解　説

数論アルゴリズムとその応用

代数幾何学的アルゴリズム†

岡本龍明††　桜井幸一†††

数論は代数幾何学と密接な関係をもって研究されてきた．本稿では，数論と代数幾何学の接点である有限体上の代数曲線に関するいくつかの基本的なアルゴリズムについて解説を行う．これらアルゴリズムは，代数曲線上で符号や暗号を構成するうえでの基本的手法として大変有益である．

1. はじめに

代数曲線の理論を含む代数幾何学が大きく発展したのは 20 世紀に入ってからであり，今世紀の数学において中心的な役割を果たしてきたといえよう．最近になって，この純粋数学上の理論が，数論との接点において多くの実用的応用をもつことが知られるようになってきた．まず，その最初は，1980 年代初頭の Goppa による代数曲線上の符号理論であろう[8]（本特集号の松本・今井氏の記事を参考[22]）．引き続き，1980 年代半ばに，Lenstra により楕円曲線を利用した素因数分解アルゴリズムが発見された[21]（本特集号の小山・静谷氏の記事を参考[19]）．さらに，Goldwasser と Kilian による楕円曲線を利用した素数判定アルゴリズム[7]（本特集号の木田・牧野氏の記事を参考[14]）が，また，Miller と Koblitz により独立に楕円曲線を利用した公開鍵暗号[15),23]が提案された（本特集号の黒澤・藤岡・宮地氏の記事を参考[13]）．以降，これらの各分野において，代数曲線を用いた手法は活発に研究されてきており，現在では，これら各分野での中心的研究課題の一つになっている．

本稿では，このような応用分野で，共通に使われる基本的な代数曲線上のアルゴリズムの紹介を行う．まず，Schoof により発見された有限体上の楕円曲線の元の数を計算するアルゴリズム[33]及びその改良アルゴリズムについて述べる．このアルゴリズムは，Goldwasser-Kilian の素数判定アルゴリズムや，楕円曲線暗号のパラメータ設定，さらに有限体上での平方根を計算する決定的 (deterministic) アルゴリズムなどに広範に用いられる大変基本的で重要なアルゴリズムである．

次に，Miller により発見された楕円曲線上の Weil 対 (Weil pairing) を計算するアルゴリズムを示す[24]．また，この Weil 対のアルゴリズムを用いて，楕円曲線上の有限群の構造を定めるアルゴリズムや楕円曲線上の離散対数問題を計算するアルゴリズムが構成できることを示す．

引き続き，超楕円曲線上のヤコビ多様体の群演算アルゴリズムやヤコビ多様体の元の数を計算するアルゴリズムなどについての結果を簡単に紹介する．

最後に，一般の代数曲線上での Riemann-Roch の問題に関するアルゴリズムとそのヤコビ多様体の群演算を計算するアルゴリズムについて述べる．

2. 準　備

本章では，本稿を理解するうえで最低限必要となる概念，用語などを簡単に説明する．ここでは，極力平易に解説することを心がけたため，数学的厳密性に欠ける点があることをお断りしておく．詳しくは，楕円曲線や代数曲線の理論に関する教科書を参照されたい（たとえば，文献 6), 34)）．なお，整数論の基礎知識については，本特集号の一松氏の記事[10]を参考にされたい．

[楕円曲線]

元の数が $q=p^r$ (p: 素数) の有限体を F_q とする．F_q 上の楕円曲線 E は，$4a^3+27b^2\neq 0$ となるようなパラメータ a, $b\in F_q$ の値を定めることにより決まり，その元の集合 $E(F_q)$ は，

$$y^2=x^3+ax+b \qquad (1)$$

† Number Theoretic Algorithms in Algebraic Geometry by Tatsuaki OKAMOTO (NTT Network Information Systems Laboratories) and Kouichi SAKURAI (Computer & Information Systems Laboratory, Mitsubishi Electric Corp.).

†† NTT 情報通信網研究所
††† 三菱電機(株)情報電子研究所

を満足する $F_q \times F_q$ 上の点 (x, y) に仮想的な点である無限遠点 $\mathcal{O}$ を加えたものである（ただし，$p > 3$. $p=2, 3$ のときは，別の標準形となる）．$E(F_q)$ 上では，$\mathcal{O}$ を単位元とするような演算（慣習上この演算を加法と呼び，＋で表記する）が定義でき，$E(F_q)$ はこの加法に関し有限可換群となることが知られている．$E(F_q)$ の元の数は，$q+1-t$ $(-2\sqrt{q} \leq t \leq 2\sqrt{q})$ となる．

[楕円曲線の群構造]

有限体上の楕円曲線 $E(F_q)$ は，一般に二つの巡回群の直積となり，それぞれの巡回群の位数を n_1, $n_2(n_1 \geq n_2)$ としたとき，$E(F_q)$ の群構造を (n_1, n_2) と表記する．このとき，n_2 は n_1 の約数であり，かつ $q-1$ の約数でもある．したがって，$E(F_q)$ の元の数は，$n_1 n_2$ であり，$E(F_q)$ の最大位数は n_1 である．

[Frobenius 写像]

次に，F_q 上の代数的閉体（F_q 及びその拡大体の集合）を $\bar{F}_q$ とする（F_q を係数とする多項式の解が必ず $\bar{F}_q$ に含まれる）．$E(\bar{F}_q)$ 上で，点 (x, y) を点 (x^q, y^q) に写像する Frobenius 写像 ϕ が定義できる．このとき，

$$\phi^2 - t\phi + q = 0 \qquad (2)$$

が成立する．ここで，左辺の演算は，写像間の演算を意味し（P が $E(\bar{F}_q)$ 上の点のとき，$[\phi^2 - t\phi + q](P)$ は，$\phi(\phi(P)) - t\phi(P) + qP$ を意味する），右辺の 0 は，零写像（全ての点を無限遠点 $\mathcal{O}$ に写像する）を意味する．ここで，t はトレースと呼ばれ，上で述べた $E(F_q)$ の元の数と関係づけられる．

[l-ねじれ点]

$E(\bar{F}_q)$ 上の点で，l 倍することにより $\mathcal{O}$ となるような点を l-ねじれ点（l-torsion point）と呼び，その集合を $E[l]$ と記す．l が q と互いに素とした場合，$E[l]$ の元の数は l^2 であり，その群構造は，(l, l) となる．

[因子]

代数曲線上の因子（divisor）を紹介する．因子 D は，曲線 C 上の点 P の形式的な和である．つまり，有限個の非零整数 n_P と $P \in C$ に対し，$D = \sum_{P \in C} n_P(P)$ と定義される（たとえば，D が P_1, P_1, P_2 の形式的な和であるとき，$D = 2(P_1) + (P_2)$ と表記する）．D の次数は，$\sum n_P$ であり，$\deg(D)$ と記す．また $|D|$ で $\sum_{P \in C} |n_P|$ を表す．次数が 0 の因子の集合は加法群となり，$\mathbf{D}_0$ と表現される．D の台は集合 $\{P \mid n_P \neq 0\}$ である．二つの因子の台が共通の点を持たないとき，排他的と呼ぶ．因子 $D = \sum_{P \in C} n_P(P)$ は，全ての P が C 上の非特異点（non-singular point）であるとき，単純（simple）と呼び，さらに全ての $P(n_P \neq 0)$ に対して $n_P = \pm 1$ であるとき，強単純（very simple）と呼ぶ．また，全ての $P(n_P \neq 0)$ に対して，$n_P > 0$ である因子 $D = \sum_{P \in C} n_P(P)$ を effective と呼ぶ．f を代数的閉体上の有理式とする．$P \in C$ において f が位数 n の零点（もしくは極）をもつとき，$v_P(f) = n$（もしくは $v_P(f) = -n$）と定義する．そこで，f が与えられたとき，それに対応した因子が $\sum v_P(f)(P)$ で定義され，(f) と表記され，主因子（principal divisor）と呼ばれる．ここで，$(f) \in \mathbf{D}_0$ である．$\mathbf{P}$ を全ての主因子の集合とする．このとき，$\mathbf{P}$ は，$\mathbf{D}_0$ の部分群となる．D_1, $D_2 \in \mathbf{D}_0$ のとき，$D_1 - D_2 \in \mathbf{P}$ ならば，$D_1 \sim D_2$ と記す．C が楕円曲線の場合，$D \in \mathbf{D}_0$ に対して，$D \sim (P) - (\mathcal{O})$ であるような点 $P \in C$ が唯一存在する．因子 $D = \sum n_P(P)$ と主因子 (f) が排他的な台をもつとき，$f(D) = \prod_{P \in C} f(P)^{n_P}$ と定義される．

[Weil 対]

いま，m が q と互いに素な整数とし，P, $Q \in E[m]$ とする．A, $B \in \mathbf{D}_0$ は排他的台をもち，$A \sim (P) - (\mathcal{O})$, $B \sim (Q) - (\mathcal{O})$ とする．f_A, f_B は，$(f_A) = mA$, $(f_B) = mB$ となるような有理関数とする．このとき，楕円曲線 E 上の 2 点 P, Q に対して，Weil 対 $e_m(P, Q)$ が以下のように定義できる．

$$e_m(P, Q) = \frac{f_A(B)}{f_B(A)}$$

[ヤコビ多様体]

楕円曲線上の点の集合が群構造をもつことは前に述べたとおりであるが，一般に任意の代数曲線の点の集合自身が群構造をもつとは限らない．そこで，任意の代数曲線に付随した群構造としてヤコビ多様体を定義する．商群 $\mathbf{D}_0/\mathbf{P}$ を曲線 C のヤコビアン（Jacobian）と呼ぶ．こうして得られた群には自然に代数多様体の構造がはいり，これを代数曲線に付随したヤコビ多様体と呼ぶ．楕円曲線に付随したヤコビ多様体は，もとの楕円曲線と一致し，それらの群は同型となることが分かる．したがって，ヤコビ多様体の群構造は楕円曲線上の群構造の自然な拡張とみなせる．

[因子に付随した線形系]

与えられた因子 D に対し，$D + (f)$ が effective

となる曲線 C 上の有理関数 f を考える．

$L(D)=\{f$ は C 上の有理関数かつ $D+(f)$ が effective$\}\cup\{0\}$

を因子 D に付随した線形系 (linear system) と呼ぶ．$\mathrm{Dim}(L(D))$ は，$L(D)$ の次元を示す．

[Riemann-Roch の定理]

非特異曲線 C と因子 D が与えられたとき，

$$\mathrm{Dim}(L(D))\geq \deg(D)+1-g$$

が成立し，等号は $\deg D>2g-2$ のときに成立する．ここで，g は C の種数（楕円曲線の場合は $g=1$）を意味する．

3. 有限体上の楕円曲線の元の数を計算するアルゴリズム

3.1 目的と用途

前章で述べたように，有限体上の楕円曲線は有限群の構造をもつ．さて，この有限群上で公開鍵暗号系を構成した場合，その安全性を評価するためには，この有限群の構造を調べることが必要となる．また，有限体上の楕円曲線を利用した素数判定アルゴリズムにおいても，対応する有限群がある構造になっていることを確認する必要がある．そこで，このような有限群の構造を知るためには，少なくともその有限群の元の数を知ることが必要となる．(逆に，元の数が分かっても，必ずしも構造が一意に決まるとは限らない．この構造を決定するアルゴリズムについては，後述する．)

曲線が特殊な場合，その有限群の構造が知られている場合がある．たとえば，$p\equiv 2(\mathrm{mod}\ 3)(p>3)$ で，曲線 E が $y^2=x^3+b(0<b<p)$ のとき，有限体 F_p 上の曲線 E は，位数が $p+1$ の巡回群となる（つまり，元の数も $p+1$ である）．一方，虚数乗法の手法を使うことにより，楕円曲線とその元の数を同時に求める方法が知られており，この手法は楕円曲線を用いた素数判定法[14]や楕円曲線上での暗号系の構成[13]で用いられた実用上有益な方法である．しかし，以上の方法では，任意の曲線が与えられて，その元の数を求めたいという要求に答えることはできない．

1985年，Schoof☆ は，有限体上の楕円曲線が与えられたとき，その元の数を計算する決定的多項式時間アルゴリズムを提案した[33]．このアルゴリズムは，問題のサイズの8乗のオーダで実行できる☆．多項式時間アルゴリズムの中でも，われわれが現実的に効率の良いと考えるアルゴリズムは，通常サイズの3乗程度以下のものがほとんどであり，8乗のオーダというのは，符号理論や暗号理論の応用分野で利用するサイズのデータに対して現実的に計算機で計算できるぎりぎりのところであろう．その意味で，この Schoof アルゴリズムは，決して効率的なアルゴリズムとは言えないが，かといって，非現実的なアルゴリズムとも言えない．実際，この Schoof のアルゴリズムの効率を改善したものを実際に計算機で実行させ，暗号に応用した実現例が報告されている[27]．

一方，このアルゴリズムの大きな意義は，上記のような実用的な目的ばかりでなく，理論的に決定的多項式時間アルゴリズムが存在することを示したことはあるといえよう．つまり，このアルゴリズムを利用することにより，いくつかの基本的問題に対して，決定的多項式時間アルゴリズムが存在することが発見されるようになった．たとえば，Schoof 自身が示した応用例として，この元の数を計算するアルゴリズムを用いて，有限体上の平方根を求める決定的多項式時間アルゴリズムが示されている．さらに，その平方根アルゴリズムを用いて，ある種の素数を平方和の形に分解する問題に対して決定的多項式時間アルゴリズムが構成できることが知られている（本特集号の一松氏の記事[10]を参考）．

3.2 Schoof のアルゴリズム

それでは，Schoof アルゴリズムの紹介を行う．まず，Schoof アルゴリズムの基本的アイデアについて説明する．有限体 F_q 上の楕円曲線 $E(F_q)$ の元の数は，$q+1-t$ $(-2\sqrt{q}\leq t\leq 2\sqrt{q})$ となるため，t の値が求まれば十分である．一方，**2.** で述べたように，t の値は，F_q の代数的閉体である $\bar{F}_q$ 上の楕円曲線 $E(\bar{F}_q)$ の Frobenius 写像 ϕ を特徴づけるパラメータでもある（式(2)：$\phi^2-t\phi+q=0$）．正整数 l に対し，$E(\bar{F}_q)$ における l-ねじれ点の集合 $E[l]$ においては，Frobenius 写像に関するパラメータが t の代わりに $\tau_l=t\ \mathrm{mod}\ l$ となる．ここで，$E[l]$ に制限した Frobenius 写像を ϕ_l と表現すると以下の関係が成立する（つまり，

☆ 英語圏では通常「スクーフ」と発音されている．ただし，本人は，オランダ人である．

☆ Schoof の原論文[33]では，9乗と評価されているが，これは，Schoof の評価誤りである．

トレースが τ_l となる).

$$\phi_l^2-\tau_l\phi_l+q=0 \qquad (3)$$

そこで，多くの小さな素数 $l=3,5,7,11,\cdots$ に対して順次 $E[l]$ での Frobenius 写像を用いて $\tau_l=t \bmod l$ を求めていけば (τ_l は，$0\le\tau_l<l$ の範囲でしらみつぶしに探索するが，l の値が小さいので，効率よく求められる)，最終的に中国人剰余定理を用いて，t の値を求めることが可能になる．

次に，このアルゴリズムの詳細を示そう．まず，l-ねじれ点の集合 $E[l]$ をうまく表現する以下のような $\bar{F}_q$ 上の2変数多項式 $\Psi_l(x,y)$ ($l=1,2,\cdots$) が存在することが知られている（この多項式は division polynomial と呼ばれている[34]).

$$\Psi_1(x,y)=1,\ \Psi_2(x,y)=2y,$$
$$\Psi_3(x,y)=3x^4+6ax^2+12bx-a^2,$$
$$\Psi_4(x,y)=4y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3),$$
$$\Psi_{2l+1}(x,y)=\Psi_{l+2}\Psi_l^3-\Psi_{l+1}^3\Psi_{l-1}\ (l\ge2), \qquad (4)$$
$$\Psi_{2l}(x,y)=\Psi_l(\Psi_{l+2}\Psi_{l-1}^2-\Psi_{l-2}\Psi_{l+1}^2)/2y\ (l\ge3). \qquad (5)$$

ここで，$E[l]$ 上の点は，$\Psi_l(x,y)=0$ を満足する点 (x,y) と一致するため，この多項式 Ψ_l が $E[l]$ を表す具体的算法となっている．

一方，この多項式を用いて lP の座標を以下のように表現することができる ($P=(x,y)\in E(\bar{F}_q)$).

$$lP=\left(x-\frac{\Psi_{l-1}\Psi_{l+1}}{\Psi_l^2},\ \frac{\Psi_{l+2}\Psi_{l-1}^2-\Psi_{l-2}\Psi_{l+1}^2}{4y\Psi_l^3}\right) \qquad (6)$$

以上より，$E[l]$ 中の点 $P=(x,y)$ が $\phi_l^2P+qP=\tau_l\phi_lP$ を満足するかどうかを Ψ を用いることにより，以下の式で検証できる．

$$(x^{q^2},y^{q^2})+\left(x-\frac{\Psi_{q-1}\Psi_{q+1}}{\Psi_q^2},\ \frac{\Psi_{q+2}\Psi_{q-1}^2-\Psi_{q-2}\Psi_{q+1}^2}{4y\Psi_q^3}\right)$$
$$=\begin{cases}\mathcal{O} & \text{if } \tau_l=0\\ \left(x^q-\left(\dfrac{\Psi_{\tau_l-1}\Psi_{\tau_l+1}}{\Psi_{\tau_l}^2}\right)^q,\right.\\ \left.\left(\dfrac{\Psi_{\tau_l+2}\Psi_{\tau_l-1}^2-\Psi_{\tau_l-2}\Psi_{\tau_l+1}^2}{4y\Psi_{\tau_l}^3}\right)^q\right) & \text{otherwise}\end{cases} \qquad (7)$$

したがって，以上の式を満足する解と $\Psi_l(x,y)=0$ を満足する解に共通部分があるかどうかを検証することにより，τ_l の値を探索することができる．しかし，2変数の多項式のままでは取扱いが複雑になるため，これを1変数の多項式に変換する（1変数の多項式では，二つの多項式が共通解をもつかどうかを GCD 演算で簡単に求められるが，2変数の場合はそれほど簡単ではない)．このために，楕円曲線の式を用いて y^2 の項を x^3+ax+b で変換することにより，2変数多項式 Ψ_l を，1変数の多項式 f_l に変換すればよい．このとき $E[l]$ 上の点の x-座標は，$f_l(x)=0$ を満足する点 x と一致する．ここで，多項式 f_l の次数は，$(l^2-1)/2$ 以下である．この多項式 f_l を用いて，Schoof のアルゴリズムは以下のように構成される．

Algorithm 1 (Schoof のアルゴリズム)

Input (p,r) (標数 p の有限体 F_q のパラメータ，$p>3$, $q=p^r$), (a,b) (楕円曲線 E のパラメータ，$a,b\in F_q$, $4a^3+27b^2\neq0$),

Output $\sharp E(F_q)$: $E(F_q)$ の元の個数

Step 1 $\prod_{l\le L,\,l\neq2,p} l>4\sqrt{q}$ を満足するような Lを定める．

Step 2 $l=3,5,\cdots,L$ について，$\tau_l(=t \bmod l)$ を求めるため以下の手順を実行する．

Step 2-1 $E[l]$ の中に，$\phi_l^2P=\pm k_lP(k_l=q \bmod l)$ が成立する点が存在するかどうかを検査する．以下の式が成立すればそのような点が存在し（ケース1)，さもなければ存在しない（ケース2).

$$\mathrm{GCD}\{(x^{q^2}-x)f_{k_l}^2(x)(x^3+ax+b)+f_{k_l-1}(x)f_{k_l+1}(x),\ f_l(x)\}\neq1 \quad (k_l:\text{偶数})$$
$$\mathrm{GCD}\{(x^{q^2}-x)f_{k_l}^2(x)+f_{k_l-1}(x)f_{k_l+1}(x)(x^3+ax+b),\ f_l(x)\}\neq1 \quad (k_l:\text{奇数})$$

Step 2-2 (ケース1のとき) $(q/l)=-1$ ならば，$\tau_l=0$. さもなければ，$w=k_l^{1/2} \bmod l$ を計算し，w か $-w$ が ϕ_l の固有値かどうか ($\phi_lP=\pm wP$) を検査する．いずれの固有値でもないとき，$\tau_l=0$. さもなければ，$\tau_l=2w \bmod l$ ($\phi_lP=wP$ のとき)，$\tau_l=-2w \bmod l$ ($\phi_lP=-wP$ のとき)．以上の検査は，f_w などから構成される多項式と $f_l(x)$ の GCD が1かどうかを検査するという，上と同様の手順で実現できる．

Step 2-3 (ケース2のとき) $\phi_l^2P+k_lP=\tau_l\phi_lP$ を満足する τ_l を $1,2,\cdots,l-1$ の範囲内で探索する．この探索は，上と同様に，多項式の GCD を計算することにより行う．

Step 3 $\tau_l=t \bmod l$ ($l=3,5,\cdots,L$) より中国人剰

余定理を用いて t を算出する．$\sharp E(F_q)$ として，$q+1-t$ を出力する．

以上の手順でケース1とケース2に場合分けする理由は，τ_l の値が0や$\pm 2w$ のときは，ケース2の方法では検証できないからである．つまり，$\tau_l\phi_l P$ が $\mathcal{O}$ の場合は，一つの項が縮退するため別の検証式 ($\phi_l^2 P=-qP$) が必要となり，$\tau_l\phi_l P$ が $2qP$ の場合 ($\phi_l^2 P=-qP+2qP=qP$) は，x 座標のみで検証した場合，$\tau_l\phi_l P$ が $\mathcal{O}$ の場合と区別がつかないからである．

3.3 Schoof アルゴリズムの改良と実現例

さて，Schoof のアルゴリズムに基づいて，いくつかの改良版が考えられている．前に述べたように，Schoof のアルゴリズムの実行時間は，問題のサイズの8乗のオーダであるが，Charlap-Coley-Robbins[5] は，実行時間が問題のサイズの6乗のオーダとなる改良アルゴリズムを考案した．この方法の基本的アイデアは，t^2-4q が l を法とする平方剰余のとき，Schoof アルゴリズムで用いた $(l^2-1)/2$ 次の多項式 f_l が $(l-1)/2$ 次の多項式 g_l を因数とすることより，f_l の代わりに次数の低い g_l を用いて Schoof アルゴリズムを構成することである．用いる多項式の次数が低くなった分だけ実行時間が短縮できることになる．また，Atkin も同様のアイデアを用いた改良 Schoof アルゴリズムを考案している．

一方，Menezes-Vanstone-Zuccherato は，標数が2の体上の楕円曲線について，Schoof アルゴリズムを実際に計算した例を報告している[27]．Schoof の論文では，標数が2と3の場合については，具体的な多項式 f_l が与えられていないが，Koblitz[17] は，標数が2の場合について，この多項式を示している．Menezes らは，この Koblitz の論文に基づき，プログラムを作成し，たとえば $E(F_{2^{135}})$ に対し，Sun Sparc Station 上で約4時間で実行できることを確認している．さらに，F_{2^r} の四則演算を実行する専用 chip を併用することにより，さらに実行時間を短縮できることも報告されている[11]．

4. 楕円曲線上の Weil 対を計算するアルゴリズムとその応用

4.1 目的と用途

数論と代数幾何学の両分野にまたがる研究において指導的役割を果たした数学者 Weil は，1946年に有限体上の代数曲線に対する Riemann 予想の証明において今日 Weil 対と呼ばれている演算を導入した[35]．

1986年に Miller は，楕円曲線上の Weil 対を確率的多項式時間で計算するアルゴリズムを示した[24]☆．

このアルゴリズムは，楕円曲線の構造に関する問題において大変有用であることが最近分かってきた．まず，Miller 自身は，この Weil 対アルゴリズムを利用することにより，有限体上の楕円曲線の群構造を計算する確率的多項式時間アルゴリズムを示した．また，Kaliski は，有限体上の楕円曲線に基づく擬似乱数生成器の構成において，この Weil 対アルゴリズムを利用している[12]．一方，Menezes-岡本-Vanstone は，Weil 対アルゴリズムを用いて，有限体上の楕円曲線の離散対数問題を通常の乗法群の離散対数問題に帰着させる方法を示した[19),26]．

4.2 Weil 対計算アルゴリズム

それでは，Weil 対を計算するアルゴリズムについて述べよう．まず，そのために必要となる楕円曲線の主因子に対応する有理式を求めるアルゴリズムを示す[24]．このアルゴリズムは，後に述べる一般の代数曲線上の Riemann-Roch 問題に関するアルゴリズムの特殊ケースである．

Algorithm 2（主因子の有理式表現）:

Input 楕円曲線 E，主因子 $D=\sum n_P(P)$

Output $D=(f)$ となるような有理式 f

Step 1 D を $D=\sum n_P((P)-(\mathcal{O}))$ に変形する．

Step 2 各 $(P-\mathcal{O})$ に対して，以下で述べる2因子の和を求めるサブルーチンを繰り返し用いて，最終的に，$D=(f)$ の形に変形することにより，f の具体的表現（有理式の積の形）を求める．このサブルーチンでは，$D_1=(P_1)-(\mathcal{O})+(f_1)$，$D_2=(P_2)-(\mathcal{O})+(f_2)$ が与えられたとき，$(P_1, P_2\in E)$，$D_1+D_2=(P_3)-(\mathcal{O})+(f_3)$を求める．以下のsubstepでこのサブルーチンを示す．

Step 2-1 $P_3=P_1+P_2$ を計算する．

Step 2-2 l を P_1 と P_2 をとおる直線を表す式，v を P_3 をとおる垂直線の式として，$f_4=l/v$ としたとき，$f_3=f_1f_2f_4$．

Step 3 f を出力する．

☆ 1986年に書かれたこの論文は，いまだに公刊されていないが，著者より原稿は入手可能である．

このアルゴリズムの実行時間は，$L=\sum\log(|n_p|+1)$ のオーダとなる．ただし，このアルゴリズムで求めた f の具体的表現は，最大 $2L$ 個の点において，f の値が定義できない（有理式の極になる）．

次に，Weil 対を計算するアルゴリズムを示す[24]．

Algorithm 3（Weil 対の計算）：

Input $P, Q\in E[m]$, F_q, (m と q は互いに素)

Output $e_m(P,Q)$

Step 1 $E(F_q)$ 上のランダムな点 T, U を選ぶ．

Step 2 $P+T$ と $Q+U$ を計算する．

Step 3 $A=(P+T)-(T), B=(Q+U)-(U)$ として，f_A と f_B を計算する．この計算のために，主因子の有理式を求める Algorithm 2 を利用する．

Step 4

$$\frac{f_A(Q+U)f_B(T)}{f_B(P+T)f_A(U)}$$

を計算する．もし，この値が零か未定義のとき，最初に戻る．さもなければ，この値を $e_m(P,Q)$ として出力する．

上記アルゴリズムにおいて，step 4 で計算値が零か未定義となるような (T,U) の対の数は，高高 16 $(\log_2 m)\#E(F_q)$ である．したがって，問題のサイズを $n=\log_2 q$ とすると，ランダムに選んだ (T,U) が step 4 で計算値が零か未定義となる確率は，$n/2^n$ のオーダとなり，十分に小さい．つまり，上記アルゴリズムは，確率的多項式時間で実行可能であり，その平均繰り返し回数はほぼ 1 である．

4.3 Weil 対計算アルゴリズムの応用

次に，この Weil 対を計算するアルゴリズムの応用例として，Miller による有限体上の楕円曲線の群構造を定める効率的アルゴリズムを示す[24]．従来，この問題に対しては効率的アルゴリズムが知られていなかったが(たとえば，文献 33) の p. 490 の下から 11 行目；文献 18) の p. 158 の Example 4 を参照)，Weil 対のアルゴリズムを利用することにより，初めて効率的な群構造の決定が可能となった．ただし，このアルゴリズムは，ある値 (Algorithm 4 で，$\mathrm{GCD}(q-1,N)$) の素因数分解が与えられていることを前提としている．

Algorithm 4（楕円曲線の群構造決定）：

Input 楕円曲線 E，有限体 F_q

Output $E(F_q)$ の群構造 (n_1,n_2)

Step 1 $E(F_q)$ の元の要素の数 N を計算する．これは，前に述べた Schoof アルゴリズムを使えば，決定的多項式時間で求められる．

Step 2 $N=N_0N_1$, $\mathrm{GCD}(N_0,N_1)=1$ であり，かつ N_0 の素因数の集合が $\mathrm{GCD}(q-1,N)$ の素因数の集合と一致するような N_0, N_1 を計算する．ここで，$\mathrm{GCD}(q-1,N)$ の素因数がなんらかの方法で求められると仮定する．

Step 3 $E(F_q)$ 上の 2 個の P_1', P_2' をランダムに選ぶ．

Step 4 $P_i=N_1P_i'(i=1,2)$ を求める．

Step 5 N_0 の素因数分解を用いて，P_i $(i=1,2)$ の位数 m_i $(i=1,2)$ を求める．

Step 6 $r=\mathrm{LCM}(m_1,m_2)$ を求める．

Step 7 $a=e_r(P_1,P_2)$ を求める．

Step 8 a の位数 s を求める．

Step 9 $rs=N_0$ ならば，(rN_1,s) を群構造として出力する．さもなければ，step 3 に戻る．

このアルゴリズムが正しく動作することは，Weil 対の性質（文献 34）を参照）より保証される．step 9 において，群構造を出力する確率は，$1/(\log\log q)^2$ のオーダであることより，step 3-9 の繰り返し回数の期待値は $(\log\log q)^2$ のオーダである．したがって，上のアルゴリズムは全体で確率的多項式時間で動作する（ただし，step 2 で，素因数分解がなんらかの形で与えられた場合に限定しているので，本当の意味の多項式時間アルゴリズムではないことに注意されたい）．

次に，Weil 対のもう一つの応用として，楕円曲線上で定義された離散対数問題（Algorithm 5 の Input から Output を求める問題）を通常の乗法群上の離散対数問題に変換させるアルゴリズム[26]の説明を行う（離散対数問題については，文献 19) を，その暗号への応用については，13) を参考にされたい）．

Algorithm 5（離散対数問題の帰着）：

Input 楕円曲線 E，有限体 $\boldsymbol{F}_q$，位数が n の点 $P\in E(F_q)$，及び $R=lP$

Output 正整数 l

Step 1 $E[n]\subseteq E(F_{q^k})$ となるような最小の正整数 k を求める．

Step 2 $\alpha=e_n(P,Q)$ の位数が n となるような $Q\in E[n]$ を求める.

Step 3 $\alpha=e_n(P,Q)$, $\beta=e_n(R,Q)$ を計算する.

Step 4 F_{q^k} での乗法群において, α を底にした β の離散対数 l' を求める. ($\beta=\alpha^{l'}$)

Step 5 $l'P=R$ かどうかを検査する. もし成立すれば, $l=l'$ として, その値を出力する. さもなければ, α の位数が n よりも低いと考えられるため, step 2 に戻る.

このアルゴリズムは, 一般には, k の値が問題のサイズ ($\log q$) に対して指数的に大きくなるため, 指数時間かかると考えられるが, 特殊な楕円曲線 (超特異楕円曲線) では, 小さい値の $k(k\leq 6)$ が存在することが知られている[26]. したがって, 従来, 楕円曲線上の離散対数問題は, 通常の乗法群上の離散対数問題よりもずっと難しいと思われていたが, この変換アルゴリズムにより, このような特殊な楕円曲線 (超特異楕円曲線) 上の離散対数問題は効率的に (確率的多項式時間で) 乗法群上の離散対数問題に変換できることになる.

5. 超楕円曲線上のアルゴリズム

これまでは, 主に楕円曲線上のアルゴリズムについて述べてきたが, ここでは, より一般的な種数をもつ曲線である超楕円曲線 (種数が 1 のときは楕円曲線である) のアルゴリズムに関して得られている結果のみを簡単に述べる.

有限体上の超楕円曲線で定義されるヤコビ多様体は有限可換群となるが, この群演算を陽に効率的に計算するアルゴリズムが 1987 年に Cantor によって初めて与えられた[3]. Koblitz は, 標数が 2, 3 の場合における Cantor のアルゴリズムを陽に示している[16].

このようなヤコビ多様体の元の数を計算することは, この有限群の構造を調べるために必要となる. 1988 年に Pila は, 楕円曲線上の Schoof のアルゴリズムのアイデアを有限体上のアーベル多様体に拡張することにより, このようなアーベル多様体上の元の数を計算する決定的多項式時間アルゴリズムを提案した. 超楕円曲線に関するヤコビ多様体は, アーベル多様体に含まれるため, Pila のアルゴリズムは, このようなヤコビ多様体の元の数を計算する決定的多項式時間アルゴリズムともなっている. ただし, Pila のアルゴリズムは, アーベル多様体上で一般的に構成されているため, 現実的な意味で決して効率的なものではない. 1991 年に, Cantor は, Schoof アルゴリズムで使われた多項式 f_l の類似の多項式が超楕円曲線のヤコビ多様体で構成できることを示している[4]. このような具体的な多項式を利用することにより, Pila のアルゴリズムをより効率的に (Schoof アルゴリズムと同程度に効率的に) 構成することが可能となるかもしれない. なお, Pila は, アーベル多様体上の元の数を計算するアルゴリズムの応用として, mod p での l 乗根 (l: 素数) を計算する決定的多項式時間アルゴリズムを示している (Schoof は平方根を計算するアルゴリズムを示したが, これはその拡張である).

超楕円曲線上のヤコビ多様体上で (もっと一般的にアーベル多様体上で), Weil 対が楕円曲線上と類似に定義される[20),28]. この Weil 対を効率的に計算するアルゴリズムが, 筆者らにより与えられている[28]. この Weil 対アルゴリズムは, ヤコビ多様体の群構造を決める問題や離散対数問題を帰着する問題に適用できる.

6. 一般の代数曲線での Riemann-Roch 問題のアルゴリズムとその応用

6.1 Riemann-Roch 問題のアルゴリズム

ベクトル空間 $L(D)$ の次元に関しては代数幾何学の基本定理の一つである Riemann-Roch の定理があるが, $L(D)$ の基底を具体的に構成することは興味深い問題であり, 代数幾何学的符号系や暗号系の構成において重要な役割をはたす. 基礎体 k が代数的閉体の場合には Brill と Noether[1] が $L(D)$ の基底の構成法を示しており, Picard と Simart[31] は Brill と Noether[1] の手法を用いて代数曲面を曲線の族という立場から調べている. また近年, Goppa[8] は代数幾何学的符号 (本特集[22]を参照) を構成するために $L(D)$ の基底の構成法を検討している.

Goppa は Brill-Noether の定理に基づき, $L(D)$ の基底を求めるアルゴリズムを示しているが, オリジナルの Brill-Noether の定理に基づいているため基礎体が代数的閉体の場合に限られていた. Le Brigrand-Risler[2] は一般の有限体上での Brill-Noether の定理の証明を与え, Goppa の構成のギャップを埋めている.

Goppa の構成法は，通常 (ordinary) 特異点と呼ばれる特異点をもつ代数曲線に限られていた．Polemi[30] は，クレモナ (二次) 変換[32]による特異点解消をもちいて Goppa[8] の基本アルゴリズムを任意の平面代数曲線に拡張している．

次の定理は代数的閉体上定義される曲線に対しては古くから知られているが，有限体上では Moreno[25] によって考察されている．

定理 6.1 全ての既約平面代数曲線はクレモナ (二次) 変換によりたかだか通常特異点のみをもつ平面代数曲線に変換できる．

ここでは Polemi[30] による Goppa[8] の基本アルゴリズムの拡張を紹介する．

Algorithm 6 (Riemann-Roch 問題):

Input $k=F_q$ 上の $F[X,Y,Z]=0$ で定義される次数 n の特異既約な平面代数曲線 C と因子 D

Output $L(D)$ の k 上の基底

Step 1 曲線 C の特異点 P とその重複度 r を計算する．$Sing(C)$ で曲線 C の特異点全体の集合を表す．

Step 2 曲線 C の特異点を解消して得られる通常特異点しかもたない平面曲線 $\tilde{C}: \tilde{F}[X,Y,Z]=0$ を構成する．なお，この特異点解消に用いられる手法はブローアップと呼ばれる．

Step 3 平面曲線 $\tilde{C}$ の上で定義される因子 (随伴 (adjoint) 因子)

$$E=\sum_{P\in Sing(C)}\sum_{Q_i\in\phi^{-1}(P)}(r-1)Q_i,$$

を見つける．ここで ϕ は Step 2 における曲線 C のブローアップに付随した写像 $\phi: \tilde{C}\to C$ を表す．

Step 4 $(G_0)=D+E+A$ (ただし A は強単純かつ A と D は排他的な台をもつ) を満たす $\tilde{C}$ 上の多項式 G_0 を見つける．

Step 5 $(G)\geq E+A$ を満たす $\deg=\deg(G)$ の多項式 G のなすベクトル空間の基底 $(G_i)(i=1,\cdots,d=\mathrm{Dim}(L(D)))$ を見つける．

Step 6 $(\phi^{-1*}(G_i)/\phi^{-1*}(G_0))\ (i=1,\cdots,d)$．ここで $\phi^{-1*}(G_i)$ は ϕ^{-1} による G_i の引き戻しを表す．

ここで，step 4, 5 では多項式の係数に関する線形連立方程式を解くことになる．

Polemi[30] は，上記のアルゴリズムの実行時間が $O(q^{12}rn^{14}\log n^3\log^3 q)$ と評価している．このうち特異点の解消に要する時間は，$O(q^{12}rn^{14}\log^3 q)$ であり，入力される曲線が非特異の場合は $O(q^4n^2\log n\log^3 q)$ である．また，Huang と Ierardi[9] も Polemi とは独立に Goppa の $L(D)$ の基底を求めるアルゴリズムを (通常特異点をもつ場合に限り) 掘り下げており，彼らの評価によると，$O(n^{14}|D|\log^3 q)$ であり，さらにこのアルゴリズムはかなりの並列処理が可能であると述べている．

6.2 ヤコビ多様体の群演算

Huang と Ierardi[9] は $L(D)$ の基底を求めるアルゴリズムを種数一般の代数曲線に付随したヤコビ多様体の群演算を計算するアルゴリズムに応用している．

Rieman-Roch の定理から，Jacobi 多様体の点は effective かつ次数 g の因子 D を用いて $D-g\mathcal{O}$ と表せるため，D で Jacobi 多様体の点を表現できる．また Jacobi 多様体の群演算を $*$ で表す．

Algorithm 7 (ヤコビ多様体の群演算):

Input 曲線 C 上の次数 g の effective な因子 D_1 と D_2

Output $D_3=D_1*D_2$ となる次数 g の effective な因子 D_3

Step 1 $L(D_1+D_2-g\mathcal{O})$ の元 f を選ぶ．(存在は Riemann-Roch の定理より保証される．)

Step 2 $D_3=(f)+D_1+D_2-g\mathcal{O}$ と置く．($D_1+D_2\sim D_3+g\mathcal{O}$, $\deg(D_3)=g$ かつ D_3 は effective.)

この結果より，楕円暗号と同様に，任意の代数曲線のヤコビアン暗号を構成できることが分かる．しかし，この Algorithm 7 は Algorithm 6 をサブルーチンに用いるため，楕円暗号ほど効率よくない．Koblitz[16] の超楕円暗号のようにもっと効率のよいヤコビン暗号を構成できる代数曲線 (のクラス) を見つけることは大変興味深い問題と考える．

謝辞 学位論文[30]について数多くご教示いただいたニューヨーク州立大学 Polemi 女史，ならびに文献 31) に関してご教示いただいた九州大学鈴木昌和助教授に謝意を表します．また，多くの有益なコメントをいただいた閲読者に感謝いたします．

参考文献

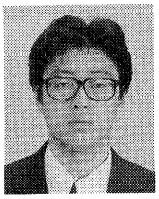
1) Brill, Von A. and Noether, M.: Uber die algebraischen Functionen und ihre Anwendung in der Geometrie, Mathematische Annalen, 7, pp. 269-310 (1974).
2) Brigrand, D. Le, and Risler, J. J.: Algorithm de Brill-Noether et Code de Goppa, Bull. Soc. math. France, pp. 231-253 (1988).

3) Cantor, D.: Computing in the Jacobian of a Hyperelliptic Curve, Math. Comp., 48, pp. 95-101 (1987).
4) Cantor, D.: Oo the Analogue of the Division Polynomials for Hyperelliptic Curves I, Manuscript (1991).
5) Charlap, L. S., Coley, R. and Robbins, D. P.: Enumeration of Rational Pointa on Ellptic Curves over Finite Fields, Manuscript (1991).
6) Fulton, W.: Algebraic Curves, Benjamin, New York (1969).
7) Goldwasser, S. and Kilian, J.: Almost All Primes Can Be Quickly Certifierd, Proceedings on ACM Symposium of Theory of Computing (STOC), pp. 316-329 (1986).
8) Goppa, V. G.: Geometry and Codes, Kluwer Academic Publishers (1988).
9) Huang, M. D. and Ierardi, D. J.: Efficient Algorithm for the Riemann-Roch Theorem and for Addition in the Jacobian of a Curve, Proceedings of IEEE Symposium on Foundations of Computer Science (FOCS), pp. 678-687 (1991).
10) 一松：数論アルゴリズムの研究動向，本特集号，pp. 144-149.
11) Harper, G., Menezes, A. J. and Vanstone, S. A.: Public-Key Cryptosystems with Very Small Key, to appear in Proceedings of Eurocrypt '92, Springer-Verlag.
12) Kaliski, B.: A Pseudorandom Bit Generator based on Elliptic Logarithms, Proceedings of Crypto '86, LNCS 293, Springer-Verlag, pp. 84-103 (1987).
13) 黒澤，藤岡，宮地：暗号理論への応用，本特集号，pp. 195-206.
14) 木田，牧野：素数判定アルゴリズム，本特集号，pp. 150-156.
15) Koblitz, N.: Elliptic Curve Cryptosystems, Math, Comp., 48, pp. 203-209 (1987).
16) Koblitz, N.: Hyperelliptic Cryptosystems, Journal of Cryptology, Vol. 1, pp. 139-150 (1989).
17) Koblitz, N.: Constructing Elliptic Curve Cryptosystems in Characteristic 2, Proc. of Crypto '90, LNCS 537, Springer-Verlag, pp. 156-167 (1991).
18) Koblitz, N.: A Course in Number Theory and Cryptography, Springer-Verlag, New York (1987).
19) 小山，静谷：素因数分解と離散対数問題アルゴリズム，本特集号，pp. 157-169.
20) Lang, S.: Abelian Varieties, Interscience, New York (1959).
21) Lenstra, H.: Factoring Integer with Elliptic Curves, Ann, of Math. 126, pp. 649-673 (1987).
22) 松本，今井：符号理論への応用，本特集号，pp. 189-194.
23) Miller, V.: Uses of Elliptic Curves in Cryptography, Proceedings of Crypto '85, LNCS 218, Springer-Verlag, pp. 417-426 (1986).
24) Miller, V.: Short Programs for Functions on Curves, unpublished manuscript (1986).
25) Moreno, C.: Algebraic Curves over Finite Fields with Appications to Coding Theory, Cambride Univ. Press (1990).
26) Menezes, A. J., Okamoto, T. and Vanstone, S. A.: Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, Proceedings of ACM Symposium on Theory of Computing (STOC), pp. 80-89 (1991).
27) Menezes, A. J., Vanstone, S. A. and Zuccherato, R, J.: Counting Points on Elliptic Curves over F_{2^m}, Manuscript (1991).
28) Okamoto, T. and Sakurai, K.: Efficient Algorithms for the Construction of Hyperelliptic Cryptosystems Proceedings of Crypto '91, LNCS 576, Springer-Verlag, pp. 267-278 (1992).
29) Pila, J.: Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields, PhD Thesis of Stanford Univ. (1988).
30) Polemi, D.: The Brill-Noether Theorem with Applications to a. g. Goppa Codes and Exponential Sums, PhD-Thesis in the City University of New York (1991).
31) Picard, E. and Simart, G.: Thèorie des Fonctions Algèbriques de Deux Variables Indèpendants, Gauthier-Villars (1906).
32) Reed, M. 著，若林　功訳：初等代数幾何講義，岩波書店 (1991).
33) Schoof, R.: Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. Mathematics of Computation, 44, pp. 483-494 (1985).
34) Silverman, J.: The Arithmetic of Elliptic Curves, Springer-Verlag, New York (1986).
35) Weil, A.: Sur les Fonctions Algebriques a Corps de Constantesfini, C. R. Academic des Sciences (1946).

(平成4年11月4日受付)

岡本　龍明（正会員）

1952年生．1976年東京大学工学部計数工学科卒業．1978年同大学院計数工学専攻修士課程修了．同年NTT入社．現在，情報通信網研究所主幹研究員，入社以来，主にネットワークアーキテクチャの研究，自然言語処理の研究，情報セキュリティの研究に従事．工学博士．電子情報通信学会会員．



桜井　幸一（正会員）

昭和38年生．昭和61年九州大学理学部数学科卒業．昭和63年同大学院工学研究科応用物理専攻修了．同年三菱電機(株)入社．情報電子研究所勤務．以来，暗号と情報セキュリティの研究・開発に従事．現在の主要テーマは，計算量理論に基づく安全性と代数多様体に付随した暗号系．電子情報通信学会，日本数学会 International Association for Cyptologic Research 各会員．