P-3

Anomalous 楕円曲線の離散対数問題の解法アルゴリズムについて

An algorithm for solving the discrete logarithm problem of anomalous elliptic curves

○若林和希 [1]
Kazuki Wakabayashi

Abstract: Using an idea inspired by the so-called Fermat quotient on $\mathbb{F}_p$, we show a polynomial-time algorithm to solve the elliptic curve discrete logarithm problem for anomalous elliptic curves.

$\mathbb{F}_p$ におけるフェルマー商というのを導入すると，離散対数問題が早く解けることを基として，楕円曲線上の離散対数問題に応用したのが本稿の主定理 (定理 8) である．

1. Anomalous 楕円曲線

$p \geq 5$ を素数，$\mathbb{F}_p$ を位数 p の有限体，$\mathbb{Z}_p$ を p 進整数環，$\mathbb{Q}_p$ を p 進数体とする．

定義 1. $\mathbb{F}_p$ 上の楕円曲線 $\widetilde{E} : y^2 = x^3 + \widetilde{a_4}x + \widetilde{a_6}$ が $\#\widetilde{E}(\mathbb{F}_p) = p$ を満たすとき $\widetilde{E}$ を ***Anomalous*** という．
また，$a_i \pmod p \equiv \widetilde{a_i}$ となるように $a_i \in \mathbb{Z}$ を選び

$$E : y^2 = x^3 + a_4x + a_6 \tag{1}$$

と定義する．以降，$\widetilde{E}$ は *anomalous* 楕円曲線とする．

2. 離散対数問題で扱う写像の紹介および証明

$\mathbb{P}^2$ を二次元射影空間として π を $\mathbb{P}^2(\mathbb{Q}_p)$ から $\mathbb{P}^2(\mathbb{F}_p)$ への法 p の還元写像 (reduction map) とする．これは $E(\mathbb{Q}_p)$ から $E(\mathbb{F}_p)$ への群準同型写像となる．$\mathscr{E}$ を E の形式群として λ_E を以下の写像の合成とする．

$$\begin{aligned}\lambda_E : \widetilde{E}(\mathbb{F}_p) \xrightarrow{u} E(\mathbb{Q}_p) \xrightarrow{h_p} \ker\pi \xrightarrow{\psi} \mathscr{E}(p\mathbb{Z}_p)\\ \xrightarrow{\log_{\mathscr{E}}} p\mathbb{Z}_p \xrightarrow{\bmod p^2} p\mathbb{Z}_p/p^2\mathbb{Z}_p \cong \mathbb{F}_p\end{aligned} \tag{2}$$

ここで $\log_{\mathscr{E}}$ は $\mathscr{E}$ の形式対数で，$\psi(x : y : z) := \frac{x}{y}$，$h_p$ を p 倍写像，u を $\widetilde{E}(\mathbb{F}_p)$ から $E(\mathbb{Q}_p)$ への持ち上げ（ヘンゼルの補題より存在）とする．λ_E は $\widetilde{E}(\mathbb{F}_p)$ から $\mathbb{F}_p$ への群準同型写像となる．特に $\widetilde{E}$ が anomalous であれば $|\widetilde{E}(\mathbb{F}_p)| = |\mathbb{F}_p| = p$ なので零写像または同型写像のいずれかになる．

定理 2. λ_E を $\alpha \in \widetilde{E}(\mathbb{F}_p) - \{\tilde{\mathcal{O}}\}$ とする．$A \in E(\mathbb{Z}_p)$ を $\pi(A) = \alpha$ を満たす点とする．$nA \neq \mathcal{O}$ となる $n \in \mathbb{N}$ に対して $nA = (x_n, y_n)$ とする．このとき以下が成り立つ．

(i) $1 \leq n < p \Rightarrow nA \in E(\mathbb{Z}_p) - \{\mathcal{O}\}$

(ii) $1 \leq n < m < p$ かつ $n+m \neq p \Rightarrow x_n \not\equiv x_m \pmod p$

(iii) 特に λ_E が零写像でなければ

$$\begin{aligned}y_{p-1} - y_1\ ,\ \tfrac{x_{p-1}-x_1}{p} \in \mathbb{Z}_p^{\times}\\ \lambda_E(\alpha) \equiv -\tfrac{x_{p-1}-x_1}{p(y_{p-1}-y_1)} \pmod p\end{aligned}$$

Proof. (i) : $\widetilde{E}$ が anomalous より $nA \neq \mathcal{O}$．$n = 1$ のときは仮定の一部なので，まず $n = 2$ を考える．$n = 2$ を考えると法 p で $y_1 \neq 0$ なので E の群演算より

$$x_2 = {c_2}^2 - 2x_1\ ,\ y_2 = -c_2x_2 - d_2 \tag{3}$$

$$c_2 = \frac{3{x_1}^2 + a_4}{2y_1}\ ,\ d_2 = \frac{-{x_1}^3 + a_4x_1 + 2a_6}{2y_1}. \tag{4}$$

$c_2\ ,\ d_2 \in \mathbb{Z}_p$ となり $x_2\ ,\ y_2 \in \mathbb{Z}_p$.
$3 \leq n < p$ は n の帰納法を用いて示す．$A\ ,\ (n-1)A \in E(\mathbb{Z}_p) - \{\mathcal{O}\}$ とする．$x_{n-1} \equiv x_1$ を仮定すると $\pi(A) = \pm\pi((n-1)A)$ となり $n\alpha = \tilde{\mathcal{O}}$ または $(n-2)\alpha = \tilde{\mathcal{O}}$ となり $\widetilde{E}$ が anomalous より $\alpha = \tilde{\mathcal{O}}$ となってしまう．よって法 p で $x_{n-1} \not\equiv x_1$ である．よって $x_{n-1} - x_1 \in \mathbb{Z}_p^{\times}$ であり，E の群演算より

$$x_n = {c_n}^2 - x_1 - x_{n-1} \tag{5}$$

$$y_n = -{c_n}^3 + c_n(x_1 + x_{n-1}) - d_n \tag{6}$$

$$c_n = \frac{y_{n-1} - y_1}{x_{n-1} - x_1}\ ,\ d_n = y_1 - x_1c_n \tag{7}$$

$c_n\ ,\ d_n \in \mathbb{Z}_p$ より $x_n\ ,\ y_n \in \mathbb{Z}_p$，即ち $nA \in E(\mathbb{Z}_p)$.
(ii) : $x_n \equiv x_m$ を仮定する．定理 2(i) より $nA, mA \in E(\mathbb{Z}_p) - \{\mathcal{O}\}$ なので $\pi(nA) = \pm\pi(mA)$ となる．つまり $(m \pm n)\alpha = \tilde{\mathcal{O}}$ であるが $\widetilde{E}$ が anomalous より $\alpha = \tilde{\mathcal{O}}$ となり矛盾．
(iii) : もし $pA = \mathcal{O}$ であれば $\lambda_E(\alpha) = \pmod{p^2} \circ \log_{\mathscr{E}} \circ\psi(\mathcal{O}) = 0$ となり λ_E が零写像でないことに矛盾するので $pA \neq \mathcal{O}$．ここで (5)，(6) を $n = p$ に対して考える．$pA = (x_p, y_p)$ とすると $\pi(pA) = \tilde{\mathcal{O}}$ であるので楕円曲線の有理点の性質より $\mathrm{ord}_p y_p < 0$ かつ $\mathrm{ord}_p x_p > \mathrm{ord}_p y_p$ が成り立つ．定理 2(i) より $A\ ,\ (p-1)A \in E(\mathbb{Z}_p)$ である．ここで $s := \mathrm{ord}_p c_p$ とおく．$s \geq 0$ なら $c_p \in \mathbb{Z}_p$，$d_p \in \mathbb{Z}_p$，$y_p \in \mathbb{Z}_p$ となり矛盾．よって $s < 0$ である．すると (5) より $\mathrm{ord}_p x_p = 2s$ であるので $\mathrm{ord}_p d_p \geq \mathrm{ord}_p(c_p) = s$ より，(6) から $\mathrm{ord}_p y_p = 3s$．つまり $\mathrm{ord}_p \psi(pA) = -s > 0$．一方，$\log_{\mathscr{E}}$ は同型，$\lambda(\alpha) \neq 0$ より $-s < 2$，即ち $s = -1$．このことから $\frac{x_p}{py_p} \in \mathbb{Z}_p^{\times}$,$\lambda_E(\alpha) = \frac{x_p}{py_p} \pmod p$ とわかる．$\widetilde{E}$ が anomalous より $\pi(pA) = \tilde{\mathcal{O}}$，即ち $\pi((p-1)A) = -\pi(A)$ なので法 p で $y_{p-1} \equiv -y_1$．よって $y_{p-1} - y_1 \equiv$

1: 日大理工・院 (前)・数学

$-2y_1 \neq 0$ なので $y_{p-1} - y_1 \in \mathbb{Z}_p^\times$．また $\mathrm{ord}_p c_p = -1$，(7) を合わせると $\frac{x_{p-1}-x_1}{p} \in \mathbb{Z}_p^\times$ である．$pc_p \in \mathbb{Z}_p^\times$ なので (5), (6) より，法 p で $p^2 x_p \equiv (pc_p)^2$, $p^3 y_p \equiv -(pc_p)^3$ より

$$\lambda_E(\alpha) = \frac{(pc_p)^2 \pmod p}{-(pc_p)^3 \pmod p} = \frac{x_1 - x_{p-1}}{p(y_{p-1} - y_1)} \pmod p. \quad (8)$$

3. Anomalous 楕円曲線の離散対数問題 □

群 G，$\alpha \in G$ を有限位数 h の元とする．α で生成された巡回群 $\langle\alpha\rangle$，$\beta \in \langle\alpha\rangle$ に対し，ある $0 \leq n \leq h-1$ に対して $\beta = n\alpha$ が成り立つ．この n を実際に求めることを G における**離散対数問題**という．本稿では，前節の写像を利用して Anomalous 楕円曲線の離散対数問題が多項式時間で解けることを示す．

定義 3 (時間計算量)**.** ある定数 C が存在して十分大きな n に対して $f(n) \leq Cg(n)$ が成り立つとき $f(n)$ は $\mathbf{O}(g(n))$ と書く．あるアルゴリズムに対しての処理時間の計算量を**時間計算量**といい，多項式時間で解けるとは，データ量 n に対して自然数 k が存在して $\mathbf{O}(n^k)$ となることをいう．

注意 4. $\mathbb{F}_p$ のデータ量は $\log p$ である。足し算、引き算の計算量を基準として考えると、掛け算は足し算を最大 $\log p$ 回行うと捉えれば $\mathbf{O}(\log p)$ となる。割り算はユークリッドの互除法で $\log p$ 回の掛け算が必要となるので $\mathbf{O}((\log p)^2)$ となる。本稿では、*anomalous* 楕円曲線の離散対数問題が時間計算量 $\mathbf{O}((\log p)^k)$ であることを示す（$k = 3$ でよい）．

定理 5. $\alpha := (s,t) \in \widetilde{E}(\mathbb{F}_p) - \{\mathcal{O}\}$ に対して以下の手順は $\lambda(\alpha)$ を時間計算量 $\mathbf{O}((\log p)^3)$ で計算する．

(i) $X_1 \bmod p = s$, $Y_1 \bmod p = t$ となる $A := (X_1, Y_1) \in E(\mathbb{Z}/p^2\mathbb{Z})$ を見つける．

(ii) $(X_{p-1}, Y_{p-1}) := (p-1)A \in E(\mathbb{Z}/p^2\mathbb{Z})$ を楕円曲線の群演算を用いて求める．

(iii) $X_{p-1} \not\equiv X_1 \pmod{p^2}$ であれば，$\lambda(\alpha)$ は

$$-\left(\frac{X_{p-1} - X_1}{p} \bmod p\right)(Y_{p-1} - Y_1 \bmod p)^{-1}. \quad (9)$$

$X_{p-1} \not\equiv X_1 \pmod{p^2}$ なら $\lambda(\alpha) = 0$ となる．

Proof. (i) を行うために X_1 , $y \in \mathbb{Z}/p^2\mathbb{Z}$ を法 p で $X_1 \equiv s$, $y \equiv t$ となるようにとり，以下の方程式を満たすように w を求める．

$$\begin{aligned}(y+pw)^2 &\equiv X_1^3 + a_4X_1 + a_6 \pmod{p^2}\\ 2pwy &\equiv X_1^3 + a_4X_1 + a_6 - y^2 \pmod{p^2}\\ w &\equiv \frac{1}{2t}\frac{X_1^3 + a_4X_1 + a_6 - y^2}{p} \pmod p \quad (10)\end{aligned}$$

法 p で $t \neq 0$，p は奇素数より $2t$ の逆元は一意的に存在する．また (1) より法 p で $X_1^3 + a_4X_1 + a_6 - y^2 \equiv 0$ なので $\frac{X_1^3+a_4X_1+a_6-y^2}{p} \in \mathbb{F}_p$ である．以上より $w \in \mathbb{F}_p$ は一意的に定まる．よって $Y_1 := y + pw$ とすることで (10) より $A = (X_1, Y_1)$ が $E(\mathbb{Z}/p^2\mathbb{Z})$ 上の点になる．(ii) で法 p^2 上で $(p-1)A$ を求めるには $\mathbb{Z}/p^2\mathbb{Z}$ の加減乗，乗法群 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ での逆元計算がある．また λ_E が零写像でなければ定理 2(iii) より法 p^2 で $X_{p-1} \not\equiv X_1$ であり，$\lambda_E(\alpha)$ も定理 2(iii) から求まる．$X_{p-1} \equiv X_1 \pmod{p^2}$ なら $\frac{X_{p-1}-X_1}{p} \notin \mathbb{Z}_p^\times$ より定理 2(iii) より λ_E は零写像となる．
(i)，(iii) の計算に含まれる $\mathbb{Z}/p^2\mathbb{Z}$ の演算の数は $p, \widetilde{E}$ に依らない．(ii) では楕円曲線上の足し算を高々$\log p$ 回行うので $\mathbf{O}(\log p)$ 回の $\mathbb{Z}/p^2\mathbb{Z}$ の演算がいる．注意 4 より時間計算量 $\mathbf{O}((\log p)^3)$ となる． □

次の定理は、$\widetilde{E}$ の canonical lift の存在と，その λ_E が零写像の時に満たす j 不変量の性質から導かれる。

定理 6 ([2])**.** (1) において $a_4, a_6 \in \mathbb{Z}$ とし、E' を

$$E'\colon \begin{cases} y^2 = x^3 + px + a_6 & (\widetilde{a_4} = 0)\\ y^2 = x^3 + a_4x + p & (\widetilde{a_6} = 0)\\ y^2 = x^3 + (a_4+p)x + a_6 & (\text{それ以外})\end{cases}$$

と定義する。ここで $0 \leq a_4 < p^2$, $0 \leq a_6 < p^2$ かつ λ_E が零写像と仮定すると $\lambda_{E'}$ は零写像ではない。

注意 7. $\widetilde{E'} = \widetilde{E}$ より E' も *anomalous* 楕円曲線となる．

定理 8 ([1])**.** $\widetilde{E}(\mathbb{F}_p)$ 上の離散対数問題は時間計算量 $\mathbf{O}((\log p)^3)$ で解くことが出来る．

Proof. $\alpha, \beta \in \widetilde{E}(\mathbb{F}_p) - \{\mathcal{O}\}$ とする．$\widetilde{E}$ が anomalous より，$\beta = n\alpha$ となる自然数 $n < p$ が存在する．(1) において $0 \leq a_4$, $a_6 < p^2$ ととる．もし，λ_E が零写像なら定理 6 の $\lambda_{E'}$ が零写像でない．このときの時間計算量は $\lambda_E(\alpha) = 0$ かを確かめる必要があるので，定理 5 より $\mathbf{O}((\log p)^3)$ である．λ が零写像にならない方を E'' と書くことにすると，$\lambda_{E''}$ は準同型なので，$\lambda_{E''}(\beta) = n\lambda_{E''}(\alpha)$ が成り立ち，$n = \frac{\lambda_{E''}(\beta)}{\lambda_{E''}(\alpha)}$．この計算量も定理 5 より $\mathbf{O}((\log p)^3)$ である． □

4. 参考文献

[1] T. Satoh and K. Araki: “Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves”, Comment. Math. Univ. Sancti Pauli, 47 (1998), no.1, 81-92.

[2] T. Satoh and K. Araki: “Errata to the paper: Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves”, Comment. Math. Univ. Sancti Pauli, 48 (1999), no.2, 211-213.