平成 30 年度　上越教育大学公開講座

はじめての整数論

日時：8 月 31 日 (金)，9 月 7 日 (金)，9 月 14 日 (金)，9 月 21 日 (金)，9 月 28 日 (金)
19:00〜21:00
場所：上越教育大学　人文棟 1 階 104 教室

目次

はじめに

素数は無限に多く存在する．さらにディリクレの算術級数中の素数定理によれば，初項と公差が 1 以外の公約数をもたない自然数であるような等差数列の中にも無限に多くの素数が存在する．本講座では 2 つの等差数列 $\{4n+1\}$ と $\{4n+3\}$ についてそれぞれの中に無限に多くの素数が存在することや，それぞれの素数のもつ特徴について，具体的な計算を通して解説する．

この講座の参考書として，西来路文朗・清水健一著「素数が奏でる物語」，ブルーバックス，講談社，2015，を挙げておく．

1　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．

$a > 1$ を自然数とする．$a = 1 \times a$ より，1 と a は a の約数である．

7 の約数は 1 と 7 だけである．11 の約数も 1 と 11 だけである．このように自然数 $p > 1$ 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，

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

このように素数は非常に不規則に現れる．この素数の列は無限に続く．この事実はどうのように証明できるのだろうか？

補題 1.1. $n > 1$ を自然数とする．a を 1 より大きい n の約数の中で最小のものとする．このとき a は素数である．

[証明]　もし a が素数でないとすれば $a = bc, 1 < b < a, 1 < c < a$ と表せる (b, c は整数)．$b > 1$ は a より小さな n の約数だから，a が 1 より大きい n の約数の中で最小のものであることに矛盾する．ゆえに a は素数でなければならない．　□

定理 1.2 (ユークリッド)**.** 素数は無数に存在する．

[証明]　素数が有限個しかないと仮定する．それらを $p_1 < p_2 < \cdots < p_k$ とする．

$$n = p_1 p_2 \cdots p_k + 1$$

とおく．a を 1 より大きい n の約数の中で最小のものとする．補題 1.1 より a は素数である．素数は $p_1, p_2, \cdots, p_k$ しかないから，$a = p_i$ となる $1 \leq i \leq k$ がある．a は n の約数だから n は a で割り切れる．しかし n を $a = p_i$ で割ると 1 余るから矛盾である．　□

上の定理は背理法を用いて証明したが，その証明は単に矛盾を導いただけでなく，もう少し生産的な意味も含んでいることを説明しよう．$2, 3, 5$ という素数のリストに対して

$$2 \times 3 \times 5 + 1 = 31$$

を作れば，31 の約数の中に $2, 3, 5$ 以外の素数があると主張している．この場合は 31 自身が素数である．同様に $2, 3, 7$ という素数のリストに対して

$$2 \times 3 \times 7 + 1 = 43$$

を作れば，43 の約数の中に $2, 3, 7$ 以外の素数がある．この場合は 43 自身が素数である．$2, 3, 5, 7, 11, 13$ という素数のリストに対して

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$$

を作れば，30031 の約数の中に $2, 3, 5, 7, 11, 13$ 以外の素数がある．この場合は $30031 = 59 \times 509$ は素数ではないが，その約数の 59, 509 は素数である．

素数が無数に存在することのオイラーによる証明も紹介しよう．まず自然数の逆数の和

$$H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

を考える．N を自然数とする．$n \geq 2^N$ とすれば

$$\begin{aligned} H_n \geq H_{2^N} &= \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \cdots + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^{N-1}+1} + \cdots + \frac{1}{2^N}\right) \\ &\geq 1 + \frac{1}{2} + \overbrace{\frac{1}{4} + \frac{1}{4}}^{2} + \overbrace{\frac{1}{8} + \cdots + \frac{1}{8}}^{4} + \cdots + \overbrace{\frac{1}{2^N} + \cdots + \frac{1}{2^N}}^{2^{N-1}} \\ &= 1 + \frac{1}{2} + \overbrace{\frac{1}{2} + \cdots + \frac{1}{2}}^{N-1} = 1 + \frac{N}{2}. \end{aligned}$$

これは $n \to \infty$ のとき $H_n \to \infty$ となることを示している．

素数 p と，$n = 1, 2, \ldots$ に対して

$$S_n(p) = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{n-1}}$$

とおく．

$$S_n(p) = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{n-1}}$$
$$\frac{1}{p}S_n(p) = \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{n-1}} + \frac{1}{p^n}$$

より

$$\left(1 - \frac{1}{p}\right) S_n(p) = 1 - \frac{1}{p^n}, \qquad S_n(p) = \frac{1 - \dfrac{1}{p^n}}{1 - \dfrac{1}{p}}$$

を得る．ここで $n \to \infty$ とすれば $1/p^n \to 0$ となるから $S_n(p) \to \dfrac{1}{1 - \dfrac{1}{p}}$ である．このこ

とを

$$S(p) = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots = \frac{1}{1 - \dfrac{1}{p}}$$

と表す．N 以下の素数の全体を $2 = p_1 < p_2 < \cdots < p_r$ として積

$$P_N = \frac{1}{1 - \dfrac{1}{p_1}} \times \frac{1}{1 - \dfrac{1}{p_2}} \times \cdots \times \frac{1}{1 - \dfrac{1}{p_r}}$$

を考える．上でみたようにこれは

$$P_N = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) \cdots \left(1 + \frac{1}{p_r} + \frac{1}{p_r^2} + \cdots\right)$$

と変形される．この右辺の積を展開すれば素因数分解の一意性 (後述の定理 2.7) により N 以下の自然数はすべて $p_1 n_1 p_2^{n_2} \cdots p_r^{n_r}$ の形に一意的に表せるから上の式を展開したとき N 以下の自然数の逆数がちょうど 1 回ずつ現れ，それ以外のものも現れるから

$$P_N = \sum_{k \text{ の素因数はすべて } N \text{ 以下}} \frac{1}{k} \geq 1 + \frac{1}{2} + \cdots + \frac{1}{N} = H_N$$

が成り立つ．$N \to \infty$ のとき $H_N \to \infty$ だから $P_N \to \infty$ となる．したがって素数は無数に存在する．これは素数が単に無数に存在すること以上のことを主張している．素数が無数に存在しても非常に希にしか現れなければ $P_N \to \infty$ とはならないからである．

上の議論をもう少し精密にすることによって N 以下の素数の逆数和

$$T_N = \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}$$

を下から評価してみよう．そのためには自然対数が必要となる．

実数 $a > 1$ に対して

$$L(a) = \int_1^a \frac{1}{x}\, dx$$

とおく．$h > 0$ を小さくとれば，$a \le x \le a + h$ において $\dfrac{1}{a+h} \le \dfrac{1}{x} \le \dfrac{1}{a}$ だから

$$\frac{h}{a+h} \le L(a+h) - L(a) \le \frac{h}{a}, \quad \frac{1}{a+h} \le \frac{L(a+h)-L(a)}{h} \le \frac{1}{a},$$
$$\lim_{h \to +0} \frac{L(a+h)-L(a)}{h} = \frac{1}{a}.$$

同様に

$$\lim_{h \to -0} \frac{L(a+h)-L(a)}{h} = \frac{1}{a}.$$

したがって

$$\lim_{h \to 0} \frac{L(a+h)-L(a)}{h} = \frac{1}{a}.$$

すなわち関数 $y = L(x)$ の $x = a$ での微分係数 $L'(a)$ は $1/a$ である．つまり

$$L'(a) = \frac{1}{a}$$

である．a に対して $L'(a)$ を対応させる関数を $L'(x)$ とかけば，$L'(x) = \dfrac{1}{x}$ である．これまで $a > 1$ としてきたが，$0 < a \le 1$ でも $L(a)$ は同じ積分で定義され，$L'(a) = 1/a$ を満たす．したがって $x > 0$ で $L(x)$ が定義され，$L'(x) = 1/x$ が成り立つ．$L(1) = 0$, $L'(1) = 1$ である．$1/2 \le x \le 1$ のとき

$$-L(x) \le (1-x) + (1-x)^2 = 2 - 3x + x^2$$

が成り立つ．実際，$f(x) = x^2 - 3x + 2 + L(x)$ とおけば

$$f'(x) = 2x - 3 + \frac{1}{x} = \frac{2x^2 - 3x + 1}{x} = \frac{(2x-1)(x-1)}{x} \le 0 \quad (\frac{1}{2} \le x \le 1)$$

だから，$f(x)$ はこの区間で単調減少である．よってこの区間で $f(x) \ge f(1) = 0$ である．上で示した不等式で x を $1 - x$ で置き換えれば

$$-L(1-x) \le x + x^2, \qquad 0 \le x \le \frac{1}{2} \tag{1.1}$$

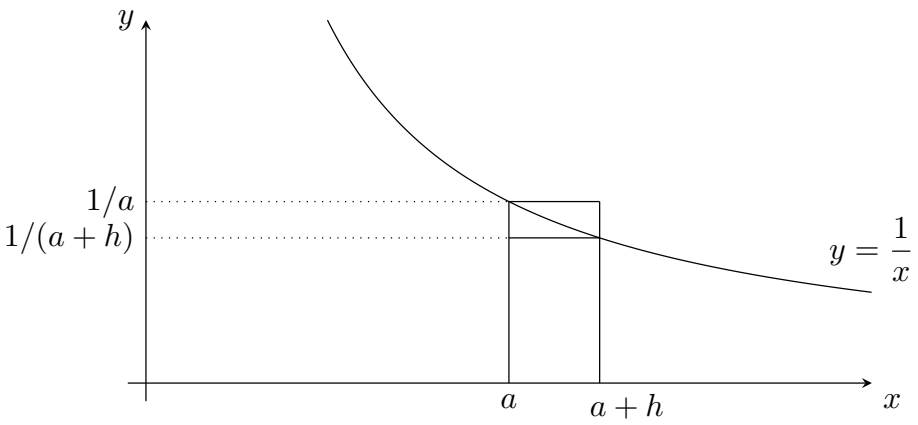

図 1　$y = 1/x$ のグラフで囲まれる図形の面積 1

が成り立つ．もう 1 つ $L(x)$ のもつ重要な性質がある．それは $a > 0, b > 0$ に対して次が成り立つことである．

(1.2)　　$$L(b/a) = L(b) - L(a).$$

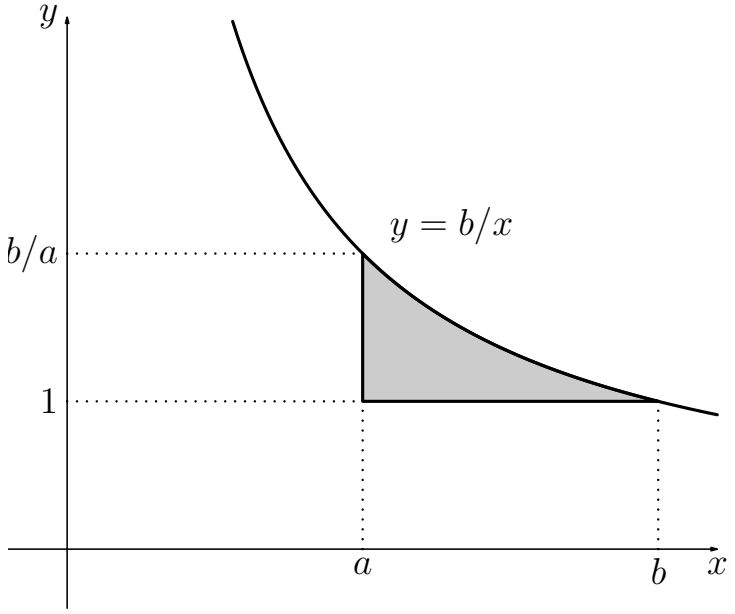

図 2　$y = 1/x$ のグラフで囲まれた図形の面積 2

(1.2) を証明しよう．$b > a$ とする．図 2 において $y = b/x$ のグラフと $x = a$, $y = 1$ で

囲まれる部分の面積を 2 通りに計算する．

$$\int_a^b \frac{b}{x}\,dx-(b-a)=b\int_a^b \frac{1}{x}\,dx-(b-a)=b\left(\int_1^b \frac{1}{x}\,dx-\int_1^a \frac{1}{x}\,dx\right)-(b-a)$$
$$=b\,(L(b)-L(a))-(b-a).$$

$y=b/x$ は $x=b/y$ とかけるから，この図形の面積は次の積分でも求まる．

$$\int_1^{b/a} \frac{b}{y}\,dy-a\left(\frac{b}{a}-1\right)=b\int_1^{b/a} \frac{1}{y}\,dy-a\left(\frac{b}{a}-1\right)$$
$$=bL(b/a)-(b-a).$$

したがって

$$b\,(L(b)-L(a))-(b-a)=bL(b/a)-(b-a),\quad L(b)-L(a)=L(b/a).$$

他の大小関係の場合にもこれは成り立つ．特に $b=1$ とすれば $L(1)=0$ より

$$L(1/a)=L(1)-L(a)=-L(a)$$

を得る．したがって

$$L(ab)=L(b/(1/a))=L(b)-L(1/a)=L(b)+L(a)=L(a)+L(b)$$

である．このように $L(x)$ は対数の性質をもっている．$L(a)$ を a の自然対数とよび，$\log a$ で表す．まとめると

$$\log a=\int_1^a \frac{1}{x}\,dx$$

であり，$\log x$ を微分すると $1/x$ になる．したがって $\log x$ は $x>0$ で単調増加である．また $0\le x\le 1/2$ に対して (1.1) が成り立つ．特に任意の素数 p に対して

$$-\log\left(1-\frac{1}{p}\right)\le\frac{1}{p}+\frac{1}{p^2} \tag{1.3}$$

が成り立つ．

自然数 k に対して $k\le x\le k+1$ のとき，$1/(k+1)\le 1/x\le 1/k$ だから

$$\frac{1}{k+1}\le\int_k^{k+1} \frac{1}{x}\,dx\le\frac{1}{k}$$

である．これを $k=1,2,\dots,N-1$ について加えれば

$$H_N-1=\frac{1}{2}+\cdots+\frac{1}{N}\le\int_1^N \frac{1}{x}\,dx=\log N\le 1+\frac{1}{2}+\cdots+\frac{1}{N-1}=H_{N-1}$$

を得る．$N \to \infty$ のとき $H_N \to \infty$ だから，$\log N \to \infty$ である．したがって $x \to \infty$ のとき $\log x \to \infty$ である．また $\log N \leq H_{N-1} < H_N$ だから $\log(\log N) < \log H_N$ である．

$P_N \geq H_N$ であった．この自然対数をとれば

$$\log P_N \geq \log H_N.$$

ここで N 以下の素数を $2 = p_1 < p_2 < \cdots < p_r$ とするとき

$$\begin{aligned}
\log P_N &= \log \frac{1}{1-\frac{1}{p_1}} + \log \frac{1}{1-\frac{1}{p_2}} + \cdots + \log \frac{1}{1-\frac{1}{p_r}} \\
&= -\log\left(1-\frac{1}{p_1}\right) - \log\left(1-\frac{1}{p_2}\right) - \cdots - \log\left(1-\frac{1}{p_r}\right) \\
&\leq \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots + \frac{1}{p_r} + \frac{1}{p_r^2} \\
&\leq \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r} + \frac{1}{p_1(p_1-1)} + \frac{1}{p_2(p_2-1)} + \cdots + \frac{1}{p_r(p_r-1)} \\
&\leq T_N + \sum_{n=2}^{N} \frac{1}{n(n-1)} = T_N + \sum_{n=2}^{N} \left(\frac{1}{n-1} - \frac{1}{n}\right) \\
&= T_N + 1 - \frac{1}{N} < T_N + 1.
\end{aligned}$$

したがって

$$T_N > \log P_N - 1 \geq \log H_N - 1 > \log(\log N) - 1$$

であり，$N \to \infty$ のとき $\log(\log N) \to \infty$ だから，N 以下の素数の逆数の和 T_N は $N \to \infty$ のとき ∞ に発散する．特に素数は無数に存在し，その逆数の和が発散する程度に頻繁に素数は現れることがわかった．

定理 1.3.

$$\sum_{p:\text{素数},\, p \leq N} \frac{1}{p} > \log(\log N) - 1.$$

$$\sum_{p:\text{素数}} \frac{1}{p} = \infty.$$

2　ユークリッドの互除法

整数 d が整数 a, b の両方の約数であるとき，d は a と b の公約数であるという．a と b の公約数で最大のものを a と b の最大公約数とよび，$\gcd(a, b)$ で表す．

例えば，21 の (正の) 約数は 1, 3, 7, 21 であり，35 の (正の) 約数は 1, 5, 7, 35 だから，1 と 7 は 21 と 35 の公約数であり，7 は 21 と 35 の最大公約数である．よって $\gcd(21, 35) = 7$ である．

a, b が大きな整数のとき，その約数をすべてリストアップすることは簡単ではない．そうしなくても最大公約数 $\gcd(a, b)$ が機械的に求める方法がある．それがユークリッドの互除法である．まず 1 つ補題を準備する．

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]　a を b で割ったときの商を q とすれば

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

d を a, b の公約数とする．$a = da_1$, $b = db_1$, a_1, b_1 は整数とかくと

$$r = a - bq = d(a_1 - b_1 q)$$

だから，d は b と r の公約数である．e を b と r の公約数として，$b = eb_2$, $r = ea_2$, a_2, b_2 は整数とかく．そのとき

$$a = bq + r = e(b_2 q + a_2)$$

だから，e は a, b の公約数である．したがって a, b の公約数の集合と b, r の公約数の集合は一致する．特に a, b の最大公約数と b, r の最大公約数も一致する．　□

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

$$\begin{aligned}
a &= ba_0 + r_1, && 0 < r_1 < b,\\
b &= r_1 a_1 + r_2, && 0 < r_2 < r_1,\\
r_1 &= r_2 a_2 + r_3, && 0 < r_3 < r_2,\\
&\cdots\cdots\cdots &&\\
r_{n-2} &= r_{n-1} a_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n a_n &&
\end{aligned}$$

とすると $\gcd(a, b) = r_n$.

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

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

□

例 **2.3.** $\gcd(2018, 831)$ を求める．

$$\begin{aligned} 2018 &= 831 \times 2 + 356, & 356 &= 2018 - 831 \times 2, \\ 831 &= 356 \times 2 + 119, & 119 &= 831 - 356 \times 2, \\ 356 &= 119 \times 2 + 118, & 118 &= 356 - 119 \times 2, \\ 119 &= 118 \times 1 + 1. & 1 &= 119 - 118 \times 1. \end{aligned}$$

したがって $\gcd(2018, 831) = 1$ である．この計算から次のようにして $2018x + 831y = 1$ を満たす整数 x, y を求めることができる．まず上の計算を，余り$=$　の形にかきなおす．これを下から順に使って

$$\begin{aligned} 1 &= 119 - 118 \times 1 = 119 - (356 - 119 \times 2) \times 1 \\ &= 119 - 356 + 119 \times 2 = 119 \times 3 - 356 \\ &= (831 - 356 \times 2) \times 3 - 356 = 831 \times 3 - 356 \times 2 \times 3 - 356 \\ &= 831 \times 3 - 356 \times 7 = 831 \times 3 - (2018 - 831 \times 2) \times 7 \\ &= 831 \times 3 - 2018 \times 7 + 831 \times 2 \times 7 = 831 \times (3 + 14) - 2018 \times 7 \\ &= 831 \times 17 - 2018 \times 7. \end{aligned}$$

よって $x = -7$, $y = 17$ は $2018x + 831y = 1$ を満たす．$(2018 \times (-7) = -14126$, $831 \times 17 = 14127)$.

上の例で示したことは一般的に成り立つ．

命題 **2.4.** 自然数 a, b の最大公約数を d とすれば

$$ax + by = d$$

を満たす整数 x, y が存在する．

系 **2.5.** p を素数とし，a を p で割り切れない自然数とすれば

$$ax + py = 1$$

を満たす整数 x, y が存在する．

命題 **2.6.** p を素数とする．整数 a, b の積 ab が p で割り切れるならば，a または b は p で割り切れる．

[証明]　a が p で割り切れないとする．系 2.5 より整数 x, y で $ax + py = 1$ となるものが存在する．また仮定より $ab = pc$ となる整数 c が存在する．このとき $1 = ax + py$ より

$$b = b \times 1 = b(ax + py) = abx + pby = pcx + pby = p(cx + by).$$

よって b は p で割り切れる．□

定理 2.7 (素因数分解の一意性)．2 以上の任意の自然数 n は有限個の素数 $p_1, \ldots, p_r$ を用いて，$n = p_1 \cdots p_r$ と素因数分解できる．またこの分解の仕方は素数 $p_1, \ldots, p_r$ の順序の違いを除いて一意的である．

[証明]　n に関する帰納法で証明する．$n = 2$ のときは明らか．$n > 2$ として，n より小さな自然数については定理の主張が正しいとする．n が素数ならば何も示すことはない．n が素数でないとすると，$n = ab$, a, b は整数，$1 < a \leq b < n$ とかける．帰納法の仮定より a, b は有限個の素数の積としてかけるので，$n = ab$ も有限個の素数の積としてかける．次に n が 2 通りの素因数分解

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (p_i,\ q_j \text{ は素数})$$

をもったとする．$n = q_1(q_2 \cdots q_s)$ は素数 p_1 で割り切れるから，命題 2.6 より q_1 または $q_2 \cdots q_s$ は p_1 で割り切れる．この議論を繰り返せば，ある i について q_i は p_1 で割り切れることがわかる．しかし q_i は素数だから $q_i = p_1$ となる．そこで $q_1, \ldots, q_s$ を並べ替えて，$q_1 = p_1$ としてよい．このとき $n' = n/p_1$ とおくと，$n' = p_2 \cdots p_r = q_2 \cdots q_s$ を得る．帰納法の仮定によって $s = r$ であり，$q_2, \cdots, q_r$ を並べ替えれば，$p_2 = q_2, \ldots, p_r = q_r$ となる．□

整数は 4 で割ったときの余りによって 4 つに分けられる．

- 4 で割りきれるもの．$4n$，n は整数とかける．
- 4 で割った余りが 1 であるもの．$4n + 1$，n は整数とかける．
- 4 で割った余りが 2 であるもの．$4n + 2$，n は整数とかける．
- 4 で割った余りが 3 であるもの．$4n + 3$，n は整数とかける．

偶数は $4n$ または $4n + 2$ とかけるものに分けられ，奇数は $4n + 1$ または $4n + 3$ とかけるものに分けられる．次のことを注意しておく．

$$\begin{aligned}
&(4m+1)(4n+1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1,\\
&(4m+3)(4n+3) = 16mn + 12m + 12n + 9 = 4(4mn + 3m + 3n + 2) + 1,\\
&(4m+1)(4n+3) = 16mn + 12m + 4n + 3 = 4(4mn + 3m + n) + 3.
\end{aligned}$$

これから特に $4n + 1$ の形の整数を何個かけても $4n + 1$ の形の整数になることがわかる．

2 以外の素数はすべて奇数である．したがって 2 以外の素数は $4n + 1$ の形のものと $4n + 3$ の形のものに分けられる．定理 1.2 によって素数は無数に存在する．それでは $4n + 1$ の形の素数，$4n + 3$ の形の素数はそれぞれ無数に存在するだろうか？

定理 2.8. $4n+3$ の形の素数は無数に存在する．

[証明]　$4n+3$ の形の素数が有限個しかないと仮定する．それらを $p_1 < p_2 < \cdots < p_k$ とする．このとき

$$N = 4p_1p_2\cdots p_k + 3$$

とおく．定理 2.7 により N は素数の積として $N = q_1q_2\cdots q_r$ と表せる (q_i は素数)．N は奇数だから各 q_i は 2 でない素数である．もし，$q_1, \ldots, q_r$ がすべて $4n+1$ の形の素数ならば，それらの積 N も $4n+1$ の形になるが，これは $N = 4p_1p_2\cdots p_k + 3$ とおいたことに矛盾する．ゆえに $q_1, \ldots, q_r$ の中に少なくとも 1 つは $4n+3$ の形の素数がある．それを q_i とする．$4n+3$ の形の素数は $p_1, p_2, \ldots, p_k$ しかないと仮定したから，$q_i = p_j$ となる．しかし N は q_i で割り切れるが，p_j で割ると 3 余るからこれは矛盾である．　□

注意 2.9. $4n+1$ の形の素数は無数に存在することは上のような方法では証明できない．$p_1 < p_2 < \cdots < p_k$ を $4n+1$ の形の素数として

$$N = 4p_1p_2\cdots p_k + 1$$

とおいて，$N = q_1q_2\cdots q_r$ をその素因数分解とする．$q_1, \ldots, q_r$ がすべて $4n+3$ の形の素数だとしても r が偶数ならば矛盾は生じないからである．$4n+1$ の形の素数は無数に存在することを証明するためには別の方法が必要になる．

注意 2.10. $2, 3$ 以外の素数は $6n+1$ または $6n+5$ の形にかける．$6n+5$ の形の素数が無数に存在することは定理 2.8 と同様に証明できる．上の注意と同様に $6n+1$ の形の素数は無数に存在することを証明するためには別の方法が必要になる．

3　合同式とフェルマーの小定理

n を 1 より大きな整数とする．整数 a, b に対して $a-b$ が n で割り切れるとき，すなわち $a-b = nc$ となる整数 c が存在するとき

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

とかいて，a と b は n を法として合同であるという．例えば，$n = 9$ とする．25 を 9 で割ったときの商は 2 で余りは 7 だから

$$25 = 9 \times 2 + 7, \quad 25 - 7 = 9 \times 2.$$

よって

$$25 \equiv 7 \pmod{9}.$$

一般に a を n で割ったときの商を q，余りを r とすれば，$a = nq + r$, $0 \leq r < n$ である．$a - r = nq$ だから

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

である．

合同式は等式と似た性質をもつ．

命題 3.1. $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ ならば次の合同式が成り立つ．

$$\begin{aligned} a + c &\equiv b + d \pmod{n}, \\ a - c &\equiv b - d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

[証明] $a - b = ns$, $c - d = nt$, s, t は整数とかける．このとき

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) = ns + nt = n(s + t), \\ (a - c) - (b - d) &= (a - b) - (c - d) = ns - nt = n(s - t) \end{aligned}$$

だから，$a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$ である．積については $a = b + ns$, $c = d + nt$ とかけるから

$$\begin{aligned} ac &= (b + ns)(d + nt) = bd + nbt + nds + n^2 st, \\ ac - bd &= nbt + nds + n^2 st = n(bt + ds + nst). \end{aligned}$$

よって $ac \equiv bd \pmod{n}$ である． □

注意 3.2. 割り算については合同式と等式では異なることに注意する．例えば a, b, c が整数で $a \neq 0$ のとき $ab = ac$ ならば $b = c$ が成り立つが，$ab \equiv ac \pmod{n}$ でも $b \equiv c \pmod{n}$ が成り立つと限らない．実際，

$$3 \times 5 \equiv 3 \times 1 \pmod{12}, \quad 5 \not\equiv 1 \pmod{12}.$$

$5 \equiv 1 \pmod{4}$ は成り立っている．

合同式を応用して，9 の倍数，11 の倍数を簡単に判定することができる．

例 **3.3.** $n = 9$ とする．

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

例 **3.4.** $n = 11$ とする．

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

命題 3.5. p を素数，a を p で割り切れない整数とすれば，整数 x で $ax \equiv 1 \pmod p$ となるものが存在する．

[証明]　系 2.5 より $ax + py = 1$ を満たす整数 x, y が存在する．$ax - 1 = -py$ だから $ax \equiv 1 \pmod p$ である． □

例えば，$p = 7$ のとき，$2 \times 4 \equiv 1 \pmod 7$, $3 \times 5 \equiv 1 \pmod 7$, $6 \times 6 \equiv 1 \pmod 7$ である．

$p = 7$, $a = 3$ とすると

$$\begin{aligned}
3 \cdot 1 &\equiv 3 \pmod 7, \quad 3 \cdot 4 \equiv 5 \pmod 7,\\
3 \cdot 2 &\equiv 6 \pmod 7, \quad 3 \cdot 5 \equiv 1 \pmod 7,\\
3 \cdot 3 &\equiv 2 \pmod 7, \quad 3 \cdot 6 \equiv 4 \pmod 7.
\end{aligned}$$

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

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．これは次のように一般的に成り立つ．

定理 3.6 (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れば

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

が成り立つ．

[証明]　まず，$ax \equiv ay \pmod{p}$ ならば $x \equiv y \pmod{p}$ であることを示す．$ax \equiv ay \pmod{p}$ とすると，$a(x-y) \equiv 0 \pmod{p}$，すなわち $a(x-y)$ は素数 p で割り切れる．a は p で割り切れないとしたから，命題 2.6 より $x-y$ は p で割り切れる．よって $x \equiv y \pmod{p}$ である．この対偶をとると，$x \not\equiv y \pmod{p}$ ならば $ax \not\equiv ay \pmod{p}$ である．したがって，x が $1, 2, \ldots, p-1$ を動くとき，ax の値は p を法として，0 でなく，また互いに合同ではない．よって ax の値は p を法として，$1, 2, \ldots, p-1$ をすべて丁度 1 回ずつとる．したがって

$$\begin{aligned}
&(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}, \\
&a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}, \\
&(p-1)!(a^{p-1}-1) \equiv 0 \pmod{p}.
\end{aligned}$$

すなわち $(p-1)!(a^{p-1}-1)$ は素数 p で割り切れる．$(p-1)!$ は p で割り切れないから，命題 2.6 より $a^{p-1}-1$ は p で割り切れる．　□

例 **3.7.** $p = 7$ 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，$125 = 6 \times 20 + 5$ だから

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

ここで $2^6 \equiv 1 \pmod{7}$, $(2^6)^{20} \equiv 1^{20} \equiv 1 \pmod{7}$ だから

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

フェルマーの小定理の証明において素数 p に対して $(p-1)!$ は p で割り切れないことを用いた．それでは $(p-1)!$ は p を法としていくつと合同になるのだろうか？

$p = 7$ のとき，$2 \times 4 \equiv 1 \pmod{7}$, $3 \times 5 \equiv 1 \pmod{7}$, $6 \times 6 \equiv 1 \pmod{7}$ だったから，

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

$p = 11$ ならば，$9 \times 5 \equiv 1 \pmod{11}$, $8 \times 7 \equiv 1 \pmod{11}$, $6 \times 2 \equiv 1 \pmod{11}$, $4 \times 3 \equiv 1 \pmod{11}$ だから

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

これは次のように一般的に成り立つ.

定理 3.8 (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]　命題 3.5 より各 $a = 1, 2, \ldots, p-1$ に対して，$ax \equiv 1 \pmod{p}$ となる x, $1 \leq x \leq p-1$ が存在する.

$$\begin{aligned} a^2 \equiv 1 \pmod{p} &\iff a^2 - 1 = (a-1)(a+1) \text{ が } p \text{ で割り切れる} \\ &\iff a-1 \text{ または } a+1 \text{ が } p \text{ で割り切れる} \\ &\iff a = 1 \text{ または } a = p-1. \qquad (1 \leq a \leq p-1 \text{ より}) \end{aligned}$$

したがって $a = 1, p-1$ を除けば，$ax \equiv 1 \pmod{p}$ を満たす x は $x \not\equiv a \pmod{p}$ である．積

$$(p-1)! = 1 \times 2 \times \cdots \times (p-2) \times (p-1)$$

において，1 と $p-1$ 以外は，積の順序をかえて，かけて p を法として 1 と合同になるようなペアに組み合わせることができるから

$$(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}.$$

□

例 3.9. $(5-1)!+1 = 25 = 5 \times 5$, $(7-1)!+1 = 721 = 7 \times 103$, $(11-1)!+1 = 3628801 = 11 \times 329891$.

演習問題 3.1. 2^{2018} を 13 で割ったときの余りを求めよ.

4　x^2+1 の素因数

$x = 1, 2, 3, \ldots$ とするとき x^2+1 の素因数にはどんな素数が現れるだろうか？

$$\begin{aligned} &1^2+1 = 2, && 7^2+1 = 50 = 2 \times 5^2, \\ &2^2+1 = 5, && 8^2+1 = 65 = 5 \times 13, \\ &3^2+1 = 10 = 2 \times 5, && 9^2+1 = 82 = 2 \times 41, \\ &4^2+1 = 17, && 10^2+1 = 101, \\ &5^2+1 = 26 = 2 \times 13, && 11^2+1 = 122 = 2 \times 61, \\ &6^2+1 = 37, && 12^2+1 = 145 = 5 \times 29. \end{aligned}$$

これからわかるように x^2+1 の素因数として現れる素数は 2 と $4n+1$ の形のもので，$4n+3$ の形のものは現れない．

命題 4.1. $4n+3$ の形の素数は x^2+1 $(x=1,2,3,\dots)$ の素因数としては現れない．

[証明]　$p=4n+3$ を素数とする．x^2+1 が p で割り切れるような自然数 x があったとする．このとき $x^2+1\equiv 0 \pmod p$ だから，$x^2\equiv -1 \pmod p$ であり，$p-1=4n+2$ だから

$$x^{p-1}=x^{4n+2}=(x^2)^{2n+1}\equiv(-1)^{2n+1}\equiv -1\equiv p-1 \pmod p$$

となる．しかし x は p で割り切れないから，フェルマーの小定理 (定理 3.6) により

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

である．$p-1\equiv x^{p-1}\equiv 1 \pmod p$ となって矛盾である． □

定理 4.2. $4n+1$ の形の素数は無数に存在する．

[証明]　$4n+1$ の形の素数が有限個しかないと仮定する．それらを $p_1<p_2<\cdots<p_k$ とする．このとき

$$N=(2p_1p_2\cdots p_k)^2+1$$

とおく．定理 2.7 により N は素数の積として $N=q_1q_2\cdots q_r$ と表せる (q_i は素数)．N は奇数だから各 q_i は 2 でない素数である．命題 4.1 より各 q_i は $4n+1$ の形の素数である．$4n+1$ の形の素数は $p_1,p_2,\dots,p_k$ しかないと仮定したから，$q_i=p_j$ となる．しかし N は q_i で割り切れるが，p_j で割ると 1 余るからこれは矛盾である． □

それでは $4n+1$ の形のすべての素数は x^2+1 $(x=1,2,3,\dots)$ の素因数として現れるだろうか？

命題 4.3. $4n+1$ の形のすべての素数は x^2+1 $(x=1,2,3,\dots)$ の素因数として現れる．

[証明]　$p=4n+1$ を素数とする．$4n=p-1$ だから，$j=1,2,\dots,2n$ のとき $2n+j=2n+1,2n+2,\dots,p-1$ である．したがって

$$(p-1)!=\overbrace{1\times 2\times\cdots\times(2n-1)\times 2n}^{2n\text{ 項}}\times\overbrace{(2n+1)\times(2n+2)\times\cdots\times(p-2)\times(p-1)}^{2n\text{ 項}}$$

であるが，$p-2n=2n+1$ だから右辺の後半部分の積は積の順序を逆にかけば

$$(p-1)\times(p-2)\times\cdots\times(p-2n)$$

と表せる．したがって

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

一方，ウィルソンの定理 (定理 3.8) により

$$(p-1)!\equiv -1 \pmod p$$

が成り立つ．したがって $x=(2n)!$ とおけば

$$x^2\equiv (p-1)!\equiv -1 \pmod p$$

となり，x^2+1 は p で割り切れる． □

例えば $p=13=4\times 3+1$ とすると $n=3$ で $x=(2n)!=6!=720$ とすれば

$$720^2+1=518401=13\times 39877.$$

もっと x の値を小さくするには $720=13\times 55+5$ より，$720\equiv 5 \pmod{13}$ だから $x=5$ とすればよい．

$$5^2+1=26=2\times 13.$$

5　2 つの平方数の和

a を整数として a^2 と表せる数を平方数とよぶ．どのような自然数が 2 つの平方数の和として表せるだろうか？

$$2=1^2+1^2,\quad 5=1^2+2^2,\quad 10=1^2+3^2,\quad 13=2^2+3^2,\quad 17=1^2+4^2,\ \ldots$$

命題 5.1. 素数 p が 2 つの平方数の和としてかけるならば，$p=2$ または $p=4n+1$ の形である．

[証明]　2 でない素数 p が 2 つの平方数の和として $p=a^2+b^2$ と表せたとする．p は奇数だから a^2, b^2 がともに偶数であることはない．a^2, b^2 がともに奇数であることもな

い．よって a^2, b^2 の一方は奇数で他方は偶数である．a^2 は奇数，b^2 は偶数であるとしてよい．このとき a は奇数，b は偶数である．$a = 2c+1$, $b = 2d$ とかけば

$$p = (2c+1)^2 + (2d)^2 = 4c^2 + 4c + 1 + 4d^2 = 4(c^2 + c + d^2) + 1.$$

□

逆に $4n+1$ の形の素数 p はすべて 2 つの平方数の和として表せるだろうか？

部屋割り論法：$n+1$ 人の旅行者が n 部屋しか空室のないホテルに宿泊するには，空室のうちのどこかの部屋に 2 人以上入るしかない．

補題 5.2. γ を実数，n を自然数とする．このとき整数 b, c で $1 \leq b \leq n$ かつ

$$\left|\gamma - \frac{c}{b}\right| \leq \frac{1}{(n+1)b}$$

を満たすものが存在する．

[証明]　0 以上 1 未満の実数の集合を I とする．$I = \{x \,|\, 0 \leq x < 1\}$．$I$ を $n+1$ 等分する．

$$I = I_0 \cup I_1 \cup I_2 \cup \cdots \cup I_n, \quad I_j = \left\{ x \;\middle|\; \frac{j}{n+1} \leq x < \frac{j+1}{n+1} \right\} \quad (j = 0, 1, \cdots, n).$$

実数 x に対して $[x]$ によって x を越えない最大の整数を表す．$[x] \leq x < [x]+1$ である．$\langle x \rangle = x - [x]$ とおけば $0 \leq \langle x \rangle < 1$ である．与えられた実数 γ に対して，$n+1$ 個の I に属する実数 $\langle k\gamma \rangle$, $k = 0, 1, \ldots, n$ を考える．これらの中で I_n に入るものがあれば，それを $\langle b\gamma \rangle$ とすると，$1 \leq b \leq n$ であり

$$\frac{n}{n+1} \leq \langle b\gamma \rangle < 1, \quad 0 < 1 - \langle b\gamma \rangle \leq \frac{1}{n+1}$$

である．$1 - \langle b\gamma \rangle = 1 - (b\gamma - [b\gamma]) = 1 + [b\gamma] - b\gamma$ だから

$$0 < 1 + [b\gamma] - b\gamma \leq \frac{1}{n+1}, \quad 0 < \frac{1 + [b\gamma]}{b} - \gamma \leq \frac{1}{(n+1)b}.$$

よって $c = 1 + [b\gamma]$ とおけば，$\left|\gamma - \dfrac{c}{b}\right| \leq \dfrac{1}{(n+1)b}$, $1 \leq b \leq n$ である．

次に $\langle k\gamma \rangle$, $k = 0, 1, \ldots, n$ のどれも I_n に入らないとする．このときこれらの $n+1$ 個の I の元は，n 個の集合 $I_0, I_1, \ldots, I_{n-1}$ のどれかに入る．したがって部屋割り論法によりどれか 2 つは同じ集合 I_j に入る．それらを $\langle k\gamma \rangle$, $\langle l\gamma \rangle$, $0 \leq k < l \leq n$ とすると

$$\frac{j}{n+1} \leq \langle l\gamma \rangle < \frac{j+1}{n+1}, \quad \frac{j}{n+1} \leq \langle k\gamma \rangle < \frac{j+1}{n+1}$$

だから

$$|\langle l\gamma\rangle| - \langle k\gamma\rangle| \leq \frac{1}{n+1}$$

である．ここで

$$\langle l\gamma\rangle - \langle k\gamma\rangle = l\gamma - [l\gamma] - (k\gamma - [k\gamma]) = (l-k)\gamma - ([l\gamma] - [k\gamma])$$

だから，$b = l - k$, $c = [l\gamma] - [k\gamma]$ とおけば，b, c は整数で $1 \leq b \leq n$ かつ

$$|b\gamma - c| \leq \frac{1}{n+1}, \quad \left|\gamma - \frac{c}{b}\right| \leq \frac{1}{(n+1)b}$$

を満たす． □

定理 5.3. $4n+1$ の形の素数 p は 2 つの平方数の和として表せる．

[証明] 命題 4.3 により自然数 x で x^2+1 が p で割り切れるものが存在する．$n = [\sqrt{p}]$ とおく．$n < \sqrt{p} < n+1$ である．この n と $\gamma = -x/p$ について補題 5.2 を適用すれば整数 b, c で $1 \leq b \leq n$ かつ

$$\left|-\frac{x}{p} - \frac{c}{b}\right| \leq \frac{1}{(n+1)b}$$

を満たすものが存在する．このとき $a = bx + cp$ とおけば

$$\frac{|a|}{bp} \leq \frac{1}{(n+1)b}, \quad |a| \leq \frac{p}{n+1} < \frac{p}{\sqrt{p}} = \sqrt{p}$$

が成り立つ．$a = bx + cp$ より $a \equiv bx \pmod{p}$ である．また $x^2 + 1 \equiv 0 \pmod{p}$ である．したがって

$$a^2 + b^2 \equiv b^2x^2 + b^2 \equiv b^2(x^2+1) \equiv 0 \pmod{p}$$

を得る．$|a| < \sqrt{p}$ かつ $1 \leq b \leq n < \sqrt{p}$ だから

$$1 \leq a^2 + b^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = p + p = 2p$$

となる．$a^2 + b^2$ は 1 以上で $2p$ 未満の p の倍数だから $a^2 + b^2 = p$ である． □

例 5.4. $p = 113$ は $4 \times 28 + 1$ とかける．$(56!)^2 + 1 \equiv 0 \pmod{113}$ である．$56! \equiv 15 \pmod{113}$ だから $15^2 + 1 \equiv 0 \pmod{113}$ である．$n = [\sqrt{113}] = 10$, $\gamma = -15/113$ とおき，$I_j = \{x \,|\, j/11 \leq x < (j+1)/11\}$ $(j = 0, 1, \ldots, 10)$ と $\langle k\gamma\rangle$ $(k = 0, 1, \ldots, 10)$ を考える．$\langle k\gamma\rangle \in I_j$ のとき，$\langle k\gamma\rangle$ の下の欄に j をかくと次の表を得る．

k	0	1	2	3	4	5	6	7	8	9	10
$[k\gamma]$	0	-1	-1	-1	-1	-1	-1	-1	-2	-2	-2
$\langle k\gamma\rangle$	0	0.86	0.73	0.60	0.46	0.33	0.20	0.07	0.93	0.80	0.67
j	0	9	8	6	5	3	2	0	10	8	7

上の表から $\langle 8\gamma\rangle \in I_{10}$ がわかる．よって $b=8$ とすると $0<1-\langle 8\gamma\rangle \le 1/11$ である．$1-\langle 8\gamma = 1+[8\gamma]-8\gamma = -1-8\gamma$ だからこれは

$$|-1-8\gamma| = \frac{8\times 15-113}{113} = \frac{7}{113} < \frac{1}{11}$$

を表している．$a=7, b=8$ は $a^2+b^2 = 49+64 = 113$ を満たす．

表から $\langle 2\gamma\rangle, \langle 9\gamma\rangle \in I_8$ もわかる．こちらを使えば，$|\langle 9\gamma\rangle - \langle 2\gamma\rangle| \le 1/11$ であり

$$\langle 9\gamma\rangle - \langle 2\gamma\rangle = 9\gamma - [9\gamma] - (2\gamma - [2\gamma]) = 7\gamma + 2 - 1 = 7\gamma + 1.$$

よって $|7\gamma+1| = |1-(7\times 15)/113| = 8/113 < 1/11$，したがって $a=8, b=7$ を得る．

素数とは限らない自然数 n が 2 つの平方数の和として表せるのはいつかについて調べる．

補題 5.5. 自然数 m と n がともに 2 つの平方数の和として表せるならば，その積 mn も 2 つの平方数の和として表せる．

[証明]　$m=a^2+b^2, n=c^2+d^2$ とかけたとすると

$$\begin{aligned}(ac-bd)^2+(ad+bc)^2 &= a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2\\ &= a^2c^2+a^2d^2+b^2d^2+b^2c^2\\ &= a^2(c^2+d^2)+b^2(d^2+c^2) = (a^2+b^2)(c^2+d^2) = mn.\end{aligned}$$

□

注意 5.6. 補題 5.5 で用いた等式は複素数の計算から次のように自然に導かれる．i を虚数単位 $(i^2=-1)$ とし，a,b,c,d を実数として $\alpha = a+bi$, $\beta = c+di$ とする．$\bar\alpha = a-bi$, $\bar\beta = c-di$ とおく．このとき

$$\begin{aligned}\alpha\bar\alpha &= (a+bi)(a-bi) = a^2-b^2i^2 = a^2+b^2,\\ \beta\bar\beta &= (c+di)(c-di) = c^2-d^2i^2 = c^2+d^2,\\ \alpha\beta &= (a+bi)(c+di) = ac+adi+bci+bdi^2 = (ac-bd)+(ad+bc)i,\\ \bar\alpha\bar\beta &= (a-bi)(c-di) = ac-adi-bci+bdi^2 = (ac-bd)-(ad+bc)i.\end{aligned}$$

これから

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= \alpha\bar{\alpha}\beta\bar{\beta} = \alpha\beta\bar{\alpha}\bar{\beta} \\ &= \{(ac-bd)+(ad+bc)i\}\{(ac-bd)-(ad+bc)i\} \\ &= (ac-bd)^2+(ad+bc)^2.\end{aligned}$$

定理 5.7. 自然数 $n>1$ の素因数分解を $n=2^{d_0}p_1^{d_1}\cdots p_r^{d_r}q_1^{e_1}\cdots q_s^{e_s}$ とする．ここで $p_1,\ldots,p_r$, $q_1,\ldots,q_s$ は $p_i\equiv 1 \pmod 4$, $q_j\equiv 3 \pmod 4$ なる相異なる素数である．このとき n が 2 つの平方数の和として表せるためには，e_j $(j=1,\ldots,s)$ がすべて偶数となることが必要十分である．

[証明]　e_j $(j=1,\ldots,s)$ がすべて偶数であるとする．定理 5.3 より 2 および各 p_i は 2 つの平方数の和として表せる．$n_1=2^{d_0}p_1^{d_1}\cdots p_r^{d_r}$ とおけば補題 5.5 より $n_1=a_1^2+b_1^2$, a_1, b_1 は整数と表せる．$e_j=2f_j$ $(j=1,\ldots,s)$ とかいて $a=a_1q_1^{f_1}\cdots q_s^{f_s}$, $b=b_1q_1^{f_1}\cdots q_s^{f_s}$ とおけば

$$a^2+b^2=(a_1^2+b_1^2)q_1^{2f_1}\cdots q_s^{2f_s}=n_1q_1^{e_1}\cdots q_s^{e_s}=n.$$

逆に $n=a^2+b^2$ とかけたとする．$e_j>0$ とする．$n=a^2+b^2$ は q_j で割り切れる．もし b が q_j で割り切れないとすると命題 3.5 より $bx\equiv 1 \pmod{q_j}$ を満たす整数 x が存在する．$a^2+b^2\equiv 0 \pmod{q_j}$ だから

$$a^2x^2+b^2x^2\equiv 0 \pmod{q_j},\quad (ax)^2+1\equiv 0 \pmod{q_j}$$

となるが，これは命題 4.1 に矛盾する．よって b は q_j で割り切れなければならない．$a^2+b^2\equiv 0 \pmod{q_j}$ より $a^2\equiv 0 \pmod{q_j}$, $a\equiv 0 \pmod{q_j}$ となり a も q_j で割り切れる．$a=q_ja_1$, $b=q_jb_1$, a_1,b_1 は整数，とかける．$n=a^2+b^2=q_j^2(a_1^2+b_1^2)$ だから $e_j\geq 2$ である．$n_1=a_1^2+b_1^2$ とおけば，n_1 の素因数分解は

$$n_1=2^{d_0}p_1^{d_1}\cdots p_r^{d_r}q_1^{e_1}\cdots q_j^{e_j-2}\cdots q_s^{e_s}.$$

これを繰り返せば，e_j は偶数であることがわかる．　□

6　原始根

$m>1$ を自然数とする．0 以上 $m-1$ 以下の整数全体の集合を R_m で表す．さらに，1 以上 $m-1$ 以下の自然数で，m と互いに素なもの全体の集合を G_m とかく．G_m は R_m の部分集合である．R_m の元の個数は m である．G_m の元の個数

$$\varphi(m)=|G_m|$$

をオイラーの関数という．p が素数ならば，$\varphi(p) = p - 1$ である．

R_m は次のように和と積を定義することによって環になる．$a, b \in R_m$ に対して

$$a + b = \text{整数としての和 } a + b \text{ を } m \text{ で割った余り},$$
$$ab = \text{整数としての } ab \text{ を } m \text{ で割った余り}.$$

G_m は R_m における積によって可換群になっている．G_m において $a + b = c$, $ab = d$ であるとは，整数 a, b, c, d について合同式

$$a + b \equiv c \pmod{m}, \quad ab \equiv d \pmod{m}$$

が成り立つことと同じである．

p を 2 でない素数とする．G_p と R_{p-1} の元の個数はともに $p - 1$ である．G_p には，$a, b \in G_p$ に対して

$$ab = \text{整数としての } ab \text{ を } p \text{ で割った余り}$$

と定義することによって積が定義されている．また R_{p-1} には，$a, b \in R_{p-1}$ に対して

$$a + b = \text{整数としての } a + b \text{ を } p - 1 \text{ で割った余り}$$

と定義することによって和が定義されている．

このとき R_{p-1} と G_p の間には 1 対 1 対応 $f : R_{p-1} \to G_p$ で和を積にうつす，すなわち $a, b \in R_{p-1}$ に対して $f(a + b) = f(a)f(b)$ となるようなものが必ず存在する．

例えば $p = 7$ とする．R_6 から G_7 への次のような対応を f とする．

R_6		G_7
0	$\longmapsto$	1
1	$\longmapsto$	3
2	$\longmapsto$	2
3	$\longmapsto$	6
4	$\longmapsto$	4
5	$\longmapsto$	5

R_6 で $3 + 5 = 2$，$f(3 + 5) = f(2) = 2$ である．また G_7 で $f(3)f(5) = 6 \cdot 5 = 2$ である．
R_6 で $3 + 4 = 1$，$f(3 + 4) = f(1) = 3$ である．また G_7 で $f(3)f(4) = 6 \cdot 4 = 3$ である．

フェルマーの小定理 (定理 3.6) により p で割り切れない整数 a は $a^{p-1} \equiv 1 \pmod{p}$ を満たす．これは $a \in G_p$ について G_p の中で $a^{p-1} = 1$ となることを意味する．

$a \in G_p$ について，$a^n = 1$ となる最小の自然数 n を a の位数という．$a^{p-1} = 1$ だから a の位数は $p - 1$ 以下である．

補題 **6.1.** $a \in G_p$ の位数は $p-1$ の約数である．

[証明]　a の位数を n とする．$a^n = 1$ かつ $1 \leq n \leq p-1$ である．$p-1$ を n で割ったときの商を q，余りを r とする．

$$p - 1 = nq + r, \quad 0 \leq r < n.$$

このとき $a^{p-1} = 1$, $a^n = 1$ だから

$$1 = a^{p-1} = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = 1a^r = a^r.$$

もし $r \neq 0$ とすると，$a^r = 1$ かつ $1 \leq r < n$ となって n が a の位数であることに矛盾する．よって $r = 0$ であり，$p - 1 = nq$ となる．すなわち a の位数 n は $p-1$ の約数である．　□

補題 **6.2.** $a \in G_p$ の位数を n とする．

(1) $a^m = 1$ を満たす整数 m は n の倍数である．
(2) $n = st$ (s, t は自然数) のとき，a^s の位数は t である．

[証明]　(1) $m = nq + r$, $0 \leq r < n$ とかく．$a^m = 1$ と $a^n = 1$ から $a^r = 1$ を得る．$r < n$ だから n が位数であることより $r = 0$ でなければならない．よって $m = nq$ である．

(2) a^s の位数を m とする．$(a^s)^t = a^{st} = a^n = 1$ より $m \leq t$ である．一方，$a^{sm} = (a^s)^m = 1$ だから (1) より sm は a の位数 $n = st$ の倍数である．よって sm は st の倍数，したがって m は t の倍数となり $m \geq t$ である．ゆえに $m = t$ である．　□

補題 **6.3.** $a, b \in G_p$ とし，a の位数を s，b の位数を t とする．このとき G_p の元で位数が s と t の最小公倍数であるものが存在する．

[証明]　$\gcd(s, t) = 1$ のとき．

$$(ab)^{st} = (a^s)^t (b^t)^s = 1 \cdot 1 = 1$$

より，ab の位数は st の約数である．ab の位数を m とする．

$$1 = ((ab)^m)^s = (ab)^{sm} = (a^s)^m b^{sm} = b^{sm}$$

だから，補題 6.2 の (1) より，sm は t の倍数である．s と t は互いに素だから m は t の倍数である．同様に

$$1 = ((ab)^m)^t = (ab)^{tm} = a^{tm}(b^t)^m = a^{tm}$$

だから，tm は s の倍数である．s と t は互いに素だから m は s の倍数である．したがって m は s と t の両方の倍数であり，s と t は互いに素だから m は st の倍数である．ゆえに $m = st$ である．st は s と t の最小公倍数である．

$\gcd(s,t) > 1$ のとき．s または t を割る素数の全体を $p_1, \ldots, p_r$ とし，$s = p_1^{e_1} \cdots p_r^{e_r}$, $t = p_1^{f_1} \cdots p_r^{f_r}$, $e_i, f_i \geq 0$ とする．g_i, h_i を

$$g_i = \begin{cases} e_i, & e_i \geq f_i, \\ 0, & e_i < f_i \end{cases}, \qquad h_i = \begin{cases} 0, & e_i \geq f_i, \\ f_i, & e_i < f_i \end{cases}$$

によって定めて，$s_1 = p_1^{g_1} \cdots p_r^{g_r}$, $t_1 = p_1^{h_1} \cdots p_r^{h_r}$ とおけば，s_1 は s の約数，t_1 は t の約数であり，s_1 と t_1 は互いに素である．また $s_1 t_1$ は s と t の最小公倍数である．$s = s_1 s_0$, $t = t_1 t_0$ とかいて $a_1 = a^{s_0}$, $b_1 = b^{t_0}$ とおけば a_1 の位数は s_1 であり，b_1 の位数は t_1 だから前半の結果により $a_1 b_1$ の位数は $s_1 t_1$ である． □

補題 6.4. n を p 以下の自然数とする．$f(x) = x^n + b_1 x^{n-1} + \cdots + b_n$, $b_1, \ldots, b_n$ は整数とする．このとき $a \in R_p$ で $f(a) \equiv 0 \pmod{p}$ を満たすものの個数は n 以下である．

[証明]　n に関する帰納法で証明する．$n = 1$ のとき $f(x) = x + b_1$ だから，$a \in G_p$ が $f(a) = a + b_1 \equiv 0 \pmod{p}$ を満たせば，$a \equiv -b_1 \pmod{p}$ である．このような $a \in G_p$ はただ 1 つである．$n > 1$ として $f(x)$ が $n-1$ 次の多項式のとき主張は正しいとする．

$f(x) = x^n + b_1 x^{n-1} + \cdots + b_n$, $b_1, \ldots, b_n$ は整数とする．$a \in G_p$ で $f(a) \equiv 0 \pmod{p}$ を満たすものが存在しなければ，主張は成り立っている．$a \in G_p$ が $f(a) \equiv 0 \pmod{p}$ を満たすとする．多項式 $f(x)$ を $x - a$ で割ったときの商を $g(x)$，余りを $r(x)$ とする．$g(x)$ は整数係数の $n-1$ 次多項式で，x^{n-1} の係数は 1 である．余りは定数だから $r(x) = r$ は整数である．よって

$$f(x) = (x - a)g(x) + r$$

が成り立つ．$x = a$ を代入すれば $f(a) = r$ である．$r = f(a) \equiv 0 \pmod{p}$ である．a と異なる G_p の元 b が $f(b) \equiv 0 \pmod{p}$ を満たすとすれば $(b-a)g(b) + r \equiv 0 \pmod{p}$ となるが $r \equiv 0 \pmod{p}$ だから $(b-a)g(b) \equiv 0 \pmod{p}$ となる．すなわち $(b-a)g(b)$ は p で割り切れる．$a, b \in G_p$ は異なるから $b - a$ は p で割り切れない．よって $g(b)$ は p で割り切れて，$g(b) \equiv 0 \pmod{p}$ が成り立つ．帰納法の仮定によりこのような $b \in G_p$ は $n-1$ 個以下である．したがって $f(b) \equiv 0 \pmod{p}$ を満たす $b \in G_p$ は a も含めて n 個以下である． □

定義 6.5. 補題 6.1 により G_p の各元の位数は $p-1$ の約数であるが，$g \in G_p$ が位数 $p-1$ であるとき，g は法 p の原始根であるという．

定理 6.6 (原始根の存在)**.** 素数 p に対して法 p の原始根が存在する.

[証明] $a \in G_p$, $a \neq 1$ をとる. 補題 6.1 より a の位数 s は $p-1$ の約数である. $s = p-1$ ならば a は法 p の原始根である. $s < p-1$ とする. $f(x) = x^s - 1$ に対して補題 6.4 を適用すれば $f(b) = b^s - 1 \equiv 0 \pmod{p}$ を満たす $b \in R_p$ の個数は s 以下である. $b = 0$ はこれを満たさないから, $b^s - 1 \equiv 0 \pmod{p}$ を満たす $b \in G_p$ の個数は s 以下である. したがって $b \in G_p$ で $b^s \neq 1$ であるものがとれる. b の位数を t とすれば t は s の約数ではない. s と t の最小公倍数を l とすれば $l > s$ である. 補題 6.3 より位数 l の元 $c \in G_p$ が存在する. この議論を繰り返せば G_p の元で位数 $p-1$ のものが存在することがわかる. □

小さな素数 p について法 p の原始根を求めてみよう.

$p = 3$ のとき. $g = 2$ は位数 2 だから原始根である.

$p = 5$ のとき. $g = 2$ は, $g^2 \equiv 4 \pmod{5}$, $g^4 \equiv 1 \pmod{5}$ だから位数 4, よって原始根である.

$p = 7$ のとき. $g = 2$ は $g^3 = 8 \equiv 1 \pmod{7}$ だから位数 3, よって原始根ではない. $g = 3$ とすると $g^2 = 9 \equiv 2 \pmod{7}$, $g^3 \equiv 6 \pmod{7}$, $g^6 \equiv 1 \pmod{7}$ だから $g = 3$ は原始根である.

$p = 11$ のとき. $g = 2$ は $g^2 \equiv 4 \pmod{11}$, $g^5 = 32 \equiv -1 \pmod{11}$, $g^{10} \equiv 1 \pmod{11}$ だから位数 10, よって原始根である.

g を法 p の原始根とする. G_p において g の位数は $p-1$ である. これは合同式のことばで述べれば

$$g^n \equiv 1 \pmod{p}$$

を満たすような最小の自然数 n が $p-1$ に等しいとなる. このとき, $p-1$ 個の整数 $1, g, g^2, \ldots, g^{p-2}$ は法 p で互いに合同にはならない. 実際, もし $0 \leq i < j \leq p-2$ として $g^j \equiv g^i \pmod{p}$ となったとすると, $g^j - g^i = g^i(g^{j-i} - 1)$ が p で割り切れるが, g は p で割り切れないから $g^{j-i} - 1$ が p で割り切れて, $g^{j-i} \equiv 1 \pmod{p}$ となる. $0 < j - i \leq p-2$ だからこれは g の位数が $p-1$ であることに矛盾する. したがって $1, g, g^2, \ldots, g^{p-2}$ は法 p で $1, 2, \ldots, p-1$ を適当に並べかえたものとそれぞれ合同になる. これは

$$G_p = \{1, g, g^2, \ldots, g^{p-2}\}$$

であることを意味する. ここで g^2 等は G_p の中での積 $g \cdot g$ 等を表す. $g^{p-1} = 1 = g^0$ だから, $m, n \in R_{p-1}$ において $m + n = l$ とすると整数としては $m + n = l + (p-1)t$, t

は整数だから，$g^{p-1}=1$ より

$$g^{m+n}=g^{l+(p-1)t}=g^l(g^{p-1})^t=g^l$$

となる．したがって R_{p-1} から G_p への対応を $n \mapsto g^n$ で定めれば，$G_p=\{1,g,g^2,\ldots,g^{p-2}\}$ が成り立つことから，この対応は 1 対 1 対応である．さらに $m+n \mapsto g^{m+n}=g^m g^n$ となるから，この対応は R_{p-1} の和を G_p の積にうつしている．

例えば，$p=11$ とすると，$g=2$ が法 11 の原始根である．R_{10} から G_{11} への対応 f を $m \mapsto 2^m$ によって定めるとこれは次のような対応である．

R_{10}		G_{11}
0	$\longmapsto$	1
1	$\longmapsto$	2
2	$\longmapsto$	4
3	$\longmapsto$	8
4	$\longmapsto$	5
5	$\longmapsto$	10
6	$\longmapsto$	9
7	$\longmapsto$	7
8	$\longmapsto$	3
9	$\longmapsto$	6

$f(3)=8$, $f(6)=9$, $f(3+6)=f(9)=6=8\cdot 9$ である．$f(4)=5$, $f(7)=7$, $f(4+7)=f(1)=2=5\cdot 7$ である．

定理 6.7. $6n+1$ の形の素数は無数に存在する．

[証明]　$6n+1$ の形の素数が有限個しかないと仮定する．それらを $p_1<p_2<\cdots<p_k$ とする．このとき $A=3p_1p_2\cdots p_k$ とおき

$$N=A^2+A+1$$

とおく．定理 2.7 により N は素数の積として $N=q_1q_2\cdots q_r$ と表せる (q_i は素数)．N は奇数で 3 で割り切れないから各 q_i は 2, 3 以外の素数である．このとき

$$A^3-1=(A-1)(A^2+A+1)\equiv 0 \pmod{q_i}$$

である．またもし $A\equiv 1 \pmod{q_i}$ とすると $A^2+A+1\equiv 3\equiv 0 \pmod{q_i}$ となって $q_i\neq 3$ に矛盾するから，$A\not\equiv 1 \pmod{q_i}$ である．よって G_{q_i} における A の位数は 3 で

ある．補題 6.1 より $q_i - 1$ は 3 の倍数である．$q_i - 1$ は 2 の倍数でもあるから $q_i - 1$ は 6 の倍数であり，q_i は $6n + 1$ の形である．$6n + 1$ の形の素数は $p_1, p_2, \ldots, p_k$ しかないと仮定したから，$q_i = p_j$ となる．しかし N は q_i で割り切れるが，p_j で割ると 1 余るからこれは矛盾である． □

7 平方剰余

定義 7.1. p を 2 でない素数とする．a を p で割り切れない整数とする．合同式

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

を満たす整数 x が存在するとき，a は法 p で**平方剰余**であるといい，そうでないとき a は法 p で**平方非剰余**であるという．

例えば，$p = 5$ のとき，

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

だから，$a = 1, 4$ は法 5 で平方剰余であるが，$a = 2, 3$ は平方非剰余である．

定理 7.2 (平方剰余の第 1 補充法則)**.** p が $4n + 1$ の形の素数ならば，-1 は法 p で平方剰余である．p が $4n + 3$ の形の素数ならば，-1 は法 p で平方非剰余である．

[証明]　最初の主張は命題 4.3，2 つ目の主張は命題 4.1 である． □

g を法 p の原始根とする．a を p で割り切れない整数とすると，$g^n \equiv a \pmod p$ となる自然数 n, $0 \le n \le p - 2$ が 1 つ定まる (n を R_{p-1} の元と思ってもよい)．この n を $\mathrm{ind}_g(a, p)$ と表す．$a, b \in G_p$ に対して

$$\mathrm{ind}_g(ab, p) \equiv \mathrm{ind}_g(a, p) + \mathrm{ind}_g(b, p) \pmod{p - 1}$$

が成り立つ．$a \mapsto \mathrm{ind}_g(a, p)$ は 1 対 1 対応 $R_{p-1} \to G_p$, $n \mapsto g^n$ の逆対応である．

補題 7.3. p で割り切れない整数 a について，a が法 p の平方剰余であるためには，$\mathrm{ind}_g(a, p)$ が偶数であることが必要十分である．

[証明]　$\mathrm{ind}_g(a, p)$ が偶数であるとする．$\mathrm{ind}_g(a, p) = 2n$ とかくと，これは $g^{2n} \equiv a \pmod p$ であることを意味する．$x = g^n$ とおけば $x^2 \equiv a \pmod p$ だから a は法 p の平方剰余である．逆に a が法 p の平方剰余であるとする．このとき $x^2 \equiv a \pmod p$ となる整数 x が存在する．よって $n = \mathrm{ind}_g(x, p)$ とおけば $g^n \equiv x \pmod p$ だから $g^{2n} \equiv x^2 \equiv a \pmod p$ となる．これは $\mathrm{ind}_g(a, p) = 2n$ を示している． □

系 **7.4.** $p-1$ 個の G_p の元の中で，法 p の平方剰余は $(p-1)/2$ 個あり，法 p の平方非剰余も $(p-1)/2$ 個ある．

[証明] $\mathrm{ind}_g(a,p)$ は R_{p-1} の元として 1 つ定まる．その中で偶数であるものは $0, 2, \ldots, 2\{(p-1)/2-1\}$ の $(p-1)/2$ であり，残りの $(p-1)/2$ 個は奇数である． □

系 **7.5.** (1) a, b が法 p の平方剰余ならば，ab も法 p の平方剰余である．

(2) a, b が法 p の平方非剰余ならば，ab は法 p の平方剰余である．

(3) a, b の一方が法 p の平方剰余で他方が平方非剰余ならば，ab は平方非剰余である．

[証明] $m = \mathrm{ind}_g(a,p)$, $n = \mathrm{ind}_g(b,p)$ とおく．

$$\mathrm{ind}_g(ab,p) \equiv \mathrm{ind}_g(a,p) + \mathrm{ind}_g(b,p) = m+n \pmod{p-1}.$$

(1) m, n ともに偶数だから $\mathrm{ind}_g(ab,p)$ も偶数．よって ab は法 p の平方剰余．

(2) m, n ともに奇数だから $\mathrm{ind}_g(ab,p)$ は偶数．よって ab は法 p の平方剰余．

(3) m, n の一方が偶数で他方が奇数だから $\mathrm{ind}_g(ab,p)$ は奇数．よって ab は法 p の平方非剰余． □

平方剰余についての性質を記述するために，p で割り切れない整数 a に対してルジャンドル記号 $\left(\frac{a}{p}\right)$ を

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ が法 } p \text{ で平方剰余のとき,} \\ -1, & a \text{ が法 } p \text{ で平方非剰余のとき} \end{cases}$$

によって定義する．さらに a が p で割り切れる整数のときは，$\left(\frac{a}{p}\right) = 0$ であるとする．

a, b が p で割り切れない整数のとき，補題 7.3 より

$$\left(\frac{a}{p}\right) = (-1)^{\mathrm{ind}_g(a,p)}$$

である．これから (あるいは系 7.5 から)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{7.1}$$

が成り立つ．

平方剰余の第 1 補充法則 (定理 7.2) はルジャンドル記号を用いれば

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{7.2}$$

と表せる．

命題 7.6 (オイラーの規準)**.** p で割り切れない整数 a に対して

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

[証明]　フェルマーの小定理 (定理 3.6) によって

$$\left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) = g^{p-1} - 1 \equiv 0 \pmod{p}$$

であるが，g の位数はちょうど $p-1$ だから $g^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$ である．したがって $g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ である．よって p で割り切れない整数 a に対して，$n = \mathrm{ind}_g(a, p)$ とおけば $a \equiv g^n \pmod{p}$ だから

$$a^{\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^n \equiv (-1)^n = \left(\frac{a}{p}\right) \pmod{p}.$$

□

$G_p = \{1, g, g^2, \ldots, g^{p-2}\}$ と $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ から

$$\begin{aligned}(p-1)! &\equiv \prod_{k=0}^{p-2} g^k \equiv g^{0+1+2+\cdots+p-2} = g^{\frac{(p-2)(p-1)}{2}} \pmod{p} \\ &\equiv (g^{\frac{p-1}{2}})^{p-2} \equiv (-1)^{p-2} \equiv -1 \pmod{p}\end{aligned}$$

となり，ウィルソンの定理 (定理 3.8) が再び得られた．

上のオイラーの規準を $a = -1$ について適用すれば $(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p}$ となるが，この合同式の両辺ともに ± 1 であり，$p > 2$ だから合同式から等式が成り立つことがわかる．すなわち

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

となり，平方剰余の第 1 補充法則が再び得られた．

(7.2) の他に $\left(\frac{2}{p}\right)$ と $\left(\frac{q}{p}\right)$ (q は p と異なる奇素数) の値がわかれば (7.1) によって p で割り切れない任意の整数 a について $\left(\frac{a}{p}\right)$ が計算できることになる．

$\left(\frac{2}{p}\right)$ について考える．$a = 2$ としてオイラーの規準を用いても，$a = -1$ のときと異なり，$2^{\frac{p-1}{2}}$ は簡単には計算できない．フェルマーの小定理の証明を思い出す．

$p = 13$, $a = 2$ とすると，x が G_{13} の各値を 1 回ずつとるとき，$2x$ も G_{13} の各値を 1 回ずつとる．x が G_{13} の半分の元からなる部分集合 $A = \{1, 2, 3, 4, 5, 6\}$ をうごくとき，$2x$ は $A' = \{2, 4, 6, 8, 10, 12\}$ をうごく．$B = \{7, 8, 9, 10, 11, 12\}$ とおけば

$$A' \cap A = \{2, 4, 6\}, \quad A' \cap B = \{8, 10, 12\}.$$

R_{13} において $8=-5$, $10=-3$, $12=-1$ だから

$$A' \cap B = \{-5, -3, -1\}.$$

したがって R_{13} において

$$\begin{aligned}(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6) &= 2\cdot 4\cdot 6\cdot(-5)\cdot(-3)\cdot(-1),\\ 2^6(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) &= (-1)^3(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6),\\ 2^6 &= (-1)^3 = -1.\end{aligned}$$

オイラーの規準より $\left(\frac{2}{13}\right) \equiv 2^6 \equiv -1 \pmod{13}$, $\left(\frac{2}{13}\right) = -1$ を得る．

今度は $p=17$, $a=2$ とする．x が G_{17} の各値を 1 回ずつとるとき，$2x$ も G_{17} の各値を 1 回ずつとる．x が G_{17} の半分の元からなる部分集合 $A=\{1,2,3,4,5,6,7,8\}$ をうごくとき，$2x$ は $A'=\{2,4,6,8,10,12,14,16\}$ をうごく．$B=\{9,10,11,12,13,14,15,16\}$ とおけば

$$A' \cap A = \{2,4,6,8\}, \quad A' \cap B = \{10,12,14,16\}.$$

R_{17} において，$10=-7$, $12=-5$, $14=-3$, $16=-1$ だから

$$A' \cap B = \{-7, -5, -3, -1\}.$$

したがって R_{17} において

$$\begin{aligned}(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6)(2\cdot 7)(2\cdot 8) &= 2\cdot 4\cdot 6\cdot 8\cdot(-7)\cdot(-5)\cdot(-3)\cdot(-1),\\ 2^8(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8) &= (-1)^4(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8),\\ 2^8 &= (-1)^4 = 1.\end{aligned}$$

オイラーの規準より $\left(\frac{2}{17}\right) \equiv 2^8 \equiv 1 \pmod{17}$, $\left(\frac{2}{17}\right) = 1$ を得る．このような考察を一般化すると，次の結果を得る．

補題 7.7 (ガウスの補題)**.** p を奇素数とし，$s=\dfrac{p-1}{2}$ とおく．G_p $(\subset R_p)$ を次のように s 個の元からなる 2 つの部分集合に分ける．

$$G_p = A \cup B, \quad A=\{1,2,\ldots,s\},\ B=\{s+1, s+2, \ldots, p-1\}.$$

$a \in G_p$ をとり ja $(j=1,\ldots,s)$ のうちで B に属するものの個数を n とすれば

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

が成り立つ．

[証明]　ja $(j=1,\dots,s)$ のうちで A に属するものを $a_1,a_2,\dots,a_m$ とし，B に属するものを $b_1,b_2,\dots,b_n$ とする．このとき $2s+1=p$ より R_p において

$$B=\{s+1,s+2,\dots,p-2,p-1\}=\{-s,-(s-1),\dots,-2,-1\}=\{-x\,|\,x\in A\}$$

である．$b_j\in B$ より $-b_j\in A$ である．したがって

$$\{a_1,a_2,\dots,a_m\}\cup\{-b_1,-b_2,\dots,-b_n\}\subset A.$$

もし $a_i=-b_j$ とすると $a_i=ax$, $b_j=ay$, $x,y\in A$ とかける．$ax=-ay$, $a(x+y)=0$ である．$a\in G_p$ より $x+y=0$, $y=-x$ である．$y\in A$, $-x\in B$ だから $y=-x\in A\cap B=\emptyset$ となって矛盾である．ゆえに

$$\{a_1,a_2,\dots,a_m\}\cap\{-b_1,-b_2,\dots,-b_n\}=\emptyset$$

であり，$m+n=s=|A|$ だから

$$\{a_1,a_2,\dots,a_m\}\cup\{-b_1,-b_2,\dots,-b_n\}=A$$

を得る．したがって A のすべての元の積をとれば

$$\begin{aligned}1\cdot 2\cdot\ \dots\ \cdot s&=a_1\cdots a_m(-b_1)\cdots(-b_n)\\&=(-1)^n a_1\cdots a_m b_1\cdots b_n\\&=(-1)^n(a\cdot 1)(a\cdot 2)\cdots(a\cdot s)\\&=(-1)^n a^s(1\cdot 2\cdot\ \dots\ \cdot s).\end{aligned}$$

ゆえに $(-1)^n a^s=1$, $a^{\frac{p-1}{2}}=a^s=(-1)^n$ を得る．オイラーの規準より

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

$\left(\frac{a}{p}\right)$ と $(-1)^n$ はともに ±1 だから合同式から等式がでる．　□

定理 7.8 (平方剰余の第 2 補充法則)**.** 奇素数 p について次が成り立つ．

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & p\equiv 1,7\pmod 8,\\ -1, & p\equiv 3,5\pmod 8.\end{cases}$$

[証明]　補題 7.7 を $a=2$ について適用する．$s=(p-1)/2$,

$$G_p=A\cup B,\quad A=\{1,2,\dots,s\},\quad B=\{s+1,s+2,\dots,p-1\}.$$

$2x$ $(x=1,2,\dots,s)$ のうち B に属するものの個数を n とする．

(1) $p = 8m+1$ のとき．$s = (p-1)/2 = 4m$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2m)\} \cup \{2(2m+1), 2(2m+2), \ldots, 2(4m)\}$$

より $n = 4m - 2m = 2m$ である．したがって $\left(\frac{2}{p}\right) = (-1)^{2m} = 1$.
(2) $p = 8m+7$ のとき．$s = (p-1)/2 = 4m+3$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2m+1)\} \cup \{2(2m+2), 2(2m+3), \ldots, 2(4m+3)\}$$

より $n = 4m+3-(2m+1) = 2m+2$ である．したがって $\left(\frac{2}{p}\right) = (-1)^{2m+2} = 1$.
(3) $p = 8m+3$ のとき．$s = (p-1)/2 = 4m+1$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2m)\} \cup \{2(2m+1), 2(2m+2), \ldots, 2(4m+1)\}$$

より $n = 4m+1-(2m) = 2m+1$ である．したがって $\left(\frac{2}{p}\right) = (-1)^{2m+1} = -1$.
(4) $p = 8m+5$ のとき．$s = (p-1)/2 = 4m+2$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2m+1)\} \cup \{2(2m+2), 2(2m+3), \ldots, 2(4m+2)\}$$

より $n = 4m+2-(2m+1) = 2m+1$ である．したがって $\left(\frac{2}{p}\right) = (-1)^{2m+1} = -1$. □

定理 7.9 (平方剰余の相互法則)．奇素数 p, q, $p \neq q$ に対して次が成り立つ．

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4 \text{ かつ } q \equiv 3 \pmod 4. \end{cases}$$

[証明] $s = (p-1)/2$, $t = (q-1)/2$ とおき

$$G_p = A \cup B, \quad A = \{1, 2, \ldots, s\}, \quad B = \{s+1, s+2, \ldots, 2s\},$$
$$G_q = A' \cup B', \quad A' = \{1, 2, \ldots, t\}, \quad B' = \{t+1, t+2, \ldots, 2t\}$$

とおく．また

$$H = \{(x, y) \,|\, x, y \text{ は整数}, 1 \leq x \leq s,\ 1 \leq y \leq t\}$$

とおく．qx $(x = 1, 2, \ldots, s)$ のうち，B に属するものを $\alpha_1, \ldots, \alpha_m$ とすれば，補題 7.7 より

$$\left(\frac{q}{p}\right) = (-1)^m.$$

同様に py $(y = 1, 2, \ldots, t)$ のうち，B' に属するものを $\beta_1, \ldots, \beta_n$ とすれば，補題 7.7 より

$$\left(\frac{p}{q}\right) = (-1)^n.$$

各 $i=1,\dots,m$ に対して，α_i の定義により整数 $x_i \in A$, $a_i \in A$ で

$$\alpha_i \equiv qx_i \equiv p - a_i \equiv -a_i \pmod{p}$$

となるものが一意的に存在する．このとき $a_i + qx_i = py_i$ となる整数 y_i が一意的に定まる．$a_i, x_i \geq 1$ より $y_i \geq 1$ である．また $a_i, x_i \leq s < p/2$ より

$$py_i = a_i + qx_i < \frac{p}{2} + \frac{p}{2}q, \quad y_i < \frac{1}{2} + \frac{q}{2} = t + 1.$$

したがって $y_i \leq t$ である．ゆえに $1 \leq y_i \leq t$ である．さらに $a_i = py_i - qx_i$ より，$0 < py_i - qx_i < p/2$ である．このように各 $i=1,\dots,m$ に対して，格子点 $(x_i, y_i) \in H$ で $0 < py_i - qx_i < p/2$ となるものが対応する．逆に $0 < py - qx < p/2$ を満たす格子点 $(x,y) \in H$ に対して $a = py - qx$ とおけば，$1 \leq a, x \leq s$, $a, x \in A$ であり $qx \equiv -a \pmod{p}$ だから $qx \in qA \cap B \subset G_p$ である．したがって

$$m = \#(qA \cap B) = \#\left\{(x,y) \in H \,|\, 0 < py - qx < p/2\right\} \tag{7.3}$$

を得る．同様に各 $j=1,\dots,n$ に対して，β_j の定義により整数 $y'_j \in A'$, $b_j \in A'$ で

$$\beta_j \equiv py'_j \equiv q - b_j \equiv -b_j \pmod{q}$$

となるものが一意的に存在する．このとき $b_j + py'_j = qx'_j$ となる整数 x'_j が一意的に定まる．$b_j, y'_j \geq 1$ より $x'_j \geq 1$ である．また $b_j, y'_j \leq t < q/2$ より

$$qx'_j = b_j + py'_j < \frac{q}{2} + \frac{q}{2}p, \quad x'_j < \frac{1}{2} + \frac{p}{2} = s + 1.$$

したがって $x'_j \leq s$ である．ゆえに $1 \leq x'_j \leq s$ である．さらに $b_j = qx'_j - py'_j$ より，$0 < qx'_j - py'_j < q/2$ である．このように各 $j=1,\dots,n$ に対して，格子点 $(x'_j, y'_j) \in H$ で $0 < qx'_j - py'_i < q/2$ となるものが対応する．逆に $0 < qx - py < q/2$ を満たす格子点 $(x,y) \in H$ に対して $b = qx - py$ とおけば，$1 \leq b, y \leq t$, $b, y \in A'$ であり $py \equiv -b \pmod{q}$ だから $py \in pA' \cap B' \subset G_q$ である．したがって

$$n = \#(pA' \cap B') = \#\left\{(x,y) \in H \,|\, 0 < qx - py < q/2\right\} \tag{7.4}$$

を得る．(7.3) と (7.4) より

$$\begin{aligned} m + n &= \#\left\{(x,y) \in H \,|\, 0 < py - qx < p/2\right\} \\ &\quad + \#\left\{(x,y) \in H \,|\, 0 < qx - py < q/2\right\} \\ &= \#\left\{(x,y) \in H \,|\, -q/2 < py - qx < p/2\right\}. \end{aligned} \tag{7.5}$$

ここで

$$H_1 = \{(x,y) \in H \,|\, py - qx \geq p/2\}\,, \quad H_2 = \{(x,y) \in H \,|\, py - qx \leq -q/2\} \tag{7.6}$$

とおけば (7.5) と (7.6) より

$$\begin{aligned} & m + n + \#H_1 + \#H_2 \\ & = \#\{(x,y) \in H \,|\, -q/2 < py - qx < p/2\} \\ & \quad + \#\{(x,y) \in H \,|\, py - qx \geq p/2\} + \#\{(x,y) \in H \,|\, py - qx \leq -q/2\} \\ & = \#H = st. \end{aligned}$$

さらに $\#H_1 = \#H_2$ である．実際，長方形 $\{(x,y) \,|\, 1 \leq x \leq s,\ 1 \leq y \leq t\}$ の中心 $C = ((s+1)/2, (t+1)/2)$ に関して点 (x,y) を点対称移動した点は

$$f(x,y) = (s+1-x, t+1-y)$$

と表される．f は H から H への 1 対 1 対応であり $f \circ f = \mathrm{id}_H$ である．ここで

$$p(t+1-y) - q(s+1-x) = \frac{p-q}{2} - (py - qx) \tag{7.7}$$

に注意する．$(x,y) \in H_1$ ならば $py - qx \geq p/2$ だから

$$\frac{p-q}{2} - (py - qx) \leq -\frac{q}{2}.$$

したがって (7.7) と (7.6) より $f(x,y) \in H_2$ である．$(x,y) \in H_2$ ならば $py - qx \leq -q/2$ だから

$$\frac{p-q}{2} - (py - qx) \geq \frac{p}{2}.$$

したがって (7.7) と (7.6) より $f(x,y) \in H_1$ である．ゆえに f は H_1 から H_2 への 1 対 1 対応を与える．特に $\#H_1 = \#H_2$ が成り立つ．よって

$$m + n + 2\#H_1 = st$$

であり

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{m+n} = (-1)^{st} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

例 **7.10.** $p = 11$, $q = 7$ とすると $s = 5$, $t = 3$ である．図 3 において太線で囲まれる長方形の中の格子点の集合が H である．$C = (3,2)$ がその中心である．直線 $11y - 7x = 0$

を ℓ，直線 $11y-7x=11/2$ を ℓ_1, 直線 $11y-7x=-7/2$ を ℓ_2 とする．ℓ と ℓ_1 の間にある H の点 (大きい黒丸) の個数が $m=3$ であり，ℓ_2 と ℓ の間にある H の点 (大きい白丸) の個数が $n=2$ である．ℓ_1 より上にある H の部分が H_1 で 5 点 (小さい黒丸) あり，ℓ_2 より下にある H の部分が H_2 で 5 点 (小さい白丸) ある．これらは中心 C に関して点対称の位置にある．H の点の個数は全部で $st=5\times 3=15$ である．$3+2+5+5=15$ となっている．$\left(\frac{7}{11}\right)=(-1)^3=-1$, $\left(\frac{11}{7}\right)=(-1)^2=1$.

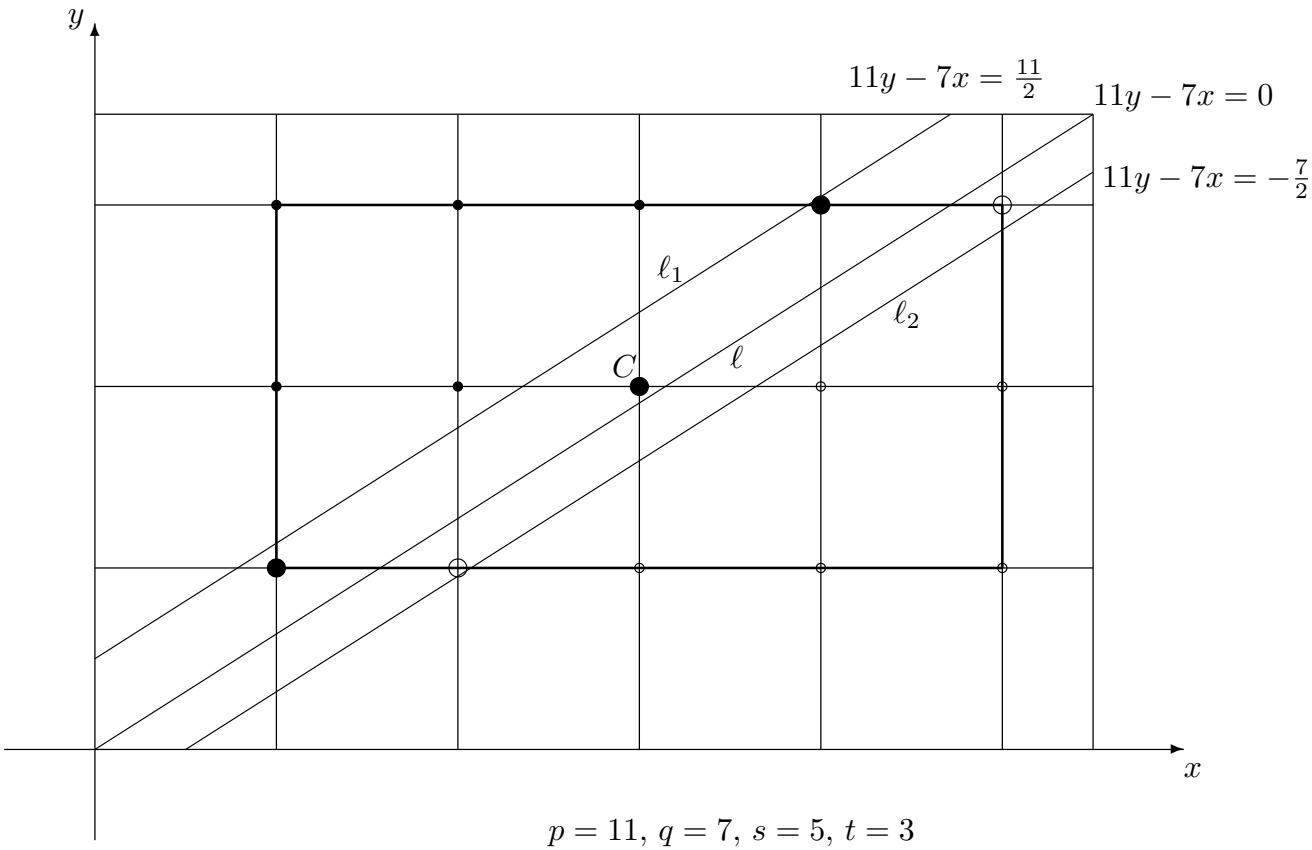

図 3　平方剰余の相互法則の証明

例 **7.11.**

$$\left(\frac{5}{43}\right)=(-1)^{\frac{5-1}{2}\frac{43-1}{2}}\left(\frac{43}{5}\right)=\left(\frac{3}{5}\right)=(-1)^{\frac{3-1}{2}\frac{5-1}{2}}\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

演習問題 **7.1.** 次のルジャンドル記号の値を求めよ．

$$\left(\frac{23}{29}\right),\quad \left(\frac{15}{17}\right),\quad \left(\frac{14}{19}\right),\quad \left(\frac{19}{37}\right).$$

[解答]

$$\begin{aligned}\left(\frac{23}{29}\right) &= (-1)^{\frac{23-1}{2}\cdot\frac{29-1}{2}}\left(\frac{29}{23}\right) = \left(\frac{6}{23}\right)\\ &= \left(\frac{2}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{3}{23}\right)\\ &= (-1)^{\frac{3-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{3}\right) = (-1)\left(\frac{2}{3}\right) = 1.\end{aligned}$$

$$\begin{aligned}\left(\frac{15}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{5}{17}\right) &= (-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)(-1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{5}\right)\\ = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) &= (-1)(-1) = 1.\end{aligned}$$

$$\begin{aligned}\left(\frac{15}{17}\right) &= \left(\frac{-2}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)\\ &= (-1)^{\frac{17-1}{2}} = 1\end{aligned}$$

$$\begin{aligned}\left(\frac{14}{19}\right) &= \left(\frac{2}{19}\right)\left(\frac{7}{19}\right) = (-1)(-1)^{\frac{7-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{7}\right)\\ &= \left(\frac{5}{7}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{5}\right)\\ &= \left(\frac{2}{5}\right) = -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{14}{19}\right) &= \left(\frac{-5}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{5}{19}\right)\\ &= (-1)^{\frac{19-1}{2}}(-1)^{\frac{19-1}{2}\cdot\frac{5-1}{2}}\left(\frac{19}{5}\right)\\ &= (-1)\left(\frac{4}{5}\right) = (-1)\left(\frac{2}{5}\right)^2 = -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{19}{37}\right) &= (-1)^{\frac{19-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{19}\right)\\ &= \left(\frac{18}{19}\right) = \left(\frac{-1}{19}\right) = (-1)^{\frac{19-1}{2}} = -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{19}{37}\right) &= (-1)^{\frac{19-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{19}\right)\\ &= \left(\frac{18}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{9}{19}\right)\\ &= (-1)\left(\frac{3}{19}\right)^2 = -1.\end{aligned}$$

参考文献

[1] 西来路文朗・清水健一，素数が奏でる物語，ブルーバックス，講談社，2015.

[2] 芹沢正三，素数入門，ブルーバックス，講談社，2008.

[3] ジョセフ・H. シルヴァーマン，はじめての数論 原著第 3 版—発見と証明の大航海 - ピタゴラスの定理から楕円曲線まで，ピアソンエデュケーション，2007.

[4] マーカス・デュ. ソートイ，素数の音楽， 新潮社，2005.