算数

上越教育大学　中川仁

平成 24 年 4 月

小学校で，算数を教えるためのバックグランドとなる数学的知識を持ってもらうことが本講義の目的である．中川担当分では，代数的な知識として，初等整数論についてのいくつかの話題について解説したい．

具体的には，例えば，小学校で分数の約分をするときには，約数とか，倍数，最小公倍数などが必要となる．それに関連して，素数もでてくる．また，分数を小数になおすと，どうなるか，それはなぜなのか．そういったことについて，小学生の素朴な疑問に答えられるか，それとも，これはそうなるんだから覚えなさい，といってごまかしてしまうのか．きちんと答えるためには，バックグランドとなる数学的知識が必要である．この授業では，少しでもそういったバックグランドで数学的にもおもしろいものを伝えたい．

目 次

1　約数，倍数，素数

自然数 a, b について，$a = bc$ となる自然数 c が存在するとき，b は a の**約数**，a は b の**倍数**という．

例えば，$15 = 3 \times 5$ より，3 は 15 の約数，15 は 3 の倍数．

6 の約数は，$1, 2, 3, 6$.

$$1 + 2 + 3 = 6.$$

12 の約数は $1, 2, 3, 4, 6, 12$.

$$1 + 2 + 3 + 4 + 6 = 16 > 12. \qquad (12 \text{ は過剰数})$$

15 の約数は $1, 3, 5, 15$.

$$1 + 3 + 5 = 9 < 15. \qquad (15 \text{ は不足数})$$

28 の約数は，$1, 2, 4, 7, 14, 28$

$$1 + 2 + 4 + 7 + 14 = 28.$$

6, 28 のように，自然数 n について，n 以外の n の約数の和が n になるとき，いいかえれば，n の約数の和が $2n$ となるとき，n は**完全数**であるという．28 の次の完全数は 496 である．

$$\begin{aligned} 496 \text{ の約数の和} &= 1 + 2 + 4 + 8 + 16 + 31 \times 1 + 31 \times 2 + 31 \times 4 + 31 \times 8 + 31 \times 16 \\ &= (1 + 2 + 4 + 8 + 16) + 31(1 + 2 + 4 + 8 + 16) \\ &= (1 + 2 + 4 + 8 + 16)(1 + 31) \\ &= 31 \times 32 = 31 \times 16 \times 2 = 2 \times 496. \end{aligned}$$

$$6 = 2 \times 3 = 2^1(2^2 - 1), \qquad 28 = 4 \times 7 = 2^2(2^3 - 1), \qquad 496 = 16 \times 31 = 2^4(2^5 - 1).$$

$a = 1 \times a$ より，1 と a は a の約数である．自然数 $p > 1$ について，p の約数が 1 と p だけのとき，p は**素数**であるという．素数を小さい方から順に挙げると，

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad \ldots.$$

このように，素数は不規則に現れる．

与えられた自然数 n が素数かどうかを判定する．

$$n \text{ が素数でない} \Longrightarrow n = ab, \quad 1 < a, b < n \text{ とかける}$$

$1 < a \leq b < n$ としてよい．そのとき，

$$a^2 \leq ab = n, \qquad a \leq \sqrt{n}.$$

したがって，n が素数でなければ，n は約数 $a,\ 1 < a \leq \sqrt{n}$ を持つ．a が素数ならば，n は素数 $a,\ 1 < a \leq \sqrt{n}$ で割り切れる．a が素数でなければ，a の 1 より大きな約数で最小のものを p とすれば，p は素数であり，n は p で割り切れる．いずれの場合も，

$$n \text{ が素数でない} \Longrightarrow n \text{ は } \sqrt{n} \text{ 以下の素数 } p \text{ で割り切れる}$$

このことから，

$$n \text{ は } \sqrt{n} \text{ 以下の素数 } p \text{ で割り切れない} \Longrightarrow n \text{ が素数である}$$

例 1.1. 109 は素数か？ $100 = 10^2 < 109 < 11^2 = 121$ より，$10 < \sqrt{109} < 11$．したがって，素数 $2, 3, 5, 7$ で割り切れなければ素数である．明らかに，2,5 では割り切れない．

$$109 = 3 \times 36 + 1,$$
$$109 = 7 \times 15 + 4.$$

よって，109 は素数．

例 1.2. 119 は素数か？ $100 = 10^2 < 119 < 11^2 = 121$ より，$10 < \sqrt{119} < 11$．素数 $2, 3, 5, 7$ で割り切れなければ素数である．明らかに，2,5 では割り切れない．

$$119 = 3 \times 39 + 2,$$
$$119 = 7 \times 17.$$

よって，119 は素数ではない．

素数は無数に存在するか？

定理 1.3 (ユークリッド)**.** 素数は無数に存在する．

[証明] $p_1, p_2, \cdots, p_n$ を相異なる素数とするとき，これら以外の素数が必ず存在することを示せばよい．

$$A = p_1 p_2 \cdots p_n + 1$$

とおく．もし，A が素数ならば，A はどの p_i よりも大きいから，これは，$p_1, p_2, \ldots, p_n$ と異なる素数である．また，A が素数でないとすると，A の 1 と A 以外の約数が存在する．そのような約数で最小のものを p とすると，p は素数である．A は素数 p で割り切れる．しかし，

$$A = p_i(p_1 \cdots p_{i-1} p_{i+1} \cdots p_n) + 1$$

であるから，A を p_i で割ると 1 余る．ゆえに，$p \neq p_i,\ i = 1, \ldots, n$ である． □

練習問題 1. $\sqrt{200} = 10\sqrt{2} = 14.142\ldots$ であることを用いて，200 以下のすべての素数を求めよ．

2　ユークリッドの互除法とその応用

自然数 a, b の**最大公約数**を $\gcd(a, b)$ で表す．例えば，

$$\left.\begin{array}{ll} 21 \text{ の約数は，} & 1,\ 3,\ 7,\ 21 \\ 35 \text{ の約数は，} & 1,\ 5,\ 7,\ 35 \end{array}\right\} \Longrightarrow 21 \text{ と } 35 \text{ の最大公約数は } 7,\ \gcd(21, 35) = 7.$$

同様に，

$$\left.\begin{array}{ll} 35 \text{ の約数は，} & 1,\ 5,\ 7,\ 35 \\ 46 \text{ の約数は，} & 1,\ 2,\ 23,\ 46 \end{array}\right\} \Longrightarrow 35 \text{ と } 46 \text{ の最大公約数は } 1,\ \gcd(35, 46) = 1.$$

$\gcd(a, b) = 1$ のとき，a と b は**互いに素**であるという．a, b が大きいとき，$\gcd(a, b)$ を効率よく求めよう．

補題 2.1. 自然数 a, b に対して，a を b で割ったときの余りを r とすれば，$\gcd(a, b) = \gcd(b, r)$.

[証明]　$m = \gcd(a, b),\ n = \gcd(b, r)$ とおく．a を b で割ったときの商を q とすれば，

$$a = bq + r, \qquad 0 \le r < b.$$

$a = ma',\ b = mb',\ a', b'$ は整数，とかく．そのとき，

$$r = a - bq = ma' - mb'q = m(a' - b'q).$$

よって，m は b と r の公約数．したがって，$m \le n$. 同様に，$b = nb'',\ r = nr'',\ b'', r''$ は整数とかく．そのとき，

$$a = bq + r = nb''q + nr'' = n(b''q + r'').$$

よって，n は a と b の公約数．したがって，$m \ge n$. ゆえに，$m = n$. □

定理 2.2 (ユークリッドの互除法)**.** 自然数 a, b に対して，

$$\begin{aligned} a &= bq_0 + r_1, & 0 < r_1 < b, \\ b &= r_1q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2, \\ &\cdots\cdots\cdots & \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n & \end{aligned}$$

とすると，$\gcd(a, b) = r_n$.

[証明]　補題 2.1 によって，$\gcd(a,b) = \gcd(b,r_1)$．これを繰り返せば，

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

例 2.3. $\gcd(1995, 1029)$ を求める．

$$\begin{aligned} 1995 &= 1029 \times 1 + 966, \\ 1029 &= 966 \times 1 + 63, \\ 966 &= 63 \times 15 + 21, \\ 63 &= 21 \times 3. \end{aligned}$$

したがって，$\gcd(1995, 1029) = 21$.

ユークリッドの互除法の応用
整数 a, b が与えられたとき，$d = \gcd(a,b)$ とすると，

$$ax + by = d \tag{2.1}$$

を満たすような整数 x, y を見つけることができる．これを具体例で説明する．

例 2.4. $\gcd(197, 41)$ を求める．

$$\begin{aligned} 197 &= 41 \times 4 + 33, \\ 41 &= 33 \times 1 + 8, \\ 33 &= 8 \times 4 + 1, \\ 8 &= 1 \times 8. \end{aligned}$$

よって，$\gcd(197, 41) = 1$ となる．この計算を利用して，

$$197x + 41y = 1$$

を満たす整数 x, y を 1 組見つけることができる．

$$\begin{aligned} 1 &= 33 - 8 \times 4 \\ &= 33 - (41 - 33 \times 1) \times 4 = 33 \times 5 - 41 \times 4 \\ &= (197 - 41 \times 4) \times 5 - 41 \times 4 = 197 \times 5 - 41 \times 24. \end{aligned}$$

したがって，$197 \times 5 + 41 \times (-24) = 1$.

練習問題 2. 2012 と 419 の最大公約数 d を求めよ．さらに，$2012x + 419y = d$ を満たす整数 x, y を一組求めよ．

3　合同式

m を自然数とする．整数 a, b の差 $a-b$ が m で割り切れるとき，

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

とかき，a と b は m を**法として合同**であるという．例えば，$m=9$ とする．

$$10 \equiv 1 \pmod{9}, \qquad 25 \equiv 7 \pmod{9}.$$

次が成り立つ．

命題 3.1. $a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ ならば，$a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$.

[証明]　$a-b=ms$, $c-d=mt$, s,t は整数とかける．そのとき，

$$(a+c)-(b+d)=m(s+t), \quad (a-c)-(b-d)=m(s-t)$$

であるから，$a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$ である．

$$ac-bd=ac-bc+bc-bd=c(a-b)+b(c-d)=cms+bmt=m(cs+bt)$$

であるから，$ac \equiv bd \pmod{m}$ である．　□

例 3.2. $m=9$ とする．

$$\begin{aligned}
10 &\equiv 1 \pmod{9},\\
10^2 &\equiv 1^2 \equiv 1 \pmod{9},\\
427 &\equiv 4\times 10^2+2\times 10+7 \equiv 4+2+7 \equiv 13 \equiv 4 \pmod{9},\\
513 &\equiv 5\times 10^2+1\times 10+3 \equiv 5+1+3 \equiv 9 \equiv 0 \pmod{9}.
\end{aligned}$$

$m=11$ とする．

$$\begin{aligned}
10 &\equiv -1 \pmod{11},\\
10^2 &\equiv (-1)^2 \equiv 1 \pmod{11},\\
321 &\equiv 3\times 10^2+2\times 10+1 \equiv 3+2\times(-1)+1 \equiv 2 \pmod{11},\\
726 &\equiv 7\times 10^2+2\times 10+6 \equiv 7+2\times(-1)+6 \equiv 11 \equiv 0 \pmod{11}.
\end{aligned}$$

定理 3.3 (フェルマーの小定理)**.** p を素数とし，a を p で割り切れない整数とする．そのとき，

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

が成り立つ．

[証明]　$p=7$, $a=3$ とすると，

$$\begin{aligned}
3\cdot 1 &\equiv 3 \pmod 7, \qquad 3\cdot 4 \equiv 5 \pmod 7,\\
3\cdot 2 &\equiv 6 \pmod 7, \qquad 3\cdot 5 \equiv 1 \pmod 7,\\
3\cdot 3 &\equiv 2 \pmod 7, \qquad 3\cdot 6 \equiv 4 \pmod 7.\\
(3\cdot 1)(3\cdot 2)(3\cdot 3)(3\cdot 4)(3\cdot 5)(3\cdot 6) &\equiv 3\cdot 6\cdot 2\cdot 5\cdot 1\cdot 4 \pmod 7,\\
3^6 6! &\equiv 6! \pmod 7,\\
6!(3^6-1) &\equiv 0 \pmod 7.
\end{aligned}$$

よって，$6!(3^6-1)$ は7で割りきれる．$6!$ は素数7で割り切れないから，3^6-1 は7で割り切れる． □

例 3.4. $p=7$ のとき，$2^6-1=63=7\times 9$, $5^6-1=15624=7\times 2232$.
$p=11$ のとき，$2^{10}-1=1023=11\times 93$, $3^{10}-1=59048=11\times 5368$.

応用として，2^{125} を7で割った余りを求めてみる．フェルマーの小定理より，$2^6\equiv 1 \pmod 7$ である．割り算によって，$125=6\times 20+5$ であるから，

$$2^{125}=2^{6\times 20+5}=2^{6\times 20}2^5=(2^6)^{20}2^5.$$

ここで，

$$2^6\equiv 1 \pmod 7, \qquad (2^6)^{20}\equiv 1^{20}\equiv 1 \pmod 7$$

であるから，

$$2^{125}=(2^6)^{20}2^5\equiv 1\times 2^5\equiv 32\equiv 4 \pmod 7.$$

定理 3.5 (ウィルソンの定理)**.** p を素数とすれば，$(p-1)!+1$ は p で割り切れる．

[証明]　$p=11$ ならば，$9\times 5\equiv 1 \pmod{11}$, $8\times 7\equiv 1 \pmod{11}$, $6\times 2\equiv 1 \pmod{11}$, $4\times 3\equiv 1 \pmod{11}$ であるから，

$$\begin{aligned}
10! &= 10\times 9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1\\
&= 10\times (9\times 5)\times (8\times 7)\times (6\times 2)\times (4\times 3)\times 1\\
&\equiv (-1)\times 1\times 1\times 1\times 1\times 1\equiv -1 \pmod{11}.
\end{aligned}$$

□

例 3.6. $(5-1)!+1=25=5\times 5$, $(7-1)!+1=721=7\times 103$,
$(11-1)!+1=3628801=11\times 329891$.

練習問題 3. 2^{1000} を7で割ったときの余りを求めよ．

4　有理数

有理数は，有限小数かまたは循環小数として表せる．これは，なぜか？

$\frac{1}{7}$ を小数に直してみる．

$$
\begin{array}{r|l}
 & 0.142857 \\
\hline
7 & 1.000000 \\
 & 0 \\
\hline
 & 10 \\
 & 7 \\
\hline
 & 30 \\
 & 28 \\
\hline
 & 20 \\
 & 14 \\
\hline
 & 60 \\
 & 56 \\
\hline
 & 40 \\
 & 35 \\
\hline
 & 50 \\
 & 49 \\
\hline
 & 1
\end{array}
$$

よって，

$$\frac{1}{7} = 0.142857142857\cdots\cdots = 0.\dot{1}42857\dot{}$$

有理数を既約分数として，$\frac{a}{b}, b > 0$ とかく．$b > 1$ とする．

$\frac{a}{b}$ が有限小数にならない $\Longrightarrow$ 小数に直す割り算において，余りは 0 でない

余りは 1 から $b-1$ までの整数

$\Longrightarrow$ b 回以上割り算すれば，同じ余りが現れる

そこから先の割り算は，同じ計算を繰り返す．

よって，循環小数になる．

次に，分子を変えるとどうなるか．結果は次のようになる．

$$\frac{1}{7} = 0.\dot{1}42857\dot{}\,, \quad \frac{3}{7} = 0.\dot{4}28571\dot{}\,, \quad \frac{2}{7} = 0.\dot{2}85714\dot{}\,,$$
$$\frac{6}{7} = 0.\dot{8}57142\dot{}\,, \quad \frac{4}{7} = 0.\dot{5}71428\dot{}\,, \quad \frac{5}{7} = 0.\dot{7}14285\dot{}\,.$$

これは

$$\frac{1}{7} = 0.\dot{1}42857\dot{}$$

の両辺を 10 倍して，整数部分を引けば，6 個の有理数 $\frac{a}{7}$, $a = 1, 2, 3, 4, 5, 6$ はすべて現れる．

今度は，循環節の長さについて考えてみる．$\frac{1}{7} = 0.\dot{1}42857\dot{}$ の循環節の長さは，$6 = 7 - 1$ である．なぜ 6 なのか？

$$10 \equiv 3 \pmod 7, \quad 10^2 \equiv 2 \pmod 7, \quad 10^3 \equiv 6 \pmod 7,$$
$$10^4 \equiv 4 \pmod 7, \quad 10^5 \equiv 5 \pmod 7, \quad 10^6 \equiv 1 \pmod 7.$$

したがって，$10^s \equiv 1 \pmod 7$ を満たす**最小の自然数** s は 6 である．特に，$10^6 - 1$ は 7 で割りきれる．実際，割り算すれば，

$$10^6 - 1 = 7 \times 142857 \qquad (\textbf{本質的に } 1 \div 7 \textbf{ の筆算の結果と同じ}).$$

定理 4.1. p を 2, 5 以外の素数として，s を $10^s \equiv 1 \pmod p$ を満たす最小の自然数とする．$\frac{a}{p}$, $a = 1, \ldots, p-1$ を循環小数で表したときの循環節の長さは丁度 s であり，それは $p - 1$ の約数である．

例 4.2. $p = 13$ とする．フェルマーの小定理により，$10^{12} \equiv 1 \pmod{13}$ である．

$$\begin{aligned}
&10^2 \equiv (-3)^2 \equiv 9 \equiv -4 \pmod{13},\\
&10^3 \equiv 10^2 \times 10 \equiv (-4) \times (-3) \equiv 12 \equiv -1 \pmod{13},\\
&10^4 \equiv (-3)(-1) \equiv 3 \pmod{13},\\
&10^6 \equiv (10^3)^2 \equiv (-1)^2 \equiv 1 \pmod{13}.
\end{aligned}$$

したがって，$10^s \equiv 1 \pmod{13}$ を満たす**最小の自然数** s は 6 である．特に，$10^6 - 1$ は 13 で割りきれる．実際，割り算すれば，

$$10^6 - 1 = 13 \times 76923, \quad \frac{1}{13} = 0.\ 076923\ 076923\ \cdots = 0.\dot{0}76923\dot{}. \tag{4.1}$$

を意味している (**本質的に** $1 \div 13$ **の筆算の結果と同じである**)．この両辺を 10 倍して，整数部分を引けば，6 個の有理数 $\frac{a}{13}$, $a = 1, 10, 9, 12, 3, 4$ はすべて現れて，

$$\frac{1}{13}, \quad \frac{10}{13}, \quad \frac{9}{13}, \quad \frac{12}{13}, \quad \frac{3}{13}, \quad \frac{4}{13}$$

の小数展開を得る．また，(4.1) に 2 をかければ，

$$2(10^6 - 1) = 13 \times 2 \times 76923 = 13 \times 153846, \quad \frac{2}{13} = 0.\dot{1}53846\dot{}.$$

この両辺を 10 倍して，整数部分を引けば，6 個の有理数 $\frac{a}{13}$, $a = 2, 7, 5, 11, 6, 8$ はすべて現れて，

$$\frac{2}{13}, \quad \frac{7}{13}, \quad \frac{5}{13}, \quad \frac{11}{13}, \quad \frac{6}{13}, \quad \frac{8}{13}$$

の小数展開を得る．

練習問題 4. $p = 13$ のとき，$10^s \equiv 1 \pmod{13}$ を満たす最小の自然数 s を求めよ．また，そのとき，$10^s - 1$ を 13 で割った商を求めよ．さらに，$\dfrac{a}{13}, a = 1, \ldots, 12$ を効率よく循環小数に直せ．

5　分母同士，分子同士を加えた有理数

$\dfrac{1}{3}$ と $\dfrac{1}{2}$ の間にある有理数で分母が最小のものは何か？

$$\frac{1}{3} = 0.333\cdots, \qquad \frac{1}{2} = 0.5$$

であるから，分母が 4 の有理数は

$$\frac{1}{4} = 0.25, \quad \frac{3}{4} = 0.75$$

だからこの間にはない．分母が 3 の有理数は

$$\frac{1}{3} = 0.333\cdots, \quad \frac{2}{3} = 0.666\cdots$$

だからこの間にはない．また，$\dfrac{2}{5} = 0.4$ はこの間にある．よって，答えは $\dfrac{2}{5}$ である．

同様に，$\dfrac{2}{5}$ と $\dfrac{3}{7}$ の間にある有理数で分母が最小のものは何か？実は，答えは $\dfrac{2+3}{5+7} = \dfrac{5}{12}$ である．前の問題の答えも $\dfrac{2}{5} = \dfrac{1+1}{2+3}$ である．

一般には次が成り立つ．

定理 5.1. 2 つの正の既約分数 $\dfrac{a}{b} > \dfrac{c}{d}$ が $ad - bc = 1$ を満たすとき，これらの間にある有理数 $\dfrac{y}{x}$ で，分母 x が最小になるものは

$$\frac{a+c}{b+d}$$

である．

[証明]

$$\frac{a}{b} > \frac{y}{x} > \frac{c}{d}$$

とする．これは，

$$ax - by > 0, \qquad dy - cx > 0$$

と同じである．

$$ax - by = u, \qquad dy - cx = v$$

とおけば，$u > 0$, $v > 0$ であり，これらは整数であるから，$u \geq 1$, $v \geq 1$ である．そのとき，x, y を u, v で表せば，

$$\begin{aligned} ax - by &= u, \\ -cx + dy &= v, \end{aligned}$$

$$\begin{aligned} adx - dby &= du, \\ -bcx + bdy &= bv, \end{aligned}$$

より，$(ad-bc)x = du+bv$ である．$ad-bc = 1$ より，$x = du+bv$ である．同様に，

$$\begin{aligned} acx - bcy &= cu, \\ -acx + ady &= av, \end{aligned}$$

より，$(ad-bc)y = cu+av$ である．$ad-bc = 1$ より，$y = cu+av$ である．$u \geq 1$, $v \geq 1$ より，$x = du+bv \geq d+b$ であり，等号は $u = v = 1$ のときに限り成り立つ．$u = v = 1$ のとき，$y = c+a$ である． □

注意 5.2.

1. 定理 5.1 において，

$$a(b+d) - b(a+c) = ad - bc = 1$$

であるから，$a+c$ と $b+d$ の公約数は 1 以外にない．よって，$\dfrac{a+c}{b+d}$ は既約分数である．

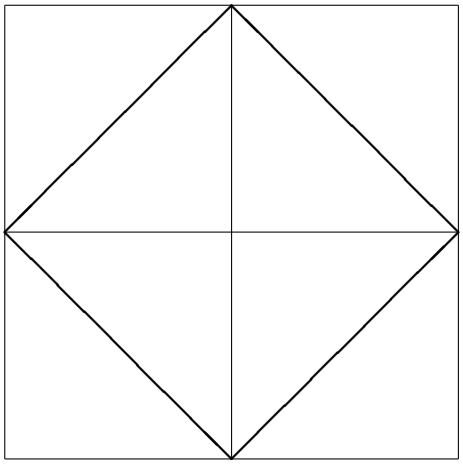
2. $ad - bc > 1$ のときも，

$$\frac{a}{b} > \frac{a+c}{b+d} > \frac{b}{d}$$

は成り立つ．

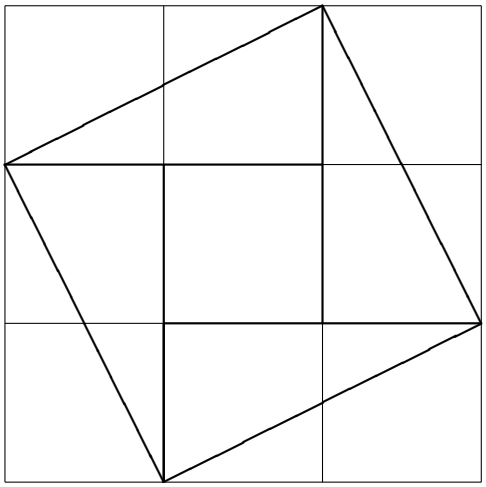
6　無理数

一辺の長さが 1 の正方形を対角線によって 2 等分して，面積 1/2 の四つの直角二等辺三角形を組み合わせて正方形を作ると，その面積は 2 である．したがって，その一辺の長さを a とすれば，$a^2 = 2$ である．a を 2 の正の平方根といい，$a = \sqrt{2}$ と表す.



$\sqrt{2}$ は有理数ではないことを示そう．$\sqrt{2}$ が有理数であると仮定して矛盾を導く．$\sqrt{2} = \dfrac{n}{m}$, m, n は互いに素な自然数とかけたとする．$2 = \dfrac{n^2}{m^2}$, $2m^2 = n^2$．左辺は偶数であるから，右辺の n^2 も偶数である．したがって，n は偶数である．$n = 2k$ とかくと，$2m^2 = 4k^2$, $m^2 = 2k^2$ となる．この右辺は偶数であるから，左辺の m^2 も偶数である．したがって，m も偶数である．これは，m, n が互いに素であることに矛盾する．

練習問題 5. 長さが 1 の正方形からなる格子を使って，一辺の長さが $\sqrt{5}$ の正方形を作れ．また，一辺の長さが $\sqrt{13}$ の正方形を作れ.



7　2つの平方数の和

$2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $10 = 1^2 + 3^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$ のように，自然数が 2 つの平方数の和に表せるのはどんなときだろうか？

まず，次の定理を証明する．

定理 7.1. p を奇素数とする．$z^2 \equiv -1 \pmod{p}$ を満たす整数 z が存在するための必要十分条件は，$p \equiv 1 \pmod{4}$ である．

[証明]　$p = 4k + 1$ とする．$p - 1, p - 2, \ldots, 2k + 2, 2k + 1$ は，

$$p - a, \quad a = 1, 2, \ldots, 2k$$

と表せるから，

$$\begin{aligned}
(p-1)! &= \{(p-1)(p-2)\cdots(p-2k+1)(p-2k)\} \times \{(2k)(2k-1)\cdots 2\cdot 1\} \\
&= \{1\cdot(p-1)\}\{2\cdot(p-2)\}\cdots\{(2k-1)(p-2k+1)\}\{2k(p-2k)\} \\
&\equiv (-1^2)(-2^2)\cdots(-(2k-1)^2)(-(2k)^2) \pmod{p} \\
&= (-1)^{2k}\{(2k)!\}^2 = \{(2k)!\}^2.
\end{aligned}$$

したがって，$z = (2k)!$ とおけば，ウィルソンの定理 (定理 3.5) より，

$$z^2 + 1 = \{(2k)!\}^2 + 1 \equiv (p-1)! + 1 \equiv 0 \pmod{p}.$$

逆に，$z^2 \equiv -1 \pmod{p}$ を満たす整数 z が存在したとする．もし，$p = 4k + 3$ とすれば，フェルマーの小定理 (定理 3.3) によって，$z^{p-1} \equiv 1 \pmod{p}$ である．しかし，

$$z^{p-1} = (z^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} = -1 \pmod{p}$$

であるから，$1 \equiv -1 \pmod{p}$, $2 \equiv 0 \pmod{p}$ となって矛盾である．ゆえに，$p = 4k + 1$ の形である．　□

定理 7.2. p を 3 以上の素数とする．そのとき，p が 2 つの平方数の和に表せるための必要十分条件は，$p \equiv 1 \pmod{4}$ である．

[証明]　$p = x^2 + y^2$, x, y は自然数とかけたとする．そのとき，

$$\begin{aligned}
&x, y \text{ ともに偶数} \Longrightarrow p = x^2 + y^2 \text{ も偶数となり，矛盾．} \\
&x, y \text{ ともに奇数} \Longrightarrow x^2, y^2 \text{ とも奇数} \\
&\qquad\qquad \Longrightarrow p = x^2 + y^2 \text{ は偶数となり，矛盾．}
\end{aligned}$$

したがって，x, y の一方は奇数でもう一方は偶数である．$x = 2x_1 + 1$, $y = 2y_1$ とすると，

$$p = (2x_1 + 1)^2 + (2y_1)^2 = 4x_1^2 + 4x_1 + 1 + 4y_1^2 = 4(x_1^2 + x_1 + y_1^2) + 1.$$

よって，$p \equiv 1 \pmod 4$.

逆は，参考資料の通り． □

a^2+b^2 は複素数を使うと，

$$(a+bi)(a-bi) = a^2+b^2$$

と表せる．これから

$$(2\text{つの平方数の和}) \times (2\text{つの平方数の和}) = 2\text{つの平方数の和}$$

がわかる．例えば，$1^2+2^2=5$, $2^2+3^2=13$ より，

$$\begin{aligned}
65 &= 5 \times 13 = (1^2+2^2)(2^2+3^2) \\
&= (1+2i)(1-2i)(2+3i)(2-3i) \\
&= \{(1+2i)(2+3i)\}\{(1-2i)(2-3i)\} \\
&= (2-6+4i+3i)(2-6-4i-3i) = (-4+7i)(-4-7i) \\
&= (-4)^2+7^2 = 4^2+7^2, \\
65 &= \{(1+2i)(2-3i)\}\{(1-2i)(2+3i)\} \\
&= (2+6+4i-3i)(2+6-4i+3i) = (8+i)(8-i) \\
&= 8^2+1^2.
\end{aligned}$$

練習問題 6. 17 を 2 つの平方数の和に表せ．29 を 2 つの平方数の和に表せ．17×29 を 2 つの平方数の和に表せ．