論　文

C_{ab}曲線のヤコビアン群加算アルゴリズムとその離散対数型暗号への応用

有田　正剛†

Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems

Seigo ARITA†

あらまし　昨今, 楕円曲線暗号が注目され, その実用化が進んでいる。しかし, その一方で, 楕円曲線は独特な数学的対象で, 楕円曲線暗号の将来的な安全性が心配だという意見もある。暗号の将来にわたる安全性を考慮すると, より広いクラスの代数曲線のヤコビアン群を用いた離散対数型暗号の可能性は, 重要な研究課題である。C_{ab}曲線は, 楕円曲線や超楕円曲線を含む, 広いクラスの代数曲線である。本論文では,C_{ab}曲線のヤコビアン群における加算を実行する効率的なアルゴリズムを求め, そのソフトウェア実装による速度評価の結果を示し, C_{ab}曲線を用いて実用的な離散対数型暗号を構成しうることを示す。

キーワード　離散対数問題, ヤコビアン群, 楕円曲線暗号,C_{ab}曲線,C_{ab}曲線暗号

1. まえがき

昨今, 楕円曲線暗号が注目され, その実用化が進んでいる。楕円曲線暗号では RSA 暗号に比べて鍵長が大幅に少なくてすむため, 将来の標準は楕円曲線暗号との声が上がっている。しかし, 一方で, 楕円曲線は独特な数学的対象で, その数学理論が余りに豊富なため, 楕円曲線暗号の攻撃法が調べつくされたとはいえず, 楕円曲線暗号の将来的な安全性が心配だという意見もある。実際, このところ,97 年 9 月,98 年 7 月と相次いで楕円曲線暗号に対する攻撃法が発見されている [1]〜[3], [12]。

楕円曲線暗号は楕円曲線のヤコビアン群を利用する離散対数型暗号である。楕円曲線に限らず, 一般に代数曲線にはヤコビアン群が付随する。暗号の将来にわたる安全性を考慮すると, 楕円曲線（や超楕円曲線）に限らず, より広いクラスの代数曲線のヤコビアン群を用いた離散対数型暗号の可能性は, 重要な研究課題である。

ある代数曲線のクラス C を用いて離散対数型暗号を構成するには, 以下の 2 つの基本的課題を解決する必要がある。

（1） クラス C に属する任意の曲線に対して, そのヤコビアン群の加算を実行する効率的なアルゴリズムを求めること。

（2） クラス C に属する曲線の中から, ヤコビアン群の位数が大きな素因子をもつ曲線を探索する効率的なアルゴリズムを求めること。

楕円曲線に対して, これら 2 つの課題は解決されており, 楕円曲線暗号の実用化が進んでいる。また, 超楕円曲線に対しては, 課題 (1) が解決され [4], [5], 課題 (2) も部分的には解決されている [6], [7], [11]。

[8] は, 代数幾何符号を動機として,C_{ab}曲線という代数曲線のクラスを発見した。C_{ab}曲線は, 楕円曲線や超楕円曲線を含む, 広いクラスの代数曲線であり, しかも計算機上で処理するのに都合のよい性質をもっている。

本論文では,C_{ab}曲線に対して, 上の課題 (1) を解決する。すなわち,C_{ab}曲線のヤコビアン群における加算を実行する効率的なアルゴリズムを求め, そのソフトウェアによる実行速度を示し, C_{ab}曲線を用いて実用的な離散対数型暗号を構成し得ることを示す。

以下,**2.** では, 代数曲線のヤコビアン群, 多項式環のイデアルの Gröbner 基底等について準備を行う. **3.** では,C_{ab}曲線を導入し, その基本的な性質をみる. **4.** では,C_{ab}曲線のヤコビアン群を因子によって表現し, その加算アルゴリズムを求める. **5.** では,**4.** で求めた,

† NEC C&C メディア研究所, 神奈川県
C&C Media Research Laboratories, NEC, 1-1, Miyakzaki 4-chome, Miyamae-ku, Kawasaki, Kanagawa 216, Japan

因子により表現された加算アルゴリズムをイデアル表現によるアルゴリズムに変換し, アルゴリズムの細部を具体化する. **6.** では,**5.** で求めた, イデアル表現による加算アルゴリズムのソフトウェア実装による速度評価を行い, 本アルゴリズムの実用性を確認する. **7.** では,C_{ab}曲線のヤコビアン群に基づく離散対数型暗号の暗号化/復号化関数を構成する.

2. 準　　備

代数曲線のヤコビアン群および多項式環のイデアルの Gröbner 基底等について後で用いる事柄をまとめる。

2.1 代数曲線のヤコビアン群

有限体 K 上定義された代数曲線 C をとる。K の代数閉包を$\overline{K}$と書く。整数 m_iと曲線 C の$\overline{K}$上の点 (厳密には, 座)P_iに対して, 形式和 $D=\sum m_iP_i$ を因子という。すべての 0 でない係数 m_iが正のとき, 因子 $D=\sum m_iP_i$は正であるという。また, 整数 $m=\sum m_i$を因子 $D=\sum m_iP_i$の次数と呼び,$deg(D)$ とかく。曲線 C 上のすべての因子は形式的な加算のもとでアーベル群$\boldsymbol{D}$を成し, 次数が 0 に等しいすべての因子はその部分群$\boldsymbol{D^0}$を成す。ガロア群 $Gal(\overline{K}\mid K)$ は$\boldsymbol{D}$および$\boldsymbol{D^0}$に自然に作用するが, その固定部分群をそれぞれ$\boldsymbol{D_K}$および$\boldsymbol{D_K^0}$とかく。$\boldsymbol{D_K}$ の元は K 上定義された因子と呼ばれる。

曲線 C 上の関数 f が, 曲線上の点 P において位数 n の零点 (or, 極) を持つとき,$v_P(f)=n(or,-n)$ とかく。このとき, 関数 f は因子 $(f):=\sum_P v_P(f)P$ を定めるが, これは常に次数 0 の因子となり, 関数 f の主因子と呼ばれる。主因子 (f) の正の部分 $(f)_0:=\sum_{P,v_P(f)\geqq 0} v_P(f)P$ を f の零因子, 負の部分 $(f)_\infty:=\sum_{P,v_P(f)\leqq 0} -v_P(f)P$ を f の極因子と呼ぶ。$(f)=(f)_0-(f)_\infty$ である。曲線 C 上のすべての主因子 $\{(f)\mid f\in\overline{K}(C)\}$ は,$\boldsymbol{D^0}$の部分群$\boldsymbol{P}$をなす。曲線 C のヤコビアン群 $J(C)$ とは,$\boldsymbol{D^0}$の部分群$\boldsymbol{P}$による剰余群である。ガロア群 $Gal(\overline{K}\mid K)$ の作用に関する固定部分群 $J_K(C)$ を K 上定義されたヤコビアン群と呼ぶ。以降で実際に計算するのは,$J_K(C)$ である。

K 上定義された因子 D に対して,

$$L(D)=\{f\in K(C)\mid (f)+D\geqq 0\}\cup\{0\}$$

は K 上の有限次元ベクトル空間となる。曲線 C の種数を g とすると,Riemann の定理より,$dim\ L(D)\geqq deg(D)+1-g$ である。

詳細は, [10], [18] を参照。

2.2 単項式順序と Gröbner 基底

負でない整数全体を$\boldsymbol{Z}_{\geqq 0}$とかく。n 変数単項式 $x^\alpha=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$に対して, n 個の整数の組 $\alpha=(\alpha_1,\cdots,\alpha_n)\in\boldsymbol{Z}_{\geqq 0}^n$をその multi-degree とよび,MD($x^\alpha$) とかく。$\boldsymbol{Z}_{\geqq 0}^n$上の整列順序<が, 任意の $\gamma\in\boldsymbol{Z}_{\geqq 0}^n$に対して, $\alpha<\beta$ならば, 常に$\alpha+\gamma<\beta+\gamma$ をみたすとき, 整列順序<は単項式順序と呼ばれる。単項式順序<が multi-degree を通して定める n 変数単項式に対する順序も単項式順序とよぶ。与えられた単項式順序に対して,n 変数多項式 f に現れる単項式のうち, 最大の単項式を f の leading monomial とよび,LM(f) とかく。単項式順序を用いれば, 多項式 f を多項式の集合 G でわるという形で,n 変数多項式の割り算アルゴリズムを記述することができる。

多項式 $g_1,\cdots,g_m$によって生成されるイデアルを $\langle g_1,\cdots,g_m\rangle$ とかく。ある単項式順序が与えられたとする。多項式環 $K[x_1,\cdots,x_n]$ のイデアル I とその部分集合 $G=\{g_1,\cdots,g_m\}$ をとる。$g_1,\cdots,g_m$ の leading monomial がイデアル I に属する多項式の leading monomial を生成するとき, すなわち, $\langle \mathrm{LM}(I)\rangle=\langle \mathrm{LM}(g_1),\cdots,\mathrm{LM}(g_m)\rangle$ が成立するとき,G はイデアル I の Gröbner 基底と呼ばれる。イデアル I の Gröbner 基底 $G=\{g_1,\cdots,g_m\}$ はイデアル I を生成する:$I=\langle g_1,\cdots,g_m\rangle$。多項式環 $K[x_1,\cdots,x_n]$ の任意のイデアルは Gröbner 基底をもつ。

イデアル I に対して, イデアル I に含まれるどのような多項式の leading monomial の multi-degree にもならない$\alpha\in\boldsymbol{Z}_{\geqq 0}^n$の全体を, イデアル I のΔ集合と呼び,$\Delta(I)$ とかく:

$$\Delta(I)=\{\alpha\in\boldsymbol{Z}_{\geqq 0}^n\mid x^\alpha\notin \mathrm{LM}(I)\}.$$

Δ集合$\Delta(I)$ の要素数を$\delta(I)$ とかく。一方, 多項式の集合 $G=\{g_1,\cdots,g_m\}$ に対して,

$$\delta(g_1,\cdots,g_m):=\sharp\,(\boldsymbol{Z}_{\geqq 0}^n-\cup_{i=1}^m(\mathrm{MD}(\mathrm{LM}(g_i))+\boldsymbol{Z}_{\geqq 0}^n)).$$

とおく ($\sharp S$ は集合 S の要素数を示す)。このとき,$\delta(I)$ が有限となる任意のイデアル I とその部分集合 $G=\{g_1,\cdots,g_m\}$ に対して,

$$\text{G が I の Gröbner basis}\Leftrightarrow\delta(I)=\delta(g_1,\cdots,g_m)\quad(1)$$

が成立する。

Gröbner 基底は n 変数多項式に対する割り算アルゴリズムを正当化する。すなわち, 多項式 f がイデアル I に属する必要十分条件は,f を I の Gröbner 基底でわった余りが 0 になることである。また, イデアル I に対してその Gröbner 基底は一意ではないが, reduced Gröbner 基底は一意である。イデアル I の Gröbner 基底が reduced であるとは, 1) G の任意の元 p について,LM(p) の係数が 1 に等しく, 2) G の任意の元 p について, p に含まれるどの単項式もイデアル $\langle \mathrm{LM}(G-\{p\})\rangle$ に含まれないときにいう。

詳細は, [17] を参照。

3. C_{ab} 曲　線

[9] に従いC_{ab}曲線を定義し, 後に必要となる基本的な性質をまとめる。

有限体 K 上定義され, 少なくとも一つは K 上の 1 次の座をもつ代数曲線 C をとる。P を曲線 C の 1 次の座とする。座 P 以外では正則な C 上の関数全体を $L(\infty P)$ とおく：

$$L(\infty P) = \{f \in K(C) \mid v_Q(f) \geqq 0 \ (\forall Q \neq P)\}.$$

$L(\infty P)$ に属する関数 f の P での極位数全体を M_P とおく：

$$M_P = \{-v_P(f) \mid f \in L(\infty P)\}.$$

M_Pは加法に関して (単位的) 半群をなす

［定義 1］(C_{ab} 曲線)　半群 M_Pが 2 つの自然数 a と b で生成されるとき, 組 (C,P) をC_{ab} 曲線とよぶ。

(C,P) をC_{ab} 曲線とする。定義より,P での極位数が a となる関数 $x \in L(\infty P)$ および b となる関数 $y \in L(\infty P)$ が存在する。これらの関数 x と y を用いて以下のようなC_{ab} 曲線のアフィンモデルが得られる：

$$\sum_{0\leqq i\leqq b, 0\leqq j\leqq a, ai+bj\leqq ab} \alpha_{i,j} x^i y^j = 0. \qquad (2)$$

ここで,$\alpha_{i,j}$は K の元で,$\alpha_{b,0}$および$\alpha_{0,a}$はともに 0 ではない。式 (2) のアフィンモデルをC_{ab} 曲線 (C,P) の三浦標準形と呼ぶ。三浦標準形では,C_{ab}曲線はアフィン平面で非特異であり, 座 P は曲線 C の唯一の無限遠点 P_∞となる。

逆に, $\alpha_{b,0}$および$\alpha_{0,a}$がともに 0 でないとき, 式 (2) で定義される平面曲線は常に絶対既約であり, さらにアフィン平面で非特異のとき, C_{ab} 曲線 (C,P_∞) となる.

楕円曲線は C_{23}曲線, 超楕円曲線は C_{2b}曲線に他ならない。C_{ab}曲線の種数は $(a-1)(b-1)/2$ に等しい。以後,C_{ab}曲線は常に三浦標準形で扱う。

C_{ab}曲線に対する計算において, 以下の, 単項式順序である,C_{ab}順序$>_{cab}$が基本的である。

［定義 2］(C_{ab}順序)　$\alpha = (\alpha_1,\alpha_2)$, と　$\beta = (\beta_1,\beta_2) \in \boldsymbol{Z}^2_{\geqq 0}$ に対して, 以下の (i) または (ii) が成立するとき,$\alpha >_{cab} \beta$とする：

$$(i)\quad a\alpha_1 + b\alpha_2 > a\beta_1 + b\beta_2$$
$$(ii)\quad a\alpha_1 + b\alpha_2 = a\beta_1 + b\beta_2,\ \alpha_1 < \beta_1.$$

単項式 $X^\alpha Y^\beta$は,C_{ab}曲線上の関数とみなしたとき, 無限遠点 P_∞以外では正則である。C_{ab}順序では, 単項式 $X^\alpha Y^\beta$は, その無限遠点 P_∞での極位数 $-v_{P_\infty}(x^\alpha y^\beta) = a\alpha + b\beta$ にもとづいて整列され, 無限遠点 P_∞での極位数が等しいときは,X に関する次数の大きいほうが小さいとされる。

4. 因子表現によるヤコビアン群加算アルゴリズム

[13] や [14] にあるように,Noether の Residue Divisor Theorem [15] を用いて, 完全体上の平面曲線のヤコビアン群の加算を計算することができる。しかしながら, この一般的で直接的な方法では, 終結式の計算を必要としたり, また場合分けが多数発生したりして, 現実の暗号ソフトウェア・装置への応用は望めない。

我々は, 対象をC_{ab}曲線に限定して, そのヤコビアン群の効率的な計算アルゴリズムを求める。本節では, まず, 因子表現によってC_{ab}曲線のヤコビアン群の演算を取り扱う。

有限体 K 上定義されたC_{ab}曲線 C をとる。曲線 C の種数を $g=(a-1)(b-1)/2$ とおく。$\boldsymbol{D_K}$,$\boldsymbol{D^0_K}$および$\boldsymbol{P_K}$を, それぞれ, 曲線 C の,K 上の因子群, 次数 0 の因子群および主因子群とする。曲線 C のヤコビアン群 $J_K(C) = \boldsymbol{D^0_K}/\boldsymbol{P_K}$の元 j が代表元として因子 $D \in \boldsymbol{D^0_K}$ をもつとき,$j=[D]$ とかく：

$$J_K(C) \simeq \boldsymbol{D^0_K}/\boldsymbol{P_K}$$
$$j \mapsto [D].$$

［定義 3］　P_∞と素な正の因子 E と g 以下の自然数 n を用いて, $D = E - n\,P_\infty$と表された 0 次の因子 D を

semi-normal な因子と呼ぶ。

［補題 4］ ヤコビアン群 $J_K(C)$ の任意の元 j は, 常に semi-normal な因子を代表元にもつ.

［証明 ］ 定義より, ある 0 次因子 D があって,$j = [D]$. Riemann の定理より,$\dim L(D + g\,P_\infty) \geqq g + 1 - g = 1$. よって, ある 0 でない関数 f があって,$D + g\,P_\infty + (f) \geqq 0$. $E = D + g\,P_\infty + (f)$ とおけば,$j = [E - g\,P_\infty]$. □

補題 4 より, ヤコビアン群の任意の元は,semi-normal な因子で表されるが, 一般に対応する semi-normal な因子は一意ではない。対応する因子を一意化するために, 以下のアルゴリズムを用いる。

［アルゴリズム 1］ 入力:次数 0 の因子 $D = E - nP_\infty$. ただし,E は正因子で,P_∞ と素.

出力： $-D$ と同値な semi-normal な因子 G.

1° $(f)_0 \geqq E$ を満たす,$L(\infty P_\infty)$ に属する関数 f で, 極位数$-v_{P_\infty}(f)$ が最小の f を求める.

2° $G \leftarrow -D + (f)$

Algorithm1 は $j \in J_K(C)$ に対応する因子を一意化する：

［命題 5］ 互いに同値な任意の semi-normal な因子に対して, アルゴリズム 1 は同一の因子を出力する.

［証明 ］ $D_1 = E_1 - nP_\infty$と $D_2 = E_2 - nP_\infty$ を互いに同値な semi-normal な因子とする. ある 0 でない関数λがあって, $E_1 - n_1P_\infty = E_2 - n_2P_\infty + (\lambda)$ である. D_1に対して, アルゴリズム 1 にあるように, $\mathrm{Supp}((f_1)_\infty) \subsetneqq \{P_\infty\}$, $(f_1)_0 \geqq E_1$ を満たす関数 f_1をとると (ここで,$\mathrm{Supp}(D)$ は因子 D の台を表す), $(f_1\lambda^{-1}) = (f_1) - (\lambda) = (f_1)_0 - E_1 + E_2 + (n_1 - k_1 - n_2)\infty$. ここで,$(f_1)_0 - E_1 + E_2 \geqq E_2$なので,$f_2 = f_1\lambda^{-1}$とおくと, f_2は, $\mathrm{Supp}((f_2)_\infty) \subsetneqq \{P_\infty\}$, $(f_2)_0 \geqq E_2$ をみたす. λは f_1 および f_2の選択とは独立なので, 対応 $f_1 \mapsto f_2 = f_1\lambda^{-1}$は P_∞での極位数が最小のもの同士を対応づける。すると, $-E_2 + n_2P_\infty + (f_2) = -E_2 + n_2P_\infty + (f_1) - E_1 + E_2 + (n_1 - n_2)P_\infty = -E_1 + n_1P_\infty + (f_1)$ より,D_1,D_2に対するアルゴリズム 1 の出力は同一であることがわかる。□

［定義 6］ アルゴリズム 1 の出力として得られる (semi-normal な) 因子を normal な因子とよぶ。

アルゴリズム 1 は入力された因子の-1 倍に同値な因子を出力するので, 2 回続けて作用させれば, 入力された因子と同値な normal な因子が得られる。補題 4 と命題 5 より,

［定理 7］ ヤコビアン群の任意の元は normal な因子によって一意的に表される。

定理 7 より, 以下のヤコビアン群における加算アルゴリズムを得る：

［アルゴリズム 2］ 入力：semi-normal な因子 $D_1 = E_1 - n_1P_\infty$と $D_2 = E_2 - n_2P_\infty$

出力：$D_1 + D_2$に同値な normal な因子 $D_3 = E_3 - n_3P_\infty$

1° $D_1 + D_2 = (E_1 + E_2) - (n_1 + n_2)P_\infty$にアルゴリズム 1 を作用させて, normal な因子 $D' = E' - n'P_\infty$ を得る.

2° normal な因子 $D' = E' - n'P_\infty$にアルゴリズム 1 を作用させて, normal な因子 $D_3 = E_3 - n_3P_\infty$を得て出力する.

アルゴリズム 1 および 2 を直接に計算機上で実行するには, 因子を取り扱う必要がある。因子の直接的な計算は, 多項式の既約因子分解等を必要とし, 効率が悪い。そこで, 次節で, 因子表現を取り止め, イデアル表現によりアルゴリズム 1 および 2 を実現する。

5. イデアル表現によるヤコビアン群加算アルゴリズム

C_{ab}曲線のヤコビアン群とその座標環のイデアル類群との自然な同型を利用して, アルゴリズム 1 および 2 をイデアル計算を用いて実現する。

5.1 加算アルゴリズムの構成

有限体 K 上の, 定義式 $F(X,Y) = \sum_{0 \leqq i \leqq b, 0 \leqq j \leqq a, ai+bj \leqq ab} \alpha_{i,j} X^i Y^j = 0$ をもつ,C_{ab}曲線 C をとる。C_{ab}曲線 C はアフィン平面で非特異なので, その座標環 $K[x,y] = K[X,Y]/(F(X,Y))$ はデデキント整域である。

一般に, 座標環 A_Kがデデキント整域になる代数曲線 C に対して, そのヤコビアン群 $J_K(C)$ は座標環 A_Kのイデアル類群 $H(A_K)$ に自然に同型となる [16]。C_{ab}曲線 C に対しては, その同型Φは

$$\Phi : \begin{array}{ccc} J_K(C) & \tilde{\to} & H(A_K) \\ [\sum_P n_P P - nP_\infty] & \mapsto & [L(\infty P_\infty - \sum_P n_P P)]. \end{array}$$

となる。

同型Φによって normal な因子に対応するイデアルを normal なイデアルとよぶ (A_Kのすべてのイデアルは semi-normal な因子に対応することに注意)。C_{ab} 順序は, 単項式を,C_{ab}曲線上の関数とみなしたときの,P_∞での極位数で順序付けたことに注意して, アル

ゴリズム 1 および 2 に同型Φを作用させて, 以下のイデアル表現によるアルゴリズム 3 および 4 を得る。

［アルゴリズム 3］ 入力：座標環 A_Kのイデアル I
出力：I の逆イデアルに同値な normal なイデアル J
1° イデアル I に属する,C_{ab}順序に関して最小の多項式 $f(\neq 0)$ を求める.
2° $(f) = I \cdot J$ となるイデアル J を求める.

［アルゴリズム 4］ 入力：座標環 A_Kのイデアル I_1と I_2
出力：イデアル積 $I_1 \cdot I_2$に同値な normal なイデアル I_3
1° イデアル積 $I_1 \cdot I_2$にアルゴリズム 3 を作用させて,normal なイデアル J を得る.
2° イデアル J にアルゴリズム 3 を作用させて,normal なイデアル I_3を得る.

アルゴリズム 4 ではアルゴリズム 3 を 2 回呼び出しているが, これらは以下のようにして融合することができる. アルゴリズム 3 の最初の呼び出しで, 多項式 f とイデアル J を得たとすると, $(f) = I_1 \cdot I_2 \cdot J$ が成立している. 同様に, アルゴリズム 3 の 2 回目の呼び出しで, 多項式 g とイデアル I_3を得たとすると, $(g) = J \cdot I_3$. これらの関係から, $I_1 \cdot I_2 \cdot (g) = I_1 \cdot I_2 \cdot J \cdot I_3 = (f) \cdot I_3$ を得る. よって, アルゴリズム 4 の出力であるイデアル I_3は, $I_3 = g/f \cdot I_1 \cdot I_2$ を満たす. このようにして,C_{ab}曲線のヤコビアン群における加算アルゴリズムとして, 以下のアルゴリズム 5 を得る. ただし, アルゴリズム 5 では, 単項式順序として,C_{ab}順序を用いる.

［アルゴリズム 5］ C_{ab}曲線の定義式を $F(X,Y) = 0$ とする.
入力: 座標環 $K[X,Y]/(F(X,Y))$ のイデアル I_1と I_2
出力：座標環 $K[X,Y]/(F(X,Y))$ の normal なイデアル I_3

1° $J \leftarrow I_1 \cdot I_2$
2° $f \leftarrow$ 最小の多項式 $f(\neq 0) \in J$
3° $g \leftarrow$ 最小の多項式 $g(\neq 0)$ s.t. $g \cdot J \subseteqq \langle f, F \rangle$
4° $I_3 \leftarrow g/f \cdot J$

5.2 C_{ab}順序に関する Gröbner 基底

アルゴリズム 5 の入出力に現れるイデアルはC_{ab}順序に関する Gröbner 基底で表示する. ここでは,C_{ab}順序に関する Gröbner 基底について考察する.

［命題 8］ 任意の semi-normal な因子 $E - n\infty$ とそれに同型Φで対応するイデアル I に対して, $\deg(E) = \delta(I)$ となる.

［証明 ］ 示したい両辺は係数体の拡大に関して不変なので, 定義体 K は代数閉体としてよい. よって, $E = \sum n_P P$ に対応するイデアル I は, $I = \Phi(E) = \prod I_P^{n_P}$である. ここで,$I_P$は点 P における極大イデアル. [17]Chap5.Sec3.Prop.4 より, $\delta(I) = \dim_K A/I$ である. 一方, $A/I = \sum_P A/I_P^{n_P}$であり,C_{ab}曲線 C はアフィン平面で非特異なので, $\dim_K A/I_P^{n_P} = n_P$. したがって,$\dim A/I = \sum_P n_P = \deg(E)$. □

命題 8 を用いれば, イデアルのC_{ab}順序に関する Gröbner 基底の形がわかる. 例えば,C_{34}曲線に関して,

［命題 9］ C_{34}曲線 C のヤコビアン群 $J_K(C)$ の一般元に対応するイデアルは, C_{34}順序に関して, $\{a_0+a_1X+a_2Y+X^2, b_0+b_1X+b_2Y+XY, c_0+c_1X+c_2Y+Y^2\}$ という形の reduced Gröbner 基底を持つ.

［証明 ］ C の種数は $g(C) = (3-1)(4-1)/2 = 3$ なので, ヤコビアン群 $J_K(C)$ の一般元 $j = [P_1 + P_2 + P_3 - 3P_\infty]$ は, 曲線 C 上の 3 点 $\{P_1, P_2, P_3\}$ に対応する. C_{34}順序に関して,4 番目の単項式は X^2,5 番目は XY, 6 番目は Y^2である. よって,j に対応するイデアル I は,$X^2 + \cdots, XY + \cdots, Y^2 + \cdots$という形の 3 つの多項式を含むことがわかる (ここで,$\cdots$はより低次の項を表す). $\delta(X^2 + \cdots, XY + \cdots, Y^2 + \cdots) = 3$ であり, 一方, 命題 8 より,$\delta(I) = deg(P_1 + P_2 + P_3) = 3$ である. よって,2.2 節の (1) より, 上の $\{X^2 + \cdots, XY + \cdots, Y^2 + \cdots\}$ はイデアル I の Gröbner 基底である. □

上では,C_{34}曲線上の normal な因子を扱ったが, 一般のC_{ab}曲線上の任意の semi-normal な因子に対しても同様にして対応するイデアルの Gröbner 基底の形を求めることができる. Δ集合の形状から容易にわかるように, 一般のC_{ab}曲線の場合でも Gröbner 基底の要素数は a 個以下である.

5.3 加算アルゴリズムの詳細

アルゴリズム 5 の実行例を示しながら, その詳細を説明する. 例として, 素体 $GF(17)$ 上の多項式 $F = Y^3 + X^4 + 1$ で定義される C_{34}曲線 C をとりあげ, そのヤコビアン群 $J_{GF(17)}(C)$ の元 (に対応するイデアル) $I = \{f_1 = X^2 + 14Y + 4X + 5, f_2 = XY + 3Y + 4X + 9, f_3 = Y^2 + 9Y + 16X + 2\}$ (命題 9 参照) の 2 倍を計算する.

C_{34}順序では, 単項式は, 小さいほうから, $1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, \cdots$ と並ぶ.

以後, 多項式 f を多項式集合 G でわった余りを$\overline{f}^G$とかく.

1° イデアル積 $I \cdot I$ を計算する.

イデアル積 $I \cdot I$ は曲線上の 6 個の点に対応し, C_{34} 順序で 7 番目の単項式が X^3であることに注意すると, 命題 9 の証明と同様にして, イデアル積 $I \cdot I$ の Gröbner 基底は, $\{X^3+\cdots, X^2Y+\cdots, XY^2+\cdots\}$ という形であることがわかる.

イデアル積 $I \cdot I$ を以下のように計算する：

$$
\begin{aligned}
g_1 &\leftarrow \overline{f_1^2}^{\{F\}} = X^4+\cdots \\
g_2 &\leftarrow \overline{f_1 \cdot f_2}^{\{g_1,F\}} = X^3Y+\cdots \\
g_3 &\leftarrow \overline{f_2^2}^{\{g_2,g_1,F\}} = X^2Y^2+\cdots \\
g_4 &\leftarrow \overline{f_1 \cdot f_3}^{\{g_3,g_2,g_1,F\}} = XY^2+\cdots \\
g_5 &\leftarrow \overline{f_2 \cdot f_3}^{\{g_4,g_3,g_2,g_1,F\}} = X^2Y+\cdots \\
g_6 &\leftarrow \overline{f_3^2}^{\{g_5,g_4,g_3,g_2,g_1,F\}} = X^3+\cdots
\end{aligned}
$$

よって, $J \leftarrow I \cdot I = \{g_6, g_5, g_4\}$ となり, これは, 上に注意したことより, イデアル J の Gröbner 基底による表示である.

2° $f \leftarrow g_6 = X^3+10Y^2+5XY+7Y+11X+4$

3° $h \cdot J \subset \langle f, F\rangle$ となる最小の多項式 $h(\neq 0)$ を求める.

$LM(f) = X^3$と $LM(F) = Y^3$は互いに素なので, $\{f, F\}$ はイデアル $\langle f, F\rangle$ の Gröbner 基底であることに注意する. 多項式 g_5と各単項式の積の $\{f, F\}$ による余りを, 昇べきの順で計算すると,

$$
\begin{aligned}
\overline{g_5}^{\{f,F\}} &= X^2Y+\cdots \\
\overline{Xg_5}^{\{f,F\}} &= XY^2+\cdots \\
\overline{Yg_5}^{\{f,F\}} &= X^2Y^2+\cdots
\end{aligned}
$$

さらに,$\overline{X^2g_5}^{\{f,F\}}$を計算すると, $4X^2Y^2+\cdots$を得るが, その leading monomial X^2Y^2は$\overline{Yg_5}^{\{f,F\}}$のそれと同じである. よって, $X^2g_5 \equiv 4Yg_5+12XY^2+\cdots$ $(\mathrm{mod}\ \{f, F\})$. さらに, ここで, XY^2 は$\overline{Xg_5}^{\{f,F\}}$ の leading monomial であることに注意して, 以下, 同様の計算を行うと,

$$X^2g_5 \equiv 4Yg_5+12Xg_5+2g_5 \pmod{\{f, F\}}.$$

よって,$h \leftarrow X^2+13Y+5X+15$.

4°

$$
\begin{aligned}
(h/f) \cdot J &= (h/f) \cdot \{g_6, g_5, g_4\} \\
&= \{h, (hg_5)/f, (hg_4)/f\}
\end{aligned}
$$

hg_5および hg_4を $\{f, F\}$ で割って, それぞれ商 $\{a_5, b_5\}$ および $\{a_4, b_4\}$ を得たとすると,

$$
\begin{aligned}
I_3 &\leftarrow \{h, (hg_5)/f, (hg_4)/f\} \\
&\equiv \{h, a_5, a_4\} \pmod{\{F\}} \\
&= \{X^2+13Y+5X+15, XY+13Y+5X+11, \\
&\quad Y^2+5Y+12X+6\}
\end{aligned}
$$

これは, イデアル I_3の Gröbner 基底による表示である.

以上の議論より, アルゴリズム 5 を詳細化して, 以下の, ヤコビアン群の加算アルゴリズム 6 を得る. 以下では,$\{\{c_1, c_2, \cdots, c_a\}, r\} \leftarrow \mathrm{Division}(g, G)$ は, 多項式 g を多項式集合 G でわって, 商として $\{c_1, c_2, \cdots, c_a\}$ を, 余りとして r を得ることを示す (詳細は [17] を参照). また,$\{\{a_1, \cdots, a_i\}, r\} \leftarrow \mathrm{Coefficients}(f, r_1, \cdots, r_i)$ は, 多項式 f を $r_1, \cdots, r_i$の線形結合で表示して, 商として $\{a_1, \cdots, a_i\}$ を, 余りとして r を得ることを示す (すなわち,$f = \sum_{k=1}^{i} a_k r_k + r$). また,$Mono_i$は$C_{ab}$ 順序で i 番目の単項式を示す ($Mono_1 = 1, Mono_2 = X, \cdots$).

[アルゴリズム 6]

algorithm JacobianSum(inputs $\mathbf{I_1}, \mathbf{I_2}$, output $\mathbf{I_3}$)
  $I_3 \leftarrow \mathrm{Compose}(I_1, I_2)$
  $f \leftarrow$ the minimum element of I_3
  $I_3 \leftarrow \mathrm{Reduce}(f, I_3)$
  RETURN $\mathbf{I_3}$

subroutine Compose(inputs $\mathbf{I_1} = \{\mathbf{f_1}, \mathbf{f_2}, \cdots, \mathbf{f_a}\}, \mathbf{I_2} = \{\mathbf{g_1}, \mathbf{g_2}, \cdots, \mathbf{g_a}\}$, output I_3)
  $I_3 \leftarrow \{F\}$
  FOR i = 1 TO a, **j = 1 TO a DO**
    $g \leftarrow \overline{f_i \cdot g_j}^{I_3}$
    $I_3 \leftarrow \{g\} \cup I_3$
  IF $\delta(\mathbf{I_3}) > \delta(\mathbf{I_1}) + \delta(\mathbf{I_2})$ **THEN** $\mathbf{I_3} \leftarrow \mathrm{Buchberger}(\delta(\mathbf{I_1}) + \delta(\mathbf{I_2}), \mathbf{I_3})$
  $I_3 \leftarrow$ the set of the minimum a elements of I_3
  RETURN $\mathbf{I_3}$

subroutine Reduce(inputs $\mathbf{f}, \mathbf{I} = \{\mathbf{f_1}, \mathbf{f_2}, \cdots, \mathbf{f_a}\}$, output $\mathbf{J}$)
  $G \leftarrow \{f, \overline{f \cdot y}^{\{F\}}, \cdots, \overline{f \cdot y^{a-1}}^{\{F\}}, F\}$
  LABEL(retry)
  $J \leftarrow \{\}$
  $h \leftarrow \sum_{i=1}^{a} (\text{random number}) \cdot f_i$
  $g \leftarrow \mathrm{Divide}(G, h)$
  FOR i = 1 TO a
    $\{\{c_1, c_2, \cdots, c_a\}, r\} \leftarrow \mathrm{Division}(g \cdot f_i, G)$
    IF r ≠ 0 THEN GOTO retry
    $k \leftarrow c_1 + c_2 \cdot y + \cdots + c_a \cdot y^{a-1}$
    $J \leftarrow J \cup \{k\}$
  RETURN J

subroutine Divide(inputs $\mathbf{G}, \mathbf{h}$, output $\mathbf{s}$)
  $r_1 \leftarrow \overline{Mono_1 \cdot h}^{G}$
  $s_1 \leftarrow Mono_1$
  $i \leftarrow 1$
  WHILE $\mathbf{r_i} \neq \mathbf{0}$ **DO**

$i \leftarrow i+1$
$r_i \leftarrow \overline{Mono_i \cdot h}^{G}$
$\{\{A_1, \cdots, A_{i-1}\}, r_i\} \leftarrow \text{Coefficients}(r_i, \{r_1, \cdots, r_{i-1}\})$
$s_i \leftarrow Mono_i - \sum_{j=1}^{i-1} A_j s_j$
RETURN $\mathbf{s_i}$

subroutine Buchberger(inputs $\mathbf{m}, \mathbf{I} = \{\mathbf{f_1}, \cdots, \mathbf{f_s}\}$,
output $G = \{g_1, \cdots, g_t\}$)
$B \leftarrow \{(i,j) \mid 1 \leqq i < j \leqq s\}$
$G \leftarrow F$
$t \leftarrow s$
WHILE $\mathbf{B} \neq \phi$ **AND** $\delta(\mathbf{G}) > \mathbf{m}$ **DO**
Select $(i,j) \in B$
IF $\text{LCM}(\text{LT}(\mathbf{f_i}), \text{LT}(\mathbf{f_j})) \neq \text{LT}(\mathbf{f_i})\text{LT}(\mathbf{f_j})$ **THEN**
$S \leftarrow \overline{\text{S}(f_i, f_j)}^{G}$
IF $\mathbf{S \neq 0}$ **THEN**
$t \leftarrow t+1; f_t \leftarrow S$
$G \leftarrow G \cup \{f_t\}$
$B \leftarrow B \cup \{(i,t) \mid 1 \leqq i \leqq t-1\}$
$B \leftarrow B - \{(i,j)\}$
RETURN G

アルゴリズム 6 において, subroutine Compose が上記計算例のステップ 1,subroutine Divide がステップ 3，subroutine Reduce がステップ 4 に相当する.

アルゴリズム 6 の計算量について考察する．アルゴリズム 6 の計算量はサブルーチン Buchberger に支配されている．サブルーチン Buchberger において, 集合 B の要素数は $O(g^2)$ 個なので, 最悪では,$O(g^2)$ 個の S 多項式に対して, その G による余りを求める必要があり, 計算量は, (定義体上の掛算の個数でみて)$O(g^4)$ となる.

しかし, アルゴリズム 6 において, サブルーチン Buchberger により Gröbner 基底を求めるとき, 常に事前に, 命題 8 を用いて, そのΔ集合の位数を知ることができる．そこで, サブルーチン Buchberger では,G のΔ集合の位数を監視し, それが入力である m, すなわち事前情報である Gröbner 基底のΔ集合の位数, に等しくなり次第アルゴリズムを終了している. これより, サブルーチン Buchberger において, 集合 B より (i,j) を選択するスケジューリングが適切であると仮定すると,$O(g)$ 個の (i,j) に対して S 式の G による余りを計算すればよく, アルゴリズム 6 の計算量は $O(g^3)$ となる.

適切な場合分けを行うことで, 上記のようなスケジューリングを施さなくても, 無駄な S 式の割り算は発生しないことが確認された．したがって, アルゴリズム 6 の計算量は, 事実上,$O(g^3)$ であるといえる.

表 1　C_{35}曲線の演算速度 (ms on 266MHZ,PentiumII).
Table 1　Performance for C_{35} curve.(ms on 266MHZ, PentiumII).

	simple	random
Sum	3.39	3.65
Double	3.76	4.21
Scalar	862	958

表 2　C_{37}曲線の演算速度 (ms on 266MHZ,PentiumII).
Table 2　Performance for C_{37} curve.(ms on 266MHZ, PentiumII).

	simple	random
Sum	1.15	1.24
Double	1.15	1.28
Scalar	273	300

6. ソフトウェア実装による速度評価

アルゴリズム 6 をソフトウェア実装し, 速度評価を行った．C_{35}曲線,C_{37}曲線および $C_{2,13}$曲線に対する結果をそれぞれ, 表 1, 表 2 および表 3 に示す. 266MHZ,Pentium II 上で実行した. 単位は millisecond である.

各ケースとも約 160 ビットのヤコビアン群をもつ曲線を取り上げている．表中,Sum,Double,Scalar はそれぞれ, 加算,2 倍算,160 ビットのスカラー倍演算を示す．また表中,simple とは $Y^a + \alpha X^b + \beta$という形の定義式をもつランダムなC_{ab}曲線, random とは各係数を一様ランダムに選んだC_{ab}曲線に対する演算速度を示す.

離散対数型暗号では, 暗号化の速度は 2 回のスカラー倍演算, 復号化の速度は 1 回のスカラー倍演算の速度にほぼ等しい. 表 2,3 より, スカラー倍演算は, 約 160 ビットのヤコビアン群をもつランダムな C_{37}曲線に対しては 300ms で, $C_{2,13}$曲線に対しては,167ms で実行されている．これは,C_{ab}曲線を用いた離散対数型暗号の実用可能性を示すものである.

7. 暗号化/復号化関数

例として, 有限体 $GF(q)$ 上の C_{34}曲線 C を取り上げ, 曲線 C のヤコビアン群に基づいて, 暗号化/復号化関数を構成する．C_{34}曲線 C の種数は 3 なので, ヤコビアン群 $J_{GF(q)}(C)$ の位数は q^3程度である．よっ

表 3 $C_{2,13}$曲線の演算速度 (ms on 266MHZ,PentiumII).
Table 3 Performance for $C_{2,13}$ curve.(ms on 266MHZ, PentiumII).

	simple	random
Sum	0.70	0.73
Double	0.65	0.68
Scalar	158	167

図 1 C_{34}曲線の暗号化/復号化関数
Fig. 1 Encryption and decryption functions on C_{34} curve.

て,160 ビットのヤコビアン群を得るには,q は 53 ビット程度あればよい.

命題 9 より, ヤコビアン群 $J_{GF(q)}(C)$ の一般元は, $\{a_0 + a_1X + a_2Y + X^2, b_0 + b_1X + b_2Y + XY, c_0 + c_1X + c_2Y + Y^2\}$ という形のイデアルで表される.

容易にわかるように, 上のイデアルは,$a_2 \neq 0$ のとき, 最初の 2 つの多項式 $a_0 + a_1X + a_2Y + X^2$ と $b_0 + b_1X + b_2Y + XY$ で生成される. 上の形のイデアルをランダムに選択するとき, $a_2 = 0$ となる確率は $1/q$ 程度なので, 定義体が十分大きいとき, ヤコビアン群 $J_{GF(q)}(C)$ の任意の元は,$6\log_2(q)$ ビットのベクトル $(a_0, a_1, a_2, b_0, b_1, b_2)$ で表される, としてよい.

ヤコビアン群 $J_{GF(q)}(C)$ の (適切な) 元 $j_0 = (a_0, a_1, a_2, b_0, b_1, b_2)$ を固定し, アルゴリズム 6 を用いて, べき和関数 $C(n) = n \cdot j_0$を構成する. 関数 $C(n)$ を一方向性関数として, 楕円曲線暗号のときと同様にして, 図 1 の暗号化/復号化関数を構成する. 図 1 で, 関数 X は,$j = (a_0, a_1, a_2, b_0, b_1, b_2) \in J_{GF(q)}(C)$ に対して, $X(j) = a0 \mid a_1 \mid a_2$('|' は連結) を出力するものとする.

8. むすび

本稿では, 楕円曲線や超楕円曲線を含む広いクラスの代数曲線であるC_{ab}曲線に対して, そのヤコビアン群における加算を実行する効率的なアルゴリズムを求めた. さらに, 上記アルゴリズムをソフトウェア実装し, 速度評価を行った. 約 160 ビットのヤコビアン群をもつ C_{37}曲線に対して, スカラー倍演算が 300ms で実行されるのをみた. これは,C_{ab}曲線を用いた離散対数型暗号の実用可能性を示すものである.

今後の課題は, 安全なC_{ab}曲線, とくにほぼ素数の位数のヤコビアン群もつC_{ab}曲線の探索である.

謝辞

本研究を進めるにあたり, 有益な御討論, 数多くの御助言をいただきました東京工業大学松本隆太郎氏,NEC 神谷典史氏そして SONY 三浦晋示氏に心より感謝致します.

文　献

[1] I.A.Semaev, "*Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p*," Math. Comp. 67, 353-356 (1998)

[2] T.Satoh, K.Araki, "*Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves*," COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI, vol. 47, No. 1, 81-92, 1998

[3] P.N.Smart, "*The discrete logarithm problem on elliptic curves of trace one*," To appear in J. Cryptology

[4] D.G.Cantor, "*Computing in the Jacobian of a hyperelliptic curve*," Mathematics of Computation, 48(177), pp.95-101,1987

[5] N.Koblitz, "*Hyperelliptic cryptosystems*," J.Cryptography,1(1989), pp.139-150

[6] N.Koblitz, "*A Very Easy Way to Generate Curves over Prime Fields for Hyperelliptic Cryptosytems*," Rump Talk, Crypto '97

[7] N.Matsuda,J.Chao,S.Tsujii, "*Efficient construction algorithms of secure hyperelliptic discrete logarithm problems*," IEICE ISEC96-18(1996)

[8] S.Miura,N.Kamiya, "*Geometric Goppa codes on some maximal curves and their minimum distance*," in Proc. IEEE Workshop on Information Theory (Susono-shi,Japan,June 1993), pp.85-86

[9] 三浦晋示, "アフィン代数曲線上の線形符号," 信学論 (A),vol. J81-A, No. 10, 1398-1421, Oct. 1998.

[10] J.H.Silverman, "*The Arithmetic of Elliptic Curves*," Springer-Verlag

[11] A.-M.Spallek, "*Kurven vom Geshlecht 2 und ihre Anwendung in Publick-Key-Kryptosystemen*," Doctor thesis, Universität GH Essen, 1994

[12] 内山 成憲, 齋藤 泰一, "トレース 2 の楕円曲線上の離散対数問題について", IEICE ISEC98(1998)

[13] E.J.Volcheck, "*Computing in the Jacobian of a plane algebraic curve*," ANTS-I, Lecture Notes in Computer Science, vol **877**(1994), Springer-Verlag, pp. 221-233
[14] M-D.Huang, D.Ierardi, "*Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve*," J. Symbolic Computation (1994) 18, 519-539
[15] W.Fulton, "*Algebraic Curves*," Addison-Wesley
[16] R.Hartshorne, "*Algebraic Geometry*," Springer-Verlag
[17] D.Cox, J.Little, D.O'Shea, "*Ideals, Varieties, and Algorithms*," Springer-Verlag
[18] H.Stichtenoth, "*Algebraic Function Fields and Codes*," Springer-Verlag

（平成年月日受付，月日再受付）

有田　正剛　（正員）

1990 年,NEC 入社。現在,C&C メディア研究所主任。電子情報通信学会, 日本数学会会員。