv 1 \mod m$ なので

$$\begin{aligned} a^{i-j} &= a^{nq+r} \\ &= (a^n)^q \times a^r \\ &\equiv a^r \mod m \end{aligned}$$

である．また $0 \leq r < n = \mathrm{ord}_m(a)$ なので，$a^{i-j} \equiv 1 \mod m$ は $r = 0$ を意味する．すなわち $i - j$ は n で割り切れる．

(2) $i = \mathrm{ord}_m(a^k)$ とする．$(a^k)^i \equiv 1 \mod m$ なので，(1) より $ik \equiv 0 \mod n$，つまり $ik \equiv 0k \mod n$ が成り立つ．命題 6.15 (2) より，$d = n/(n, k)$ とすれば $i \equiv 0 \mod d$ である．位数の最小性より，$i = d$ を得る． □

さてこの節のメインは次である．

定理 10.7. 各素数に対して原始根は存在する．

Proof. 素数 p に対し，d を $p-1$ の約数とし，

$$R_d := \{a \in \{1, 2, \ldots, p-1\} \mid \mathrm{ord}_p(a) = d\}$$

とする．$\sharp R_{p-1} > 0$ が定理の主張であるので，各 d に対し $\sharp R_d = \varphi(d) > 0$ を示せば良い．まず $\sharp R_d \leq \varphi(d)$ を示す．ここで φ は Euler 関数である．もし $R_d = \emptyset$ ならば $\sharp R_d = 0 < \varphi(d)$ であるから，$R_d \neq \emptyset$ の場合を考える．

$a \in R_d$ とすると，補題 10.6 (1) より $1, a, a^2, \ldots, a^{d-1}$ は p を法として相異なる．そして $(a^k)^d \equiv (a^d)^k \equiv 1 \mod p$ なので，これら d 個の数は d 次合同式 $x^d \equiv 1 \mod p$ の解であり，命題 10.1 より，これらの解が d 次合同式 $x^d \equiv 1 \mod p$ の全てである．また補題 10.6 (2) より $\mathrm{ord}_p(a^k) = d$ の必要十分条件は $d/(d,k) = d$，つまり $(d,k) = 1$ である．従って $R_d = \{a^k \mid (d,k) = 1, 0 \leq k < d\}$ であり，$\sharp R_d = \varphi(d)$ である．以上によって $p-1$ の約数 d に対し $\sharp R_d \leq \varphi(d)$ が成り立つ．

これと命題 8.20 より

$$\sum_{d|p-1} \sharp R_d \leq \sum_{d|p-1} \varphi(d) = p-1$$

が成り立つ．また Fermart の小定理（定理 9.5）から $a^{p-1} \equiv a^0 \mod p$ であるので，補題 10.6 (1) [13]より $a \in \{1, 2, \ldots, p-1\}$ の位数 $\mathrm{ord}_p(a)$ は $p-1$ の約数である．位数を二種類もつ元は存在しないので $p-1$ の約数 d を動かしたとき $\coprod_{d|p-1} R_d = \{1, 2, \ldots, p-1\}$ が成り立つ．従って $\sum_{d|p-1} \sharp R_d = p-1$ である．つまり

$$\sum_{d|p-1} \sharp R_d = \sum_{d|p-1} \varphi(d)$$

であるが，これは各 d に対して $\sharp R_d = \varphi(d)$ を意味している． □

次の補題は次節で断りなしに頻繁に用いる．

[13]つまるところ $i = p-1, j = 0$ の場合である．

補題 10.8. p を素数とし，g を p を法とする原始根とする．整数 a が $(a,p)=1$ をみたすとき $a \equiv g^i \mod p$ をみたす整数 i が $\{0,1,2,\dots,p-2\}$ の中に唯一つ存在する．

Proof. p を法とした話なので $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ として良く，集合 $\{1,g,g^2,\dots,g^{p-2}\}$ が $(\mathbb{Z}/p\mathbb{Z})^\times$ の既約剰余系であることを示せば良い．

g は原始根であるから $(g,p)=1$ である．従って $(g^i,p)=1$ $(i=0,1,2,\dots,p-2)$ である．つまり g^i は $(\mathbb{Z}/p\mathbb{Z})^\times$ の代表元である．また，補題 10.6 (1) より $g^i \not\equiv g^j \mod p$ $(i,j=0,1,2,\dots,p-2)$ に注意する．$\sharp(\mathbb{Z}/p\mathbb{Z})^\times = p-1$ なので $\{1,g,g^2,\dots,g^{p-2}\}$ は既約剰余系である． □

問題 10.9. 例 10.4 を参考に，$\{1,5,5^2,5^3,5^4,5^5\}$ が $(\mathbb{Z}/7\mathbb{Z})^\times$ の既約剰余系 $\{1,2,3,4,5,6\}$ になることを示せ．また $\{1,4,4^2,4^3,4^4,4^5\}$ はどうか?

11. 平方剰余の相互法則

この節では二次合同式を扱う．順番的にも相場[14]であろう．ここでは具体的な解を求めるというよりは，与えられた 2 次合同式が整数解を持つか否かを判定する．

11.1. Legendre 記号と平方剰余.

定義 11.1. p を奇素数とし，a を $a \not\equiv 0 \mod p$ をみたす整数とする．2 次合同式 $x^2 \equiv a \mod p$ が整数解を持つとき a を法 p の**平方剰余**，そうでないとき a を法 p の**平方非剰余**という．

定義 11.2. p を奇素数とし，a を $a \not\equiv 0 \mod p$ をみたす整数とする．このとき

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ は法 } p \text{ の平方剰余} \\ -1 & a \text{ は法 } p \text{ の平方非剰余} \end{cases}$$

と定め，これを **Legendre 記号**という．

[14] 今の中学生もそうだと思うが，私は一次方程式の後に連立一次方程式を勉強し，それから二次方程式を勉強した（はず）．

例 11.3. $1^2 \equiv 1 \mod p$ なので 1 は法 p の平方剰余である．すなわち任意の奇素数 p に対して $\left(\frac{1}{p}\right) = 1$ である．

また，$2^2 \equiv 5^2 \equiv 4 \mod 7, 3^2 \equiv 4^2 \equiv 2 \mod 7, 6^2 \equiv 1 \mod 7$ なので 7 の平方剰余は 1,2,4 であり，残りの 3,5,6 は平方非剰余である．Legendre 記号で表すと

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

である．

以下 Legendre 記号 $\left(\frac{a}{p}\right)$ の値が 1 か -1 かを判定していくのだが，最初の命題が次である．

命題 11.4. g を素数 p を法とする原始根，a を $(a, p) = 1$ をみたす整数とする．このときある整数 i が存在して $a \equiv g^i \mod p$ をみたせば，$\left(\frac{a}{p}\right) = (-1)^i$ である．

Proof. $\left(\frac{a}{p}\right) = 1$ の必要十分条件は i が偶数であることを示す．

i が偶数のとき $i = 2j$ とすると，$(g^j)^2 \equiv a \mod p$ なので $\left(\frac{a}{p}\right) = 1$ である．逆に $\left(\frac{a}{p}\right) = 1$ であれば $x^2 \equiv a (\equiv g^i) \mod p$ をみたす整数 x が存在する．補題 10.8 より $x = g^k$ とでき，このとき $g^{2k} \equiv g^i \mod p$ であるが，補題 10.6 (1) より $2k \equiv i \mod p - 1$ である．$p - 1$ は偶数なので i は偶数である． □

命題 11.5. p を奇素数，$a, b \not\equiv 0 \mod p$ をみたす整数とする．このとき次が成り立つ．

(1) $a \equiv b \mod p$ ならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ が成り立つ．
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof. (1) は当たり前である．(2) 補題 10.8 より g を p を法とする原始根とすると，$a \equiv g^i, b \equiv g^j \mod p$ とできる．$ab \equiv g^{i+j} \mod p$ なの

で，命題 11.4 より

$$\begin{aligned}\left(\frac{ab}{p}\right) &= (-1)^{i+j} \\ &= (-1)^i \times (-1)^j \\ &\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\end{aligned}$$

である． □

この命題は素因数分解の一意性（定理 5.1）を用いることで，Legendre 記号の計算の本質的は素数の場合である事を主張している．たとえば

$$\left(\frac{20}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$$

である．しかし通常 $\left(\frac{2}{p}\right)$ や $\left(\frac{3}{p}\right)$ の値を決定するのは簡単ではない．これを計算するのが次である：

定理 11.6 (Euler の規準)**.** p を奇素数，a を $(a,p)=1$ をみたす整数とするとき

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

が成り立つ．

Proof. g を素数 p を法とする原始根とし，$a \equiv g^i \mod p$ とする．命題 11.4 より $\left(\frac{a}{p}\right) = (-1)^i \equiv (-1)^i \mod p$ が成り立つ．また

$$a^{\frac{p-1}{2}} \equiv \left(g^i\right)^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^i \mod p$$

に注意する．

さて g は原始根であるから $g^{p-1} \equiv 1 \mod p$ が成り立ち，$g^{\frac{p-1}{2}} \equiv \pm 1 \mod p$ をみたす．また $\mathrm{ord}_p(g) = p-1 > (p-1)/2$ より，$g^{\frac{p-1}{2}} \not\equiv 1 \mod p$ である．従って

$$\left(g^{\frac{p-1}{2}}\right)^i \equiv (-1)^i \mod p$$

が成り立つ． □

注意 11.7. Fermat の小定理（定理 9.5）をもう一度見よ．

例 11.8. Euler の規準を用いて

$$\left(\frac{2}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = -1$$

であることを確認する．

$$2^{\frac{7-1}{2}} = 2^3 = 8 \equiv 1 \mod 7$$

と

$$3^{\frac{7-1}{2}} = 3^3 = 27 \equiv -1 \mod 7$$

より，

$$\left(\frac{2}{7}\right) \equiv 1, \quad \left(\frac{3}{7}\right) \equiv -1 \mod 7$$

であるのだが，左辺は 1 か -1 しか取り得ず，7 を法としたとき $1 \not\equiv -1$ であるからこの合同 $\equiv$ は等号 $=$ としても成り立つ．

また以上より $\left(\frac{20}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = -1$ であることが分かる．つまり $x^2 \equiv 20 \mod 7$ は整数解を持たない．

原理的にはこの Euler の規準を用いれば，Legendre 記号 $\left(\frac{a}{p}\right)$ の値の決定はできる．しかし a や p の値が大きくなると $a^{\frac{p-1}{2}}$ の計算などは困難である．その意味でも次の定理は大変ありがたいものである．ここが初等整数論のひとつのハイライトである．

定理 11.9 (平方剰余の相互法則，補充法則)**.** p, q を相異なる奇素数とする．このとき次が成り立つ．

(1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ （第一補充法則）

(2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ （第二補充法則）

(3) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$ （平方剰余の相互法則）

例 11.3 によって，1 に関しては平方剰余の問題は終了しているが，それら以外の整数は素因数分解（定理 5.1）と命題 11.5 によって，上の 3 つの式から Legendre 記号の値が決定できる．

証明に入る前に一つ補題を準備する．

補題 11.10. 自然数 n に対し，$\zeta_n := e^{(2\pi\sqrt{-1})/n} = \cos(2\pi/n)+\sqrt{-1}\sin(2\pi/n)$ と定め，**1 の原始 n 乗根**という．a を奇数とするとき

$$\zeta_8^a + \zeta_8^{-a} = (-1)^{\frac{a^2-1}{8}}\sqrt{2}$$

が成り立つ．

Proof. 整数 m に対して，$\zeta_n^{n+m} = \zeta_n^m$ なので，$a = 1, 3, 5, 7$ に関して確かめれば良い．

$$\begin{aligned}
\zeta_8 &= \cos\frac{2\pi}{8} + \sqrt{-1}\sin\frac{2\pi}{8} \\
&= \cos\frac{\pi}{4} + \sqrt{-1}\sin\frac{\pi}{4} \\
&= \frac{1+\sqrt{-1}}{\sqrt{2}} \\
\zeta_8^{-1} &= \cos\frac{-2\pi}{8} + \sqrt{-1}\sin\frac{-2\pi}{8} \\
&= \cos\frac{2\pi}{8} - \sqrt{-1}\sin\frac{2\pi}{8} \\
&= \frac{1-\sqrt{-1}}{\sqrt{2}}
\end{aligned}$$

なので $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ である，$\zeta_8^7 = \zeta_8^{-1}, \zeta_8^{-7} = \zeta_8$ であるので $\zeta_8^7 + \zeta_8^{-7} = \sqrt{2}$ も成り立つ．同様の計算によって $\zeta_8^3 + \zeta_8^{-3} = \zeta_8^5 + \zeta_8^{-5} = -\sqrt{2}$ を得る．また

$$(-1)^{\frac{a^2-1}{8}} = \begin{cases} 1 & a \equiv 1, 7 \mod 8 \\ -1 & a \equiv 3, 5 \mod 8 \end{cases}$$

なので

$$\zeta_8^a + \zeta_8^{-a} = (-1)^{\frac{a^2-1}{8}}\sqrt{2}$$

が成り立つ． □

ここでは定理 11.9 の (1) と (2) のみ証明を与える．

Proof. (1) Euler の規準（定理 11.6）より

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$$

である．左辺は 1 か -1 しか取り得ず，p を法としたとき $1 \not\equiv -1$ であるからこの合同 $\equiv$ は等号 $=$ としても成り立つ．

(2) Euler の規準より

$$\begin{aligned}\left(\frac{2}{p}\right) &\equiv 2^{\frac{p-1}{2}} \mod p \\ &\equiv (\sqrt{2})^{p-1} \mod p \\ &\equiv (\zeta_8 + \zeta_8^{-1})^{p-1} \mod p \dots (*)\end{aligned}$$

である．一方，二項定理と補題 11.10 を用いれば

$$\begin{aligned}(\zeta_8 + \zeta_8^{-1})^p &= \sum_{k=0}^{p} \binom{p}{k} \zeta_8^{p-k} (\zeta_8^{-1})^k \\ &= \sum_{k=0}^{p} \binom{p}{k} \zeta_8^{p-2k} \\ &= \zeta_8^p + \zeta_8^{-p} + \sum_{k=1}^{p-1} \binom{p}{k} \zeta_8^{p-2k} \\ &= (-1)^{\frac{p^2-1}{2}} \sqrt{2} + \sum_{k=1}^{p-1} \binom{p}{k} \zeta_8^{p-2k}\end{aligned}$$

である．この両辺を $\zeta_8^p + \zeta_8^{-p} = \sqrt{2}$ で割ると，

$$(\zeta_8 + \zeta_8^{-1})^{p-1} = (-1)^{\frac{p^2-1}{8}} + \frac{1}{\sqrt{2}} \sum_{k=1}^{p-1} \binom{p}{k} \zeta_8^{p-2k}$$

である．従って補題 9.1 より $(\zeta_8 + \zeta_8^{-1})^{p-1} \equiv (-1)^{\frac{p^2-1}{8}} \mod p$ である．これと $(*)$ より第二補充法則を得る． □

11.2. **Gauß和.** 定理 11.9 (3) を証明するための準備がしばらく続く．

補題 11.11. p を奇素数とする．このとき $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$ である．

Proof. g を p を法とする原始根，$a \equiv g^i \mod p$ とする．言い換えれば，集合 $\{1, 2, \dots, p-1\}$ も $\{g, g^2, \dots, g^{p-1}\}$ も $(\mathbb{Z}/p\mathbb{Z})^\times$ の既約剰余系をな

している（補題 10.8 も見よ.）ので，命題 11.4 より

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{g^i}{p}\right)=\sum_{i=1}^{p-1}(-1)^i=0$$

である. □

定義 11.12. ζ_n を 1 の原始 n 乗根とする．このとき奇素数 p に対して

$$G_p=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$$

を **Gauss 和**という.

例 11.13. G_3 を計算する．計算すべきものは ζ_3^a と $\left(\frac{a}{3}\right)$ の値である.（ただし $a=1,2$ である.）1 の原始 3 乗根に関しては定義通りに計算すれば良い.

$$\begin{aligned}\zeta_3&=\cos\frac{2\pi}{3}+\sqrt{-1}\sin\frac{2\pi}{3}\\&=-\frac{1}{2}+\sqrt{-1}\frac{\sqrt{3}}{2}\\&=\frac{-1+\sqrt{-3}}{2}\end{aligned}$$

この値を 2 乗すれば $\zeta_3^2=\frac{-1-\sqrt{-3}}{2}$ を得られるが，de Moivre の定理：$(\cos\theta+\sqrt{-1}\sin\theta)^n=\cos n\theta+\sqrt{-1}\sin n\theta$ を用いても計算できる．Legendre 記号に関しては例 11.3 より $\left(\frac{1}{3}\right)=1$ である．また $2\equiv -1 \mod 3$ なので，命題 11.5 より $\left(\frac{2}{3}\right)=\left(\frac{-1}{3}\right)$ であり，第一補充法則（定理 11.9(1) なのでこれは証明済み[15]である.）より $\left(\frac{2}{3}\right)=\left(\frac{-1}{3}\right)=(-1)^{(3-1)/2}=-1$

[15]そういうことならば，直接第二補充法則を使ってもよいのだが.

である．以上より

$$\begin{aligned} G_3 &= \sum_{a=1}^{3-1} \left(\frac{a}{p}\right) \zeta_3^a \\ &= \left(\frac{1}{3}\right) \zeta_3 + \left(\frac{2}{3}\right) \zeta_3^2 \\ &= \frac{-1+\sqrt{-3}}{2} - \frac{-1-\sqrt{-3}}{2} \\ &= \sqrt{-3} \end{aligned}$$

である．

例 11.14. $G_5 = \left(\frac{1}{5}\right)\zeta_5 + \left(\frac{2}{5}\right)\zeta_5^2 + \left(\frac{3}{5}\right)\zeta_5^3 + \left(\frac{4}{5}\right)\zeta_5^4$ の値を求める．$\left(\frac{1}{5}\right) = 1$ は明らか．また第一補充法則より $\left(\frac{4}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{(5-1)/2} = 1$ である．あえて第二補充法則は用いず，Euler の規準（定理 11.6）より

$$\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \equiv -1, \quad \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} \equiv -1 \mod 5$$

である．従って $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$ を得る．つまり $G_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$ である．

さて，$\zeta_5^5 - 1 = 0$ なので左辺を因数分解すると，$(\zeta_5 - 1)(1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) = 0$ であり，$\zeta_5 \neq 1$ より $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0 \ldots (*)$ が成り立つ．つまり $-(\zeta_5^2 + \zeta_5^3) = 1 + \zeta_5 + \zeta_5^4$ である．これより

$$\begin{aligned} G_5 &= \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \\ &= 1 + 2(\zeta_5 + \zeta_5^4) \end{aligned}$$

である．ところで $(*)$ の両辺を $\zeta_5^2 \neq 0$ で割ると，$\zeta_5^{-2} + \zeta_5^{-1} + 1 + \zeta_5 + \zeta_5^2 = 0$ なので $(\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 = 0$ である．$\zeta_5^{-1} = \zeta_5^4$ に注意すれば，

$$(\zeta_5 + \zeta_5^4)^2 + (\zeta_5 + \zeta_5^4) - 1 = 0$$

が成り立つ．この二次方程式を解けば $\zeta_5+\zeta_5^4=(-1\pm\sqrt{5})/2$ である．そして $\zeta_5=\cos\frac{2\pi}{5}+\sqrt{-1}\sin\frac{2\pi}{5}$ と

$$\begin{aligned}\zeta_5^4&=\zeta_5^{-1}\\&=\cos\frac{-2\pi}{5}+\sqrt{-1}\sin\frac{-2\pi}{5}\\&=\cos\frac{2\pi}{5}-\sqrt{-1}\sin\frac{2\pi}{5}\end{aligned}$$

から $\zeta_5+\zeta_5^4=2\cos\frac{2\pi}{5}>0$ である．[16]従って $\zeta_5+\zeta_5^4=(-1+\sqrt{5})/2$ であり，

$$G_5=1+2\times\frac{-1+\sqrt{5}}{2}=\sqrt{5}$$

を得る．

注意 11.15. 一般に

$$G_p=\begin{cases}\sqrt{p} & p\equiv 1 \mod 4\\ \sqrt{-p} & p\equiv 3 \mod 4\end{cases}$$

が知られている．

問題 11.16. Euler の規準ではなく，第一補充法則と第二補充法則を用いて

$$\left(\frac{2}{5}\right)=\left(\frac{3}{5}\right)=-1$$

を確かめよ．

定義 11.17. 奇素数 p に対し

$$p^*=(-1)^{\frac{p-1}{2}}p=\begin{cases}p & p\equiv 1 \mod 4\\ -p & p\equiv 3 \mod 4\end{cases}$$

と定める．

命題 11.18. p を奇素数とする．このとき $G_p^2=p^*$ が成り立つ．

[16] $-\pi\le\theta\le\pi$ において $\cos\theta\ge 0$ である．

Proof. 直接計算する：

$$\begin{aligned} G_p^2 &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \times \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta_p^b \\ &= \sum_{a=1}^{p-1} \left(\sum_{b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta_p^{a+b} \right) \end{aligned}$$

ここで $b = at$ とすると

$$\begin{aligned} &= \sum_{a=1}^{p-1} \left(\sum_{t=1}^{p-1} \left(\frac{a^2 t}{p}\right) \zeta_p^{a(1+t)} \right) \\ &= \sum_{a=1}^{p-1} \left(\sum_{t=1}^{p-1} \left(\frac{a^2}{p}\right) \left(\frac{t}{p}\right) \zeta_p^{a(1+t)} \right) \\ &= \sum_{t=1}^{p-1} \left(\left(\frac{t}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{a(1+t)} \right) \dots (\clubsuit) \end{aligned}$$

今 $(a, p) = 1$ なので,

$$\sum_{a=1}^{p-1} \zeta_p^{a(1+t)} = \begin{cases} p-1 & 1+t \equiv 0 \mod p \\ -1 & 1+t \not\equiv 0 \mod p \end{cases}$$

に注意する．($\clubsuit$) の計算を続けると,

$$\begin{aligned} (\clubsuit) &= \sum_{t=1}^{p-2} \left(\left(\frac{t}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{a(1+t)} \right) + \left(\frac{p-1}{p}\right) \left(\sum_{a=1}^{p-1} \zeta_p^{ap} \right) \\ &= -\sum_{t=1}^{p-2} \left(\frac{t}{p}\right) + \left(\frac{p-1}{p}\right) (p-1) \\ &= \left(\frac{p-1}{p}\right) p - \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \end{aligned}$$

補題 11.11 と $p - 1 \equiv -1 \mod p$ より

$$= \left(\frac{-1}{p}\right) p$$

である．また第一補充法則（定理 11.9 (1)）より

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

なので $\left(\frac{-1}{p}\right) p = p^*$ である．故に $G_p^2 = p^*$ である． □

11.3. **平方剰余の相互法則の証明.** 定理 11.9 (3)：平方剰余の相互法則

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$$

を示す．この命題を示すために，色々な言い換えをする．次はよく知られている言い換えで，(2) を平方剰余の相互法則と呼ぶ場合も多い．

補題 11.19. p, q を相異なる奇素数とする．このとき次は同値である．

(1) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$

(2) $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$

(3) $G_q^{p-1} \equiv \left(\frac{p}{q}\right) \mod p$

Proof. (1) と (2) の同値について：命題 11.5 と第一補充法則（定理 11.9 (1)）より

$$\begin{aligned}\left(\frac{q^*}{p}\right) &= \left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right)\\ &= \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right)\\ &= \left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)\\ &= (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\left(\frac{q}{p}\right) \dots (*)\end{aligned}$$

が成り立つ．(1) の式を $(*)$ に代入することで (2) が得られる．また (2) を仮定して，$(*)$ の両辺に $\left(\frac{q}{p}\right)$ を代入すれば (1) を得る．

(2) と (3) の同値について：命題 11.18 と Euler の規準（定理 11.6）より

$$G_q^{p-1} = (q^*)^{\frac{p-1}{2}} \equiv \left(\frac{q^*}{p}\right) \mod p$$

なので (2) と (3) は同値である． □

以下で行う平方剰余の相互法則（定理 11.9 (3)）の証明方針としては (3) が成り立つことを示す．そこで Gauss 和 G_q を p 乗する：

$$\begin{aligned} G_q^p &= \left(\sum_{a=1}^{q-1} \left(\frac{a}{q} \right) \zeta_q^a \right)^p \\ &= \sum_{a_1=1}^{q-1} \left(\frac{a_1}{q} \right) \zeta_q^{a_1} \times \sum_{a_2=1}^{q-1} \left(\frac{a_2}{q} \right) \zeta_q^{a_2} \times \cdots \times \sum_{a_p=1}^{q-1} \left(\frac{a_p}{q} \right) \zeta_q^{a_p} \\ &= \sum_{(a_1,a_2,\ldots,a_p)\in A} \left(\frac{a_1 a_2 \ldots a_p}{q} \right) \zeta_q^{a_1+a_2+\cdots+a_p} \end{aligned}$$

ここで $A := \{(a_1, a_2, \ldots, a_p) \in \mathbb{Z}^p \mid 0 < a_i < q\}$ である．さらに

$$A_t = \{(a_1, a_2, \ldots, a_p) \in A \mid a_1 + a_2 + \cdots + a_p \equiv t \mod q\}$$

として，

$$J_t := \sum_{(a_1,a_2,\ldots,a_p)\in A_t} \left(\frac{a_1 a_2 \ldots a_p}{q} \right)$$

と定めれば，

$$G_q^p = \sum_{t=0}^{q-1} J_t \zeta_q^t \ldots (\diamondsuit)$$

である．

補題 11.20. s, t を整数とする．$(s, q) = 1$ のとき $J_{st} = \left(\frac{s}{q} \right) J_t$ が成り立つ．

Proof. 整数 x を q で割った余りを $\langle x \rangle_q$ で表す．$(s, q) = 1$ なので，

$$A_{st} = \{(\langle sa_1 \rangle_q, \langle sa_2 \rangle_q, \ldots, \langle sa_p \rangle_q) \in \mathbb{Z}^p \mid (a_1, a_2, \ldots, a_p) \in A_t\}$$

が成り立つ．従って

$$\begin{aligned}
J_{st} &= \sum_{(b_1,b_2,\ldots,b_p)\in A_{st}} \left(\frac{b_1 b_2 \ldots b_p}{q}\right) \\
&= \sum_{(a_1,a_2,\ldots,a_p)\in A_t} \left(\frac{(sa_1)(sa_2)\ldots(sa_p)}{q}\right) \\
&= \sum_{(a_1,a_2,\ldots,a_p)\in A_t} \left(\frac{ss\ldots s}{q}\right)\left(\frac{a_1 a_2 \ldots a_p}{q}\right) \\
&= \left(\frac{s}{q}\right)^p \sum_{(a_1,a_2,\ldots,a_p)\in A_t} \left(\frac{a_1 a_2 \ldots a_p}{q}\right) \\
&= \left(\frac{s}{q}\right)^p J_t
\end{aligned}$$

である．今 p は奇素数なので $(\pm 1)^p = \pm 1$ なので $\left(\frac{s}{q}\right)^p = \left(\frac{s}{q}\right)$ である．従って $J_{st} = \left(\frac{s}{q}\right) J_t$ が成り立つ． □

問題 11.21. 上の設定で,

$$A_{st} = \{(\langle sa_1\rangle_q, \langle sa_2\rangle_q, \ldots, \langle sa_p\rangle_q) \in \mathbb{Z}^p \mid (a_1, a_2, \ldots, a_p) \in A_t\}$$

を示せ.

命題 11.22. p, q を相異なる奇素数とすると $G_q^{p-1} = J_1$ が成り立つ.

Proof. 補題 11.20 で $t = 0$ のとき $\left(\frac{s}{q}\right) = -1$ となる s を取る[17]と，$J_0 = -J_0$ なので $J_0 = 0$ である．また $(s, q) = 1$ をみたす整数 s に対し，$t = 1$

[17]たとえば s として原始根を取れば良い.

とすれば $J_s = \left(\frac{s}{q}\right) J_1$ なので $(\diamondsuit)$ より

$$\begin{aligned} G_q^p &= \sum_{s=0}^{q-1} J_s \zeta_q^s \\ &= \sum_{s=1}^{q-1} \left(\frac{s}{q}\right) J_1 \zeta_q^s \\ &= J_1 \sum_{s=1}^{q-1} \left(\frac{s}{q}\right) \zeta_q^s \\ &= J_1 G_q \end{aligned}$$

が成り立つ．両辺を $G_q \neq 0$ で割ると $G_q^{p-1} = J_1$ が成り立つ． □

補題 11.19 (3) によって，平方剰余の相互法則（定理 11.9 (3)）を証明するために $J_1 \equiv \left(\frac{p}{q}\right) \mod p$ を示せば良い．

命題 11.23. p, q を相異なる奇素数とすると $J_1 \equiv \left(\frac{p}{q}\right) \mod p$ が成り立つ．

Proof. $\boldsymbol{a} = (a_1, a_2, \ldots, a_p) \in A$ に対し，

$$\left(\frac{\boldsymbol{a}}{q}\right) := \left(\frac{a_1 a_2 \ldots a_p}{q}\right)$$

と記す．つまり

$$J_1 = \sum_{\boldsymbol{a} \in A_1} \left(\frac{\boldsymbol{a}}{q}\right)$$

である．

整数 u が q と互いに素のとき，$\boldsymbol{a}_0 = (u, u, \ldots, u) \in A_1$ とおくと $pu \equiv 1 \mod q$ であり，命題 6.17 よりこの合同式の解 u は q を法として唯一つ存在する．つまり $\boldsymbol{a}_0$ は A_1 において唯一つ存在する元である．また

$$\left(\frac{\boldsymbol{a}_0}{q}\right) = \left(\frac{u}{q}\right)^p = \left(\frac{u}{q}\right) \quad \text{かつ} \quad \left(\frac{pu}{q}\right) = \left(\frac{1}{q}\right) = 1$$

なので

$$\left(\frac{\boldsymbol{a}_0}{q}\right) = \left(\frac{p}{q}\right)$$

が成り立つ.

さてここで，$\boldsymbol{a}_0$ とは異なる $\boldsymbol{a} = (a_1, a_2, \ldots, a_p) \in A_1$ に対して

$$\boldsymbol{a}^{(k)} = (a_{1+k}, a_{2+k}, \ldots, a_p, a_1, \ldots, a_k)$$

と定める．つまり $\boldsymbol{a}^{(k)}$ は $\boldsymbol{a}$ の左から k 個の成分を a_p の右側へズラしたものである．このとき $\boldsymbol{a}^{(0)} = \boldsymbol{a}, \boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(p-1)}$ は A_1 の相異なる p 個の元であるが,

$$\left(\frac{\boldsymbol{a}^{(0)}}{q}\right) = \left(\frac{\boldsymbol{a}^{(1)}}{q}\right) = \cdots = \left(\frac{\boldsymbol{a}^{(p-1)}}{q}\right)$$

をみたす．故に

$$\begin{aligned}\sum_{k=0}^{p-1}\left(\frac{\boldsymbol{a}^{(k)}}{q}\right) &= p\left(\frac{\boldsymbol{a}^{(0)}}{q}\right)\\ &= p\left(\frac{\boldsymbol{a}}{q}\right)\\ &\equiv 0 \mod p\end{aligned}$$

である．つまり p を法として $J_1 = \sum_{\boldsymbol{a}\in A_1}\left(\frac{\boldsymbol{a}}{q}\right)$ の値を考えたとき，$\boldsymbol{a}_0$ 以外の A_1 の元は J_1 へ寄与しない．従って

$$J_1 = \sum_{\boldsymbol{a}\in A_1}\left(\frac{\boldsymbol{a}}{q}\right) \equiv \left(\frac{\boldsymbol{a}_0}{q}\right) \equiv \left(\frac{p}{q}\right) \mod p$$

が成り立つ. □

以上によって平方剰余の相互法則（定理 11.9 (3)）が証明された.

例 11.24. 491 は 223 を法として平方剰余か否かを調べる．つまり $\left(\frac{491}{223}\right)$ の値を求めれば良い．

$$\begin{aligned}\left(\frac{491}{223}\right) &= \left(\frac{45}{223}\right) = \left(\frac{3^2}{223}\right)\left(\frac{5}{223}\right) = 1 \times \left(\frac{223^*}{5}\right) \\ &= \left(\frac{(-1)^{\frac{223-1}{2}}223}{5}\right) = \left(\frac{-223}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) \\ &= (-1)^{\frac{5-1}{2}}\left(\frac{5^*}{3}\right) = \left(\frac{(-1)^{\frac{5-1}{2}}5}{3}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{5}\right) \\ &= (-1)^{\frac{5^2-1}{8}} \\ &= -1\end{aligned}$$

なので 491 は 223 を法として平方非剰余である．

なお上の計算で $\left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) = (-1)^{\frac{5-1}{2}}\left(\frac{5^*}{3}\right)$ では第一補充法則を用いたが，$\left(\frac{3}{5}\right) = \left(\frac{-2}{5}\right)$ を用いた方が計算を少し省ける．つまり $\left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = \left(\frac{2}{5}\right)$ である．

問題 11.25. Legendre 記号の値をいろいろ計算してみよ．

12. 試験問題

ここまでの話で，持ち込みなし制限時間 90 分程度の試験を行うとすると，次のような問題を出す．

問題 次の問に答えよ．

(1) n を自然数とする．$4n^3 - n$ は 3 を約数に持つことを数学的帰納法を用いて示せ．

(2) V を $\mathbb{R}$ 上の n 次元ベクトル空間とし，$f : V \to V$ を線形写像とする．V 上の関係 $\boldsymbol{x} \sim \boldsymbol{y}$ を $\boldsymbol{x} - \boldsymbol{y} \in \operatorname{Ker} f$ と定める．このとき関係 $\sim$ は同値関係である事を示せ．なお $\operatorname{Ker} f := \{\boldsymbol{x} \in V | f(\boldsymbol{x}) = \boldsymbol{0}\}$ である．

(3) $1985 \times 1016 - 910 \times 3608$ を 13 で割ったときの余りを求めよ．

(4) 27^{100} を 28 で割ったときの余りを求めよ．

(5) 7^{20} を 66 で割ったときの余りを求めよ．

(6) 現金 1070 円を持って，62 円切手と 82 円切手を買いに行く．現金を丁度使い切るにはそれぞれ何枚買えば良いか？

(7) 連立一次合同式 $\begin{cases} 2x \equiv 3 \pmod 5 \\ 3x \equiv 1 \pmod 8 \\ 4x \equiv 5 \pmod 9 \end{cases}$ を解け．

(8) 明確な数が分からない品物がある．パッと見たところ，200 個以上はあるが 300 個もない．それらを 3 個ずつ数えると 2 個余り，5 個ずつ数えると 3 個余り，7 個ずつ数えると 2 個余る．品物の数は幾つか？

(9) 5 を法とする原始根を求めよ．

(10) 2 次合同式 $x^2 \equiv 45 \mod 19$ は整数解を持つか？

Appendix A. 代数方程式の解の公式

ここでは代数方程式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

を扱う．最高次の係数が 0 だとあまり意味がないので $a_n \neq 0$ と仮定する．よく知られている通り，$n = 1$ の時は 1 次方程式であり，$a_1 x + a_0 = 0$ の解は $x = -a_0/a_1$ である．$n = 2$ の時は 2 次方程式であり，その解き方は高校入試などで問われる．つまり $a_2 x^2 + a_1 x + a_0 = 0$ である．左辺を因数分解して解く場合も多いが，一般にその因数分解が簡単かどうかはわからない．しかし我々は「解の公式」を知っている．

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}$$

である．これは $a_2 x^2 + a_1 x + a_0$ を平方完成することで得られる．つまり

$$\begin{aligned} a_2 x^2 + a_1 x + a_0 &= a_2 \left(x^2 + \frac{a_1}{a_2} x \right) + a_0 \\ &= a_2 \left(x + \frac{a_1}{2a_2} \right)^2 + a_0 - a_2 \left(\frac{a_1}{2a_2} \right)^2 \\ &= a_2 \left(x + \frac{a_1}{2a_2} \right)^2 + \frac{4a_2 a_0 - a_1^2}{4a_2} \end{aligned}$$

なので,

$$a_2\left(x+\frac{a_1}{2a_2}\right)^2+\frac{4a_2a_0-a_1^2}{4a_2}=0$$

を解けば良い．これを整理すると,

$$\left(x+\frac{a_1}{2a_2}\right)^2=\frac{a_1^2-4a_2a_0}{4a_2^2}$$
$$x+\frac{a_1}{2a_2}=\pm\sqrt{\frac{a_1^2-4a_2a_0}{4a_2^2}}$$
$$x=-\frac{a_1}{2a_2}\pm\frac{\sqrt{a_1^2-4a_2a_0}}{2a_2}$$

を得る．この節では，3 次以上の方程式の「解の公式」について調べて行く．

A.1. **3 次方程式.** まず 3 次方程式 $x^3-px-q=0\ldots(*)$ の解の公式を調べる．$x=u+v$，$p=3uv$ と変数変換し，$(*)$ の左辺に代入すると：$(u+v)^3-3uv(u+v)-q=u^3+v^3+3u^2v+3uv^2-3u^2v-3uv^2-q=u^3+v^3-q$ なので，$q=u^3+v^3$ を得る．一方 $(u^3-v^3)^2=(u^3+v^3)^2-4u^3v^3=q^2-\frac{4}{27}p^3$ であるから,

$$u^3-v^3=\pm\sqrt{q^2-\frac{4}{27}p^3}$$

である．従って

$$u^3=\frac{1}{2}\left(q\pm\sqrt{q^2-\frac{4}{27}p^3}\right),\quad v^3=\frac{1}{2}\left(q\mp\sqrt{q^2-\frac{4}{27}p^3}\right)\quad\text{（複合同順）}$$

である．u と v の対称性から,

$$u^3=\frac{1}{2}\left(q+\sqrt{q^2-\frac{4}{27}p^3}\right),\quad v^3=\frac{1}{2}\left(q-\sqrt{q^2-\frac{4}{27}p^3}\right)$$

でも

$$u^3=\frac{1}{2}\left(q-\sqrt{q^2-\frac{4}{27}p^3}\right),\quad v^3=\frac{1}{2}\left(q+\sqrt{q^2-\frac{4}{27}p^3}\right)$$

でも議論は変わらない．そこで $u^3 = \frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right) \dots (1)$ として議論を進める．つまり，

$$u = \sqrt[3]{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)} \dots (2)$$

である．

注意 A.1. 1 の 3 乗根，つまり $z^3 = 1$ をみたすものは $1, \omega, \omega^2$ の 3 つある．ここで $\omega = (-1 + \sqrt{-3})/2$ である．

すなわち，(1) をみたす u は (2) 以外に

$$u = \omega\sqrt[3]{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)} \dots (3)$$

と

$$u = \omega^2\sqrt[3]{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)} \dots (4)$$

がある．$uv = p/3$ であったので，注意 A.1 より，(2) のときは

$$v = \frac{p}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}}$$

であり，(3) のときは

$$v = \frac{p\omega^2}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}}$$

であり，(4) のときは

$$v = \frac{p\omega}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}}$$

である．以上をまとめると次の定理を得る．($x = u + v$ としていたことは忘れてはいけない．)

定理 A.2 (Cardano の公式)**.** 方程式 $x^3 - px - q = 0$ の 3 つの解は

$$\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{\frac{1}{3}} + \frac{p}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}},$$

$$\omega\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{\frac{1}{3}} + \frac{p\omega^2}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}},$$

$$\omega^2\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{\frac{1}{3}} + \frac{p\omega}{3}\left\{\frac{1}{2}\left(q + \sqrt{q^2 - \frac{4}{27}p^3}\right)\right\}^{-\frac{1}{3}}$$

である.

さて，上では特殊な 3 次方程式を扱った．しかしこれが 3 次方程式の本質的である．実際に次が成り立つ.

補題 A.3. $a \neq 0$ とする．3 次方程式 $ax^3 + bx^2 + cx + d = 0 \ldots (**)$ は $x^3 - px - q = 0$ の型へ変形できる.

Proof. $a \neq 0$ なので，$(**)$ の両辺を a で割り整理する：

$$\begin{aligned} x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} &= \left(x + \frac{b}{3a}\right)^3 - \frac{b^2}{3a^2}x + \frac{c}{a}x + \frac{d}{a} - \frac{b^3}{27a^3} \\ &= \left(x + \frac{b}{3a}\right)^3 + \left(\frac{c}{a} - \frac{b^2}{3a^2}\right)\left(x + \frac{b}{3a}\right) \\ &\quad + \frac{d}{a} - \frac{b^3}{27a^3} - \frac{b}{3a}\left(\frac{c}{a} - \frac{b^2}{3a^2}\right) \\ &= X^3 - \frac{b^2 - 3ac}{3a^2}X - \frac{9abc - 27a^2d - 2b^3}{27a^3} \end{aligned}$$

である．ここで $X = x + b/3a$ とおいた. □

これより，$(**)$ の解法は本質的に 3 次方程式

$$X^3 - \frac{b^2 - 3ac}{3a^2}X - \frac{9abc - 27a^2d - 2b^3}{27a^3} = 0$$

を解くことにある．つまり定理 A.2 を用いて解を求め，それらが $X = \alpha_1, \alpha_2, \alpha_3$ とすると，$(**)$ の 3 つの解は $x = \alpha_1 - b/3a, \alpha_2 - b/3a, \alpha_3 - b/3a$ である.

A.2. **4 次方程式.** 4 次方程式を考察するが，4 次の項の係数をあらかじめ 1 にしておいて差し支えない．つまり $x^4+bx^3+cx^2+dx+e=0\dots(*)$ の解法を見る．$X=x-b/4$ とすると $(*)$ は $X^4+pX^2+qX+r=0$ と変形できる．ここで p,q,r は b,c,d,e を用いて表せる．

問題 A.4. p,q,r をそれぞれ b,c,d,e を用いて表せ．

つまり 4 次方程式の解法の本質は $x^4+px^2+qx+r=0$ という型の方程式の解法にある．この 4 次方程式を未知数 λ を用いて

$$(x^2+\lambda)^2=(2\lambda-p)x^2-qx+(\lambda^2-r)\dots(**)$$

と変形できることに注意する．この右辺が $(mx+n)^2$ の型になれば $(x^2+\lambda)^2=(mx+n)^2$ であるから，$(x^2+\lambda)=\pm(mx+n)$ となる．つまり 2 つの 2 次方程式 $(x^2+\lambda)=(mx+n)$ と $(x^2+\lambda)=-(mx+n)$ を解く事で 4 次方程式の解を得る事ができる．

そこで $(**)$ の右辺が $(mx+n)^2$ の型になる条件を求める．それはもちろん $(2\lambda-p)x^2-qx+(\lambda^2-r)$ の判別式を調べれば良い．すなわち

$$D:=(-q)^2-4(2\lambda-p)(\lambda^2-r)=0$$

である．この D は λ に関する 3 次方程式なので，上で扱った解法により解を求めることができる．そこで $D=0$ の解の一つを λ_0 とすると，$(**)$ は $(x^2+\lambda_0)^2=(mx+n)^2$ となり，あとは上の方法で 4 つの解を求めることができる．

例 A.5. 4 次方程式 $x^4+5x^2+2x+5=0$ の 4 つの解を求める．これが $(x^2+\lambda)^2=(mx+n)^2$ の型になるためには $D=(-2)^2-4(2\lambda-5)(\lambda^2-5)=0$ をみたさなくてはならない．また明らかに $\lambda=2$ はこの方程式の解の一つである．

このとき 4 次方程式 $x^4+5x^2+2x+5=0$ は $(**)$ より

$$\begin{aligned}(x^2+2)^2&=-x^2-2x-1\\&=-(x+1)^2\end{aligned}$$

となる．つまり求める 4 つの解は

$$x^2+2=\sqrt{-1}(x+1),\quad x^2+2=-\sqrt{-1}(x+1)$$

を解けば得られる．実際それらは

$$\frac{\sqrt{-1}\pm\sqrt{4\sqrt{-1}-9}}{2},\quad \frac{-\sqrt{-1}\pm\sqrt{-4\sqrt{-1}-9}}{2}$$

である．

A.3. **対称群，対称式，交代式.** 今までと少し話しが変わるが，5 次以上の方程式を扱う準備をする．ここでは置換の復習をする．線形代数の授業で行列式を定義したが，そこに使われたものである．いまいちど線形代数の教科書を開くことを薦める．いくつか命題を準備するが，それらの証明は線形代数の本を参照されたし．

定義 A.6. n 文字からなる集合 $X_n:=\{1,2,\dots,n\}$ に対し，$\sigma: X_n\to X_n$ が全単射であるとき，σ を n 次の**置換**という．また n 次の置換全体を $\mathfrak{S}_n$ と記し，n 次**対称群**という．

記号を一つ設定する．$j\in X_n$ に対して $\sigma(j)=i_j$ のとき σ を

$$\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix}$$

と記す．

例 A.7. 2 次の置換は 2 文字の入れ替え，つまり 1 と 2 を入れ替えない置換と入れ替えかる置換の 2 種類である．従って 2 次対称群は集合としては

$$\mathfrak{S}_2=\left\{\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix},\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\}$$

である．同様に 3 次対称群は 6 個の置換から構成されており，

$$\mathfrak{S}_3=\left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$$

である．一般に $\mathfrak{S}_n$ は $n!$ 個の置換から成る．

さて $\mathfrak{S}_n$ に次のように演算を定める．$\sigma,\tau\in\mathfrak{S}_n$ に対し，積 $\sigma\tau$ を写像の合成として定める．すなわち $(\sigma\tau)(j):=\sigma(\tau(j))$ である．

例 A.8. $\mathfrak{S}_3$ で考える．

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

とすると，

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

である．これからも分かるように $\mathfrak{S}_n$ に定めたこの演算は非可換である．

定義 A.9. $\sigma \in \mathfrak{S}_n$ とする．σ が $i_1, i_2, \ldots, i_l$ 以外は動かさず，$i_1, i_2, \ldots, i_l$ を

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_l \mapsto i_1$$

と動かすとき，つまり，

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & i_1 & i_2 & \ldots & i_{l-1} & i_l & \ldots n \\ 1 & 2 & \ldots & i_2 & i_3 & \ldots & i_l & i_1 & \ldots n \end{pmatrix}$$

のとき σ を l 次の**巡回置換**という．特に 2 次の巡回置換を**互換**という．

以下では l 次の巡回置換を $\begin{pmatrix} i_1 & i_2 & \ldots & i_l \end{pmatrix}$ と略記する．

命題 A.10. 任意の置換は巡回置換の積で，また巡回置換は互換の積で表せる．そして置換を互換の積で表した時，その個数は一意に定まらないが個数の偶・奇は定まる．

この命題の証明は線形代数の教科書に任せる．

例 A.11.

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 1 & 8 & 7 & 4 & 2 \end{pmatrix} &= \begin{pmatrix} 1 & 3 & 6 & 7 & 4 \end{pmatrix} \begin{pmatrix} 2 & 5 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 8 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 8 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \end{aligned}$$

定義 A.12. 偶数個の互換で表せる置換を**偶置換**，奇数個の互換で表せる置換を**奇置換**という．

問題 A.13. 5 次の巡回置換は偶置換であることを示せ．

今までで準備した置換を用いて対称式と交代式を定義する．$x_1, x_2, \ldots, x_n$ を不定元とする多項式 $P(x_1, x_2, \ldots, x_n)$ と $\sigma \in \mathfrak{S}_n$ に対し，$\sigma(P)(x_1, x_2, \ldots, x_n) := P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ と定める．

例 A.14. $P(x_1, x_2, x_3) = x_1^2 + 2x_2 + 3x_3^3$，$\sigma = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ とすると，

$$\begin{aligned} \sigma(P)(x_1, x_2, \ldots, x_n) &= P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \\ &= P(x_2, x_3, x_1) \\ &= x_2^2 + 2x_3 + 3x_1^3 \end{aligned}$$

である．

定義 A.15. 任意の $\sigma \in \mathfrak{S}_n$ に対し，$\sigma(P)(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$ のとき $P(x_1, x_2, \ldots, x_n)$ を**対称式**という．

例 A.16. $P(x_1, x_2) = x_1 + x_2$ や $Q(x_1, x_2) = x_1 x_2$ はどちらも対称式である．

定義 A.17. $X, x_1, x_2, \ldots, x_n$ を不定元とした多項式 $(X - x_1)(X - x_2) \ldots (X - x_n)$ を考える．これを展開すると，

$$(X - x_1)(X - x_2) \ldots (X - x_n) = X^n + \sum_{k=1}^{n} (-1)^k \gamma_k(x_1, x_2, \ldots, x_n) X^{n-k}$$

と表せる．このとき $\gamma_k(x_1, x_2, \ldots, x_n)$ は対称式であり，特に**基本対称式**とよばれる．

問題 A.18. $\gamma_k(x_1, x_2, \ldots, x_n)$ が対称式であることを示せ．なお

$$\begin{aligned} \gamma_1(x_1, x_2, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\ \gamma_2(x_1, x_2, \ldots, x_n) &= x_1 x_2 + x_1 x_3 + \ldots x_1 x_n + x_2 x_3 + \cdots + x_2 x_n + \cdots + x_{n-1} x_n \\ &\vdots \\ \gamma_n(x_1, x_2, \ldots, x_n) &= x_1 x_2 \ldots x_n \end{aligned}$$

である．

定義 A.19. 多項式 $P(x_1, x_2, \ldots, x_n)$ が任意の互換 $\sigma = \begin{pmatrix} i & j \end{pmatrix}$ $(1 \leq i < j \leq n)$ に対し $\sigma(P)(x_1, x_2, \ldots, x_n) = -P(x_1, x_2, \ldots, x_n)$ となるとき，$P(x_1, x_2, \ldots, x_n)$ を**交代式**と言う．

例 A.20. $P(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$ は交代式である．

注意 A.21. 差積

$$\Delta(x_1, x_2, \ldots, x_n) = \prod_{1 \leq k < l \leq n} (x_k - x_l)$$

は交代式である．

これより次が従う．

命題 A.22. 対称式 $S_1(x_1, x_2, \ldots, x_n)$ と $S_2(x_1, x_2, \ldots, x_n)$ に対し，多項式 $P(x_1, x_2, \ldots, x_n)$ を

$$P(x_1, x_2, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n) + \Delta(x_1, x_2, \ldots, x_n) S_2(x_1, x_2, \ldots, x_n)$$

と定める．このとき $\sigma \in \mathfrak{S}_n$ が偶置換のとき

$$\sigma(P)(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$$

であり，$\sigma \in \mathfrak{S}_n$ が奇置換のとき

$$\sigma(P)(x_1, x_2, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n) - \Delta(x_1, x_2, \ldots, x_n) S_2(x_1, x_2, \ldots, x_n)$$

である．

A.4. 体の拡大.

定義もどき A.23. 集合 K 上に四則演算が定義され，分配法則などが成り立つとき，K を体という．

例 A.24. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体であるが，$\mathbb{Z}$ は割り算で閉じていない（1 と 2 は整数であるが，1/2 は整数でない）ので体ではない．

定義 A.25. K を体，$\alpha \notin K$ とする．

$$K(\alpha) := \left\{ \frac{a + b\alpha}{a' + b'\alpha} \middle| a, a', b, b' \in K \right\}$$

を K に α を**添加**してできた体という．また $K(\alpha)$ を K の**拡大体**という．

例 A.26. $\sqrt{2} \notin \mathbb{Q}$ なので,

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a+b\sqrt{2}}{a'+b'\sqrt{2}} \middle| a, a', b, b' \in \mathbb{Q} \right\}$$
$$= \{ s + t\sqrt{2} \mid s, t \in \mathbb{Q} \}$$

である．これより $\mathbb{Q}(\sqrt{2})$ を $\mathbb{Q}$ 上の 2 次元ベクトル空間とみなすことができる．もちろん基底は $\{1, \sqrt{2}\}$ である．また $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ である．

さて，そもそも我々が考えるべき問題は次である：

そもそもの問題

n 次方程式 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$ が与えられたとき，この方程式の解はどのような数であるか？

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ とする．このとき体 $K := \mathbb{Q}(a_0, a_1, \ldots, a_n)$ を方程式 $f(x) = 0$ の**定義体**という．一般に方程式 $f(x) = 0$ の解は K の拡大体に含まれる．（もちろん拡大しなくて良い場合もある．たとえば $x^2 - 3x + 2 = 0$ の解は $\mathbb{Q}$ に含まれている.）

例 A.27. 2 次方程式 $a_2 x^2 + a_1 x + a_0 = 0 \ldots (*)$ の解は

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}$$

で与えられる．$D = a_1^2 - 4a_2 a_0$ とすると，2 次方程式 $(*)$ の 2 つの解は $K := \mathbb{Q}(a_0, a_1, a_2)$ に $\sqrt{D}$ を添加してできる体 $K(\sqrt{D})$ に含まれる．

例 A.28. 3 次方程式 $a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ の解は $K = \mathbb{Q}(a_0, a_1, a_2, a_3)$ の中で $x^3 - px - q = 0 \ldots (**)$ と変形できた．つまり $p, q \in K$ であった．$D = q^2 - 4/27p^3$ とする．方程式 $(**)$ の解法を見ると，まず $K(\sqrt{D})$ を考え，次に $\frac{1}{2}\left(q + \sqrt{D}\right)$ の 3 乗根を考えた．この 3 乗根の一つを

$$\beta := \left(\frac{1}{2} \left(q + \sqrt{D} \right) \right)^{1/3}$$

とすると，残りの二つは $\omega\beta$ と $\omega^2\beta$ で与えられた．ここで ω は 1 の原始 3 乗根である．

定理 A.2 より 3 次方程式 $(**)$ の 3 つの解は K の拡大体 $L_1 = K(\sqrt{D})$ の拡大体 $L = K(\sqrt{D})(\beta, \omega\beta, \omega^2\beta) = L_1(\beta, \omega\beta, \omega^2\beta)$ に含まれる．L は体であるから $\omega = \omega\beta/\beta \in L$ であり，$L = L_1(\beta, \omega) = K(\sqrt{D}, \beta, \omega)$ である．

例 A.27 と例 A.28 より，2 次方程式と 3 次方程式の解法は，累乗根を定義体に次々と添加して体を拡大していくことで，与えられた方程式の解をすべて含む体を作ることと関係している．

問題 A.29. 4 次方程式で同じことをやれ．

定義 A.30. n 次方程式 $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \ldots (\heartsuit)$ が与えられた時，定義体 $K = \mathbb{Q}(a_0, a_1, \ldots, a_n)$ に何かしらの累乗根を添加してできる拡大体の列

$$K_0 = K \subset K_1 = K_0(\sqrt[m_1]{\alpha_1}) \subset K_2 = K_1(\sqrt[m_2]{\alpha_2}) \subset \cdots \subset K_l = K_{l-1}(\sqrt[m_l]{\alpha_l})$$

$(\alpha_j \in K_{j-1},\ j = 1, 2, \ldots, l)$ を考える．$(\heartsuit)$ の解がすべて K_l 含まれるように拡大列を取れるとき，n 次方程式 $(\heartsuit)$ は**四則演算と累乗根によって解ける**，または**代数的に解ける**という．

A.5. **5 次以上の方程式．** ここでは一般に 5 次以上の方程式は代数的に解けない，という事を見る．

定義 A.31. K を体とし，$\alpha_1, \alpha_2, \ldots, \alpha_n \notin K$ とする．0 でない任意の K 係数多項式 $f(x_1, \ldots, x_n)$ に対し，$f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ であるとき，$\alpha_1, \alpha_2, \ldots, \alpha_n$ は K 上**代数的独立**という．

例 A.32. π は $\mathbb{Q}$ 上代数的独立である．この事実は決して自明ではない．「円積問題」とよばれる古代の幾何学者を悩ませた問題とも密接に関係する．（というか，これが答え．）なお $\mathbb{Q}$ 上代数的独立な数は超越数とよばれる．

$\alpha_1, \alpha_2, \ldots, \alpha_n$ が K 上代数的独立のとき，気持ちとしては「$\alpha_1, \alpha_2, \ldots, \alpha_n$ を不定元のように思って良い」ということである．そこで

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) = x^n - \gamma_1 x^{n-1} + \gamma_2 x^{n-2} + \cdots + (-1)^n \gamma_n$$

を考えると，$\gamma_1, \gamma_2, \ldots, \gamma_n$ は $\alpha_1, \alpha_2, \ldots, \alpha_n$ の基本対称式であった．$\alpha_1, \alpha_2, \ldots, \alpha_n$ は K 上代数的独立なので $\gamma_1, \gamma_2, \ldots, \gamma_n$ も K 上代数的独立であることに注意する．つまり方程式 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ の係数 $a_1, a_2, \ldots, a_n$ が $\mathbb{Q}$ 上代数的独立とすると，$a_1, a_2, \ldots, a_n$ はこの方程式の解の基本対称式である．

ところで，2 次，3 次，4 次方程式の解法において，添加していった累乗根はその方程式の解に関する有理式のみであった．

例 A.33. 2 次方程式 $x^2 + a_1 x + a_0 = 0$ の解は

$$\alpha_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_0}}{2} \text{ と } \alpha_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_0}}{2}$$

であり，添加した累乗根は

$$\sqrt{a_1^2 - 4a_0} = \frac{\alpha_1 - \alpha_2}{2}$$

である．

問題 A.34. 3 次方程式と 4 次方程式でチェックせよ．

ここで一つの仮定の下に議論をすすめる．もちろんこの仮定は後で示すべきことである．

仮定

（5 次以上の）方程式が代数的に解けるとする．このとき定義体に添加すべき累乗根は解の有理式で表せる．

$a_1, a_2, \ldots, a_n$ が $\mathbb{Q}$ 上代数的独立とし，方程式 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ の解法を考察する．定義体は $K := \mathbb{Q}(a_1, a_2, \ldots, a_n)$ である．

補題 A.35. K の元は方程式の解 $x_1, x_2, \ldots, x_n$ の $\mathbb{Q}$ 係数対称式で表せる．

Proof. $a_1, a_2, \ldots, a_n$ が $x_1, x_2, \ldots, x_n$ の基本対称式で表せることは既にみた．$q \in \mathbb{Q}$ は対称式 $P(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} 0x_i^{m_i} + q$ で表せる． □

さて，これから K を拡大していくのだが，これに添加すべき累乗根を $\sqrt[p]{r}$ とする．ここで $r \in K$ であり，p は素数である．

補題 A.36. 最初に定義体に添加すべき累乗根は平方根である．すなわち $p = 2$ である．

Proof. 上の「仮定」により $\sqrt[p]{r}$ は $x_1, x_2, \ldots, x_n$ の有理式 $\varphi(x_1, x_2, \ldots, x_n)$ で表せ，さらに補題 A.35 より $\varphi^p(x_1, x_2, \ldots, x_n)$ は対称式である．もちろん $\sqrt[p]{r} \notin K$ であるから，$\varphi(x_1, x_2, \ldots, x_n)$ は対称式[18]ではない．

$\varphi(x_1, x_2, \ldots, x_n)$ は対称式ではないので，ある互換，たとえば $\begin{pmatrix}1 & 2\end{pmatrix}$ によって変わる．つまり

$$\begin{aligned}\begin{pmatrix}1 & 2\end{pmatrix}\varphi(x_1, x_2, \ldots, x_n) &= \varphi'(x_1, x_2, \ldots, x_n)\\ &\neq \varphi(x_1, x_2, \ldots, x_n)\end{aligned}$$

である．一方 $\varphi^p(x_1, x_2, \ldots, x_n)$ は対称式なので

$$\begin{aligned}\varphi'^p(x_1, x_2, \ldots, x_n) &= \left(\begin{pmatrix}1 & 2\end{pmatrix}\varphi(x_1, x_2, \ldots, x_n)\right)^p\\ &= (\varphi(x_2, x_1, \ldots, x_n))^p\\ &= \begin{pmatrix}1 & 2\end{pmatrix}\varphi^p(x_1, x_2, \ldots, x_n)\\ &= \varphi^p(x_1, x_2, \ldots, x_n)\end{aligned}$$

である．故に $\varphi'(x_1, x_2, \ldots, x_n) = \epsilon\varphi(x_1, x_2, \ldots, x_n) \ldots (\spadesuit)$ を得る．ここで ϵ は 1 の p 乗根である．ただし $\varphi'(x_1, x_2, \ldots, x_n) \neq \varphi(x_1, x_2, \ldots, x_n)$ であったので $\epsilon \neq 1$ である．

今 $x_1, x_2, \ldots, x_n$ は K 上代数的独立なので $(\spadesuit)$ は $x_1, x_2, \ldots, x_n$ に関する恒等式である．つまり x_1 と x_2 を入れ替えても $(\spadesuit)$ と同様の結果：$\varphi'(x_2, x_1, \ldots, x_n) = \epsilon\varphi(x_2, x_1, \ldots, x_n)$ を得る．これは $\begin{pmatrix}1 & 2\end{pmatrix}\varphi'(x_1, x_2, \ldots, x_n) = \epsilon\begin{pmatrix}1 & 2\end{pmatrix}\varphi(x_1, x_2, \ldots, x_n)$ を意味するが，$\varphi'(x_1, x_2, \ldots, x_n) = \begin{pmatrix}1 & 2\end{pmatrix}\varphi(x_1, x_2, \ldots, x_n)$

[18] 対称式は基本対称式を用いて表せることに注意.

であったことに注意すれば，$\varphi(x_1, x_2, \ldots, x_n) = \epsilon\varphi'(x_1, x_2, \ldots, x_n)$ を得る．これと (♠) を合わせると $\varphi(x_1, x_2, \ldots, x_n) = \epsilon^2\varphi(x_1, x_2, \ldots, x_n)$ である．すなわち $\epsilon = -1$（1 の 2 乗根）である．つまり $\sqrt[p]{r} = \sqrt{r}$ である．$\sqrt[p]{r}$ は最初に K に添加するものであったので，最初に用いる累乗根は平方根であることが分かった．さらにこの平方根は互換によって符号が変わるだけである．すなわち交代式でなくてはならない．以上により $K_1 = K(\sqrt{r})$ の元は $S_1 + \Delta S_2$ の形をしていることが分かった．ここで S_1 と S_2 は $x_1, x_2, \ldots, x_n$ の対称式であり，Δ は差積 $\Delta(x_1, x_2, \ldots, x_n) = \prod_{1\leq k<l\leq n}(x_k - x_l)$ である． □

次に K_1 に添加すべき元を $\sqrt[q]{r_1}$ とする．

補題 A.37. 次に添加すべき累乗根は 3 乗根である．すなわち $q = 3$ である．

Proof. $\sqrt[q]{r_1}$ を $x_1, x_2, \ldots, x_n$ で表す.「仮定」により $\sqrt[q]{r_1} = \psi(x_1, x_2, \ldots, x_n)$ とできるが，右辺は有理式であるが対称式ではない．つまり 3 次の巡回置換 $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ によって変わる．すなわち

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\psi = \psi' \neq \psi \ldots (\diamondsuit)$$

である．$r_1 = \psi^q(x_1, x_2, \ldots, x_n) \in K_1$ なので，これは対称式であり $\begin{pmatrix}1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}$ によって変わらない．すなわち $\psi^q = \psi'^q$ であり，$\psi' = \omega\psi$ を得る．ただし ω は 1 の q 乗根であり，$\omega \neq 1$ である．

$x_1, x_2, x_3, \ldots, x_n$ の恒等式 $(\psi' =)\psi(x_2, x_3, x_1, \ldots, x_n) = \omega\psi(x_1, x_2, x_3, \ldots, x_n)$ の両辺に置換 $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ を 2 回施すことで，

$$\psi(x_3, x_1, x_2, \ldots, x_n) = \omega\psi(x_2, x_3, x_1, \ldots, x_n)$$
$$\psi(x_1, x_2, x_3, \ldots, x_n) = \omega\psi(x_3, x_1, x_2, \ldots, x_n)$$

を得る．以上より $\psi(x_1, x_2, x_3, \ldots, x_n) = \omega^3\psi(x_1, x_2, x_3, \ldots, x_n)$ であり，$\omega^3 = 1$ すなわち $q = 3$ である． □

定理 A.38 (Abel)**.** 一般に，5 次以上の代数方程式は代数的に解けない．

Proof. $n \geq 5$ とし，5 つの解の巡回置換を考える．上の議論から ψ^3 は解の対称式であるから，この 5 次巡回置換によって変わらない．ψ が変わったとしても[19] $\omega\psi$ である（ω は 1 の 3 乗根）．この巡回置換を 5 回行うと，上と同様の議論により $\omega^5 = 1$ を得る．すなわち $\omega = 1$ となり，ψ は 5 次の巡回置換では不変である．しかし

$$\begin{pmatrix} 3 & 2 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

であるから，ψ が $\begin{pmatrix} 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ と $\begin{pmatrix} 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ によって不変であれば $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ でも不変である．しかしこれは $(\diamondsuit)$ に反する．

問題 A.13 により，この 5 つの解の巡回置換は偶置換であることに注意する．以上の議論により，$n \geq 5$ のとき ψ が偶置換で不変ではなく，ψ^q が偶置換で不変であるという解の有理式 ψ は存在しないことが分かる．つまりこのとき方程式 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ が代数的に解けるとすると，それは平方根のみで解かれてしまうことになり，解としては $x_i = S_1 + \Delta S_2$ の形になる．しかしこれは $x_1, x_2, \ldots, x_n$ の恒等式ではない．つまり 5 次以上の代数方程式は一般に代数的に解けない． □

以上の議論は「仮定」の下に行われた．ここに一つ課題が残っている．

問題 A.39. 「仮定」の主張を示せ．

Appendix B. 集合の濃度

さりげなく補題 8.6 で用いるので，ごく簡単に「集合の濃度」について触れておく．補題 8.6 は有限集合を扱っているので，濃度という概念を持ち出す必要もないのだが．カリキュラムの都合上，ここで簡単に紹介する．

定義 B.1. 集合 X と Y の間に全単射が存在するとき，X と Y は**対等**という．

命題 B.2. 集合 X と Y が対等のとき $X \sim Y$ と記す．このとき関係 $\sim$ は同値関係である．つまり

[19] ψ は対称式ではないが，特別な置換に関しては不変になるかもしれない．

(1) $X \sim X$
(2) $X \sim Y$ ならば $Y \sim X$
(3) $X \sim Y$ かつ $Y \sim Z$ ならば $X \sim Z$

をみたす.

Proof. (1) 恒等写像は全単射である．(2) 全単射の逆写像も全単射である．(3) 全単射の合成も全単射である． □

定義 B.3. 集合 X と Y が対等のとき，X と Y の**濃度**が等しいといい，$\sharp X = \sharp Y$ と記す．また X が n 個の元からなる集合 $X_n := \{1, 2, \ldots, n\}$ と対等なとき，X を**有限集合**と呼び，$\sharp X = n$ と表す．X が有限集合でないときは**無限集合**と言う.

命題 B.4. 全単射 $f : X_n \to X_m$ が存在するとき，$n = m$ である.

Proof. n に関する帰納法で示す．$n = 1$ ならば $m = 1$ は明らか．$s > 1$ として，$f : X_s \to X_t$ が全単射ならば $s = t$ と仮定する．また全単射 $f : X_{s+1} \to X_{t+1}$ に対し $f(s+1) = l \in X_{t+1}$ とする．$g : X_{t+1} \to X_{t+1}$ を

$$g(i) = \begin{cases} i & i \neq l, t+1 \\ l & i = t+1 \\ t+1 & i = l \end{cases}$$

で定めると，これは全単射である（$g^2 = id_{X_{t+1}}$ である）．従って f と g の合成 $g \circ f$ も全単射である.

さらに $g \circ f(s+1) = g(l) = t+1$ なので $g \circ f$ は全単射

$$X_s = X_{s+1} \setminus \{s+1\} \to X_t = X_{t+1} \setminus \{t+1\}$$

を引き起こす．帰納法の仮定より $s = t$ なので，以上より $s+1 = t+1$ である. □

命題 B.5. $\mathbb{N}$ は無限集合である.

Proof. n に関する帰納法で全単射 $f : X_n \to \mathbb{N}$ が存在しない事を示す．明らかに全単射 $X_1 = \{1\} \to \mathbb{N}$ は存在しない．$k > 1$ として全単射

$X_k \to \mathbb{N}$ が存在しないと仮定する．さて，$f : X_{k+1} \to \mathbb{N}$ を全単射とし，$f(k+1) = k+1$ とする．$g : \mathbb{N} \setminus \{k+1\} \to \mathbb{N}$ を

$$g(i) = \begin{cases} i & i < k+1 \\ i-1 & i > k+1 \end{cases}$$

と定めると g は全単射であり，f を $X_k = X_{k+1} \setminus \{k+1\}$ を制限した写像

$$f_{|X_k} : X_k = X_{k+1} \setminus \{k+1\} \to \mathbb{N} \setminus \{k+1\}$$

も全単射でなので，合成 $g \circ f_{|X_k} : X_k \to \mathbb{N}$ も全単射である．しかしこれは帰納法の仮定に反する．従って $f : X_n \to \mathbb{N}$ という全単射は存在しない． □

有限集合の場合，その濃度は元の個数と言ってしまえば良いのだが，無限集合の場合は「個数」というのは適切ではないように思える．そこで「濃度」という言葉を用いる．

定義 B.6. X を集合とする．全単射 $\mathbb{N} \to X$ が存在するとき，X を**可算無限集合**という．特に X が有限集合または可算無限集合のとき，X は**（高々）可算（集合）**という．

命題 B.7. $\mathbb{Z}$ と $\mathbb{N}$ は対等である．つまり $\mathbb{Z}$ は高々可算集合である．

Proof. $f : \mathbb{N} \to \mathbb{Z}$ を

$$f(n) = \begin{cases} m-1 & n = 2m \\ -m & n = 2m-1 \end{cases}$$

と定めると，これは全単射である． □

命題 B.8. $\mathbb{Q}$ と $\mathbb{N}$ は対等である．つまり $\mathbb{Q}$ は高々可算集合である．

Proof. これはレポート問題とする． □

以上によって $\sharp\mathbb{N} = \sharp\mathbb{Z} = \sharp\mathbb{Q}$ であることが分かった．可算でない集合の典型例は次である．「対角線論法」と呼ばれるもので，これをやらなければ「集合論を勉強した」と言ってはいけないレベルの話である．

定理 B.9 (Cantor)**.** 開区間 $I := (0,1)$ は可算集合ではない.

Proof. I の任意の元は小数点を用いて $0.a_1a_2\dots a_n\dots$ と表せる．ここで $a_i \in \{0,1,2,\dots,9\}$ である．もし I が可算集合であれば，$\mathbb{N}$ の元と一対一に対応する．$n \in \mathbb{N}$ に対応する元を $b_n \in I$ とし，

$$\begin{aligned} b_1 &= 0.a_{11}a_{12}a_{13}\dots a_{1n}\dots \\ b_2 &= 0.a_{21}a_{22}a_{23}\dots a_{2n}\dots \\ &\vdots \\ b_n &= 0.a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots \\ &\vdots \end{aligned}$$

と表す.（ここで $a_{ij} \in \{0,1,2,\dots,9\}$ である.）このとき I の任意の元は b_k のいずれかであることに注意する.

さて，$c = 0.c_1c_2\dots c_n\dots$ を考える．ただし $c_k \in \{0,1,2,\dots,9\}$ は $c_k \neq a_{kk}$ とする．このとき $c \in I$ であるから，$b_j = c$ をみたす I の元 $b_j \in I$ が存在する．しかし c の作り方から $c_j \neq a_{jj}$ である．これは矛盾．従って I は可算ではない. □

命題 B.10. 次が成り立つ.

(1) $\sharp[a,b] = \sharp[c,d]$ および $\sharp(a,b) = \sharp(c,d)$
(2) $\sharp(a,b) = \sharp\mathbb{R}$

Proof. (1) $f : [a,b] \to [c,d]$ $\left(x \mapsto \dfrac{d-c}{b-a}(x-a)+c\right)$ は全単射である．これを $(a,b) \to (c,d)$ に制限すれば，これも全単射である．(2) $g : (-1,1) \to \mathbb{R}$ $(x \mapsto x/(1-x^2))$ は全単射である. □

以上によって $\sharp\mathbb{N} \neq \sharp\mathbb{R}$ である.

References

[1] 青木 昇，素数と 2 次体の整数論，共立出版.
[2] 楫 元，工学系のための初等整数論入門，培風館.
[3] 高木 貞治，代数学講義，共立出版.
[4] 高木 貞治，初等整数論講義，共立出版.

[5] 上野 健爾，代数入門 (現代数学への入門)，岩波書店.

Department of Mathematics, Tokai University, 4-1-1, Kitakaname, Hiratsuka, Kanagawa, 259-1292, JAPAN
Email address: taki@tsc.u-tokai.ac.jp
URL: http://www2.sm.u-tokai.ac.jp/taki/