| | |
|---|---|
| 称号及び氏名 | 博士（理学）中澤　直也 |
| 学位授与の日付 | 平成 18 年 3 月 31 日 |
| 論　文　名 | Construction of elliptic curves with cyclic groups of Fp-rational points and modular function fields of genus 0<br>（巡回的な F_p-有理点群をもつ楕円曲線の構成および種数 0 のモジュラー関数体） |
| 論文審査委員 | 主査　石井 伸郎<br>副査　加茂　静夫<br>副査　馬野 元秀<br>副査　高橋　哲也 |

# 論文要旨

1. はじめに

有限体上で 巡回的な有理点群を持つ楕円曲線を構成する問題への興味は，楕円曲線暗号での必要性から生じている．暗号でよく使われている実際的な方法としては，有限体と一つの素数を与え，Deuring の虚数乗法をもつ楕円曲線への持ち上げを利用し，その素数を位数にもつ有理点群を構成するというものである．

この問題への理論的なアプローチの一つは，ある代数体$K$上で定義される楕円曲線$E$に対して，$E$ の $\mathfrak{P}$ でのreduction $\overline{E}$ の有理点群 $\overline{E}(F_{\mathfrak{P}})$ が巡回群となるような $K$ の素イデアル $\mathfrak{P}$ の集合を求めることである．これに関しては，A.C.Cojocaru, R.Gupta, M.R.Murty たちによる，上記の性質を持つ素イデアルの分布について確率論的立場からの研究があるが，彼らの研究では，暗号で必要とされる具体的な楕円曲線は与えられていない．

本研究においては，巡回的な $\overline{E}(F_{\mathfrak{P}})$ を parametric に構成する問題を考え，具体的な形をもつ楕円曲線の族 $\{E_\lambda\}$ と特別な形の素数 $\{p_\mu\}$ に対して，$\overline{E_\lambda}(F_{\mathfrak{P}_\mu})$ が巡回群となるための条件を与える．

虚数乗法を持つ楕円曲線を利用すれば，そのFrobenius準同型写像の情報から，上記で述べた$\{E_\lambda, p_\mu\}$を構成することが可能である．すなわち，虚数乗法を持つ楕円曲線$E$においては，Frobenius準同型写像は$E$の自己準同型環の商体である虚２次体の元と見なせるので，素数の2次normの表示から，Frobenius準同型写像のtraceを計算することができ，traceから$\overline{E}(F_p)$の群の構造と位数を定めることができる．しかし，虚数乗法を持たない楕円曲線に対して，素イデアルでのreductionを考えたときに，Frobenius準同型写像を含む虚２次体が変化するので，この方法を適用するのは，困難である．虚数乗法を持たない楕円曲線においては，reductionをしたときに，有理点群が巡回群になるのは確率的に高いということが知られているが，具体的に素イデアルを与えたとき，そこでのreductionの結果，巡回群が得られるかどうかは，実際に有理点群の構造を調べてみなければ判らない．

本論文の主な目的は，genus 0のモジュラー関数体の生成元によるモジュラー不変関数$J$の有理表現を用いることにより，巡回的な$\overline{E}(F_p)$が得られるような，（一般的には虚数乗法を持たない）楕円曲線と素数の族$\{E, p\}$を構成することである． なお，次の定理とその系は，この問題を考える時に基本的に利用する結果である．

Theorem　楕円曲線$E/Q$について，$K_n(E)$を$E$の$n$等分点の全ての座標によって生成される$Q$上の拡大体とする． $p$を$E$が good reduction を持つ素数とする．このとき，

a)．$\overline{E}(F_p)$が巡回群であるための必要十分条件は，任意の素数$l$について$p$が$K_l(E)$で完全分解しないことである．

b)．任意の正整数$n$に対して，円分体$Q(\zeta_n)$は$K_n(E)$に含まれる．

Corollary　素数$p$が相異なる素数$l_1,\cdots,l_n$によって，$p = l_1^{m_1}\cdots l_n^{m_n} + 1$なる形で与えられるとする．このとき， $p$が$K_{l_1}(E),\cdots,K_{l_n}(E)$で完全分解しなければ， $\overline{E}(F_p)$は巡回群である．

以下の章で本研究で得られた結果を述べる.

2. 次数 $N$ のモジュラー関数体を用いた構成

モジュラー群

$$\Gamma(N)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(Z)\mid a-1\equiv b\equiv c\equiv d-1\equiv 0 \bmod N\right\}$$

に関するモジュラー関数体 $A(N)$ は, $C(J)$ 上 Galois 拡大で, その Galois 群は $G=PSL_2(Z/NZ)$ と同型である. $N$ が素数で, $C(J)$ 上, 次数 $N$ の部分体をもつならば, $N\le 11$ であることが判っている. また, $N=5,7$ の場合にはその部分体の定義方程式はすでに計算されている. この定義方程式が $J$ のその部分体の生成元による表現を与えているのでそれを用い, $N=5,7$ のときに, $\overline{E}(F_p)$ が巡回群であるような楕円曲線 $E/Q$ の族を構成した. 例えば, $A(5)$ の次数 5 の部分体は, genus 0 であり, 定義方程式は,

$$g_5(X,J)=X^5+5X^4+40X^3-J$$

である. 楕円曲線 $E/Q$ の $j$-invariant を $j_E$ とする. $g_5(X,j_E)$ の分解体は $K_5(E)$ に含まれる. この性質および Corollary を利用して, $g_5(X,j_E)$ が modulo $p$ で 2 次の既約な因子を持つための条件を考えることにより, $p=2^{m_2}5^{m_5}+1$ の形の素数に対して次の結果を得た.

Theorem 1 $5\lambda^2-1>0$ であるような有理数 $\lambda$ を取り, $T(\lambda)=R(\lambda)/S(\lambda)$,

$$R(\lambda)=(\lambda-1)(10\lambda^2+5\lambda+1)^3,$$

$$S(\lambda)=(15\lambda^2+10\lambda+2)(5\lambda^2-5\lambda-1)^2(15\lambda^2+10\lambda+7)^2$$

とする. 次の式で与えられる楕円曲線 $E_\lambda: y^2=x^3+3375T(\lambda)x-6750T(\lambda)$

を考える. $\varepsilon=9+4\sqrt{5}$, $\varepsilon^n=c_n+\sqrt{5}d_n$, $\lambda=\lambda_n=(-1-d_n)/3$ とおく. このとき,

$p=2^\alpha 5^\beta+1$ の形の素数に対して, $\left(\dfrac{5d_n^2+10d_n-4}{p}\right)=1$ かつ $E_{\lambda_n}$ が modulo $p$ で good

reduction を持つならば，$\overline{E_{\lambda_n}}(F_p)$ は巡回群である．

3. 次数 11 のモジュラー関数体の定義方程式

$A(N)$ の $N$ 次部分体の定義方程式は，$N=11$ については知られていなかったが，$N=11$ についても，$N=5,7$ と同様の結果を得た．$\mathrm{PSL}_2(\mathrm{F}_{11})$ の部分群

$$H=\left\langle \begin{pmatrix} 9 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix} \right\rangle$$

は，5 次交代群と同型，指数 11 である．この $H$ に対応する $A(11)$ の部分体 $A_H$ の genus は 0 であることを示し，Klein form から $A_H$ の生成元 $X_H$ を構成することにより，次の結果が得られた．

Theorem 2　モジュラー不変関数 $J$ は，$X_H$ によって，

$$J=X_H^{11}+11\mu X_H^9-22X_H^8-33(\mu+4)X_H^7-176\mu X_H^6+33(-7\mu+5)X_H^5+165(\mu+4)X_H^4 \\ +693(\mu+1)X_H^3+220(5\mu-1)X_H^2-33(8\mu+47)X_H-18(11\mu-1)$$

と表される．ただし，$\mu=(-1+\sqrt{11})/2$ である．

この方程式を用いて，11-等分点でのガロワ表現についての結果を得ることができた．またこの結果の構成問題への応用について研究している．

4. モジュラー関数体$A_{0}(N)$を用いた構成

モジュラー部分群

$$\Gamma_0(N)=\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) \mid c\equiv 0 \bmod N \right\}$$

に対応する $A(N)$ の部分体を $A_0(N)$ と表す．モジュラー不変関数 $J$ は，$A_0(N)$ の元なので，$A_0(N)$ の genus が 0 のとき，その生成元 $X$ により，$J$ は $X$ の有理関数 $J_N(X)$ として表される．なお，$N$ が素数のとき，$A_0(N)$ の genus が 0 であるのは，$N=2,3,5,7,13$ の場合に限る．例えば $N=5,7,13$ の場合，$J=J_N(X)$ は，

$$(N=5) \qquad J=\frac{(X^2+10X+5)^3}{X}$$

$$(N=7) \qquad J=\frac{(X^2+13X+49)(X^2+5X+1)^3}{X}$$

$$(N=13) \qquad J=\frac{(X^2+5X+13)(X^4+7X^3+20X^2+19X+1)^3}{X}$$

と表される．　これらの $A_0(N)$ の生成元による $J$ の表示を用いて，$\overline{E}(F_{\mathrm{P}})$ が巡回群であるような楕円曲線 $E/Q$ および素数 $p$ の族 $\{E,p\}$ を構成した．

以下，$N=3,5,7,13$ とする．有理数 $s$ に対して，$J_N(s)$ を $j$-invariant に持つ楕円曲線

$$E_N(s):y^2=x^3-3\frac{J_N(s)}{J_N(s)-1728}x-2\frac{J_N(s)}{J_N(s)-1728}$$

を考える．$E_N(s)$ の $N$ 等分多項式 $\psi_N(x)$ は，$(N-1)/2$ 次の因子 $d_N(x)$ を持つ．$p=2^\alpha N^\beta+1$ なる形の素数に対して，$d_N(x)$ が modulo $p$ で分解せず，かつ $p$ が $K_2(E_N(s))$ で完全分解しないならば，Corollary によって $\overline{E_N(S)}(F_{\mathrm{P}})$ は巡回群である．例えば $N=13$ のとき，次の結果を得ている．

Theorem 3　$\lambda$ を $\lambda\equiv 0 \bmod 13$ でない整数とする．素数 $p$ が $p=2^\alpha 13^\beta+1$ なる形で与えられ，$\left(\frac{\lambda^4+6\lambda^2+13}{p}\right)=-1$ を満たすとする．楕円曲線

$$\mathrm{E}(\lambda):V^2=U^3-4\lambda^4(\lambda^4+6\lambda^2+13)^2U-3\lambda^6(\lambda^4+6\lambda^2+13)^3$$

を考え，$\varepsilon(\lambda)=(\lambda^4+6\lambda^2+13)/\lambda^2$ とおく．このとき，

(i) $\mathrm{E}(\lambda)$ は，変換公式

$$S=S(U,V)=-\frac{\lambda((3\lambda^2+13)U+V+\lambda^2(5\lambda^2+13)(\lambda^4+6\lambda^2+13))}{\lambda^2(\lambda^2+3)U-V+\lambda^4(\lambda^2+5)(\lambda^4+6\lambda^2+13)}$$

および

$$T=T(U,V)=\frac{\lambda(U^3+A_1U^2+A_2U+BV+C)}{(\lambda^2(\lambda^2+3)U-V+\lambda^4(\lambda^2+5)(\lambda^4+6\lambda^2+13))^2}$$

によって，曲線 $S^4+6S^2+13=\varepsilon(\lambda)T^2$ に変換される．但し，$A_1=3\lambda^2(\lambda^4+10\lambda^2+13)$,

$A_2 = 4\lambda^2(\lambda^4 + 6\lambda^2 + 13)^2$, $B = -4\lambda^2(\lambda^4 - 13)$, $C = 2\lambda^6(\lambda^4 - 2\lambda^2 + 13)(\lambda^4 + 6\lambda^2 + 13)^2$

である.

(ii) 点 $Q(\lambda) = ((\lambda^4 + 2\lambda^2 + 13)(\lambda^4 + 6\lambda^2 + 13)/4, (\lambda^4 - 13)(\lambda^4 + 6\lambda^2 + 13)^2/8)$ は $\mathrm{E}(\lambda)$ の位数 $\infty$ の有理点である.

(iii) $[m]Q(\lambda) = \overbrace{Q(\lambda) + \cdots + Q(\lambda)}^{m} = (U_m(\lambda), V_m(\lambda))$ および $S_m(\lambda) = S(U_m(\lambda), V_m(\lambda))$ とする. このとき, 楕円曲線 $E_{13}(S_m(\lambda)^2)$ が $p$ で good reduction をもつならば, $\overline{E_{13}(S_m(\lambda)^2)}(F_{\mathrm{P}})$ は巡回群である.

$N = 3,5,7$ の場合も, 同様に上記, 定理 3 に対応する結果を得ている.

# 審査結果の要旨

本学位論文の主要な内容は有限体上に巡回的有理点群を持つ楕円曲線の系統的な構成に関する研究である．有限体上にこのような性質を持つ楕円曲線を構成する問題は，楕円曲線暗号における必要性から生じている．暗号における実用性を別にしても，モジュラー曲線の有限体上の有理点の研究，整数における Artin 予想の類似としての研究などと関係が深く理論的にも興味深いものである．今までに行われてきた研究としては，代数体上で定義された 1 つの楕円曲線を reduction したときに, 有理点群が巡回群となるような素イデアルの分布を確率的に調べるものがある．

本研究では，その立場とは異なり，巡回的有理点群を持つ楕円曲線と素体の系列を構成的に与えることを目的としている．このような構成的な結果は，あまり発表されていないので，中澤氏の結果は貴重である．

楕円曲線が虚数乗法を持つ場合には，その楕円曲線の reduction から，フロベニウス準同型のトレースの情報を用いて構成する研究が中澤氏によりなされているが，虚数乗法を持たない場合には，トレースの情報が使えないので，構成はできていない．

本研究では，種数 0 のモジュラー関数体の生成元によるモジュラー不変関数の表現を用いる新たな方法を考案し，楕円曲線の構成を行っている．用いられているモジュラー関数体は２種類あり，１つは，素数レベル N の主合同部分群を含む $SL_2(Z)$ の指数 N の部分群に関するにモジュラー関数体であり，他は Hecke 群に関するモジュラー関数体である．特に Hecke 群のモジュラー関数体を使った構成は注目に値するものである．

Nを素数として，$p=2^sN^t+1$ 型の素数の族を考え，この型の素数に対して，巡回的有理点群をもつ楕円曲線を得るためには，2-等分方程式とN-等分方程式がその素数pを法として 1 次因子に完全分解しないという条件を満たすように楕円曲線を作れば良いことが示されている．

この関数体の生成元でのモジュラー関数の表現を有理数に特殊化して与えられる j-不変量を持つ楕円曲線を考えると，次数が $(N^2-1)/2$ となる N-等分方程式が$(N-1)/2$ 次の次数が小さな因子を持つという事実に着目し，その因子が 1 次因子に分解しないような条件を求めることにより，次数が大きく分解の型の決定が困難な N-等分多項式に対する非分解性を巧妙に処理し楕円曲線の構成に繋げている．例えば N=13 ならば，84 次の多項式を扱う代わりに 6 次の多項式を扱えばよいことになる．ここで用いられたこのアイデアは独創的であり，高く評価できる．得られた楕円曲線の系列は実 2 次体の単数群，楕円曲線の無限位数の有理点，さらには楕円曲面の無限位数の有理点を媒介として与えられており，非常に興味深い結果である．

以上のように，中澤氏の研究は独創的なアイデアに基づいた，これからの発展も期待できる興味深い結果を与えている優れたものであると評価でき，審査委員会において学位論文として十分な内容であると判断する．