符号と暗号の数理

花木 章秀

2008 年度後期
(2008/09/30)

目次

はじめに

現在の我々の生活において、インターネットや携帯電話などを用いた通信は必要不可欠なものになりつつある。しかし、伝えられるべき情報が通信の際に生じる雑音などによって正確に伝わらなかったとしたら、どうだろう。例えば 10,000 円と思って購入したものが、実は 1,000,000 円で、その間違えが業者のミスや詐欺などではなく、通信のエラーだったとしたらどうだろう。法律的なことは知らないので、何とも言えないが、このようなことが起これば、購入した方だけでなく、販売する業者も困るであろう。そこでこのようなことを避けるために、現在の通信のほとんどで、簡単な誤りを検出したり、また訂正するための工夫がこらされている。これが「符号」(code) と呼ばれるものである。

また、例えば携帯電話による通信の場合、無線による通信なので、原理的にその通信のすべてを盗聴することができる。インターネットも、その通信には当事者同士以外の多くの計算機を通過するため、その計算機の管理者は通信を盗聴することができる。インターネットショッピングなどでクレジットカードの番号などを入力すれば、それはすべて他人に知られてしまうことになるのである。このような場合には、盗聴を防ぐことは原理的にできない。そこで用いられるのが「暗号」(cryptography) である。適切な暗号を用いれば、その通信のすべて、鍵の配送までもが盗聴されたとしても、その内容を知られることはない。

この講義では多くの人が意識することなく利用している「符号」と「暗号」について、特にその数学的な理論についての理解を目標とする。実用的なものはやや複雑になるので、比較的容易に、しかしながら本質的なことを理解できるように話題を選んだ。仮定する知識は特になく、誰でも理解できるように準備したつもりではあるが、ある程度の計算能力がないと理解が難しいかも知れない。「暗号」を学ぶときに現れる大きな数の計算では電卓やパソコンなどを用いて計算した方が良いだろう。

Chapter 1

ISBN

一般に書店で売られている書籍には ISBN (International Standard Book Number, 国際標準図書番号) という記号が付けられている (通常は本の後に書いてある)。この記号は書籍を特定するだけでなく、その番号が正しいかどうかを判定する機能も持っている。ISBN は 2007 年より新しい規格に変更されたが、ここでは 2006 年までの古い規格を扱うことにする。

例えば「ISBN 4-7973-0148-1」と書いてある本がある。ハイフンは今は意味がないと思って良い。すなわち ISBN は 10 個の数字からなる (違う場合もあるが、それはあとで説明する)。このうち、はじめの 9 個の数字だけで本は特定される。最後の数字は誤りを見つけるために付けられているのである。似たような仕組みは色々なところで見られる。例えば学生の学籍番号は、例えば「04S1099Z」のようになっていて、最後のアルファベットが同様の役目を果たしている。この章では ISBN の場合に、どのように最後の記号が決められているのか、なぜそれによって誤りを見つけることができるのかを解説する。

1.1 ISBN の決め方

ISBN は先に述べたように 10 個の数字からなる。このうちのはじめの 9 個は本を特定するためにあり、どのような数字の並びでも良い。最後の数字の決め方を説明しよう。まず、先ほどの例「ISBN 4-7973-0148-?」を考える。ただし最後の数字は知らないものとして ? と書いておく。9 つの数字に順に 1 から 9 をかけて、その和を取る。

$$4\times1+7\times2+9\times3+7\times4+3\times5+0\times6+1\times7+4\times8+8\times9=199$$

この答え 199 を 11 で割って 18 余り 1 と計算する。この余り 1 を最後の数字とするのである。

問 1.1.1. ISBN 「479730267?」、「479790267?」、「084933988?」の最後の数字を決めなさい。

さて、ここで問題が起こる。11 で割った余りを考えるので、その値は 0 から 10 のいずれかになる。もし余りが 10 となると困ってしまう。そこでこの場合は最後に 10 の代わりに X という記号を書くことになっている。したがって正確には「ISBN は 10 個の数字の並びであるが、最後の桁は数字ではなく X である場合もある」と言える。

1.2 一つの記号が読めないとき

今説明したのは、言い換えると「ISBN の最後の一つが分からなくても計算によって求めることができる」ということである。最後とは限らない他の部分が分からなかったらどうであろうか。これを考えるために、一般的な考察をする。ISBN を

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$$

とする。ただし $a_1, \cdots, a_9$ は 0 から 9 までの整数で、a_{10} は 0 から 10 までの整数であるとする (記号 X を 10 と思えば良い)。このとき前に説明したのは、総和記号 $\sum$ を用いて

$$\left(\sum_{1=1}^{9} ia_i\right) \div 11 =? \ \cdots \ a_{10}$$

ということである。? はどんな数でも良い。さらに言い換えると

$$\sum_{1=1}^{9} ia_i - a_{10}$$

が 11 で割り切れるということである。この式に $11 \times a_{10}$ を足しても 11 で割り切れるという性質は変わらない。そうすると、これは

$$\sum_{1=1}^{9} ia_i + 10 \times a_{10} = \sum_{1=1}^{10} ia_i$$

が 11 で割り切れるということと同じになる。これまで最後の数字を特別扱いしてきたが、この式を見ると他の数字と同じように扱えるように思える。実際にそうなのである。

さて、ここで記述を容易にするために記号を導入しよう。正の整数 n を一つ固定する。二つの正の整数 a, b を n で割った余りが等しいとき

$$a \equiv b \pmod{n}$$

と書いて a **と** b **は** n **を法として合同である**という。またこのような式を**合同式**という。すぐ分かるように $a \equiv b \pmod{n}$ であるということは、ある整数 ℓ があって $a = b + n\ell$ と書けるということと同じである。この記号を用いると $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ が正しい ISBN であることは

$$\sum_{1=1}^{10} ia_i \equiv 0 \pmod{11}$$

であることと同じになる。

さて一つの記号が読めなかった場合を考えよう。例えば $4797a_501481$ を考えよう (はじめの例で 5 番目の記号が読めないとしたもの)。a_5 以外の部分は計算できるので、計算してまとめると

$$5a_5 + 249 \equiv 5a_5 + 7 \equiv 0 \pmod{11}$$

となる。両辺に 4 を足して

$$5a_5 \equiv 4 \pmod{11}$$

を得る。普通の方程式ならば両辺を 5 で割って a_5 を求めることができるが、今は整数だけを考えているので右辺の 4 を 5 で割ることはできない。a_5 には 0 から 9 までの整数が入るので、全部確かめてみれば

$$5 \times 3 = 15 \equiv 4 \pmod{11}$$

だけがこの条件を満たし $a_5 = 3$ とわかる。

問 1.2.1. ISBN 123?567890 と 123456?890 の ? の数字を求めよ。

1.3 合同一次方程式

ISBN の一つの文字が読めないときには

$$ax \equiv b \pmod{11}$$

という未知数 x についての方程式のようなものを解けば良いことが分かった。このような式を**合同方程式**という。特にこの場合は未知数 x についての一次式なので**合同一次方程式**という。ここでは合同一次方程式について考える。

例題 1.3.1. 合同一次方程式 $3x \equiv 1 \pmod{10}$ の解を求めよ。

解答. x に $0, 1, 2, 3, \cdots$ と順番に代入して計算すると

$$\begin{aligned} 3 \times 7 &\equiv 1 \pmod{10} \\ 3 \times 17 &\equiv 1 \pmod{10} \\ 3 \times 27 &\equiv 1 \pmod{10} \\ &\cdots \end{aligned}$$

となり $x = 7, 17, 27, \cdots$ などが解として求まる。実際 ℓ を正の整数とすると

$$3 \times (7 + 10\ell) = 21 + 30\ell \equiv 1 \pmod{10}$$

となり $x = 7 + 10\ell$ はすべて解である。

次が成り立つ。

命題 1.3.2. 合同一次方程式 $ax \equiv b \pmod{n}$ の一つの解を x_0 とする。このとき $x_1 \equiv x_0 \pmod{n}$ となるすべての x_1 はこの合同一次方程式の解である。

証明. $x_1 \equiv x_0 \pmod{n}$ のとき、ある整数 ℓ があって $x_1 = x_0 + \ell n$ と書ける。よって

$$ax_1 = a(x_0 + n\ell) = ax_0 + an\ell \equiv ax_0 \equiv b \pmod{n}$$

となる。 □

すぐに分かるようにどんな正の整数も n を法として 0 から $n-1$ までの整数のどれかと合同である。したがって合同方程式の解は 0 から $n-1$ までの整数で求めればよい (n を法として求めれば良い、ともいう)。

問 1.3.3. 合同一次方程式 $4x \equiv 1 \pmod 9$ の解を (9 を法として) 求めよ。

例題 1.3.4. 合同一次方程式 $2x \equiv 4 \pmod 6$, $2x \equiv 1 \pmod 6$ の解を求めよ。

解答. 6 を法として求めれば良いので 0 から 5 までの数について計算してみる。

$$\begin{aligned} 2 \times 0 &\equiv 0 \pmod 6 \\ 2 \times 1 &\equiv 2 \pmod 6 \\ 2 \times 2 &\equiv 4 \pmod 6 \\ 2 \times 3 &\equiv 0 \pmod 6 \\ 2 \times 4 &\equiv 2 \pmod 6 \\ 2 \times 5 &\equiv 4 \pmod 6 \end{aligned}$$

これによって $2x \equiv 4 \pmod 6$ の解は $x = 2, 5$ であり $2x \equiv 1 \pmod 6$ の解は存在しないことが分かる。

この例から分かるように、合同一次方程式では解はいつでも唯一つ存在するという訳ではない。ISBN に戻って考えると、計算によって得られた合同一次方程式は常に解を持たなくてはならず、また唯一つの解を持つことが要求される。したがって合同一次方程式は「**どのような条件の下で解を持つのか**」、また「**どのような条件の下で唯一つの解を持つのか**」という問題を考える必要がある。

合同一次方程式 $ax \equiv b \pmod n$ が解を持つということは

$$ax + ny = b$$

となる整数 x, y が存在するということと同じである。これについて次のよく知られた定理がある。

定理 1.3.5. a, b を正の整数とする。d を a と b の最大公約数とすると、ある整数 x, y があって

$$ax + by = d$$

となる。

(ここではこの定理の証明はしないが、後で条件を満たす x, y の計算法を紹介する。) a と b の最大公約数 (greatest common divisor) を $\gcd(a, b)$ と書くことにする。もしも m が $d = \gcd(a, b)$ の倍数であるならば $m = d\ell$ と書けて、$ax_0 + by_0 = d$ を満たす x_0, y_0 に対して $a(x_0\ell) + b(y_0\ell) = d\ell = m$ となるから $ax + by = m$ を満たす整数 $x = x_0\ell$, $y = y_0\ell$ は存在する。もし m が d の倍数でないならば $ax + by = m$ の右辺 は d で割り切れず、左辺は常に d で割り切れるので、このような整数 x, y は存在しない。まとめると次の結果を得る。

定理 1.3.6. a, b を正の整数とし、$d = \gcd(a, b)$ とする。

$$ax + by = m$$

を満たす整数 x, y が存在するための必要十分条件は d が m を割り切ることである。

定理 1.3.7. 合同一次方程式 $ax \equiv b \pmod{n}$ が解を持つための必要十分条件は $\gcd(a, n)$ が b を割り切ることである。

次に合同一次方程式 $ax \equiv b \pmod{n}$ が唯一つの解を持つための条件を考えよう。$d = \gcd(a, n)$ とおき $d \neq 1$ とする。$a = a_o d$, $n = n_0 d$ とする。$0 < n_0 < n$ であることに注意しておく。x_0 を $ax \equiv b \pmod{n}$ の一つの解とする。このとき

$$a(x_0 + n_0) = ax_0 + a_0 d n_0 = ax_0 + a_0 n \equiv ax_0 \equiv b \pmod{n}$$

となり $x = x_0 + n_0$ も解である。しかし $0 < n_0 < n$ であるので $x_0 + n_0 \not\equiv x_0 \pmod{n}$ であり、このときの解は唯一つではない。

次に $d = \gcd(a, n) = 1$ の場合を考える。x_0, x_1 を共に $ax \equiv b \pmod{n}$ の解とする。このとき $ax_0 \equiv b \pmod{n}$, $ax_1 \equiv b \pmod{n}$ であるが両辺を引き算して

$$a(x_0 - x_1) \equiv 0 \pmod{n}$$

である。これは $a(x_0 - x_1)$ が n で割りきれることを意味するが a は n と互いに素なので $x_0 - x_1$ が n で割りきれる。よって $x_0 \equiv x_1 \pmod{n}$ であり、このとき $ax \equiv b \pmod{n}$ の解は n を法として一意的である。

以上をまとめて次を得る。

定理 1.3.8. 合同一次方程式 $ax \equiv b \pmod{n}$ が唯一つの解を持つための必要十分条件は $\gcd(a, n) = 1$ となることである。特に n が素数で $a \not\equiv 0 \pmod{n}$ ならば $ax \equiv b \pmod{n}$ は唯一つの解を持つ。

問 1.3.9. $7x + 9y = 1$ となる整数 x, y を求めよ。

問 1.3.10. $14x + 6y = 4$ となる整数 x, y を求めよ。

問 1.3.11. $14x + 6y = 1$ となる整数 x, y を求めよ。

ISBN では素数 11 を法として考えるので、この定理により常に唯一つの解を持つことが保証されるのである。ISBN は 10 個の記号の列を用いるが、仮に 9 個や 11 個の記号の列を用いると $10 = 9 + 1$ や $12 = 11 + 1$ が素数ではないので、計算がうまく行かないことが分かる。

一般に合同一次方程式 $ax \equiv b \pmod{n}$ が唯一つの解を持つとしても、a, b, n が大きいときには、それを求めるのは容易ではない。これは後に学ぶ**ユークリッドの互除法**を用いて効率的に計算できる。

1.4 ISBN の能力の限界

書店などで、注文された書籍を ISBN で確認しようとしたとする。実際には一文字だけが読めないということは多くないだろう。予想されるのは注文をした人の書き間違えである。一文字だけ書き違えているならば ISBN の満たす合同式を満たさなくなり、それが誤りであることを確実に検出できる。二文字書き違えた場合は、検出できない場合もある。しかし実際には書籍名なども同時に伝えているので、大きな問題はない。また ISBN では誤りを検出することはできても、それを訂正することはできない。例えば 1234567890 は誤った ISBN である。また一文字だけ書き違えていることが分かっているとする。これだけの情報が得られても、正しい ISBN は分からない。例えば 123456789X や 2234567890 はこの番号と一文字しか違わない正しい ISBN なのである。(誤りの位置を決めれば、それから正しい ISBN が作れるので誤った ISBN と一文字しか違わない番号は 10 個作れる。ただし 10 桁目以外にも X が現れることがあると、それは誤りであると判断できる。上の例は誤り位置を 10 番目、1 番目として計算したものである。しかし正しい ISBN を一文字書き換えると、必ず誤った ISBN になってしまうのである。)

以上のように ISBN は、それほど高い性能を持ったものではないことがわかる。しかし誤りを訂正したり、複数の誤りを検出したりするためには更に多くの情報を付け加える必要があり、効率的ではない。誤り訂正 (検出) 能力と利用効率を考えて、用途に応じたものを使うのがよく、書籍を表すには ISBN は適当であると言ってもよいであろう。

Chapter 2

誤り訂正符号

ISBN では一つの誤りを検出することができた。誤りが検出されれば、注文者に聞き直すなどすれば良いので、書籍を分類するためにはこれで十分と考えられる。同様にスーパーマーケットなどの商品に付けられている「バーコード」も誤り検出能力を持っている。(バーコードがうまく読み取れないときに、何度も読み取りの機械をあてているときがあるが、これは聞き直していることと同じである。) しかし情報を聞き直すことができない場合もある。例えばテレビやラジオでは、情報は一方的に入ってきて、仮に誤りを検出したとしてもこちらから聞き直すことはできない。そこで誤りを検出するだけでなく訂正する能力を持った仕組みが必要となる。これを**誤り訂正符号**という。ここでは簡単であるが実用的な誤り訂正符号である**ハミング符号** (Hamming code) について解説する。

2.1 ハミング符号を理解するための準備

誤り訂正符号の多くは、その操作が計算機によってなされる。計算機内ではすべての情報が 0 と 1 の列で表されるため、そこで利用される数学は 0 と 1 だけを使った特別な数学である。まずはこれを説明する。$\mathbb{F}_2 = \{0, 1\}$ とおいてこれを**二元体**という。0 と 1 だけを使った計算を $\mathbb{F}_2$ 上の計算などということにする。$\mathbb{F}_2$ 上では以下のように足し算と掛け算が行われる。

$$\begin{array}{llll} 0+0=0, & 0+1=1, & 1+0=1, & \boxed{1+1=0} \\ 0\times 0=0, & 0\times 1=0, & 1\times 0=0, & 1\times 1=1 \end{array}$$

普通と違うのは $1+1=2$ の部分で、この世界には 2 はないので 0 としている。またこれは偶数を 0、奇数を 1 とした計算と同じである。

$$\begin{array}{llll} \text{偶数}+\text{偶数}=\text{偶数}, & \text{偶数}+\text{奇数}=\text{奇数}, & \text{奇数}+\text{偶数}=\text{奇数}, & \text{奇数}+\text{奇数}=\text{偶数} \\ \text{偶数}\times\text{偶数}=\text{偶数}, & \text{偶数}\times\text{奇数}=\text{偶数}, & \text{奇数}\times\text{偶数}=\text{偶数}, & \text{奇数}\times\text{奇数}=\text{奇数} \end{array}$$

引き算は足し算と同じになる。なぜならば、この世界では $2 = 1+1 = 0$ なので $a+a = 2a = 0\times a = 0$ となり、移項して $a = -a$ が成り立つからである。また割り算はほとんど意味がない。普通の数と同じように 0 で割ることは考えてはいけないので、1 で割る

ことしかできず、この場合何もしないのと同じだからである。しかし実際には「割り算ができる」ということがとても重要な性質なのである。

少し一般的に考えよう。上記の $\mathbb{F}_2$ における計算は、言い換えると「2 で割った余りだけを考えている」ということになる。すなわち合同式の考え方と同じなのである。一般に、正の整数 n に対して n で割った余りだけを考えて $\{0, 1, \cdots, n-1\}$ だけの数の世界を考えよう。この世界でも足し算、引き算、掛け算は問題なく考えることができる。しかし一般に割り算は考えることができない。なぜならば合同一次方程式 $ax \equiv b \pmod{n}$ は常に解を持つわけではないからである (割り算ができるならば両辺を a で割れば解が得られる)。しかし n が素数ならば、定理 1.3.8 より合同一次方程式は常に唯一つの解をもつ。n が素数の場合を考えよう。このとき $ax \equiv 1 \pmod{n}$ は解 c を持つ。c はこの世界で $\dfrac{1}{a}$ の役割をもつので、a で割るということを c を掛けると考えてよく、この場合には割り算も問題なく考えることができる。一般に素数 p に対して $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ にこのような四則演算を定義して、これを p **元体**という。$\mathbb{F}_2$ は p として素数 2 を考えた場合である。

一般に四則演算が問題なく行える数の集まりを**体**という。例えば、有理数全体の集合、実数全体の集合、複素数全体の集合、などは体である。また整数全体の集合は割り算ができない (割り算をすると整数でなくなってしまう) ので体ではない。特に p 元体のように有限個の要素しか持たない体を**有限体**という。体の上では四則演算だけを基に成り立っている多くの数学理論がそのまま成り立つ。例えば、この後で述べるベクトルや行列の計算も普通の数と同じように行うことができる。

いくつかの数字を一列に並べて書いてカッコでくくったものを**ベクトル**という。特に数字を横に並べたとき**行ベクトル**、数字を縦に並べたとき**列ベクトル**という。また数字を n 個並べたとき n **次元ベクトル**という。例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

はそれぞれ 4 次元行ベクトル、3 次元列ベクトルである。すべての成分が 0 であるベクトルを**零ベクトル**といい $\mathbf{0}$ と書く。

同じ次元の二つのベクトルの足し算、引き算は、対応する成分ごとに行う。例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & -1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 & 6 \end{pmatrix}$$

である。

同じ次元の二つのベクトルの**内積**とは、対応する成分どうしをかけて、その和をとったものをいう。例えば $(1\ 2\ 3\ 4)$ と $(1\ -1\ 0\ 2)$ の内積は

$$1 \times 1 \ + \ 2 \times (-1) \ + \ 3 \times 0 \ + \ 4 \times 2 \ = \ 7$$

である。二つのベクトル $\boldsymbol{u}, \boldsymbol{v}$ に対して、その内積を $(\boldsymbol{u}, \boldsymbol{v})$ と表す。$(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{v}, \boldsymbol{u})$ が成り立つことは明らかであろう。$(\boldsymbol{u}, \boldsymbol{v}) = 0$ のとき $\boldsymbol{u}$ と $\boldsymbol{v}$ は**直交する**という。

問 2.1.1. O を原点とする xy-平面上に二点 $\mathrm{A}(a, b)$, $\mathrm{B}(c, d)$ をとる。線分 OA と OB が (普通の意味で) 直交するためにはベクトル $(a\ b)$ と $(c\ d)$ が直交することが必要十分であることを示せ。また 3 次元の場合にも同様のことを考えよ。

問 2.1.2. $(\boldsymbol{u}, \boldsymbol{v}+\boldsymbol{w}) = (\boldsymbol{u}, \boldsymbol{v}) + (\boldsymbol{u}, \boldsymbol{w})$ であることを示せ。(特に $(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{w}) = 0$ ならば $(\boldsymbol{u}, \boldsymbol{v}+\boldsymbol{w}) = 0$ である。)

いくつかの数を長方形に並べたものを**行列**という。縦に m 個、横に n 個の数字を並べたとき、特に $m \times n$ **行列**という。例えば次の例は 2×3 行列である。

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

行列の横の並びを**行**といい、縦の並びを**列**という。行は順番に第 1 行、第 2 行、などといい、列は順番に第 1 列、第 2 列、などという。

$$\begin{array}{c} \\ \text{第 1 行} \\ \text{第 2 行} \\ \text{第 3 行} \end{array} \begin{array}{c} \begin{array}{ccc} \text{第 1 列} & \text{第 2 列} & \text{第 3 列} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 2 & 3 \end{pmatrix} \end{array}$$

第 i 行で第 j 列の位置にある数をこの行列の (i,j)-**成分**という。すべての成分が 0 である行列を**零行列**といい $\mathbf{0}$ と書く。

$m \times n$ 行列 A に対して、その行と列を入れ替えた行列を A の**転置行列**といい ${}^tA$ と書く。このとき ${}^tA$ は $n \times m$ 行列で、その (i,j)-成分は A の (j,i)-成分である。

二つの $m \times n$ 行列の足し算と引き算はベクトルの場合と同じように対応する成分どうしで足し算、引き算を行う。行列の掛け算はやや難しい。$\ell \times m$ 行列 M と $m \times n$ 行列 N に対して、その積 MN は $\ell \times n$ 行列で、その (i,j) 成分は M の i 行と N の j 列の (ベクトルとしての) 内積で定める (正確には、そのいずれかを転置して、その内積をとる)。具体例を見た方が分かりやすいだろう。例えば

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 5 \\ 0 & 9 \end{pmatrix}$$

である。この場合 2×3 行列と 3×2 行列の積なので 2×2 行列となる。左から掛ける行列の列の数と、右から掛ける行列の行の数が一致しないときは内積が計算できないので、積は考えられない。

問 2.1.3. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \end{pmatrix}$ を計算しなさい。

ベクトルは行列の特別なものと考えることができる。n 次元行ベクトルは $1 \times n$ 行列、n 次元列ベクトルは $n \times 1$ 行列である。$m \times n$ 行列と n 次元列ベクトル ($n \times 1$ 行列) の積は m 次元列ベクトル ($m \times 1$ 行列) であり、ベクトルに行列を掛けることによって、ベクトルの次元を変えることができる。この事実は符号理論で重要な役割を果たす。

これまで、ベクトルや行列で用いる数は普通の数であったが、$\mathbb{F}_2$ 上でも全く同じことができる。

問 2.1.4. $\mathbb{F}_2$ 上で $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ を計算しなさい。

問 2.1.5. 行列の演算に関して

$$\begin{aligned} \text{積の結合法則} &: (AB)C = A(BC) \\ \text{分配法則} &: (A+B)C = AC + BC, \quad A(B+C) = AB + AC \end{aligned}$$

が成り立つことを示せ。

$n \times n$ 行列で、その対角線上の成分は 1, その他の成分はすべて 0 であるものを n **次の単位行列**といい I_n と書くことにする。

問 2.1.6. $\ell \times n$ 行列 M, $n \times m$ 行列 N について $MI_n = M$, $I_nN = N$ が成り立つことを示せ。

2.2 ハミング符号

「誤り訂正符号」の理論とは情報通信の際に、何らかの付加的な情報を同時に送ることで、通信に「雑音」が入ったとしても正しい情報を得ることができるようにする理論である。これは現在の電子通信機器にはほとんどすべてに用いられている「技術」である。付加的な情報を付け加えるのに、前節で学んだ行列とベクトルとの積が用いられる。与えられたベクトルに適当な行列をかけることによって、ベクトルの長さ (次元) を大きくするのである。

ここでは比較的易しい**ハミング**[1]**符号**とその誤り訂正の様子を説明する。ハミング符号では長さ 4 の情報 (すなわち 0 または 1 を 4 つ並べたもの) を長さ 7 の情報にして送信することによって、この 7 つの記号のうち、一つだけが雑音によって書き換えられても、それを訂正することができる。

以下の計算はすべて $\mathbb{F}_2$ 上で行う。次の二つの行列 G, H を考える。

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

G を符号の**生成行列**といい H を**検査行列**という。

送信する情報は $\mathbb{F}_2$ の元、すなわち 0 または 1、を 4 つ並べたものとする。(一般に 4 以上の長さを持つ情報を扱いたいときには、それを 4 つずつに区切って考えればよ

[1] R. W. Hamming, 1915–1998, アメリカ

い。) これを行ベクトルと見る。例えば $\boldsymbol{v} = (1\,0\,1\,0)$ としよう。符号化は $\boldsymbol{v}G$ によって行う。すなわち

$$(1\,0\,1\,0)\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1\,0\,1\,0\,1\,0\,1)$$

である。これで長さ 4 が長さ 7 になり 3 つの情報が付け加えられたことになる。(はじめの 4 つは元の情報になっている。) 通信の際に一つの記号が書き換えられたとしよう。例えば 3 番目が書き換えられ $(1\,0\,0\,0\,1\,0\,1)$ を受信したとする。受信者はこのベクトルの転置をとって (縦横を入れ替えて) 列ベクトルと考え、H に右からかける。

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

011 を 2 進数と見れば

$$0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 0 + 2 + 1 = 3$$

である。これは 3 番目にノイズがあることを意味している。(その理由は後で説明する。) したがって 3 番目を書き換えて、正しい送信語 $(1\,0\,1\,0\,1\,0\,1)$ を得ることができ、それから正しい情報 (前の 4 つの情報) $(1\,0\,1\,0)$ を得る。もしも計算結果が $\mathbf{0}$ となったら、誤りはなく、そのままで正しい情報であると判断する。

問 2.2.1. 上の例で $\boldsymbol{v}$ を自分で適当に定め $\boldsymbol{v}G$ を求めよ。この結果の一つの情報を書き換え、誤り訂正が正しくできることを確認せよ。

問 2.2.2. 二つの情報が書き換えられた場合には、誤り訂正が正しくできないことを確認せよ。

2.3 ハミング符号の作り方と仕組み

ハミング符号において誤り訂正ができるのは二つの行列 G, H が巧妙に作られているからである。どのように作られているのだろうか。ここでは G, H の作り方の概要を説明する。

性質 1. H の各列は 1 から 7 までを 2 進数で表したものを並べたものになっている。

H の作り方は簡単で、ここに述べた通りである。これがどのような意味をもつかは後で説明する。

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

性質 2. G のはじめの 4 列だけを見ると、対角線上だけに 1 があり、それ以外は 0 (すなわち単位行列) である。

こうすることによって $\boldsymbol{v}G$ のはじめの 4 つの成分が $\boldsymbol{v}$ と一致する。詳しくは後で説明するが 4 という数字は H の列の数 7 から行の数 3 を引いたものである。

性質 3. G の各行と H の各行は互いに直交している。

これが最も重要な性質である。この性質を満たすようにすると G が決定される。例えば G の第 1 行は $(1000abc)$ となっているが、H の各行と直交するためには

$$\begin{aligned} a+b+c &= 0 \\ b+c &= 0 \\ 1+a+c &= 0 \end{aligned}$$

でなければならない。これを解いて $(a,b,c) = (0,1,1)$ を得る。他の行についても同様である。

問 2.3.1. 行列 G を完成させなさい。

G と H が得られたので、その性質を考えよう。はじめの情報を表すベクトル $\boldsymbol{v}$ の成分のうち、一つだけが 1 で、他は 0 だったとしよう。例えば 1 番目だけが 1 とすると

$$(1\,0\,0\,0) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1\,0\,0\,0\,0\,1\,1)$$

となり、これは単に G の第 1 行を取り出しているだけである。他の成分でも同様である。行列の積について、分配法則が成り立つので、例えば $\boldsymbol{v} = (1\,0\,1\,0)$ とすると $\boldsymbol{v}G$ は G の第 1 行と第 3 行の和になる。

$$(1\,0\,1\,0) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1\,0\,1\,0\,1\,0\,1) = (1\,0\,0\,0\,0\,1\,1) + (0\,0\,1\,0\,1\,1\,0)$$

次に $\boldsymbol{v}G$ の縦横を入れ替えたものを H に右から掛けるのであるが、H の各行は G の各行と直交するので、ここでも分配法則を使って、その積はすべての成分が 0 となる。

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

これで誤りがなかったときには結果が $\mathbf{0}$ となることが分かる。

さて、誤りが生じたとしよう。正しく受信されるべきベクトルを $\boldsymbol{w}$ (7 次元列ベクトル) とする。i 番目の成分だけが 1 で他は 0 である 7 次元列ベクトルを $\boldsymbol{e}_i$ で表すことにする。i 番目に誤りが生じたとき、受信するベクトルは $\boldsymbol{w} + \boldsymbol{e}_i$ である ($\mathbb{F}_2$ では 1 を足すと 0 は 1 に、1 は 0 になる)。$\boldsymbol{w}$ には誤りがないので $H\boldsymbol{w} = 0$ である。よって

$$H(\boldsymbol{w} + \boldsymbol{e}_i) = H\boldsymbol{w} + H\boldsymbol{e}_i = H\boldsymbol{e}_i$$

となる。前と同様に H に $\boldsymbol{e}_i$ を掛けることは H の第 i 列を抜き出すことと同じであるから、性質 1 よりこれを 10 進数に直せば誤りの位置を特定することができる。

以上がハミング符号の仕組みである。

2.4 連立一次方程式とベクトル空間

符号の計算をするときには連立一次方程式を考える必要がある。まずは一般の連立一次方程式の解法を説明する。普通の数を使って説明するが $\mathbb{F}_2$ 上でも同様である。

次のような連立一次方程式を考える。

$$\begin{cases} x + y + z = 6 & (1) \\ 2x + 3y + 4z = 20 & (2) \\ 3x + 2y + 3z = 16 & (3) \end{cases}$$

この方程式を解くということは、これを式の変形によって

$$\begin{cases} x = * \\ y = * \\ z = * \end{cases}$$

の形にすることである。このためには例えば次のような計算を行えばよい。

$$\begin{cases} x + y + z = 6 & (1)' = (1) \\ \quad y + 2z = 8 & (2)' = (2) - (1) \times 2 \\ - y \quad = -2 & (3)' = (3) - (1) \times 3 \end{cases}$$

$$\begin{cases} x + y + z = 6 & (1)'' = (1)' \\ \quad y + 2z = 8 & (2)'' = (2)' \\ \quad + 2z = 6 & (3)'' = (3)' + (2)' \end{cases}$$

$$\begin{cases} x + y + z = 6 & (1)''' = (1)'' \\ \quad y + 2z = 8 & (2)''' = (2)'' \\ \quad z = 3 & (3)''' = (3)'' \times (1/2) \end{cases}$$

$$\begin{cases} x \quad = 1 & (1)''' - (2)''' - (3)''' \\ \quad y \quad = 2 & (2)''' - (3)''' \times 3 \\ \quad z = 3 \end{cases}$$

これによって解 $x = 1, y = 2, z = 3$ を得る。連立一次方程式を解く際に行ってもよい操作は以下の通りである。

(1) ある式を (0 でない) 定数倍する。

(2) 二つの式を入れ換える。

(3) ある式に別の式の定数倍を加える (引く)。

方程式の係数だけを並べて次のようなものを考える。

$$\begin{pmatrix} 1 & 1 & 1 & 6 \\ 2 & 3 & 4 & 20 \\ 3 & 2 & 3 & 16 \end{pmatrix}$$

これを連立方程式の**拡大係数行列**という。右辺の定数項を書かないで

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

としたものを**係数行列**という。拡大係数行列や係数行列を用いるときには係数 0 も省略しないで書く。拡大係数行列を用いて先の計算を書き直せば

$$\begin{pmatrix} 1 & 1 & 1 & 6 \\ 2 & 3 & 4 & 20 \\ 3 & 2 & 3 & 16 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & -1 & 0 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 2 & 6 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 1 & 3 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

となり記述がやや簡単になる。

連立方程式を解く際に行ってよい操作を行列の言葉で書くと以下のようになる。

(1) ある行を (0 でない) 定数倍する。

(2) 二つの行を入れ換える。

(3) ある行に別の行の定数倍を加える (引く)。

これを行列の**行の基本変形**という。

次の行列を前と同じように変形してみよう。

$$\begin{pmatrix} 1 & 1 & 1 & 6 \\ 2 & 3 & 4 & 20 \\ 3 & 4 & 5 & 26 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 1 & 2 & 8 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

最後の行列を方程式に戻してみると 3 番目の行は意味がないので

$$\begin{cases} x & & - & z & = & -2 \\ & y & + & 2z & = & 8 \end{cases}$$

となる。この方程式には $(x, y, z) = (-2, 8, 0),\ (-3, 10, 1)$ など、多くの解がある。

次に

$$\begin{pmatrix} 1 & 1 & 1 & 6 \\ 2 & 3 & 4 & 20 \\ 3 & 4 & 5 & 27 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 1 & 2 & 9 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 1 & 1 & 6 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

を考えてみる。3 番目の行が意味することは

$$0 = 1$$

であるから、この方程式に解はない。

これらの例から、一般の連立方程式には色々な場合があることが分かる。以下で連立方程式のすべての解を求める方法を説明する。まず、行の基本変形で拡大係数行列を以下の条件を満たすように変形する。

(1) 0 でない成分が右上に階段状になるようにする。ただし

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & \boxed{1} & \boxed{2} & 3 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

のように横に平らな部分が続いてもよいが

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & \boxed{1} & 2 \\ 0 & \boxed{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

のように縦に平らな部分が続いてはいけない。

(2) 階段の角の部分はすべて 1 にする。例えば

$$\begin{pmatrix} \boxed{1} & 2 & 3 & 4 \\ 0 & \boxed{1} & 2 & 3 \\ 0 & 0 & 0 & \boxed{1} \end{pmatrix}$$

である。

(3) 階段の角にあたる数がある列は、その部分に 1 がある以外はすべて 0 である。例えば

$$\begin{pmatrix} \boxed{1} & \underline{0} & 3 & \underline{0} \\ 0 & \boxed{1} & 2 & \underline{0} \\ 0 & 0 & 0 & \boxed{1} \end{pmatrix}$$

である。

この三つの条件を満たす行列を**被約階段行列**、または**解行列**とよぶ。行の基本変形によって解行列を作ると、一般に下の方の行は **0** となる。解行列の **0** でない行の数を (元の) 行列の**階数**という。解行列を求めるには以下のような手順を行えばよい。

Step 1.
第 1 列に 0 でない成分があるならば、それが第 1 行になるように行を入れ換える。もしも第 1 列のすべての成分が 0 ならば第 2 列を見て、第 2 列のすべての成分も 0 ならば第 3 列を見て、同様に行う。第 1 行にある 0 でないはじめの成分を使って、それより下にある行のその列の成分をすべて 0 にする。

次に第 2 行に移る。第 2 行より下の行で、はじめて 0 でない成分が現れる列を考え、その成分が第 2 行に来るように行を入れ換える。その成分を使ってその列のそれより下にある成分がすべて 0 になるようにする。

以下、第 3 行、第 4 行についても同様に繰り返す。これによって行列は (1) の条件を満たす階段状になる。

Step 2.
その行にある階段の角が a ならば、その行を $1/a$ 倍して階段の角が 1 になるようにする。

Step 3.
(i, j) 成分が階段の角であり (i', j) 成分が $a \neq 0$ とする。このとき 第 i' 行から第 i 行の a 倍を引く。そうすれば (i', j) 成分は 0 となる。

Step 1, 2, 3 によって、それぞれ (1), (2), (3) の条件が満たされることが分かる。実際、これまでに計算した例ではこの手順にそって行列を変形している。この方法を (行に関する) **掃き出し法**といい、後で他の計算にも用いる。

解行列の求め方はわかったので、次に解行列から実際に方程式の解を求める方法を説明する。考える方程式は変数 $x_1, \cdots, x_n$ に関するものであるとする。もっとも簡単なのは解行列が

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & b_1 \\ 0 & 1 & \cdots & 0 & b_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & b_n \\ 0 & \cdots & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

となる場合で、このときの解は $(x_1, \cdots, x_n) = (b_1, \cdots, b_n)$ である。

次に解行列の零でない成分をもつ一番下の行の最後の成分だけが 0 でないとき、すなわち

$$\begin{pmatrix} * & \cdots & * & * \\ \vdots & & \vdots & \vdots \\ * & \cdots & * & * \\ 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

であるとき ($*$ は何でもよいという意味)、この行は $0 = 1$ を意味するので、この方程式に解はない。

もっとも難しいのが階段に平らな部分がある場合である。この場合は具体例を用いて説明する。解行列が

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

であったとしよう。階段の角がない列で、最後の列以外のものを考える。今の場合は第 3 列と第 5 列である。対応する変数は x_3 と x_5 である。この変数に任意の定数を入れる。例えば $x_3 = s$、 $x_5 = t$ としよう。第 1 行は

$$x_1 + x_3 + x_5 = 2$$

という意味なので、$x_3 = s$、 $x_5 = t$ を代入して右辺に移項すれば

$$x_1 = -s - t + 2$$

となる。他の行も同様に計算して以下の解を得る。

$$\begin{cases} x_1 &= -s-t+2 \\ x_2 &= -2s-2t \\ x_3 &= s \\ x_4 &= -3t+3 \\ x_5 &= t \end{cases} \qquad (s,\, t \text{ は任意の定数})$$

このとき s, t は任意にとることができて、解は無数に存在する。

以上が一般の連立一次方程式の解法である。

例 2.4.1 (ベクトルと行列を用いた連立一次方程式の表示)**.** 連立一次方程式

$$\begin{cases} x + y + z = 3 \\ x - y + z = 1 \\ x \quad\;\; + z = 2 \end{cases}$$

は以下の式と同じ意味をもつ。

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$$

これを連立一次方程式の**行列表示**という。これを解くと、その解は s を任意の数として

$$\begin{cases} x &= 2-s \\ y &= 1 \\ z &= s \end{cases}$$

となるが、これもベクトルを用いて

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

と表すことができる。

例 2.4.2 (同次形連立一次方程式)**.** 連立一次方程式ですべての式の定数項が 0 であるものを**同次形連立一次方程式**と呼ぶ。同次形連立一次方程式は常にすべての変数が 0 という解をもつ。同次形連立一次方程式を行列の変形によって解く場合には拡大係数行列ではなく係数行列を用いればよい。例えば次は同次形連立一次方程式とその解である。

$$\begin{cases} x + y + z = 0 \\ x - y + z = 0 \\ x \quad\;\; + z = 0 \end{cases}, \qquad \begin{cases} x &= -s \\ y &= 0 \\ z &= s \end{cases}$$

行列を使って表せば

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} x \\ y \\ z \end{pmatrix} = s \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

となる。この例と前の例をくらべると、同次形連立一次方程式の解は非同次形連立一次方程式の解の定数部分を除いたものになっていることが分かる。

問 2.4.3. 以下の連立一次方程式を解け。

(1) $\begin{cases} x + y + z = 4 \\ 2x + y + z = 6 \\ x - y + 2z = 3 \end{cases}$ (2) $\begin{cases} x + y + z = 3 \\ x + y + 2z = 6 \\ -x - y + z = 2 \end{cases}$

(3) $\begin{cases} x + y + z = 3 \\ x + y + 2z = 6 \\ -x + y + z = 3 \end{cases}$ (4) $\begin{cases} x + 2y + 3z = 4 \\ 2x + 3y + 4z = 5 \end{cases}$

(5) $\begin{cases} x + y + 2z + 2u = 2 \\ 2x + y + z + 2u = -4 \\ x + 2y + 5z + 5u = 6 \end{cases}$ (6) $\begin{cases} x + 2y + z = 0 \\ 2x - 3y - 3z = 0 \\ -3x + y + 2z = 0 \\ 4x + y - z = 0 \end{cases}$

問 2.4.4. 以下の $\mathbb{F}_2$ 上の連立一次方程式を解け。

(1) $\begin{cases} x + y + z = 1 \\ x + y = 0 \\ x + z = 0 \end{cases}$ (2) $\begin{cases} x + y = 1 \\ x + z = 1 \\ y + z = 1 \end{cases}$

次にベクトル空間とその部分空間について解説する。実数全体の集合を $\mathbb{R}$ と表す。実数を成分とする n 次元行 (または列) ベクトル全体の集合を n **次元ベクトル空間**といい、$\mathbb{R}^n$ と書く。$\mathbb{F}_2$ 上で考えるときには $\mathbb{F}_2$ **上の** n **次元ベクトル空間**といい、${\mathbb{F}_2}^n$ と書く。以後、実数を成分とするベクトルを考えるが、$\mathbb{F}_2$ 上でも同様の議論が成り立つ。

$\mathbb{R}^n$ には加法 (成分ごとの和) が定義されてる。実数 a とベクトル $\boldsymbol{v} = (v_1 \ \cdots \ v_n)$ に対して

$$a\boldsymbol{v} = (av_1 \ \cdots \ av_n)$$

とおいて、これを**スカラー倍**という。ベクトル空間においては、加法とスカラー倍が基本的な操作である。

$\mathbb{R}^n$ の部分集合 V が $\mathbb{R}^n$ の**部分空間**であるとは

(1) $\boldsymbol{v}, \boldsymbol{w}$ が V に含まれるならば $\boldsymbol{v} + \boldsymbol{w}$ も V に含まれる。

(2) $\boldsymbol{v}$ が V に含まれ、a を実数とすると $a\boldsymbol{v}$ も V に含まれる。

を満たすことである。

例 2.4.5. $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_r$ を n 次元ベクトルとする。$\sum_{i=1}^{r} a_i \boldsymbol{v}_i$ (a_i は実数) の形をしたベクトル全体の集合は $\mathbb{R}^n$ の部分空間である。これを $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_r$ **の張る部分空間**という。

問 2.4.6. $\sum_{i=1}^{r} a_i \boldsymbol{v}_i$ (a_i は実数) の形をしたベクトル全体の集合は $\mathbb{R}^n$ の部分空間であることを示せ。

$\boldsymbol{v}_1, \cdots, \boldsymbol{v}_r$ の張る部分空間 V を考える。もし $\boldsymbol{v}_r = \boldsymbol{0}$ であるならば、V は $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_{r-1}$ の張る部分空間にも等しい。V はもっと少ない数のベクトルで張られるかも知れないのである。V を張るベクトルの数の最小値を部分空間 V の**次元**という。また、このときの V を張るベクトルの集合を V の**基底**という。

例 2.4.7. $V = \mathbb{R}^n$ は $\mathbb{R}^n$ の部分空間である。$\boldsymbol{e}_i$ を i 番目の成分のみが 1 で、他の成分は 0 であるベクトルとする。このとき $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ は V の基底で、V の次元は n である。

さて、$\boldsymbol{v}_1, \cdots, \boldsymbol{v}_r$ の張る部分空間 V の基底と次元を求める方法を説明しよう。$\boldsymbol{v}_1, \cdots, \boldsymbol{v}_r$ を行ベクトルとして並べた $r \times n$ 行列を M とする。M に行の基本変形を施して得られる行列を M' としよう。このとき M' の行ベクトルの張る部分空間は V に等しい。連立一次方程式を解くときと同じように M' が階段状になるように変形してやれば、M' の $\mathbf{0}$ でない行ベクトルの集合が V の基底となる。したがって V の次元は M の階数に等しい。(一般に、階段上にしたときには下の方の行は $\mathbf{0}$ となるため、次元は r よりも小さくなることがある。)

例 2.4.8. $\boldsymbol{v}_1 = (1\ 1\ 0)$, $\boldsymbol{v}_2 = (1\ 0\ 1)$, $\boldsymbol{v}_3 = (2\ 1\ 1)$ の張る部分空間の基底と次元を求めるには、行列

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

を行の基本変形によって階段行列に変形すればよい。計算をすれば

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

となるから、基底として $(1\ 0\ 1)$, $(0\ 1\ -1)$ がとれて、その次元は 2 である。(基底は一つに定まるものではない。例えば $\boldsymbol{v}_1, \boldsymbol{v}_2$ はこの空間の基底である。)

問 2.4.9. $\boldsymbol{v}_1 = (1\ 2\ 3)$, $\boldsymbol{v}_2 = (4\ 5\ 6)$, $\boldsymbol{v}_3 = (7\ 8\ 9)$ の張る部分空間の基底と次元を求めよ。

問 2.4.10. $\mathbb{F}_2$ 上のベクトルと見て $\boldsymbol{v}_1 = (1\ 1\ 0)$, $\boldsymbol{v}_2 = (1\ 0\ 1)$, $\boldsymbol{v}_3 = (0\ 1\ 1)$ の張る部分空間の基底と次元を求めよ。

例 2.4.11 (同次形連立一次方程式の解空間)**.** 同次形連立一次方程式の解は

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = s_1 \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1n} \end{pmatrix} + s_2 \begin{pmatrix} a_{21} \\ a_{22} \\ \vdots \\ a_{2n} \end{pmatrix} + \cdots + s_m \begin{pmatrix} a_{m1} \\ a_{m2} \\ \vdots \\ a_{mn} \end{pmatrix}$$

という形をしていることを前に見た。したがってその解の全体、すなわち $s_1, s_2, \cdots, s_m$ を自由に動かして得られるベクトルの全体、は $\mathbb{R}^n$ の部分空間になる。これを同次形連立一次方程式の**解空間**と呼ぶ。前に説明した方法で解行列を求めたとする。係数行列の階数が r だったとすると、自由に動ける定数の個数 m は $n - r$ である。また解の表示に現れるベクトルは解空間の基底になることが分かっていて、したがって解空間の次元は $m = n - r$ となる。

V を $\mathbb{R}^n$ の部分空間とする。V のすべての元と直交するベクトル全体の集まりを V の**直交空間**といい $V^\perp$ と書く。

問 2.4.12. $V^\perp$ は $\mathbb{R}^n$ の部分空間であることを示せ。

V の基底 (次元) が分かっているものとし、$V^\perp$ の基底 (次元) を求めよう。V の次元を r とする。V の基底を行ベクトルとして並べた $r \times n$ 行列を M とする。ベクトル $\boldsymbol{w}$ が $V^\perp$ に属するためには $\boldsymbol{w}$ を n 次元列ベクトルと見て

$$M\boldsymbol{w} = \mathbf{0}$$

となればよい。よって $V^\perp$ は同次形連立一次方程式

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{0}$$

の解空間に一致する。したがってその次元は $n - r$ であることも分かる。

問 2.4.13. (1 1 1) で張られる $\mathbb{R}^3$ の部分空間を V とする。$V^\perp$ の基底を求めよ。

問 2.4.14. (1 1 1 1) で張られる ${\mathbb{F}_2}^4$ の部分空間を V とする。$V^\perp$ の基底を求めよ。

2.5 一般の符号とその誤り訂正

ハミング符号と同じように別の符号を作ることもできる。ここではその概略を述べる。

一般に符号では、元の情報に余分な情報を付け加えることによって誤り検出や誤り訂正を行う。元の情報の長さを k、情報を付け加えた後の長さを n とするとき、その符号を (n, k) 符号という。以下では (n, k) 符号を考えるものとする。

まず、ハミング符号と同じように検査行列 H を作る。

作り方 1. 検査行列 H は $(n-k) \times n$ 行列で、その階数が $n-k$ であるものとする。

実は H の作り方が最も重要なのであるが、ここでは単にその階数が $n-k$ であることだけを要求する。H の行ベクトルの張る部分空間を V とする。H の階数が $n-k$ であるから V は ${\mathbb{F}_2}^n$ の $n-k$ 次元部分ベクトル空間である。$C = V^\perp$ とする (一般にこの部分空間 C を符号という)。C は k 次元部分ベクトル空間である。

作り方 2. 生成行列 G は $k \times n$ 行列で、C の基底を行ベクトルとして並べたものとする。

以上で一般の符号ができあがる。しかし、このままでは誤り検出や誤り訂正はできない。まずは一つの誤りを訂正できるためには、どのような条件があればよいかを考える。

はじめに誤りがない場合を考えよう。元の情報 (k 次元ベクトル) を $\boldsymbol{v}$ とする。ハミング符号と同じように $\boldsymbol{v}G$ は G の行ベクトルをいくつか足したものに等しい。したがって $\boldsymbol{v}G$ は C に含まれており、H の各行と直交する。したがって $\boldsymbol{v}G$ の行と列を入れ替えたベクトルを H に右から掛けると $\mathbf{0}$ となる。よって誤りがない場合は結果が $\mathbf{0}$ となることが分かる。

次に一つの誤りが起きたとしよう。誤りのない受信ベクトル ($\boldsymbol{v}G$ の行と列を入れ替えたベクトル) を $\boldsymbol{w}$ とする。前と同じように i 番目の成分だけが 1 で、他の成分が 0

である n 次元列ベクトルを $\boldsymbol{e}_i$ と書くことにする。このとき一つの誤りを含む受信ベクトルは $\boldsymbol{w}+\boldsymbol{e}_i$ である。$H\boldsymbol{w}=\boldsymbol{0}$ なので

$$H(\boldsymbol{w}+\boldsymbol{e}_i)=H\boldsymbol{e}_i$$

で、これは H の第 i 列に等しい。したがって、もし H のすべての列が異なり、かつ H の列に $\boldsymbol{0}$ がないならば、これを計算することによって誤りの位置を特定し、それを訂正することができる。

命題 2.5.1. 検査行列 H のすべての列が異なり、かつ H の列に $\boldsymbol{0}$ がないならば、一つの誤りを訂正することができる。

例 2.5.2. n を正の整数とする。1 から 2^n-1 を 2 進数で表し、それを列ベクトルとして並べたものを検査行列 H とする。このとき H は $n\times(2^n-1)$ 行列で、その階数は n である。このとき H の各列は $\boldsymbol{0}$ でなく、またすべて異なる。よって H から作られる符号は $(2^n-1,\ 2^n-n-1)$ 符号で、一つの誤りを訂正できる。(これはハミング符号の自然な拡張で、一般にこれも**ハミング符号**と呼ばれる。)

さて、二つ以上の誤りを訂正することを考えよう。そのために一つの定義をする。一般に $\mathbb{F}_2$ 上のベクトルに対し、その成分のうち 1 であるものの個数を、そのベクトルの**重み**という。例えば、一つの成分だけが 1 であるベクトルは重み 1 である。t 個の誤りを訂正することを考える。誤りのない受信ベクトルを $\boldsymbol{w}$ とし、受信ベクトルを $\boldsymbol{w}+\boldsymbol{e}$ とする。$\boldsymbol{e}$ は重みが t 以下のベクトルであるとする。

$$H(\boldsymbol{w}+\boldsymbol{e})=H\boldsymbol{e}$$

なので、もしも重みが t 以下のベクトル $\boldsymbol{e}$ に対して $H\boldsymbol{e}$ がすべて異なれば、$H\boldsymbol{e}$ から $\boldsymbol{e}$ を特定することができ、したがって t 個以下の誤りを訂正できる。

この条件を満たす H が得られたならば、重みが高々 t のすべてのベクトル $\boldsymbol{e}$ を列挙し、それに対応する $H\boldsymbol{e}$ を計算しておく。すると比較的簡単に誤り訂正をすることができる。

問 2.5.3. $(23,12)$ 符号で 3 つの誤りを訂正したい。重みが 3 以下のベクトルはいくつあるか。

以上で、誤り訂正の方法は分かった。次に元の情報を取り出すことを考えよう。ハミング符号では長さ 4 のベクトルを長さ 7 にし、元の戻すときにははじめの 4 文字を取り出すだけでよかった。これは生成行列 G が

$$G=\begin{pmatrix} 1 & 0 & \cdots & 0 & * & \cdots & * \\ 0 & 1 & \cdots & 0 & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & * & \cdots & * \end{pmatrix}$$

という形をしているからである。一般にこの形の生成行列を持つ符号を**組織符号**という。G はベクトル空間 C の基底を行ベクトルとして並べたものなので、基底をうまく取ってやれば組織符号に出来る場合もあるが、常にそうできるわけではない。一般には列を適当に入れ替えれば、常に組織符号にできるでのはあるが、ここでは次の事実を用いることにする。

命題 2.5.4. G を $m \times n$ 行列とし、その階数を m とする。このとき、ある $n \times m$ 行列 K があって $GK = I_m$ (I_m は m 次単位行列) となる。

証明. $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ とする。また $\boldsymbol{e}_i$ を i 番目の成分だけが 1 である n 次元列ベクトルとする。このとき G の階数が m であることから、連立方程式

$$G\boldsymbol{x} = \boldsymbol{e}_i$$

は解 $\boldsymbol{y}_i$ を持つ。$K = (\boldsymbol{y}_1 \ \cdots \ \boldsymbol{y}_n)$ とすれば、これは $GK = I_m$ を満たす。 □

命題 2.5.4 のような K を用意しておけば

$$\boldsymbol{v}GK = \boldsymbol{v}$$

なので、受信ベクトルを誤り訂正した後に K を右から掛けることによって、元の情報を取り出すことができる。

問 2.5.5. 階数 2 の 2×3 行列

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

に対して $GK = I_2$ となる 3×2 行列 K を求めよ。

2.6 誤り訂正符号の性能と限界

0 か 1、 あるいは YES か NO、という情報を確実に相手に伝えたいとする。例えば直接、目の前にいる相手に伝えたかったらどうするであろうか。答えは簡単で、多くの人が「繰り返しいう」という方法をとるであろう。これはまさに誤り訂正符号そのものである。一度いうだけで伝わる内容を、繰り返しいうことでその情報量を増やし、誤りが起きないようにしているのである。これと同じことを携帯電話などの通信で行ったとしよう。例えば同じ情報を 100 回繰り返して送るとする。こうすればまず間違いなく正確な情報が伝わる。しかしながら通信にはコストがかかる。通話料金が 100 倍かかるのである。よほど重要なことならば仕方ないと思えるかも知れないが、通常の通信でそのようなことは許容できないであろう。「情報量の増加は少なく、誤り訂正能力は高く」というのが理想である。しかし 100 倍かかっても正確に伝えたい場合もないことはない。したがって、どのような符号を用いるのが良いかはその状況に応じて変るもので一概にいえるものではない。目の前にいる相手との会話においては、人間は無意識に色々な符号を使い分けていると考えることもできる。ここでは「情報量の増加」と「誤り訂正能力」との関係について、簡単に解説する。

まずは符号理論を概念として理解しよう。幾つかの的があり、ある人がその内の一つを狙ってボールを投げるとする。二つの的の間隔は少なくとも 1 m あるとする。その人はコントロールが良く、狙った的から 50 cm 以上外れることがないとすれば、そ

れを見た人は、どの的を狙って投げたのかを知ることができる。これが符号の原理である。しかし実際には「50 cm 以上外れることがない」などということはありえないことで、状況によっては大きく外れてしまうだろう。この場合には狙った的を正しく言い当てることはできない。そして二つの的の間隔を大きくすることで正しく言い当てる確率を高めることができる。

さて符号の話に戻ろう。(n,k) 符号では長さ k の情報を長さ n にするのであった。このとき 2^k 個の異なる情報を扱うことができる。2^k 個の “点” を 2^n 個の “点” をもつ “空間” に埋め込むのである。このように埋め込まれた点を**符号語**という。この点が上のボール投げの例における的である。$\mathbb{F}_2$ 上 n 次元の二つのベクトル $\boldsymbol{u},\boldsymbol{v}$ に対して、その距離を異なる成分の数として定める。2^k 個の符号語を考え、その二点間の距離の最小値を d とする。また d が偶数のとき $t=d/2-1$、奇数のとき $t=(d-1)/2$ とする。このようにすれば、各符号語を中心とする半径 t の “球” は共通部分をもたない。情報の通信が行われたとしよう。もし誤りがなければ、受信語は符号語と一致する。一般に誤りが生じると受信語は ${\mathbb{F}_2}^n$ の任意のベクトルに成り得る。このとき受信語の誤りが t 個以下ならば、それはある唯一つの球に含まれることになり、その中心として符号語が定まる。これが誤り訂正の仕組みである。

「情報量の増加」と「誤り訂正能力」について考えよう。「情報量の増加」が少ないということは n と k がそれほど変らないということである。例えば n を固定したとすると ${\mathbb{F}_2}^n$ にたくさんの球を交わりなく詰め込むということになる。一方、「誤り訂正能力」が高いということは球の半径、すなわち上記の t が大きいということである。つまり「情報量の増加は少なく、誤り訂正能力は高く」ということは、「(限られた空間に) 大きな半径の球をたくさん詰め込め」ということで、普通に考えればこれは相容れない要求で、限界があることが分かるであろう。

一般に上記の記号の下で以下の関係式が成り立つことが知られている。

(Singleton の限界式) $$n-k+1 \geqq d$$

これは n を固定したとき k と d が同時に大きくはなれないことを示している。

一般に上記の設定を考えると、空間内の点でどの球にも属さない点が存在し得る。このような点がたくさんあると、球をうまく詰め直すことによってもう少したくさんの球を入れることができるかも知れない。しかしそのような点が一つもなかったら、どのように工夫してもそれ以上の球を入れることはできない。このような符号を**完全符号**という。完全符号はある意味でもっとも良い符号であると考えられる。

ハミング符号を考えよう。実はハミング符号は完全符号であり、上記のようにもっとも良い符号の一つなのである。これを確認しよう。まずハミング符号は $(7,4)$ 符号であるから 2^7 個の点から成る空間に 2^4 個の球が詰め込まれている。また一つの誤りを訂正できたので、球の半径は少なくとも 1 である。半径を 1 として一つの球にいくつの点が含まれるかを考えると、符号語自身、および一つの成分を書き換えた 7 つのベクトル、の合計 8 個であることが分かる。したがってすべての球に含まれる点の総数は

$$2^4 \times 8 = 2^7$$

となり、空間の点の数と一致する。したがってハミング符号は完全符号である。

問 2.6.1. 例 2.5.2 で一般のハミング符号を定義した。これも完全符号であることを示せ。

問 2.6.2. 問 2.5.3 で考えた $(23, 12)$ 符号で 3 つの誤りを訂正できるものは 2 元ゴーレイ符号と呼ばれるもので、実際に存在する。これが完全符号であることを示せ。

Chapter 3

暗号

暗号とは、文章に何らかの変換を加えて、意味の通らない文字列に変換し、もし傍受されても原文が分からないようにする方法である。そこから元の文章を得ることを**復号**という。

3.1 秘密鍵暗号と公開鍵暗号 – シーザー式暗号

次の文字列を考える。

SHINSHUUNIVERSITY

これを 3 文字ずらしてみよう。つまり

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

の上段の文字を下段で置き換える。すると

VKLQVKXXQLYHUVLWB

となり、意味の分からない文字列になる。これはジュリアス・シーザー[1]が利用したといわれていることから**シーザー式暗号**と呼ばれる。シーザー式暗号が利用されていることが分かれば、その復号は簡単である。

問 3.1.1. シーザー式暗号による暗号文

QDJDQRNHQPDWVXPRWRVKL

を復号せよ。

シーザー式暗号を少しだけ改良して n 文字ずらすことを考えたとする。例えば SHINSHUUNIVERSITY を 10 文字ずらして

CRSXCREEXSFOBCSDI

[1] J. Caesar, BC100 頃–BC44, ローマ

などとする。この場合は n が分からないとやや面倒であるが、それでも高々 25 ずらして、意味のある文が現れるかどうかを調べればよい。(26 ずらすと元に戻ってしまう。)

更に改良を加えよう。26 文字のアルファベットを適当に別の文字に対応させたとする。例えば A は Z, B は H, C は T などと無作為に対応をつける。この場合は対応表を持っていないと解読は不可能なように思えるが、ある程度の長さをもつ文であれば以下のように解読できる。英文では、アルファベット毎にその出現頻度は異なる。例えば e は出現頻度が高く z は出現頻度が低い。長文になればこの傾向はよりはっきりとして、出現頻度によって対応表を類推することが可能となる。

更に改良を考える。この方法では適当な文を鍵とする。例えば NAGANO を鍵としよう。A から順に 1, 2, 3 と番号をふることにすれば、鍵は $14, 1, 7, 1, 14, 15$ となる。暗号は 1 文字目は 14 ずらし、2 文字目は 1、3 文字目は 7、4 文字目は 1、5 文字目は 14、6 文字目は 15、7 文字目ははじめに戻って 14、などとずらすとする。十分長い鍵を用意してやれば、この暗号の解読は困難となる。

これまで説明した暗号はどれも文字の置き換えによるもので**換字式暗号**と呼ばれる。換字式暗号でも複雑なものは鍵を入手しなければ解くことは困難である。しかし鍵さえ入手できれば簡単に解読できるので、鍵を厳重に管理しなければならない**秘密鍵暗号**である。秘密鍵暗号にはこの他にも、文字の並び順を変えるものなど色々とある。

秘密鍵暗号では鍵が最も重要であり、他人に分かってはいけない。したがって、例えば 10 人の相手と暗号を用いた通信をする場合には、それぞれ違う鍵を用意しなくてはならず、鍵の管理が煩雑になる。これに対して次の節で解説する**公開鍵暗号**は暗号化の鍵を公開してしまう暗号であるため、何人の人と通信をする場合でも、鍵は各自が一つもてば済む。

問 3.1.2. 10 人がそれぞれ、すべての人と秘密鍵暗号を使って通信するとき、鍵は全部でいくつ必要か？ また公開鍵暗号のときはどうか？

一般に公開鍵暗号では、その暗号化、復号化に多くの計算を要するため、これを多くの情報に対して行うことは効率的ではない。そこで秘密鍵暗号の鍵を公開鍵暗号で暗号化し、これを相手に渡し、実際の通信にはこの鍵による秘密鍵暗号を用いるというのが実際に行われている方法である。この方法で、通信のすべてを盗聴されたとしても、その秘密は守られる。

例 3.1.3 (転置式暗号)**.** マス目のある原稿用紙に縦書きに書いた文章を横に読めば、その意味は分からなくなる。このように文章を読む順番を変えれば、それは暗号となる。このような暗号を**転置式暗号**という。転置式暗号も、その作り方が鍵であり、これが分かってしまえばすぐに解読できる秘密鍵暗号である。

3.2 初等整数論、素数

次の節で代表的な公開鍵暗号である RSA 暗号を説明するために、ここで初等整数論についてのいくつかの事柄を解説する。暗号とは直接関係のないことも説明するが、初等整数論の面白さを感じてもらいたい。

2 以上の自然数で 1 と自分自身だけを約数に持つものを**素数**という。素数でない 2 以上の自然数を**合成数**という。合成数は 2 以上の二つの自然数 m, n を用いて mn と書

くことができる。特に m として素数を取ることができる。1 は素数でも合成数でもないとする。

例 3.2.1. 100 以下の素数は

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

である。

RSA 暗号ではとても大きな素数が必要になる。次の定理は基本的であるが重要である。

定理 3.2.2. 素数は無限に存在する。特にいくらでも大きな素数が存在する。

証明. 素数が $p_1 < p_2 < \cdots < p_r$ しかなかったとする。このとき $n = p_1 p_2 \cdots p_r + 1$ は p_r より大きいので素数ではない。よって n は合成数であり、ある素数 m を約数にもつ。しかし n はどの素数 p_i でも割りきれないので矛盾である。よって素数はいくらでも存在する。 □

このことからいくらでも大きな素数が存在することは保証されるが、実際に大きな素数を求めることは難しい。

問 3.2.3. 100 より大きい素数を一つ見つけなさい。

例 3.2.4 (メルセンヌ素数)**.** n を自然数とする。$2^n - 1$ が素数であるとき、これを**メルセンヌ**[1]**素数**という。メルセンヌ素数に対しては「ルカス・テスト」と呼ばれる、素数判定法が存在し、比較的効率よく素数かどうかの判定ができる。現在知られている最大の素数はメルセンヌ素数である。メルセンヌ素数は**完全数**と呼ばれる数と関係がある。メルセンヌ素数が無限個あるかどうかは分かっていない。

例題 3.2.5. $2^n - 1$ が素数 (すなわちメルセンヌ素数) であるとき n は素数である。

解答. 対偶を示す。一般に

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$$

が成り立つ。n を合成数とし $n = \ell m$, $\ell \geqq 2$, $m \geqq 2$ とすると

$$2^n - 1 = (2^\ell)^m - 1 = (2^\ell - 1)((2^\ell)^{m-1} + (2^\ell)^{m-2} + \cdots + (2^\ell) + 1)$$

となり、$1 < 2^\ell - 1 < 2^n - 1$ なので $2^n - 1$ は素数ではない。

一般に n が素数であっても $2^n - 1$ が素数であるとは限らない。例えば $2^{11} - 1 = 2047 = 23 \times 89$ である。

問 3.2.6. 6 の 6 以外の約数は $1, 2, 3$ でその和は

$$1 + 2 + 3 = 6$$

で、もとの数に一致する。このような数を**完全数**と呼ぶ。6 以外の完全数を見つけよ。

[1] Mersenne, 1588–1648, フランス

2^n-1 がメルセンヌ素数であるとき $2^{n-1}(2^n-1)$ は完全数であることが知られている (それほど難しくはないので興味のある人は証明してみるといいだろう)。また偶数の完全数はこの形のものに限ることが知られている。奇数の完全数は一つも見つかっていないが、その非存在も証明されてはいない。

例 3.2.7 (フェルマー素数)**.** n を自然数とする。2^n+1 が素数であるとき、これを**フェルマー**[1]**素数**という。フェルマー素数は $n=1,2,4,8,16$ の場合しか知られていない (それぞれ $2^n+1=3,5,17,257,65537$)。フェルマー素数は**作図可能な正多角形**と関係がある。すなわち、素数 n に対して、正 n 角形が定規とコンパスだけを使って作図出来るには n がフェルマー素数であることが必要十分条件である。したがって、例えば正 7 角形は作図できない。

例題 3.2.8. 2^n+1 が素数 (すなわちフェルマー素数) であるとき n は 2 のべき (2^e という形の数) である。

解答. 対偶を示す。一般に m が奇数であるとき

$$x^m+1=(x+1)(x^{m-1}-x^{m-2}+\cdots-x+1)$$

が成り立つ。n が奇数の約数 m をもち $n=\ell m$ と書けたとすると

$$2^n+1=(2^\ell)^m+1=(2^\ell+1)((2^\ell)^{m-1}-(2^\ell)^{m-2}+\cdots-2^\ell+1)$$

であり、$1<2^\ell+1<2^n+1$ なので 2^n+1 は素数ではない。

一般に n が 2 のべきであっても 2^n+1 が素数であるとは限らない。例えば

$$\begin{aligned} 2^{32}+1 &= 4294967297=641\times 6700417,\\ 2^{64}+1 &= 18446744073709551617=274177\times 67280421310721 \end{aligned}$$

である。上にあげた 5 つ以外にフェルマー素数が存在するかどうは分かっていない。

素数に関するいくつかの定理を紹介する。

定理 3.2.9 (ウィルソンの定理)**.** n が素数であるための必要十分条件は

$$(n-1)!\equiv -1 \pmod{n}$$

が成り立つことである。($(n-1)!=1\times 2\times\cdots\times(n-2)\times(n-1)$ である。)

例 3.2.10. ウィルソンの定理を具体的に確かめてみる。まず素数について

$$\begin{aligned} (3-1)! &= 1\times 2=2\equiv -1 \pmod 3\\ (5-1)! &= 1\times 2\times 3\times 4=24\equiv -1 \pmod 5\\ (7-1)! &= 1\times 2\times\cdots\times 6=720\equiv -1 \pmod 7\\ (11-1)! &= 1\times 2\times\cdots\times 10=3628800\equiv -1 \pmod{11} \end{aligned}$$

[1] Fermat, 1607 頃–1665, フランス

である。また合成数については

$$\begin{aligned}(4-1)! &= 1\times 2\times 3 = 6 \not\equiv -1 \pmod 4\\ (6-1)! &= 1\times 2\times 3\times 4\times 5 = 120 \not\equiv -1 \pmod 6\end{aligned}$$

などとなる。

問 3.2.11. $n = 13, 15$ についてウィルソンの定理を確認せよ。

ウィルソンの定理は美しい定理であるが、素数判定法としては効率が悪すぎて使えない。

定理 3.2.12 (フェルマーの小定理)**.** p を素数とし a を p で割り切れない自然数とする。このとき

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

例 3.2.13. $p = 5$, $a = 3$ としてフェルマーの小定理を確認する。

$$3^{5-1} = 81 \equiv 1 \pmod 5$$

である。p が素数でないときにはフェルマーの小定理は、一般に成り立たない。例えば $p = 4$, $a = 3$ とすると

$$3^{4-1} = 27 \equiv 3 \pmod 4$$

である。もちろん、例えば $a = 1$ とすればどんな p に対しても成り立つので、p が素数でなくても同じ式が成り立つ場合もある。

フェルマーの小定理は以下のように一般化される。n を自然数とする。n 以下の自然数で n と互いに素であるものの数を $\varphi(n)$ で表す。これを**オイラー**[1]**関数**という。このとき次が成り立つ。

定理 3.2.14 (フェルマーの小定理の一般化)**.** n を自然数とし a を n と互いに素な自然数とする。このとき

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

もし p が素数ならば $\varphi(p) = p - 1$ であり、p で割り切れないことと p と互いに素であることは同値になる。よって素数に対して定理 3.2.14 を適用すれば定理 3.2.12 となる。

問 3.2.15. $\varphi(4)$, $\varphi(6)$, $\varphi(8)$, $\varphi(9)$, $\varphi(10)$ を求めよ。また $3^{\varphi(8)} \equiv 1 \pmod 8$ であることを確認せよ。

後で利用するために、二つの異なる素数 p, q に対して $n = pq$ とした場合を考える。まず、一般的な定理を一つ用意する (証明はしない)。

定理 3.2.16 (中国剰余定理)**.** m, n を互いに素な自然数とする。任意の自然数 a, b に対して $x \equiv a \pmod m$, $x \equiv b \pmod n$ となる自然数 x が mn を法として一意的に存在する。

[1] Euler, 1707–1783, スイス–ロシア

問 3.2.17. 5 で割ると 3 余り、7 で割ると 2 余る最小の自然数を求めよ。

命題 3.2.18. 二つの異なる素数 p, q に対して $\varphi(pq) = (p-1)(q-1)$ である。

証明. pq 以下の自然数で pq と互いに素でないものを数える。p の倍数は q 個、q の倍数は p 個ある。p の倍数であって q の倍数でもあるものは pq のみであるから、pq と互いに素でないものは $p+q-1$ 個ある。したがって $\varphi(pq) = pq-p-q+1 = (p-1)(q-1)$ である。 □

命題 3.2.19. p, q を二つの異なる素数とする。このとき任意の自然数 a と任意の自然数 m に対して

$$a^{m(p-1)(q-1)+1} \equiv a \pmod{pq}.$$

証明. a が pq と互いに素であるときは定理 3.2.14、命題 3.2.18 から $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ であるから

$$a^{m(p-1)(q-1)+1} = (a^{(p-1)(q-1)})^m \times a \equiv a \pmod{pq}$$

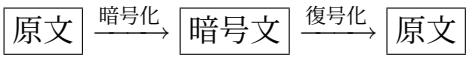
である。a が pq と互いに素でないとき、(1) a は p で割り切れて q で割り切れない、(2) a は q で割り切れて p で割り切れない、(3) a は p でも q でも割り切れる、の 3 つの場合がある。(3) のときは $a^{m(p-1)(q-1)+1} \equiv 0 \equiv a \pmod{pq}$ なので主張は成り立つ。(1) としよう。このとき $a^{q-1} \equiv 1 \pmod{q}$ であり、よって

$$a^{m(p-1)(q-1)+1} = (a^{q-1})^{m(p-1)} \times a \equiv a \pmod{q}.$$

また $a \equiv 0 \pmod{p}$ だから $a^{m(p-1)(q-1)+1} \equiv 0 \pmod{p}$ である。定理 3.2.16 より、このような自然数が pq を法として一意的に存在するが a はこれを満たすので、その一意性から $a^{m(p-1)(q-1)+1} \equiv a \pmod{pq}$ である。(2) も同様である。 □

3.3 RSA 暗号

ここで説明する **RSA 暗号** (Rivest, Shamir, Adleman, 1977) は**公開鍵暗号**である。すなわち秘密鍵暗号ではもっとも重要である鍵が公開されている暗号である。



秘密鍵暗号では暗号化と復号化で (本質的に) 同じ鍵が使われるため、その秘密性が重要となるが、公開鍵暗号では異なる鍵が使われるため、暗号化の際に使われた鍵が分かっても、この解読は出来ないのである。

実際には、例えば A さんから 「この鍵を使って暗号化したものを送って下さい。」といって暗号化鍵をもらい、それで暗号化した文を送ったとする。この場合、復号化鍵は A さんだけの秘密であるとすれば、この通信の全てを盗聴したとしても、その解読は出来ない。

理由などは後にして、実際の利用の様子を見てみよう。暗号を利用する人は以下の数を用意する。

(1) 二つの異なる素数 p, q. (実際の暗号で使うには、安全性を確保するために p, q 共に大きくなければならない。現在は 200 桁程度で安全とされている。)

(2) $N = pq$.

(3) $L = (p-1)(q-1)$.

(4) L と互いに素な自然数 e.

(5) $ed \equiv 1 \pmod{L}$ を満たす d.

このうち N と e を公開鍵として公開する。p, q, L, d は秘密にしておかなければならない。文 $\mathcal{M}$ を適当な方法で N 未満の正の数に置き換えておく。暗号化は

$$\mathcal{M} \to \mathcal{M}^e \pmod{N}$$

によって行う。したがってメッセージを送る人は公開鍵 e, N のみを知っていればよい。暗号化されたメッセージ $\mathcal{C} = \mathcal{M}^e$ を受け取った人は秘密鍵 d を用いて

$$\mathcal{C} \to \mathcal{C}^d \pmod{N}$$

によって復号化を行う。

$$\mathcal{C}^d \equiv \mathcal{M}^{ed} \equiv \mathcal{M} \pmod{N}$$

が成り立ち、原文 $\mathcal{M}$ を得ることができる。

例 3.3.1. $p = 7$, $q = 11$ とすると $N = 7 \times 11 = 77$, $L = (7-1)(11-1) = 60$ である。$e = 7$ としよう。$7d \equiv 1 \pmod{60}$ を解いて $d = 43$ を得る (効率的な計算方法は後で説明する)。またメッセージを $\mathcal{M} = 50$ とする。このとき暗号化は

$$\mathcal{C} = \mathcal{M}^e = 50^7 \equiv 8 \pmod{77}$$

となる。

$$\mathcal{C}^d = 8^{43} \equiv 50 \pmod{77}$$

を計算して原文 $\mathcal{M} = 50$ を得る。

問 3.3.2. $p = 3$, $q = 11$, $e = 7$ とする。N, L, d を求めよ。また $\mathcal{M} = 15$ として暗号化、復号化を計算せよ。

さて RSA 暗号の原理を考えてみよう。

$$\mathcal{C}^d \equiv \mathcal{M}^{ed} \equiv \mathcal{M} \pmod{N}$$

以外の部分は単なる計算である。またこの式は次のことから分かる。$ed \equiv 1 \pmod{L}$, $L = (p-1)(q-1)$ より、ある整数 m があって $ed = m(p-1)(q-1)+1$ と書ける。よって命題 3.2.19 が適用できて、任意の a に対して $a^{ed} \equiv a \pmod{pq}$ である。

なぜこれが暗号として利用できるのであろうか。解読しようと思うならば秘密鍵 d を求めればよい。d は $ed \equiv 1 \pmod{L}$ を満たす数である。$L = (p-1)(q-1)$ が分か

れば、後で説明するユークリッドの互除法を用いて d は求められる。L を求めるのは $N = pq$ を素因数分解するのと同じくらいに難しいことが分かっている。p, q を十分大きな素数とすれば pq から、それらを求めるのは非常に困難で、したがって暗号は解読できない。現在安全とされている素数の大きさは p, q 共に 200 桁程度である。(現在の最も速い計算機を用いても数百年の計算時間がかかれば安全と考えられる。) 素因数分解によらない RSA 暗号の解読方法は知られていない。

「二つの素数の掛け算」と「二つの素数の積の素因数分解」はちょうど反対の操作である。例えば素数が 3 桁程度とする。手計算でその積を計算するのは容易であるが、素因数分解をするのは容易ではない。このように双方向の操作で、一方は易しく、他方は困難であるものを**疑一方向関数**という。一般に疑一方向関数からは暗号が作られる可能性があり、この考え方によって RSA 暗号以外にもいくつかの公開鍵暗号が作られている。

問 3.3.3. 55973 を素因数分解せよ。また 223×251 を計算せよ。

このように RSA 暗号の理論は非常に簡単である。しかし、実際に利用することを考えるといくつかの問題がある。安全な暗号のためには p, q 共に 200 桁程度の大きさが必要で、このとき N, L, e, d はどれも 400 桁程度である。以下の問題がある。

1. どのようにして 200 桁もある大きな素数を見つけるか。
2. p, q を定めれば N, L は定まる。e を適当に選んだとして $ed \equiv 1 \pmod{L}$ となる d をどのように見つければよいか。
3. メッセージ $\mathcal{M}$ も 400 桁程度の数である。$\mathcal{M}^e \pmod{N}$ (400 桁の 400 桁乗) をどのように計算するか。

以下でこれらの問題を一つずつ考えていく。

3.4 具体的な計算のために (1) − ユークリッドの互除法

ユークリッド[1]の互除法は与えられた二つの自然数の最大公約数を求めるためのアルゴリズムである。ここではユークリッドの互除法を説明し、またその拡張である拡張ユークリッドの互除法も解説する。これを利用することによって合同一次方程式の解を求めることができる。

補題 3.4.1 (割り算の一意性)**.** a, b を自然数とする。このとき

$$a = qb + r$$

となる 0 以上の整数 q と $0 \leqq r < b$ を満たす整数 r が一意的に存在する。

定理 3.4.2 (ユークリッドの互除法)**.** a, b を自然数とする。$r_0 = a$, $r_1 = b$ として $i > 1$ に対して

$$r_{i-1} = q_{i-1} r_i + r_{i+1} \qquad (0 \leqq r_{i+1} < r_i)$$

[1]Euclid, BC365 頃–BC275 頃, ギリシア

として r_{i+1} を順に定める。$0 \leqq r_{i+1} < r_i$ なので、数列 $\{r_i\}$ は $r_i > 0$ である間は単調減少数列である。したがって、ある n があって $r_{n+1} = 0$ となる。このとき $\gcd(a, b) = r_n$ である。

例題 3.4.3. $\gcd(200, 144)$ を求めよ。

解答. ユークリッドの互除法により

$$\begin{aligned} 200 &= 1 \times 144 + 56 \\ 144 &= 2 \times 56 + 32 \\ 56 &= 1 \times 32 + 24 \\ 32 &= 1 \times 24 + 8 \\ 24 &= 3 \times 8 + 0 \end{aligned}$$

となり $\gcd(200, 144) = 8$ である。

問 3.4.4. $\gcd(240, 252)$ を求めよ。

ユークリッドの互除法を証明するために少し準備をする。

補題 3.4.5. a, b を自然数とする。

$$a = qb + r \qquad (0 \leqq b < r,\ q \text{ は整数})$$

とすると $\gcd(a, b) = \gcd(b, r)$ である。

証明. $d = \gcd(a, b)$ とする。d は b の約数であり、$r = a - qb$ の約数にもなるので b と r の公約数である。よって $d \mid \gcd(b, r)$ である。

$d' = \gcd(b, r)$ とする。d は b の約数であり、$a = qb + r$ の約数にもなるので a と b の公約数である。よって $d' \mid \gcd(a, b)$ である。

以上より $d = d'$ である。 □

ユークリッドの互除法の証明. 補題 3.4.5 より

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n)$$

である。$r_{n+1} = 0$ ということは r_{n-1} が r_n で割り切れるということで、すなわち $\gcd(r_{n-1}, r_n) = r_n$ である。 □

定理 1.3.5 を思いだそう。

定理 3.4.6 (定理 1.3.5)**.** a, b を正の整数とする。d を a と b の最大公約数とすると、ある整数 x, y があって

$$ax + by = d$$

となる。

この定理は整数 x, y の存在だけを主張し、具体的にどのように求めれば良いのかを示していない。ここで x, y を具体的に求めるアルゴリズム (拡張ユークリッドの互除法) を解説する。

定理 3.4.7 (拡張ユークリッドの互除法)**.** ユークリッドの互除法により $r_0 = a$, $r_1 = b$, $r_{i-1} = q_{i-1}r_i + r_{i+1}$ $(0 \leq r_{i+1} < r_i)$, $r_{n+1} = 0$ を計算する。

$r_i = x_i a + y_i b$ で x_i, y_i を定める。このとき x_n, y_n が求める s, t である。

実際に x_i, y_i を求めるには次のようにすればよい。

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i-1}r_i \\ &= (x_{i-1}a + y_{i-1}b) - q_{i-1}(x_i a + y_i b) \\ &= (x_{i-1} - q_{i-1}x_i)a + (y_{i-1} - q_{i-1}y_i)b \end{aligned}$$

であるから $x_{i+1} = x_{i-1} - q_{i-1}x_i$, $y_{i+1} = y_{i-1} - q_{i-1}y_i$ である。$r_0 = a = 1 \times a + 0 \times b$, $r_1 = b = 0 \times a + 1 \times b$ であるから $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$ となることに注意して x_i, y_i を順番に求める。

例題 3.4.8. $200s + 144t = \gcd(200, 144) = 8$ となる s, t を求めよ。

解答. ユークリッドの互除法は例題 3.4.3 を用いる。

$$\begin{array}{lll} x_0 = 1 & , & y_0 = 0 \\ x_1 = 0 & , & y_1 = 1 \\ x_2 = 1 - 1 \times 0 = 1 & , & y_2 = 0 - 1 \times 1 = -1 \\ x_3 = 0 - 2 \times 1 = -2 & , & y_3 = 1 - 2 \times (-1) = 3 \\ x_4 = 1 - 1 \times (-2) = 3 & , & y_4 = -1 - 1 \times 3 = -4 \\ x_5 = -2 - 1 \times 3 = -5 & , & y_5 = 3 - 1 \times (-4) = 7 \end{array}$$

よって $200 \times (-5) + 144 \times 7 = 8$ である。

問 3.4.9. $\gcd(220, 252)$ と $220s + 252t = \gcd(220, 252)$ となる s, t を求めよ。

合同一次方程式

$$ax \equiv b \pmod{n}$$

を解くことを考えよう。この方程式は $\gcd(a, n) \mid b$ のときだけ解を持つ (定理 1.3.7)。よって $\gcd(a, n) \mid b$ と仮定する。$b = b_0 \times \gcd(a, n)$ とする。これを解くには

$$ax + nq = b$$

となる整数 x, q を求めれば良い。今

$$ax_0 + nq_0 = \gcd(a, n)$$

となる x_0, q_0 は拡張ユークリッドの互除法によって求めることができる。このとき $x = b_0 x_0$, $q = b_0 q_0$ と置けば、これは $ax + nq = b$ を満たす。したがって拡張ユークリッドの互除法によって (解を持つ) 任意の合同方程式の解を少なくとも一つは求めることができる。(すべての解を求めるにはもう少し議論が必要である。)

問 3.4.10. 合同一次方程式 $240x \equiv 36 \pmod{252}$ の解を一つ求めよ。

問 3.4.11. RSA 暗号で $p = 7$, $q = 11$ とする。$e = 13$ として d を求めよ。($ed \equiv 1 \pmod{(p-1)(q-1)}$ である。)

3.5 具体的な計算のために (2) – 高速指数演算法

RSA 暗号では、大きな (400 桁程度の) 自然数 a, e, n に対して

$$a^e \pmod{n}$$

を求める必要がある。この計算は普通に行ったのでは計算機を用いても時間がかかりすぎて実行不可能である。

まず $102^{100} \pmod{123}$ を考えてみよう。例えば 100^{100} は 200 桁の数であるから、これはもっと大きい数である。これをこのままで計算するのは賢くない。少し考えると、最後に 123 で割った余りを求めるのではなく、計算途中でも 123 で割った余りに置き換えて良いということが分かる。したがって

$$\begin{aligned} 102^2 &= 10404 \equiv 72 \\ 102^3 \equiv 72 \times 102 &= 7344 \equiv 87 \\ 102^4 \equiv 87 \times 102 &= 8874 \equiv 18 \\ &\cdots \end{aligned}$$

となり、それほど大きな数を用いなくても済む。しかし、この方法でも掛け算を 100 回繰り返さなくてはならない。ここではこの計算をより高速に行う方法 (高速指数演算法) を解説する。

$102^{100} \pmod{123}$ の指数 100 を 2 進数で表すと 1100100 となる。すなわち

$$100 = 2^6 + 2^5 + 2^2$$

である。これを使うと

$$102^{100} = 102^{(2^6+2^5+2^2)} = 102^{(2^6)} \times 102^{(2^5)} \times 102^{(2^2)}$$

である。よって $102^{(2^i)}$ を計算できれば良いが $102^{(2^i)} = (102^{(2^{i-1})})^2$ なので、これは効率よく計算できる。

$$\begin{aligned} 102^{(2^0)} &\equiv 102^1 = 102 \\ 102^{(2^1)} &\equiv 102^2 = 10404 \equiv 72 \\ 102^{(2^2)} &\equiv 72^2 = 5184 \equiv 18 \\ 102^{(2^3)} &\equiv 18^2 = 324 \equiv 78 \\ 102^{(2^4)} &\equiv 78^2 = 6084 \equiv 57 \\ 102^{(2^5)} &\equiv 57^2 = 3249 \equiv 51 \\ 102^{(2^6)} &\equiv 51^2 = 2601 \equiv 18 \end{aligned}$$

したがって

$$102^{100} \equiv 18 \times 51 \times 18 \equiv 42 \pmod{123}$$

を得る。

このように $a^e \pmod{n}$ を計算する方法を**高速指数演算法**と呼ぶ。この方法だとおよそ $2\log_2 e$ 回の掛け算を行えばよい。例えば e が 400 桁程度の数であっても約 1300 回程度の掛け算で済むことになる。

問 3.5.1. 100 を二進数で表せ。またこれを用いて $1200^{100} \bmod 1234$ を求めよ。

問 3.5.2. $31^{31} \pmod{71}$, $3^{100} \pmod{127}$ を求めよ。

この方法を用いて $a^e \pmod N$ を計算するとする。先に述べたように e が 400 桁程度の数とすると約 1300 回程度の掛け算を行うことになり、また $a^{(2^i)} \pmod N$ を保存しておく “場所” (メモリー) が約 1300 個必要になる。計算機を用いた計算では、その速度だけでなく、いかにメモリーの消費を押さえるかということも重要な問題である。実際の計算では以下のようなアルゴリズムを用いることによって非常に少ないメモリーで高速指数演算法を行うことができる。

(1) a, e, N をそれぞれメモリーに書き込む。

(2) $\mathrm{ans} = 1$ をメモリーに書き込む。

(3) $e = 0$ であれば ans が求める数である。

(4) $e \equiv 1 \pmod 2$ であれば ans に $\mathrm{ans} \times \mathrm{a} \pmod{\mathrm{N}}$ を書き込む。

(5) e に $e/2$ の少数点以下を切り捨てたものを書き込む。

(6) a に $a^2 \pmod N$ を書き込む。

(7) (3) に戻る。

この方法だと必要とするメモリーは a, e, N, ans の 4 つだけである。また e は (5) によってどんどん小さくなっていくので、いつかは (3) の $e = 0$ が成り立ち、この計算は終了する。この方法で前の例 $102^{100} \pmod{123}$ を計算してみよう。

[1] $N = 123$ (以後変化しない) $e = 100$, $a = 102$, $\mathrm{ans} = 1$ (後で書き換えられる)

[2] $e \equiv 0 \pmod 2 : \mathrm{ans} = 1, \quad e = 50, \quad a = 102^2 \pmod N = 72$

[3] $e \equiv 0 \pmod 2 : \mathrm{ans} = 1, \quad e = 25, \quad a = 72^2 \pmod N = 18$

[4] $e \equiv 1 \pmod 2 : \mathrm{ans} = 1 \times 18 \pmod{\mathrm{N}} = 18, \quad e = 12, \quad a = 18^2 \pmod N = 78$

[5] $e \equiv 0 \pmod 2 : \mathrm{ans} = 18, \quad e = 6, \quad a = 78^2 \pmod N = 57$

[6] $e \equiv 0 \pmod 2 : \mathrm{ans} = 18, \quad e = 3, \quad a = 57^2 \pmod N = 51$

[7] $e \equiv 1 \pmod 2 : \mathrm{ans} = 18 \times 51 \pmod{\mathrm{N}} = 57, \quad e = 1, \quad a = 51^2 \pmod N = 18$

[8] $e \equiv 1 \pmod 2 : \mathrm{ans} = 57 \times 18 \pmod{\mathrm{N}} = 42, \quad e = 0, \quad a = 18^2 \pmod N = 78$

[9] $e = 0$ なので $\mathrm{ans} = 42$ が求める数。

見やすく表の形でまとめると以下のようになる。

ans	e	a
1	100	102
1	50	72
1	25	18
$1 \times 18 = 18$	12	78
18	6	57
18	3	51
$18 \times 51 = 57$	1	18
$57 \times 18 = 42$	0	

問 3.5.3. RSA 暗号において、秘密鍵となる二つの素数を $p = 13$, $q = 17$ とする。$N = pq$ と $e = 11$ を公開鍵とする。

(1) $L = \varphi(pq)$ を求めよ。

(2) もう一つの秘密鍵 d を求めよ。(d は $ed \equiv 1 \pmod{L}$ を満たす数。)

(3) メッセージ $m = 3$ を上の鍵で暗号化せよ。

(4) (3) で暗号化した情報を復号し、原文 ($m = 3$) が得られることを確認せよ。

3.6 電子署名と暗号解読

情報通信の際に考慮されるべきもう一つの問題を考える。それは、情報の発信源が確かにその人本人であることを確認することである。このためにも公開鍵暗号と同様の方法が用いられる。

A さんは公開鍵暗号のための公開鍵を公開していて、誰でもそれを知ることができるものとする。A さんからの通信を受ける B さんは、その情報が確かに A さんからのものであることを確認したいとしよう。このとき A さんは B さんの公開鍵で情報を暗号化し、暗文 $\mathcal{M}$ を作り、更に自分の秘密鍵でそれを暗号化し 文 $\mathcal{N}$ を作る。B さんは $\mathcal{N}$ から、A さんの公開鍵、自分の秘密鍵を使って元の情報を得ることができる。$\mathcal{M}$ から $\mathcal{N}$ を作ることができるのは A さんだけなので、B さんは確かにそれが A さんからのものであることを確認できる。

実際に利用する場合にはこれとはやや違う手順を用いることが多いが、原理的には上記の方法で情報の発信源を確認できる。これを**電子署名**という。

極論すれば、電子署名をするということは、ある文を自分の秘密鍵で暗号化することである。これを利用すると暗号解読の恐れが生じる。A さんが B さんに送った暗号文を入手した C さんが、これの解読を試みたとしよう。C さんは B さんに対して暗号文 (あるいはそれにやや手を加えたもの) に対する署名を求める。もしも B さんがこれに応えると、出来上がるものは元の情報である。したがって C さんは暗号解読に成功する。署名はあくまでも自分で作ったものに対して行うべきであり、人から頼まれたものに安易に署名をしてはいけない。

Chapter 4

巨大素数

RSA 暗号を利用するには大きな素数を用意しなくてはならない。これは RSA 暗号の強度が、その素因数分解の難しさに因るからであり、現在、安全とされている大きさは 200 桁程度の二つの素数の積である。また、鍵となる素数は他人と共有することは出来ないので、利用者の数だけ素数が必要となる。しかし 200 桁もある素数はそんなに簡単に作ることはできない。そこで実際には、数学的に素数であることが証明されなくても、素数であることが十分に確らしい数を素数と思って利用する。このような数を**産業用素数**と呼び、暗号などでの利用には十分役に立つ。ここでは、与えられた数が「素数であることが十分に確らしい」かどうかを判定する方法を解説する。

とても大きな整数の計算を計算機で行う場合は、それに対応した特別なソフトウェアを利用するか、または多倍長計算ライブラリなどを用いて自作のプログラムを書くことになる。興味があれば、色々と試してみると良いだろう。

4.1 エラトステネスのふるい

まずは、与えられた数が素数かどうかを判定する素朴な方法を紹介する。

方法 4.1.1. 与えられた数 N が素数であるためには 2 から $N-1$ までのすべての数で割り切れなければよい。

この方法を改良することを考える。

まず 2 以外の偶数は素数ではないので、計算する必要がない。また奇数は偶数で割りきれないので、割ってみる必要がない。よって次の方法を得る。

方法 4.1.2. 与えられた数 N が 2 以外の偶数ならば N は素数ではない。N は奇数であるとする。N が素数であるためには 3 から $N-1$ までのすべての奇数で割り切れなければよい。

次に N が合成数とすると $N = mn$ となる 2 以上の整数 m, n がある。このとき m, n の少なくとも一方は $\sqrt{N}$ 以下になる。したがって $\sqrt{N}$ 以下の数で割りきれなければよい。

方法 4.1.3. 与えられた数 N が 2 以外の偶数ならば N は素数ではない。N は奇数であるとする。N が素数であるためには 3 以上 $\sqrt{N}$ 以下のすべての奇数で割り切れなければよい。

N の最小の素因数は N の 1 を除く最小の約数である。したがって N が合成数ならば $N = mn$, m は素数で $m \leqq n$ となる。

方法 4.1.4. 与えられた数 N が 2 以外の偶数ならば N は素数ではない。N は奇数であるとする。N が素数であるためには 3 以上 $\sqrt{N}$ 以下のすべての素数で割り切れなければよい。ただしこの場合 $\sqrt{N}$ 以下のすべての素数を知っている必要がある。

さてこの方法では $\sqrt{N}$ 以下のすべての素数を知っている必要があるが、これを効率よく行うのが**エラトステネス**[1]**のふるい**と呼ばれる方法である。

方法 4.1.5 (エラトステネスのふるい)**.** 与えられた数 N が素数であるかどうかを判定する。

(1) 1 から N までの数 (奇数のみでもよい) をすべて書く。

(2) 1 を消す。

(3) 消されていなく、しかも ○ もついていない最小の数に ○ をつけ、その数の倍数をすべて消す。(N が消されれば N は合成数であり、この時点で計算は終了する。)

(4) $\sqrt{N}$ を越えるまで (3) を繰り返す。

(5) N が消されていなければ N は素数である。(このとき消されていない数はすべて素数である。)

エラトステネスのふるいでは N だけでなく、N 以下の素数をすべて求められる。しかしこの方法は、例えば 200 桁程度の、大きな数については実行不可能である。

問 4.1.6. エラトステネスのふるいによって 100 以下のすべての素数を求めよ。

他にも素数を判定するアルゴリズムは色々と考えられているが、大きな数を判定することは一般に難しい。そこで素数であることを完全に決定するものではないが、有効に用いられるのが、後で説明する**確率的アルゴリズム**である。

4.2 フェルマーの小定理を利用する方法

まずは先に説明したファルマーの小定理を用いて「素数でない」ことを示すことを考える。フェルマーの小定理とは、素数 p と p で割り切れない任意の整数 a に対して

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

が成り立つということであった。したがって、p が素数であるかどうかを調べるときに、適当な a、例えば $a = 2, 3$ など、に対して $a^{p-1} \pmod{p}$ を計算し、それが 1 でないならばただちに p は素数でないといえる。しかし、いくつかの a に対して、このテストをパスしたからといって p が素数であると信じる根拠としては弱い。このような p に対しては、更に以下に述べる方法を行う。

[1] Eratosthenes, BC275–BC194, ギリシア

4.3 平方剰余の相互法則、ルジャンドル記号、ヤコビ記号

p を奇素数とし a を p で割り切れない自然数とする。x を未知数とする合同方程式

$$x^2 \equiv a \pmod{p}$$

が解を持つとき a を p を法とする**平方剰余**といい、そうでないとき**平方非剰余**という。また**ルジャンドル**[1]**記号** $\left(\frac{a}{p}\right)$ を以下のように定める。

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & (a \text{ が } p \text{ で割り切れるとき}) \\ 1 & (a \text{ が } p \text{ を法とする平方剰余のとき}) \\ -1 & (a \text{ が } p \text{ を法とする平方非剰余のとき}) \end{cases}$$

(かっこの中は分数ということではないので、約分などしてはいけない。)

例 4.3.1. $p = 7$ とするとき

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1$$

なので、1, 2, 4 は平方剰余であり 3, 5, 6 は平方剰余ではない。よって

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

である。

問 4.3.2. $\left(\frac{a}{11}\right)$, $a = 1, 2, \cdots, 10$, を求めなさい。

ルジャンドル記号について次が成り立つ。

定理 4.3.3. p を奇素数、a, b は自然数とする。

(1) $a \equiv b \pmod{p}$ ならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ である。

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(3) b が p で割り切れないならば $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ である。

(4) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

[1] Legendre, 1752–1833, フランス

(5) [**平方剰余の相互法則**] q を p と異なる奇素数とするとき $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ である。書き換えると $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$ である。

注意. $\left(\frac{-1}{p}\right)$ は $p \equiv 1 \pmod 4$ のとき 1 で $p \equiv 3 \pmod 4$ のとき -1 である。$\left(\frac{2}{p}\right)$ は $p \equiv 1, 7 \pmod 8$ のとき 1 で $p \equiv 3, 5 \pmod 8$ のとき -1 である。$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ は $p \equiv 3 \pmod 4$ かつ $q \equiv 3 \pmod 4$ のとき -1 で、それ以外のとき 1 である。

例題 4.3.4. $\left(\frac{24}{31}\right)$ を求めなさい。

解答. 定理 4.3.3 (2) より

$$\left(\frac{24}{31}\right) = \left(\frac{2}{31}\right)^3\left(\frac{3}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right)$$

である。また (4) より

$$\left(\frac{2}{31}\right) = (-1)^{(31^2-1)/8} = (-1)^{120} = 1$$

である。(5), (1) より

$$\left(\frac{3}{31}\right) = (-1)^{(3-1)(31-1)/4}\left(\frac{31}{3}\right) = (-1)^{15}\left(\frac{1}{3}\right) = (-1) \times 1 = -1$$

以上より $\left(\frac{24}{31}\right) = -1$ となる。

問 4.3.5. $\left(\frac{21}{31}\right)$ を求めなさい。

素因数分解が出来るならば定理 4.3.3 を使ってルジャンドル記号を計算することができるが、大きな数では素因数分解は難しい。そこでルジャンドル記号を拡張する。

n を奇数とし a を整数とする。n の素因数分解を

$$n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

とするとき

$$J(a,n) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_r}\right)^{e_r}$$

と置いて、これを**ヤコビ**[1]**記号**という。すぐに分かるように n が素数ならばヤコビ記号はルジャンドル記号と等しい。したがってヤコビ記号はルジャンドル記号の一般化であるといえる。ヤコビ記号について定理 4.3.3 と同じようなことが成り立つ。

[1] Jacobi, 1804–1851, ドイツ

定理 4.3.6. n を奇数、a, b は自然数とする。

(1) $a \equiv b \pmod{n}$ ならば $J(a,n) = J(b,n)$ である。

(2) $J(ab,n) = J(a,n)J(b,n)$

(3) $\gcd(a,n) > 1$ ならば $J(a,n) = 0$ である。

(4) $J(1,n) = 1$, $J(-1,n) = (-1)^{(n-1)/2}$, $J(2,n) = (-1)^{(n^2-1)/8}$

(5) a, b が互いに素な奇数のとき $J(a,b)J(b,a) = (-1)^{(a-1)(b-1)/4}$ である。書き換えると $J(a,b) = (-1)^{(a-1)(b-1)/4}J(b,a)$ である。

例題 4.3.7. $J(26,45)$ を求めなさい。

解答. 定理 4.3.6 (2) より

$$J(26,45) = J(2,45)J(13,45)$$

である。(4) より $J(2,45) = -1$ である。また (5) より

$$J(13,45) = (-1)^{(13-1)(45-1)/4}J(45,13) = J(6,13) = J(2,13)J(3,13)$$

$J(2,13) = -1$ で

$$J(3,13) = (-1)^{(3-1)(13-1)}J(13,3) = J(1,3) = 1$$

となるから、まとめると $J(26,45) = 1$ である。

$J(a,b)$ の計算の要点は a が偶数ならば $a = 2^e a_0$ (a_0 は奇数) とし、$J(a,b) = J(2,b)^e J(a_0,b)$ とすることである。こうすることによって (5) が利用でき、より小さい数の計算に帰着できる。ここでは偶数を 2 で割っているだけで、素因数分解はしていない。

問 4.3.8. $J(28,45)$ を求めなさい。

この方法によって大きな a, b に対してもヤコビ記号 $J(a,b)$ を効率よく計算できる。

この節の最後に、後で利用するためにルジャンドル記号についての一つの結果を示しておく。

定理 4.3.9. p を素数 a を自然数とするとき

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

証明はやや難しいので、その雰囲気だけを説明する。まず a が p で割り切れるならば両辺共に 0 となり、定理は成り立つ。a が平方剰余であるとする。$\left(\frac{a}{p}\right) = 1$ である。このとき、ある自然数 b があって $a \equiv b^2 \pmod{p}$ である。よって

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$$

となり、定理は成り立つ。a が平方剰余でないとすると $\left(\frac{a}{p}\right) = -1$ である。$a^{(p-1)/2} \pmod{p}$ は 2 乗すると 1 になるので ± 1 のいずれかであり、実際に -1 となることが分かっている。

4.4 素数判定法 (Solovay – Strassen 法)

ここでは素数判定を行う確率的アルゴリズムの一つである Solovay – Strassen 法を解説する。計算にはヤコビ記号と高速指数演算法を用いる。

定理 4.4.1 (Solovay – Strassen 法)**.** p を正の奇数とする。

(1) $1 < a < p-1$ をランダムにとる。

(2) $\gcd(a,p) > 1$ なら p は合成数である。

(3) $j \equiv a^{(p-1)/2} \pmod{p}$ を求める (高速指数演算法)。

(4) $J(a,p)$ を求める。

(5) $j \not\equiv J(a,p) \pmod{p}$ ならば p は合成数である。

(6) $j \equiv J(a,p) \pmod{p}$ ならば p が合成数である確率は 1/2 以下である。

p が素数であるならば $\left(\frac{a}{p}\right) = J(a,p)$ なので定理 4.3.9 より $j \equiv J(a,p) \pmod{p}$ が成り立つはずである。p が素数でないならば、一般にこれは成り立たないという事実を利用している。確率が 1/2 以下ということは以下の例を見ると様子が分かる。(200 以下の p についての表を示す。)

p	個数	Solovay – Strassen 法で合成数と判定できない a
25	2	7, 18
45	2	19, 26
49	4	18, 19, 30, 31
65	6	8, 14, 18, 47, 51, 57
85	6	13, 16, 38, 47, 69, 72
91	16	9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82
105	6	8, 13, 41, 64, 92, 97
117	2	53, 64
121	8	3, 9, 27, 40, 81, 94, 112, 118
125	2	57, 68
133	16	11, 12, 27, 30, 31, 39, 58, 64, 69, 75, 94, 102, 103, 106, 121, 122
145	6	12, 17, 59, 86, 128, 133
153	6	35, 55, 64, 89, 98, 118
165	2	34, 131
169	10	19, 22, 23, 70, 80, 89, 99, 146, 147, 150
175	4	24, 51, 124, 151
185	6	36, 43, 68, 117, 142, 149

選ばれ得る a は $p-3$ 個あり、表を見ると合格する数はいずれも $(p-3)/2$ 個以下である。表にない合成数 (9, 15, 21, 27, 33, 35, 39, 51, 55, 57, 63, 69, 75, 77, 81, 87, 93, 95,

99, 111, 115, 119, 123, 129, 135, 141, 143, 147, 155, 159, 161, 171, 177, 183, 187, 189, 195) はいずれも任意の a に対して合成数であることが判定できる。

Solovay – Strassen 法では、合成数である確率が 1/2 以下であることを保証してくれるが、このままでは素数でない確率も高く、素数としては使えない。合成数である確率を低くするためには Solovay – Strassen 法を異なる多くの a について行い、すべての判定に合格したものを使えばよい (正確にはこれを繰り返して行う方法を Solovay – Strassen 法と言うべきである)。例えば 10 回の判定に合格した数が合成数である確率は $1/2^{10} = 1/1024$ 以下である。(上記の表にある数ばかりを選んだ場合である。)

問 4.4.2. 奇数 p に対する Solovay – Strassen 法で a を用いて合成数と判定できないとすると $p - a$ を用いても合成数と判定できないことを示せ。

おわりに

「日常の生活には小学校、あるいは中学校程度の数学があれば十分で、それ以上のことは必要はない」などという人がいる。確かに普段の生活で、難しい数学を意識する必要はないだろう。しかし、ここで学んだ符号や暗号は意識することはなくても日常の生活の中で利用されている。それを完全に理解する必要はないが、「使われている」ということを知っていることには意味がある。存在を知らないことと、存在は知っているが詳しくは知らないということには大きな違いがある。これ以外にも日常の中に利用されている数学などの科学を見付けてみてもらいたい。

また、ここで使われた数学の多くは、このような形で利用されることを意識して研究されたわけではなく、純粋に「知」への欲求から得られたものである。最先端の研究は、それが解決されたからといって、すぐに何かの役に立つというわけではない。しかし、そのうちのいくつかは遠い将来、何かの役に立つことであろう。そして、それが何であるかは今の我々には分からない。

ここで学んだ内容を更に勉強するための文献を紹介する。符号、暗号、ともにきちんと学ぶためには数学の知識が不可欠であるが、比較的読みやすい本として、符号については [4]、暗号については [3] がある。また専門的に学びたいのであれば、線形代数について [2]、代数学全般について [1] をお薦めする。(番号はいずれもテキストの最後にある参考文献リストの番号である。)

問題の解答

計算問題の解答のみを示し、証明などは省略する。

問 1.1.1. 順に 4, 1, X.
問 1.2.1. 順に 7, 4.
問 1.3.3. $x \equiv 7 \pmod 9$.
問 1.3.9. $(x, y) = (4, -3)$ など。
問 1.3.10. $(x, y) = (2, -4)$ など。
問 1.3.11. 存在しない。
問 2.1.3. $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 4 \\ 3 & 3 & 1 \end{pmatrix}$
問 2.1.4. $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
問 2.4.3. s は任意の数とする。(1) $(x, y, z) = (2, 1, 1)$ (2) 解なし
(3) $(x, y, z) = (0, 0, 3)$ (4) $(x, y, z) = (-2 + s, 3 - 2s, s)$
(5) $(x, y, z, u) = (-6 + s, 16 - 3s, s, -4)$ (6) $(x, y, z) = (3s, -5s, 7s)$
問 2.4.4. (1) $(x, y, z) = (1, 1, 1)$ (2) 解なし
問 2.4.9. 例えば (1 2 3), (0 1 2). 2 次元
問 2.4.10. 例えば (1 1 0), (0 1 1). 2 次元
問 2.4.13. 例えば (1 0 -1), (0 1 -1).
問 2.4.14. 例えば (1 0 0 1), (0 1 0 1), (0 0 1 1).
問 2.5.3. $1 + 23 + {}_{23}C_2 + {}_{23}C_3 = 2048$.
問 3.1.1. `NAGANOKENMATSUMOTOSHI`
問 3.1.2. 45 個、10 個。
問 3.2.3. 101, 103, 107 など。
問 3.2.6. 例えば 28.
問 3.2.15. $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$.
問 3.2.17. 23.
問 3.3.2. $N = 33$, $L = 30$, $d = 3$ であり $15^7 \equiv 27 \pmod{33}$, $27^3 \equiv 15 \pmod{33}$.
問 3.3.3. $55973 = 223 \times 251$, $223 \times 251 = 55973$.
問 3.4.4. 12
問 3.4.9. $\gcd(220, 252) = 4$, $(s, t) = (8, -7)$.
問 3.4.10. $x = 249$.
問 3.4.11. $d = 37$.

問 3.5.1. 1100100, 926.
問 3.5.2. $31^{31} \equiv 68 \pmod{71}$, $3^{100} \equiv 79 \pmod{127}$.
問 3.5.3. (1) $L = 192$ (2) $d = 35$ (3) $3^{11} \equiv 126 \pmod{221}$ (4) $126^{35} \equiv 3 \pmod{221}$.
問 4.3.2. 順に $1, -1, 1, 1, 1, -1, -1, -1, 1, -1$.
問 4.3.5. -1.
問 4.3.8. -1.

参考文献

[1] 永尾汎、代数学、朝倉書店、1983. (ISBN4-254-11434-6)

[2] 佐竹一郎、線形代数学、裳華房、1958. (ISBN4-7853-1301-3)

[3] 澤田秀樹、暗号理論と代数学、海文堂、1997. (ISBN4-303-72330-4)

[4] 内田興二、有限体と符号理論、SGC ライブラリ **5**, サイエンス社、2000. (ISSN0386-8257)