数論，楕円曲線の美と暗号理論

横川 光司
お茶の水女子大学大学院人間文化研究科

２００６年7月２７，２８日

目次

本講義ノートは，7月２７，２８日の「数学教材開発法（基礎)」，東京都教員研修，および，２８日，２９日に開催される「お茶の水女子大学夏期数学講習会」の初日２８日分の講義のためのものである．夏期講習会では，主に後半の５章から７章の範囲を講義する．

記号の説明

1. 整数 $a_1, a_2, \ldots, a_n$ の最大公約数を $(a_1, a_2, \ldots, a_n)$ で表す．例えば，
$$(4, 6) = 2, \qquad (12, 18, 45) = 3$$
である．従って $(m, n) = 1$ は m と n が互いに素，つまり最大公約数が 1 であることを意味する．
2. 整数 m が整数 n の約数のとき，$m \mid n$ と書き，m は n を割り切るという．例えば，$2 \mid 6,\ 5 \mid 10$ である．また，m が n を割り切らないことを $m \nmid n$ で表す．
3. 英小文字 $a, b, c, \ldots$ は特に断らない限り整数を表すものとする．
4. 整数 a, b を整数 m で割った余りが同じであるとき，
$$a \equiv b \pmod{m}$$
と書き，a と b は m を法として合同，または a は m を法として b に合同と言われる．これは $m \mid a - b$ と同なじことである．$a \equiv b \pmod{m}$ のような式は合同式と呼ばれるが，これは足し算，引き算，掛け算に関して，通常の等式と同様に扱える．すなわち，
$$a \equiv a',\ b \equiv b' \pmod{m}$$
のとき，
$$a \pm b \equiv a' \pm b', \quad ab \equiv a'b' \pmod{m}$$

が成り立つ.

1　ユークリッドの原論における数論

1.1　「原論」の概要

数論は古代ギリシャの時代から（恐らくはもっと昔のバビロニアの時代から）研究されており，紀元前３００年頃に著されたユークリッドの「原論」にも数論に属する定理が幾つか記されている.「原論」は１３巻からなっており，以下のような構成になっている.

- １巻 〜 ４巻　平面幾何,
- ５巻　比例論（実数論）
- ６巻　比例論の平面幾何への応用
- ７巻 〜 ９巻　数論
- １０巻　無理 “量” 論 (無理数論)
- １１巻 〜 １３巻　立体幾何学

「原論」で数と呼ばれているものは，１と呼ばれる「単位」が集まったものであり，つまり２以上の自然数である．１は単位であり，数と区別されている．また，５巻の比例論は２線分の比を実数とみた実数論とみなすことができる.「原論」には数を表す代数的記号は一切なく，線分によって表されており，数の間の演算は線分に対する定規とコンパスのみを用いた作図によって表される．そのため古代ギリシャの代数は「幾何学的代数」と呼ばれている．定規とコンパスで作図できるのは直線と円であり，その作図で可能な線分比は１から四則演算，平方根のみを用いて表される数のみである．１０巻の無理量論は平方根を用いて表される数，例えば $\sqrt{\sqrt{a}+\sqrt{b}}$ のような数に対する代数を扱っている．１１巻から１３巻では立体幾何学を扱っており，正多面体には５種類（正四面体，正六面体，正八面体，正十二面体，正二十面体）しかないことが最終定理である.

1.2　「原論」における数論

ユークリッドの「原論」では７巻から９巻が数論にあてられている．７巻の冒頭は数，約数，倍数，素数等の定義から始まり，２数の最大公約数を求める互除法，素数 p が積 ab を割り切れば p は a または b の約数になること，自然数の素因数分解とその一意性，素

数が無限に多く存在すること，そして

$1+2+2^2+\cdots+2^{n-1}=2^n-1$ が素数ならば $2^{n-1}(2^n-1)$ が完全数となること，

が９巻の最後で示されている．自然数 m が完全数とは，m の m 以外のすべての約数の和が m となることである．例えば，

$$6=1+2+3, \qquad 28=1+2+4+7+14$$

であるから，$6, 28$ は完全数である．6 が完全数なのは「神が６日間で世界を作ったから」，28 が完全数なのは「月の公転周期が２８日だから」だというように，完全数は神聖な数とみなされ特別な興味をもたれていた．古代の人たちに知られていた完全数は，$n=2,3,5,7$ に対応する

$$6,\ 28,\ 496,\ 8128$$

の４つである．完全数については次節で扱う．完全数については，未だわかっていないことがほとんどで，その神秘性は現在でもなお失われていないが，逆にそれだけ数学に与えた影響は大きいとは言えない．それに反して，数論の巻では扱われていないが，ピタゴラスの定理（１巻）に関係して，三辺の長さが自然数である直角三角形（以後**ピタゴラス三角形**と呼ぶことにしよう）を与える式（１０巻）

$$2mn,\ m^2-n^2,\ m^2+n^2 \tag{1}$$

は近代数論を生み出すきっかけを与える重要な式である．この３数が直角三角形の３辺となることは，代数記法の発達した今日では明らかであるが，古代ギリシャでは作図によって示されているので，それほど自明なことではない．ピタゴラス三角形を求める問題はもっと古くから興味を持たれており，古代バビロニアの粘土版（B.C. １９００～１６００？） には１５個のピタゴラス三角形が記されている．

完全数を求める問題は，簡単だが数論の至る所で大活躍するフェルマの小定理を生み出すきっかけとなった．また，ピタゴラス三角形をすべて求める問題，それらを特徴づける問題は，平方和で表される素数に関するフェルマの定理，ファルマの大定理（ワイルズの定理）を生み出すのだが，どちらも「原論」が書かれてより２０００年近く後の，フランスの天才数学者ピエール・ド・フェルマ[*1]（１６０１－１６６５）を待たねばならなかったのである．

[*1] 本職は裁判所の参事官．パスカル (1623–1662) の同時代人である．

2　完全数とフェルマの小定理

2.1　完全数とメルセンヌ素数

これまでに知られている完全数は，すべて「原論」にある型の完全数

$$2^{n-1}(2^n-1) \qquad (2^n-1 \text{ は素数})$$

である．実際，奇数の完全数は今日に至るまで一つも発見されておらず，また，偶数の完全数はこの型のものしかないことが，オイラー（１７０７－１７８３）により証明されている．

定理 2.1 (オイラー)**.** 偶数の完全数は

$$2^{p-1}(2^p-1) \qquad (2^p-1 \text{ は素数})$$

と表される．

Proof. 自然数 m に対し，その約数すべての和を $S(m)$ で表す．偶数の完全数 N を $N = 2^{p-1}M$ とおく．ここで M を奇数とし，$p \geq 2$ とする．M の約数全体を $m_1, m_2, \ldots, m_r$ とすると N の約数全体は $2^i m_j$ $(0 \leq i \leq p-1,\ 1 \leq j \leq r)$ である．よって N が完全数のとき，

$$2^p M = 2N = S(N) = \sum_{i,j} 2^i m_j = (\sum_i 2^i)(\sum_j m_j) = S(2^{p-1})S(M) = (2^p-1)S(M).$$

従って $M = (2^p-1)m$ なる自然数 m がとれる．ここで $m \geq 2$，または $m = 1$ であっても 2^p-1 が素数でなければ，

$$S(M) \geq 1 + m + M$$

である．よって

$$\begin{aligned} 2^p M &= (2^p-1)S(M) \\ &\geq (2^p-1)(1+m+M) \\ &= (2^p-1) + M + (2^p-1)M = (2^p-1) + 2^p M \end{aligned}$$

これは $p \geq 2$ に反する．よって $m = 1$ で $M = 2^p-1$ は素数でなければならない．　□

2^n-1 型の素数については，フェルマと大変親交の深かったマラン・メルセンヌ神父（１５８８－１６４８）が，１６４４年，2^n-1 が素数となるのは $n \leq 257$ では

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

だけであると発表した．これは一部誤りを含んでいて，実際には

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$$

であるが，2^n-1 型の素数は**メルセンヌ素数**と呼ばれている．

$$2^{ab}-1 = (2^a-1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

であるから，2^n-1 が素数であるためには，n も素数でなければならない．メルセンヌ素数は無限個あるかどうかもわからない．現在知られているメルセンヌ素数は４３個あり２００５年１２月に発見された

$$2^{30402457}-1$$

が最大のものである．これは９１５万２０５２桁[*2]の数で，現在知られている最大の素数である．[*3] メルセンヌ素数を見つけるには，次のリュカ (Lucas) 法が有効である．以後 $M_p = 2^p - 1$ とおく．

定理 2.2 (リュカ)**.** 数列 r_m $(m = 1, 2, \dots)$ を以下のように定める．

$$r_1 = 4,\ \ r_2 = 4^2 - 2 = 14,\ \ r_3 = 14^2 - 2 = 194,\ \dots,\ r_m = r_{m-1}^2 - 2$$

このとき，M_p が素数であるための必要十分条件は $M_p \mid r_{p-1}$ となることである．

奇数の完全数については，現在に至るまで一つも発見されていない．

2.2 正多角形の作図とファルマ素数

関連した話題として**フェルマ素数**についても少し触れておこう．メルセンヌ素数は 2^n-1 型の素数であったが，フェルマ素数とは 2^n+1 型の素数である．2^n-1 が素数であるためには n が素数であることが必要であったが，2^n+1 が素数であるためには n

[*2] １０００万桁の素数の発見には，１０万ドルの賞金がかかっている．

[*3] これは GIMPS(http://www.mersenne.org/) というメルセンヌ素数の発見を目的として１９９６年に発足した分散型コンピューティングを利用したプロジェクトによって発見された．このプロジェクトでは発足時から９個のメルセンヌ素数を発見している．

が 2^m の形の数でなくてはならない．実際，$n = lm$ で m が 3 以上の奇数であったとすると，

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

と分解するためである．従って, フェルマ素数とは $2^{2^m}+1$ 型の素数である．$F_m = 2^{2^m}+1$ はフェルマ数と呼ばれている．フェルマは，すべての自然数 m に対して F_m が素数であると言っているが，これは誤りである．

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537,\ F_5 = 4294967297 = 641 \times 6700417$$

であり，現在までに知られているフェルマ素数は F_0, F_1, F_2, F_3, F_4 の５つのみである．F_5 の素因数分解はオイラーによって与えられた．

メルセンヌ素数は偶数の完全数を完全に記述するものであったが，フェルマ素数は定規とコンパスを用いて作図可能な正多角形を完全に記述する．

定理 2.3 (ガウス)**.** 正 n 角形が定規とコンパスで作図可能であるための必要十分条件は n の素因数分解が $2^m p_1 p_2 \cdots p_r$ で，$p_1, \ldots, p_r$ が相異なるフェルマ素数となることである．特に，p が素数のとき，正 p 角形が定規とコンパスのみを用いて作図できるための必要十分条件は p がフェルマ素数となることである．

従って，正３角形，正５角形，正１７角形，正２５７角形，正６５５３７角形は定規とコンパスで作図可能である．この他の素数 p で，正 p 角形が作図可能となるものがあるかどうか，ガウスのこの発見から２００年経った今日でもわからないままである．

系 2.4. 角度 n° (n は自然数) が定規とコンパスを用いて作図できるための必要十分条件は n が 3 の倍数となることである．特に，角の三等分は一般に定規とコンパスのみでは作図不可能である．

Proof. 正５角形は作図可能だから 72° は作図可能である．また 60° も作図可能だから $72^\circ - 60^\circ = 12^\circ$ も作図可能である．よって，その４等分の 3°，従ってその倍数の $3n^\circ$ も作図可能である．$3n + 1^\circ$ または $3n + 2^\circ$ が作図可能なら，そこから $3n^\circ$ を引いた 1° または 2° が作図可能となり，どちらにしても正９角形が作図できてしまう．これはガウスの定理により不可能である．特に，120° の三等分を定規とコンパスでは作図できない． □

2.3 メルセンヌ数，フェルマ数の素因子とフェルマの小定理

ピエール・ド・フェルマは１６０１年フランス西部で生まれ，１６３１年トゥールージュの州高等裁判所の参事官に任ぜられ，この法院の官として終世を過ごした．フェルマがいつごろから数学に興味を持つようになったのかはわからないが，遅くとも２０代後半あたりだと考えられている．

数論に関するフェルマの定理いろいろあるが，フェルマの小定理と呼ばれているものが，最も有名なものであろう．フェルマがこの定理を発見するきっかけとなったのは，完全数の問題であった．１６４０年フェルマはフレニクルから 10^{20} と 10^{22} の間に完全数があるかどうかを問われた．オイラーの上の定理が証明されるのは，この１００年後であるが，当時までに知られている完全数はすべて原論で与えられた型の完全数しかなかった．そこで，フェルマは $10^{20} < 2^{p-1}(2^p - 1) < 10^{22}$ を満たす素数 $2^p - 1$ を探すことを試みたのである．p がこの範囲にあるためには $34 \leq p \leq 37$ でなければならない．p は素数でなければならないから，$2^{37} - 1 = 137438953471$ のみが候補となる．フェルマは $2^{37} - 1$ の素因数分解を試みて，分解

$$2^{37} - 1 = 223 \times 616318177$$

を発見した．この素因数 223 が満たすべき条件を探す課程で，フェルマは次の「フェルマの小定理」を発見したのであろう．

定理 2.5 (フェルマの小定理)**.** p を素数，m を p で割れない整数とすると，

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

Proof. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$ は群．（実は巡回群になる．）よって，$(\mathbb{Z}/p\mathbb{Z})^\times$ において $m^{p-1} = 1$. □

(初等的証明) $0 < n < p \Longrightarrow p \mid \binom{p}{n}$ に注意する．

$$\begin{aligned} m^p &= ((m-1)+1)^p \\ &= (m-1)^p + \binom{p}{1}(m-1)^{p-1} + \cdots + \binom{p}{p-1}(m-1) + 1 \\ &\equiv (m-1)^p + 1 \pmod{p} \end{aligned}$$

これを繰り返して，$m^p \equiv m \pmod{p}$ を得る．$p \nmid m$ なら，$\pmod{p}$ での m の逆元を掛けて，$m^{p-1} \equiv 1 \pmod{p}$ を得る．

例 2.1. フェルマの小定理を幾つかの素数について確かめてみる.

$$\begin{aligned}
2^4 &= 16 \equiv 1 \pmod 5 \\
3^4 &= 81 \equiv 1 \pmod 5 \\
4^4 &\equiv (-1)^4 = 1 \pmod 5 \\
2^6 &= 8^2 \equiv 1 \pmod 7 \\
3^6 &= 9^3 \equiv 2^3 \equiv 1 \pmod 7 \\
5^{16} &= 25^8 \equiv 8^8 = 64^4 = (-4)^4 = 16^2 \equiv (-1)^2 = 1 \pmod{17}
\end{aligned}$$

問 1. フェルマの小定理を $p = 11, 13$ について確かめよ.

系 2.6 (フェルマ)**.** p, q を素数, $m \not\equiv 0, 1 \pmod p$ とする.

$$m^q \equiv 1 \pmod p \Longrightarrow p \equiv 1 \pmod q$$

Proof. $(p-1, q) = 1$ なら, $l(p-1) + nq = 1$ となる整数 l, n がとれる. すると定理 2.5 より, $m = m^{l(p-1)+nq} \equiv 1 \pmod p$ となって仮定に反する. q は素数だから, $q \mid p-1$, (群論を使えば, m の $(\mathbb{Z}/p\mathbb{Z})^\times$ における位数が q となるから明らか.) □

この系を使って, $2^{37} - 1$ の素因数を探してみよう. p を素数とする. $p \mid 2^{37} - 1$ なら系より $37 \mid p - 1$ である. p は奇数だから, $p = 74m + 1$ と書ける. $m = 1$ なら素数でない. $m = 2$ のとき $p = 149$ は素数. 149 を法として,

$$\begin{aligned}
2^{37} &= 2 \cdot 16 \cdot 256^4 \equiv 2 \cdot 16 \cdot (-42)^4 = 2 \cdot 16 \cdot 16 \cdot 21^4 \\
&\equiv 65 \cdot 441^2 \equiv 65 \times (-6)^2 = -44 \not\equiv 1
\end{aligned}$$

よって, 149 は $2^{37} - 1$ の因数ではない. $m = 3$ のとき, $p = 223$ は素数. 223 を法として,

$$\begin{aligned}
2^{37} &\equiv 2 \cdot 16 \cdot 33^4 = 2 \cdot 16 \cdot 81 \cdot 121^2 \equiv 8 \cdot 81 \cdot 242^2 \equiv 648 \times 19^2 \\
&= -21 \cdot 361 \equiv 21 \cdot 85 \equiv 7 \cdot 255 \equiv 224 \equiv 1
\end{aligned}$$

従って, $2^{37} - 1$ は 223 で割り切れる. 実際, $2^{37} - 1 = 223 \cdot 616318177$.

問 2. 系 2.6 を使って, $2^{17} - 1$ が素数であることを確かめよ.

同様にして, フェルマ数 $F_5 = 2^{2^5} + 1$ の素因子 641 をみつけることができる. 実際, p を フェルマ数 F_5 の素因数とすると,

$$2^{2^5} \equiv -1 \pmod p, \quad \text{従って,} \quad 2^{2^6} \equiv 1 \pmod p$$

である．このことから，$2^k \equiv 1 \pmod{p}$ となる最小の自然数 k をとると，$k \mid 2^6$ となり，$k = 2^i (i \leq 6)$ とかけることがわかるが，ここで $i \leq 5$ とすると $2^{2^5} \equiv -1 \pmod{p}$ に反する．よって $k = 2^6$ である．一方，フェルマの小定理から $2^{p-1} \equiv 1 \pmod{p}$ となるので，$2^6 \mid p-1$ すなわち，$p = 2^6 m + 1 = 64m + 1$ と表せることがわかる．$m = 1, 2, \ldots$ を代入し p が素数となるとき，それで F_5 が割れるかどうかをチェックしていくと $m = 10$ で $p = 641$ が F_5 の素因数となることがわかる．(オイラーはさらに $p = 128n + 1$ と表せることを示し，労力を半分に減らしている．)

フェルマ数のうち，素数であることがわかっているものは F_0 から F_4 の 5 個のみであり，現在に至るまで新たにフェルマ素数は見つかっていない．しかし，フェルマ数の素因数となっているような素数は無限にあることが次の命題により，容易にわかる．

命題 2.7. 異なるフェルマ数 F_i と F_j は互いに素である．特に，フェルマ数の素因数となっているような素数は無限にある．

Proof. 素数 p が $2^{2^i} + 1$ と $2^{2^j} + 1$ の共通の素因数だとする．$i < j$ とする．

$$2^{2^i} \equiv -1 \pmod{p}$$

だから，両辺を 2^{j-i} 乗すれば，

$$2^{2^j} \equiv 1 \pmod{p}$$

となる．これと $2^{2^j} \equiv -1 \pmod{p}$ より，$1 \equiv -1 \pmod{p}$ でなければならないが，これは $p = 2$ を意味する．フェルマ数は奇数だからこれは不可能である． □

素数が無限に存在することは，ユークリッドの「原論」で証明されている．それは背理法を使うもので有名であるが，この命題の証明は背理法を用いていないという点で興味深い．

3 平方和で表される数

3.1 ピタゴラス三角形

三辺の長さの最大公約数が 1 となるピタゴラス三角形を**固有なピタゴラス三角形**と呼ぶことにする．よく知られているように，三辺の長さが，$3, 4, 5$ のもの，$5, 12, 13$ のものは固有なピタゴラス三角形である．

ピタゴラス三角形の三辺 x, y, z (以後 z は常に斜辺を表す) の最大公約数を d とすれば，$\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ は固有なピタゴラス三角形の三辺となる．そこでピタゴラス三角形を決定する問題は固有なピタゴラス三角形を決定する問題に帰着される．

自然数 m, n $(m > n)$ に対して，次の三辺

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2 \tag{2}$$

がピタゴラス三角形を与えること，つまり

$$x^2 + y^2 = z^2 \tag{3}$$

を満たすことは，既に古代ギリシャの数学者ユークリッドの「幾何学原論」第１０巻の２８の補助定理 I で示されている．小さい m, n に対して (2) の与える値は下表のようになる．

m	n	x	y	z
2	1	4	3	5
4	1	8	15	17
6	1	12	35	37
3	2	12	5	13
5	2	20	21	29
4	3	24	7	25

固有なピタゴラス三角形は次の定理のように (2) の形のもので尽くされる．従って，ピタゴラス三角形は (2) の形のものを定数倍したもの，ということになる．

定理 3.1. 固有なピタゴラス三角形の三辺 x, y, z は（必要なら x, y を入れ換えて）$m - n$ が正の奇数となるような互いに素な自然数 m, n によって

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2 \tag{4}$$

と表される．また逆に m, n を $m - n$ が正の奇数となるような互いに素な自然数とすると，$2mn, m^2 - n^2, m^2 + n^2$ は固有なピタゴラス三角形の三辺となる．

(証明) まず，固有なピタゴラス三角形においては，斜辺以外の二辺の一方は偶数で他方は奇数となることに注意する．実際，

$$x^2 + y^2 = z^2$$

より，x, y が偶数なら z も偶数となり，$(x, y, z) = 1$ とはならない．x, y が奇数のときは，x^2, y^2 共に 4 で割った余りが 1 となるから，$x^2 + y^2$ を 4 で割った余りは 2 である．よって z^2 を 4 で割った余りは 2 となるが，このとき z 偶数でなくてはならないからこれもあり得ない．よって x, y の一方が偶数で他方が奇数でなければならない．そこで x を偶数，y を奇数としよう．このとき z は奇数である．さらに，$x^2 + y^2 = z^2$ より y, z の最大公約数は x も割り切り，x, y, z の公約数となる．$(x, y, z) = 1$ であったから $(y, z) = 1$ でないといけない．

このとき，つまり x が偶数，y, z が奇数で $x^2 + y^2 = z^2$，$(y, z) = 1$ のとき，適当な自然数 m, n によって $x = 2mn, y = m^2 - n^2, z = m^2 + n^2$ と表されることを示す．

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$
$$\left(\frac{x}{2}\right)^2 = \frac{z + y}{2} \cdot \frac{z - y}{2} \tag{5}$$

であるが，x は偶数，y, z は奇数だから，$\dfrac{x}{2}, \dfrac{z + y}{2}, \dfrac{z - y}{2}$ は自然数である．

$$y = \frac{z + y}{2} - \frac{z - y}{2}, \quad z = \frac{z + y}{2} + \frac{z - y}{2}$$

より，$(\dfrac{z + y}{2}, \dfrac{z - y}{2}) | (y, z)$．$(y, z) = 1$ であったから $\dfrac{z + y}{2}$ と $\dfrac{z - y}{2}$ は互いに素でなくてはならない．さてここで

$$\frac{x}{2} = p_1^{l_1} \cdots p_k^{l_k}$$

を $\dfrac{x}{2}$ の素因数分解とする．式 (5) より $\dfrac{z + y}{2}$ と $\dfrac{z - y}{2}$ の素因数分解も

$$\frac{z + y}{2} = p_1^{s_1} \cdots p_k^{s_k}, \qquad \frac{z - y}{2} = p_1^{t_1} \cdots p_k^{t_k}$$

のでなくてはならない．さらに式 (5) より

$$s_1 + t_1 = 2l_1, \ \cdots, \ s_k + t_k = 2l_k$$

でなければならない．しかし $\dfrac{z + y}{2}$ と $\dfrac{z - y}{2}$ は互いに素であるから各 i について $s_i > 0, t_i > 0$ となることはなく，s_i, t_i のどちらかが 0 で他方が $2l_i$ でなければならない．従って $p_1, \ldots, p_k$ の番号を適当に付け代えれば

$$\frac{z + y}{2} = p_1^{2l_1} \cdots p_j^{2l_j}, \qquad \frac{z - y}{2} = p_{j+1}^{2l_{j+1}} \cdots p_k^{2l_k}$$

とすることができる．ここで

$$m = p_1^{l_1} \cdots p_j^{l_j}, \qquad n = p_{j+1}^{l_{j+1}} \cdots p_k^{l_k}$$

とおけば $(m,n)=1$ であり，

$$x=2mn,\quad y=m^2-n^2,\quad z=m^2+n^2$$

を得る．y は正の奇数であったから $m-n$ も正の奇数でなくてはならない．これで前半の証明が終った．

次に後半を示す．まず

$$(2mn)^2+(m^2-n^2)^2=(m^2)^2+2m^2n^2+(n^2)^2=(m^2+n^2)^2$$

より，$2mn, m^2-n^2, m^2+n^2$ はピタゴラス三角形の三辺となる．$(m,n)=1$ で $m-n$ が正の奇数のとき，$(2mn, m^2-n^2, m^2+n^2)=1$ を示せばよい．$(2mn, m^2-n^2, m^2+n^2)=d$ とおく．

$$d \mid (m^2-n^2)+(m^2+n^2)=2m^2,\quad d \mid (m^2+n^2)-(m^2-n^2)=2n^2$$

より，$d \mid (2m^2, 2n^2)=2$．しかし $m-n$ が奇数であるから m,n の一方が偶数，他方が奇数である．よって m^2-n^2, m^2+n^2 も奇数であり，d も奇数でなくてはならない．これで $d=1$ となることがわかった． □

この定理の後半は上にも述べたように，古代ギリシャの時代，恐らくはもっと昔から知られていた．前半部が証明されたのはいつかはわからないが，少なくとも１０世紀のアラビアの本には書かれているそうである．この証明は自然数の素因数の一意性を用いているが，それは既にユークリッドの「幾何学原論」に現れているので，古代ギリシャから１０世紀の間のかなり早い時期に証明が得られていたとしても何ら不思議なことはない．

これで我々は（固有な）ピタゴラス三角形を無限に，しかも原理的には全て見つけることができる．しかし，ピタゴラス三角形をめぐる話題はこれで終わりではない．実際，近代整数論を生み出すきっかけとなる素数の間の神秘的な関係がピタゴラス三角形の中に隠されているのである．次節でそれを見てみよう．

3.2 平方数の和に関するフェルマの定理

以後，簡潔に述べるため自然数 z を

$$z=m^2+n^2$$

と二つの平方数の和としての表示を z の**表現**と呼び，さらにここで m と n が互いに素のとき，z の**固有表現**と呼ぶことにする．定理 3.1 から直ちに

命題 3.2. 2 以上の自然数 z が固有なピタゴラス三角形の斜辺であるための必要十分条件は，z が固有表現を持つ奇数となることである．

従って，前節の最後で提起した問題は

固有表現を持つ奇数はどのようなものであるか？

という問題と同じになる．恒等式

$$(x^2+y^2)(z^2+w^2) = (xz \mp yw)^2 + (xw \pm yz)^2 \tag{6}$$

により，表現を持つ数の積も表現を（一般に二通り）持つことがわかる．
100 以下の固有表現を持つ奇数について調べてみよう．すべてリストアップすると，次のようになる．

$$5,\quad 13,\quad 17,\quad 25,\quad 29,\quad 37,\quad 41,\quad 53,\quad 61,\quad 65,\quad 73,\quad 85,\quad 89,\quad 97$$

このうち素数でないものは $25 = 5^2,\ 65 = 5 \times 13,\ 85 = 5 \times 17$ であるが，その素因数 $5, 13, 17$ はまたこのリストに載っている．そこで固有表現を持つ奇数の素因数はまた固有表現を持つのではないかと予想されるであろう．この予想が実際に正しいことは，系 3.6 で示される．それを仮定すれば，固有表現を持つ奇数を求める問題は**固有表現を持つ奇素数**[*4]**を決定する問題**と同じことになる．ここで**素数の表現は必ず固有表現となる**ことを注意しておこう．実際，p を素数とし，$p = m^2 + n^2, (m, n) = d$ とすると，$d^2 \mid p$ となるから $d = 1$ でなくてはならない．そこで問題は表現を持つ奇素数，すなわち二つの平方数の和として表せる奇素数を求める問題となる．

100 以下の奇素数を二平方数の和で表せるものとそうでないものに分けると次のようになる．

表 1　100 以下の奇素数

2 平方数の和	5	13	17	29	37	41	53	61	73	89	97		
そうでないもの	3	7	11	19	23	31	43	47	59	67	71	79	83

さてここで，隣り合う 2 数の差をとると上段では $8, 4, 12, 8, 4, 12, 8, 12, 16, 8$，下段では $4, 4, 8, 4, 8, 12, 4, 12, 8, 4, 8, 4$ となり，すべて 4 の倍数である! このことはフェルマによって証明された．

[*4] 奇素数＝奇数の素数＝ 2 以外の素数

定理 3.3 (フェルマ)**.** 二つの平方数の和として表される奇素数は，4 で割った余りが 1 である素数に他ならない．またそのような素数を二つの平方数の和として表す表し方はただ一通りである．

Proof. p を奇素数とする．$p = m^2 + n^2$ と表されるとき，m が偶数，n が奇数であるとしてよい．すると $x^2 \equiv 0,\ y^2 \equiv 1 \pmod 4$ だから $p \equiv 1 \pmod 4$ である．

逆に $p \equiv 1 \pmod 4$ を満たす素数が二つの平方数の和としてただ一通りに表せることを示す．複素数を用いる現代的証明は次節で与えることにして，まずフェルマがやったと思われる証明を与えよう．証明は二段階に分かれる．

第一段階： $\quad p \mid a^2 + b^2, \quad (a, b) = 1 \quad \Longrightarrow \quad \exists m,\ n \in \mathbb{Z}; \quad p = m^2 + n^2.$

第二段階： $\quad p \equiv 1 \pmod 4 \quad \Longrightarrow \quad \exists a,\ b \in \mathbb{Z}; \quad p \mid a^2 + b^2, \quad (a, b) = 1.$

補題 3.4. $q = x^2 + y^2$ が素数，$q \mid a^2 + b^2 \Longrightarrow \exists c,\ d\ ; \quad \dfrac{a^2 + b^2}{q} = c^2 + d^2$．ここで $(a, b) = 1$ なら $(c, d) = 1$ となるものが取れる．

Proof.

$$(a^2 + b^2)q = (a^2 + b^2)(x^2 + y^2) = (ax \mp by)^2 + (ay \pm bx)^2 \qquad \text{(複合同順)}$$

だから $q \mid ay + bx$ または $q \mid ay - bx$ が言えれば，$q \mid ax - by$ または $q \mid ay + bx$ となることがわかる．このとき $c = \dfrac{ax \mp by}{q},\ d = \dfrac{ay \pm bx}{q}$ とおけば，$\dfrac{a^2 + b^2}{q} = c^2 + d^2$ が従う．$q \mid ay + bx$ または $q \mid ay - bx$ となることは，

$$(ay + bx)(ay - bx) = a^2y^2 - b^2x^2 = y^2(a^2 + b^2) - b^2(x^2 + y^2) = y^2(a^2 + b^2) - b^2q$$

からわかる．また，

$$cx + dy = (\frac{ax + by}{q})x + (\frac{ay - bx}{q})y = a, \quad cy - dx = (\frac{ax + by}{q})y - (\frac{ay - bx}{q})x = b$$

より $(a, b) = 1$ なら $(c, d) = 1$ でなければならない． □

この証明より，定理 3.3 の分解の一意性が分かる．実際，$q = x^2 + y^2 = a^2 + b^2$ として，証明の中のように c, d を決めると，$c^2 + d^2 = 1$ より，$c = \pm 1, d = 0$ または $c = 0, d = \pm 1$．よって $a = cx + dy = \pm x, b = cy - dx = \pm y$ または $a = \mp y, b = \pm x$.

第一段階の証明.
次の条件を満たす素数 p 全体の集合を $\mathcal{A}$ とする．

(D_p)　　$\exists a, b \in \mathbb{Z};\ p \mid a^2 + b^2,\ (a, b) = 1$ であるが，p は二つの平方数の和として表せない．

$\mathcal{A} \neq \emptyset$ として矛盾を導けばよい．それには

(*)　$p \in \mathcal{A} \implies \exists q \in \mathcal{A};\ p > q$

を示せばよい．というのは，もしこの条件が成り立てば，素数の無限減少列が作れることになってしまうからである．[*5]

$p \in \mathcal{A}$ とする．もちろん $p \neq 2$ である．$a = pn + a'$, $b = pm + b'$, $|a'|, |b'| < \dfrac{p}{2}$ となるように $m,\ n,\ a',\ b'$ をとる．a' と b' の最大公約数を d とし，$a' = da''$, $b' = db''$ とおくと，$p \mid a''^2 + b''^2$ である．実際，$p \mid a'^2 + b'^2 = d^2(a''^2 + b''^2)$ であるが，もし $p \mid d$ であれば $p \mid a',\ b'$ となり，よって $p \mid a,\ b$ となってしまい，$(a, b) = 1$ に反するからである．この $a'',\ b''$ をあらためて $a,\ b$ と書くことにすれば，

$$p \mid a^2 + b^2, \quad (a, b) = 1, \quad \frac{p}{2} > |a|,\ |b|$$

が成り立つ．$a^2 + b^2 = p^l q_1 \cdots q_r$ を $a^2 + b^2$ の素因数分解とし，$q_1, \ldots, q_r$ を p と異なる素因数とする．もし $q_1, \ldots, q_r$ のすべてが二つの平方数の和として表されるなら，補題を繰り返し使って，$p^l = c^2 + d^2$ と表せる．このとき，

$$p^l \leq a^2 + b^2 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 = \frac{p^2}{2}$$

となるから $l = 1$，よって $p = c^2 + d^2$ と表せる．これは $p \in \mathcal{A}$ に反する．よって，少なくとも一つの q_i は二つの平方数の和として表せない．$q_i p \mid a^2 + b^2 < \dfrac{p^2}{2}$ より $q_i < p$. これで (*) が示された．　□

第二段階の証明.

$p = 4k + 1$ と書く．フェルマの小定理より

$$x \not\equiv 0 \pmod{p} \Longrightarrow x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1) \equiv 0 \pmod{p}$$

体 $\mathbb{Z}/p\mathbb{Z}$ 上の方程式 $x^{2k} - 1 = 0$ が高々 $2k$ 個しか解を持たないことと $2k < 4k = p - 1$ から $x \not\equiv 0, x^{2k} - 1 \not\equiv 0 \pmod{p}$ となる $x \in \mathbb{Z}$ の存在がわかる．そのような x について $p \mid x^{2k} + 1$ となり，$(x, 1) = 1$ より，第二段階の証明が終わる．　□

[*5] いわゆるフェルマの無限降下法である．フェルマはこの方法で多数の定理を発見した．

素数 p が表現を持つための条件はわかったが，素数でない場合はどうであろうか．奇数 z が固有表現 $z = m^2 + n^2$ を持てば，m, n の一方は偶数で他方は奇数であるから，z を 4 で割った余りは 1 である．しかしこれらは十分条件ではない．例えば 21 は表現を持たない．フェルマはこれについても解答を与えている．

定理 3.5 (フェルマ)**.** 固有表現を持つ正の奇数は，4 で割った余りが 1 となるような素数の積として表されるものに他ならない．そのような正の奇数 z ($z = 1$ は除く) の相異なる素因数の数を t とすると，z を固有表現する仕方は丁度 2^{t-1} 通りある．

この証明も次節で与える．ここでは幾つかの例で確かめておこう．

例 3.1. (1) $21 = 3 \times 7$ であり，$3, 7$ は 4 で割って 3 余る素数だから 21 は固有表現を持たない．

(2) $65 = 5 \times 13$ だから 65 は二通りの固有表現を持つはずである．実際,

$$65 = 1^2 + 8^2 = 4^2 + 7^2.$$

(3) $1105 = 5 \times 13 \times 17$ だから 1105 は四通りの固有表現を持つはずである．実際,

$$1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2.$$

定理 3.5 から直ちに次の系を得る．

系 3.6. 固有表現を持つ正の奇数の約数はまた固有表現を持つ．また，固有表現を持つ正の奇数の積も固有表現を持つ.

z が固有表現を持つ奇数のとき，z^2 もまた固有表現を持つ奇数で，その相異なる素因数の数はどちらも同じである．よって z を斜辺の長さとするピタゴラス三角形の取り方（z^2 を固有表現する仕方）は z を固有表現する仕方と同じだけある．これで次の系が得られた.

系 3.7. 2 以上の自然数 z が固有なピタゴラス三角形の斜辺となるための必要十分条件は z の素因数がすべて $4m + 1$ 形であることである．このとき，z を斜辺とするようなピタゴラス三角形の取り方は，z の相異なる素因数の数を t とすると，丁度 2^{t-1} 通りである.

例 3.2. 定理 3.1 により, ピタゴラス三角形の三辺 x, y, z は斜辺 z の固有表現 $z = m^2 + n^2$ $(m > n)$ から $x = 2mn, y = m^2 - n^2$ によって得られる．ここで斜辺 z のピタゴラス三角形をすべて求める問題を具体的に解いてみよう.

(1) 17 を斜辺とするピタゴラス三角形：17 の固有表現は $17 = 4^2 + 1^2$ のみだから，$(8, 15, 17)$ のただ 1 組.

(2) 65 を斜辺とするピタゴラス三角形：65 の固有表現は $65 = 8^2 + 1^2 = 7^2 + 4^2$ の 2 通りだから，$(16, 63, 65), (56, 33, 65)$ の 2 組ある．

(3) 169 を斜辺とするピタゴラス三角形：$13 = 2^2 + 3^2$ だから $169 = 13^2$ の固有表現は $13^2 = (2 \cdot 2 \cdot 3)^2 + (3^2 - 2^2)^2 = 12^2 + 5^2$ のみ．よって，求めるピタゴラス三角形は $(119, 120, 169)$ のただ一組.

従って，定理 3.5 を証明すれば，我々の問題はすべて解けることになる．次節では，複素数を用いた定理 3.3 の別証明と，定理 3.5 の証明を与える．そのための準備として次節ではガウス (1777–1855) による複素整数の概念を導入する．

4 ガウスの複素整数

複素数 $m + n\sqrt{-1}$ において m, n が整数であるとき，これを**ガウスの整数**という．以下では複素数を英大文字 $A, B, C, \ldots$ などを用いて表す．英小文字は特に断りのない限り，実数 (大体は整数) を表すものとする．

4.1 複素共役，ノルム

定義 4.1. 複素数 $A = a + b\sqrt{-1}$ の**ノルム** $N(A)$ を

$$N(A) = a^2 + b^2$$

と定義する．複素数 $a - b\sqrt{-1}$ は A の**共役複素数**と呼ばれ，$\overline{A}$ と書かれる．A のノルムは $A\overline{A}$ である．

$$N(A) = A\overline{A} = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2$$

ノルム，共役についての以下の性質は基本的である．

$$\overline{\overline{A}} = A \tag{7}$$

$$N(\overline{A}) = N(A) \tag{8}$$

$$\overline{AB} = \overline{A}\ \overline{B} \tag{9}$$

$$N(AB) = N(A)N(B) \tag{10}$$

$$N(A) \geq 0 \tag{11}$$

$$N(A) = 0 \text{ ならば } A = 0 \tag{12}$$

証明はどれも容易であるから略す.

4.2 ガウスの整数の整除理論

定義 4.2. A, B をガウスの整数，$B \neq 0$ とする．複素数 $\dfrac{A}{B}$ がまたガウスの整数となるとき，B は A を**割り切る**といい，$B \mid A$ と表す．またこのとき，B は A の**約元**であるといい，A は B の**倍元**であるという.

例 4.1. (1) $2 = (1+\sqrt{-1})(1-\sqrt{-1})$ であるから $1 \pm \sqrt{-1}$ は 2 の約元である.

(2) d を 0 でない整数とする.

$$\frac{a+b\sqrt{-1}}{d} = \frac{a}{d} + \frac{b}{d}\sqrt{-1}$$

により，$a+b\sqrt{-1}$ が d の倍元というのは，a, b が共に d の倍数となることを意味する.

0 でないガウスの整数のノルムは自然数である．またノルムが積を保つことから，次は明らかであろう.

補題 4.1. B が A の約元ならば，整数 $N(B)$ は整数 $N(A)$ の約数である.

整数の場合には 1 と -1 はすべての整数の約数であり，従って n が m を割り切るかどうかは n, m に -1 を掛けても変わらない．ガウスの整数の場合には，± 1 にあたるものは他にもあり，$\pm\sqrt{-1}$ がそうである．これらに名前を付けておこう.

定義 4.3. 1 の約元を**単元**という．A が B の単元倍であるとき (このとき B も A の単元倍である)，A と B は**同伴**であるという.

整数の場合には，単元は ± 1 で，n と同伴なものは $\pm n$ である．補題 4.1 とノルムの定義から次も明らかであろう.

補題 4.2. ガウスの整数 A, B について,

(1) A が単元であるということは $N(A) = 1$ ということと同じである.
(2) A と B は同伴であることと $A \mid B$ かつ $B \mid A$ であることは同じである.

系 4.3. 単元は $1, -1, \sqrt{-1}, -\sqrt{-1}$ の 4 つである.

系 4.4. $m+n\sqrt{-1}$ と同伴なものは次の 4 つ.

$$m+n\sqrt{-1},\quad -m-n\sqrt{-1},\quad -n+m\sqrt{-1},\quad n-m\sqrt{-1}.$$

次に素数の概念をガウスの整数に対しても拡張しよう.

定義 4.4. ガウスの整数 A が**ガウスの素数**であるとは，A が単元でなく，また A の約元が $1, A$ およびそれらに同伴なものに限ることをいう.

命題 4.5. $N(A)$ が素数のとき，A はガウスの素数である.

Proof. B を A の約元とする．$A=BC$ とおくと $N(A)=N(B)N(C)$ であり $N(A)$ は素数だから $N(B)=1$ または $N(C)=1$．よって B または C が単元であるから A はガウスの素数となることがわかる. □

ガウスの整数をガウスの素数の積として表すことを素元分解するという.

定理 4.6. 任意の 0 でないガウスの整数の素元分解は順序と同伴を無視すればただ一つ存在する.

証明は多くの準備を要するので省略する．証明を知りたい人は参考文献 [3] の第 4 章を参照されたい．通常の素数の持つ最も重要な性質は,「素数 p が整数 a, b の積を割り切れば a か b のどちらかを割り切る」ということである．この性質はガウスの素数に対しても成り立つ.

系 4.7. ガウスの素数 P がガウスの整数 A, B の積 AB を割り切れば P は A か B のどちらかを割り切る.

Proof. $AB=PC$ とする．C の素元分解を $P_1\cdots P_t$ とすると，$PP_1\cdots P_t$ が AB の素元分解となる．素元分解の一意性より，P は A または B の素元分解の中に現れなければならない. □

例 4.2. (1) 素数 p が表現 $p=x^2+y^2$ を持つとき，$N(x\pm y\sqrt{-1})=p$ だから，命題 4.5 より $x\pm y\sqrt{-1}$ はガウスの素数である．よって,

$$p=(x+y\sqrt{-1})(x-y\sqrt{-1})$$

は p の素元分解を与える.

(2) $3+11\sqrt{-1}$ の素元分解：

$$3+11\sqrt{-1}=(1-\sqrt{-1})(1+2\sqrt{-1})(2+3\sqrt{-1}).$$

4.3 ガウスの素数とフェルマの定理

ガウスの素数の分類問題は結局フェルマの定理 3.3 に帰着される．まず，素数 p がガウスの素数になるための条件を求めよう．

命題 4.8. 素数 p がガウスの素数でないならば，p は二つの平方数の和として表される．

Proof. p がガウスの素数でないなら，単元でない A, B により $p = AB$ と分解する．ノルムをとると

$$p^2 = N(p) = N(A)N(B).$$

A, B は単元でないから，$N(A) \neq 1, N(B) \neq 1$．よって $N(A) = N(B) = p$ となる．$A = x + y\sqrt{-1}$ とおくと $p = N(A) = x^2 + y^2$ となる． □

ではここで定理 3.3 の「4 で割った余りが 1 となる素数 p が二つの平方数の和で表せる」という部分の別証明を与える．ただし，第二段階の部分はそのまま用いる．

p を 4 で割って 1 余る素数とする．このとき $p = 4m + 1$ と表しておく．p を二平方数の和として表したい．命題 4.8 より p がガウスの素数でないことを示せばよい．

このような n をとると，p はガウスの整数として

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

の約元である．しかし p は $n^m \pm \sqrt{-1}$ の約元ではない．よって 系 4.7 により，p はガウスの素数ではない．

最後に，素数 p が $p = x^2 + y^2$ と表せたとき，その仕方がただ一通りであることを示す．$p = x^2 + y^2 = z^2 + w^2$ とする．ただし x, y, z, w は自然数とする．$N(x \pm y\sqrt{-1}) = N(z \pm w\sqrt{-1}) = p$ だから $x \pm y\sqrt{-1}, z \pm w\sqrt{-1}$ はすべてガウスの素数である．よって

$$(x + y\sqrt{-1})(x - y\sqrt{-1}) = (z + w\sqrt{-1})(z - w\sqrt{-1})$$

は 2 通りの p の素元分解を与える．よって，定理 4.6 の一意性の部分から $x + y\sqrt{-1}$ は $z + w\sqrt{-1}$ または $z - w\sqrt{-1}$ の単元倍に等しい．x, y, z, w は全て正だから，可能な組み合わせは $x + y\sqrt{-1} = z + w\sqrt{-1}$ または $w + z\sqrt{-1}$ しかない．前者なら $x = z, y = w$ で，後者なら $x = w, y = z$ であり，いずれにしろ p の表現としては同じものである． □

ではガウスの素数を全て決定しよう．

定理 4.9. ガウスの素数は次のどれかに同伴なものである．

(1) 4 で割った余りが 1 となる素数 p の表現 を $p = x^2 + y^2$ としたときの $x + y\sqrt{-1}$ およびその複素共役 $x - y\sqrt{-1}$,
(2) 4 で割った余りが 3 となる素数 p,
(3) $1 - \sqrt{-1}$.

Proof. $N(1 - \sqrt{-1}) = 2$ だから $1 - \sqrt{-1}$ はガウスの素数である．p が 4 で割って 3 余る素数だとすると，定理 3.3 より p は表現を持たない．よって命題 4.8 より p はガウスの素数である．(1) についても $N(x \pm y\sqrt{-1})$ が素数だから $x \pm y\sqrt{-1}$ はガウスの素数である．

次にガウスの素数がこれらのどれかと同伴になることを示す．$P = a + b\sqrt{-1}$ をガウスの素数とする．$P \mid N(P)$ であるから P は $N(P)$ の（整数としての）素因数の少なくとも一つを割り切る．その一つを p とおく．$P \mid p$ より $N(P) \mid N(p) = p^2$．よって，$N(P) = p$ または p^2．$N(P) = p$ のとき，$p = a^2 + b^2$ であるから $p = 2$ または p を 4 で割った余りは 1 となる．$p = 2$ のとき $a = \pm 1, b = \pm 1$ であり，P は $1 - \sqrt{-1}$ に同伴となる．p を 4 で割った余りが 1 のとき，P は (1) のものになる．$N(P) = p^2$ のとき，$P \mid p$ かつ $N(P) = N(p)$ より P は p に同伴で (2) のものとなる． □

(1) のタイプのガウスの素数を **I 型のガウスの素数**，(2) のタイプのものに同伴なものを **II 型のガウスの素数**ということにする．

(1) の $x + y\sqrt{-1}$ と $x - y\sqrt{-1}$ は同伴ではない．実際，同伴だとすると，系 4.4 により $x - y\sqrt{-1}$ は $x + y\sqrt{-1}, -x - y\sqrt{-1}, -y + x\sqrt{-1}, y - x\sqrt{-1}$ のどれかに等しい．よって $y = 0, x = 0, x = -y, x = y$ のどれかが成り立たねばならない．しかし，どれも $p = x^2 + y^2$ と $p \neq 2$ より成り立たない．

補題 4.10. $m + n\sqrt{-1}$ が $1 - \sqrt{-1}$ で割り切れるならば，$m - n$ は偶数である．

Proof. 実際,

$$m + n\sqrt{-1} = (1 - \sqrt{-1})(a + b\sqrt{-1}) = a + b + (b - a)\sqrt{-1}$$

なら $m - n = 2a$ である． □

最後に，定理 3.5 を証明しよう．

(定理 3.5 の証明)
正の奇数 z が固有表現 $z = m^2 + n^2$ を持つとする．$m + n\sqrt{-1}$ の素元分解を

$$m + n\sqrt{-1} = P_1 P_2 \cdots P_t \tag{13}$$

とする．$P_1, P_2, \ldots, P_t$ の中に II 型のものがあれば m, n が互いに素でなくなってしまう．また $1-\sqrt{-1}$ が含まれていれば，上の補題より $m-n$ が偶数となり，z が偶数となってしまう．よって $P_1, P_2, \ldots, P_t$ はすべて I 型の素数である．式 (13) の両辺のノルムをとれば z は 4 で割って 1 余る素数の積として表される．

逆に z の素因数分解が 4 で割って 1 余る素数 $p_1, p_2, \ldots, p_t$ により

$$z = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t} \tag{14}$$

と表されているとする．ここで，$p_1, p_2, \ldots, p_t$ はすべて異なるとする．p_i は 4 で割って 1 余る素数だから

$$p_i = x_i^2 + y_i^2 = (x_i + y_i\sqrt{-1})(x_i - y_i\sqrt{-1})$$

と表される．$P_i = x_i + y_i\sqrt{-1}$ とおく．ここで

$$P_1^{l_1} \cdots P_t^{l_t} = m + n\sqrt{-1} \tag{15}$$

とおくと，ノルムをとれば $z = m^2 + n^2$ を得る．さらに $(m, n) = 1$ である．実際，$(m, n) > 1$ のとき，m, n の共通の素因数 p がとれる．$z = m^2 + n^2$ の右辺は p^2 で割れるから p はある p_i に一致する．すると $p = P_i\overline{P_i}$ であり，$\overline{P_i}$ が (15) の右辺を割り切ることになるが，これはあり得ない．よって $(m, n) = 1$ でなければならない．これで z が固有表現を持つ正の奇数であることがわかった．

最後に固有表現の数を求める．簡単のため $t = 2$ としよう．一般の場合も全く同様である．z の素因数分解を (14) として引き続き同じ記号を用いる．まず z の異なる固有表現を 2 通り作ろう．

$$P_1^{l_1} P_2^{l_2} = m_1 + n_1\sqrt{-1}, \qquad P_1^{l_1}\overline{P_2}^{l_2} = m_2 + n_2\sqrt{-1}$$

とおく．このとき上で示したように $z = m_1^2 + n_1^2 = m_2^2 + n_2^2$ となる．この二つの分解は相異なる．というのは，もし同じ分解を与えるとすると，$m_1 = \pm m_2, n_1 = \pm n_2$ または $m_1 = \pm n_2, n_1 = \pm m_2$ (復号同順ではない) となるが，このとき $P_1^{l_1} P_2^{l_2}$ は $P_1^{l_1}\overline{P_2}^{l_2}$ または $\overline{P_1^{l_1}\overline{P_2}^{l_2}} = \overline{P_1}^{l_1} P_2^{l_2}$ と同伴でなければならない．しかしこれは素元分解の一意性よりあり得ない．

そこで定理の証明を終えるためには，z のすべての固有表現がこのどちらかと同じであることをいえばよい．$z = a^2 + b^2$ を z の固有表現とする．z の素元分解を考えると

$$P_1^{l_1}\overline{P_1}^{l_1} P_2^{l_2}\overline{P_2}^{l_2} = (a + b\sqrt{-1})(a - b\sqrt{-1})$$

である．I 型のガウスの素数 P で $a+b\sqrt{-1}$ と $a-b\sqrt{-1}$ の両方を割り切るものはないことに注意しよう．実際, $P \mid a \pm b\sqrt{-1}$ ならば $P, \overline{P} \mid a+b\sqrt{-1}$ となり, $P\overline{P} \mid a+b\sqrt{-1}$ となる．$P\overline{P}$ は素数であるから，これは a と b が互いに素であることに反する．よって $P_1^{l_1}$ は $a+b\sqrt{-1}$ か $a-b\sqrt{-1}$ を割り切る．必要なら b を $-b$ と置き換えて $a+b\sqrt{-1}$ の方を割り切るとする．このとき $\overline{P_1}^{l_1}$ は $a-b\sqrt{-1}$ の方を割り切る．次に $P_2^{l_2}$ も $a+b\sqrt{-1}$ か $a-b\sqrt{-1}$ を割り切るが, $a+b\sqrt{-1}$ を割り切れば $\overline{P_2}^{l_2}$ は $a-b\sqrt{-1}$ を割り切り，従って $a+b\sqrt{-1}$ は $P_1^{l_1}P_2^{l_2}$ と同伴となる．同様に $P_2^{l_2}$ が $a-b\sqrt{-1}$ を割り切れば $a+b\sqrt{-1}$ は $P_1^{l_1}\overline{P_2}^{l_2}$ と同伴となる．よって，z の分解 $z=a^2+b^2$ は $m_1^2+n_1^2$ または $m_2^2+n_2^2$ のどちらかに一致する．これで定理の証明がすべて終わった． □

例 4.3. 15457 を斜辺の長さとする固有なピタゴラス三角形を全て求めよう．

$15457 = 13 \times 29 \times 41$．$13 = 4+9,\ 29 = 4+25,\ 41 = 16+25$.

$$(2+3\sqrt{-1})(2+5\sqrt{-1})(4+5\sqrt{-1}) = (-11+16\sqrt{-1})(4+5\sqrt{-1}) = -124+9\sqrt{-1}$$
$$(2+3\sqrt{-1})(2+5\sqrt{-1})(4-5\sqrt{-1}) = (-11+16\sqrt{-1})(4-5\sqrt{-1}) = 36+119\sqrt{-1}$$
$$(2+3\sqrt{-1})(2-5\sqrt{-1})(4+5\sqrt{-1}) = (19-4\sqrt{-1})(4+5\sqrt{-1}) = 96+79\sqrt{-1}$$
$$(2+3\sqrt{-1})(2-5\sqrt{-1})(4-5\sqrt{-1}) = (19-4\sqrt{-1})(4-5\sqrt{-1}) = 56+111\sqrt{-1}$$

よって,

$$155457 = 124^2+9^2 = 36^2+119^2 = 96^2+79^2 = 56^2+111^2$$

の 4 つが 15457 の固有表現のすべてである．これより，求めるピタゴラス三角形の 2 辺 (x, y) は

$$(2\cdot 124\cdot 9,\ 124^2-9^2) = (2232,\ 15295)$$
$$(2\cdot 119\cdot 36,\ 119^2-36^2) = (8568,\ 12865)$$
$$(2\cdot 111\cdot 56,\ 111^2-56^2) = (12432,\ 9185)$$
$$(2\cdot 96\cdot 79,\ 96^2-79^2) = (15168,\ 2975)$$

の 4 組である．

5　フェルマの小定理と暗号

フェルマの小定理は暗号システムによく用いられている．古典的な暗号システムでは，例えば A さんが B さんに暗号を送る場合に次のような手順をとっていた．（実際には以下の方法を電子的に実現する．）

(1) A さんは鍵の掛かる箱に文書を入れて鍵を締め，B さんに送る．
(2) A さんは更に，別の方法で B さんに鍵を送る．
(3) B さんは，A さんから送られてきた鍵で箱を開けて目的の文書を得る．

しかし，この方法では箱と鍵が途中で盗まれてしまえば終わりである．そこで次のような公開鍵暗号システムという方法が考案された．

(1) B さんはあらかじめ鍵の掛かる箱を用意しておくのだが，鍵を締めるための鍵 A と，開けるための鍵 B が別々であるようなものにしておき，その箱と締める鍵を公開しておく．
(2) A さんは B さんが公開している箱と鍵を持ってきてそれに送りたい文書を入れて鍵 A で鍵を締め，B さんに送る．
(3) B さんは送られてきた箱を，あらかじめ作ってあった開ける鍵 B を使って開け文書を得る．

この方法なら開ける鍵は二人の間で送る必要はなく，最初から B さんが保管しておけばよいので前の方法に比べ格段に安全である．

1978 年に発明された RSA 暗号[*6]はこの公開鍵暗号システムをフェルマの小定理を用いて実現したものである．まず暗号の手順を示す．

(1) B さんは大きい二つの異なる素数 p, q を用意して $(p-1)(q-1)$ と互いに素な自然数 r を一つ選んでおく．また $rs-1$ が $(p-1)(q-1)$ で割り切れるような自然数 s を一つ求めておく．(このような s の求め方は既に学んだ．) 更に，$n = pq$ を計算し n, r を公開する．この n が箱，r が鍵 A，s が鍵 B の役割を果たす．
(2) A さんは送りたい文書を適当な長さに区切り，それぞれを適当な方法で数値化し，$a_1, a_2, \ldots, a_l$ とする．ここで各 a_i が n より小さい自然数となるようにしておく．

[*6] RSA はこの暗号システムの発明者 Rivest, Shamir, Adleman の頭文字を並べたもの

(例えば，文書で使用する文字の数が 50 なら文字を順に並べて 0 から 49 までの数字と同一視すれば m 個の文字の列を 50 進数で書かれた m 桁の数字と見ることができる．$50^m < n$ となるような m を選び，文書を m 文字づつに区切ればよい．)
A さんは a_i^r を n で割った余り b_i を計算し，$b_1, b_2, \ldots, b_l$ を B さんに送る．

(3) B さんは b_i^s を n で割った余りを計算する．これが a_i になっている．

これを証明しよう．$a = a_i, b = b_i$ とおく．$rs - 1$ は $(p-1)(q-1)$ で割り切れるから

$$rs = (p-1)(q-1)l + 1$$

とおける．$p \nmid a$ のとき，フェルマの小定理により，

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

両辺を $(q-1)l$ 乗してから両辺に a を掛けて

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

$p \mid a$ のときは，この式は明らかに正しい．同様に

$$a^{(p-1)(q-1)l+1} \equiv a \pmod{q}$$

も成り立つから，

$$b^s \equiv (a^r)^s \equiv a^{(p-1)(q-1)l+1} \equiv a \pmod{n}$$

これで B さんは $a_1, a_2, \ldots, a_l$ を得ることができ，これを文字に直してもとの文書を得る．

このシステムでは s が開ける鍵となっている．この s は B さんのみが知っており公開されていないが, 第三者も n の素因数分解 pq を求められれば $rx \equiv 1 \pmod{(p-1)(q-1)}$ を解いて s を求めることができる．そこで，この暗号が有効に機能するためには n の素因数分解が出来ないことが前提となっている．理論的には素因数分解はいつでも可能であるが，大きな素数 p, q を求めてそれを掛け合わせて n を計算する時間に比べてそれを素因数分解する時間は飛躍的に長くなることが知られている．このことを利用して，n を素因数分解するのが現実的に不可能であるぐらい大きな素数を選んでこの暗号システムが運用されている．

6　楕円曲線上の加法と暗号

整数係数の (連立) 代数方程式の有理数解を求める問題は，A.D.3 世紀ごろのディオフォントスによって始められ，ディオフォントス問題といわれる．ディオフォントスは「算術」[*7]という書物でそのような問題を多数解いている．３節では，不定方程式

$$X^2 + Y^2 = Z^2$$

のすべての整数解を求めたが，この問題は

$$x^2 + y^2 = 1$$

を解くディオフォントス問題と同じものである．ディオフォントスの「算術」で扱っている問題の中には，２変数の高々３次の代数方程式を解くことに帰着されるものが多くみられる．二変数の代数方程式の解集合が定める座標平面上の曲線を (平面) 代数曲線という．ディオフォントスは高々３次のいろいろな代数曲線上の有理点 (座標が有理数である点) を求めたことになる．２次の代数曲線は円錐曲線と呼ばれ，楕円，放物線，双曲線などである．そして３次の代数曲線がこの講義の主題の一つである楕円曲線なのである．これらの代数曲線はより高次のの代数曲線と異なり良い対称性を持っている．この 3 次以下の代数曲線を C とすると，C の各二点 P, Q に対してその和となる C の点 $P + Q$ を定めることができるのである．この点の和は通常の和と同じく，結合法則などを満たすものである．しかも，もし P, Q が有理点なら $P + Q$ も有理点となる．このことから有理点の和をとることにより，次々と新しい有理点をみつけることができる．もちろんディオフォントス自身はこのような背景は知り得なかったが，彼の計算の中にこの加法が隠れていることがわかる．

6.1　楕円曲線上の加法

K を体とし，簡単のため この体では $2 \neq 0, 3 \neq 0$ であるとする．a, b を K の元とし，$4a^3 + 27b^2 \neq 0$ とする．

$$y^2 = x^3 + ax + b$$

[*7] 13 巻からなり，そのうち 6 巻が現在残っている．

を満たす (x, y) の全体集合に無限遠点と呼ばれ，O と書かれるものを付け加えた集合

$$E := \{(x, y) \mid x, y \in K,\ y^2 = x^3 + ax + b\} \cup \{O\}$$

を体 K 上の楕円曲線という．例えば $K = \mathbb{R}$ とすれば，楕円曲線

$$y^2 = x^3 - x$$

は次の図の曲線に無限遠点を付け加えたものである．

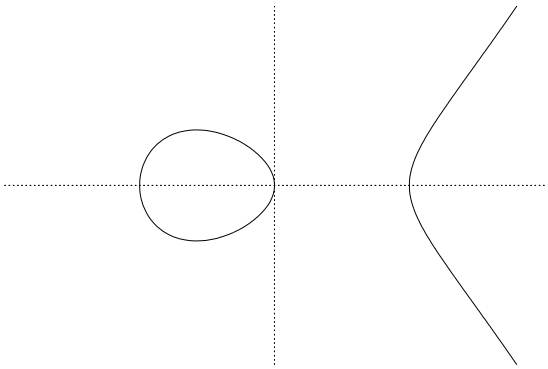


図 1　$y^2 = x^3 - x$

条件 $4a^3 + 27b^2 = 0$ の場合には，曲線 $y^2 = x^3 + ax + b$ は ” 特異点 ” を持つ．特異点とは，その点で接線が引けない点のことである．

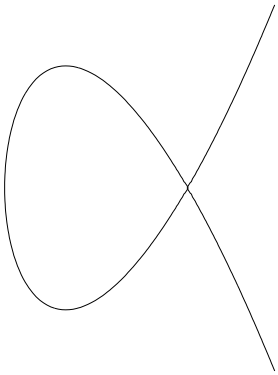


図 2　$y^2 = x^3 - 3x + 2$

楕円曲線の美しさ，重要性は，その上に加法が定まることに起因している．曲線上に加法が定まるとはどういうことかはっきり定義しておこう．

一般に集合 G の各二元 g, h に対して，その和と呼ばれる元 $g + h$ が定められていて，次の法則を満たすとき，G はこの和に関して加法群になっているという．

(1) 任意の $g,h,k \in G$ に対して，$(g+h)+k = g+(h+k)$.
(2) G の元 0 で，任意の $g \in G$ に対し，$g+0 = 0+g = g$ を満たすものが存在する．
(3) 各 $g \in G$ に対して，$g+h = 0 = h+g$ を満たす $h \in G$ が存在する．
(4) 任意の $g,h \in G$ に対して，$g+h = h+g$ が成り立つ．

加法群 G に対して，条件 (2) にある 0 を単位元または零元という．単位元はただ一つに定まることは容易にわかる．また，(3) の h を g の逆元という．g の逆元も g を決めればただ一つに定まる．

楕円曲線に加法を入れる前に，直線，円上の加法について見ておこう．

例 6.1. (i) 直線上に一点 O をとり，それが単位元となるような加法を定めよう．直線上の 2 点 P,Q をとるとき，直線の向きを保ったまま O が P に重なるように平行移動する．このとき Q が移動した先の点を $P+Q$ と定める．これは直線上に座標を導入し数直線としたときに，我々が通常行っている実数の足し算を幾何的におこなったものにすぎない．実数の加法が加法群の定義の (1) から (4) の性質を満たしていることから，直線がこの加法に関して加法群となることがわかる．

(2) 平面上に 1 点 A で交わる二つの直線 l と m をとる．また，l 上に A と異なる 1 点 O をとる．l から 1 点 A を除いたもの $l^\times$ に O を単位元とする加法を定めよう．

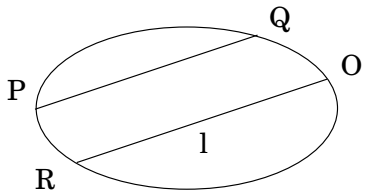
$l^\times$ 上に 2 点 P,Q をとる．A を中心とし半径 OA の円 C_O を描き，O から円 C_O に沿って反時計回りに動き，最初に直線 m とぶつかる点を O' とする．同様に，直線 m 上の点 Q' を定める．次に，Q' を通って直線 $O'P$ と平行な直線を描き，それと l との交点を $P+Q$ と定める．

直線 l 上に座標を A が 0，O が 1 となるように入れ，l を数直線とみなすと，今定義した加法は，$l^\times = \mathbb{R} - \{0\}$ 上の乗法に他ならない．

(3) 次に楕円[*8]の上に加法を幾何学的に定義しよう．放物線，双曲線にも同様に加法が定義できる．楕円 C を一つ固定し，その上に一点 O をとり固定しておく．C 上の二点 P,Q をとる．直線と楕円が (交われば) 2 点で交わることを利用する．

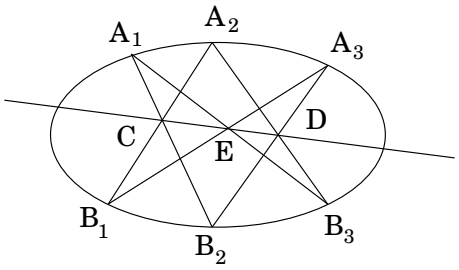
O から直線 PQ と並行に直線 $l_{P,Q}$ を引き，それと C との交点を $P+Q$ とする．$P=Q$ のときは直線 PQ の代わりに P における C の接線を用いる．$l_{P,Q}$ が C に O で接するときは $P+Q=O$ とする．

[*8] 楕円と楕円曲線は異なる．楕円曲線の命名の理由は，楕円の弧長を求める積分から発見されたことによる．



上の (1) から (4) を確かめよう．(2)，(4) は定義から明らかである．(3) を確かめる．C 上の点 P を通り O での C への接線に平行な直線 l と C の交点で，P 以外の点を Q とおく．ただし l が C に接する場合は $Q = P$ とする．このとき $P + Q = O$ となることは定義より明らかである．最後に (1) を示す．これには射影幾何学のパスカルの定理が必要である．

定理 6.1 (パスカルの定理)**.** 射影平面内の二次曲線上に六点 $A_1, A_2, A_3, B_1, B_2, B_3$ を任意に取る．直線 A_1B_2 と A_2B_1 の交点を C，A_2B_3 と A_3B_2 の交点を D，A_3B_1 と A_1B_3 の交点を E とすると C, D, E は一直線上にある．



この定理を用いれば，結合法則 (1) は容易に従うのだが，２直線が平行な場合，その交点は ” 無限遠点 ” として存在するという風に解釈しなくてはならない．射影幾何学では，一つの直線 l 上に点 P をとり，一方向に動かして行くと無限遠の彼方には１点 ∞_l があると考える．また，P を逆方向に動かして行ってもやはり無限遠には先ほどの点 ∞_l があると考えるのである．従って，P を一方向にずっと動かして行けば，無限遠点 ∞_l を通過して，今度は直線の反対方向の無限遠の彼方から戻って来る．また，二つの直線 l, m 上の無限遠点 ∞_l, ∞_m は l と m が平行なとき，そのときに限り一致すると考える．そして，無限遠点すべてが集まって一つの無限遠直線になっている．パスカルの定理はこのように直線の交点を拡大解釈してもなお成り立つ定理なのである．ちなみにパスカルはこの定理を１６才のときに発見した．

パスカルの定理を $A_1B_2//A_2B_1, A_2B_3//A_3B_2$ の場合に適用すると，C, D は無

限遠点であり，それらを通る直線は無限遠直線である．よって E は無限遠点でなければならない．これは $A_3B_1//A_1B_3$ を意味する．

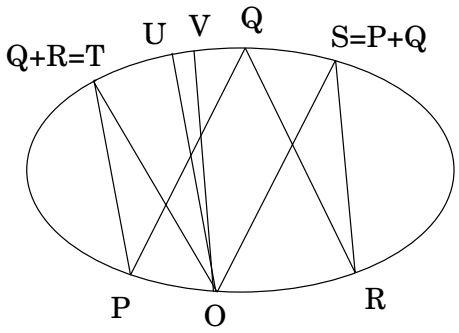
では (1) の証明に戻ろう．下図のように P,Q,R,O を取り，$S=P+Q, T=Q+R$ を求める．

$$PT//OU, \qquad RS//OV$$

となるように楕円 C 上に U,V をとれば

$$U=P+(Q+R), \qquad V=(P+Q)+R$$

となっている．今，$PQ//OS$, $QR//OT$ だから，$A_1=P, A_2=O, A_3=R, B_1=S, B_2=Q, B_3=T$ としてパスカルの定理を適用すれば，$RS//PT$ を得る．よって $OU//OT$ となり，$U=T$ でなければならない．



ではいよいよ楕円曲線上に加法を導入しよう．まず $K=\mathbb{R}$ の場合を考える．E を式

$$y^2=x^3+ax+b, \qquad (4a^3+27b^2\neq 0)$$

で定義される体 $\mathbb{R}$ 上の楕円曲線とする．以後，E の元を E 上の点とよぶ．E の点は無限遠点 O と $E_0:=\{(x,y)\mid x,y\in K, y^2=x^3+ax+b\}$ の点とから成り立っている．

この無限遠点 O は直線 $x=0$ 上の無限遠点であるとする．よって直線 $x=t$ $(t\in\mathbb{R})$ はすべてこの点 O を通る．また直線 $y=cx+d$ は O を通らない．O を通る直線には，この他にただ一つ無限遠直線 L_∞ がある．

さて楕円曲線 E には，各点 $P\in E$ において接線 l_P が引ける．これを保証しているのが条件 $4a^3+27b^2\neq 0$ である．l_P の方程式は $P=(x_1,y_1)$ で $y_1\neq 0$ のとき，

$$l_P: y=\frac{3x_1^2+a}{2y_1}(x-x_1)+y_1 \tag{16}$$

$y_1 = 0$ のとき，

$$l_P : x = x_1 \tag{17}$$

である．$P = O$ のときは，この講義では天下り的に

$$l_O = \text{ 無限遠直線 } L_\infty \tag{18}$$

と定義しなければならない．

これで，射影平面上の直線と楕円曲線 E が接するということが定義できたので，射影平面上の直線と E との交わり方を分類しておこう．

直線 $l : y = cx + d$ と E_0 との交点は $y^2 = x^3 + ax + b$ に $y = cx + d$ を代入して得られる x についての 3 次方程式を解いて得られる．この 3 次方程式の解について，次の 4 通りが考えられる．

(i)' 3 つの異なる実数解 x_1, x_2, x_3 を持つ．
(ii)' 一つの実数解 x_1 と二つの虚数解 x_2, x_3 を持つ．
(iii)' 一つの 2 重解 x_1 と，それと異なる一つの実数解 x_2 を持つ．
(iv)' 一つの 3 重解 x_1 のみを持つ．

$P_i = (x_i, cx_i + d)$ とおくと，(i)' から (iv)' に応じて，l と E の交わり方は，以下のようになっている．

(i) l と E は異なる 3 点 P_1, P_2, P_3 で交わる．
(ii) l と E はただ 1 点 P_1 で交わる．
(iii) l と E は 1 点 P_1 で接し，他の 1 点 P_2 で交わる．
(iv) l と E は 1 点 P_1 で接し，他の点では交わらない．

次に，直線 $l : x = e$ と E との交わり方は，

(v) $e^3 + ae + b > 0$ のとき，異なる 3 点 $O, P = (e, \sqrt{e^3 + ae + b}), Q = (e, -\sqrt{e^3 + ae + b})$ で交わる．
(vi) $e^3 + ae + b = 0$ のとき，$P = (e, 0)$ で接し，他の 1 点 O で交わる．
(vii) $e^3 + ae + b < 0$ のとき，ただ 1 点 O で交わる．

無限遠直線 L_∞ と E については

(viii) L_∞ と E は 1 点 O で接し，他の点では交わらない．

これで，射影平面上の直線と楕円曲線 E との交わり方がすべて分類できた．

以後，$l \cdot E = [P, Q, R]$ と書いたら，

- (i)，(v) のように l と E が異なる 3 点 P, Q, R で交わっている，
- P, Q, R のうち，二つが等しく，残り一つは異なり，(iii) や (vi) のように l と E は等しい二つの点で接し，残りの点で交わっている，
- $P = Q = R$ で (iv) や (viii) のように l と E はただ 1 点 $P = Q = R$ のみで接し，他の点では交わらない，

のどれかを表すとする．従ってこのように書かれた場合には，l と E の交わり方は，(ii)，(vii) のようになっていない．

以上の準備の元に，E 上に加法を定義しよう．まず $E \ni P = (x, y)$ に対し，

$$-P := (x, -y)$$

と定義する．また，

$$-O := O$$

とする．E 上の 2 点 P, Q に対し，

$$l_{P,Q} := \begin{cases} P, Q \text{ を結ぶ直線} & (P \neq Q \text{ のとき}) \\ \text{接線 } l_P & (P = Q \text{ のとき}) \end{cases}$$

とおく．そして，$P + Q$ を

$$l_{P,Q} \cdot E = [P, Q, -(P + Q)]$$

であるように定める．すなわち，$l = l_{P,Q}$ と E の交わり方が (i), (v) のときは，$-(P+Q)$ を l と E との P, Q 以外の交点とする．(iii), (vi) のときは，$P = Q$ なら，l と E が交わる P 以外の点を $-(P+Q)$ とし，$P \neq Q$ ならば P で接しているときは $-(P+Q) = P$，Q で接しているときは $-(P+Q) = Q$ とする．(iv), (viii) のときは，$-(P+Q) = P$ とする．

これで E 上の 2 点の和が定義できたが，それが加法群の条件 (1)〜(4) を満たすことを確かめなくてはならない．(2), (3), (4) は容易であるが，(1) については，射影幾何についてさらに多少の準備が必要となる．ここではそれを省略するので，興味ある人は参考文献を参照されたい．

これで二次曲線や実数体上の楕円曲線に，加法を導入することができたが，定義するだけでは何も面白いことは出てこない．楕円曲線や二次曲線の理論が数論や暗号理論などに応用できる理由は，この加法が点の座標によって代数的に書き表せることにある．

そこで E 上の $P=(x_1,y_1), Q=(x_2,y_2)$ の和 $P+Q$ の座標 (x_3,y_3) を x_1,y_1,x_2,y_2 を用いて表してみよう．まず $P\neq Q$ とする．$x_1=x_2$ のときは $P=-Q$ となるしかない．よってこのときは $P+Q=O$ である．$x_1\neq x_2$ としよう．このとき，直線 $l_{P,Q}$ の方程式は

$$y=\frac{y_2-y_1}{x_2-x_1}(x-x_1)+y_1$$

である．これを $y^2=x^3+ax+b$ に代入して，x の 3 次方程式が得られるが，その解が x_1,x_2,x_3 であるから，解と係数の関係により，

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2 \tag{19}$$

を得る．$(x_3,-y_3)$ は直線 $l_{P,Q}$ 上にあるから，

$$y_3=\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)-y_1 \tag{20}$$

である．$P=Q$ の場合は，P での接線 l_P は (16) で与えられているから，それを $y^2=x^3+ax+b$ に代入して x の 3 次方程式を得る．これは x_1 を重根に持ち，残り一つの解が x_3 だから解と係数の関係を用いれば，

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1 \tag{21}$$

を得る．$(x_3,-y_3)$ は直線 l_P 上にあるから，

$$y_3=\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3)-y_1 \tag{22}$$

さて，一旦 (19), (20), (21), (22) のように，楕円曲線上の加法が座標を用いて表されれば，体 K を $\mathbb{R}$ としなくても，一般の体で E 上の加法を定義できる．その定義の詳細は読者に任せよう．また，そうして定義したものが加法群の条件を満たしていることも確認しなくてはならないが，それについても参考文献を参照されたい．

例 6.2 (複素数体上の楕円曲線)**.** 複素数体上の楕円曲線は，大変重要なものであるが，ここでは詳しく扱うことができない．この場合は，E は $\mathbb{C}^2$ の中の曲面となる．それは，浮き輪の表面の形をしている．円の上の加法は円を回転させることで視覚化することができるが，楕円曲線の場合も浮き輪 2 方向の回転により，その加法をみることができる．また，円の上の関数が三角関数として重要であるのと同様に，複素数体上の楕円曲線上の関数にもテータ関数と呼ばれる二重周期関数があり，数学の多くの分野で重要な役割を担っている．

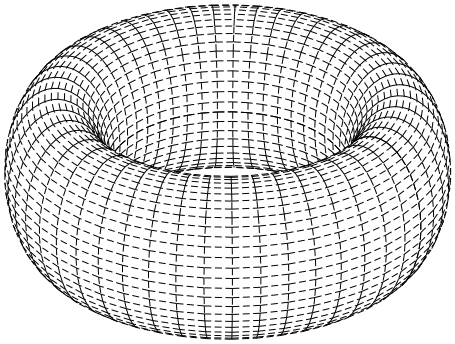


図 3　複素数体上の楕円曲線

6.2　楕円曲線の群構造

体 K 上の楕円曲線 E は，式 $y^2 = f(x) = x^3 + ax + b$ で定義されていた．従って，K が別の体 L に含まれていれば，同じ式で定義される L 上の楕円曲線を考えることができる．そこで，このようなときは K 上のものを $E(K)$，L 上のものを $E(L)$ で表すことにする．このとき

$$E(K) = \{(x, y) \in K^2 \mid y^2 = f(x)\} \cup \{O\} \subseteq E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{O\}$$

と $E(K)$ は $E(L)$ の部分集合となっているだけではなく，$E(K)$ は $E(L)$ の部分群になっている．すなわち $E(L)$ の加法を $E(K)$ に制限したものが，$E(K)$ の加法でもある．これらの群の構造は K によって，かなり異なったものになっている．楕円曲線のみならず，前節で定義した，直線や二次曲線も含めて群構造を比較しよう．

群の構造について述べるために，幾つか群論の用語を導入しよう．群といっても加法群しか扱わないので，加法群に限定する．まず，比較のために，群の同型の定義をしておこう．

定義 6.1. 二つの群 G_1 と G_2 が同型とは，全単射 $f : G_1 \to G_2$ で．和，差を保つものが存在することである．

同型な群は，群として同じものとみなされる

定義 6.2. 二つの加法群 G_1 と G_2 の直和とは，G_1 の元 P と G_2 の元 Q の対 (P, Q) 全体の集合 $G_1 \times G_2$ に，

$$(P, Q) + (P', Q') = (P + P', Q + Q')$$

によって加法を定めた加法群である．

$K=\mathbb{R}$ の場合は，曲線の群は幾何学的にみることができる．例 6.1 の (i) は数直線 $\mathbb{R}$, (ii) は 数直線から 1 点 0 を除いたものを積を群としてみたものである．この群は正の部分 $\mathbb{R}_+$ と負の部分 $\mathbb{R}_-$ に分かれていて，$\mathbb{R}_+$ の方は部分群になっている．この $\mathbb{R}_+$ は指数関数によって $\mathbb{R}$ と同型である．

$$f:\mathbb{R}\to\mathbb{R}_+ \qquad f(x)=e^x$$

$\mathbb{R}-\{0\}$ は $\mathbb{R}_+$ と部分群 $\{-1,1\}$ の直和と同型である．円は直線とは同型でない群である．円上の加法は回転とみなすことができる．ここで証明することは出来ないが，楕円は群として円と同型である．放物線は直線と，双曲線は $\mathbb{R}-\{0\}$ と同型である．楕円曲線は $x^3+ax+b=0$ が異なる 3 実解を持つ場合，円と $\{-1,1\}$ の群の直和と同型である．$x^3+ax+b=0$ がただ一つの実解を持つ場合は円と同型である．また，$K=\mathbb{C}$ 複素数体で考えた場合，楕円曲線は二つの円群の直和と同型である．このように，$K=\mathbb{R}$ または $\mathbb{C}$ で考えると，楕円曲線と二次曲線の間にはあまり大きな違いは見られない．ところが $K=\mathbb{Q}$ とすると，様子は大きく変わってくる．そして素数の性質が顔を見せてくるのである．実際に，楕円曲線は素数についてのすべてを ” 知っている ” とも思えるのである．

まず，直線の有理点の集合は $\mathbb{Q}$ である．$\mathbb{R}-\{0\}$ の有理点は $\mathbb{Q}-\{0\}$ であるが，これは素因数分解の一意性から無限個の $\mathbb{Z}$ と同型な群の直和と $\{-1,1\}$ の直和に同型である．半径 1 の円の有理点の集合はピタゴラス三角形の理論を記述する．実際，円の有理点と固有なピタゴラス三角形は ±1 倍を無視すれば，完全に対応するといってもよい．この場合も群構造は $\mathbb{Q}-\{0\}$ と似ており，有限群と無限個の $\mathbb{Z}$ と同型な群との直和と同型となっている．

ところが，楕円曲線の場合は様子がかなり違ってきて，有限性が出てくるのである．

定義 6.3. 加法群 G の元 P の位数とは，$nP=O$ となる自然数 n の最小値である．どの自然数 n に対しても $nP\neq O$ となるとき，P の位数は無限であるという．また，位数有限の元をねじれ元ともいう．

二つのねじれ元 P,Q の和はまたねじれ元である．実際，$nP=O, mQ=O$ ならば $(nm)(P+Q)=O$ であるから．

このことは加法群 G のねじれ元全体の部分集合 G_{tors} が部分群となることを意味する．この部分群 G_{tors} を G のねじれ部分群という．

定理 6.2 (モーデルの定理)**.** 有理数体上の楕円曲線 $E(\mathbb{Q})$ は有限生成な群である．こ

れは，次のことを意味する．$E(\mathbb{Q})_{\mathrm{tors}}$ は有限群であり，さらに $E(\mathbb{Q})$ に有限個の元 $P_1, \ldots, P_r$ があって，$E(\mathbb{Q})$ の任意の元は

$$P + n_1 P_1 + \cdots n_r P_r \qquad (P \in E(\mathbb{Q})_{\mathrm{tors}},\ n_1, \ldots, n_r \in \mathbb{Z})$$

の形にただ一通りに書ける．

定義 6.4. モーデルの定理の r を楕円曲線 $E(\mathbb{Q})$ の階数という．

階数が 0 ということと，$E(\mathbb{Q})$ が有限群であることは同値である．楕円曲線の群構造は，数論に豊かな応用を持つが，その例として，この階数を調べることによって解ける数論の問題を最後の節で扱う．

楕円曲線の有理点のなす群は大変豊かな構造を持っており，数学的にとても面白い対象であるといえる．では，もっと次数の高い曲線の有理点の集合を考えれば，もっといろいろなことがわかるのではないかと想像するだろう．しかし，フェルマー予想（ワイルズの定理）でもそうであるが，次数の高い曲線にはほとんど有理点はないのである．実際，モーデルによって予想され 1983 年にファルティングスによって証明された次の定理が成り立つ．

定理 6.3 (ファルティングス)**.** 種数 2 以上の代数曲線は，有限個の有理点しか持たない．

代数曲線の方程式を複素数の範囲で解き，その解のなす曲面をみたとき，それは何人か用の浮き輪のような形になる．その浮き輪が g 人用の形をしているとき，種数 g の曲線という．楕円曲線は種数 1 の曲線であり，次数が 4 以上の曲線の種数は 2 以上なのである．

ファルティングスは 24 歳のとき，大変困難だと見られていたモーデル予想を解き，フィールズ賞を受賞した．

6.3 有限体

楕円曲線を暗号に応用するには，体 K をより計算機で扱いやすいものにする必要がある．体 K に有限個しか元がないものにするのである．そのような体があるのかというと，簡単に見つかる．

例 6.3. ”偶数 + 偶数 = 偶数，奇数 × 奇数 = 奇数 ” などのように，偶数，奇数という言葉（概念）をあたかも数のように扱って演算を考えることは，よくなされていることであろう．言葉のままだと気持ち悪いので，偶数を代表する数として，0，奇数を代表する

数を 1 として，それらの式を書き下してみれば，

$$0+0=0,\ 0+1=1+0=1,\ 1+1=0,\ 0\times 0=0\times 1=1\times 0=1,\ 1\times 1=1$$

となる．$K=\{0,1\}$ に，このようにして $+,\times$ を導入すれば，体となる．これは 2 個の元からなる体として $\mathbb{F}_2$ と書かれる．

定義 6.5. 体 K の元の個数が有限であるとき，K を有限体という．その元の個数が q である体を $\mathbb{F}_q$ で表す．q をその体の位数という．

実は同じ有限位数を持つ体はすべて同型（体として構造が同じということ）であり，しかも体 K の中に K_1, K_2 と二つの体が含まれていて，K_1 と K_2 の位数が同じ q のときには，$K_1=K_2$ でなければならないことが知られている．実際，

$$K_1=K_2=\{x \mid x\in K, x^q=x\}$$

となるのである．このため，同じ位数の体を $\mathbb{F}_q$ と一つの記号で書いても混乱は起こらないのである．

例 6.4. p を素数とする．$K=\{\overline{0},\overline{1},\dots,\overline{p-1}\}$ の 2 元に和，積を次の方法で定める．

$$\overline{m}+\overline{n}=\overline{m+n\text{ を }p\text{ で割った余り}},\quad \overline{m}\,\overline{n}=\overline{mn\text{ を }p\text{ で割った余り}}.$$

ただし，p で割った余りは $0,1,\dots,p-1$ から選ぶものとする．このように定義した演算で，加法，乗法が通常の演算と同様な法則を満たすことは容易に確かめられる．$\overline{0}$ が通常の 0 の役割を果たし，$\overline{1}$ が 1 の役割を果たす．また，$\overline{n}+\overline{p-n}=\overline{0}$ であり，$\overline{p-n}$ は $-\overline{n}$ の役割を果たす．このように K は，加減乗の 3 演算を持つ ” 環 ” である．さらに p が素数であることから，割り算もできることが次のようにわかる．というのは $\overline{n}\neq\overline{0}$ のとき，

$$\overline{n}\overline{i}=\overline{n}\overline{j}\qquad (0\le i,j\le p-1)$$

ならば，$ni-nj=n(i-j)$ が p で割れなければならないが，$p\neq n$ だから $p\mid i-j$，よって $\overline{i}=\overline{j}$ となるからである．特に，

$$\overline{n}\overline{0},\ \overline{n}\overline{1},\ \dots,\overline{n}\overline{p-1} \tag{23}$$

はすべて異なる．これは K における一次方程式

$$\overline{n}X=\overline{m}$$

が K の中にただ一つ解を持つことを意味する．よって K は体である．上の記号を使えば $K=\mathbb{F}_p$ である．

どのような有限体 K にも必ずある素数 p があって K は $\mathbb{F}_p$ を含む．このような素数 p を体 K の標数という．これを示そう．K には（体の定義から）1 は必ずある．K において 1 を n 個（n は自然数）足したものを $\overline{n}$ と書くことにする．

$$\overline{1}, \overline{2}, \overline{3}, \ldots$$

と K の元の列を考えれば，K には有限個しか元がないのだから必ずどこかに同じ元がでてくる．$\overline{n} = \overline{m}$ $(n < m)$ とすれば，$\overline{m-n} = 0$ $(m-n > 0)$ となる．p を $\overline{p} = 0$ となる最小の自然数とすれば p は素数である．なぜならば $p = nm$ $(1 < n, m < p)$ とすると，$\overline{n}\,\overline{m} = 0, \overline{n} \neq 0, \overline{m} \neq 0$ となり，K が体であることに反するからである．

体 K の部分集合 L が K の演算で体になっているとき，L を部分体という．これは $L \ni 1$ で，$L \ni a, b$ $(a \neq 0)$ のとき，$a \pm b, ab, b/a \in L$ を満たすことと同じである．以後，L が K の部分体であることを単に $L \subseteq K$ で表す．

次の証明もそれほど難しくはないが，ここでは省略する．

命題 6.4. K を位数 q の有限体とすると，q は体 K の標数 p のベキ p^n である．よって $K = \mathbb{F}_{p^n}$ と表せる．さらに $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$ が成り立つ．

例 6.5. $\mathbb{F}_3$ においては $-\overline{1} = \overline{2}$ である．$\mathbb{F}_3$ のどの元の 2 乗も $-\overline{1}$ ではない．実際，$\overline{0}^2 = \overline{0}, \overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{1}$．そこで，実数の中に 2 乗して -1 になる数，すなわち $\sqrt{-1}$ が無かったから，無理矢理 $\sqrt{-1}$ を作って，複素数を定義したように，この場合も $\sqrt{-\overline{1}}$ を作れば，

$$a + b\sqrt{-\overline{1}} \qquad a, b \in \mathbb{F}_3$$

の全体 K は体となる．K の元の個数は a, b が独立に $\mathbb{F}_3$ の中を動くので 9 である．すなわち，$K = \mathbb{F}_9 = \mathbb{F}_{3^2}$．このような方法を一般化して，すべての素数 p とすべての自然数 n に対して，体 $\mathbb{F}_{p^n}$ が存在することを証明できる．

6.4 有限体上の楕円曲線

楕円曲線を定義する際，K の標数から 2, 3 を除外した．それは K の標数が 2, 3 の場合，楕円曲線の方程式が少し複雑なものになるので，簡単のため除外したにすぎず，実は標数に依らずに楕円曲線は定義できるものである．特に標数 2 のものは計算機に応用する場合効率がよく欠かせることができない．

楕円曲線 E が有限体 $\mathbb{F}_q$ で定義されているとする．これは楕円曲線を定義する式の係数が $\mathbb{F}_q$ に属しているということを意味する．K の標数が 2 または 3 のときは，これまでの式と違う式を考えれば除外しなくてよい．

E が $\mathbb{F}_q$ で定義されれば，$\mathbb{F}_{q^r}$ ででも定義できる．

$$N_r := \#E(\mathbb{F}_{q^r})$$

とおく．$\#$ はそれに続く集合の元の個数を表す記号である．この N_r から ”母級数 ” $Z(E/\mathbb{F}_q;T)$ を作る．

$$Z(E/\mathbb{F}_q;T) := e^{\sum N_r T^r/r}$$

これは T に関する形式的ベキ級数で，E の合同ゼータ関数と呼ばれるものである．

これに関して次の定理は大変重要である．

定理 6.5 (ハッセ)**.** 楕円曲線の合同ゼータ関数は，次の形の t の有理関数である．

$$Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

ここで $a = q+1-N_1$ である．分子の二次多項式は負または 0 の判別式 a^2-4q を持ち，その根を $\alpha, \overline{\alpha}$ とすると，

$$N_r = q^r + 1 - \alpha^r - \overline{\alpha}^r$$

である．特に N_r は N_1 から求めることができる．

系 6.6. $\mathbb{F}_q$ 上定義された楕円曲線 E に対して，

$$q+1-2\sqrt{q} \leq N_1 \leq q+1+2\sqrt{q}$$

が成り立つ．

6.5 楕円曲線暗号

楕円曲線暗号系は１９８５年にコブリッツとミラーによって独立に提案された．フェルマの小定理を用いる暗号系では，群は $\mathbb{F}_q$ の乗法群のみで，選択肢が少ないが，楕円曲線暗号系では，いろいろな楕円曲線を選べるという利点がある．

ここでは ElGamal 暗号の類似の方法を紹介する．まず，暗号化したい文を適当な長さの数に直し，それを適当な楕円曲線の有理点と対応づけなくてはならない．

すでに送りたいメッセージが数 m に置き換えられているとする．この m から楕円曲線の点を作る．これには確率的な方法を用いる．有限体 $\mathbb{F}_q$ $(q = p^r)$ をとる．q は大きな奇数となるようにする．k を確率 $1/2^k$ が十分小さくなるように大きくとる．これには $k = 50$ で十分である．m は $0 \leq m \leq M$ の範囲にあるとする．$q > Mk$ となるように選ばれているとする．1 から Mk までの数 i それぞれに対して $\mathbb{F}_q$ の異なる元 $\varphi(i)$ を対応させる．このとき $\varphi(i)$ から i がすぐに求まるような対応にしておかねばならない．

まず $mk+1$ に対応する $\mathbb{F}_q \ni x = \varphi(mk+1)$ を求め，

$$y^2 = x^3 + ax + b$$

の右辺を計算する．計算した右辺の平方根があるかどうかを試す．もし $y \in \mathbb{F}_q$ が見つかれば，$P_m = (x, y)$ とする．見つからなければ x を $\varphi(mk+2)$ として，再度右辺の平方根があるかどうかを試す．平方根があるかどうかの確率は約５０％であることが知られている．よって，この試みが k 回連続失敗する確率は $1/2^k$ である．今 $1/2^k$ は十分小さいとしているから，k 回までには，成功すると仮定しよう．何回かの失敗の後に得られた点 $P_m = (x, y)$ から，もとの m を得るには，$[\widetilde{x} - 1/k]$ を計算すればよい．ここで $\widetilde{x}$ は $\varphi(\widetilde{x}) = x$ となる整数である．

これで，送りたいメッセージを楕円曲線の点として表現する方法がわかった．

A さんが B さんに m という数字を暗号化して送りたいとしよう．

(1) B さんは $\mathbf{F}_q$ 上の楕円曲線 E と，その上の点 B を選ぶ．更に整数 r を選び $(\mathbf{F}_q, E, B, rB)$ を公開する．(r は秘密．)

(2) A さんは m から上記の方法で P_m を作り，整数 k を適当に選び，B さんに $(kB, P_m + k(rB))$ を伝える．

(3) B さんは

$$(P_m + k(rB)) - r(kB) = P_m$$

より，P_m を得る．これより B さんは m を求めることができる．

この方法は，rB と B がわかっていても，容易には r を求めることが出来ないという事実に基づいている．

7　合同数と楕円曲線

ディオフォントスの「算術」の第６巻のバシェの注釈に次の問題が載っている．

与えられた数に等しい面積を持つ直角三角形を求めよ.

フェルマーはこの注釈に対して，平方数を面積に持つピタゴラス三角形が存在しないことを証明し，その概略を書き残している．ではどういう数がピタゴラス三角形の面積となりうるのか，本説ではこの問題を考察し，それが楕円曲線の有理点に関する性質から効果的に解決されることを見る.

7.1 合同数

三辺の長さが有理数であるような直角三角形の面積となっているような有理数を**合同数**という．例えば，三辺が 3, 4, 5 のピタゴラス三角形の面積

$$6 = \frac{3 \times 4}{2}$$

は合同数である．もっと一般に三辺 $2mn,\ m^2 - n^2,\ m^2 + n^2$ を持つ三角形は，直角三角形だから,

$$C(m, n) := mn(m^2 - n^2) = mn(m - n)(m + n)$$

は合同数である．$m,\ n$ に小さい値を入れてみると,

$$6,\ 30,\ 60,\ 84,\ 180,\ 210,\ 330,\ 486,\ 504,\ 546,\ 630,\ 924,\ 1320,\ \ldots \qquad (24)$$

などが合同数であることがわかる.

正の有理数 r が合同数ならば，$x^2 + y^2 = z^2$ を満たす正の有理数 x, y, z があって $r = \dfrac{xy}{2}$ と表せる．このとき任意の正の有理数 s に対して三辺 sx, sy, sz を持つ直角三角形を考えれば $s^2 r$ が合同数となることがわかる．また $s^2 r$ が合同数なら r も合同数となる.

$$r = p_1^{n_1} \cdots p_l^{n_l} \qquad (n_1, \ldots, n_l \in \mathbb{Z})$$

を r の素因数分解としたとき，$n_1, \ldots, n_i$ が奇数，$n_{i+1}, \ldots, n_l$ が偶数となるようにしておけば，$r = p_1 \cdots p_i s^2\ (s \in \mathbb{Q})$ とかける．このとき r が合同数であるためには $p_1 \cdots p_i$ が合同数であることが必要十分である．以後，r から平方因子を除いたものを $R(r)$ と書くことにする．すなわち,

$$R(r) := p_1 \cdots p_i$$

とおく．合同数を決定する問題は，平方因子を持たない自然数で合同数となっているものを決定することに帰着される．すなわち，平方因子を持たない合同数は $R(C(m, n))$ のリ

ストの中に必ず含まれる．上記の $C(m,n)$ のリスト (24) から作った $R(C(m,n))$ のリストを見ると，

$$6,\ 30,\ 15,\ 21,\ 5,\ 210,\ 330,\ 6,\ 14,\ 546,\ 70,\ 231,\ 330,\ \ldots$$

が合同数となることがわかる．また，平方因子を持たない合同数は，必ず適当な m,n によって $R(C(m,n))$ と表されるから，このリストのどこかには現れる筈である．しかし，このリストでは数字は大きさの順に並んでいるわけではなく，また同じ数字が繰り返し出て来ることもある．そのため具体的に平方因子を持たない数を与えても，それがこのリストにいつ現れるかはわからない．よって，その与えられた数が，合同数**でない**ことは，いつまでたっても判定できないことになる．例えば 157 は合同数であるが，157 を面積に持つ最も単純な有理直角三角形は，次の三辺を持つものである．これは D. Zagier の計算による．

$$x=\frac{6803298487826435051217540}{411340519227716149383203},\quad y=\frac{411340519227716149383203}{21666555693714761309610},$$

$$z=\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

命題 7.1. 自然数 n が合同数であるための必要十分条件は，有理数 x で

$$x-n,\qquad x,\qquad x+n$$

がすべて有理数の平方となるものが存在することである．

Proof. n が合同数のとき，$n=\dfrac{XY}{2}$，$X^2+Y^2=Z^2$ を満たす正の有理数 X,Y,Z がとれる．

$$\left(\frac{X\pm Y}{2}\right)^2=\frac{X^2\pm 2XY+Y^2}{4}=\left(\frac{Z}{2}\right)^2\pm n.$$

よって $x=\left(\dfrac{Z}{2}\right)^2$ とおけば，$x,\ x\pm n$ はすべて有理数の平方である．

逆に x を $x,\ x\pm n$ がすべて有理数の平方となるものとする．

$$X=\sqrt{x+n}-\sqrt{x-n},\quad Y=\sqrt{x+n}+\sqrt{x-n},\quad Z=2\sqrt{x}$$

とおけば X, Y, Z はすべて正の有理数であり，

$$X^2 + Y^2 = (\sqrt{x+n} - \sqrt{x-n})^2 + (\sqrt{x+n} + \sqrt{x-n})^2 = 2(x+n) + 2(x-n) = 4x = Z^2$$
$$\frac{XY}{2} = \frac{(\sqrt{x+n} - \sqrt{x-n})(\sqrt{x+n} + \sqrt{x-n})}{2} = \frac{(x+n) - (x-n)}{2} = n$$

よって n は合同数である． □

定理 7.2 (フェルマー)**.** 次の連立不定方程式は自然数解を持たない．

$$\begin{cases} X^2 + Y^2 &= U^2 \\ X^2 - Y^2 &= V^2 \end{cases} \tag{25}$$

特に 1 は合同数ではない．

Proof. 連立不定方程式 (25) が自然数解 $(X, Y, U, V) = (x, y, u, v)$ を持っているとし，矛盾を導く．任意の自然数解 $(X, Y, U, V) = (x, y, u, v)$ に対して，必ず別の自然数解 (x', y', u', v') で $x > x'$ となるものが存在することを示す．そうすれば自然数の無限減少列 $x > x' > \cdots$ が作れることになり，矛盾が生ずるのである．

x, y, u, v の最大公約数 d が 1 でない場合，$(\frac{x}{d}, \frac{y}{d}, \frac{u}{d}, \frac{v}{d})$ も解になるから，この場合はよい．

$d = 1$ とする．(25) より x, y の最大公約数は u, v をも割り切らねばならないから，$d = 1$ のときは x と y も互いに素である．このとき x, u, v は奇数，y は偶数である．実際，y が奇数なら (25) の第一式より x は偶数である．ところがこのとき第二式から v^2 を 4 で割った余りは 3 でなければならない．平方数を 4 で割った余りは 0 か 1 なので，これはあり得ない．y が偶数なら x は奇数となるから，u, v も奇数となる．よって $\frac{u \pm v}{2}$ は整数となり，

$$\left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2 = \frac{u^2 + v^2}{2} = x^2 \tag{26}$$

が成り立つ．ここで $\frac{u+v}{2}$ と $\frac{u-v}{2}$ は互いに素である．実際，素数 p がこれら二数を割り切れば，その和と差である u, v も割り切る．よって (25) より $x^2 \pm y^2$，さらにその和と差の $2x^2, 2y^2$ も割り切る．u, v は奇数だから $p \neq 2$．よって p は x^2, y^2 を割り切る．これは x と y が互いに素だから不可能である．このとき定理 3.1 より，$a - b$ が正の奇数，$(a, b) = 1$ となる自然数 a, b で，

$$\{\frac{u+v}{2}, \frac{u-v}{2}\} = \{a^2 - b^2, 2ab\}, \qquad x = a^2 + b^2$$

を満たすものが存在する．よって

$$\left(\frac{y}{2}\right)^2 = \frac{u^2 - v^2}{8} = \frac{1}{2} \cdot \frac{u+v}{2} \cdot \frac{u-v}{2} = ab(a+b)(a-b)$$

となる．y は偶数であったから $\dfrac{y}{2}$ は整数である．また $a, b, a+b, a-b$ はどの二つをとっても互いに素である．実際，素数 $p \mid a+b, a-b$ とすると，$p \mid 2a, 2b$．$a-b$ は奇数だから $p \neq 2$．よって $p \mid a, b$．$(a,b) = 1$ であったから矛盾．他の場合は明らかである．よって両辺の素因数分解を考えれば $a, b, a+b, a-b$ はどれも平方数でなければならない．自然数 x', y', u', v' により，

$$a = x'^2, \quad b = y'^2, \quad a+b = u'^2, \quad a-b = v'^2$$

と表せば，x', y', u', v' は連立不定方程式 (25) の解である．さらに

$$x' \leq a \leq a^2 < a^2 + b^2 = x$$

だから，(x', y', u', v') が求める解である． □

系 7.3. 不定方程式 $X^4 - Y^4 = U^2$ は自然数解を持たない．よって，不定方程式 $X^4 + Y^4 = Z^4$ は非自明な整数解を持たない．

Proof. $X^4 - Y^4 = U^2$ が自然数解 $(X, Y, Z) = (x, y, z)$ を持っているとする．三辺 $x^4 - y^4, 2x^2y^2, x^4 + y^4$ を持つ直角三角形の面積は

$$x^2y^2(x^4 - y^4) = x^2y^2z^2$$

となる．これは 1 が合同数となることを意味し，上の定理に矛盾する． □

このように, 与えられた数が合同数でないことを示すのは大変難しい．1983 年, Tunnell は次の驚くべき定理を発見した.

定理 7.4 (Tunnell)**.** n を平方因子を持たないとする．n が奇数の合同数のとき，条件 (i) が成り立つ．n が偶数の合同数のとき，条件 (ii) が成り立つ.

(i) $2x^2 + y^2 + 8z^2 = n$ を満たす $(x, y, z) \in \mathbb{Z}^3$ の数は $2x^2 + y^2 + 32z^2 = n$ を満たす $(x, y, z) \in \mathbb{Z}^3$ の数の 2 倍である.

(ii) $8x^2 + 2y^2 + 16z^2 = n$ を満たす $(x, y, z) \in \mathbb{Z}^3$ の数は $8x^2 + 2y^2 + 64z^2 = n$ を満たす $(x, y, z) \in \mathbb{Z}^3$ の数の 2 倍である.

また，もし楕円曲線 $E_n : y^2 = x^3 - n^2x$ に関する Birch-Swinnerton-Dyer 予想の弱形（以後，このノートでは弱 BSD 予想という）が正しければ，この逆が成り立つ．

Birch-Swinnerton-Dyer 予想については，次節で述べる．この定理により，与えられた n が合同数**でない**ことが有限回の簡単な計算で確かめられる．例えば，上記の $n = 1$ の場合，$2x^2 + y^2 + 8z^2 = 1$ の整数解は $(0, \pm 1, 0)$ の二つで，$2x^2 + y^2 + 32z^2 = 1$ の整数解も $(0, \pm 1, 0)$ の二つであるから，1 が合同数でないことがわかる．

例 7.1. 10 以下の自然数 n について，Tunnell の条件 (i)，(ii) が成り立つかどうか確かめ，合同数かどうかをみてみよう．

($n = 2$) $8x^2 + 2y^2 + 16z^2 = 2$ なら $z = 0$ で $8x^2 + 2y^2 + 64z^2 = n$ でも $z = 0$ だから，両者の整数解は同じである．また少なくとも一つの整数解を持っているので (ii) は成り立たない．よって 2 は合同数ではない．

($n = 3$) $2x^2 + y^2 + 8z^2 = 3$ なら $z = 0$ で $2x^2 + y^2 + 32z^2 = 3$ でも $z = 0$ だから，両者の整数解は同じである．また，少なくとも一つの整数解を持っているので (i) は成り立たない．よって 3 は合同数ではない．

($n = 4$) 4 は 1 が合同数でないから，合同数でない．

($n = 5$) $2x^2 + y^2 + 8z^2 = 5$ も $2x^2 + y^2 + 32z^2 = 5$ も整数解を持たない．よって (i) が成り立つ．弱 BSD 予想が正しければ，このことから 5 が合同数だとわかる．実際に，5 は三辺が $\dfrac{20}{3}, \dfrac{3}{2}, \dfrac{41}{6}$ の直角三角形の面積である．

$$\left(\frac{20}{3}\right)^2 + \left(\frac{3}{2}\right)^2 = \frac{1600 + 81}{36} = \left(\frac{41}{6}\right)^2, \qquad \frac{1}{2} \cdot \frac{20}{3} \cdot \frac{3}{2} = 5$$

($n = 6$) 6 が合同数であることは既にみたが，$8x^2 + 2y^2 + 16z^2 = 6$ も $8x^2 + 2y^2 + 64z^2 = 6$ も整数解を持たない．よって条件 (ii) が成り立つ．

($n = 7$) $2x^2 + y^2 + 8z^2 = 7$ も $2x^2 + y^2 + 32z^2 = 7$ も整数解を持たない．よって条件 (i) が成り立つ．実際に，7 は三辺が $\dfrac{24}{5}, \dfrac{35}{12}, \dfrac{337}{60}$ の直角三角形の面積である．

$$\left(\frac{24}{5}\right)^2 + \left(\frac{35}{12}\right)^2 = \frac{82944 + 30625}{3600} = \left(\frac{337}{60}\right)^2, \qquad \frac{1}{2} \cdot \frac{24}{5} \cdot \frac{35}{12} = 7$$

($n = 8, 9$) $8, 9$ は $2, 1$ が合同数でないから，合同数ではない．

$(n = 10)$ $8x^2 + 2y^2 + 16z^2 = 10$ でも $8x^2 + 2y^2 + 64z^2 = 10$ でも $z = 0$ となる．また少なくとも一つの整数解を持っているので (ii) は成り立たない．よって 10 は合同数でない．

7.2 合同数と楕円曲線 E_n の有理点

n が合同数であるための条件はある楕円曲線の有理点の条件として次のように言い直せる．

命題 7.5. n を平方因子を持たない自然数とする．n が合同数であるための必要十分条件は，$Y^2 = X^3 - n^2X$ が $(X, Y) = (0, 0), (\pm n, 0)$ 以外の有理数解を持つことである．

Proof. n が合同数のとき，正の有理数 a, b, c で $a^2 + b^2 = c^2$, $n = \dfrac{ab}{2}$ を満たすものをとると，

$$\left(\frac{a \pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n$$

である．よって

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2.$$

この両辺に $\left(\dfrac{c}{2}\right)^2$ を掛けて，$x = \left(\dfrac{c}{2}\right)^2, y = \dfrac{a^2 - b^2}{4} \cdot \dfrac{c}{2}$ とおけば，$y^2 = x^3 - n^2x$ となる．$a, b, c > 0$ だから $y = 0$ ならば $a = b$ であるが，このときは $n = \left(\dfrac{c}{2}\right)^2$ が合同数ということになり，フェルマの定理 7.2 に反する．これで (x, y) が求める有理数解であることがわかった．

逆に，$Y^2 = X^3 - n^2X$ が $(X, Y) = (0, 0), (\pm n, 0)$ 以外の有理数解 $P = (x, y)$ を持つとする．$y = 0$ ならば，x は $0, \pm n$ のどれかでなくてはならないので，$y \neq 0$ である．さ

て前節の楕円曲線の点の加法により，$P+P$ を求め，その座標を (a,b) とする．このとき

$$\begin{aligned} a &= \left(\frac{3x^2-n^2}{2y}\right)^2 - 2x = \frac{9x^2-6x^2n^2+n^4-8xy^2}{(2y)^2} \\ &= \frac{9x^4-6x^2n^2+n^4-8x(x^3-n^2x)}{(2y)^2} = \frac{x^4+2x^2n^2+n^4}{(2y)^2} = \left(\frac{x^2+n^2}{2y}\right)^2 \\ a \pm n &= \left(\frac{x^2+n^2}{2y}\right)^2 \pm n = \frac{9x^2-6n^2x^2+n^4-8xy^2}{(2y)^2} \\ &= \frac{x^4+2n^2x^2+n^4 \pm 4n(x^3-n^2x)}{(2y)^2} = \left(\frac{x^2-n^2 \pm 2nx}{2y}\right)^2 \end{aligned}$$

となるから，命題 7.1 により n は合同数である． □

この命題の条件のままでは，合同数の存在の判定を与える Tunnell の美しい結果には結びつかなかったであろう．それを可能にしたのは，この有理点の存在が楕円曲線の群の構造に関しての重要な性質を記述するものだったことである．

ここでは証明できないが，有理数体上の楕円曲線 $E_n(\mathbb{Q})$ のねじれ部分群は

命題 7.6. $E_n(\mathbb{Q})_{\mathrm{tors}} = \{O,(0,0),(n,0),(-n,0)\}$ である．

証明については，[6] 1 章 §9 命題 17 参照．従って，

命題 7.7. n を平方因子を持たない自然数とする．n が合同数であるための必要十分条件は，楕円曲線 $E_n(\mathbb{Q})$ が無限群，すなわちその階数が正となることである．

1977 年 コーツとワイルズは次の定理を証明した．

定理 7.8. E が $\mathbb{Q}$ 上の楕円曲線で虚数乗法をもつとき，もし E が無限に多くの有理点を持てば，$L(E,1)=0$ である．

ここで $L(E,s)$ は E の L-関数と呼ばれる複素関数である．虚数乗法については，ここでは定義しないが，我々の興味の対象である楕円曲線 E_n は虚数乗法を持つことがわかる．よって，コーツとワイルズの定理の系として次が得られる．

系 7.9. n を平方因子を持たない自然数とする．n が合同数ならば $L(E_n,1)=0$ である．

Birch, Swinnerton-Dyer 予想は，簡単に言えば L-関数 $L(E,s)$ の $s=1$ における様子が $E(\mathbb{Q})$ の階数を記述しているというものである．その特別な場合として，弱 Birch, Swinnerton-Dyer 予想とは，$L(E,1)=0$ ならば $E(\mathbb{Q})$ の階数が正，すなわち $E(\mathbb{Q})$ が無

限群となることを主張するものである．従って，弱 BSD 予想が正しければ，$L(E,1)=0$ から n が合同数であることがわかる．

Tunnell は $L(E,1)=0$ となるための条件を求め，定理 7.4 を得たのである．

付録 A　群，環，体の定義

数学の研究対象となるもの（例えば，数，関数，図形など）の中で，重要なもの，美しいもの，面白いもの，不思議な性質を持つものには，対称性 (ここで対称性とは，ある種の変換に関する不変性という意味で使っている) が隠れている場合が多い．例えば，三角関数の周期性，円や球の回転に関する対称性，正多角形，正多面体もその角数や，面の数に応じた回転に関する対称性を持っているし，直線や，平面も平行移動に関して不変という性質を持っている．整数も数直線の中の図形と見ると，自然数の長さ分の右，または左への平行移動で不変という性質を持っているし，複素数の共役も対称性と見ることができるだろう．

群とはこの対称性を記述するものである．一つの数学的対象を不変にする変換全体の集合を，この数学的対象の変換群という．変換群は単に集合というだけでなく構造を持っている．すなわち，一つの変換 f を施した後，別の変換 g を施すとこれを合わせた変換となる．これを変換の合成といい，$g\circ f$ や gf などで表す．変換の種類によっては $g+f$ や $g\times f$ などと書かれることもある．このように，何か集合 A の二元 a,b に対して，別の A の元 c を与える対応が定まっているとき，その対応を A の上の（二項）演算という．良く知っている例としては，二つの実数の加法や乗法，行列の和や積などがあげられる．

集合 A の上に二項演算を定めることは，写像 $m:A\times A\to A$ を与えることと同じである．以下では簡単のため $m(g,h)$ を単に gh，$m(m(g,h),k)$ を $(gh)k$ などと書き表す．

定義 付録 A.1 (群)**.** 集合 G に二項演算 $m:G\times G\to G$ が与えられていて，以下の条件を満たすとき，この集合 G は m に関して群をなすという．(通常，このことを G は群をなすと略していうことが多いが，どの二項演算に関して群をなすのかが指定されていないと意味がないので注意されたい．)

(1) 任意の $g,h,k\in G$ に対して $(gh)k=g(hk)$ が成り立つ．
(2) ある元 $e\in G$ があって，すべての $g\in G$ に対して $ge=eg=g$ が成り立つ．
(3) 各 $g\in G$ に対して，$gh=hg=e$ となる元 $h\in G$ が存在する．

(2) の元 e をこの群の単位元と呼ぶ．単位元はただ一つに定まることは容易に示される．

また，(3) の元 h を g の逆元といい，通常 g^{-1} で表す．この逆元も g によってただ一つに定まる．さらに，条件

(4) 任意の $g, h \in G$ に対して $gh = hg$ が成り立つ．

が満たされるとき，G は可換群をなすという．

G が演算 m に関して可換群をなすとき，$m(g, h)$ を gh と書く代わりに，$g + h$ と書くこともある．この時は，G は加法群をなすといい，単位元を 0 と書く．またこのとき g の逆元 g^{-1} を $-g$ と表す．

最初に述べた変換群は変換の合成を演算として群となる．実はどのような群もある種の変換群とみなすことができるから，変換群のことを群と考えることもできる．(厳密には区別すべきだが．)

先に，整数の例をあげたが，整数全体の集合 $\mathbb{Z}$ は二つの演算 $+$ と $\times$ を持っており，$+$ に関しては可換群をなしているが，$\times$ に関しては群をなさない．この二つの演算は分配法則で結びついている．

定義 付録 A.2 (環)**.** 集合 R に和と呼ばれる演算 $(x, y) \mapsto x + y$ と積と呼ばれる演算 $(x, y) \mapsto xy$ が定まっていて，以下の条件を満たすとき，R はこの二つの演算に関して可換環 (本講義では単に環) をなすという．通常略して，R は環であるという．

(1) R は加法に関して加法群をなす．
(2) 任意の $x, y, z \in R$ に対して結合法則 $(xy)z = x(yz)$ が成り立つ．
(3) 任意の $x, y, z \in R$ に対して分配法則 $(x + y)z = xz + yz, x(y + z) = xy + xz$ が成り立つ．
(4) 任意の $x, y \in R$ に対して $xy = yx$ が成り立つ．
(5) 1 と書かれる R の元があり，R のすべての元 x に対して $1x = x1 = x$ が成り立つ．

1 をこの環の単位元と呼ぶ．R の単位元であることを示すのに，1 を 1_R と書くこともある．

一般には，環の定義に (4)，(5) の公理は入れない．その場合，(4)，(5) の公理を入れたものを単位的可換環と呼ぶ．

整数全体の集合 $\mathbb{Z}$，有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$，複素数全体の集合 $\mathbb{C}$ は環になっているが，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は次の体と呼ばれるものにもなっている．

定義 付録 A.3 (体)**.** 環 R の 0（加法の単位元）でない全ての元 x に対して，$xy = 1$ を満たす $y \in R$ が存在するとき，R は（可換）体をなすという．この y を x^{-1} または $\dfrac{1}{x}$ で表す.

参考文献

[1] アンドレ・ヴェイユ, **数論 – 歴史からのアプローチ**, 日本評論社 (1987).

[2] 小野孝, **オイラーの主題による変奏曲**, 実教出版，(1980).

[3] 高木貞治, **初等整数論講義　第２版**, 共立出版，(1971).

[4] 中村幸四郎，寺阪英孝，伊東俊太郎，池田美恵 (訳・解説), **ユークリッド原論**, 共立出版，(1971).

[5] 小林昭七, **なっとくする オイラーとフェルマー**, 講談社, (2003).

[6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms, Second Editioin,* Springer，(1993).

[7] N. コブリッツ,(櫻井幸一 訳)，**数論アルゴリズムと楕円暗号理論入門**, シュプリンガー・フェアラーク東京，(1997).

[8] N. コブリッツ,(林 彬 訳)，**暗号の代数理論**, シュプリンガー・フェアラーク東京，(1999).

[9] J.H. シルヴァーマン，J. テイト，(足立恒雄，木田雅成，小松啓一，田谷久雄 訳)，**楕円曲線論入門**, シュプリンガー・フェアラーク東京，(1995).

[10] J.H. シルヴァーマン，(鈴木治郎 訳)，**はじめての数論**, ピアソン・エデュケーション，(2001).