# 数学集中講義

# 高校数学でみる応用数学　～整数編～

吉田　信夫

**大学への数学　13 年 12 月号　掲載**

数学は様々な分野で応用されている．本稿では，整数論が暗号理論に応用されていることを紹介する．暗号の意味と，現在も使われる RSA 暗号の原理を簡単に紹介したい．説明に「合同式」を用いるので，不慣れなら，本誌 2013 年 11 月号などを参照してほしい．

さて，ここで言う暗号は，クイズ番組などで登場する類いのものではなく，

1) ルールに基づいて文字列を別の文字列に変換

2) 変換された文字列から元の文字列を復元

が数学的になされるものである．さらに，実用上は，通信の過程で第 3 者に傍受される可能性があるため，

3) 第 3 者には，暗号文と作成ルールからは復元困難

でなければならない．つまり，安全性の保証である．

まずは，順番の入れ替えの基本．“シャッフルの周期性”の問題 (2002 年の東大理科前期 ) から．

**問題** 1．$N$ を正の整数とする．$2N$ 個の項からなる数列 $\{a_1,\ a_2,\ \cdots\cdots,\ a_N,\ b_1,\ b_2,\ \cdots\cdots,\ b_N\}$ を

$$\{b_1,\ a_1,\ b_2,\ a_2,\ \cdots\cdots,\ b_N,\ a_N\}$$

という数列に並べ替える操作を「シャッフル」と呼ぶことにする．並べ替えた数列は $b_1$ を初項とし，$b_i$ の次に $a_i$，$a_i$ の次に $b_{i+1}$ が来るようなものになる．また，数列 $\{1,\ 2,\ \cdots\cdots,\ 2N\}$ をシャッフルしたときに得られる数列において，数 $k$ が現れる位置を $f(k)$ で表す．

たとえば，$N=3$ のとき，$\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ をシャッフルすると $\{4,\ 1,\ 5,\ 2,\ 6,\ 3\}$ となるので，

$$f(1)=2,\ f(2)=4,\ f(3)=6,$$
$$f(4)=1,\ f(5)=3,\ f(6)=5$$

である．

（1）　数列 $\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}$ を 3 回シャッフルしたときに得られる数列を求めよ．

（2）　$1\leqq k\leqq 2N$ を満たす任意の整数 $k$ に対し，$f(k)-2k$ は $2N+1$ で割り切れることを示せ．

（3）　$n$ を正の整数とし，$N=2^{n-1}$ のときを考える．数列 $\{1,\ 2,\ 3,\ \cdots\cdots,\ 2N\}$ を $2n$ 回シャッフルすると，$\{1,\ 2,\ 3,\ \cdots\cdots,\ 2N\}$ にもどることを証明せよ．

**解**　（1）　順にシャッフルしていくと

$$\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}$$
$$\to\ \{5,\ 1,\ 6,\ 2,\ 7,\ 3,\ 8,\ 4\}$$
$$\to\ \{7,\ 5,\ 3,\ 1,\ 8,\ 6,\ 4,\ 2\}$$
$$\to\ \mathbf{\{8,\ 7,\ 6,\ 5,\ 4,\ 3,\ 2,\ 1\}}$$

となる ( ちょうど逆の並びになった ).

（2）　$1\leqq k\leqq N$ のとき，

$$f(k)=2k$$
$$\therefore\quad f(k)-2k=0$$

より，$2N+1$ で割り切れる．

$N+1\leqq k\leqq 2N$ のとき，

$$f(k)=2(k-N)-1=2k-(2N+1)$$
$$\therefore\quad f(k)-2k=-(2N+1)$$

より，$2N+1$ で割り切れる．

以上で示された．

（3）　$N=2^{n-1}$ なので，（2）より，

$$f(k)\equiv 2k\pmod{2^n+1}$$

である．ここで，シャッフルを $m$ 回行った後に $k$ が現れる位置を $f^m(k)$ と表すことにする ($f^1(k)=f(k)$)．すると，証明すべきは，

$$f^{2n}(k)=k$$

が成り立つことである．

まず，

$$f^{m+1}(k)=f(f^m(k))\equiv 2f^m(k)\pmod{2^n+1}$$

であるから，

$$f^m(k)\equiv 2^m k\pmod{2^n+1}$$

が成り立つ．特に，$m=2n$ のとき，

$$f^{2n}(k)\equiv 2^{2n}k\pmod{2^n+1}$$

である．さらに，

$$2^{2n}=(2^n)^2\equiv(-1)^2=1\pmod{2^n+1}$$

より，

$$f^{2n}(k)\equiv k\pmod{2^n+1}$$

である．$1\leqq f^{2n}(k)\leqq 2N=2^n$ であるから，

$$f^{2n}(k)=k$$

である．これで題意は示された．

*　　*

本問で登場した $f(k)$ は集合 $A=\{1,\ 2,\ \cdots\cdots,\ 2N\}$ から $A$ への関数である．これを用いると，文字列の変換を行うことができる．例えば，$N=4$ $(n=3)$ のとき，（1）から，

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $f(k)$ | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |

なので，1，2，3，4，5，6，7，8 ( アルファベット ) を並べた文字列 ( 平文 : plaintext)

$$p=132615$$

を，各文字を $f$ に代入することで，

$$c=264321$$

という文字列 ( 暗号文 : ciphertext) を作ること ( 暗号化 ) ができる．しかも，（3）から，

$$f^6(k)=k$$

なので，

$$f^5(f(k))=k$$

となる．つまり，関数 $f^5$ を用いると，暗号文から平文を求めること ( 復号化 ) ができる：

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $f^5(k)$ | 5 | 1 | 6 | 2 | 7 | 3 | 8 | 4 |

と分かるので，これを用いれば，暗号文

$$c=264321$$

から，平文

$$p=132615$$

を逆に求めることができる．

これで暗号条件 1)，2) は満たされる．

では，暗号の条件 3) : 安全性はどうだろうか？

某所 X に秘密情報を送りたい人物 $p$ は，X が指定するルール $f$ で暗号化した文を送る ($f$ は一般に公開されている )．その暗号文を第 3 者 $q$ に傍受されたとしよう．すると，少し数学を知っていれば，$f^5$ が復号化関数になっていることが分かるので，$q$ は $p$ の秘密情報を簡単に知ることができる．

これでは暗号条件 3) は満たされず，実用化できない．

＊　　＊

では，本題の RSA 暗号について説明していこう．暗号というと「乱数のようなむちゃくちゃな数列を利用するのかな？」などと考えるかも知れないが，この暗号はそんなものではない．実は，整数論の有名定理「フェルマーの小定理」を利用するのである．まずは，定理の確認を，次の問題 (2010 年阪大後期 ) で行おう．

**問題 2.** $p$ は素数，$r$ は正の整数とする．以下の問いに答えよ．

（1） $x_1$，$x_2$，……，$x_r$ についての式 $(x_1+x_2+\cdots\cdots+x_r)^p$ を展開したときの単項式 $x_1^{p_1}x_2^{p_2}\cdots\cdots x_r^{p_r}$ の係数を求めよ．ここで，$p_1$，$p_2$，……，$p_r$ は 0 または正の整数で $p_1+p_2+\cdots\cdots+p_r=p$ をみたすとする．

（2） $x_1$，$x_2$，……，$x_r$ が正の整数のとき，

$$(x_1+x_2+\cdots\cdots+x_r)^p-(x_1^p+x_2^p+\cdots\cdots+x_r^p)$$

は $p$ で割り切れることを示せ．

（3） $r$ は $p$ で割り切れないとする．このとき，$r^{p-1}-1$ は $p$ で割り切れることを示せ．

**解** （1） $x_1+x_2+\cdots\cdots+x_r=☆$ とおく．☆を順に $p$ 個かけるので，展開して得られる項は，「1 個目の☆から $x_○$，2 個目の☆から $x_△$，……などと，各☆から 1 つずつ項を選んで，単項式を作る」と考える．すると，$x_1^{p_1}x_2^{p_2}\cdots\cdots x_r^{p_r}$ の形は，

「$p$ 個の☆から，$x_1$ を選ぶ☆を $p_1$ 個決める」

「$(p-p_1)$ 個の☆から，$x_2$ を選ぶ☆を $p_2$ 個決める」

……

と考えて作ることになる．このような作り方の個数が求める係数になる．その個数は，「$p_1$ 個の $x_1$，$p_2$ 個の $x_2$，……」を並べる“同じものを含む順列”で考えることができるので，求める係数は，

$$\frac{p!}{p_1!\,p_2!\cdots\cdots p_r!}$$

である．

（2） $(x_1+x_2+\cdots\cdots+x_r)^p-(x_1^p+x_2^p+\cdots\cdots+x_r^p)$ を展開すると，（1）より，

$$\frac{p!}{p_1!\,p_2!\cdots\cdots p_r!}\,x_1^{p_1}x_2^{p_2}\cdots\cdots x_r^{p_r}$$

$(p_1,\ p_2,\ \cdots\cdots,\ p_r$ はすべて $p$ と異なる ) という形の項の和になる ( 例えば，$p_1=p$ でその他が 0 のものが $x_1^p$ になり，差を計算したら消えている )．

（1）より $\dfrac{p!}{p_1!\,p_2!\cdots\cdots p_r!}$ は整数であるが，分母に登場する自然数は $0\leqq p_k<p$ $(1\leqq k\leqq r)$ より，素因数として $p$ を含まない．つまり，約分しても分子の $p$ が残る．

よって，$\dfrac{p!}{p_1!\,p_2!\cdots\cdots p_r!}$ はすべて $p$ の倍数であるから，$x_1$，$x_2$，……，$x_r$ が正の整数のとき，

$$(x_1+x_2+\cdots\cdots+x_r)^p-(x_1^p+x_2^p+\cdots\cdots+x_r^p)$$

は $p$ で割り切れることが分かる．以上で示された．

（3）（2）で $x_k=1$ $(1\leqq k\leqq r)$ とすることで，

$$(1+1+\cdots\cdots+1)^p-(1^p+1^p+\cdots\cdots+1^p)$$
$$=r^p-r$$

は $p$ で割り切れることになるので，

$$r^p-r=Np \quad (N\text{は自然数})$$
$$\therefore \quad r(r^{p-1}-1)=Np$$

とおける．$r$ が素数 $p$ で割り切れないので，$r^{p-1}-1$ が $p$ で割り切れることが分かる．以上で示された．

＊　　＊

問題 2（3）から分かる通り，一般に，素数 $p$ と整数 $r$ に対し，

$$r^p\equiv r \pmod p$$

が成り立つ．さらに，『$r$ が $p$ の倍数でないとき，

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

が成り立つ』が，これが「フェルマーの小定理」である．

入試問題でよく見かけるテーマであり，『マスター・オブ・整数』には，全く異なる鮮やかな証明法も紹介されているので，ぜひ，参照していただきたい．

念のために確認しておこう．

$p=5$ のとき，$r=1,\ 2,\ 3,\ 4$ を考えると

$$1^4=1 \pmod 5$$
$$2^4=16\equiv 1 \pmod 5$$
$$3^4=81\equiv 1 \pmod 5$$
$$4^4=256\equiv 1 \pmod 5$$

である．

では，これがどのように暗号に利用されるかを，次の問題で見ていこう．

問題 3.　2 つの素数 $p=5$，$q=11$ の積 $n=55$ を考える．また，$N=(p-1)(q-1)=40$ とする．$1<e<N$ の範囲から，$N$ と互いに素な自然数として $e=7$ を選ぶ．$m$ は $1\leqq m<n$ を満たす自然数とするとき，次の問いに答えよ．（必要ならば，問題 2 の結果を用いて良い）

（1）　$m=3$ のとき，$m^e=3^7$ を $n=55$ で割った余りを求めよ．

（2）　$m^4$ を 5 で割った余りを求めよ．

（3）　$N$ と互いに素な自然数 $d$ $(1<d<N)$ で，$de=7d$ を $N=40$ で割った余りが 1 になるものを求め，$m^{de}$ を $n=55$ で割った余りを求めよ．

解　（1）　以下，合同式は mod 55 とする．

$$3^4=81\equiv 26,\ 3^6\equiv 26\cdot 9=234\equiv 14,$$
$$\therefore \quad 3^7\equiv 14\cdot 3\equiv 42$$

より，求める余りは **42** である．

（2）　$m$ が 5 の倍数のとき，$m^4$ を 5 で割った余りは **0** である．

$m$ が 5 の倍数でないとき，問題 2 より，

$$m^{5-1}\equiv 1 \pmod 5$$

であるから，$m^4$ を 5 で割った余りは **1** である．

（3）　40 と 7 は互いに素である．40 を 7 で割ると，

$$40=5\cdot 7+5$$

となる．次に，7 を 5 で割ると，

$$7=1\cdot 5+2$$

となる．さらに，5 を 2 で割ると，

$$5=2\cdot 2+1$$

となる．これらを利用すると，

$$1=5-2\cdot 2$$
$$=5-2(7-1\cdot 5)=3\cdot 5-2\cdot 7$$
$$=3(40-5\cdot 7)-2\cdot 7=3\cdot 40-17\cdot 7$$
$$\therefore \quad -17\cdot 7\equiv 1 \pmod{40}$$

となる（“ユークリッドの互除法”という計算法）．

$$-17\equiv 23 \quad \therefore \quad 23\cdot 7\equiv 1 \pmod{40}$$

より，$d=23$ は求める $d$ の 1 つである．

7 と 40 が互いに素より，$7D\equiv 1 \pmod{40}$ となるのは

$$D=23,\ 23\pm 40,\ 23\pm 80,\ \cdots\cdots$$

であるから，求める $d$ $(1<d<40)$ は

$$d=\mathbf{23}$$

のみである $(23\cdot 7=161)$．

次に，$m^{ed}=m^{161}$ を $n=55$ で割った余りを考える．それには，5，11 で割った余りが分かれば良い（それを保証する定理は“中国の剰余定理”と呼ばれている）．

まず，問題 2 から，$m^{10}$ を 11 で割った余りを求めよう．

$m$ が 11 の倍数のとき，$m^{10}$ を 11 で割った余りは 0 である．$m$ が 11 の倍数でないとき，

$$m^{11-1}\equiv 1 \pmod{11}$$

であるから，$m^{10}$ を 11 で割った余りは 1 である．

1)　$m$ が 5，11 の倍数でないとき，

$$m^4\equiv 1 \pmod 5,\ m^{10}\equiv 1 \pmod{11}$$
$$\therefore \quad m^{161}\equiv m(m^4)^{40}\equiv m \pmod 5$$
$$m^{161}=m(m^{10})^{16}\equiv m \pmod{11}$$

である．5，11 で割った余りがいずれも $m$ と合同なので，

$$m^{161}\equiv m \pmod{55}$$

となる．

2)　$m$ が 5 の倍数のとき，

$$m^{161} \equiv 0 \equiv m \pmod 5$$

である．$m\ (<55)$ は 11 の倍数でないから，1) と同様に，

$$m^{10} \equiv 1 \quad \therefore \quad m^{161} \equiv m \pmod{11}$$

より，

$$m^{161} \equiv m \pmod{55}$$

となる．

3)　$m$ が 11 の倍数のとき，

$$m^{161} \equiv 0 \equiv m \pmod{11}$$

である．$m\ (<55)$ は 5 の倍数でないから，1) と同様に，

$$m^4 \equiv 1 \quad \therefore \quad m^{161} \equiv m \pmod 5$$

より，

$$m^{161} \equiv m \pmod{55}$$

となる．

以上から，$m^{161}$ を 55 で割った余りは $\boldsymbol{m}$ である．

＊　　＊

$1 \leqq m < 55$ で $m^{7 \cdot 23} \equiv m \pmod{55}$ ……　(＊)

と分かった．これが，どんな暗号化，復号化につながるか見ていこう．

実は，{1，2，……，54} に対し，暗号化関数が

$f(m)=$（$m^7$ を 55 で割った余り）

であり，復号化関数が

$g(k)=$（$k^{23}$ を 55 で割った余り）

である．

具体例で考えよう．2 を暗号化すると，

$2^7=128 \equiv 18 \pmod{55}$　$\therefore$　$f(2)=18$

である．これを復号化 $(g(18)=2)$ するには，

$18^{23} \equiv ? \pmod{55}$

を計算する．すると，$18^{23} \equiv 2 \pmod{55}$ となるので，$g(18)=2$ と分かるのである．

これで，$f$，$g$ が暗号条件 1)，2) を満たしていることが分かった．その裏付けが (＊) なのである．

ここで，暗号化について少し補足しておこう．

上記の関数 $f$ は，1，2，……，54 という 54 個の数を $f(1)$，$f(2)$，……，$f(54)$ という数に変えるルールである．つまり，01，02，……，54 の 54 種類の記号を並べた文字列 ( 平文 ) を，$f(1)$，$f(2)$，……，$f(54)$ を並べた文字列 ( 暗号文 ) に変換するのである (1 文字ずつではなく，決まった長さの文字列に区切って変換する )．

＊　　＊

これが公開鍵暗号 (RSA 方式 ) の原理である．

実際に運用するには，$e=7$，$n=55$ ( 公開鍵 ) を公開し，$d=23$ ( 秘密鍵 ) が第 3 者に漏れないようにする．しかし，$e$，$n$ から $d=23$ が簡単に見つかるので，傍受されたら，第 3 者に解読されてしまうのではないか？

もちろん，対策は講じられている．$p$，$q$ を十分大きい素数にするのである (150 桁以上 )．すると，公開される $n=pq$ は非常に大きくなる (300 桁以上 ) ので，高性能のコンピュータでも，$n$ を素因数分解して $p$，$q$ を求めることは困難になる．これで，$N=(p-1)(q-1)$ が簡単には分からなくなる．そして，$N$ と互いに素な $e$ が公開されているのだが，秘密鍵 $d$ を求めるには，さらに，

$$de \equiv 1 \pmod N$$

を解かなければならない ( 問題 3（3）の前半のように，ユークリッドの互除法を実行する )．

このように，$p$，$q$ を十分大きくすれば，公開鍵 $e$，$n$ から秘密鍵 $d$ を求めるためには，途方もない計算量が必要になる．現実的には特定不可能となるのである．

しかし，第 3 者は，数学的解読法を作りたいわけではなく，情報を盗み取りたいだけである．ゆえに，数学的攻撃が無理なら，別の手段を考える．では，あなたが第 3 者なら，どのようにして暗号を解読するだろうか？

1 つ 1 つシラミツブシで特定していくような力技で攻めるのではないだろうか．つまり，変換ルールが

$f(m)=$（$m^7$ を 55 で割った余り）

だと分かっていたら，$m=1$，2，……，54 を $f(m)$ に代入して，

$f(1)=$（$1^7$ を 55 で割った余り）$=1$，

$f(2)=$（$2^7$ を 55 で割った余り）$=18$，

……

$f(53)=$（$53^7$ を 55 で割った余り）$=37$

（$53^7 \equiv (-2)^7 \equiv -18 \equiv 37 \pmod{55}$ より），

$f(54)=$（$54^7$ を 55 で割った余り）$=54$

（$54^7 \equiv (-1)^7 = -1 \equiv 54 \pmod{55}$ より）

を求める．少し頑張れば，完全な対応表

| $m$ | 1 | 2 | …… | 53 | 54 |
|---|---|---|---|---|---|
| $f(m)$ | 1 | 18 | …… | 37 | 54 |

が得られ，暗号文から簡単に平文を復元できるのである．

しかし，$n$ $(=pq)$ が 300 桁の自然数だったとしたら？すべて代入する力技で解読できるだろうか？

「大きな素数」により，RSA 暗号は，暗号条件 3)：安全性も満たす．大きな素数が暗号の番人であるのは，とても興味深い．ちなみに，大きい素数といえば，2013 年 1 月に発見された 48 個目のメルセンヌ素数

$2^{57\,885\,161}-1=581887\cdots\cdots285951$ (17 425 170 桁 )

が有名だが…暗号作成に使うにはさすがに大き過ぎる．

（よしだ　のぶお，予備校講師）