数理解析研究所講究録
1160巻 2000年 251-258

θ-congruent numbers and modular parametrizations

早稲田大学理工学総合研究センター 日比野 剛士 (Takeshi Hibino)
お茶の水女子大学人間文化研究科 菅 真紀子 (Makiko Kan)

1 Introduction

θ を $0<\theta<\pi$ なる実数とする. この様な θ について, 3辺の長さが有理数で θ をその一角として持つような三角形のことを θ-有理三角形と呼ぶことにする. ここで, このような三角形が存在するには $\cos\theta$ が有理数であることが必要条件であることに注意する. 有理数 $\cos\theta$ は $\cos\theta=s/r$, $\gcd(r,s)=1$, $r>0$ であるような有理整数 r, s によって一意的に表される. このようにして導入された θ に付随する値 r, s について, α_θ を $\sqrt{r^2-s^2}$ で与える. これは, θ について一意的に定まる高々2次の数である. このような表記を用いて θ-合同数は次のように定義される.

Definition 1.1 n を自然数とする. θ-有理三角形で面積 $n\alpha_\theta$ なるものが存在する時, n を θ-合同であるという.

$\theta=\pi/2$ とした時は $\alpha_{\frac{\pi}{2}}=1$ となるので, $\pi/2$-合同数は従来の合同数に他ならない. 自然数 n が θ-合同ならば, 任意の自然数 α に対して $n\alpha^2$ も θ-合同であることは明らかである. なおこの報告において, θ は常に $0<\theta<\pi$, $\cos\theta\in\mathbb{Q}$, 自然数 n は平方因子を含まないものとし, 全ての楕円曲線は $\mathbb{Q}$ 上定義されているものと仮定する.

さらに $E_{n,\theta}$ は $y^2=x(x+(r+s)n)(x-(r-s)n)$ (r,s は上記の θ で定まる値) で定義される楕円曲線とする.

Theorem 1.1 (Fujiwara,[2]) 実数 θ $(0<\theta<\pi)$ は $\cos\theta$ が有理数であるものとする. 任意の自然数 n に対して次が成り立つ.
(1) n が θ-合同であることと $E_{n,\theta}$ が位数2以上の $\mathbb{Q}$-有理点を持つことは同値.
(2) $n\neq 1,2,3,6$ である時, n が θ-合同であることと $E_{n,\theta}$ の $\mathbb{Q}$-*rank* が正であることは同値.

この Theorem から, $E_{n,\theta}$ 上の有理点は θ-合同数に関する重要な情報を与えてくれることがわかる. $E_{n,\theta}(\mathbb{Q})$ の様子を調べることによって, 具体的には 2-descent と呼ばれる方法で $E_{n,\theta}$ の Tate-Shafarevich 群の 2-tortion 部分を調べることによって, 素数 $p \equiv 5, 7, 19 \pmod{24}$ の非 $\frac{\pi}{3}$-合同性 (Fujiwara, [2]), $p \equiv 7, 11, 13 \pmod{24}$ の非 $\frac{2\pi}{3}$-合同性が確かめられている (Kan,[4]).

また, 次の Lemma は, 固定したある θ について θ-合同数が充分たくさん存在するということを保証している.

Lemma 1.1 (Kan,[4]) 自然数 n が θ-合同数であることと, n が

$$pq(p+q)(2rq+p(r-s))$$

(p, q は $\gcd(p,q) = 1$ なるある自然数) の非平方部分となっていることは同値.

8 を法として 5, 6, 7 に合同な自然数は全て $\frac{\pi}{2}$-合同 (つまり従来の意味での合同) であろうと予想されている. Birch-Swinnerton-Dyer 予想が確かめられればこの事実もその正当性を確定される. 同様にして, $\theta = \frac{\pi}{3}, \frac{2\pi}{3}$ についても理論的または実験的根拠に基づいて次のような Conjecture を得ることができる (Kan,[4]).

Conjecture 1.1 n を自然数とする. n が 24 を法として 11, 13, 17 又は 23 に合同なら, n は $\frac{\pi}{3}$-合同である. 同様に n が 5, 17, 19 又は 23 に合同なら, n は $\frac{2\pi}{3}$-合同である.

これまで知られていたのは, 自然数 n が素数 p で $p \equiv 23 \pmod{24}$ である場合に $\frac{2\pi}{3}$-合同であることのみであった ([4]). 今回は, その結果の別証明と $\frac{\pi}{3}$-合同についての新しい結果を得ることができたのでここに報告する.

Theorem 1.2 p を 24 を法として 23 に合同な素数とすると, p は $\frac{\pi}{3}$-合同かつ $\frac{2\pi}{3}$-合同である.

2 Heegner points

自然数 N について $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$ とおき, $\mathfrak{H}$ を上半平面 $\{z \in \mathbb{C} \mid Im(z) > 0\}$ とする. すると, $\Gamma_0(N)$ は $\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ 上に 1 次分数変換の形で作用する. その作用で割った商空間 $\Gamma_0(N)\backslash\mathfrak{H}^*$ は閉 Riemann 面の構造を持ち, 対応する代数曲線を $X_0(N)$ と記す. さらに $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ に

よって得られる $X_0(N)$ の位数 2 の自己同型 W_N を Atkin-Lehner involution と呼ぶ. 以下, $z \in \mathfrak{H}^*$ に対して z で代表される $X_0(N)$ の点も z と書く.

ω を虚 2 次数で, $A\omega^2 + B\omega + C = 0$, $A, B, C \in \mathbb{Z}$, $\gcd(A, B, C) = 1$, 判別式 : $\Delta(\omega) := B^2 - 4AC < 0$ を満たすものとする. この時, $X_0(N)$ の Heegner point は次のように定義される.

Definition 2.1 虚 2 次数 ω について, 判別式に関する条件式 $\Delta(\omega) = \Delta(N\omega)$ が成り立つ時 ω は $X_0(N)$ の *Heegner point* であるという.

ここで特に ω が Heegner point なら $W_N(\omega)$ も Heegner point であるということに注意しておく.

$\mathbb{Q}$ 上定義された楕円曲線 E は $X_0(N)$ による modular parametrization を持つとする. この時, $\mathbb{Q}$ 上定義される $X_0(N)$ から E への被覆写像 $\varphi : X_0(N) \to E$ で cusp $i\infty$ を E の単位元 $\mathcal{O}$ に写すようなものが存在する. この写像をかいして, Atkin-Lehner involution W_N は $W_N(\varphi(z)) := \varphi(W_N(z))$ の形で E 上に作用する. 特にその作用が 非自明である時, 楕円曲線 E は even であると言う. これは, Birch-Swinnerton-Dyer 予想を仮定した際に, 楕円曲線 E が even であるなら $E(\mathbb{Q})$ の rank も even であるという事実に基づいている.

上のような被覆写像 φ について次のような関係式が成り立つことが知られている :

$$\varphi(W_N(z)) = \varphi(0) - \varphi(z).$$

さらに, $\varphi(0)$ は E 上有限位数の $\mathbb{Q}$- 有理点となることも知られている.

上で定義した Heegner point ω については, その性質から φ による像 $\varphi(\omega)$ が $E(\mathbb{Q}(\omega,\, j(\omega)))$ に含まれることが確かめられる. ここで, j とは $X_0(1)$ の modular j-function である. $\mathbb{Q}(\omega, j(\omega))$ が虚 2 次体 $\mathbb{Q}(\omega)$ 上 Galois 拡大となっていることを用いて, $z = \omega$, $W_N(\omega)$ に対して

$$P(z) := \sum_{\sigma \in G} \varphi(z)^\sigma$$

とおく. ここで $G :=\mathrm{Gal}(\mathbb{Q}(\omega, j(\omega))/\mathbb{Q}(\omega))$ である. 定義から $P(\omega)$ は $E(\mathbb{Q}(\omega))$ の点であることは明らかである. さらに, $\overline{P}$ を点 P の複素共役とすれば

$$P(W_N(\omega)) = \overline{P(\omega)}$$

となることが知られている. G の位数を h とすれば, $P(z)$ の定義から

$$\overline{P(\omega)} = P(W_N(\omega)) = h\varphi(0) - P(\omega)$$

という等式を得る. このような準備のもと, E の純虚点

$$P(\omega) - \overline{P(\omega)} = 2P(\omega) - h\varphi(0)$$

は, E に相応の条件を付け加えると非自明な, 即ち無限位数を持つ $\mathbb{Q}(\omega)$- 有理点となる. この点を ω で "ひねった" ある楕円曲線 (twist) 上に移すとその楕円曲線上の非自明な $\mathbb{Q}$- 有理点になる. 以上を整理すると,

Theorem 2.1 (Birch,[1]) E は $X_0(N)$ による *modular parametrization* を持つ *even* な楕円曲線とする. $\varphi(0)$ が $E(\mathbb{Q})$ の 2 倍点でなく, かつ 素数 p について $-p$ が $4N$ を法として平方数に合同なら, E の $(-p)$-*twist* $E^{(-p)}$ は無限個の有理点を持つ.

一般に 楕円曲線 $E : y^2 = x^3 + ax^2 + bx + c$ の n-twist $E^{(n)}$ は $ny^2 = x^3 + ax^2 + bx + c$ で与えられ, これは $\mathbb{Q}(\sqrt{n})$ 上 E と同型である. $E_{p,\frac{2\pi}{3}}$ は $E_{1,\frac{\pi}{3}}^{(-p)}$ と, $E_{p,\frac{\pi}{3}}$ は $E_{1,\frac{2\pi}{3}}^{(-p)}$ とそれぞれ $\mathbb{Q}$ 上同型となっていることに注意する. $\mathbb{Q}$ 上同型な楕円曲線の全体を同一視すると, $E_{p,\frac{2\pi}{3}}$ は $E_{1,\frac{\pi}{3}}$ の, $E_{p,\frac{\pi}{3}}$ は $E_{1,\frac{2\pi}{3}}$ のそれぞれ $(-p)$-twist となっている.

3 Modular parametrizations

楕円曲線 $E_{1,\frac{\pi}{3}}$ と $E_{1,\frac{2\pi}{3}}$ はそれぞれ conductor 24, 48 であるから, $X_0(24)$, $X_0(48)$ からの被覆写像 (modular parametrization) の存在がうかがえる. この章ではこの二つの楕円曲線についてそれぞれ modular parametrization を具体的に構成する. これらの写像 φ を用いて楕円曲線の evenness 性と $\varphi(0)$ の位数を確認することができた.

Proposition 3.1 $X_0(24)$ と $E_{1,\frac{\pi}{3}}$ の定義方程式をそれぞれ $Y^2 = X^4 - 22X^2 - 48X - 23$, $y^2 = x(x-1)(x+3)$ とした時, $X_0(24)$ から $E_{1,\frac{\pi}{3}}$ への被覆写像 $\varphi((X,Y)) = (x,y)$ が次のように与えられる.

$$\begin{aligned} x &= \frac{X^2 - 5 + Y}{2}, \\ y &= \frac{X^3 - 11X - 12 + XY}{2}. \end{aligned}$$

さらに $\varphi(i\infty) = \mathcal{O}$, $\varphi(0) = (3,6)$ は $E_{1,\frac{\pi}{3}}(\mathbb{Q})$ 内の 2 倍点ではない.

同様に $X_0(48)$ と $E_{1,\frac{2\pi}{3}}$ の定義方程式をそれぞれ $Y^2 = X^8 + 14X^4 + 1$, $y^2 = x(x+1)(x-3)$ とした時 $X_0(48)$ から $E_{1,\frac{2\pi}{3}}$ への被覆写像 $\varphi((X,Y)) = (x,y)$ が次のように与えられる.

$$\begin{aligned} x &= \frac{X^4+1-Y}{2X^2}, \\ y &= \frac{(X-1)(X+1)(X^4+1-Y)}{2X^3}. \end{aligned}$$

さらに $\varphi(i\infty) = \mathcal{O}$, $\varphi(0) = (3,0)$ は $E_{1,\frac{2\pi}{3}}(\mathbb{Q})$ 内の 2 倍点ではない.

Proof. 次のように Yamamoto の方法 ([5]) を用いると楕円曲線 $E_{1,\frac{\pi}{3}}$, $E_{1,\frac{2\pi}{3}}$ のそれぞれの座標 x,y を modular funciton として $i\infty$ でフーリエ展開することができる. canonical system, canonical parameter 等の用語については [5] の参照をお願いしたい. まず, $E_{1,\frac{\pi}{3}}$, $E_{1,\frac{2\pi}{3}}$ それぞれに $\mathbb{Q}$ 上同型な minimal model の canonical system を求める. 実際、minimal model $v^2 = u^3 - u^2 - 4u + 4$ によって定義される楕円曲線は $E_{1,\frac{\pi}{3}}$ $(y^2 = x(x+1)(x-3))$ に $\mathbb{Q}$ 上同型であって次のような canonical system を持つ :

$$\begin{aligned} u &= \frac{1}{q^2} + 1 + 2q^2 + q^6 - 2q^{14} - 2q^{18} + 2q^{22} + 4q^{26} + 3q^{30} - \cdots, \\ v &= \frac{1}{q^3} + \frac{1}{q} + q + 3q^3 + q^5 + 2q^7 + q^9 - 2q^{11} - q^{13} - 5q^{15} - \cdots \end{aligned}$$

ここで q は canonical parameter である. $q = exp(2\pi iz)$ とおく. 同型写像として $x = u - 1$, $y = v$ で定義されるものを考える. 座標 x, y を $X_0(24)$ 上の modular function と見なせて $i\infty$ における次のようなフーリエ展開を得る ;

$$\begin{aligned} x &= \frac{1}{q^2} + 2q^2 + q^6 - 2q^{14} - 2q^{18} + 2q^{22} + 4q^{26} + 3q^{30} - \cdots, \\ y &= \frac{1}{q^3} + \frac{1}{q} + q + 3q^3 + q^5 + 2q^7 + q^9 - 2q^{11} - q^{13} - 5q^{15} - \cdots. \end{aligned}$$

同様に, $E_{1,\frac{2\pi}{3}}$ の場合には, 座標 x, y を $X_0(48)$ 上の modular function と見なせ $i\infty$ における次のようなフーリエ展開を得る ;

$$\begin{aligned} x &= \frac{1}{q^2} + 2q^2 + q^6 - 2q^{14} - 2q^{18} + 2q^{22} + 4q^{26} + 3q^{30} - \cdots, \\ y &= \frac{1}{q^3} - \frac{1}{q} + q - 3q^3 + q^5 - 2q^7 + q^9 + 2q^{11} - q^{13} + 5q^{15} + \cdots. \end{aligned}$$

また, $X_0(24)$, $X_0(48)$ のそれぞれの座標 X, Y を $i\infty$ でフーリエ展開することはその構成から容易に実行できる (Hibino, [3]). 実際に $X_0(24)$ の場合には, それらの関数としての展開は

$$\begin{aligned} X &= \frac{1}{q} + 4q + 6q^2 + 11q^3 + 18q^4 + 28q^5 + 42q^6 + 62q^7 + \cdots, \\ Y &= \frac{1}{q^2} - 3 + 12q - 34q^2 - 84q^3 - 180q^4 - 360q^5 - 683q^6 - \cdots, \end{aligned}$$

$X_0(48)$ の場合には,

$$\begin{aligned} X &= \frac{1}{q} - q^3 + 2q^7 - 2q^{11} + 3q^{15} - 4q^{19} + 5q^{23} - 7q^{27} + \cdots, \\ Y &= -\frac{1}{q^4} - 3 + 10q^4 - 36q^8 + 83q^{12} - 180q^{16} - 360q^{20} - \cdots. \end{aligned}$$

したがって, 各々の展開を考察することによって, x, y を X, Y で表し, Proposition 3.1 の被覆写像を得ることができる.

さらに, $X_0(24)$, $X_0(48)$ を上のような定義方程式で表した時に Atkin-Lehner involution の作用, cusp の座標などは [3] において具体的に既に得られている. W_N から誘導される $\mathbb{Q}(X_0(N))$ の自己同型写像を W_N^* とする, ただし, $\mathbb{Q}(X_0(N))$ は $\mathbb{Q}$ 上定義される $X_0(N)$ の関数体である. $X_0(24)$ の場合には, W_{24}^* の X, Y への作用は $W_{24}^*X = X$, $W_{24}^*Y = -Y$ である. よって, x, y への作用は次のようになる ;

$$\begin{aligned} W_{24}^*x &= \frac{X^2 - 5 - Y}{2} = 3 + 12q + \cdots, \\ W_{24}^*y &= \frac{X^3 - 11X - 12 - XY}{2} = 6 + 36q + \cdots. \end{aligned}$$

これらの作用から, 次が従う ;

$$\begin{aligned} \varphi(0) &= (x(0),\ y(0)) = (x(W_{24}(i\infty)),\ y(W_{24}(i\infty))) \\ &= (W_{24}^*x(i\infty),\ W_{24}^*y(i\infty)) = (3, 6). \end{aligned}$$

容易にこの点 $(3,6)$ が $2E_{1,\frac{\pi}{3}}(\mathbb{Q})$ に属さないこと, すなわち, $E_{1,\frac{\pi}{3}}$ 上の 2 倍点ではないことが確かめられる.

同様に, $X_0(48)$ の場合には $W_{48}^*X = (X+1)/(X-1)$, $W_{48}^*Y = 4Y/(X-1)^4$ である. したがって, x, y への作用は

$$\begin{aligned} W_{48}^*x &= \frac{X^4+6X^2+1-2Y}{(X-1)^2(X+1)^2} = 3+12q^2+\cdots, \\ W_{48}^*y &= \frac{4X(X^4+6X^2+1-2Y)}{(X-1)^3(X+1)^3} = 12q+60q^3+\cdots. \end{aligned}$$

それゆえに, $\varphi(0) = (x(0), y(0)) = (x(W_{48}(i\infty)), y(W_{48}(i\infty))) = (W_{48}^*x(i\infty), W_{48}^*y(i\infty)) = (3,0)$ であり, $(3,0)$ は $E_{1,\frac{2\pi}{3}}$ の 2 倍点でないことも直ちに解る. □

Proof of theorem 1.2. Proposition 3.1 により, 楕円曲線 $E_{1,\frac{\pi}{3}}$, $E_{1,\frac{2\pi}{3}}$ は Theorem 2.1 の関連する条件をみたす. 一方, $N = 24, 48$ のとき, 素数 p について $-p$ が $4N$ を法として平方数に合同であることは $p \equiv 23 (\mathrm{mod}\ 24)$ であることと同値になる. したがって, $p \equiv 23 (\mathrm{mod}\ 24)$ ならば $E_{1,\frac{\pi}{3}}$, $E_{1,\frac{2\pi}{3}}$ は Birch の定理の条件をみたすことが確かめられ, その $(-p)$-twist $E_{p,\frac{2\pi}{3}}$, $E_{p,\frac{\pi}{3}}$, それぞれが無限位数の $\mathbb{Q}$- 有理点を持つことが解る. □

Example 3.1 23 は $2\pi/3$- 合同数である. 実際, $23\sqrt{3}$ は $\frac{14}{5}$, $\frac{230}{7}$, そして $\frac{1202}{35}$ を 3 辺の長さとして持つ $2\pi/3$- 有理三角形の面積となっている.

同様に $2039\sqrt{3}$ は $\frac{8913393110786957347 3198}{7031144327156015001179}$, $\frac{28673006566142229174807962}{44566965553934786736599}$, そして $\frac{2036193258877906366441529848343726435356779132 02}{3133567670331061034744344902646726065474502 21}$ を 3 辺の長さとして持つ $2\pi/3$- 有理三角形の面積となっている.

References

[1] Birch,B.J., Heegner Points of Elliptic Curves, Symposia Mathematica XV, 1973, 441-445

[2] Fujiwara, M., θ-congruent numbers, Number Theory, ed. by Györy, Pethó, Sós, Walter de Gruyter, 1997, 235–241

[3] Hibino, T., Formulae for relating the modular invariants and defining equations of $X_0(40)$ and $X_0(48)$, Tokyo J. of Math. **22**, 1999, 279–288.

[4] Kan, M., θ-congruent Numbers and Elliptic Curves, preprint.

[5] Yamamoto, Y., Canonical power series associated with elliptic curves over $\mathbb{Q}$ (Japanese), Algebraic number theory and related topics (Japanese) (Kyoto, 1997), Sūrikaisekikenkyūsho Kōkyūroku **1026**, 1998, 204–211

日比野 剛士
早稲田大学 理工学総合研究センター
169-8555 東京都新宿区大久保 3-4-1
E-mail: hibino@mse.waseda.ac.jp

菅 真紀子
お茶の水女子大学 人間文化研究科
112-8610 東京都文京区大塚 2-1-1
E-mail: kan@math.ocha.ac.jp