直角三角形についての未解決問題

上越教育大学　中川　仁

平成16年7月2日

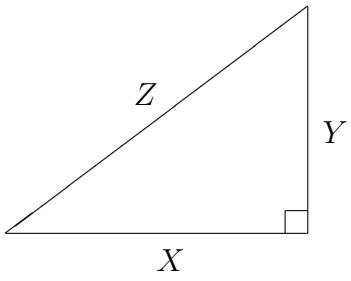
直角三角形に関する整数論の2つの問題から始めて，楕円曲線と呼ばれる曲線の整数論に至る話をします．楕円曲線は，現在最も盛んに研究されている整数論の対象であり，フェルマー予想の解決などにも使われ，いくつかの大きな未解決問題が残されているものです．

1　ピタゴラス数

3辺の長さが X, Y, Z の直角三角形は

$$X^2 + Y^2 = Z^2 \tag{1}$$

を満たす．等式 (1) を満たす自然数 X, Y, Z を**ピタゴラス数**と呼ぶ．最も簡単なピタゴラス数は $3, 4, 5$ である．$5, 12, 13$ もピタゴラス数である．これら以外にどんなピタゴラス数があるだろうか？



紀元前1900から1600年頃のものと推定されるバビロニアの粘土板には，15組からなるピタゴラス数の表が楔形文字で残されている．さらに，驚くべきことにバビロニア人はピタゴラス数を利用して原始的な**三角関数表**まで作っていた．

ユークリッドの原論には，ピタゴラス数をすべて与えるような公式が証明されている．最初に，この公式を証明しよう．

2つの整数 a, b について，a と b の最大公約数が1であるとき，a と b は**互いに素である**という．今，X, Y, Z がピタゴラス数であるとする．X, Y の最大公約数を d とす

れば，$X = dX_1, Y = dY_1, X_1, Y_1$ は自然数，とかける．そのとき，$d^2(X_1^2+Y_1^2) = Z^2$ より，

$$X_1^2 + Y_1^2 = \left(\frac{Z}{d}\right)^2$$

である．この左辺は整数であるから，$Z_1 = \dfrac{Z}{d}$ も整数である．$X_1^2 + Y_1^2 = Z_1^2$ であるから，X_1, Y_1, Z_1 もピタゴラス数であり，X_1 と Y_1 は互いに素である．そのとき，X_1 と Z_1 も互いに素であり，Y_1 と Z_1 も互いに素である．このようなピタゴラス数 X_1, Y_1, Z_1 を**原始的なピタゴラス数**という．$X = dX_1$, $Y = dY_1$, $Z = dZ_1$ であるから，一般のピタゴラス数は原始的なピタゴラス数を何倍かして得られることが示された．

はじめから，X, Y, Z を原始的なピタゴラス数とする．そのとき，X, Y ともに偶数となることはない．さらに，X, Y ともに奇数となることもない．実際，もし，そうだとすると，X^2, Y^2 ともに奇数であり，$Z^2 = X^2 + Y^2$ は偶数になる．したがって，Z も偶数である．そのとき，$X = 2X_1 + 1$, $Y = 2Y_1 + 1$, $Z = 2Z_1$, X_1, Y_1, Z_1 は整数，とかける．しかし，これらを (1) に代入すれば，

$$\begin{aligned} 4Z_1^2 &= (2X_1+1)^2 + (2Y_1+1)^2 \\ &= 4X_1^2 + 4X_1 + 1 + 4Y_1^2 + 4Y_1 + 1 \\ &= 4(X_1^2 + X_1 + Y_1^2 + Y_1) + 2. \end{aligned}$$

これから，2 が 4 の倍数となって矛盾である．ゆえに，X, Y ともに奇数となることもない．したがって，X, Y の一方は奇数で，もう一方は偶数である．そのとき，Z は奇数である．X が奇数で，Y が偶数であるとしても一般性を失わないので，そう仮定する．$\dfrac{X}{Z}, \dfrac{Y}{Z}$ は既約分数であり，

$$\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1$$

であるから，単位円

$$C:\ x^2 + y^2 = 1 \tag{2}$$

上の点で，x 座標と y 座標がともに有理数であるような点を求めればよい．そのような点を C 上の**有理点**という．これは次のようにして求められる．C 上の有理点 P と点 $A(-1, 0)$ を結ぶ直線 ℓ の傾きを t とすれば，t は有理数であり，直線 ℓ の方程式は，

$$\ell:\ y = t(x+1) \tag{3}$$

である．

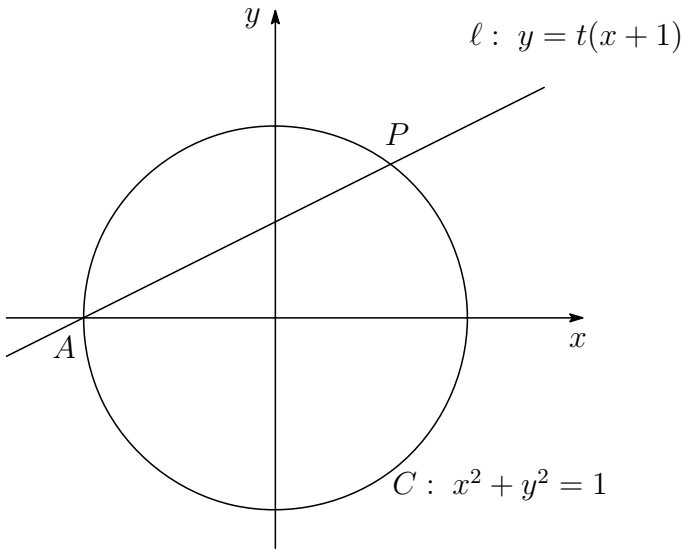


図 1: 単位円のパラメータ表示

直線 ℓ と単位円 C の交点は A と P であるから (図 1)，P の x 座標は，(2) に (3) を代入して得られる x の 2 次方程式

$$\begin{aligned} &x^2 + t^2(x+1)^2 = 1, \\ &x^2 + t^2(x^2 + 2x + 1) - 1 = 0, \\ &(1+t^2)x^2 + 2t^2 x + t^2 - 1 = 0 \end{aligned}$$

の -1 でない方の解である．これは，$x = -1$ を解として持つから，$(x+1)$ で因数分解できるはずである．割り算を実行すれば，

$$(x+1)\left\{(1+t^2)x + t^2 - 1\right\} = 0.$$

これを解いて，

$$x = -1, \quad x = \frac{1-t^2}{1+t^2}$$

を得る．P の y 座標は，(3) に $x = \dfrac{1-t^2}{1+t^2}$ を代入して，

$$y = t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}$$

である．このようにして，単位円 C 上の有理点は，有理数 t を用いて，

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \tag{4}$$

と表せる．ただし，$A(-1,0)$ は除かれる．このことから，有理数 t を用いて，

$$\frac{X}{Z}=\frac{1-t^2}{1+t^2},\quad \frac{Y}{Z}=\frac{2t}{1+t^2}$$

と表せる．$X,Y,Z>0$ より，$0<t<1$ である．$t=\dfrac{b}{a}$ と既約分数の形にかく．a,b は整数，$a>b>0$，a と b は互いに素である．そのとき，

$$\frac{X}{Z}=\frac{a^2-b^2}{a^2+b^2},\quad \frac{Y}{Z}=\frac{2ab}{a^2+b^2}$$

である．$\dfrac{X}{Z}$ は既約分数であるから，自然数 k を用いて，$a^2-b^2=kX$, $a^2+b^2=kZ$ と表せる．そのとき，$2ab=kY$ である．

$$\begin{aligned} 2a^2 &= (a^2+b^2)+(a^2-b^2)=k(Z+X),\\ 2b^2 &= (a^2+b^2)-(a^2-b^2)=k(Z-X) \end{aligned}$$

であり，a と b は互いに素であるから，$k=1$ または $k=2$ である．もし，$k=2$ とすると，$a^2+b^2=2Z$ より，a,b ともに奇数でなければならない．しかし，そのとき，$Y=ab$ は奇数となって，仮定に矛盾する．ゆえに，$k=1$ でなければならない．したがって，$X=a^2-b^2$, $Y=2ab$, $Z=a^2+b^2$ である．X は奇数であるから，a, b の一方は奇数で，もう一方は偶数である．以上まとめると，

定理 1.1. 原始的なピタゴラス数 X,Y,Z は，X を奇数，Y を偶数とすれば，

$$X=a^2-b^2,\ Y=2ab,\ Z=a^2+b^2$$

と表せる．ここで，$a>b$ は互いに素な自然数で一方は奇数，もう一方は偶数である．

a,b にいろいろな値を代入することによって，原始的なピタゴラス数が次々に得られる (表 1).

定理 1.1 から，特に，

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

を満たす整数 X,Y,Z は無数に存在することがわかる．それでは，指数 2 をもっと大きな自然数にしたらどうなるだろうか？

17 世紀のフランスの数学者フェルマーは愛読書の余白に次の予想を書き残した.

予想 1.2. n を 3 以上の自然数とすれば，

$$X^n+Y^n=Z^n,\quad XYZ\neq 0 \tag{5}$$

を満たす整数 X,Y,Z は存在しない.

フェルマー以降，多くの数学者の挑戦の歴史を経て，約 350 年後の 1995 年にワイルスが「志村–谷山予想」という別の予想を解決することによってこの予想が正しいことを証明した.

a	b	$X = a^2 - b^2$	$Y = 2ab$	$Z = a^2 + b^2$
2	1			
3	2			
4	1			
4	3			
5	2			
5	4			
6	1			
6	5			
7	2			
7	4			
7	6			
8	1			
8	3			
8	5			
8	7			
9	2			
9	4			
9	8			

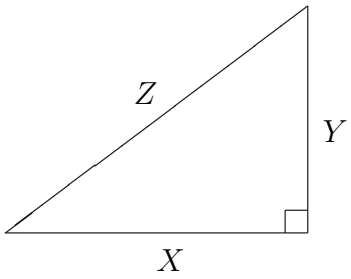
表 1: ピタゴラス数

2　合同数の問題

定義 2.1. 三辺の長さが有理数である直角三角形の面積となるような正の有理数 r を**合同数**という．すなわち，

$$X^2 + Y^2 = Z^2,$$
$$\frac{1}{2}XY = r$$

を満たすような正の有理数 X, Y, Z が存在するとき，r は合同数である．



例えば，$3^2 + 4^2 = 5^2$ であるから，三辺の長さが $3, 4, 5$ の直角三角形の面積 $\frac{1}{2} \times 3 \times 4 = 6$ は合同数である．同様に，$5^2 + 12^2 = 25 + 144 = 169 = 13^2$ であるから，三辺の長さが $5, 12, 13$ の直角三角形の面積 $\frac{1}{2} \times 5 \times 12 = 30$ は合同数である．

正の有理数 X, Y, Z が $X^2 + Y^2 = Z^2$ を満たせば，点 $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ は単位円の第 1 象限の有理点であるから，§ 1 でみたように，有理数 t を用いて，

$$\frac{X}{Z} = \frac{1 - t^2}{1 + t^2}, \quad \frac{Y}{Z} = \frac{2t}{1 + t^2}$$

と表せる．したがって，

$$Z = s(1 + t^2), \quad X = s(1 - t^2), \quad Y = 2st$$

とかける．ここで，s, t は有理数で，$s > 0,\ 0 < t < 1$ である．そのとき，X, Y, Z を三辺とする直角三角形の面積 r は，

$$r = \frac{1}{2}XY = s^2 t(1 - t^2) \tag{6}$$

で与えられる．s, t にいろいろな有理数の値を与えることによって，合同数が次々に得られる (表 2).

定義から，r が合同数ならば，r は正の有理数 X, Y, Z を三辺とする直角三角形の面積である．したがって，任意の正の有理数 u について，$u^2 r$ は uX, uY, uZ を三辺とする直角三角形の面積であるから，$u^2 r$ も合同数である．特に，$r = \frac{b}{a}$ と既

t	s	$X = s(1-t^2)$	$Y = 2st$	$Z = s(1+t^2)$	$r = s^2t(1-t^2)$
$\frac{1}{2}$	4	3	4	5	6
$\frac{2}{3}$	9	5	12	13	30
$\frac{1}{4}$	8	$\frac{15}{2}$	4	$\frac{17}{2}$	15
$\frac{3}{4}$	8	$\frac{7}{2}$	12	$\frac{25}{2}$	21
$\frac{4}{5}$	$\frac{25}{6}$	$\frac{3}{2}$	$\frac{20}{3}$	$\frac{41}{6}$	5
$\frac{9}{16}$	$\frac{64}{15}$	$\frac{35}{12}$	$\frac{24}{5}$	$\frac{337}{60}$	7

表 2: 合同数

約分数の形にかき，さらに，$a = a_0^2 a_1$, $b = b_0^2 b_1$, a_0, b_0 は自然数，a_1, b_1 は平方数 $(4, 9, 16, 25, \ldots)$ で割れない自然数とかいて，$u = \dfrac{a_0 a_1}{b_0}$ とおけば，

$$u^2 r = \frac{a_0^2 a_1^2}{b_0^2} \frac{b_0^2 b_1}{a_0^2 a_1} = a_1 b_1$$

であり，a_1 と b_1 の公約数は 1 だけであるから，$u^2 r$ は平方数で割れない自然数である．すなわち，合同数は適切な正の有理数の平方をかけることによって，平方数で割れないような自然数の合同数になる．以下，**平方数で割れないような自然数の合同数**のことを，単に合同数と呼ぶことにする．(6) において，t, s にいろいろな有理数の値を与えれば，すべての合同数が得られるはずである．しかし，与えられた自然数 n が合同数かどうかはこれではわからない (r, s にいろいろな値を入れてもなかなか n が現れない場合に，n が合同数でないのか，それともももっと別の r, s の値を入れれば出てくるのか，どちらかわからない)．表 2 から，5, 6, 7 は合同数である．1 は合同数ではないことはフェルマーによって証明された．これについては，最後にその証明を与える．

「与えられた n が合同数かどうかを簡単に決定する方法を求める」を合同数問題という．これは 10 世紀のアラビアに起源をさかのぼることができる古典的な問題であるが，現在でも完全には解決されていない．ここで，合同数問題を少し言い換えてみる．

命題 2.2. n を平方数で割れないような自然数とする．そのとき，n が合同数であるための必要十分条件は，$x^2 + n$, $x^2 - n$ がともに有理数の 2 乗であるような有理数 x が存在することである．

[証明]　n が合同数であるとする．正の有理数 X, Y, Z で，

$$X^2 + Y^2 = Z^2, \quad \frac{1}{2}XY = n$$

を満たすものが存在する．$x = \dfrac{Z}{2}$ とおけば，

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

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

逆に，$x^2 + n = A^2$, $x^2 - n = B^2$, A, B は有理数ならば，

$$\begin{aligned} 2x^2 &= (x^2 + n) + (x^2 - n) = A^2 + B^2, \\ 2n &= (x^2 + n) - (x^2 - n) = A^2 - B^2 \end{aligned}$$

であるから，

$$\begin{aligned} n &= \frac{1}{2}(A^2 - B^2) = \frac{1}{2}(A+B)(A-B), \\ (A+B)^2 + (A-B)^2 &= A^2 + 2AB + B^2 + A^2 - 2AB + B^2 \\ &= 2(A^2 + B^2) = 4x^2 = (2x)^2. \end{aligned}$$

ゆえに，n は合同数である．　□

3　楕円曲線

一般に，$x^3 + ax^2 + bx + c = 0$ が重解を持たないような 3 次方程式であるとき，方程式

$$y^2 = x^3 + ax^2 + bx + c$$

によって定義される曲線を**楕円曲線**という．このように呼ばれるのは，この曲線が楕円の弧の長さと関係するためである．

n を平方数で割れないような自然数とし，楕円曲線

$$E_n : \ y^2 = x(x+n)(x-n) \tag{7}$$

を考える．次の 3 点は明らかに E_n 上の有理点である (図 2)．

$$(-n, 0), \quad (0, 0), \quad (n, 0).$$

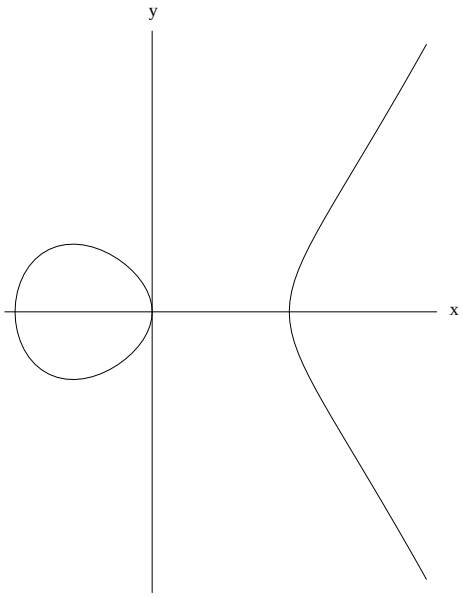


図 2: 楕円曲線 E_n

命題 2.2 より，n が合同数であることは，有理数 x_0 で，x_0^2+n, x_0^2-n ともに有理数の平方であるものが存在することと同値である．したがって，n が合同数ならば，

$$x_0^2+n=A^2,\quad x_0^2-n=B^2$$

となる有理数 x_0, A, B が存在する．そのとき，$AB\neq 0$ であり，

$$x_0^2(x_0^2+n)(x_0^2-n)=x_0^2A^2B^2=(x_0AB)^2$$

であるから，点 (x_0^2, x_0AB) は楕円曲線 E_n 上の $(-n,0)$, $(0,0)$, $(n,0)$ 以外の有理点である．

逆に，楕円曲線 E_n 上に $(-n,0)$, $(0,0)$, $(n,0)$ 以外の有理点 $P(x_1,y_1)$ が存在したとする．単位円のときと同様に，有理数を傾きとする直線と楕円曲線との交点を考えよう．E_n は 3 次方程式で定義されているから，交点は 3 点あると考えられる．今，E_n 上の有理点 $P(x_1,y_1)$ が 1 点だけわかっている．そこで，点 P における曲線 E_n の接線を考え，それと E_n の交点を考えれば，P 以外にもう 1 点 Q が得られるだろう．Q も有理点になることが期待できる (図 3)

そのために，

$$t=\frac{3x_1^2-n^2}{2y_1}$$

とおいて，点 P を通る傾き t の直線

$$\ell:\ y=t(x-x_1)+y_1$$

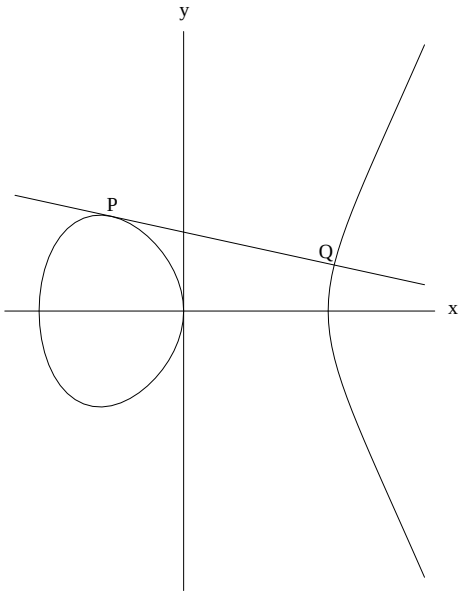


図 3: 楕円曲線 E_n の接線

を考える．楕円曲線 E_n と直線 ℓ の交点を求めよう．交点の x 座標は,

$$y^2 = x(x+n)(x-n) = x^3 - n^2x, \quad y = t(x-x_1) + y_1$$

より，3 次方程式

$$\begin{aligned} x^3 - n^2x &= \left(t(x-x_1) + y_1\right)^2, \\ x^3 - n^2x &= t^2(x-x_1)^2 + 2t(x-x_1)y_1 + y_1^2 \end{aligned}$$

を満たす．ここで，$y_1^2 = x_1^3 - n^2x_1$, $2y_1t = 3x_1^2 - n^2$ であるから,

$$\begin{aligned} &x^3 - n^2x = t^2(x-x_1)^2 + (3x_1^2 - n^2)(x-x_1) + x_1^3 - n^2x_1, \\ &x^3 - n^2x - x_1^3 + n^2x_1 - t^2(x-x_1)^2 - (3x_1^2 - n^2)(x-x_1) = 0, \\ &(x^3 - x_1^3) - n^2(x-x_1) - t^2(x-x_1)^2 - (3x_1^2 - n^2)(x-x_1) = 0, \\ &(x-x_1)\{x^2 + x_1x + x_1^2 - n^2 - t^2(x-x_1) - (3x_1^2 - n^2)\} = 0, \\ &(x-x_1)\{x^2 + x_1x - 2x_1^2 - t^2(x-x_1)\} = 0, \\ &(x-x_1)\{(x-x_1)(x+2x_1) - t^2(x-x_1)\} = 0, \\ &(x-x_1)^2(x + 2x_1 - t^2) = 0. \end{aligned}$$

したがって，この 3 次方程式の解は，$x = x_1$(重解) と $x = t^2 - 2x_1$ である．$x_2 =$

$t^2 - 2x_1$, $y_2 = t(x_2 - x_1) + y_1$ とおけば,

$$\begin{aligned}
x_2 &= t^2 - 2x_1 \\
&= \frac{(3x_1^2 - n^2)^2}{4y_1^2} - 2x_1 \\
&= \frac{9x_1^4 - 6n^2x_1^2 + n^4 - 8y_1^2}{4y_1^2} \\
&= \frac{9x_1^4 - 6n^2x_1^2 + n^4 - 8(x_1^3 - n^2x_1)}{4y_1^2} \\
&= \frac{x_1^4 + 2n^2x_1^2 + n^4}{4y_1^2} \\
&= \left(\frac{x_1^2 + n^2}{2y_1}\right)^2,
\end{aligned}$$

$$\begin{aligned}
y_2 &= t(x_2 - x_1) + y_1 \\
&= \frac{3x_1^2 - n^2}{2y_1}\left(\left(\frac{x_1^2 + n^2}{2y_1}\right)^2 - x_1\right) + y_1 \\
&= \frac{3x_1^2 - n^2}{2y_1}\left(\frac{x_1^4 + 2n^2x_1^2 + n^4 - 4x_1y_1^2}{4y_1^2}\right) + y_1 \\
&= \frac{8y_1^4 + (3x_1^2 - n^2)(-3x_1^4 + 6n^2x_1^2 + n^4)}{8y_1^3} \\
&= \frac{8(x_1^3 - n^2x_1)^2 + (3x_1^2 - n^2)(-3x_1^4 + 6n^2x_1^2 + n^4)}{8y_1^3} \\
&= -\frac{x_1^6 - 5n^2x_1^4 - 5n^4x_1^2 + n^6}{8y_1^3} \\
&= -\frac{(x_1^2 + n^2)(x_1^4 - n^2x_1^2 + n^4) - 5n^2x_1^2(x_1^2 + n^2)}{8y_1^3} \\
&= -\frac{(x_1^2 + n^2)(x_1^4 - 6n^2x_1^2 + n^4)}{8y_1^3} \\
&= -\frac{(x_1^2 + n^2)((x_1^2 - n^2)^2 - (2nx_1)^2)}{8y_1^3} \\
&= -\frac{(x_1^2 + n^2)(x_1^2 + 2nx_1 - n^2)(x_1^2 - 2nx_1 - n^2)}{8y_1^3}.
\end{aligned}$$

$$
\begin{aligned}
x_2+n &= \frac{x_1^4+2n^2x_1^2+n^4}{4y_1^2}+n \\
&= \frac{x_1^4+2n^2x_1^2+n^4+4ny_1^2}{4y_1^2} \\
&= \frac{x_1^4+2n^2x_1^2+n^4+4nx_1^3-4n^3x_1}{4y_1^2} \\
&= \frac{(x_1^2-n^2)^2+4nx_1(x_1^2-n^2)+(2nx_1)^2}{4y_1^2} \\
&= \left(\frac{x_1^2+2nx_1-n^2}{2y_1}\right)^2,
\end{aligned}
$$

$$
\begin{aligned}
x_2-n &= \frac{x_1^4+2n^2x_1^2+n^4}{4y_1^2}-n \\
&= \frac{x_1^4+2n^2x_1^2+n^4-4ny_1^2}{4y_1^2} \\
&= \frac{x_1^4+2n^2x_1^2+n^4-4nx_1^3+4n^3x_1}{4y_1^2} \\
&= \frac{(x_1^2-n^2)^2-4nx_1(x_1^2-n^2)+(2nx_1)^2}{4y_1^2} \\
&= \left(\frac{x_1^2-2nx_1-n^2}{2y_1}\right)^2.
\end{aligned}
$$

したがって，点 $Q(x_2,y_2)$ は E_n の有理点であり，$x_2,\ x_2+n,\ x_2-n$ はいずれも有理数の平方である．命題 2.2 より，n は合同数である．

以上まとめると，

命題 3.1. n を平方数で割れないような自然数とする．そのとき，n が合同数であるための必要十分条件は，楕円曲線 E_n 上に $(-n,0),\ (0,0),\ (n,0)$ 以外の有理点が存在することである．

合同数である $n=5$ について，楕円曲線 E_5 の有理点を具体的に計算してみよう．

例 3.2. $n=5$ とする．楕円曲線 E_5 は

$$y^2=x(x+5)(x-5)=x^3-25x$$

によって定義される．

$$(-4)((-4)+5)((-4)-5)=(-4)(-9)=36=6^2$$

より，点 $P(-4,6)$ は E_5 上の有理点である．命題 3.1 より，$n=5$ は合同数である．

$$t=\frac{3(-4)^2-5^2}{2\cdot 6}=\frac{48-25}{12}=\frac{23}{12}$$

とおいて，直線

$$y = \frac{23}{12}(x+4)+6$$

と曲線 E_5 との交点の x 座標を求めれば，

$$x = -4 \text{ (重解)}, \quad x = \left(\frac{23}{12}\right)^2 - 2(-4) = \frac{1681}{12^2} = \left(\frac{41}{12}\right)^2$$

である．P 以外の交点の y 座標は，

$$\frac{23}{12}\left(\frac{1681}{12^2}+4\right)+6 = \frac{23}{12}\left(\frac{1681+576}{12^2}\right)+6 = \frac{23\cdot 2257+6\cdot 12^3}{12^3} = \frac{62279}{1728}.$$

$$\begin{aligned}
\left(\frac{41}{12}\right)^2+5 &= \frac{41^2+5\cdot 12^2}{12^2} \\
&= \frac{1681+720}{12^2} = \frac{2401}{12^2} = \left(\frac{49}{12}\right)^2, \\
\left(\frac{41}{12}\right)^2-5 &= \frac{41^2-5\cdot 12^2}{12^2} \\
&= \frac{1681-720}{12^2} = \frac{961}{12^2} = \left(\frac{31}{12}\right)^2.
\end{aligned}$$

命題 2.2 の証明から，

$$\begin{aligned}
\frac{49}{12}+\frac{31}{12} &= \frac{80}{12} = \frac{20}{3}, \\
\frac{49}{12}-\frac{31}{12} &= \frac{18}{12} = \frac{3}{2}, \\
2\times\frac{41}{12} &= \frac{41}{6}
\end{aligned}$$

を三辺とする三角形は直角三角形であり，その面積は 5 である．実際，

$$\left(\frac{20}{3}\right)^2+\left(\frac{3}{2}\right)^2 = \frac{400}{9}+\frac{9}{4} = \frac{1600+81}{36} = \left(\frac{41}{6}\right)^2,$$

$$\frac{1}{2}\times\frac{20}{3}\times\frac{3}{2} = 5.$$

今度は，$n=1$ は合同数でないことを証明しよう．そのために，定理 1.1 を応用して，次の定理を証明しておく．

定理 3.3. 方程式

$$X^4-Y^4 = Z^2 \tag{8}$$

は自然数解を持たない．したがって，方程式

$$X^4+Y^4 = Z^4 \tag{9}$$

も自然数解を持たない．

この定理の証明において，素因数分解の一意性から容易にわかる次の事実を何度も使う．

事実 3.4. A, B, C を自然数とし，A と B は互いに素であるとする．そのとき，

$$AB = C^2$$

ならば，互いに素な自然数 a, b が存在して，$A = a^2,\ B = b^2$ と表せる．

[定理 3.3 の証明]　(8) が自然数解 X, Y, Z を持ったとする．さらに，X, Y, Z は自然数解の中で X が最小になるものをとったとしてよい．そのとき，X, Y, Z は互いに素である．$(Y^2)^2 + Z^2 = (X^2)^2$ とみれば，定理 1.1 より，互いに素な自然数 $A > B$ で，A, B の一方だけが奇数，が存在して，

$$Y^2 = A^2 - B^2,\ Z = 2AB,\ X^2 = A^2 + B^2$$

または，

$$Z = A^2 - B^2,\ Y^2 = 2AB,\ X^2 = A^2 + B^2$$

と表せる．前者の場合，X, Y は奇数，Z は偶数である．よって，

$$X^4 - Y^4 = (X^2 + Y^2)(X^2 - Y^2) = Z^2$$

において，$X^2 + Y^2$ と $X^2 - Y^2$ はともに偶数である．

$$Z_1 = \frac{Z}{2}, \quad U = \frac{X^2 + Y^2}{2}, \quad V = \frac{X^2 - Y^2}{2}$$

とおけば，Z_1, U, V は自然数である．$U + V = X^2, U - V = Y^2$, X, Y は互いに素であるから，U と V は互いに素である．

$$UV = \left(\frac{X^2 + Y^2}{2}\right)\left(\frac{X^2 - Y^2}{2}\right) = \frac{Z^2}{4} = Z_1^2$$

より，$U = X_1^2, V = Y_1^2, X_1, Y_1$ は自然数，とかける．そのとき，

$$X_1^4 - Y_1^4 = U^2 - V^2 = (U + V)(U - V) = (XY)^2$$

である．$Y < X$ であるから，

$$X_1^2 = U = \frac{X^2 + Y^2}{2} < X^2, \quad X_1 < X$$

である．これは X, Y, Z が (8) の自然数解の中で X が最小であることに矛盾する．

後者の場合は，$Y^2 = 2AB$, A と B は互いに素であることから，U, V を互いに素な自然数，U は奇数として，$A = U^2, B = 2V^2$ または $A = 2V^2, B = U^2$ とかける．これを $X^2 = A^2 + B^2$ に代入して，

$$X^2 = U^4 + 4V^4 = (U^2)^2 + (2V^2)^2$$

を得る．再び定理 1.1 を適用すれば，互いに素な自然数 a, b が存在して，

$$U^2 = a^2 - b^2, \quad 2V^2 = 2ab, \quad X = a^2 + b^2$$

である．$V^2 = ab$, a と b は互いに素であるから，自然数 X_1, Y_1 によって，$a = X_1^2$, $b = Y_1^2$ とかける．そのとき，

$$X_1^4 - Y_1^4 = a^2 - b^2 = U^2$$

である．

$$X_1 \leq X_1^2 = a \leq a^2 < a^2 + b^2 = X$$

であるから，これも X, Y, Z が (8) の自然数解の中で X が最小であることに矛盾する．後半は簡単に示せる．もし，(9) が自然数解 X, Y, Z を持ったとすると，$X^4 + Y^4 = Z^4$ より，$Z^4 - Y^4 = (X^2)^2$ である．これは，(8) が自然数解を持つことになって矛盾である． □

例 3.5. $n = 1$ とする．楕円曲線 E_1 は

$$y^2 = x(x+1)(x-1) = x^3 - x$$

によって定義される．E_1 の $(-1, 0), (0, 0), (1, 0)$ 以外の有理点 $P(x_1, y_1)$ が存在したとする．$x_1 = \dfrac{u}{v}$, u, v は互いに素な整数，$v > 0$ とかく．同様に，$y_1 = \dfrac{s}{t}$, s, t は互いに素な整数，$s \neq 0$, $t > 0$ とかく．そのとき，

$$\frac{s^2}{t^2} = \frac{u(u^2 - v^2)}{v^3}$$

であるが，両辺ともに既約分数であるから，

$$t^2 = v^3, \quad s^2 = u(u^2 - v^2)$$

である．$\left(\dfrac{t}{v}\right)^2 = v$ であるから，$V = \dfrac{t}{v}$ とおけば，$v = V^2$ である．v は整数だから，有理数 $V > 0$ も整数である．u と $u^2 - v^2$ は互いに素であるから，$s^2 = u(u^2 - v^2)$ より，u も $u^2 - v^2$ もともに平方数である．$u = U^2$, $u^2 - v^2 = W^2$, U, W は自然数とかける．よって，

$$U^4 - V^4 = W^2$$

である．しかし，そのような自然数 U, V, W は定理 3.3 によって存在しないから，これは矛盾である．ゆえに，E_1 の $(-1, 0), (0, 0), (1, 0)$ 以外の有理点は存在しない．命題 3.1 より，$n = 1$ は合同数ではない．

4　楕円曲線上の有理点の構造

命題 3.1 の証明において，楕円曲線 E_n 上の有理点 P が既知のとき，点 P における接線と楕円曲線 E_n との P 以外の交点 Q が一意的に定まり，Q も有理点になることを示した．

同様に，楕円曲線 E_n 上の 2 つの有理点 P, Q，$P \neq Q$，が既知のとき，P，Q を結ぶ直線と E_n との P, Q 以外の交点 R がただ一つ定まり，R も有理点になることがわかる．R と x 軸に関して対称な点を R' とする．そのとき，

$$P + Q = R'$$

によって P と Q の**和**を定義する．この定義によって，楕円曲線 E_n 上の有理点同士の”足し算”がうまく定義される．

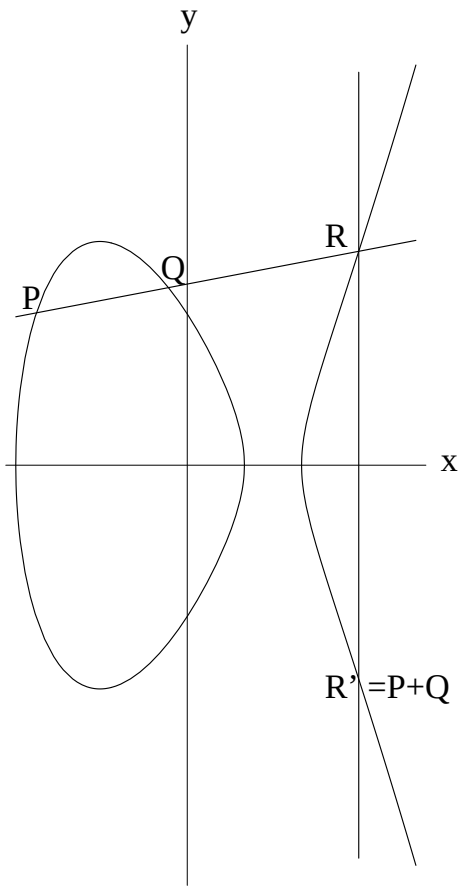


図 4: 楕円曲線上の加法

E_n 上に $(-n, 0), (0, 0), (n, 0)$ 以外の有理点 P があれば，上の足し算の意味で次々に，有理点

$$2P = P + P, \quad 3P = 2P + P, \quad 4P = 3P + P, \ldots$$

を作ることができ，これらはすべて相異なることが示される．このようにして，無数の有理点を作ることができる．したがって，命題 3.1 は次のように言い換えられる．

定理 4.1. n を平方数で割れないような自然数とする．そのとき，n が合同数であるための必要十分条件は，楕円曲線 E_n 上に無限に多くの有理点が存在することである．

課題 4.2. 楕円曲線 E_n において，$P(x_1, y_1)$, $Q(x_2, y_2)$, $P \neq Q$ について，$R' = P+Q$ の座標を求める公式を導け．さらに，楕円曲線 E_5 上の有理点 $P(-4, 6)$ から出発して，$2P$, $3P$, $4P$, $5P$, ..., を求めよ．

参考文献

[1] J. シルバーマン，はじめての数論―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，2001，ピアソンエデュケーション．

[2] J. シルバーマン・ J. テイト，楕円曲線論入門，1995，シュプリンガー東京．

[3] A. ヴェイユ，数論―歴史からのアプローチ，1987，日本評論社．

[4] 加藤和也，解決! フェルマーの最終定理，1995，日本評論社．

[5] 藤原正彦，天才の栄光と挫折―数学者列伝，2002 年，新潮社．

[1] は文系の大学生向けに書かれた整数論の入門書で，内容が豊富であるにもかかわらず記述はわかりやすい．[2] は理系の大学生向けに書かれたものでもう少し専門的である．フェルマー予想の解決について数学的に知りたい方には，読み物としてもおもしろい [4] をお薦めする．フェルマー予想を解決したワイルスの人物について知りたい方には，[5] を読むことを薦める．ピタゴラス数やフェルマーなどに関する数学史的なことについては，[3] を見てほしい．