古典的 Diophantus 問題に対応する楕円曲線のセルマー群と有向グラフ

東京理科大学理工学部数学科　後藤丈志　(Takeshi Goto)

概要

本稿では，楕円曲線のセルマー群について復習し，その大きさをグラフで表現する試みについて紹介する．§1 でいくつかの古典的問題と楕円曲線との関連を述べ，§2 で楕円曲線のセルマー群について復習する．§3 で本稿で用いるグラフ理論の用語について解説し，Feng and Xiong (J. Number Theory, 2004) の結果を紹介する．§4 で類似の結果を述べ，証明を与える．

1　古典的問題と楕円曲線

古典的 Diophantus 問題の中には，楕円曲線の有理点を求める問題に帰着されるものがある．本節ではそのような問題をいくつか紹介する．一般に，有理数体上定義された楕円曲線 $E : y^2 = f(x)$ ($f(x)$ は重根を持たない有理数係数三次多項式) に対し，曲線上の有理点全体の集合 $E(\mathbb{Q})$ はアーベル群をなすが，Mordell の定理によりこれは有限生成であって，

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}}$$

となる．ここに，r は非負整数であって階数といい，$\operatorname{rank} E(\mathbb{Q})$ で表す．また，$E(\mathbb{Q})_{\mathrm{tors}}$ は有限位数の点の集合である．$E(\mathbb{Q})_{\mathrm{tors}}$ は Nagell-Lutz の定理により計算可能であるが，階数 $\operatorname{rank} E(\mathbb{Q})$ を求めることは一般には難しい．楕円曲線の入門的な内容については Silverman-Tate の本 [21] を参照されたい．

1.1　合同数問題

三辺の長さが有理数である直角三角形の面積になり得る有理数を合同数という．すなわち，正の有理数 n に対し，Diophantus 方程式

$$X^2 + Y^2 = Z^2, \quad XY = 2n \tag{1.1}$$

が有理数解 (X, Y, Z) を持つとき，n を合同数と呼ぶ．例えば，直角三角形 $(3, 4, 5)$ の面積 6 や，直角三角形 $(9/6, 40/6, 41/6)$ の面積 5 は合同数である．また，1 は合同数でないことを Fermat が証明した．与えられた正の有理数が合同数か否かを判定する方法を求めよという問題を合同数問題という．合同数問題については，Koblitz [14] に詳しい．n が合同数であることと，0 でない有理数 k に対する k^2n が合同数であることは同値であるから，n として平方因子を持たない自然数のみを考えれば十分である．合同数問題は，楕円曲線

$$E_n : y^2 = x(x+n)(x-n)$$

の有理点を考えることに帰着される．なぜならば，(1.1) の有理数解 (X, Y, Z) に対し，

$$x = (Z/2)^2, \quad y = Z(X+Y)(X-Y)/8 \tag{1.2}$$

と置けば，(x,y) は E_n の有理点となるからである．逆に，E_n の有理点 (x,y) で $y \neq 0$ なるものがあれば，

$$X = \left|\frac{(x+n)(x-n)}{y}\right|, \quad Y = 2n\left|\frac{x}{y}\right|, \quad Z = \left|\frac{x^2+n^2}{y}\right|$$

により，(1.1) の有理数解 (X,Y,Z) を得る．$y=0$ なる E_n の有理点は，式の形より $(0,0),(\pm n,0)$ で全てであるが，実は $E_n(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O},(0,0),(\pm n,0)\}$ ($\mathcal{O}$ は無限遠点，すなわち加法における単位元を表す) であることが確かめられ，したがって

$$n \text{ が合同数} \iff \operatorname{rank} E_n(\mathbb{Q}) > 0$$

である．

上の説明では，E_n の有理点毎に異なる三角形が得られるか，という疑問が残るが，答えは No である．正確には，E_n の二倍点 (x,y) で $y>0$ なるものと，面積 n の直角三角形が一対一に対応する．二倍点 (x,y) については，$x, x+n, x-n$ の全てが平方数であって，

$$X = \sqrt{x+n} - \sqrt{x-n}, \quad Y = \sqrt{x+n} + \sqrt{x-n}, \quad Z = 2\sqrt{x} \tag{1.3}$$

とすれば，$X<Y$ なる (1.1) の解を得る ([13, p. 53])．(1.2) と (1.3) は互いに逆写像である．したがって，面積 n の直角三角形が一つでもあれば，E_n における二倍写像を通じて，いくらでも面積 n の直角三角形を構成できる．

例. 面積 6 の直角三角形 $(3,4,5)$ から，対応 (1.2) によって $E_6 : y^2 = x(x+6)(x-6)$ の無限位数の有理点 $(25/4, -35/8)$ を得る．この点は $P = (-2,-8)$ の二倍である．さらに，$4P = (1442401/19600, 1726556399/2744000)$ から，対応 (1.3) によって，面積 6 の別の直角三角形 $(7/10, 120/7, 1201/70)$ を得る．

さて，楕円曲線の階数を調べる際に基本的なのは，2-descent method と呼ばれる方法である．E_n については，[1], [6], [7], [17], [15], [19] などで調べられている．2-descent method は，ある種のセルマー群を計算することに対応する．その詳細は §2 で復習する．例えば，E_n の 2-descent method により，以下に列挙した平方因子を含まない自然数 n は合同数でないことが知られている．ここに，p,q,r,p_i は素数を表し，$(*/*)$ はルジャンドル記号を表す．

- $n = p \equiv 3 \pmod 8$
- $n = 2p,\ p \equiv 5 \pmod 8$
- $n = pq,\ (p,q) \equiv (3,3) \pmod 8$
- $n = pq,\ (p,q) \equiv (1,3) \pmod 8,\ (p/q) = -1$
- $n = pqr,\ (p,q,r) \equiv (1,1,3) \pmod 8,\ (p/q),(p/r),(q/r)$ のうち，少なくとも二つが -1
- $n = 2p_1 \cdots p_t,\ p_i \equiv 5 \pmod 8,\ (p_j/p_i) = 1 \text{ for } i<j$

§4 で述べる Feng and Xiong [5] の結果は，これらの非合同数の満たす条件を，グラフ理論の用語を用いて表している．

1.2 θ-合同数問題

直角三角形に限らず，一般の角 θ $(0<\theta<\pi)$ を持つ三角形を考えることにより，θ-合同数が定義される ([3])．三辺の長さが全て有理数のとき，余弦定理により $\cos\theta \in \mathbb{Q}$ である．

定義. $\cos\theta = s/r$ $((s,r) = 1, r > 0)$ とする．次の三条件を満たす三角形が存在するとき，n を θ-合同数と呼ぶ．

(1) 三辺の長さが全て有理数．

(2) 一つの角が θ に等しい．

(3) 面積が $n\sqrt{r^2 - s^2}$ に等しい

言い換えれば，n が θ-合同数であるとは，

$$Z^2 = X^2 + Y^2 - 2XY\frac{s}{r}, \quad XY = 2rn \tag{1.4}$$

が有理数解 (X, Y, Z) を持つ，ということである．$\theta = \pi/2$ のときは，$r = 1, s = 0$ と考えれば，従来の合同数の定義に他ならない．θ-合同数問題とは，与えられた自然数が θ-合同数であるか否か判定する方法を求めよ，という問題であり，やはり平方因子を持たない自然数のみ考えればよい．自然数 n が θ-合同数問題であることと，楕円曲線

$$E_{n,\theta} : y^2 = x(x + (r+s)n)(x - (r-s)n).$$

が $y \neq 0$ なる有理点 (x, y) を持つことは同値である．なぜならば，(1.4) の有理数解 (X, Y, Z) に対し，従来の合同数問題の場合と同様の対応 (1.2) によって (x, y) は $E_{n,\theta}$ の有理点となり，逆に $E_{n,\theta}$ の有理点 (x, y) $(y \neq 0)$ に対し，

$$X = \left|\frac{x^2 - (r^2 - s^2)n^2}{y}\right|, \quad Y = 2rn\left|\frac{x}{y}\right|, \quad Z = \left|\frac{x^2 + (r^2 - s^2)n^2}{y}\right|$$

と置けば，(X, Y, Z) は (1.4) の有理数解になるからである．また，従来の合同数問題と同様に，$X < Y$ なる (1.4) の解は，$E_{n,\theta}$ の二倍点 (x, y) で $y > 0$ なるものと一対一に対応する．実際，二倍点 (x, y) に対しては $x, x + (r+s)n, x - (r-s)n$ の全てが平方数であって，

$$X = \sqrt{x + (r+s)n} - \sqrt{x - (r-s)n},\ Y = \sqrt{x + (r+s)n} + \sqrt{x - (r-s)n},\ Z = 2\sqrt{x} \tag{1.5}$$

と置けば (1.4) の解を得る．(1.2) と (1.5) は互いに逆写像である．

Fujiwara [3] は，$n \neq 1, 2, 3, 6$ の場合，$E_{n,\theta}(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (0,0), (-(r+s)n, 0), ((r-s)n, 0)\}$ であることを示した．したがって，この場合，n が θ-合同数であることと，$\operatorname{rank} E_{n,\theta}(\mathbb{Q}) > 0$ であることは同値である．

例. (1) $E_{1,\pi/3} : y^2 = x(x+3)(x-1)$ の階数は 0 であるが，位数 4 の点 $(-1, 2)$ が存在するため，1 は $\pi/3$-合同数である．実際，正三角形 $(2, 2, 2)$ の面積は $\sqrt{3}$ であり，これ以外に条件を満たす三角形は存在しない．

(2) $E_{6,\pi/3} : y^2 = x(x+18)(x-6)$ の階数は 1 であって，$P = (-2, 16)$ が生成元である．したがって 6 は $\pi/3$-合同数である．実際，対応 (1.5) により，$2P$ から三角形 $(3, 8, 7)$ を，$4P$ から三角形 $(55/14, 336/55, 4129/770)$ を得る．この場合，条件を満たす三角形は無数に存在する．

$E_{n,\pi/3}$ についても，[3], [8], [9], [12], [22] などで，2-descent method により階数が調べられている．例えば，以下に列挙した平方因子を含まない自然数 n は $\pi/3$-合同数でないことが知られている．

- $n = p$, $\quad p \equiv 5, 7, 19 \pmod{24}$
- $n = 2p$, $\quad p \equiv 7, 13 \pmod{24}$
- $n = 3p$, $\quad p \equiv 5, 11, 17, 19 \pmod{24}$
- $n = pq$, $\quad (p, q) \equiv (7, 7) \pmod{24}$
- $n = pq$, $\quad (p, q) \equiv (1, 7) \pmod{24}$, $\quad (p/q) = -1$

本稿では，Feng and Xiong と同様の結果を $\pi/3$-合同数問題について与える．§4 で主結果を述べて証明を与える．証明には §2 で述べる結果が役に立つ．

1.3 Leech の問題

完全直方体が存在するか，という未解決問題がある ([10, D18]). 完全直方体とは，辺の長さ，面の対角線の長さ，立体の対角線の長さが全て有理数である直方体のことである．すなわち，

$$X^2+Y^2+Z^2=W_0^2,\quad X^2+Y^2=W_1^2,\quad Y^2+Z^2=W_2^2,\quad Z^2+X^2=W_3^2$$

の自明でない有理数解のことである．ここから派生して，四個の方程式のうち，一個を除いて，三個の方程式を同時に満たす有理数解は存在するか，という問題が考えられる．例えば，立体の対角線の有理性を諦めた場合，

$$X^2+Y^2=W_1^2,\quad Y^2+Z^2=W_2^2,\quad Z^2+X^2=W_3^2 \tag{1.6}$$

の解として，Euler は $(X,Y,Z,W_1,W_2,W_3)=(44,117,240,125,267,244)$ を与えた．さらに特殊な場合として，(1.6) の先頭の二つの方程式のみを考え，$X=1, Z=n$ (n は定められた有理数) とすると，

$$1+Y^2=W_1^2,\quad Y^2+n^2=W_2^2 \tag{1.7}$$

を得る．この方程式の有理数解を求める問題は Leech の問題と呼ばれることがある. (1.7) の非自明な有理数解 (Y,W_1,W_2) に対し，

$$x=\frac{n^2(W_2-W_1)}{n^2(Y+W_1)-(Y+W_2)}$$

と置くことにより，

$$L_n\ :\ y^2=x(x+1)(x+n^2)$$

の有理点を得る．$n\neq 0,\pm 1$ ならば，L_n は非特異であって，$L_n(\mathbb{Q})_{\mathrm{tors}}=\{\mathcal{O},(0,0),(-1,0),(-n^2,0),(n,\pm n(n+1)),(-n,\pm n(n-1))\}\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ である．これ以外の有理点 (x,y) が存在したならば，

$$Y=\left|\frac{(x+y+n^2)(x-y+n^2)}{2y(x+n^2)}\right|$$

と置くことにより，(1.7) の非自明な有理数解 (Y,W_1,W_2) を得る．したがって，(1.7) が非自明な有理数解を持つことと $\operatorname{rank}L_n(\mathbb{Q})>0$ は同値である．あらかじめ，n を n^2+1 が平方数となるように取っておき，運良く $\operatorname{rank}L_n(\mathbb{Q})>0$ となれば，(1.6) の有理数解が得られる．

例. (1) $n=24/7$ とすると，$\sqrt{n^2+1}=25/7$ である．さらにこの場合 $\operatorname{rank}F_n(\mathbb{Q})=1$ であって生成元として $(8,264/7)$ を得る．これより，(1.7) の解 $(Y,W_1,W_2)=(160/231,281/231,808/231)$ を得，(1.6) の解 $(X,Y,Z,W_1,W_2,W_3)=(1,160/231,24/7,281/231,808/231,25/7)$ を得る．一斉に $7\cdot 231$ 倍すれば，整数解 $(X,Y,Z,W_1,W_2,W_3)=(1617,1120,5544,1967,5656,5775)$ を得る．
(2) MacLeod [16] は $2\leq n\leq 999$ なる自然数 n に対して数値計算を行い，$n=502,808,863$ では $\operatorname{rank}F_n(\mathbb{Q})=1$ であるが，非自明な有理点が見付からなかったと報告している．しかし，$n=502$ については，高性能な数式処理ソフト MAGMA を用いることにより比較的簡単に次の有理点が見付かる．

$$\Bigg(\frac{68768536371492755934822942303945283279568763213285 62}{21809690151556369746749191231551096198815062089121},$$
$$\frac{16157618865691892222282545851695371948971404746410816155947890643214591448310554}{10185309806178639406228084149852276797746897557477596817270875033642140516 9}\Bigg).$$

1.4 Knight の問題

与えられた自然数 n に対し，

$$n = (X+Y+Z)\left(\frac{1}{X}+\frac{1}{Y}+\frac{1}{Z}\right) \tag{1.8}$$

の整数解を見付ける問題は Knight の問題と呼ばれることがある．(X,Y,Z) が解ならば，0 でない k に対して (kX,kY,kZ) も解であるから，整数解を見付けることと有理数解を見付けることは同等である．変数が二つで

$$n = (X+Y)\left(\frac{1}{X}+\frac{1}{Y}\right)$$

ならば $n = 0, 4$ のみで解を持ち，変数が四つで

$$n = (X+Y+Z+W)\left(\frac{1}{X}+\frac{1}{Y}+\frac{1}{Z}+\frac{1}{W}\right)$$

ならば任意の n に対して解

$$(X,Y,Z,W) = (m^2+m+1, m(m+1)(n-1), (m+1)(n-1), -m(n-1))$$

を持つ．変数が三つである (1.8) は，n によって解を持ったり持たなかったりする微妙な方程式なのである．(1.8) の整数解 (X,Y,Z) に対し，

$$x = \frac{-4(XY+YZ+ZX)}{Z^2}, \quad y = \frac{2(x-4n)Y}{Z} - (n-1)x$$

と置くことにより，

$$K_n : y^2 = x^3 + (n^2-6n-3)x^2 + 16nx$$

の有理点 (x,y) を得る．判別式は $2^{12}n^2(n-1)^3(n-9)$ なので，$n \neq 0, 1, 9$ のとき K_n は非特異であって，$K_n(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (0,0), (4, \pm 4(n-1)), (4n, \pm 4n(n-1))\} \cong \mathbb{Z}/6\mathbb{Z}$ である．これ以外の有理点 (x,y) が存在したならば，

$$X = y-(n-1)x, \quad Y = -y-(n-1)x, \quad Z = 2(4n-x)$$

と置くことにより，(1.8) の有理数解 (X,Y,Z) を得る．したがって，(1.8) が整数解を持つことと，$\operatorname{rank} K_n(\mathbb{Q}) > 0$ は同値である．Bremner ら [2] は，$-1000 \leq n \leq 1000$ に対して $\operatorname{rank} E_n(\mathbb{Q})$ を求めている．

例. $K_{11} : y^2 = x^3 + 52x^2 + 176x$ の階数は 1 であり，$(-4, 8)$ が生成元である．対応する (1.8) の解は $(2,3,6)$ である．すなわち，

$$11 = (2+3+6)\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{6}\right).$$

また，$2(-4,8) = (100, 1240)$ であって，対応する (1.8) の解は $(X,Y,Z) = (-15, 7, 140)$ である．

2 セルマー群

本節では，セルマー群について復習する．定義などについて詳しくは [21, chap.3], [20, chap.10] を参照されたい．§2.3 では，§4 で用いる予定の，[8] の結果を復習する．§1 の楕円曲線のセルマー群を手っ取り早く計算するためには，§2.1, 2.2 は最初は読み飛ばしても構わない．

2.1 セルマー群の定義

E, E' を $\mathbb{Q}$ 上定義された楕円曲線とし，$\mathbb{Q}$ 上の同種写像 $\varphi : E \to E'$ が存在すると仮定する．また，k は $\mathbb{Q}$ を含む体とする．$\mathrm{Gal}(\bar{k}/k)$-加群の完全系列

$$0 \to E[\,\varphi\,] \to E \xrightarrow{\varphi} E' \to 0$$

のガロアコホモロジーを取って，完全系列

$$0 \to E'(k)/\varphi(E(k)) \xrightarrow{\delta_k} H^1(k, E[\,\varphi\,]) \to H^1(k, E)[\,\varphi\,] \to 0$$

を得る．ここに，$E[\,\varphi\,] = \mathrm{Ker}(\varphi)$ であって，また，$H^1(k,E)[\,\varphi\,]$ は写像 $H^1(k,E) \xrightarrow{\varphi} H^1(k,E')$ の核を表す．δ_k は連結準同型と呼ばれる．$k = \mathbb{Q},\, \mathbb{Q}_p,\, \mathbb{R}$ のときは，δ_k をそれぞれ $\delta,\, \delta_p,\, \delta_\infty$ と略記する．さて，次の可換図式を考える．

$$\begin{array}{ccccccccc}
0 & \to & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[\,\varphi\,]) & \to & H^1(\mathbb{Q}, E)[\,\varphi\,] & \to & 0 \\
 & & \downarrow & & \downarrow \prod \mathrm{res}_p & & \downarrow & & \\
0 & \to & \prod E'(\mathbb{Q}_p)/\varphi(E(\mathbb{Q}_p)) & \xrightarrow{\prod \delta_p} & \prod H^1(\mathbb{Q}_p, E[\,\varphi\,]) & \to & \prod H^1(\mathbb{Q}_p, E)[\,\varphi\,] & \to & 0
\end{array}$$

ここに，$\prod$ は $\prod_{p \in M}$ $(M = \{\text{primes}\} \cup \{\infty\})$ を表す．(φ-) セルマー群 $S^{(\varphi)}(E/\mathbb{Q})$ とテイト-シャハレビッチ群 $Ш(E/\mathbb{Q})$ を次で定義する．

$$S^{(\varphi)}(E/\mathbb{Q}) = \mathrm{Ker}\left\{ H^1(\mathbb{Q}, E[\,\varphi\,]) \to \prod H^1(\mathbb{Q}_p, E)[\,\varphi\,] \right\},$$
$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left\{ H^1(\mathbb{Q}, E) \to \prod H^1(\mathbb{Q}_p, E) \right\}.$$

先の可換図式およびこれらの定義より，直ちに完全系列

$$0 \to E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \to S^{(\varphi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\,\varphi\,] \to 0 \tag{2.1}$$

を得る．$\varphi' : E' \to E$ を φ の双対写像とし，E と E' の役割を入れ替えると，もう一つの完全系列

$$0 \to E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) \to S^{(\varphi')}(E'/\mathbb{Q}) \to Ш(E'/\mathbb{Q})[\,\varphi'\,] \to 0 \tag{2.2}$$

を得る．

2.2 2-descent method

以下，E, E' は

$$E : y^2 = x^3 + Ax^2 + Bx,$$
$$E' : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$$

で与えられているとする．ただし，$A, B \in \mathbb{Z}$ であって，$B(A^2 - 4B) \neq 0$ とする．E, E' の間には，2 次の同種写像

$$\varphi : E \to E' \quad (\mathcal{O}_E, (0,0) \mapsto \mathcal{O}_{E'},\ (x,y) \mapsto (y^2/x^2,\, y(B - x^2)/x^2)),$$
$$\varphi' : E' \to E \quad (\mathcal{O}_{E'}, (0,0) \mapsto \mathcal{O}_E,\ (x,y) \mapsto (y^2/(4x^2),\, y(A^2 - 4B - x^2)/(8x^2)))$$

が存在し，$\varphi' \circ \varphi = [2]_E$, $\varphi \circ \varphi' = [2]_{E'}$ である．完全系列

$$0 \to \frac{E'(\mathbb{Q})[\,\varphi'\,]}{\varphi(E(\mathbb{Q})[\,2\,])} \to \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \xrightarrow{\varphi'} \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\varphi'(E'(\mathbb{Q}))} \to 0$$

より，

$$\dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) = \dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) + \dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) - \dim_{\mathbb{F}_2} E'(\mathbb{Q})[\,\varphi'\,]/\varphi(E(\mathbb{Q})[\,2\,])$$

であり，

$$\dim_{\mathbb{F}_2} E'(\mathbb{Q})[\,\varphi'\,]/\varphi(E(\mathbb{Q})[\,2\,]) = \begin{cases} 0 & (\,A^2-4B \text{ が平方数のとき}) \\ 1 & (\text{その他の場合}) \end{cases}$$

$$\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) + \begin{cases} 2 & (\,A^2-4B \text{ が平方数のとき}) \\ 1 & (\text{その他の場合}) \end{cases}$$

より，階数の公式

$$\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) + \dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) - 2 \tag{2.3}$$

を得る．また，(2.1), (2.2) より

$$\dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) = \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш\,(E'/\mathbb{Q})[\,\varphi'\,],$$
$$\dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) = \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш\,(E/\mathbb{Q})[\,\varphi\,]$$

であるから，

$$\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш\,(E/\mathbb{Q})[\,\varphi\,] - \dim_{\mathbb{F}_2} Ш\,(E'/\mathbb{Q})[\,\varphi'\,] - 2$$

であって，特に

$$\operatorname{rank} E(\mathbb{Q}) \le \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - 2 \tag{2.4}$$

が成り立つ．右辺を (φ-) セルマー階数と呼ぶ．

さて，$\delta : E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \to H^1(\mathbb{Q}, E[\,\varphi\,])$ や $\delta' : E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) \to H^1(\mathbb{Q}, E'[\,\varphi'\,])$ は単射であるから，(2.3) は

$$\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} \operatorname{Im}(\delta') + \dim_{\mathbb{F}_2} \operatorname{Im}(\delta) - 2$$

と書き直せる．すなわち，δ, δ' の像が分かれば，階数が求まる．$E[\,\varphi'\,] = \{\mathcal{O}_E, (0,0)\} \cong \mathbb{Z}/2\mathbb{Z}$ より $H^1(\mathbb{Q}, E[\,\varphi'\,]) \cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ である．δ' より導かれる写像 $E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ も δ' と書くことにすると，連結準同型の定義から

$$\delta'(P) = \begin{cases} x & (\,P = (x,y) \neq \mathcal{O}, (0,0) \text{ のとき}) \\ B & (\,P = (0,0) \text{ のとき}) \\ 1 & (\,P = \mathcal{O} \text{ のとき}) \end{cases} \tag{2.5}$$

を得る．よって，連結準同型の像を求めるには，有理点の x 座標に現れる数を (平方数を法として) 決定すればよい．$(x,y) \neq \mathcal{O}, (0,0)$ に対して $\delta'((x,y)) = d$ とすると，

$$x = \frac{dM^2}{e^2}, \quad y = \frac{dMN}{e^3}$$

と表せる．ここに，M, N, e は 0 でない整数で，$(M,e) = (N,e) = 1$ を満たす．E の式より，

$$N^2 = dM^4 + AM^2e^2 + \frac{B}{d}e^4 \tag{2.6}$$

を得る．これより，$d \in \mathrm{Im}(\delta')$ であるためには $d \mid B$ が必要である．逆に，この不定方程式の解 (M, N, e) が存在すれば，$d \in \mathrm{Im}(\delta')$ である．同様に，

$$N^2 = dM^4 - 2AM^2e^2 + \frac{A^2 - 4B}{d}e^4$$

が $MNe \neq 0, (M, e) = (N, e) = 1$ なる整数解 (M, N, e) を持つことが，$d \in \mathrm{Im}(\delta)$ と同値であって，そのためには $d \mid (A^2 - 4B)$ が必要である．しかし，これらの不定方程式は四次式であるため，整数解が存在するか否かを判定する方法は現在のところ知られていない．

さて，セルマー群の定義と，先の可換図式の完全性より

$$\begin{aligned} S^{(\varphi)}(E/\mathbb{Q}) =& \{x \in H^1(\mathbb{Q}, E[\varphi]) \mid \mathrm{res}_p(x) \in \mathrm{Im}(\delta_p) \text{ for } \forall p\} \\ =& \bigcap_p \mathrm{Im}(\delta_p) \end{aligned}$$

である．ただし，res_p の引き戻しにより，$\mathrm{Im}(\delta_p)$ を $H^1(\mathbb{Q}, E[\varphi])\,(\cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2})$ の部分群と見なしている．したがって，大雑把に言って，セルマー群は連結準同型たちの共通部分である．同様に，

$$S^{(\varphi')}(E'/\mathbb{Q}) = \bigcap_p \mathrm{Im}(\delta'_p)$$

である．同型 $H^1(\mathbb{Q}_p, E'[\varphi']) \cong \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ によって，δ'_p を $E(\mathbb{Q})$ から $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ への写像と考えると，δ'_p は (2.5) と同じ式で与えられ，よって，$d \in \mathrm{Im}(\delta'_p)$ であることは，(2.6) が p 進数解を持つことと同値である．このことは判定可能であり，セルマー群は計算可能である．しかし，一般に，全ての p で p 進数解を持つからといって有理数解を持つとは限らない．その局所大域原理とのずれを表すものがテイト-シャハレビッチ群であり，この部分が階数を計算することを難しくしている．

2.3 連結準同型の像

§2.1, 2.2 の内容を要約すると，位数 2 の有理点を持つ楕円曲線 E と $\varphi' \circ \varphi = [2]_E$, $\varphi \circ \varphi' = [2]_{E'}$ なる φ, φ' に対し，

$$S^{(\varphi)}(E/\mathbb{Q}) = \bigcap_p \mathrm{Im}(\delta), \quad S^{(\varphi')}(E'/\mathbb{Q}) = \bigcap_p \mathrm{Im}(\delta')$$

で与えられるセルマー群を用いて，階数が

$$\mathrm{rank}\, E(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - 2$$

と評価される．筆者の以前の結果 [9] では，位数 2 の有理点を持つ任意の楕円曲線と任意の p に対し，連結準同型の像 $\mathrm{Im}(\delta_p)$, $\mathrm{Im}(\delta'_p)$ を具体的に書き下しており，これを用いるとセルマー群を簡単に計算することができる．

ここでは，$E_{n,\pi/3}$ に関する §4 の定理の証明のために必要な部分のみ復習する．簡単のために，以下の形の楕円曲線のみを考える (cf. [8])．

$$y^2 = x(x - \alpha)(x - \beta).$$

ここに，α, β は相異なる 0 でない有理数とする．必要ならば変数変換をすることにより，α, β は整数であって，$\gcd(\alpha, \beta)$ は平方因子を含まないとしてよい．$E(\mathbb{R})$ の描く軌跡より明らかなように，$\mathrm{Im}(\delta'_\infty)$, $\mathrm{Im}(\delta_\infty)$ は次で与えられる．

- $\alpha > 0$ かつ $\beta > 0$ ならば $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2},\ \mathrm{Im}(\delta_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$.
- $\alpha < 0$ または $\beta < 0$ ならば $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2},\ \mathrm{Im}(\delta_\infty) = \mathbb{R}^{\times 2}/\mathbb{R}^{\times 2}$.

また，一般に p が判別式を割らない奇素数ならば，

$$\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2},\ \mathrm{Im}(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$$

である．

以下，素数 p に対して $p^e \mid N$ かつ $p^{e+1} \nmid N$ であるときに $\mathrm{ord}_p(N) = e$ と書くことにする．また，$c_1, \cdots, c_n$ で生成される $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ または $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ の部分群を $\langle c_1, \cdots, c_n\rangle$ で表す．

補題 2.1 $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 0$ とすると，以下の場合を除いて $\mathrm{Im}(\delta'_2) = \langle \alpha, \beta\rangle$ である．
(1) $\mathrm{ord}_2(\alpha - \beta) = 2$ かつ $\alpha + \beta \equiv 14 \pmod{16}$ ならば $\mathrm{Im}(\delta'_2) = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
(2) $\mathrm{ord}_2(\alpha - \beta) = 3$ かつ $\alpha \equiv 3 \pmod 4$ ならば $\mathrm{Im}(\delta'_2) = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
(3) $\mathrm{ord}_2(\alpha - \beta) = 4$ かつ $\alpha \equiv 1 \pmod 8$ ならば $\mathrm{Im}(\delta'_2) = \langle 5\rangle$.

補題 2.2 $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 1$ のとき，以下が成り立つ．
(1) $\mathrm{ord}_2(\alpha - \beta) = 2$ ならば $\mathrm{Im}(\delta'_2) = \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.
(2) $\mathrm{ord}_2(\alpha - \beta) = 3$ ならば $\mathrm{Im}(\delta'_2) = \langle \alpha, 5\rangle$.
(3) $\mathrm{ord}_2(\alpha - \beta) \geq 4$ ならば $\mathrm{Im}(\delta'_2) = \langle \alpha\rangle$.

補題 2.3 p を奇素数とする．$\mathrm{ord}_p(\alpha) = a \geq 1$ かつ $p \nmid \beta$ であるとき，次が成り立つ．
(1) a が偶数かつ $(-\beta/p) = -1$ ならば $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.
(2) その他の場合は $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

補題 2.4 p を奇素数とする．$\mathrm{ord}_p(\alpha) \geq 1$, $\mathrm{ord}_p(\beta) = 1$ ならば $\mathrm{Im}(\delta'_p) = \langle \alpha, \beta\rangle$ である．

これらの補題より，$\pi/3$-合同数問題に対応した楕円曲線 $E_{n,\pi/3} : y^2 = x(x+3n)(x-n)$ に関して，直ちに次を得る．

補題 2.5 $E_{n,\pi/3}$ に対して，連結準同型の像 $\mathrm{Im}(\delta'_p)$ は次で与えられる．
(1) $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$.
(2) $\mathrm{Im}(\delta'_2) = \begin{cases} \langle 5\rangle & (n \equiv 5 \pmod 8 \text{ のとき}) \\ \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & (n \equiv \pm 1, -5 \pmod 8 \text{ のとき}) \\ \langle 2, 5\rangle & (n \equiv 2 \pmod 8 \text{ のとき}) \\ \langle -2, 5\rangle & (n \equiv -2 \pmod 8 \text{ のとき}) \end{cases}$
(3) $\mathrm{Im}(\delta'_3) = \begin{cases} \langle -3\rangle & (n \equiv 6 \pmod 9 \text{ のとき}) \\ \mathbb{Q}_3^\times/\mathbb{Q}_3^{\times 2} & (n \not\equiv 6 \pmod 9 \text{ のとき}) \end{cases}$
(4) $p \neq 2, 3$ かつ $p \mid n$ ならば

$$\mathrm{Im}(\delta'_p) = \begin{cases} \langle n\rangle & (p \equiv 1 \pmod 3 \text{ のとき}) \\ \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} & (p \equiv -1 \pmod 3 \text{ のとき}) \end{cases}$$

次の補題により，$\mathrm{Im}(\delta'_p)$ と $\mathrm{Im}(\delta_p)$ の一方が分かれば，他方も分かる．$(*,*)_p$ をヒルベルト記号とし，$V \subset \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ に対して，$V^\perp = \{x \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \mid (x, y)_p = 1\ (\forall y \in V)\}$ と定義する．

補題 2.6 $\mathrm{Im}(\delta_p) = \mathrm{Im}(\delta'_p)^\perp$.

補題 2.5, 2.6 より，直ちに次を得る．

補題 2.7 $E_{n,\pi/3}$ に対して，連結準同型 $\mathrm{Im}(\delta_p)$ の像は次で与えられる．

(1) $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^{\times 2}/\mathbb{R}^{\times 2}$.

(2) $\mathrm{Im}(\delta_2) = \begin{cases} \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & (n \equiv 5 \pmod 8 \text{ のとき}) \\ \langle 5 \rangle & (n \equiv \pm 1, -5 \pmod 8 \text{ のとき}) \\ \langle -1 \rangle & (n \equiv 2 \pmod 8 \text{ のとき}) \\ \langle -5 \rangle & (n \equiv -2 \pmod 8 \text{ のとき}) \end{cases}$

(3) $\mathrm{Im}(\delta_3) = \begin{cases} \langle 3 \rangle & (n \equiv 6 \pmod 9 \text{ のとき}) \\ \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & (n \not\equiv 6 \pmod 9 \text{ のとき}) \end{cases}$

(4) $p \neq 2, 3$ かつ $p \mid n$ ならば，

$$\mathrm{Im}(\delta_p) = \begin{cases} \langle -n \rangle & (p \equiv 1 \pmod 3 \text{ のとき}) \\ \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2} & (p \equiv -1 \pmod 3 \text{ のとき}) \end{cases}$$

平方因子を含まない自然数 $n = p_1 \cdots p_r$ に対し，

$$K_n = \langle -1, 2, 3, p_1, \cdots, p_r \rangle \subset \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

と置くと，$S^{(\varphi)}(E_{n,\pi/3}/\mathbb{Q}) \subset K_n$, $S^{(\varphi')}(E'_{n,\pi/3}/\mathbb{Q}) \subset K_n$ である．補題 2.5, 2.7 はより素朴に次のように言い換えられる．

補題 2.8 $d \in K_n$ とする．$E_{n,\pi/3}$ に対して次が成り立つ．

(1) $d \in \mathrm{Im}(\delta'_\infty)$.

(2) $2 \mid d$ なる d に対して $d \in \mathrm{Im}(\delta'_2) \Leftrightarrow 2 \mid n$ かつ $d \equiv n \pmod 8$.

(3) $2 \nmid d$ なる d に対して $d \notin \mathrm{Im}(\delta'_2) \Leftrightarrow n \equiv 5, \pm 2 \pmod 8$ かつ $d \equiv 3 \pmod 4$.

(4) $3 \mid d$ なる d に対して $d \notin \mathrm{Im}(\delta'_3) \Leftrightarrow n \equiv 6 \pmod 9$ かつ $(\frac{d/3}{3}) = 1$.

(5) $3 \nmid d$ なる d に対して $d \notin \mathrm{Im}(\delta'_3) \Leftrightarrow n \equiv 6 \pmod 9$ かつ $(\frac{d}{3}) = -1$.

(6) $p \mid d$ なる d に対して $d \notin \mathrm{Im}(\delta'_p) \Leftrightarrow p \equiv 1 \pmod 3$ かつ $(\frac{n/d}{p}) = -1$.

(7) $p \nmid d$ なる d に対して $d \notin \mathrm{Im}(\delta'_p) \Leftrightarrow p \equiv 1 \pmod 3$ かつ $(\frac{d}{p}) = -1$.

補題 2.9 $d \in K_n$ とする．$E_{n,\pi/3}$ に対して次が成り立つ．

(1) $d \in \mathrm{Im}(\delta_\infty) \Leftrightarrow d > 0$.

(2) $2 \mid d$ なる d に対して $d \notin \mathrm{Im}(\delta_2)$.

(3) $2 \nmid d$ なる d に対して $d \in \mathrm{Im}(\delta_2)$ であるための必要十分条件は，以下の四条件のいずれかが成り立つことである．

(a) $n \equiv 5 \pmod 8$.

(b) $n \equiv \pm 1, -5 \pmod 8$ かつ $(\frac{-1}{d}) = 1$.

(c) $n \equiv 2 \pmod 8$ かつ $(\frac{2}{d}) = 1$.

(d) $n \equiv -2 \pmod 8$ かつ $(\frac{-2}{d}) = 1$.

(4) $3 \mid d$ なる d に対して $d \in \mathrm{Im}(\delta_3) \Leftrightarrow n \equiv 6 \pmod 9$ かつ $(\frac{d/3}{3}) = 1$.

(5) $3 \nmid d$ なる d に対して $d \in \mathrm{Im}(\delta_p) \Leftrightarrow (\frac{d}{3}) = 1$.

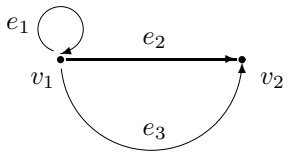
(6) $p \mid d$ なる $p \neq 2, 3$ に対して $d \in \mathrm{Im}(\delta_p) \Leftrightarrow p \equiv 1 \pmod 3$ かつ $(\frac{-n/d}{p}) = 1$.

(7) $p \nmid d$ なる $p \neq 2, 3$ に対して $d \in \mathrm{Im}(\delta_p) \Leftrightarrow (\frac{d}{p}) = 1$.

3　グラフ理論からの準備

本節では，奇グラフについて定義を述べ，Feng and Xiong [5] の結果を紹介する．

V, E を有限集合とし，写像 $\psi : E \to V \times V$ を合わせた三つ組 (V, E, ψ) を有向グラフと呼ぶ．$G = (V, E, \psi)$ のとき，V を $V(G)$，E を $E(G)$ と表すこともある．ψ が明らかであるとき，省略して $G = (V, E)$ と書くこともある．V の元を頂点，E の元を弧と呼ぶ．例えば，$V = \{v_1, v_2\}$, $E = \{e_1, e_2, e_3\}$, $\psi(e_1) = (v_1, v_1)$, $\psi(e_2) = (v_1, v_2)$, $\psi(e_3) = (v_1, v_2)$ で与えられるグラフ $G = (V, E, \psi)$ は次のように図示される．



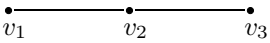
有向グラフ $G = (V, E, \psi)$ は次の二条件を満たすとき，単純グラフと呼ばれる．

- 任意の $e \in E$ に対して $\psi(e) \notin \mathrm{diag}(V) := \{(v, v) \mid v \in V\}$．
- 写像 ψ が単射．

以後，単純グラフのみを考え，$\psi(E)$ の元は E の元と同一視する．$(v, w) \in E$ のとき，この弧を $\overrightarrow{vw}$ で表す．また，(v, w), $(w, v) \in E$ のとき，$\overline{vw}$ でこの二つの弧を表すことにし，これを辺と呼ぶ．図示するときは，頂点 v, w を矢印無しの線分で結ぶ．全ての弧が辺の一部であるとき，すなわち条件

$$(v, w) \in E(G) \Rightarrow (w, v) \in E(G)$$

を満たすとき，G を無向グラフと呼ぶ．例えば，$V(G) = \{v_1, v_2, v_3\}$, $E(G) = \{\overline{v_1v_2}, \overline{v_2v_3}\} = \{(v_1, v_2), (v_2, v_1), (v_2, v_3), (v_3, v_2)\}$ で与えられる無向グラフ G は次のように図示する．



定義.　$G = (V, E)$ を単純有向グラフとする．

- $V_1 \cup V_2 = V$ かつ $V_1 \cap V_2 = \emptyset$ であるとき，$\{V_1, V_2\}$ を V の分割と呼ぶ．
- $V_1 = \emptyset$ または $V_2 = \emptyset$ のとき，分割 $\{V_1, V_2\}$ を自明な分割と呼ぶ．
- ある $v \in V_1$ が存在して $\#\{v \to V_2\}$ が奇数であるか，ある $v \in V_2$ が存在して $\#\{v \to V_1\}$ が奇数であるとき，分割 $\{V_1, V_2\}$ は奇であるという．
- 奇でない分割は偶であるという．
- 非自明な分割が全て奇であるとき，グラフ G は奇であるという．
- 奇でないグラフは偶であるという．
- 非自明で偶な分割が唯一つ存在するとき，グラフ G は準奇であるという．

明らかに，不連結なグラフは偶である．また，以下のグラフは奇である (cf. [5])．

- 有向サイクル：$V = \{v_1, \cdots, v_m\}$, $E = \{\overrightarrow{v_1v_2}, \overrightarrow{v_2v_3}, \cdots, \overrightarrow{v_{m-1}v_m}, \overrightarrow{v_mv_1}\}$.
- 頂点の個数が奇数である無向サイクル：
  m：奇数, $V = \{v_1, \cdots, v_m\}$, $E = \{\overline{v_1v_2}, \overline{v_2v_3}, \cdots, \overline{v_{m-1}v_m}, \overline{v_mv_1}\}$.
- 頂点の個数が奇数である完全グラフ (全ての頂点が辺で結ばれている無向グラフ)．
- 木 (辺を一つでも除くと不連結になる，連結無向グラフ)．

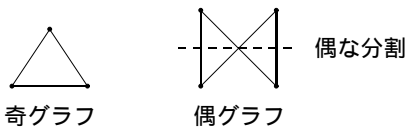


Figure 1: 無向サイクル．

グラフが奇か否かは，線形代数の用語を用いて表すことができる．G を有向グラフとし，その頂点集合を $V(G) = \{v_1, \cdots, v_m\}$ とする．G の隣接行列 $A(G) = (a_{ij})_{1 \le i,j \le m}$ は次で定義される．

$$a_{ij} = \begin{cases} 1 & \overrightarrow{v_iv_j} \in E(G) \text{ のとき}, \\ 0 & \text{その他の場合}. \end{cases}$$

頂点 v_i を起点とする弧の個数を d_i とする．すなわち，

$$d_i = \sum_{j=1}^{m} a_{ij}.$$

G の Laplace 行列 $L(G)$ を

$$L(G) = \mathrm{diag}(d_1, \cdots, d_m) - A(G)$$

で定義する．定義より $L(G)$ の各行の和は 0 であるので，$\mathrm{rank}_{\mathbb{Z}}(L(G)) \le m-1$ である．

命題 3.1 ([4], [5]) G を有向グラフとし，$m = |V(G)|$, $r = \mathrm{rank}_{\mathbb{F}_2} L(G)$ と置く．このとき，$V(G)$ の偶な分割の個数は 2^{m-r-1} に等しい．特に，G が奇グラフであるための必要十分条件は $r = m-1$ であり，G が準奇グラフであるための必要十分条件は $r = m-2$ である．

G を無向グラフとする．G の部分グラフ H が spanning tree であるとは，tree (木) であって，$V(G) = V(H)$ であることを意味する．上記の命題と Kirchhoff の定理 ([11, §1.2.4], 連結無向グラフの spanning tree の個数は，Laplace 行列の任意の余因子の絶対値に等しい) より直ちに次を得る．

命題 3.2 ([5]) 無向グラフ G が奇グラフであるための必要十分条件は，G の spanning tree の個数が奇数であることである．

例えば，Figure 1 の，頂点の個数が 4 である無向サイクルは，4 個の spanning tree を持つので偶グラフである．

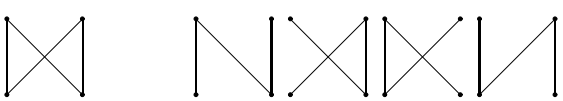


Figure 2: Spanning trees.

以下に [5] の結果の一つを紹介する．

定義. 奇数 $n = p_1 \cdots p_t$ に対して，有向グラフ $G(n)$ を次で定義する．

$$V(G(n)) = \{p_1, \cdots, p_t\}, \quad E(G(n)) = \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\}.$$

すなわち，$G(n)$ は，頂点は n の素因子で，ルジャンドル記号が -1 のときに弧で結ばれているというグラフである．平方剰余の相互法則により，$\bmod 4$ で 3 の素数同士は必ず片方向の弧で結ばれ，そうでない場合は，結ばれないか双方向で結ばれる (すなわち辺で結ばれる) かのいずれかである．

定理 **3.3** ([5]) $n = p_1 \cdots p_t \equiv 3 \pmod 8$ とする．E_n のセルマー階数が 0 であるための必要十分条件は，次の二条件を満たすことである．
(1) $p_1 \equiv 3 \pmod 4$ かつ $p_i \equiv 1 \pmod 4$ $(i \ge 2)$.
(2) $G(n)$ は奇グラフである．

例. §1 で述べたように，次の n は合同数でない．

$$n = pqr, \ (p,q,r) \equiv (1,1,3) \pmod 8, \ (p/q), (p/r), (q/r) \text{ のうち，少なくとも二つが } -1.$$

このことは，定理 3.3 を用いると，次のグラフが奇であることからすぐに従う．

E_n のセルマー階数が偶数であるための必要十分条件は $n \equiv 1, 2, 3 \pmod 8$ であることが知られている (cf. [1], [18]). Feng and Xiong [5] は $n \equiv 1, 2 \pmod 8$ の場合も同様にセルマー階数が 0 であるための必要十分条件を与えているが，その場合は上の定理に比べてやや複雑な条件になる．

4 $\pi/3$-合同数問題

本節では，$\pi/3$-合同数問題での，定理 3.3 に相当する定理を与える．

定義. 奇数 $n = p_1 \cdots p_t$ に対して二つのグラフ $g(n)$, $g'(n)$ を次で定義する．

$$\begin{aligned}
V(g(n)) &= \{-1, p_1, \cdots, p_t\}, \\
E(g(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\} \\
&\qquad \cup \left\{ \overrightarrow{p_i(-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}, \\
V(g'(n)) &= \{-1, (-1)', p_1, \cdots, p_t\}, \\
E(g'(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\} \\
&\qquad \cup \left\{ \overrightarrow{p_i(-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\} \\
&\qquad \cup \left\{ \overrightarrow{p_i(-1)'} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}.
\end{aligned}$$

$g'(n)$ の定義より，$V(g'(n))$ の分割 $V_1 = \{-1, (-1)'\}$, $V_2 = V(g'(n)) \setminus V_1$ は常に偶である．

定理 4.1 $n \equiv 1, 7, 19 \pmod{24}$ とする．$E_{n,\pi/3}$ のセルマー階数が 0 であるための必要十分条件は次の三条件を満たすことである．

(1) $\forall p \mid n,\ p \equiv 1 \pmod{3}$.

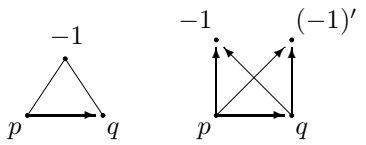
(2) $g(n)$ は奇グラフ．

(3) $g'(n)$ は準奇グラフ．

例. §1 で述べたように，次の n は $\pi/3$-合同数でない．

$$n = pq,\ (p, q) \equiv (7, 7) \pmod{8}.$$

定理 4.1 を用いてこのことを確かめよう．$(p/q) = -1$ と仮定しても一般性は失われない．このとき $g(n)$, $g'(n)$ はそれぞれ次のようになる．



$g(n)$ は奇，$g'(n)$ は準奇である．実際，それぞれの Laplace 行列は，

$$L(g(n))_{\mathbb{F}_2} = \begin{array}{c} \\ -1 \\ p \\ q \end{array} \begin{array}{c} \begin{array}{ccc} -1 & p & q \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \end{array}, \qquad L(g'(n))_{\mathbb{F}_2} = \begin{array}{c} \\ -1 \\ (-1)' \\ p \\ q \end{array} \begin{array}{c} \begin{array}{cccc} -1 & (-1)' & p & q \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

であるから，$\operatorname{rank}_{\mathbb{F}_2}(L(g(n))) = \operatorname{rank}_{\mathbb{F}_2}(L(g'(n))) = 2$ である．

$E_{n,\pi/3}$ のセルマー階数が 0 であるための必要十分条件は

$$n \equiv 1, 2, 3, 5, 7, 9, 14, 15, 19 \pmod{24}$$

である (cf. [14], [18], [22])．補題 2.8, 2.9 を用いて $n \equiv 2, 3, 5, 9, 14, 15 \pmod{24}$ の場合もセルマー階数が 0 であるための条件を与えられるが，やや複雑になる．

その他の角 θ に関する θ-合同数問題や，他の古典的 Diophantus 問題に関係する楕円曲線のセルマー群について考えるのも面白いだろう．楕円曲線によっては，グラフの定義が複雑になったり，グラフ以外の条件 (定理 3.3, 4.1 の (1) に相当する部分) が複雑になったり，そもそもグラフを考える必要がなかったりするかもしれない．

残りの紙面で，定理 4.1 を証明する．簡単のために $S^{(\varphi)}(E_{n,\pi/3}/\mathbb{Q}), S^{(\varphi')}(E'_{n,\pi/3}/\mathbb{Q})$ をそれぞれ S_n, S'_n と略記する．$E_{n,\pi/3}$ のセルマー階数は $\dim_{\mathbb{F}_2} S_n + \dim_{\mathbb{F}_2} S'_n - 2$ であった．$\{1, n, -3n, -3\} \subset S'_n$ は明らかである．

定義. n は奇数で，$n = p_1 \cdots p_t q_1 \cdots q_s$, $p_i \equiv 1 \pmod 3$, $q_j \equiv -1 \pmod 3$ とする．有向グラフ $h'(n)$ を次で定義する．

$$\begin{aligned}
V(h'(n)) &= \{-1, (-1)', p_1, \cdots, p_t, q_1, \cdots, q_s\}, \\
E(h'(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\} \\
&\quad \cup \left\{ \overrightarrow{p_i q_j} \;\middle|\; \left(\frac{q_j}{p_i}\right) = -1 \ (1 \le i \le t,\, 1 \le j \le s) \right\} \\
&\quad \cup \left\{ \overrightarrow{p_i (-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\} \\
&\quad \cup \left\{ \overrightarrow{p_i (-1)'} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}.
\end{aligned}$$

補題 4.2 $n \equiv 1, 7, 19 \pmod{24}$ とする．$S'_n = \{1, n, -3n, -3\}$ であるための必要十分条件は，有向グラフ $h'(n)$ が準奇であることである．

証明. $h'(n)$ が準奇グラフであるとすると，$V := V(h'(n))$ の $\{\emptyset, V\}$, $\{\{-1, (-1)'\}, V \backslash \{-1, (-1)'\}\}$ 以外の分割 $\{V_1, V_2\}$ は奇である．$d = \prod V_1$ と置くと，$d \ne 1, n$ である．分割が奇であるから，次の少なくとも一方が成り立つ．

- ある $p_i \in V_1$ が存在して $\#\{p_i \to V_2\}$ が奇数である，すなわち $(\frac{n/d}{p}) = -1$.
- ある $p_i \in V_2$ が存在して $\#\{p_i \to V_1\}$ が奇数である，すなわち $(\frac{d}{p}) = -1$.

いずれの場合も補題 2.8 (6), (7) より $d \notin \mathrm{Im}(\delta'_p)$ である．以上で $\langle -1, p_1, \cdots, p_t, q_1, \cdots, q_s \rangle \setminus \{1, n\}$ の任意の元はセルマー群 S'_n に属していないことが示された．したがって，S'_n は自明な元のみを持ち，$S'_n = \{1, n, -3n, -3\}$ である．

逆に，$h'(n)$ が準奇でないと仮定すると，$V := V(h'(n))$ の偶な分割 $\{V_1, V_2\}$ で $\{\emptyset, V\}$ でも $\{\{-1, (-1)'\}, V \backslash \{-1, (-1)'\}\}$ でもないものが存在する．$d = \prod V_1$ と置くと $d \ne 1, n$ である．補題 2.8 (1), (3), (5), (6), (7) より，$d \in \mathrm{Im}(\delta'_\infty), \mathrm{Im}(\delta'_2), \mathrm{Im}(\delta'_3), \mathrm{Im}(\delta'_{q_j})$ である．分割が偶であるから，次の両方が成り立つ．

- 任意の $p_i \in V_1$ に対して $\#\{p_i \to V_2\}$ が偶数である，すなわち $(\frac{n/d}{p}) = 1$.
- 任意の $p_i \in V_2$ に対して $\#\{p_i \to V_1\}$ が偶数である，すなわち $(\frac{d}{p}) = 1$.

したがって，$d \in \mathrm{Im}(\delta'_{p_i})$ となり，S'_n は非自明な元 d を持つ． □

上記の証明では，実際には次を示している．

$$\mathrm{rank}_{\mathbb{F}_2} S'_n = t + s + 2 - \mathrm{rank}_{\mathbb{F}_2} L(h'(n)).$$

$s \ge 2$ ならば，少なくとも $L(h'(n))$ の四つの行が全て 0 であるので，セルマー階数は正になる．$s = 1$ とすると，$n \equiv 2 \pmod 3$ となって仮定に反する．したがって，セルマー階数が 0 となるのは，$s = 0$ の場合に限られ，この場合には $h'(n) = g'(n)$ であるから，次の補題を確かめたことになる．

補題 4.3 $n \equiv 1, 7, 19 \pmod{24}$ とする．$S'_n = \{1, n, -3n, -3\}$ であることと，n の全ての素因子 p が $p \equiv 1 \pmod 3$ を満たし，かつ $g'(n)$ は準奇グラフであることは同値である．

定理 4.1 の証明を完成するには，次の補題を示さなければならない．

補題 4.4 $n = p_1 \cdots p_t \equiv 1, 7, 19 \pmod{24}$, $p_i \equiv 1 \pmod 3$ とする．$S_n = \{1\}$ であるための必要十分条件は，$g(n)$ が奇グラフであることである．

証明. 補題 2.9 (1), (2), (4) より $S_n \subset \langle p_1, \cdots, p_t \rangle$ である．$g(n)$ が奇グラフであるとすると，任意の非自明な $V(g(n))$ の分割 $\{V_1, V_2\}$ は奇である．一般性を失わずに $-1 \notin V_1$, $-1 \in V_2$ と仮定してよい．$d = \prod V_1$ と置くと，$d \neq 1$ である．分割が奇であるから，次の三条件のいずれかが成り立つ．

- ある $p_i \in V_1$ が存在して $\#\{p_i \to V_2\}$ が奇数である，すなわち $(\frac{-n/d}{p}) = -1$.
- ある $p_i \in V_2$ が存在して $\#\{p_i \to V_1\}$ が奇数である，すなわち $(\frac{d}{p}) = -1$.
- $\#\{-1 \to V_1\}$ が奇数である，すなわち $(\frac{-1}{d}) = -1$.

補題 2.9 (3), (6), (7) より $d \notin \mathrm{Im}(\delta_p)$ または $d \notin \mathrm{Im}(\delta_2)$ である．いずれの場合も $d \notin S_n$ である．

逆に，$g(n)$ が偶グラフであるとすると，$V(g(n))$ の非自明な偶の分割 $\{V_1, V_2\}$ が存在する．一般性を失わずに $-1 \notin V_1$, $-1 \in V_2$ としてよい．$d = \prod V_1$ と置くと $d \neq 1$ である．補題 2.9 (1) より，$d \in \mathrm{Im}(\delta_\infty)$ である．分割が偶であるから，$d \in \mathrm{Im}(\delta_2)$ かつ任意の i に対して $d \in \mathrm{Im}(\delta_{p_i})$ である．$p_i \equiv 1 \pmod 3$ より $d \equiv 1 \pmod 3$ であるから，$d \in \mathrm{Im}(\delta_3)$ となり，S_n は非自明な元 d を持つ．□

補題 4.3, 4.4 より直ちに定理 4.1 を得る．

参考文献

[1] N. Aoki, *On the* 2*-Selmer groups of elliptic curves arising from the congruent number problem*, Comment. Math. Univ. St. Paul., **48** (1999), 77–101.

[2] A. Bremner, R. K. Guy and R. J. Nowakowski, *Which integers are representable as the product of the sum of three integers with the sum of their reciprocals?*, Math. Comp., **61** (1993), 117–130.

[3] M. Fujiwara, *θ-congruent numbers*, in: Number Theory, de Gruyter, Berlin, 1998, 235–241.

[4] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. **80** (1996), 71–83.

[5] K. Feng and M. Xiong, *On elliptic curves* $y^2 = x^3 - n^2x$ *with rank zero*, J. Number Theory **109** (2004), 1-26.

[6] A. Genocchi, *Sur l'impossibilite de quelques egalites doubles*, C. R. Acad. Sci. Paris, **78** (1874), 423–436.

[7] T. Goto, *A note on the Selmer group of the elliptic curve* $y^2 = x^3 + Dx$, Proc. Japan Acad., **77A** (2001), 122–125.

[8] T. Goto, *Calculation of Selmer groups of elliptic curves with rational 2-torsions and θ-congruent number problem*, Comment. Math. Univ. St. Paul., **50** (2001), 147–172.

[9] T. Goto, *A study on the Selmer groups of the elliptic curves with a rational* 2*-torsion*, Doctoral Thesis, Kyushu University, 2002 (`http://www.ma.noda.tus.ac.jp/u/tg/files/thesis.pdf`).

[10] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, New York, 2004.

[11] J. M. Harris, J. L. Hirst and M. J. Mossinghoff, *Combinatorics and Graph Theory*, Undergrad. Texts Math., Springer, New York, 2000.

[12] M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith., **94** (2000), 153–160.

[13] A. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, 1992.

[14] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. 97, Springer, 1984.

[15] J. Lagrange, *Nombres congruents et courbes elliptiques*, Sém. Delange-Pisot-Poitou, 16e année, 1974/75, no. 16, 17pp.

[16] A. J. MacLeod, *On a problem of John Leech*, Expo. Math., **23** (2005), 271–279.

[17] P. Monsky, *Appendix* in: D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem II*, Invent. Math., **118** (1994), 331–370.

[18] P. Monsky, *Generalizing the Birch-Stephens theorem I*, Math. Z., **221** (1996), 415–420.

[19] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, de Gruyter, Berlin, 1991, 227–238.

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[21] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts Math., Springer, New York, 1992.

[22] S. Yoshida, *Some variants of the congruent number problem I*, Kyushu J. Math., **55** (2001), 387–404.

後藤丈志
東京理科大学理工学部数学科
〒 278-8510 千葉県野田市山崎 2641

email: goto_takeshi@ma.noda.tus.ac.jp
URL: http://www.ma.noda.tus.ac.jp/u/tg/

Takeshi Goto
Department of Mathematics
Faculty of Science and Technology
Tokyo University of Science
Noda, Chiba 278-8510