数理解析研究所講究録
第1955巻 2015年 146-157

楕円曲線の同種写像の公式計算

横山 和弘
KAZUHIRO YOKOYAMA
立教大学理学部
COLLEGE OF SCIENCE, RIKKYO UNIVERSITY *
野呂正行
MASAYUKI NORO
立教大学理学部
COLLEGE OF SCIENCE, RIKKYO UNIVERSITY †

1 はじめに

楕円曲線とは, 種数1の非特異な3次の代数曲線であり, 数論における非常に重要な対象である. 楕円曲線上の2点に加法が各成分の有理式として定義され, この加法に関して群をなすことが知られている. 近年, 有限体 $\mathbb{F}_q$ 上定義される楕円曲線の有理点群 $E(\mathbb{F}_q)$ は数論的興味以外に, その計算的性質に注目されている.

この有理点群の位数計算に使われたのが, 楕円曲線の同種写像であり, この計算にはモジュラー多項式などの数論での重要な対象が使われている. 計算自体は複雑ではないが, より簡潔な同種写像の計算として, 直接有理関数として同種写像を求めることが考えられる. そこで, この直接的な計算法について, 楕円曲線理論からの興味に加えて計算面からの連立代数方程式の解法ととらえ, 以下の2点を研究の対象とする.

(1) [同種写像の計算公式の存在] 直接, 同種写像が満たす連立代数方程式を導くことで実際の計算機上で公式が導出可能であることを示す.

(2) [イデアル計算としてのよい問題] 公式計算を消去法, すなわちGröbner計算問題と捉え, 今まで得られた効率化技法がどこまで有効であるかを検証する. (新たな効率化技法を生み出すよい例題とする.)

本論文では, 途中経過ではあるが, 小さい素数 $\ell \leq 61$ において, 実際に公式の作成が可能であること, さらにこの公式計算において, 中国人剰余定理型のモジュラー技法が効率的に適応可能であることを報告する.

*kazuhiro@rikkyo.ac.jp
†noro@rikkyo.ac.jp

2 楕円曲線と同種写像

楕円曲線とは, 種数 1 の 3 次の非特異代数曲線である. ([11, 12] 等を参照) 実際には, 体 K の標数が 2,3 以外であれば, K 上の楕円曲線 E の方程式は Weierstrass の標準をさらに簡略化することで以下になる. (ここで $a, b \in K$ である.)

$$E : y^2 = x^3 + ax + b$$

この場合の非特異である条件は $4a^3 + 27b^2 \neq 0$ となる. 体 K の元を x, y 座標にもつ楕円曲線 E 上の点を K 有理点といい, 有理点全体の集合に, 無限遠点と呼ばれる O を加えた集合を $E(K)$ と書く. $E(K)$ には, 特殊な加法が定義され, この加法に関して群となる. ($E(K)$ は代数群であり, アーベル多様体である.)

有限体 $\mathbb{F}_q$ 上定義される楕円曲線の有理点群 $E(\mathbb{F}_q)$ は数論的興味以外に, 計算的性質に注目されている. そこでは, $E(\mathbb{F}_q)$ の位数の計算が重要となっている. 応用例として, 素数証明法 (ECPP) や楕円曲線暗号などがある. ([4, 3] 等を参照) 有理点群 $E(\mathbb{F}_q)$ の位数計算法として Schoof 法があり, その改良として SEA (Schoof-Elkies-Atkin) 法がある. SEA 法では, 同種写像を利用して高速化が図られる.

ここでは, 同種写像の定義と重要な性質をあげておく. ([11, 12] 等を参照)

定義 1 (楕円曲線と同種写像) 2つの K 上定義された楕円曲線 E_1, E_2 に対して, E_1 から E_2 への同種写像とは, K の代数閉体を $\bar{K}$ とするとき, $E_1(\bar{K})$ から $E_2(\bar{K})$ への有理写像で群としての準同型写像となるものをいう. このような同種写像があるとき, E_1, E_2 を同種という.

定理 1 (同種写像に関する性質) E を K 上定義された楕円曲線とし, U を $E(\bar{K})$ の有限部分群とする. このとき, 楕円曲線 E' で E から E' への同種写像の核が U に一致するようなものが存在する. U が $\bar{K}/K$ のガロア群で不変であれば, E' として K 上で定義された曲線が取れる. 有限体 $\mathbb{F}_q$ 上の2つの同種な楕円曲線 E_1, E_2 では有理点群 $E_1(\mathbb{F}_q), E_2(\mathbb{F}_q)$ の位数は等しい.

2.1 Schoof 法と SEA 法の概略

本研究の発端となった有限体上の楕円曲線の有理点群の位数計算法を通して同種写像の計算について説明する. ([10, 3] 等を参照) 以下では, 有限体 $\mathbb{F}_p$ を考える. (ここで p を素数とする.) Schoof 法は $\mathbb{F}_p$ 上の楕円曲線 $E(\mathbb{F}_p)$ の位数 $|E(\mathbb{F}_p)|$ の計算を行う. その特徴は以下である.

(1) いくつかの小さい素数 ℓ に対する $|E(\mathbb{F}_p)| \bmod \ell$ の値を計算する. この計算には, ℓ 分点 (ℓ 倍すると無限遠点になる点) 全体のなす部分群 $E[\ell]$ 上の Frobenius 写像 (各点の x, y 成分をそれぞれ p 乗する写像) の作用を利用する.

(2) 中国人剰余定理 (CRT) を用いて $|E(\mathbb{F}_p)|$ を求める.

(3) Schoof 法の計算量は p のサイズ $\log(p)$ に対して $O(\log(p)^8)$ である. 高速演算により, $O(\log(p)^{5+\varepsilon})$ となる.

Schoof 法の改良の SEA 法は以下の特徴を持つ. (Atkin 素数の利用法については [10, 3] を参照)

(1) $|E(\mathbb{F}_p)| \bmod \ell$ の計算に ℓ 次の E からの同種写像を利用する.

(2) 計算量は $O(\log(p)^6)$ となる. 高速演算により, $O(\log(p)^{4+\varepsilon})$ となる. さらなる効率化技法により, 実際の計算ではそれ以下の振る舞いを見せる. ([6] を参照)

同種写像の核, つまり有理写像として各成分を x, y の有理関数であらわした時の分母にくる多項式が $|E(\mathbb{F}_p)| \bmod \ell$ の計算に非常に有用になる.

注意 1 (SEA 法早分かり) SEA 法のポイントをいくつかあげておく.

(1) $E(\mathbb{F}_p)$ の位数については以下が成り立つ. (Hasse の定理)

$$p+1-2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq p+1+2\sqrt{p}$$

(2) E の ℓ 分点のなす部分群 $E[\ell]$ について以下が成り立つ. (ここで $\ell << p$ とする)

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \quad (\mathbb{F}_\ell \text{ 上の2次元ベクトル空間と見ることができる.})$$

(3) $\mathbb{F}_p$ 上の Frobenius 写像 ϕ_p は $E[\ell]$ に線形写像として作用し, $t = q+1-|E(\mathbb{F}_p)|$ とすれば, 写像として $\phi_p^2 - t\phi_p + p = 0$ を満たす.

(4) $\mathbb{F}_p$ 上で定義される ℓ 次の同種写像の核 C は位数 ℓ の部分群であり, ϕ_p 不変となるので, C は ϕ_p の固有空間となる. つまり C に属する点が, ϕ_p の固有ベクトルとなり, 固有値計算により t が求まる.

SEA 法における同種写像計算は以下の手順となる.

Procedure 1 (SEA 法における同種写像計算)

1. E の j-不変量 $j = j(E)$ を計算し, ℓ 次モジュラー多項式 $\Phi_\ell(x, y)$ の y に代入し, $\mathbb{F}_p$ 上の一変数多項式 $\Phi_\ell(x, j)$ の $\mathbb{F}_p$ 上の根を求める.
2. 根が存在した場合, そのひとつを j' とし, いくつかの関係式より $j' = j(E')$ であり, 同種となる楕円曲線 E' の係数 a', b' を計算する. また, 同種写像の核 C の各点の x 座標の和 $2c_1$ も計算する.
3. a', b', c_1 により, 同種写像 $\left(\frac{N_1}{D_1}, \frac{yN_2}{D_2}\right)$ の分母の多項式 $D_1(x), D_2(x)$ が求まる. ($D_1(x) = F_\ell^2(x), D_2(x) = F_\ell^3(x)$ である.)

3 同種写像計算問題の設定

楕円曲線 E の係数を a, b とし, ℓ を素数とする. このとき, 以下のような問題を設定する.

1. ℓ 次の同種である楕円曲線 E' の係数 a', b' を a, b の関数としてあらわす. ここで $E' : y^2 = x^3 + a'x + b'$ とする.
2. ℓ 次の同種である楕円曲線 E' への同種写像の核 C を与える多項式 F_ℓ の係数 $c_1, \ldots, c_{\frac{\ell-1}{2}}$ を a, b の関数として求める. ここで $F_\ell = x^{\frac{\ell-1}{2}} + c_1 x^{\frac{\ell-1}{2}-1} + \cdots + c_{\frac{\ell-1}{2}}$ とする. (C を核とするとき, F_ℓ は C の元の異なる x 座標を根とする多項式である.)

動機は有限体上の同種写像であるが, ここでは $\bar{\mathbb{Q}}$ を $\mathbb{Q}$ の代数閉体として, $E(\bar{\mathbb{Q}})$ の $\bar{\mathbb{Q}}$ 上での同種写像の公式を考える. この問題を解くために, 同種写像を具体的に表して連立代数方程式を構成する. このとき, 連立代数方程式は $\mathbb{Q}$ 上で定義される. 有限体上の同種写像としての公式は, この連立代数方程式を $\bmod p$ で考えることで得られる.

$E: y^2 = x^3 + ax + b$ から $E': y^2 = x^3 + a'x + b'$ への同種写像は以下で表される. (正規化された形という)

$$\varphi : E(\mathbb{F}_p) \ni (x, y) \mapsto \left(\frac{N_1(x)}{D_1(x)}, \frac{yN_2(x)}{D_2(x)} \right) \in E'(\mathbb{F}_p)$$

この各多項式 D_1, D_2, N_1, N_2 の係数を未知数とおき, E 上の点 (x, y) の φ による像が, 同種である楕円曲線 E' 上にあることから, 各係数と a, b, a', b' に関する連立代数方程式 S_ℓ が得られる.

3.1 同種写像から導かれる連立方程式の特徴

ℓ 次の同種写像 $\varphi : E \to E'$ を $\varphi((x, y)) = \left(\frac{N_1(x)}{D_1(x)}, \frac{yN_2(x)}{D_2(x)} \right)$ とあわわすとき, $\varphi((x, y))$ が E' 上にあるので,

$$\left(\frac{yN_2(x)}{D_2(x)} \right)^2 - \left(\frac{N_1(x)}{D_1(x)} \right)^3 - a' \left(\frac{N_1(x)}{D_1(x)} \right) - b' = 0$$

となる. $y^2 = x^3 + ax + b$ であるので, x のみの現れる等式となる. これより得られる連立方程式を S_ℓ で表すことにする. S_ℓ は以下の特徴を持つ.

(1) 同種写像の核を与える多項式を F_ℓ とすれば, $D_1 = F_\ell^2, D_2 = F_\ell^3$ であり, N_1, N_2 は F_ℓ 自体とその微分を用いてあらわされる. ([2])

(2) F_ℓ はモニックな多項式でその次数は $\frac{\ell-1}{2}$ である. よって, 連立代数方程式は $\frac{\ell-1}{2} + 4$ 個の変数からなる. $(a, b, a', b', c_1, \ldots, c_{\frac{\ell-1}{2}})$

実際, Vélu の公式 ([12] 等を参照) を拡張することで, 以下のように表される ([2]). ここで, $G'(x)$ は $G(x)$ の微分を表す.

$$\begin{aligned} D_1(x) &= F_\ell^2(x), \quad \frac{N_2(x)}{D_2(x)} = \left(\frac{N_1(x)}{D_1(x)} \right)', \\ \frac{N_1(x)}{D_1(x)} &= \ell x + 2c_1 - (3x^2 + a)\frac{D_1(x)'}{D_1(x)} - 2(x^3 + ax + b)\left(\frac{D_1(x)'}{D_1(x)} \right)' \end{aligned}$$

このとき $\deg(N_1) = \ell, \deg(D_1) = \ell - 1$ となる. よって, この形での連立方程式の解があれば, それによる写像は無限遠点を無限遠点に写すので, 同種写像となる ([11, 12] 等を参照). また, 正規化しているので, 同種写像の核となる位数が ℓ の部分群 C に対して解は唯一定まる. 以上により以下の補題が得られる.

補題 1 連立方程式 S_ℓ の異なる解と $E(\mathbb{C})$ における位数 ℓ の部分群とは一対一に対応する.

以下では $k = \frac{\ell-1}{2}$ とし,

$$F_\ell(x) = x^k + c_1 x^{k-1} + \cdots + c_k$$

とする. このとき, 次が成り立つ.

補題 2

(1) $c_2, \ldots, c_k$ は a, a', b, b', c_1 の多項式としてあらわされる. ([10]) すなわち, 連立方程式は実質 5 変数である.

(2) (a, b) の値により定まる (a', b') は a, b 間に特殊な関係がない条件の下で $\ell + 1$ 個である. (ここで a', b' は $\bar{\mathbb{Q}}$ もしくは $\mathbb{F}_p$ の代数閉包 $\bar{\mathbb{F}}_p$ で考える.) $E[\ell]$ の位数 ℓ の部分群は $\ell + 1$ 個あり, これらより同種写像が定まる. 各部分群はモジュラー多項式 $\Phi_\ell(x, j(E))$ の根に対応する.

注意 2 この補題の証明は [10] の結果より直ちに示される. 実際, 楕円曲線 E を $\mathbb{C}$ 上で考え, E の同種写像も $\mathbb{C}$ 上で考える. 同種写像は, 適当なトーラスへの同型 $E \cong \mathbb{C}/L, E' = \mathbb{C}/L'$, ここで $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}, L' = \omega_1\mathbb{Z} + \frac{1}{\ell}\omega_2\mathbb{Z}$, で考えることにより,

$$\mathbb{C}/L \ni z \mapsto z \in \mathbb{C}/L'$$

に対応する写像となる. $\mathcal{P}_L(z) = \frac{1}{z} + \sum_{k=1}^{\infty} d_k z^k, \mathcal{P}_{L'}(z) = \frac{1}{z} + \sum_{k=1}^{\infty} d'_k z^k$ と展開すれば, d_k, d'_k はそれぞれ a, b と a', b' の多項式である. さらに, [10] により,

$$z^{\ell-1} F_\ell(\mathcal{P}_L(z)) = exp\left(c_1 z^2 - \sum_{k=1}^{\infty} \frac{d'_k - \ell d_k}{(2k+1)(2k+2)} z^{2k+2}\right)$$

となり, 両辺を展開して係数を比較すれば, $c_2, \ldots, c_{\frac{\ell-1}{2}}$ が逐次的に c_1, a, b, a', b' の有理数係数の多項式として表されることがわかる.

以下 φ より導かれる連立方程式として a, b, a', b', c_1 に関する方程式を S_ℓ とし (今までと同じ記号を用いる), S_ℓ に付属する $\mathbb{Q}[a, b, a', b', c_1]$ におけるイデアルを I_ℓ とする. I_ℓ の性質として以下が導かれる.

補題 3 (同種写像に付随するイデアルの特徴)

(1) I_ℓ は 2 次元イデアルである. E が特異になる条件から来る埋没成分が存在する. I_ℓ の $\mathbb{Q}$ 上の孤立成分は唯一である. そこで, この成分を generic と呼ぶことにする.

(2) I_ℓ により生成される $\mathbb{Q}(a, b)[a', b', c_1]$ のイデアル I_ℓ^e (I_ℓ の拡大イデアル) を考えると, その根基 $\sqrt{I_\ell^e}$ は $Q(a, b)[a', b', c_1]$ の 0 次元素イデアル (極大イデアル) であり, その線形次元は $\ell + 1$ である. (さらに, $\sqrt{I_\ell^e} = I_\ell^e$ であることが予想される.)

変数順序を考えて, より詳細にイデアル I_ℓ を考えると以下がわかる.

(3) c_1 の $\sqrt{I_\ell^e}$ に関する最小多項式の次数は $\ell + 1$ であり, a', b' は c_1 の多項式であらわされる. (すなわち Shape Form となる.) さらに F_ℓ の係数 $c_2, \ldots, c_k$ も $\mathbb{Q}(a, b)$ 上の c_1 の多項式であらわされる.

(4) a' の $\sqrt{I_\ell^e}$ に関する最小多項式の次数が $\ell + 1$ であれば, Shape Form となり, b' は a' の多項式であらわされる. ($\ell \leq 53$ までの実験ではみな Shape Form となっている.)

(5) 変数 a, b, a', b', c_1 にそれぞれ重み 2,3,2,3,1 を与えると I_ℓ は斉次イデアルである. これより, Gröbner 基底計算にモジュラー技法が有効に使える.

4 公式計算の方針

イデアル I_ℓ の性質をふまえて, 公式作成を以下のステップで行う.

1. イデアルの生成系の生成: 同種写像 φ より導かれる連立方程式および $a, b, a', b', c_1, c_2, \ldots, c_k$ の関係式を合わせて $\mathbb{Q}[a, b, a', b', c_1]$ のイデアル I_ℓ の生成元を計算する.
2. I_ℓ の Gröbner 基底の計算: I_ℓ は重み付き斉次イデアルであるので, 重み付きの項順序にて Gröbner 基底を計算する.

c_1 の公式: $\{a,b\} \prec\prec \{c_1\} \prec \{a',b'\}$ の消去順序を設定する.

a',b' の公式: $\{a,b\} \prec\prec \{a' \prec b'\} \prec c_1$ の消去順序を設定する.

また, イデアル I_ℓ には埋没成分が存在するので, それを除去することが必要になる.

3. 埋没成分の除去: 曲線 E が非特異である条件式 $4a^3+27b^2 \neq 0$ より埋没成分を除去する. そこで $J_\ell = I_\ell : (4a^3+27b^2)^\infty$ を計算する. これには, 新たな変数 t と $g=(4a^3+27b^2)t-1$ を導入し, $\mathbb{Q}[a,b,a',b',c_1,t]$ のイデアル $I_\ell + \langle g \rangle$ から消去イデアル $J_\ell = (I_\ell + \langle g \rangle) \cap \mathbb{Q}[a,b,a',b',c_1]$ を計算する.

   このとき, $I_\ell + \langle g \rangle$ は斉次ではなくなる. しかし, I_ℓ の Gröbner 基底に g を加えた集合は項順序 $\{a,b,a',b',c_1\} \prec\prec t$ での消去イデアルの Gröbner 基底であるので, この計算は基底変換に相当する.

4. $\mathbb{Q}(a,b)$ での公式計算: $\mathbb{Q}(a,b)[a',b',c_1]$ 上で J_ℓ の生成するイデアル ${J_\ell}^e$ の根基 $\sqrt{J_\ell^e}$ の Gröbner 基底 (Shape Form) が公式となる. この計算のため, 逐次的な係数成分の除去も必要となる. (たとえば, $a=0$ や $b=0$ は超特異曲線などに対応する.)

例 1 一番簡単な場合である $\ell=3$ では, 以下のようになる.

I_3 の生成元: すなわち連立方程式 S_3 の各方程式の多項式部分

$$
\begin{aligned}
&9a+30c_1^2+a',\\
&-6c_1a+27b+50c_1^3+4a'c_1+b',\\
&12a^2+(36c_1^2+2a')a+36c_1b+98c_1^4+12'_ac_1^2+4b'c_1,\\
&(36b+78c_1^3+2a'c_1)a+(66c_1^2+4a')b+174c_1^5+18a'c_1^3+6b'c_1^2,\\
&4a^3-48c_1^2a^2+(120c_1b-105c_1^4-2a'c_1^2)a+(276c_1^3+8a'c_1)b\\
&+68c_1^6+11a'c_1^4+4b'c_1^3
\end{aligned}
$$

$I_3(=J_3)$ の Gröbner 基底 (項順序 $\{a,b\} \prec c_1 \prec \{a',b'\}$):

$$
-3c_1^4-6ac_1^2+12bc_1+a^2, a'+30c_1^2+9a, b'-70c_1^3-42ac_1+27b
$$

I_3 の Gröbner 基底 (項順序 $\{a,b\} \prec a' \prec b' \prec c_1$):

$$
\begin{aligned}
&-a'^4+84aa'^3-246a^2a'^2+(-432000b^2-63756a^3)a'-3888000ab^2-576081a^4,\\
&-10800bb'-7a'^3+357aa'^2+2667a^2a'-291600b^2-47817a^3,\\
&(a'^2-42aa'-759a^2)b'-253ba'^2-1134aba'+2187a^2b,\\
&-5400b'^2-791a'^3-819aa'^2+7371a^2a'+3936600b^2+576639a^3,\\
&-2464a^2c1+(-a'+33a)b'+253ba'+3411ab,\\
&3600bc_1-a'^2+42aa'+759a^2,\\
&(-7a'+63a)c_1-3b'-81b,\\
&3600b'c_1-253a'^2-1134aa'+2187a^2,\\
&30c1^2+a'+9a
\end{aligned}
$$

I_3^e の Gröbner 基底 (項順序 $\{a,b\} \prec a' \prec b' \prec c_1$):

$-a'^4+84aa'^3-246a^2a'^2+(-432000b^2-63756a^3)a'-3888000ab^2-576081a^4$,

$-10800bb'-7a'^3+357aa'^2+2667a^2a'-291600b^2-47817a^3$,

$3600bc_1-aa^2+42aa'+759a^2$

モジュラー多項式の再構成:

$I_\ell \cup \{(4a^3+27b^2)j-1728\times 4a^3, (4a'^3+27b'^2)j'-1728\times 4a'^3\}$ の消去順序 $\{j,j'\} \prec\prec \{$その他の変数$\}$ で計算すると j, J' の間の関係式が得られる. これはモジュラー多項式に他ならない. (ただし, a^6 がかかっていることに注意する.)

$(j^4+(-j'^3+2232j'^2-1069956j'+36864000)j^3$

$+(2232j'^3+2587918086j'^2+8900222976000j'+452984832000000)j^2$

$+(-1069956j'^3+8900222976000j'^2-770845966336000000j'$

$+1855425871872000000000)j+j'^4+36864000j'^3$

$+452984832000000j'^2+1855425871872000000000j')a^6$

以下に I_ℓ の Gröbner 基底計算のデータを示す. このデータより I_ℓ の埋没成分の影響で計算時間と基底の大きさが膨大になることが見てとれる.

例 2 F_4 アルゴリズムを用いた I_ℓ の Gröbner 基底の計算
(重み付き項順序+trace 型, 1 CPU 逐次計算, check は 20 並列)

ℓ	11	13	17	19	23	29	31
計算時間 (秒)	0.07	0.2	1.6	5.5	61	2087	5000
GB のサイズ (MB)	0.14	0.36	1.95	4.82	22.7	227	475

5 計算の効率化技法の適用

以下に Gröbner 基底計算における中国人剰余定理型モジュラー技法 (以下 CRT 型モジュラー技法という) の枠組みを示す. ここでは [7] のものがより一般的であるのでそれを採用することにする.

以下では, $X=\{x_1,\ldots,x_n\}$ を変数の集合とし, $\mathbb{Q}[X]$ のイデアル I の項順序 $\prec$ に関する Gröbner 基底計算を考える. CRT 型モジュラー技法では, 素数 p に対して, $\mathbb{Z}_p^0=\{\frac{a}{b} \mid a,b\in\mathbb{Z}, b\not\equiv 0 \pmod p\}$ とし, $\mathbb{Z}_p^0[X]$ から $\mathbb{F}_p[X]$ の射影 ϕ_p を考え, $I\cap Z_p^0[X]$ の像 I_p (またはそれに「相当する」イデアル) の Gröbbner 基底 G_p を計算するアルゴリズムが与えられているとして, G_p より I の Gröbbner 基底 G を構成する.

実際には, $\phi_p(I\cap Z_p^0[X])$ の計算は一般には難しく, 代わりに I の生成系 $F\subset\mathbb{Z}_p^0[X]$ に対して, $\phi_p(F)$ で生成される $\mathbb{F}_p[X]$ のイデアルを考える場合が多い.

Procedure 2 (CRT 型モジュラー計算の枠組み)
Input: An algorithm to compute the reduced Gröbner basis G_p of I_p.
(I_p is a certain modular image of I in $\mathbb{F}_p[X]$.)
Output: the reduced Gröbner basis of I.

```
choose P, a list of random primes;
GP = ∅;
loop
  for p ∈ P do
    compute G_p of I_p(F) with respect to ≺;
```

$\mathcal{GP} = \mathcal{GP} \cup \{G_p\}$;
$(\mathcal{GP}_{lucky}, \mathcal{P}_{lucky}) = deleteUnluckyPrimes(\mathcal{GP}, \mathcal{P})$;
lift $\mathcal{GP}_{lucky}$ to G_{can} by CRA and rational reconstruction;
if G_{can} passes $VerificationTests$ **then**
return G_{can}
enlarge $\mathcal{P}$ with primes not used so far;

CRT 型モジュラー技法の問題点は計算結果の正答性 ($VerificationTests$ の部分) である. しかし, 今回の計算に対しては, 以下の点において正答性の検証が比較的容易になるものと考えられる.

(1) 重み付き斉次イデアル: イデアル I が斉次であれば, Arnold の結果 [1] により, 項順序が degree-compatible であれば, I の Gröbner 計算の結果の正答性検証が容易である.

(2) イデアル商, Saturation: 野呂・横山の結果 [8, 13] により, イデアル I の Gröbner 基底が与えられていれば, $I : f$ や $I : f^{\infty}$ の Gröbner 基底計算の結果の正答性検証が容易である.

(3) 基底変換: 野呂・横山の結果 [8, 13] により, イデアル I のある項順序での Gröbner 基底が与えられていれば, 別の項順序での Gröbner 基底計算の結果の正答性検証が容易である.

これらは皆, **イデアル包含性検査**により検証される.

5.1 CRT 型モジュラー技法における正答検証

以下では, 上記 (1),(2),(3) についての主定理を挙げておく. そのために, **p-Gröbner basis candidate** を定義しておく.

定義 2 (p-Gröbner Basis Candidate [8]) 以下, p を素数とし, $\prec$ を項順序とする.

(1) F を $\mathbb{Q}[X]$ の有限部分集合とする. p が $(F, \prec)$ に対して permissible であるとは $F \subset Z_p^0[X]$ であり, p は F の各要素の $\prec$ に関する主係数の分子を割らないときにいう. また, p が F に対して compatible であるとは $F \subset Z_p^0[X]$ であり, $\phi_p(\langle F \rangle \cap Z_p^0[X]) = \langle \phi_p(F) \rangle$ のときにいう.

(2) F をイデアル I の生成系とする. $\mathbb{Q}[X]$ の部分集合 G_{can} が $(F, \prec)$ に関する I の p-Gröner basis candidate であるとは, $F, G_{can} \subset \mathbb{Z}_p^0[X]$ であり, p は $(G_{can}, \prec)$ に対して permissible であり, $\phi_p(G_{can})$ は $\langle \phi_p(F) \rangle$ の $\prec$ に関する Gröbner 基底になるときにいう.

(3) $\mathbb{Q}[X]$ の部分集合 G_{can} が $\prec$ に関する I の p-compatible Gröner basis candidate であるとは, $G_{can} \subset I \cap \mathbb{Z}_p^0[X]$ であり, p は $(G_{can}, \prec)$ に対して permissible であり, $\phi_p(G_{can})$ は $\phi_p(I \cap \mathbb{Z}_p^0[X])$ の $\prec$ に関する Gröbner 基底になるときをいう.

重み付き斉次イデアルの場合: I が重み付き斉次イデアルとし, 項順序 $\prec$ が重みに対して compatible とする. すなわち, 項 T の重み付き全次数を $\mathrm{tdeg}(T)$ とするとき, 項 T, T' に対して, $\mathrm{tdeg}(T) < \mathrm{tdeg}(T')$ ならば $T \prec T'$ となるものとする. また, F を I の生成系とし, p は $(F, \prec)$ に対して permissible である素数とする. このとき, 以下が成り立つ.

定理 2 (Theorem 7.1 in [1]) $\mathbb{Q}[X]$ の部分集合 G_{can} が $(F, \prec)$ に関する I の p-Gröner basis candidate であるとする. さらに, $\langle G_{can} \rangle \supset I$ であり, G_{can} が自分自身が生成する $\mathbb{Q}[X]$ のイデアルの $\prec$ に関する Gröbner 基底であるなら, G_{can} は I の $\prec$ に関する Gröbner 基底である.

G_{can} が自分自身が生成する $\mathbb{Q}[X]$ のイデアルの Gröbner 基底であるならば, $\langle G_{can} \rangle \supset I$ の確認は I の生成系 F の各元が G_{can} で 0 に reduction されるかどうかを計算すればよい.

基底変換の場合: 一般のイデアルに対しては, 以下が有用である.

定理 3 (Theorem 2.6 in [8]) $\mathbb{Q}[X]$ の部分集合 G_{can} が $\prec$ に関する I の p-compatible Gröner basis candidate であるとする. このとき, G_{can} は I の $\prec$ に関する Gröbner basis である.

一般に, G_{cam} が p-compatible Gröbner basis candidate あることを示すことは I の Gröbner 基底が分からない状況下では困難になる場合が多い. しかし, 基底変換 (すなわち, 他の項順序での Gröbner 基底が分かっている場合) では, これが容易になる. このような状況は基底変換でおこるもので, 基底変換には定理 3 が有効に使える.

系 1 (基底変換) F が I のある別の項順序 $\prec'$ における Gröbner 基底であり, p が $(F, \prec')$ に対して permissible とする. このとき, G_{can} が $(F, \prec)$ に関する p-Gröbner basis candidate であれば, G_{can} は I の $\prec$ に関する Gröbner 基底である.

イデアル商, Saturation の場合: $\mathbb{Q}[X]$ のイデアル I と $g \in \mathbb{Q}[X]$ に対して, イデアル商 $I : g$ の CRT 型モジュラー技法による Gröbner 基底計算を考える. I はその生成系 F により与えられるものとする.

CRT 型モジュラー技法では, Procedure 2 において各素数 p に対して, $\langle \phi_p(F) \rangle : \phi_p(g)$ の Gröbner 基底 G_p を計算するアルゴリズムが入力となり, G_p より Gröbner 基底の候補 G_{can} が CRT より計算される. F が I の Gröbner 基底である場合には, $G_{can} \subset (I : f)$ が F を使って確認できるので, G_{can} の正答性の検証が容易になる. saturation $I : g^{\infty}$ の場合も同様である.

定理 4 (Theorem 2.8 in [8]) p が $(F, \prec)$ に対して permissible であり, p が $(G_{can}, \prec)$ に対しても permissible であるとする. さらに, $\phi_p(G_{can})$ は $(\langle \phi_p(F) \rangle : \phi_p(f))$ の $\prec$ に関する reduced Gröbner 基底 G_p に一致するものとする. このとき, $G_{can} \subset (I : f)$ であれば, G_{can} は $(I : f)$ の $\prec$ に関する reduced Gröbner 基底である.

注意 3 (generic な場合の特定の多項式のみの構成) CRT 型モジュラー技法において, さらに特定の変数のみを含む多項式が効果的に計算できる. 野呂・横山の結果 [8] により, イデアル I のある項順序での Gröbner 基底が与えられていれば, 別の項順序でのモジュラー技法による Gröbner 基底計算において, 項順序の下から決まる. すなわち, それらがイデアル I の元であることが検証できれば, その元の正答性が保障される. すなわち, Gröbner 基底の元すべてを計算しなくても, 欲しい元, (たとえば消去イデアルの元) が正しく計算できる.

以上をまとめると, 正答性の検証は具体的には以下のようになる.

(1) 斉次イデアル: 斉次イデアル I の Gröbner 基底全体の計算が必要である. 計算された Gröbner 基底 G の候補の正答性には以下の 2 点が必要である.

  (i) G が $\langle G \rangle$ の Gröbner 基底である.

  (ii) I が $\langle G \rangle$ に含まれる. すなわち I の生成元 F が G で 0 簡約される.

(2) 基底変換, イデアル商, Saturation: Gröbner 基底全体の計算は必要ない. 計算された特定の元に対してその元がイデアル I に含まれることを示せばよい.

一方, 公式は埋没成分を取り除いているので, イデアルとしての一致性はない.

(3) 連立代数方程式の解となっていることの確認: 代入により確認できる. (公式の生成するイデアルに連立方程式から導かれるイデアルが含まれるかどうかを判定してもよい.)

(4) モジュラー多項式の再計算: 公式から変数消去法により j, j' のみが変数として現れる多項式を計算し, それがモジュラー多項式と一致するかどうかを確認する. (十分条件ではないが, 興味深い計算となる.)

5.2 公式計算の高速化とその計算結果の正答性

イデアル I_ℓ の Gröbner 基底計算は実験よりかなり時間がかかり, サイズも膨大になる. 一方で $J_\ell = I_\ell : (4a^3 + 27b^2)^\infty$ はかなり小さい Gröbner 基底をもち, mod$p$ での計算も効率がよい. そこで, I_ℓ の Gröbner 基底計算を実行せずに, 直接 J_ℓ の Gröbner 基底計算を計算することで, 公式計算の高速化が可能になる.

定理 5 (計算結果の正答性) CRT 型モジュラー技法で構成した J_ℓ の Gröbner 基底の候補 G_{can} に対して, $J' = \langle G_{can} \rangle$ とおき, 以下が成り立つとする.

(1) G_{can} は J' の Gröbner 基底である.

(2) $I_\ell \subset J'$ である.

(3) J' の $\mathbb{Q}(a,b)[c_1, a', b']$ への拡大イデアル $(J')^e$ が素イデアルとなる.

このとき, J_ℓ^e を J_ℓ の拡大イデアルとすれば, $\sqrt{J_\ell^e} = (J')^e$ であり, $\sqrt{I_\ell} = \sqrt{J_\ell} = J'$ が成り立つ. よって G_{can} は I_ℓ の孤立成分の Gröbner 基底である.

$(J')^e$ が素イデアルであることのチェックには以下が使える.

補題 4 ($(J')^e$ のチェック)

(1) $(J')^e$ が全体と一致しないこと: 消去順序 $\{a,b\} \prec\prec \{c_1, a', b'\}$ での $\langle G_{can} \rangle$ の Gröbner basis であり, $\mathbb{Q}[a,b] \cap G_{can} = \emptyset$ であることより確認できる.

(2) $(J')^e$ が素イデアルであること: $\mathbb{Q}[a,b,c_1] \cap G_{can}$ が唯ひとつの元からなり, それが c_1 について $\ell+1$ 次の $\mathbb{Q}$ 上の既約多項式であり, G_{can} の他の元は a', b' についての 1 次式であるとき, 素イデアルであることが確認できる.

以上により, 以下の手続きにより, J_ℓ の Gröbner 基底が計算される.

Procedure 3 ($J = I : (4a^3 + 27b^2)^\infty$ の基底候補 G_{can} の計算) $J_0 = I + \langle (4a^3 + 27b^2)t - 1) \rangle$ に対し $J = J_0 \cap \mathbb{Q}[a,b,a',b',c_1]$ の Gröbner 基底候補 G_{can} を次の手順で求める. $\prec$ を $\{a,b,a',b',c_1\} \prec\prec t$ なる消去順序とする.

1. J_0 のある有限体 F_{p_0} 上での $\prec$ に関する Gröbner 基底を計算し, 必要な S 多項式を記録する.
2. J_0 の有限体 F_{p_i} $(i = 1, 2, \ldots)$ 上での Gröbner 基底計算では, 1. で記録した S 多項式のみ生成する. 結果を G_{p_i} とする.
3. 2. の計算を並列に行い, G_{p_i} を CRT で結合し, 適当な頻度で整数-有理数変換を行う. 結果を G_{can} とする. この場合, $G_{p_i} \cap F_{p_i}[a,b,a',b',c_1]$ の元のみを CRT で結合する.
4. G_{can} が $\langle G_{can} \rangle$ の Gröbner 基底であることのチェックと $I \subset \langle G_{can} \rangle$ のチェックを行う. さらに拡大イデアルの素イデアル性のチェックを行う. これらのチェックが通れば, G_{can} は I の孤立成分の Gröbner 基底であり, もとの連立方程式の generic な解を表すことが分かる.

例 3 $J = I : (4a^3 + 27b^2)^\infty$ の基底候補 G_{can} の計算: ここでは, Procedure 3 の 3 までに要した時間を挙げる. (20 core を用いた CRT 型モジュラー計算)

ℓ	11	13	17	19	23	29	31	37	41	43	47	53
時間 (秒)	0.35	0.74	3.3	4.6	13	74	160	710	2300	2600	8500	36000

59	61
113000	189000

注意 4 例 2 と比較して, I の Gröbner 基底の計算はこれに比べて時間がかかることがわかる. $\ell = 29$ のとき, 2087 秒であり, 基底のサイズが 227MB になる. 一方, G_{can} の方は, 74 秒でサイズは 135KB と圧倒的に小さい.

6 まとめ (楕円曲線理論への Feed Back)

以上, 途中経過ではあるが, 公式計算の試みがある程度まで可能であることが検証できた. より計算法を改良し, より大きな素数 ℓ まで計算可能にする予定である. この実験により, Gröbner 基底計算におけるモジュラー技法の効果をより深く調べ, 今回の公式計算に留まらずに, より一般のイデアルにも適用できるようにさらなる改良を試みて行きたい.

最後に本公式計算の楕円曲線理論への Feed Back として以下が考えられることを報告する.

(1) 公式による位数計算の効率化の可能性:

(i) a, b より, 直接 $F_\ell = x^k + c_1 x^{k-1} + \cdots + c_k$ の係数 $c_1, c_2, \ldots, c_k$ が計算される. ($c_2, \ldots, c_k$ は a, b, c_1 の多項式になっている.)

核 C の点が $\mathbb{F}_p$ 有理点でない場合にも, 体拡大により固有値計算ができる.

拡大次数は $\ell + 1$ の約数であるので, 拡大次数が小さい場合には有効と思われる.

(ii) $c_1 \prec\prec \{a', b'\}$ の公式に現れる係数が小さい. a, b を固定して, p を動かす場合には, さらにコンパクトな公式となる.

(2) generic な位置にある変数: c_1 は generic な位置にある. 計算結果では a' が generic な位置にあるものと予想される.

(3) モジュラー多項式の再構成: モジュラー多項式の計算としては, 計算量的にはあまりよい方法ではない. 楕円曲線理論が単純な方程式の解より確認される点で興味深い.

(4) Gröbner 基底の各元の主係数に現れる式の意味: $\mathbb{Q}(a, b)$ 上では Shape Form になるが, $\mathbb{Q}$ 上では Shape Form にならずに, 主係数に a, b の多項式があらわれる. $4a^3 + 27b^2$ や a, b が現れるのは理論から予想されるが, それ以外のものが楕円曲線理論においてどのような意味があるのかが興味深い.

参 考 文 献

[1] Arnold, E.: Modular algorithms for computing Gröbner bases. J. Symb. Comp. **35** 403–419 (2003)

[2] Bostan,A., Morain,F., Salby,B., Schost, É.: Fast algorithms for computing isogenies between elliptic curves. Math. Comp. **77** 1755–1778 (2008)

[3] Blake,I., Seroussi,G., Smart,N.: Elliptic Curves in Cryptography. London Math. Soc. Lecture Note Series **265**. Cambridge University Press (1999)

[4] Crandall,R., Pommerance,C.: Prime Numbers, A Computational Perspective. Springer-Verlag (2001)

[5] Idrees, N., Pfister, G., Steidel, S.: Parallelization of modular algorithms. J. Symb. Comp. **46** 672–684 (2011)

[6] Izu,T., Kogure,J., Noro,M., Yokoyama,K.: Efficient Implementation of Schoof's Algorithm. ASIACRYPT 1998: 66–79 (1998)

[7] Böhm,J., Decker,W., Laplagne,S., Pfister,G., Steenpass,A, Steidel,S.: Parallel algorithms for normalization. J. Symb. Comput. **51** 99–114 (2013)

[8] Noro, M., Yokoyama, K.: A modular method to compute the rational univariate representation of zero-dimensional Ideals. J. Symb. Comp. **28** 243–263 (1999)

[9] Noro, M., Yokoyama, K.: Verification of Grbner Basis Candidates. ICMS 2014. 419–424 (2014)

[10] Schoof,R.: Counting points on elliptic curves over finite fields. J. Théorie des Nombres de Bordeaux. **7** 219–254 (1995)

[11] Silverman,J.: The Arithmetic of Elliptic Curves. Springer GTM 106 Springer-Verlag (1985)

[12] Washington,L.C.: Elliptic Curves (second edition) CRC Press (2008)

[13] Yokoyama, K.: Usage of Modular Techniques for Efficient Computation of Ideal Operations - (Invited Talk). CASC 2012: 361–362 (2012) (Noro, M. との共著論文として雑誌に投稿予定)