GCDを含む、あるDIOPHANTOS方程式の解の研究

学習院大学 理学部 数学科 ４年
鄭 立舜

◆◆目的◆◆

曲線(パスカルの真珠型曲線)

$$y^m = x^a(1-x)^b$$

の種数gは次の式で求められる。

$$2g-2 = m-\delta_1-\delta_2-\delta_3 \cdots (*)$$

ただし、(m, a, bは自然数とする。)

$$\begin{aligned}
&\gcd(m,a,b) = 1,\\
&\delta_1 = \gcd(m,a),\\
&\delta_2 = \gcd(m,b),\\
&\delta_3 = \gcd(m,a+b).
\end{aligned}$$

種数が$0 \leq g \leq 10$ のとき、$(*)$をみたすそれぞれの (m,a,b) を求め、どのような性質をみたす解があるかを調べる。

いくつかのパスカルの真珠型曲線の例

- $(m, a, b) = (5, 3, 2)$の場合（$g = 0$の場合）

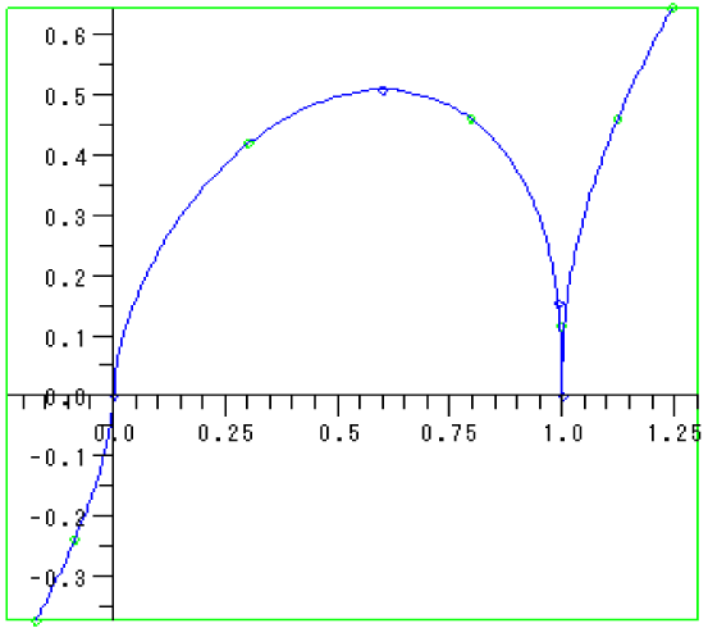

FIGURE 1. $(m, a, b) = (5, 3, 2)$

・$(m,a,b)=(4,5,6)$の場合（$g=1$の場合）

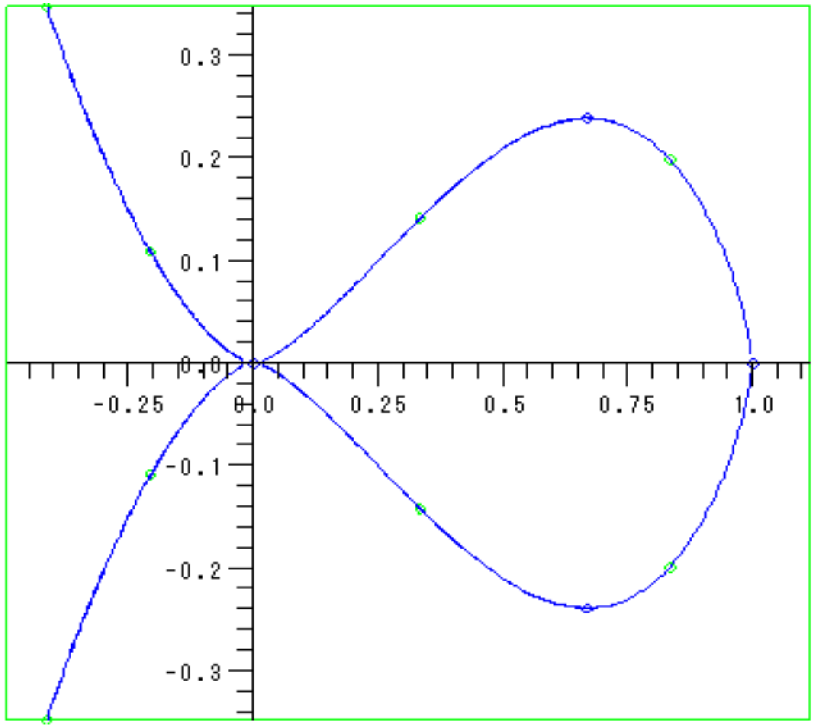

FIGURE 2. $(m,a,b)=(4,5,6)$

◆◆方法◆◆

$$\gcd(m, a, b) = 1$$

をみたす、ある(m, a, b)を与えたとき、

$$2g - 2 = m - \delta_1 - \delta_2 - \delta_3$$

をみたすgを求めるため、Prologを利用してデータを集める。
今回、$m, a, b \leq 50$としてプログラムを作成した。

◆◆結果◆◆

Prologを用いて得られた結果をexcelで表にまとめた。

◆◆考察①◆◆

Prologで得られた結果から、以下の性質を持つことが予想される。

$g = 0$の場合

$$\begin{cases} a \equiv 0 \bmod m \\ b \equiv 0 \bmod m \\ a + b \equiv 0 \bmod m \end{cases}$$

のいずれかをみたす(m, a, b)。

$g=1$の場合

TABLE 1. $g=1$

m	$a \bmod m$	$b \bmod m$
3	1	1
	2	2
4	1	1,2
	2	1,3
	3	2,3
6	1	2,3
	2	1,3
	3	1,2,4,5
	4	3,5
	5	3,4

$g=2$の場合

TABLE 2. $g=2$

m	$a \bmod m$	$b \bmod m$
5	1	1,2,3
	2	1,2,4
	3	1,3,4
	4	2,3,4
6	1	1,4
	2	5
	4	1
	5	2,5
8	1	3,4
	3	1,4
	4	1,3,5,7
	5	4,7
	7	4,5

TABLE 3. $g = 2$

m	$a \bmod m$	$b \bmod m$
10	1	4,5
	2	3,5
	3	2,5
	4	1,5
	5	1,2,3,4,6,7,8,9
	6	9,5
	7	8,5
	8	7,5
	9	6,5

$g=3$の場合

TABLE 4. $g=3$

m	$a \bmod m$	$b \bmod m$
7	1	1,2,3,4,5
	2	1,2,3,4,6
	3	1,2,3,5,6
	4	1,2,4,5,6
	5	1,3,4,5,6
	6	2,3,4,5,6
8	1	1,2,5,6
	2	1,3,5,7
	3	2,3,6,7
	5	1,2,5,6
	6	1,3,5,7
	7	2,3,6,7

TABLE 5. $g = 3$

m	$a \bmod m$	$b \bmod m$
9	1	2,3,5,6
	2	1,3,4,6
	3	1,2,4,5,7,8
	4	2,3,6,8
	5	1,3,6,7
	6	1,2,4,5,7,8
	7	3,5,6,8
	8	3,4,6,7

TABLE 6. $g = 3$

m	$a \bmod m$	$b \bmod m$
12	1	3,5,6,8
	3	1,4,5,8
	4	3,5,9,11
	5	1,3,4,6
	6	1,5,7,11
	7	6,8,9,11
	8	1,3,7,9
	9	4,7,8,11
	11	4,6,7,9

TABLE 7. $g = 3$

m	$a \bmod m$	$b \bmod m$
14	1	6,7
	2	5,7
	3	4,7
	4	3,7
	5	2,7
	6	1,7
	7	1,2,3,4,5,6,8,9,10,11,12,13
	8	7,13
	9	7,12
	10	7,11
	11	7,10
	12	7,9
	13	7,8

＜証明＞

$g=0$について　(k_1, k_2, k_3は自然数とする。)

$$\begin{cases} \delta_1 = \gcd(m, a) \Rightarrow m = \delta_1 k_1 \\ \delta_2 = \gcd(m, b) \Rightarrow m = \delta_2 k_2 \\ \delta_3 = \gcd(m, a+b) \Rightarrow m = \delta_3 k_3 \end{cases}$$

したがって、$(*)$は、

$$-2 = m - \frac{m}{k_1} - \frac{m}{k_2} - \frac{m}{k_3}$$

$$\frac{-2}{m} = 1 - \frac{1}{k_1} - \frac{1}{k_2} - \frac{1}{k_3}$$

$$\frac{1}{k_1} + \frac{1}{k_2} + \frac{1}{k_3} > 1$$

$k_1 \geq k_2 \geq k_3 \geq 1$ とすると、

$$\frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}>1$$

が常に成り立つ。

$k_1 \geq k_2 \geq k_3 \geq 2$ として考える。

$k_3 = 2$ とすると、

$$\frac{1}{k_1}+\frac{1}{k_2}>\frac{1}{2}$$

$k_1 \geq k_2 \geq 4$ とすると、

$$\frac{1}{k_1}+\frac{1}{k_2}\leq\frac{1}{2}$$

となり、矛盾。

ゆえに、$k_2 = 2\ or\ 3$ 。

$k_2 = 2$のとき、

$$\frac{1}{k_1} > 0$$

から、$k_1 \geq 2$。

$k_2 = 3$のとき、

$$\frac{1}{k_1} > \frac{1}{6}$$

から、

$$3 \leq k_1 < 6$$

より、$k_1 = 3\ or\ 4\ or\ 5$。

以下の場合に分けて証明を行っていく。

$0 < a \leq b \leq m, a + b \leq m$とする。
(1) $k_3 = 1$の場合
(2) $k_1 \geq 2, (k_2, k_3) = (2, 2)$の場合
(3) $(k_1, k_2, k_3) = (3, 3, 2)$の場合
(4) $(k_1, k_2, k_3) = (4, 3, 2)$の場合
(5) $(k_1, k_2, k_3) = (5, 3, 2)$の場合
(6) $b \equiv 0 \bmod m$の場合

(1)の場合

$m = k_3\delta_3$ より、$m = \delta_3$

$\delta_3 = \gcd(m, a+b)$

$\delta_3 = \gcd(\delta_3, a+b)$

ゆえに、$a+b = \delta_3 N = mN$ （Nは自然数）

したがって、

$$a+b = mN$$

をみたす(m, a, b)のとき成立する。

(2)の場合

$m = 2\delta_2 = 2\delta_3 \ \Rightarrow \ \delta_2 = \delta_3$

$\delta_2 = \gcd(m, b) = \gcd(2\delta_2, b)$

$b = \delta_2$

$\delta_3 = \gcd(m, a+b) = \gcd(2\delta_3, a+b)$

$\delta_2 = \gcd(2\delta_2, a+\delta_2)$

すなわち、$a = 0$

しかし、$0 < a$なので、矛盾。

(3)〜(5)の場合も同様に考える。

(6)の場合

$\delta_1 = \gcd(m, a) = 1$

$\delta_2 = \gcd(m, b) = \gcd(m, 0) = m$

$\delta_3 = \gcd(m, a + b) = \gcd(m, a + 0) = \gcd(m, a) = 1$

$2g - 2 = m - \delta_1 - \delta_2 - \delta_3$

$2g - 2 = -2$

したがって、$b \equiv 0 \bmod m$のとき、$g = 0$が成り立つ。

$a \equiv 0 \bmod m$の場合も同様。（証明終）

$g=1$について

$g=0$の場合と同様に考えると、

$$1=\frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}$$

このとき、

$$(k_1,k_2,k_3)=(3,3,3),(2,4,4),(4,2,4),(4,4,2),(2,3,6),$$
$$(2,6,3),(3,2,6),(3,6,2),(6,2,3),(6,3,2).$$

が考えられる。

(1) $(k_1, k_2, k_3) = (3, 3, 3)$の場合 $(n, p, q \geq 0$の自然数とする。$)$

$m = 3\delta_1 = 3\delta_2 = 3\delta_3$ $\cdots (**)$

が成り立ち、$m = 3n$とおける。

（イ）$a = 3p + 1$

$\delta_1 = \gcd(3n, 3p + 1) = 1$

ゆえに、$m = 3\delta_1 = 3$

$b = 3q + 1$ or $3q + 2$

・$b = 3q + 1$

$\Rightarrow$ $\delta_2 = \gcd(3, 3q + 1) = 1$から、$m = 3\delta_2 = 3$,

$\delta_3 = \gcd(3, 3p + 3q + 2) = 1$から、$m = 3\delta_3 = 3$となり$(**)$を

みたす。

・$b = 3q + 2$

$\Rightarrow$ $\delta_2 = \gcd(3, 3q + 2) = 1$から、$m = 3\delta_2 = 3$,

$\delta_3 = \gcd(3, 3p + 3q + 3) = 3$から、$m = 3\delta_3 = 9 \neq 3$ゆえに不適。

（ロ）$a = 3p + 2$として、同様に考える。

$m = 3$の場合

$$a \equiv 1 \bmod 3, b \equiv 1 \bmod 3,$$
$$a \equiv 2 \bmod 3, b \equiv 2 \bmod 3.$$

である。

$$(k_1, k_2, k_3) = (2, 4, 4), (4, 2, 4), (4, 4, 2), (2, 3, 6), (2, 6, 3),$$
$$(3, 2, 6), (3, 6, 2), (6, 2, 3), (6, 3, 2).$$

の場合も同様。（証明終）

$g=2$について

$g=0$の場合と同様に考えると、

$$1>\frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}$$

これをみたす(k_1,k_2,k_3)は多数存在する。

$\delta_1,\delta_2,\delta_3\geq 1$より、

$$\delta_1+\delta_2+\delta_3\geq 3$$

$$2=m-\delta_1-\delta_2-\delta_3$$

なので、

$$m\geq 5$$

（イ）$m=5$

$\delta_1=\gcd(m,a)=1$

$\delta_2=\gcd(m,b)=1$

$g=2$ より、$\delta_3=1$

ゆえに、$a+b\not\equiv 0 \bmod 5$

したがって、

$$\begin{cases} a\not\equiv 0 \bmod 5, \\ b\not\equiv 0 \bmod 5, \\ a+b\not\equiv 0 \bmod 5. \end{cases}$$

をみたす(a,b)のとき成り立つ。

（ロ）$m=6$　$(\delta_1$のとりうる値は、$\delta_1=1,2,3)$

（ i ）$\delta_1=1$

$2g-2=m-\delta_1-\delta_2-\delta_3$

$\delta_2+\delta_3=3$

このことから、$(\delta_2,\delta_3)=(1,2),(2,1)$

$(\delta_2,\delta_3)=(1,2)$ をみたす(a,b)は、

$(a,b)\equiv(1,1),(5,5) \bmod 6$

$(\delta_2,\delta_3)=(2,1)$ をみたす(a,b)は、

$(a,b)\equiv(1,4),(5,2) \bmod 6$

（ii）$\delta_1 = 2$

$2g - 2 = m - \delta_1 - \delta_2 - \delta_3$

$\delta_2 + \delta_3 = 2$

このことから、$(\delta_2, \delta_3) = (1, 1)$

$(\delta_2, \delta_3) = (1, 1)$ をみたす (a, b) は、

$(a, b) \equiv (2, 5), (4, 1) \bmod 6$

（iii）$\delta_1 = 3$

$2g - 2 = m - \delta_1 - \delta_2 - \delta_3$

$\delta_2 + \delta_3 = 1$

$\delta_2, \delta_3 \geq 1$ より、矛盾。

したがって（ｉ）～（iii）より、

$a \equiv 1 \bmod 6, b \equiv 1, 4 \bmod 6,$

$a \equiv 2 \bmod 6, b \equiv 5 \bmod 6,$

$a \equiv 4 \bmod 6, b \equiv 1 \bmod 6,$

$a \equiv 5 \bmod 6, b \equiv 2, 5 \bmod 6.$

となる(a, b)のとき成り立つ。

$m = 8, 10$の場合も同様に考える。（証明終）

$g = 3$について

$g = 2$の場合と同様に考える。（証明終）

◆◆考察②◆◆

証明できた事柄を、基本関係を用いて考察してみる。

＜基本関係＞

(1) $(m, a, b) \sim (m, a+m, b)$

(2) $(m, a, b) \sim (m, a, b+m)$

(3) $(m, a, b) \sim (m, b, a)$

(4) $m \geq a+b$のとき、

$(m, a, b) \sim (m, m-(a+b), b)$

(5) $m \leq a+b$のとき、

$(m, a, b) \sim (m, m-a, a+b-m)$

(1)〜(5)の関係によって生成される関係を、
同じ記号で示し、同値関係と呼ぶ。

＜例＞

$(m, a, b) = (6, 3, 4)$の場合

$$(6, 3, 4) \sim (6, 3, 1) \sim (6, 1, 3)$$

$g = 0$について

$$a \equiv 0 \bmod m,$$

$$a + b \equiv 0 \bmod m.$$

これら２通りのいずれかと同値である。

$g = 1$について

$$(m, a, b) \sim (3, 1, 1), (4, 1, 2), (6, 1, 3).$$

これら3通りのいずれかと同値である。

$g = 2$について

$(m, a, b) \sim (5, 1, 2), (5, 1, 3), (6, 1, 4), (8, 1, 4), (10, 1, 5), (10, 2, 5).$

これら6通りのいずれかと同値である。

$g=3$について

$$(m,a,b) \sim (7,1,3),(7,1,4),(7,1,5),(7,2,3),(8,1,5),(8,1,6),$$
$$(8,2,3),(9,1,5),(9,1,6),(9,2,4),(12,1,6),$$
$$(12,1,8),(12,3,5),(14,1,7),(14,2,7),(14,3,7).$$

これら１６通りのいずれかと同値である。

◆◆まとめ◆◆

Prologから得られた結果を考察したことで、$0 \leq g \leq 3$のとき、それぞれの解がどのような性質を持つかがわかった。

さらに、同値関係を用いることで、
$g = 0$では２通り、
$g = 1$では３通り、
$g = 2$では６通り、
$g = 3$では１６通り
のうち、いずれかの性質から成り立つということがわかった。