Xedni Calculus について

谷戸 光昭 (中大理工)

Xedni Calculus とは，1999 年に Silverman が提案した楕円離散対数問題に対する攻撃法である．本稿では有限素体上の Xedni Calcus について基本的な事柄を説明する．詳細は Silverman [5] を参照されたい.（本報告集所収の小暮淳氏（富士通研究所）の講演記録 [2] の補足となれば幸いである.）

通常の有限体上の離散対数問題に対しては，Index Calculus と呼ばれる方法が現在知られている中で最も効果的な攻撃法である．この方法を楕円離散対数問題に適用しようとする場合，まず有限体上の楕円曲線を有理数体上に持ち上げ，その後有理点を持ち上げる，そして有理点の間の relation を使って問題を解くという手順を取る．しかし，この方法は有効ではないことが知られている．

一方，今回紹介する Xedni Calculus は，有理点を先に持ち上げ，その後曲線を持ち上げるという手順を取る．手順が Index Calculus の逆になることから,「Xedni」の名が付けられている．

まず第一節において楕円離散対数問題について簡単に触れる．そして第二節において Xedni Calculus の説明を行う．この節では 2-descent 法を用いた独立性判定がひとつの key になっている．また height 法による独立性判定についても触れるが，楕円曲線の height についての詳細は土屋和由氏（中央大）の論説 [6] にある．第三節では第二節の補足の意味を込めて 2-descent についての解説を試みる．

1 楕円離散対数問題

q を素数または素数のべき乗，$\mathbb{F}_q^\times$ を q 個の元からなる有限体の乗法群とする．周知のように $\mathbb{F}_q^\times$ は位数 $q-1$ の巡回群である．β を $\mathbb{F}_q^\times$ の生成元のひとつとすれば，各 $\alpha \in \mathbb{F}_q^\times$ に対して $\alpha = \beta^m$ となる m は $0 \le m < q-1$ の範囲で一意に決まる．q が大きければ m を見つけるのが困難．有限体上の離散対数問題（DLP）は次のように述べられる:

有限体上の離散対数問題（DLP）
上のように (q, α, β) を与えたとき，$\alpha = \beta^m$ を満たす整数 m を決定せよ．

q を素数または素数のべき乗，E を $\mathbb{F}_q$ 上の楕円曲線とする．このとき，E の $\mathbb{F}_q$–有理点全体のなす集合 $E(\mathbb{F}_q)$ は，単位元 $\mathcal{O}$ を指定することによって有限アーベル群になる．$S, T \in E(\mathbb{F}_q)$，$T \neq \mathcal{O}$ とする．このとき，楕円離散対数問題（ECDLP）は次のように述べられる:

楕円離散対数問題（ECDLP）
上のように (q, E, S, T) を与えたとき，$S = mT$ を満たす整数 m を決定せよ．

補注 1.1. S が T によって生成された $E(\mathbb{F}_q)$ の巡回部分群に属していなければ，このような m が存在するとは限らない．しかし実用的な理由から，以後 m が存在する（ように S, T を選んだ）と仮定して話を進める．(時折り $m = \log_T S$ と書くこともある．)

記号． 以下，本稿では $q = p$（素数）の場合のみを扱う．E_p を $\mathbb{F}_p$ 上の楕円曲線

$$E_p : y^2 + a_{p,1}xy + a_{p,3}y = x^3 + a_{p,2}x^2 + a_{p,4}x + a_{p,6}$$

とし，$N_p = \#E_p(\mathbb{F}_p)$ とおく．$S, T \in E_p(\mathbb{F}_p)$ とする．また $P_i = [x_i, y_i, z_i] \in \mathbb{P}^2(\mathbb{F}_p)$, $(1 \leq i \leq r)$ に対して，r 行 10 列の行列 B を

$$B = B(P_1, \ldots, P_r) = \begin{pmatrix} x_1^3 & x_1^2y_1 & x_1y_1^2 & y_1^3 & x_1^2z_1 & x_1y_1z_1 & y_1^2z_1 & x_1z_1^2 & y_1z_1^2 & z_1^3 \\ x_2^3 & x_2^2y_2 & x_2y_2^2 & y_2^3 & x_2^2z_2 & x_2y_2z_2 & y_2^2z_2 & x_2z_2^2 & y_2z_2^2 & z_2^3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_r^3 & x_r^2y_r & x_ry_r^2 & y_r^3 & x_r^2z_r & x_ry_rz_r & y_r^2z_r & x_rz_r^2 & y_rz_r^2 & z_r^3 \end{pmatrix}$$

と定義する．

2 Xedni Calculus

Xedni Calculus とは楕円離散対数問題に対する攻撃法である．まずそのアルゴリズムを説明し，その後この攻撃法の key となる有理点の独立判定法について説明する．

2.1 アルゴリズム

Silverman [5] では,「Mestre 条件」と呼ばれる楕円曲線のランクを低く抑えるための条件を加えて書かれているが，見通しを良くするため，本稿ではその条件を省いた形で説明する．

Step 0. 前節の記号にしたがって (p, E_p, S, T) を入力する．

Step 1. $4 \leq r \leq 9$ なる整数 r を固定する．

— 持ち上げる有理点の数の指定．平面三次曲線は 9 つの点が指定されれば決まることに注意．

Step 2. 任意の $1 \leq i \leq r$ に対して整数の組 (s_i, t_i) をランダムに選び，

$$P_{p,i} = s_iS - t_iT \in E_p(\mathbb{F}_p)$$

とおく．ただし，$1 \leq s_i, t_i < N_p$.

— $P_{p,i} \neq \mathcal{O}$, $P_{p,i} \neq \pm P_{p,j}$ $(i \neq j)$ と仮定してよい.

Step 3. $P_{p,1}, \ldots, P_{p,4}$ がそれぞれ $[1,0,0], [0,1,0], [0,0,1], [1,1,1] \in \mathbb{P}^2(\mathbb{F}_p)$ に移るような射影変換を作り，その変換で E_p を

$$E'_p/\mathbb{F}_p : u_{p,1}x^3 + u_{p,2}x^2y + u_{p,3}xy^2 + u_{p,4}y^3 + u_{p,5}x^2z + u_{p,6}xyz + u_{p,7}y^2z + u_{p,8}xz^2 + u_{p,9}yz^2 + u_{p,10}z^3 = 0$$

に移す.

— （$\mathbb{F}_p$ 上）9 変数の 8 つの斉次方程式を解くことによって，射影変換は簡単に求まる．もし求まらない場合は，$P_{p,1}, \ldots, P_{p,4}$ のうち 3 つが colinear.

Step 4. 任意の $1 \leq i \leq r$ に対して，$P_i \equiv P_{p,i} \mod p$ なる $P_i \in \mathbb{P}^2(\mathbb{Q})$ を選ぶ.

— 点の持ち上げ．特に $P_1, \ldots, P_4$ はそれぞれ $[1,0,0], [0,1,0], [0,0,1], [1,1,1] \in \mathbb{P}^2(\mathbb{Q})$ とする．

Step 5. $P_1, \ldots, P_r \in \mathbb{P}^2(\mathbb{Q})$ を通る曲線

$$C_{\boldsymbol{u}}/\mathbb{Q} : u_1x^3 + u_2x^2y + u_3xy^2 + u_4y^3 + u_5x^2z + u_6xyz + u_7y^2z + u_8xz^2 + u_9yz^2 + u_{10}z^3 = 0$$

を見つける．

— $\boldsymbol{u} = [u_1, \ldots, u_{10}]$ は $B(P_1, \ldots, P_r)\boldsymbol{u} = 0$ の小さな整数解.

— $C_{\boldsymbol{u}}/\mathbb{Q}$ が $E'_p/\mathbb{F}_p$ の持ち上げとなるために，$[u_1, \ldots, u_{10}] \equiv [u_{p,1}, \ldots, u_{p,10}] \mod p$ を満たす.

Step 6. 座標変換で，$C_{\boldsymbol{u}}$ を standerd minimal Weierstrass form $\mathcal{E}$ に書き換える．このとき，$P_1, \ldots, P_r$ に対応する点を $Q_1, \ldots, Q_r \in \mathcal{E}(\mathbb{Q})$ とする．特に $Q_1 = \mathcal{O}$ となるようにする.

Step 7. $Q_2, \ldots, Q_r \in \mathcal{E}(\mathbb{Q})$ の独立性を調べる．独立なら Step 1 または Step 2 に戻る．独立でないなら，$n_2Q_2 + \cdots + n_rQ_r = Q_1$ となる $n_2, \ldots, n_r \in \mathbb{Z}$ を求める．$n_1 = -n_2 - \cdots - n_r$ とおく.

— 上の従属関係式は $n_2((Q_2) - (Q_1)) + \cdots + n_r((Q_r) - (Q_1)) \sim 0$ と同値．よって，$C_{\boldsymbol{u}}$ 上で $n_1(P_1) + \cdots + n_r(P_r) \sim 0$.

— 独立性判定については，2.2, 2.3, 2.4 を参照.

Step 8. $s = \sum_{i=1}^{r} n_i s_i$ と $t = \sum_{i=1}^{r} n_i t_i$ を計算する（s_i, t_i は Step 2 で選んだもの）.

— もし $(s, N_p) \neq 1$ なら Step 1 または Step 2 に戻る.

— もし $(s, N_p) = 1$ なら $ss' \equiv 1 \mod N_p$ なる s' を求める．このとき，$\log_T S \equiv s't \mod N_p$ となり，ECDLP が解けた.

2.2 2-descent 法による独立性判定

$\mathcal{E}$ を $\mathbb{Q}$ 上の楕円曲線とし，$P_1, \ldots, P_r \in \mathcal{E}(\mathbb{Q})$ とする．この節では $P_1, \ldots, P_r$ の $\mathcal{E}(\mathbb{Q})$ における独立性判定について考える．結論から先に言うと，これは $P_1, \ldots, P_r$ の $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ における独立性判定に帰着される．実際，我々の目的は以下の繰り返し操作を実行することによって達せられる．

Step 0. $R_1 = P_1, \ldots, R_r = P_r$ とし，$H = \{P_1, \ldots, P_r\}$ とおく．

Step 1. $R_1, \ldots, R_r$ の $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ における独立性を判定する．(2.3 参照)

Step 2. 独立なら終了．従属なら，$\varepsilon_1 R_1 + \cdots + \varepsilon_r R_r = 2Q$ となる $\varepsilon_i \in \{0, 1\}$ $(i = 1, \ldots, r)$ と $Q \in \mathcal{E}(\mathbb{Q})$ が存在する．ここで Q が H に含まれているかを調べ，含まれていたらそこで終了．そうでなければ H を $H \cup \{Q\}$ で置き換え，さらに $\varepsilon_i = 1$ となるいずれかの R_i を Q で置き換えて (1) に戻る．

この繰り返しが有限回の操作の後，独立と判定されて終了した場合，$P_1, \ldots, P_r$ は $\mathcal{E}(\mathbb{Q})$ においても独立である．その結果得られた有理点の集合 $H = \{P_1, \ldots, P_r, Q_1, \ldots, Q_m\}$ は $\mathcal{E}(\mathbb{Q})$ の真に大きな部分群になる．

一方，$H = \{P_1, \ldots, P_r, Q_1, \ldots Q_m\}$ の中に同じ点が含まれる状態で終了した場合，得られた線型関係式を連立させて容易に

$$\varepsilon_1' P_1 + \varepsilon_2' P_2 + \cdots + \varepsilon_r' P_r = \mathcal{O}$$

なる自明でない線型関係式を導き出せる．

さて，この繰り返し操作が終わらない場合も考えられる．有理点の集合 H が大きくなりすぎてしまったらあるところで操作を終了させ，$P_1, \ldots, P_r$ の従属性はほぼ間違いないと判断し別の方法（例えば Height 法）に移行して従属関係式を探索する．

2.3 $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ における独立性の判定

$\mathcal{E}$ を $\mathbb{Q}$ 上の楕円曲線

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

とする．$q_1, \ldots, q_n$ を，任意の $1 \leq i \leq n$ について $\mathcal{E}[2](\mathbb{F}_{q_i}) \neq \{\mathcal{O}\}$ を満たす小さな奇素数とする．この条件は合同式

$$4x^3 + b_2 x^2 + 2b_4 x + b_6 \equiv 0 \mod q_i$$

が解を持つことと同値．約 $1/2$ の素数に対し上の合同式はちょうど 1 つの解を持ち，約 $1/6$ の素数に対し 3 つの解を持つことが知られている．簡単のため，任意の $1 \leq i \leq n$ に対して解は 1 つだけであると仮定し，それを $x \equiv \alpha_i \mod q_i$ とする．また，$\mathcal{E}$ は q_i で good reduction を持つと仮定する．これは上の合同式が重根を持たないことと同値．

任意の $q \in \{q_1, \ldots, q_n\}$ に対し，(加法的な) quadratic residue map ψ_q を

$$\psi_q : \mathbb{F}_q^\times \to \mathbb{F}_2, \quad \beta \mapsto \begin{cases} 0 & \beta \in (\mathbb{F}_q^\times)^2 \\ 1 & \beta \notin (\mathbb{F}_q^\times)^2 \end{cases}$$

によって定義する．このとき，準同型写像の合成

$$\phi_q : \frac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} \to \frac{\mathcal{E}(\mathbb{Q}_q)}{2\mathcal{E}(\mathbb{Q}_q)} \xrightarrow{\bmod q} \frac{\mathcal{E}(\mathbb{F}_q)}{2\mathcal{E}(\mathbb{F}_q)} \xrightarrow{\gamma} \frac{\mathbb{F}_q^\times}{(\mathbb{F}_q^\times)^2} \overset{\psi_q}{\simeq} \mathbb{F}_2$$
$$(x, y) \mapsto x - \alpha$$

を得る．ここで，γ は 2-descent による準同型（§3, 3.7 参照）．これより，準同型

$$\phi_q : \frac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} \to \mathbb{F}_2, \quad P = (x, y) \mapsto \begin{cases} \psi_q(x - \alpha) & \mathrm{ord}_q(x) \geq 0 \\ 0 & \mathrm{ord}_q(x) < 0 \end{cases}$$

を得る．さらに，準同型

$$\Phi : \frac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} \to \mathbb{F}_2^n, \quad P \mapsto (\phi_{q_1}(P), \ldots, \phi_{q_n}(P))$$

を得る．

$\Phi(P)$ は先の合同式の解の計算と平方剰余計算によって得られる．n を十分大きく取れば，Φ はかなりの高確率で単射になる（[5, Table 1]）．故に，我々の問題は（線型代数が使える）$\mathbb{F}_2^n$ の中における $\Phi(P_1), \ldots, \Phi(P_r)$ の独立性の判定に帰着される．

2.4 Height 法による独立性判定

Height 法とは，楕円曲線 $\mathcal{E}$ の canonical height を用いて $P_1, \ldots, P_r \in \mathcal{E}(\mathbb{Q})$ の独立性を判定する方法である．楕円曲線の height については本報告集の土屋氏の論説 [6] が詳しいので，ここでは簡単な概略を述べるだけにとどめる．

K を代数体とする．K 上の楕円曲線 $\mathcal{E}$ に対し，canonical height と呼ばれる実数値関数 $\hat{h} : \mathcal{E}(K) \to \mathbb{R}$ が次にように定義される:

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f([2^N]P).$$

ここで $f \in K(E)$ は定数でない偶関数．この定義は f によらない．このとき，canonical height は $\mathcal{E}(K)$ 上の半正値二次形式．すなわち次を満たす．

(1) $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$,

(2) $\hat{h}([m]P) = m^2 \hat{h}(P)$,

(3) $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ によって定義される pairing

$$\langle\ ,\ \rangle : \mathcal{E}(K) \times \mathcal{E}(K) \to \mathbb{R}$$

は双線型.

$P_1, \ldots, P_r \in \mathcal{E}(K)$ を $\mathcal{E}(K)/\mathcal{E}(K)_{\mathrm{tors}}$ の代表生成系とする．このとき，elliptic regulator (height regulator) を

$$\mathrm{Reg}_{E/K} = \det(\langle P_i, P_j\rangle)_{1\le i,j\le r}$$

によって定義する．$\hat{h}$ は $\mathbb{R}\otimes_{\mathbb{Z}} E(K)$ 上の正定値二次形式なので，elliptic regulator は常に正の値を取る.

ここで，$P_1, \ldots, P_r \in \mathcal{E}(\mathbb{Q})$ の独立性（従属性）を求める Xedni Calculus の立場に戻ると，

$$\det(\langle P_i, P_j\rangle)_{1\le i,j\le r} = 0$$

ならば $P_1, \ldots, P_r$ が $\mathcal{E}(\mathbb{Q})$ において従属であると結論づけできる．しかし，実装の際には高い精度の浮動小数点計算が必要になるため，Silverman 自身 [5] の中で「2-descent 法よりも効果的ではないかもしれない」と述べている.

3 2-descent について

2.3 節の中で，2-descent による準同型写像 γ が用いられた．この節ではその定義（2 等分点がすべて有理点になっている場合の）を与えることを目標とする.

3.1. K を完全体，E, E' を K 上の楕円曲線，$\phi : E \to E'$ を K-同種写像とすると，群スキームの完全列

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

を得る．ここで，$E[\phi] = \mathrm{Ker}\,\phi$.

$G = G_{\bar{K}/K}$ を K の絶対 Galois 群とすると，これより G-加群の完全列

$$0 \to E[\phi](\bar{K}) \to E(\bar{K}) \xrightarrow{\phi} E'(\bar{K}) \to 0$$

を得る．さらに，Galois cohomology の長完全列を取ることにより

$$\begin{aligned} 0 \to H^0(G, E[\phi](\bar{K})) \to H^0(G, E(\bar{K})) \xrightarrow{\phi} H^0(G, E'(\bar{K})) \\ \xrightarrow{\delta_E} H^1(G, E[\phi](\bar{K})) \to H^1(G, E(\bar{K})) \xrightarrow{\phi} H^1(G, E'(\bar{K})) \end{aligned}$$

を得る．ここで $H^0(G, E(\bar{K})) = E(\bar{K})^G = E(K)$ 等となることに注意して，短完全列

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta_E} H^1(G, E[\phi](\bar{K})) \to H^1(G, E(\bar{K}))[\phi] \to 0$$

を得る.

長完全列の連結準同型 δ_E は次のように定義される：$\phi : E \to E'$ の全射性から，任意の $P \in E'(K)$ に対して $P = \phi(Q)$ となる $Q \in E(\bar{K})$ が存在する．$\kappa(P, \sigma) = Q^\sigma - Q$ （$\sigma \in G$）とおく．$\kappa(P, \sigma)$ は Q の取り方によらない．また $\phi(\kappa(P, \sigma)) = \mathcal{O}'$ で，$\kappa(P, \cdot) \in Z^1(G, E[\phi](\bar{K}))$（1-cocycle）となる．そこで $\delta_E(P)$ を $\kappa(P, \cdot)$ の cohomology class として定義する．

3.2.（Kummer 理論）$n \geq 2$ とし，K を標数が 0 もしくは n と互いに素で，1 の n 乗根をすべて含む体とする．$\mathbb{G}_{m,K}$ を K 上の乗法的群スキーム，$n : \mathbb{G}_{m,K} \to \mathbb{G}_{m,K}$ を n 乗写像とすると，群スキームの完全列

$$0 \to \mu_n \to \mathbb{G}_{m,K} \xrightarrow{n} \mathbb{G}_{m,K} \to 0$$

を得る．ここで，$\mu_n = \operatorname{Ker} n$.

$G = G_{\bar{K}/K}$ を K の絶対 Galois 群とすると，これより G-加群の完全列

$$0 \to \mu_n(\bar{K}) \to \bar{K}^\times \xrightarrow{n} \bar{K}^\times \to 0$$

を得る．さらに，Galois cohomology の長完全列を取ることにより

$$\begin{aligned} 0 \to H^0(G, \mu_n(\bar{K})) \to H^0(G, \bar{K}^\times) \xrightarrow{n} H^0(G, \bar{K}^\times) \\ \xrightarrow{\delta_K} H^1(G, \mu_n(\bar{K})) \to H^1(G, \bar{K}^\times) \xrightarrow{n} H^1(G, \bar{K}^\times) \end{aligned}$$

を得る．ここで $H^0(G, \bar{K}^\times) = (\bar{K}^\times)^G = K^\times$ となることに注意して，短完全列

$$0 \to K^\times/(K^\times)^n \xrightarrow{\delta_K} H^1(G, \mu_n(\bar{K})) \to H^1(G, \bar{K}^\times)[n] \to 0$$

を得る．ところが，$H^1(G, \bar{K}^\times) = 0$（Hilbert 90）なので，同型

$$\delta_K : K^\times/(K^\times)^n \xrightarrow{\sim} H^1(G, \mu_n(\bar{K}))$$

を得る．

長完全列の連結準同型 δ_K は次のように定義される：$n : \mathbb{G}_{m,K} \to \mathbb{G}_{m,K}$ の全射性から，任意の $b \in K^\times$ に対して $b = \beta^n$ となる $\beta \in \bar{K}^\times$ が存在する．$\kappa'(b, \sigma) = \beta^\sigma/\beta$（$\sigma \in G$）とおく．$\kappa'(b, \sigma)$ は β の取り方によらない．また $\kappa'(b, \sigma)^n = 1$ で，$\kappa'(b, \cdot) \in Z^1(G, \mu_n(\bar{K}))$（1-cocycle）となる．そこで $\delta_K(b)$ を $\kappa'(b, \cdot)$ の cohomology class として定義する．

3.3.（Weil pairing）$m \geq 2$ とし，K を標数が 0 もしくは m と互いに素な体とする．E を K 上の楕円曲線，$S, T \in E[m](\bar{K})$ とする．E の因子

$$\sum_{[m]T'=T} (T') - \sum_{[m]R=\mathcal{O}} (R)$$

を考えると，これは 0 と線型同値．これを因子に持つ関数 $g \in K(E)$ をとり，$X \in E$ を任意に取って

$$e_m(S, T) = \frac{g(X+S)}{g(X)}$$

とおく．これは $X \in E$ の取り方によらず S, T のみによる．e_m の値は 1 の m 乗根で

$$e_m : E[m](\bar{K}) \times E[m](\bar{K}) \to \mu_m(\bar{K})$$

は双線型，交代的，非退化な，Galois 群の作用と可換な pairing である．これを Weil pairing という．

Weil pairing を用いて示される重要な事実: $E[m](\bar{K}) \subset E(K)$ ならば，$\mu_m(\bar{K}) \subset K^\times$.

（Weil pairing については，第 1 回本ワークショップ報告集における栗原将人先生（都立大）の論説 [3] も参照されたい.）

3.4. $m \geq 2$ とする．K を標数が 0 もしくは m と互いに素な完全体とし，$G = G_{\bar{K}/K}$ を K の絶対 Galois 群とする．E を K 上の楕円曲線とし，$E[m](\bar{K}) \subset E(K)$ と仮定する．この仮定から，以下の事柄が従う.

- $H^1(G, E[m](\bar{K})) = \mathrm{Hom}(G, E[m](\bar{K}))$
- $H^1(G, \mu_m(\bar{K})) = \mathrm{Hom}(G, \mu_m(\bar{K}))$
- $\mu_m(\bar{K}) \subset K^\times$

このとき，次の定理を得る.

定理 3.5.

(1) 双線型な pairing

$$b : E(K)/[m]E(K) \times E[m](\bar{K}) \to K^\times/(K^\times)^m$$

で，$e_m(\delta_E(P), T) = \delta_K(b(P, T))$ を満たすものが存在する.

(2) b は左側に関して非退化.

(3) b は次のように計算される: $T \in E[m]$ に対して，

$$\mathrm{div}(f_T) = m(T) - m(\mathcal{O}),$$
$$f_T \circ [m] = g_T^m$$

となるような関数 $f_T, g_T \in K(E)$ を選ぶ．$P \in E(K)$ とする．このとき，もし $P \neq T$ ならば

$$b(P, T) \equiv f_T(P) \mod (K^\times)^m.$$

（$P = T$ の場合は $b(T, T) = f_T(T + P) f_T(P)^{-1}$ とすればよい.）

補注 3.6. (3) について，f_T の取り方によらないことをいう．$f_T, f_T' \in K(E)$ とする．条件

$$\mathrm{div}(f_T) = m(T) - m(\mathcal{O}) = \mathrm{div}(f_T')$$

より，ある $\alpha \in K^\times$ が存在して $f'_T = \alpha f_T$．また，ある $g'^m_T \in K(E)$ に対して $f'_T \circ [m] = g'^m_T$ だから，

$$g'^m_T = f'_T \circ [m] = (\alpha f_T) \circ [m] = \alpha g_T^m$$

よって，$\alpha \in (K^\times)^m$．これより，

$$f_T(P) \equiv f'_T(P) \mod (K^\times)^m$$

が従う．

証明．(1) $b = (\delta_K)^{-1} \circ e_m \circ (\delta_E, \mathrm{id})$ とすればよい:

$$\begin{aligned} E(K)/[m]E(K) \times E[m](\bar{K}) &\xrightarrow{(\delta_E, \mathrm{id})} \mathrm{Hom}(G, E[m](\bar{K})) \times E[m](\bar{K}) \\ &\xrightarrow{e_m} \mathrm{Hom}(G, \mu_m(\bar{K})) \xrightarrow[\sim]{(\delta_K)^{-1}} K^\times/(K^\times)^m. \end{aligned}$$

b の双線型性は Weil pairing の双線型性による．

(2) 任意の $T \in E[m]$ に対して $b(P,T) = 1$ と仮定すると，(1) の性質から，任意の $T \in E[m]$，$\sigma \in G$ に対して $e_m(\kappa(P,\sigma), T) = 1$ が成り立つ．Weil pairing の非退化性より $\kappa(P,\sigma) = \mathcal{O}$. また，

$$\delta_E : E(K) \to \mathrm{Hom}(G, E[m](\bar{K})), \quad P \mapsto \kappa(P, \cdot)$$

の kernel は $[m]E(K)$ と同型（$E' = E, \phi = [m]$ として 3.1 の長完全列を見よ）．したがって，$P \in [m]E(K)$ を得る．

(3) $P \in E(K)$ とする．$P = [m]Q$ となる $Q \in E(K)$ を取る．また，$b(P,T) = \beta^m$ となる $\beta \in \bar{K}^\times$ を取る．定義より，任意の $\sigma \in G$ に対して

$$\begin{aligned} e_m(\delta_E(P)(\sigma), T) &= \delta_K(b(P,T))(\sigma), \\ e_m(Q^\sigma - Q, T) &= \beta^\sigma/\beta, \\ g_T(X + Q^\sigma - Q)/g_T(X) &= \beta^\sigma/\beta \end{aligned}$$

となるが，最後の式で $X = Q$ とおくと，

$$g_T(Q)^\sigma/g_T(Q) = \beta^\sigma/\beta$$

を得る．$\delta_K : K^\times/(K^\times)^m \to \mathrm{Hom}(G, \mu_m(\bar{K}))$ は同型なので，

$$g_T(Q)^m \equiv \beta^m \mod (K^\times)^m.$$

したがって，

$$f_T(P) = f_T \circ [m](Q) = g_T(Q)^m \equiv \beta^m = b(P,T) \mod (K^\times)^m$$

を得る．

例 3.7. （2-descent）$m = 2$ の場合に上の定理を適用する．仮定 $E[2](\bar{K}) \subset E(K)$ より，E の標準形を

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_1, e_2, e_3 \in K$$

と取れる．自明でない 2 等分点は，$T_1 = (e_1, 0)$，$T_i = (e_2, 0)$，$T_i = (e_3, 0)$ の 3 つである．

今，$T = (e, 0)$ を上のいずれかの点とし，$f_T(x, y) = x - e$ とおく．これは (3) の 2 つの条件を満たす．実際,

$$\mathrm{div}(x - e) = 2(T) - 2(\mathcal{O}).$$

さらに，$P = (x, y) \in E(K)$ に対して $[2]P$ の x 座標は

$$(x^4 - b_4x^2 - 2b_6x - b_8)/(2y)^2$$

で与えられるが，今の場合

$$\begin{aligned}
b_2 &= -4(e_1 + e_2 + e_3),\\
b_4 &= 2(e_1e_2 + e_1e_3 + e_2e_3),\\
b_6 &= -4e_1e_2e_3,\\
b_8 &= 4e_1e_2e_3(e_1 + e_2 + e_3) - (e_1e_2 + e_1e_3 + e_2e_3)^2
\end{aligned}$$

であり，これを用いて計算すると

$$\begin{aligned}
(f_T \circ [2])(P) &= x([2]P) - e\\
&= \left[\{x^2 - 2ex - 2e^2 + 2(e_1 + e_2 + e_3)e - (e_1e_2 + e_1e_3 + e_2e_3)\}/2y\right]^2
\end{aligned}$$

を得る．故に，$P \neq T$ なら

$$b(P, T) \equiv x - e \mod (K^\times)^2.$$

今，$T = T_1$ とすると，

$$\begin{aligned}
b(T_1, T_1) &= b(T_1, T_1 + T_2)b(T_1, T_2)^{-1}\\
&= b(T_1, T_3)b(T_1, T_2)^{-1}\\
&\equiv (e_1 - e_3)/(e_1 - e_2) \mod (K^\times)^2.
\end{aligned}$$

同様に,

$$b(T_2, T_2) = (e_2 - e_3)/(e_2 - e_1).$$

したがって

$$P = (x, y) \mapsto \begin{cases}
(x - e_1, x - e_2) & x \neq e_1, e_2\\
((e_1 - e_3)/(e_1 - e_2), e_1 - e_2) & x = e_1\\
(e_2 - e_1, (e_2 - e_3)/(e_2 - e_1)) & x = e_2\\
(1, 1) & P = \mathcal{O}
\end{cases}$$

によって定義される単射準同型

$$\gamma : E(K)/[2]E(K) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$$

が得られる．

References

[1] M. Jacobson, N. Koblitz, J. H. Silverman, A. Stein, E. Teske, *Analysis of the xedni calculus attack*, Designs, Codes and Cryptography 20 (2000), 41–64.

[2] 小暮淳, Koblitz 曲線への Xedni Calculus 適用について, 本報告集所収.

[3] 栗原将人, 相互律と Weil pairing, 暗号理論とそれを支える代数曲線理論, 第 1 回ワークショップ報告集 (2000), 43–48.

[4] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, GTM 106.

[5] J. H. Silverman, *The xedni calculus and the elliptic curve discrete logarithm problem*, Designs, Codes and Cryptography 20 (2000), 5–40.

[6] 土屋和由, 楕円曲線上の標準的高さについて, 本報告集所収.

Mitsuaki Yato
Department of Mathematics,
Graduate School of Science and Engineering,
Chuo University,
Kasuga 1-13-27, Bunkyo-ku,
Tokyo, 112-8551, Japan,
E-mail: yato@grad.math.chuo-u.ac.jp