有限体における平方根の計算法について
Calculation of square roots in finite fields

数学専攻 阿部　隼大
Shunta ABE

序

本論文は，有限体において平方根を求めるアルゴリズムに関する論文 Tsz-Wo Sze, On taking square roots without quadratic nonresidues over finite fields, Mathematics of Computation, 80 (2011) に基づく総合報告である．さらに，論文で扱われている有限可換群 G_α の幾何的な解釈を Silverman, Arithmetic of elliptic curves, Springer を参照して補足した．

論文は本論である 3 節と実際に作成したプログラムを記載した付録からなっている．第 1 節は序論に相当し，平方剰余の相互法則に遡り，Jacobi 記号の相互法則，Tonelli-Shanks のアルゴリズムについて説明した．第 2 節では原論文に基づき，Sze のアルゴリズムについてその根拠とステップを説明した．有限体において平方根を求めるアルゴリズムは，第 1 節で説明した Tonelli-Shanks のアルゴリズムが従来から知られていたが，このアルゴリズムの適用できる有限体は p 元体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ に限られ，一般の有限体に対しては適用できない．Sze の創意は有限体 $\mathbb{F}_q$ の乗法群に同型な群 G_α を導入し，G_α における議論に持ち込んだことにある．これは対数を用いて乗法除法を加法減法の計算に帰着させた古来の知恵に通ずるものであろうか．第 3 節では Sze が導入した群 G_α が特異点をもつ三次曲線によって記述されることを説明した．これによって，Sze のアルゴリズムがそれだけでも興味深い上に，理論的に非常に深い背景があることが明らかになった．

修士論文作成にあたって参考にした論文で提唱されているアルゴリズムを実際に実装するには数々の技術的困難を解決しなければならなかった．何かしらアルゴリズムを学んだところで，実際にそれをプログラムに組み，動かしてみなければ，絵に描いた餅でしかない．プログラムを作成するにあたっては，有限体の加減乗除を組んでおくことが必要であった．本論文では有限体を素朴に多項式環の剰余環として捉え，すべてを多項式の計算に持ち込んだ．アルゴリズムの高速化は次の課題であろう．

1　準備

Tonelli-Shanks のアルゴリズム

p を奇素数，$\mathbb{F}_p$ を p 元体とする．有限体 $\mathbb{F}_p$ において平方根を求めるアルゴリズムとして従来から Tonelli-Shanks のアルゴリズムが知られている．

アルゴリズム 1.1. (Calculating a square root in $\mathbb{F}_p$)
入力: 素数 p, p で割り切れない整数 a
出力：$\sqrt{a}$

StepI　　mod p での非平方元 g を求める．
StepII　$p-1 = 2^r q$, $2 \nmid q$ となる整数 r, q を求める．
StepIII　$h \equiv g^q \pmod{p}$ と $b \equiv a^q \pmod{p}$ を計算する．
StepIV　$s := 1$, $h \equiv h^{-1} \pmod{p}$ と初期化し，$i = r-2$ から 0 まで以下の操作を繰り返す．
　StepIV.1　$b^{2^i} \equiv -1 \pmod{p}$ なら，$s := sh \pmod{p}$, $b := bh^2 \pmod{p}$ とする．
　StepIV.2　$h := h^2 \pmod{p}$ とする．
StepV　出力として，$\sqrt{a} := a^{(q+1)/2} s \pmod{p}$ を返す．

2　平方根の計算

最近 Sze によって有限体における平方根を計算するアルゴリズムが提唱された．第 2 節では，そのアルゴリズムの根拠とあらましについて，以下の項目について整理して論述した．

$\mathbb{F}_q^\times$ に同型な群 G_α について

定義 2.1. q を奇素数の冪，$\mathbb{F}_q$ を有限体，$\alpha \in \mathbb{F}_q^\times$ とする．

$$G'_\alpha = \{[a]\ ;\ a \in \mathbb{F}_q,\ a \neq \pm\alpha\}$$

と記す．G'_α と $\mathbb{F}_q$ の元を区別するために，G'_α の元は $[\,\cdot\,]$ と表わす．

また，

$$G_\alpha = G'_\alpha \cup \{[\infty]\}$$

と記す．定義から G_α の基数は $q-1$．さらに，G_α に演算*を

$$[a] * [\infty] = [\infty] * [a] = [a],$$
$$[a] * [-a] = [\infty],$$
$$[a] * [b] = \left[\frac{ab+\alpha^2}{a+b}\right]$$

によって定義する．ここで，$[a], [b] \in G'_\alpha\ (a+b \neq 0)$.

命題 2.2. $(G_\alpha, *)$ は $[\infty]$ を単位元に持つ可環群である．さらに，写像 $\psi : G_\alpha \to \mathbb{F}_q^\times$

$$[\infty] \mapsto 1,\ [a] \mapsto \frac{a+\alpha}{a-\alpha}$$

によって定義すると，ψ は群の同型である．

補注 2.3. $\mathbb{F}_q^\times$ が巡回群なので G_α も巡回群である．q は奇数なので，G_α はただ一つ位数 2 の元を持つ．実際

$$\psi([0]) = \frac{0+\alpha}{0-\alpha} = -1$$

したがって，$[0]$ は位数 2 の G_α の元で，α の選び方に依存しない．

平方根の計算

$\beta \in \mathbb{F}_q^\times$ を平方数と仮定する．このとき，$\alpha^2 = \beta$ となるような $\alpha \in \mathbb{F}_q^\times$ が存在する．定義 2.1 で定義した群 G_α について考える．$\zeta_d \in \mathbb{F}_q$ を 1 の原始 d 乗根とする．ここで，$d|(q-1)$ と仮定する．このとき，次の定理を得る．

命題 2.4. $[a] \in G_\alpha$ とし，$[a]^2 \neq [\infty]$ と仮定する．$d > 0$ を $[a]^d = [\infty]$ を満たす整数とする．このとき，$0 < k < d/2$ が存在して，

$$\alpha = \pm\frac{a(\zeta_d^k - 1)}{\zeta_d^k + 1}$$

が成立する．

補注 2.5. 集合 G_α の定義では α を用いている．しかし，群 G_α の演算 $*$ は $\beta = \alpha^2$ がわかっていれば計算できる．したがって，α の値が分からなくても次のアルゴリズムは進行する．

アルゴリズムについて

$p_1, \cdots, p_n$ を互いに相異なる n 個の奇数，$t, e, e_1, \cdots e_n$ を $(2p_1 \cdots p_n, t) = 1$ となるような正の整数とするとき，q を次のように表す．

$$q = 2^e p_1^{e_1} \cdots p_n^{e_n} t + 1$$

$e > 1$ と仮定する．$e = 1$ ならば，平方根の計算は簡単である．このとき，次のアルゴリズムを得る．

アルゴリズム 2.6. (Calculating a square root)
入力 : β, q ($\beta \in \mathbb{F}_q^\times$ は平方元)
出力 : $\pm\sqrt{\beta}$

StepI　$2t-1$ 個の相異なる元 $g_1, g_2 \cdots g_{2t-1} \in \mathbb{F}_q^\times$ を考える．
　StepI.1　もし，$g_{t'}^2 = \beta$ となるような t' が存在するならば，出力として，$\pm g_{t'}$ を返す．
　StepI.2　そうでなければ，$[g_{t''}]^{2t} \neq [\infty]$ となる t'' で $g = g_{t''}$ として g を置き換える．
StepII　もし，$[g]^{(q-1)/2^{e-1}} \neq [\infty]$ ならば，次のようにする．
　StepII.1　$[g]^{(q-1)/2^k} = [\infty]$ となるような最大の k を見付ける．$(0 \leq k < e-1)$
　StepII.2　位数 4 の G_α の元 $[a] = [g]^{(q-1)/2^{k+2}}$ を計算する．
　StepII.3　出力として，$\pm a\sqrt{-1}$ を返す．
StepIII　$[g]^{(q-1)/p_m^{e_m}} \neq [\infty]$ となるような m を見付ける．
StepIV　$r = p_m$ として，次の操作を行う．
　StepIV.1　$[g]^{(q-1)/r^k} = [\infty]$ となるような最大の k を見付ける．
　StepIV.2　位数 r の G_α の元 $[a] = [g]^{(q-1)/r^{k+1}}$ を計算する．
　StepIV.3　1 の r 乗原始根 $\zeta_r \in \mathbb{F}_q$ を計算し，$\zeta = \zeta_r$ とする．
　StepIV.4　$(a(\zeta^j - 1)/(\zeta^j + 1))^2 = \beta$, $1 \leq j \leq (r-1)/2$ となるような j を見付ける．
　StepIV.5　出力として，$\pm a(\zeta^j - 1)/(\zeta^j + 1)$ を返す．

定理 2.7. アルゴリズム 2.6 は β の平方根を返す．

1 の原始根の計算方法について

アルゴリズム 2.8. (Calculating a primitive r-th root of unity)
入力 : r, q (r は奇素数，$q = r^e t + 1$, $(r, t) = 1$)
出力 : $\mathbb{F}_q$ における 1 の原始 r 乗根

StepI　$t+1$ 個の相異なる $\mathbb{F}_q^\times$ の元 $g_1, ..., g_{t+1}$ を与える．
　　$g_j^t \neq 1$ となるような g_j を選び，$g = g_j$ とおく．
StepII　$g^{(q-1)/r^k} = 1$ となるような最大の k を見付ける．
StepIII　出力として $g^{(q-1)/r^{k+1}}$ を返す．

定理 2.9. アルゴリズム 2.8 は 1 の原始 r 乗根を返す．

アルゴリズム 2.10. (Calculating a primitive 4th root of unity)
入力 : q ($q = 2^e t + 1$, $e > 1$, t は奇数)
出力 : $\mathbb{F}_q$ における 1 の原始 4 乗根

StepI　$2t+1$ 個の相異なる $\mathbb{F}_q^\times$ の元 $g_1, ..., g_{2t+1}$ を与える．
　　$g_j^{2t} \neq 1$ となるような g_j を選び，$g = g_j$ とおく．
StepII　$g^{(q-1)/2^k} = 1$ となるような最大の k を見付ける．
StepIII　出力として $g^{(q-1)/2^{k+2}}$ を返す．

定理 2.11. アルゴリズム 2.10 は 1 の原始 4 乗根を返す．

3　二重点を持つ特異曲線

第 3 節では，第 2 節で定義した群 G_α の幾何的な解釈についてまとめた．
次のことが知られている．

3.1. 代数的閉体 K の上の E を射影三次曲線とする．
(1) E が非特異なら，E は可環群の構造を持つ．
(2) E が結節点 P をもつなら，$E_{\mathrm{ns}} = E \setminus \{P\}$ は群の構造をもち，E_{ns} は乗法群 $K^\times$ に同型．
(3) E を尖点 P をもつなら，$E_{\mathrm{ns}} = E \setminus \{P\}$ は群の構造をもち，E_{ns} は加法群 K に同型．

この事実を用いて「特異曲線」の点から群法則を解釈し直すことができる．

3.2. E を $y^2 = x^2(x+\alpha^2)$ によって定義される三次曲線とする．$E(\mathbb{F}_q)$ を E の $\mathbb{F}_q$ 有理点全体とする．このとき，$E(\mathbb{F}_q)$ 上の特異点は二重点 (0,0) ただ一つである．$E_{\mathrm{ns}}(\mathbb{F}_q)$ を $E(\mathbb{F}_q)$ 上の非特異点とする．さらに，写像 $\tau : E_{\mathrm{ns}}(\mathbb{F}_q) \to \mathbb{F}_q^\times$ を

$$\infty \mapsto 1,\ (x,y) \mapsto \frac{(y/x)+\alpha}{(y/x)-\alpha}$$

によって定義する．このとき，写像 τ は群の同型．実際，τ の逆写像 $\tau^{-1} : \mathbb{F}_q^\times \to E_{\mathrm{ns}}(\mathbb{F}_q)$ は

$$1 \mapsto \infty,\ \lambda \mapsto \left(\frac{4\alpha^2\lambda}{(\lambda-1)^2}, \frac{4\alpha^3(\lambda+1)}{(\lambda-1)^3} \right)$$

によって与えられる．

命題 2.2 で定義した同型 ψ と合わせて考えることにより，同型

$$G_\alpha \xrightarrow[\psi]{\sim} \mathbb{F}_q^\times \xrightarrow[\tau^{-1}]{\sim} E_{\mathrm{ns}}(\mathbb{F}_q)$$

を得る．一方，同型 $\psi^{-1} \circ \tau : E_{\mathrm{ns}}(\mathbb{F}_q) \to G_\alpha$ は

$$\infty \mapsto [\infty],\ (x,y) \mapsto [y/x]$$

で与えられる．

参考文献

[1] Tsz-Wo Sze，On taking square roots without quadratic nonresidues over finite fields

[2] Joseph H. Silverman，The arithmetic of elliptic curves, Springer-Verlag