素体 GF(p) 上の数体篩法における多項式選択方法

早坂 健一郎　　高木 剛

公立はこだて未来大学 システム情報科学部
041-8655 北海道函館市亀田中野町 116-2

あらまし GF(p) 上の離散対数問題の困難性を評価することは，DSA 署名方式や Diffie-Hellman 鍵共有の安全性を考察する上で重要である．本稿では，GF(p) 上の離散対数問題に対して漸近的に最速な解読アルゴリズムとして知られている数体篩法の実装を行う．また，多項式 f で決まる最大整数環 $\mathcal{O}_K$ と整環 $\mathcal{O}$ に対して，$[\mathcal{O}_K : \mathcal{O}]$ を割る素数を因子基底に含まないような多項式 f(good な多項式 f) の判定法について述べる．75 ビットの素数 p に対して多項式 f が good である確率が，Lenstra 等によって予想された $[\mathcal{O}_K : \mathcal{O}] = 1$ である確率 $6/\pi^2$ とほぼ一致した．さらに，75 ビットの素数 p に対して代数体を定義する多項式 f の違いによる数体篩法の関係探索の実行時間の比較を行う．この結果，多項式 f の違いによる関係探索の実行時間の差は，最大で約 46 倍であった．

How to Choose the Polynomials for Number Field Sieve over GF(p)

Kenichiro HAYASAKA　　Tsuyoshi TAKAGI

School of Systems Information Science, Future University Hakodate,
116-2, Kamedanakano-cho, Hakodate, Hokkaido, 041-8655, Japan

Abstract DSA and Diffie-Hellman key exchange are cryptographic protocols whose security is based on the difficulty of the discrete logarithm problems (DLP) over GF(p). It is important to evaluate the difficulty of DLP over GF(p) for discussing the security of these protocols. In this paper, we implement the number field sieve which is the asymptotically fastest algorithm for solving DLP over GF(p). We show how to generate the good polynomials which contain no singular prime in the factor base. Our experiment confirms the probability of generating good polynomials for a 75-bit prime p is about 0.61 which is equivalent to the conjecture by Lenstra et al. We also compare the running time of collection of relations for different polynomials with fixed prime p, and there is about 46 times difference in their speeds for a 75-bit prime p.

1　はじめに

アメリカ政府標準のデジタル署名方式である DSA や，PGP などで利用されている Diffie-Hellman 鍵共有は，素体 GF(p) 上の離散対数問題の困難性を安全性の根拠としている．この GF(p) 上の離散対数問題に対する漸近的に最速な解読アルゴリズムとして，数体篩法 [3, 5, 13] が知られている．数体篩法の計算量は $p \to \infty$ に対して，

$$L_p[1/3; c] = \exp((c + o(1))(\log p)^{1/3}(\log\log p)^{2/3})$$

である．但し，c は定数，$o(1)$ は $p \to \infty$ に対して $o(1) \to 0$ となる関数である．GF(p) 上の離散対数問題に対して数体篩法を初めて適用した Gordon は $c = (81/9)^{1/3}$ と見積もった [3]．その後，Schirokauer が単数に対する指標を用いることで Gordon の数体篩法を改良し，$c = (64/9)^{1/3}$ の計算量とした [13]．更に，Schirokauer のアルゴリズムでは，離散対数を求める対象の元を変化させた場合，アルゴリズムを初めからやり直す必要があったのに対し，Joux-Lercier は virtual logarithm といわれる手法を用いて，対象の元の離散対数を求める処理を独立させたアルゴリズムを提案した [5]．一方，数体篩法の実行時間は選択される代数体を定義する多項式により大きく異なることが知られている [6, 11]．また，GF(p) 上の離散対数問題解読実験は盛んに行われており [10]，現在の世界記録として Kleinjung 等が 532 ビットの解読に成功している [7]．Kleinjung 等の解読実験では多項式として skew な base-m 法により生成した 5 次式を利用している．

本稿では，数体篩法の多項式選択法に関して以下の 2 点の考察を行う．(a) 多項式 f で決まる最大整数環 $\mathcal{O}_K$ と整環 $\mathcal{O}$ に対して，$[\mathcal{O}_K : \mathcal{O}]$ を割る素数 (bad prime)[3] を因子基底に含まないような多項式 f(good な多項式 f) の判定法．(b) 固定した p における多項式 f の違いによる数体篩法の実行時間の変化．(a) に関しては，代数体を定義する多項式 f に対して，クンマー・デデキントの定理 [15, p.229] を用いた bad prime の判定法及び good な多項式 f の判定法の実装について述べる．この good な多項式 f の判定法を用いて，75 ビットの 1 つの p に対して決まる範囲からランダムに選んだ f の振り分けを行った結果，good である f の確率が文献 [9, p.39] で予想された $[\mathcal{O}_K : \mathcal{O}] = 1$ である確率 $6/\pi^2 \approx 0.61$ とほぼ一致した．(b) に関しては，まず，75 ビットの固定した p に対して定まる範囲から，skew でない base-m 法を利用して代数体を定義する多項式 f を生成した．次に，生成したそれぞれの多項式 f に対して smoothness bound B を変化させて関係探索の実行時間を計測した．$B \in \{6000, 7000, 8000, 9000\}$ に対して関係探索時間を計測した結果，最も速い f と最も遅い f は共に $B = 6000$ としたときの f で，その差は約 46 倍であった．

2 数体篩法の概要

本節では Joux-Lercier の数体篩法 [5] の概要について説明する．

2.1 GF(p) 上の離散対数問題

大きな素数 p に対して，p を標数とする素体の乗法群を $\mathrm{GF}(p)^\times = \{1, 2, 3, \ldots, p-1\}$，$\mathrm{GF}(p)^\times$ の生成元を g としたとき，ある特定の元 $a \in \mathrm{GF}(p)^\times$ に対して $g^x = a$ を満たす $x \in \{0, 1, 2, \ldots, p-2\}$ を求めるという問題を $\mathrm{GF}(p)$ 上の離散対数問題といい，この x を a の離散対数と呼ぶ．以降では，a の離散対数を $\log_g a$ と書く．

本稿では，smoothness bound B(2.3 節で定義する)，素数 l に対して，g が B-smooth かつ $p - 1 = 2l$ である場合を扱う．ここで，g が B-smooth であるとは g の全ての素因数が B 以下であることをいう．B が小さいとき高速な B-smooth の判定法として試行割算法 (trial division) がある．試行割算法とは，B 以下の全ての素数を用いて割り切れる限り判定対象の整数を割った結果，剰余が 1 になった場合に B-smooth とする方法である．

2.2 多項式選択

整数係数の次数 n の多項式 $f(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ が次の 4 つの条件を満たすとする．(i) f は既約，(ii) f はモニック，(iii) $f(m) \equiv 0 \bmod p$，(iv) l は f の判別式を割り切らない．ここで，l は 2.1 節で定義した $(p-1)/2$ である．f の根 α に対して，代数体 K を $K = \mathbb{Q}(\alpha)$，K の最大整数環を $\mathcal{O}_K$ とする．このとき，整環 $\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathcal{O}_K$ に対して，準同型写像

$$\begin{aligned} \phi : \mathcal{O} &\to \mathrm{GF}(p), \\ \alpha &\mapsto m \bmod p \end{aligned}$$

を利用する．本稿では，$b_n \neq 1$ で skew な多項式 [6, 11] については考察しない．

2.3 関係探索

実数 $B > 0$，2.2 節で選択された代数体を定義する多項式 f とその根 α に対して集合 B_R，B_A を次のように定義する．

$$\begin{aligned} B_R &= \{q \in \mathbb{P} \mid q \leq B\} \\ B_A &= \{(q, \alpha - t) \mid q \in B_R, f(t) \equiv 0 \bmod q\} \end{aligned}$$

但し，$\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ は素数全体の集合とする．B_R は B 以下の素数の集合であり，B_A は B 以下の素数の上にある一次の素イデアルの集合である．ここで，B_R の元の上界 B を smoothness bound，集合 B_R を有理側の因子基底 (rational factor base)，B_A を代数側の因子基底 (algebraic factor base) と呼ぶ．

次に，$r_R = \sharp B_R, r_A = \sharp B_A$ とし，r を $\mathcal{O}^\times$ の torsion-free rank とする．この r は f の実数根，虚数根の個数を $n_R, 2n_I$ としたとき $r = n_R + n_I - 1$ で求められる．このとき，$c, d \in \mathbb{Z}$，実数 $C > 0$ に対して，$-C/2 \leq c \leq C/2, d > 0$ の範囲から次の 3 つの条件

1. $\gcd(c, d) = 1$,
2. $c + dm = \prod_{q_i \in B_R} q_i^{e_i}$,
3. $(c + d\alpha) = \prod_{\mathfrak{q}_i \in B_A} \mathfrak{q}_i^{\varepsilon_i}$,

を満たす c, d の組 (hit pair) を $r_R + r_A + r$ 個以上集め，その集合を S とする．hit pair を探す c の範囲の大きさ C を篩区間 (sieving interval) と呼ぶ．

ある c, d に対して上記 hit pair の条件 3. を満たすかどうかは $(c + d\alpha)$ のノルム

$$N(c + d\alpha) = (-d)^n f(-c/d)$$

の絶対値によって判断する．$|N(c+d\alpha)|$ が B-smooth であるとき，つまり，

$$|N(c + d\alpha)| = \prod_{q_i \in B_R} q_i^{e_i}$$

であるとき，c, d は条件 3. を満たす．このとき，$|N(c+d\alpha)|$ を割る $\forall q_i$ に対して，$q_i \nmid [\mathcal{O}_K : \mathcal{O}]$ であるならば $(q_i, \alpha - t_i)$ が B_A に存在する．但し，$t_i \equiv -c/d \bmod q_i$ である．そして，次が成り立つ．

$$(c + d\alpha) = \prod_{(q_i, \alpha - t_i) \in B_A} (q_i, \alpha - t_i)^{e_i}.$$

これにより hit pair の条件 3. の ε_i が求められる．

2.3.1 Schirokauer の指標 λ

2.3 節で集められた全ての hit pair (c_j, d_j) に対して，Schirokauer の指標 λ を計算する [13]．$\mathcal{O}_K$ の部分集合 Γ を次のように定義する．

$$\Gamma = \{\gamma \in \mathcal{O}_K \mid N(\gamma) \not\equiv 0 \bmod l\}.$$

このとき，$\lambda : \Gamma \to l\mathcal{O}_K/l^2\mathcal{O}_K$ である写像 λ の像は n 個の成分で表される．集められた全ての hit pair (c_j, d_j) に対して，

$$\lambda(c_j + d_j\alpha) = (\lambda_{j,1}, \lambda_{j,2}, \ldots, \lambda_{j,n})$$

を計算する．そして，$e_{j,i}, \varepsilon_{j,i}, \lambda_{j,i}$ に対して，$\log_g q_i$, $\log_g \mathfrak{q}_i, x_i$ を未知数とした次のような関係式を得る．

$$\begin{aligned}&\sum_{q_i \in B_R} e_{j,i} \log_g q_i \\ &\quad\equiv \sum_{\mathfrak{q}_i \in B_A} \varepsilon_{j,i} \log_g \mathfrak{q}_i + \sum_{i=1}^{r} \lambda_{j,i} x_i \bmod l\end{aligned} \tag{1}$$

但し，x_i は $\{0, 1, 2, \ldots, l-1\}$ に含まれる整数値である．$\log_g \mathfrak{q}_i$ は virtual logarithm と呼ばれ [5]，Schirokauer がこの関係式が成立する条件について考察した [14]．

2.4 線形代数

2.3.1 節で得られた関係式 (1) の係数から行列を構成し，連立一次合同式を解くことで，mod$l$ での $\log_g q_i$, $\log_g \mathfrak{q}_i$, x_i を求める．ここで，2.1 節より生成元 g が B-smooth であったことから，$g = \prod_{q_i \in B_R} q_i^{e_{0,i}}$ としたとき次の関係式も連立一次合同式に加える．

$$\sum_{q_i \in B_R} e_{0,i} \log_g q_i \equiv 1 \bmod l$$

2.3 節の集合 S に対して $r_S = \sharp S + 1$ とし，$r_S \times (r_R + r_A + r)$ 型行列 A，$(r_R + r_A + r)$ 次列ベクトル $\vec{x}$，r_S 次列ベクトル $\vec{y}$ を次のように定義する．

$$A = \begin{pmatrix} e_{0,1} & \ldots & e_{0,r_R} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ e_{1,1} & \ldots & e_{1,r_R} & \varepsilon_{1,1} & \ldots & \varepsilon_{1,r_A} & \lambda_{1,1} & \ldots & \lambda_{1,r} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ e_{r_S,1} & \ldots & e_{r_S,r_R} & \varepsilon_{r_S,1} & \ldots & \varepsilon_{r_S,r_A} & \lambda_{r_S,1} & \ldots & \lambda_{r_S,r} \end{pmatrix},$$

$$\vec{x} = \begin{pmatrix} \log_g q_1 \\ \vdots \\ \log_g q_{r_R} \\ -\log_g \mathfrak{q}_1 \\ \vdots \\ -\log_g \mathfrak{q}_{r_A} \\ -x_1 \\ \vdots \\ -x_r \end{pmatrix}, \quad \vec{y} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ただし，$\vec{x}$ の成分は未知数で，

$$A\vec{x} \equiv \vec{y} \bmod l$$

を解くことで求められる．ここで，有理側の因子基底 B_R の元 q_i のうち，大きな q_i ほど 2.3 節で集められた hit pair (c_j, d_j) に対して $q_i \mid c_j + d_j m$ である確率が低い．集められた全ての hit pair (c_j, d_j) に対して $q_i \nmid c_j + d_j m$ かつ $q_i \nmid g$ を満たす場合は，そのような $\log_g q_i$ は求められない．この $\log_g q_i$ を求める必要がある場合は，篩区間 C を増やし，関係式を行列に追加する必要がある．代数側の因子基底 B_A の元にも同様のことが言える．

2.5 最適なパラメータの見積もり

数体篩法の漸近的な実行時間は代数体を定義する多項式の次数 n，smoothness bound B，篩区間 C(パラメータ) によって決まる．B に関しては，B の大きさによって関係探索及び線形代数の実行時間が次のように変化する．B を小さく (大きく) した場合，関係探索では集める hit pair の数が減少 (増加) するが，hit pair を得られる確率が低く (高く) なる．線形代数では行列の規模が小さく (大きく) なり連立一次合同式を解く時間が短く (長く) なる．

いくつかの適切な仮定を用いることで実行時間を漸近的に最小にするパラメータを 1 節の L_p 関数を用いて次のように見積もることができる [17]．

$$n = \left(\frac{(3 + o(1)) \log p}{\log \log p}\right)^{1/3}, \tag{2}$$

$$B = L_p[1/3; (8/9)^{1/3}], \tag{3}$$

$$C = 2L_p[1/3; (8/9)^{1/3}]. \tag{4}$$

3 数体篩法の実装

本節では数体篩法の実装手法について説明する．

3.1 多項式選択

多項式選択では 2.2 節で述べた 4 つの条件を満たすような，代数体を定義する n 次の多項式 f を構成する．以下の選択法は [13] を基にした，p の倍数を m 進展開する base-m 法である．以下の選択法を用いると，素体 GF(p) の標数 p と多項式 f の次数 n，多項式 f の mod$p$ の根 m に対して多項式 f が一意的に定まる．次数 n は標数 p から 2.5 節の式 (2) により計算され，多項式 f の mod$p$ の根 m は n と p により定まる区間 $[p^{1/n}, 2p^{1/n})$ から選択される．

代数体を定義する多項式 f の mod p の根 m を $p^{1/n} \leq m < 2p^{1/n}$ を満たすように選ぶ．ここで，$h \in \mathbb{N}$

に対して $hp \geq m^n$ を満たす最小の hp を求め，m 進展開する．つまり，次を満たすような $b_i \in \mathbb{Z}$ $(0 \leq b_i < m)$ を求める．

$$\sum_{i=0}^{n} b_i m^i = hp.$$

ここで，$f(X) = \sum_{i=0}^{n} b_i X^i$ とする．

3.1.1 good な多項式の判定法

3.1 節で選択された，代数体を定義する n 次の多項式 f によって定まる最大整数環 $\mathcal{O}_K$ 及び整環 $\mathcal{O}$ に対して，$q \mid [\mathcal{O}_K : \mathcal{O}]$ を満たす素数 q の上にある素イデアルは 2.3 節のように $\{(q, \alpha - t) \mid f(t) \equiv 0 \bmod q\}$ として求めることができない．この様な素数 q を bad prime，bad prime 以外の素数を good prime と定義する [3]．この bad prime の上にある素イデアルの計算については [2] の 6 章に詳しい解説がある．ここで，bad prime が有理側の因子基底 B_R に含まれないような多項式 f を good である，含まれるならば bad であると定義する．以下で good な多項式 f の判別法を説明する．

bad prime であれば代数体を定義する多項式 f の判別式

$$D_f = (-1)^{n(n-1)/2} R(f, f')$$

の平方因子であることが知られている [2, Prop 4.4.4]．ここで，n は多項式 f の次数，$R(f, f')$ は f と f' の終結式である．D_f の平方因子を得るには D_f を素因数分解する必要があるが，f が good であるかを判定するには B_R に bad prime が存在しないことを調べればよいため，B_R の元に対して D_f の平方因子であるかどうかを 2.1 節の試行割算法で判別することで十分である．D_f の平方因子が bad prime であるかはクンマー・デデキントの定理 [15, p.229] を利用することで判別できる．

定理 4.1.1 (クンマー・デデキント [15, p229]). 多項式 $f(X)$ によって定まる最大整数環を $\mathcal{O}_K$，整環を $\mathcal{O}$ とする．素数 q に対して $f(X)$ が次のように分解されたとする．

$$f(X) \equiv \prod_i g_i(X)^{e_i} \bmod q$$

但し，$g_i(X)$ は既約かつモニックである．ここで，$e_i > 1$ かつ次数が 1 である $g_i(X)$ に対して $\mathbb{Z}$ 上で $g_i(X)$ を法とした $f(X)$ の剰余を r_i とする．このとき，少なくとも 1 つの r_i が $q^2 \mid r_i$ を満たすことと $q \mid [\mathcal{O}_K : \mathcal{O}]$ は同値である．

ここで，$g_i(X)$ の次数は 1 であることから r_i は定数であることに注意する．この定理を利用した多項式の判定アルゴリズムを Algolithm 1 に示す．

Algorithm 1：多項式 f の good,bad 判定

INPUT: polynomial f, rational factor base $B_R = \{q_1, q_2, \ldots, q_{r_R}\}$
OUTPUT: f is $\{good, bad\}$

```
D_f ← discriminant of f.
for i ← 1 to r_R do
  if q_i^2 | D_f then
    factor f in GF(q_i)[X]
    as f(X) ≡ ∏_{j=1}^{s} g_j(X)^{e_j} mod q_i
    for j ← 1 to s do
      if degree of g_j is 1 and e_j > 1 then
        r_j ← f(X) mod g_j(X)
        (Note that r_j ∈ Z)
        if q_i^2 | r_j then
          return bad
        end if
      end if
    end for
  end if
end for
return good
```

Algorithm 1 では，B_R の元であり D_f の平方因子でもある素数 q のうち 1 つでも $q \mid [\mathcal{O}_K : \mathcal{O}]$ を満すような多項式 f を bad，そうでなければ good であると判定している．

$p \to \infty$ としたとき，p によって定まる範囲からランダムに選ばれた m で構成した f に対して $[\mathcal{O}_K : \mathcal{O}] = 1$ となる確率は $6/\pi^2 \approx 0.61$ となることが知られている [9, p.39]．

3.2 関係探索

2.3 節にあるように，関係探索では $-C/2 \leq c \leq C/2, d > 0$ の範囲から hit pair を $r_R + r_A + r$ 個以上集める．hit pair とは $\gcd(c, d) = 1$ であり，$c + dm, |N(c + d\alpha)| = |(-d)^n f(-c/d)|$ が共に B-smooth であるような (c, d) であった．この hit pair を得るために，線篩を用いて $c + dm, |N(c + d\alpha)|$ が共に B-smooth である可能性の高い (c, d) を見つけ，この (c, d) に対してユークリッド互除法及び 2.1 節の試行割算法を用いて hit pair であるかの判定を行う．また，それぞれの hit pair に対して Schirokauer の指標 λ を計算し，関係式 (1) を構成する．

3.2.1 線篩による hit pair の探索

線篩では固定した d に対して $-C/2 \leq c \leq C/2$ から $g(c, d)$ が B-smooth である可能性の高い (c, d) を見つける．ここで，多項式

$$g(X, Y) = \begin{cases} X + Ym & (5) \\ |N(X + Y\alpha)| & (6) \end{cases}$$

を篩多項式 (sieve polynomial) と定義する．但し，有理側では式 (5) を，代数側では式 (6) を用いる．固定した d に対する有理側の線篩のアルゴリズムを Algorithm 2 に示す．

Algorithm 2：有理側の線篩 (d を固定)

INPUT: sieving interval C, rational factor base $B_R = \{q_1, q_2, \ldots, q_{r_R}\}$, sieve polynomial $g(X, d) = X + dm$

OUTPUT: $T = \{(c, d) \mid g(c, d)$ is probably B-smooth$\}$ $s.t.$ $-C/2 \le c \le C/2$

1: $L[c] \leftarrow 0$ $(-C/2 \le \forall c \le C/2)$
2: **for** $i \leftarrow 1$ **to** r_R **do**
3: $\quad c \leftarrow c_0$, where c_0 is the least integer such that $c_0 \ge -C/2$ and $q_i \mid g(c_0, d)$
4: $\quad$ **while** $c \le C/2$ **do**
5: $\quad\quad L[c] \leftarrow L[c] + \lceil \log_2 q_i \rceil$
6: $\quad\quad c \leftarrow c + q_i$
7: $\quad$ **end while**
8: **end for**
9: **for** $c \leftarrow -C/2$ **to** $C/2$ **do**
10: $\quad$ **if** $L[c] \approx \log_2 g(c, d)$ **then**
11: $\quad\quad T \leftarrow T \cup \{(c, d)\}$
12: $\quad$ **end if**
13: **end for**
14: **return** T

代数側の線篩では Step 3-7 を $|N(X, d)| \bmod q_i$ の零点の個数分の c_0 に対して行う．本実装では Step 10 の $L[c] \approx \log_2 g(c, d)$ かどうかの判断には，$L[c] \ge 0.75 \log_2 g(c, d)$ という条件を用いた．

固定した d に対して線篩を有理側及び代数側で行い，両側で B-smooth である可能性が高いと判断された (c, d) に対して，ユークリッド互除法，2.1 節の試行割算法を用いて 2.3 節の hit pair の条件を満たすかどうかを判定する．2.4 節の行列を構成する成分 $e_{j,i}, \varepsilon_{j,i}$ はこの判定における試行割算法で得られる．この様な線篩と判定を行う手順を $d = 1, 2, 3, \ldots$ に対して，得られた hit pair の数が $r_R + r_A + r$ 以上になるまで繰り返していく．

3.2.2 Schirokauer の指標 λ

3.2.1 節で集めた全ての hit pair (c_j, d_j) に対して $\lambda(c_j + d_j\alpha) = (\lambda_{j,1}, \lambda_{j,2}, \ldots, \lambda_{j,n})$ を計算する．ℓ が l の上にある素イデアルの全体を動くとして，ϵ を $\sharp(\mathcal{O}_K/\ell)^\times$ たちの最小公倍数とする．このとき，$(\mathbb{Z}/l^2\mathbb{Z})[X]$ 上で

$$r(X) = (c_j + d_j X)^\epsilon - 1 \bmod f(X)$$

を計算する．$r(X)$ の k 次の項を r_{k+1} $(k = 0, 1, \cdots, n-1)$ とすると，$r_k \equiv 0 \bmod l$ が成り立つ．ここで，$\lambda_{j,i}$ は $\lambda_{j,i} = r_i/l$ で求まる．

3.3 線形代数

本稿の線形代数の実装では，ガウスの消去法を用いて 2.4 節の $\vec{x}$ の成分を求めた．具体的には，行列 A と列ベクトル $\vec{y}$ に対して前進消去と後退代入を行うことで，行列 A を対角化して $\vec{x}$ の成分を計算した．但し，行列のサイズを小さくする Structured Gaussian Elimination[8, 12] などの前処理は行っていない．

4 実装結果

本節では実装した数体篩法の計算実験の結果と考察について述べる．

4.1 実装環境とパラメータ選択

実装は C++言語で行い，コンパイラは gcc，多倍長ライブラリは gnu mp，多項式演算には NTL を用いた．実験は Core2 Duo E8400(3.00GHz), 2GB RAM を搭載した計算機 1 台で行った．但し，CPU の 2 つのコアのうち 1 コアのみを用いて計算を行った．

上記の環境で 2 節及び 3 節を実装した結果から，我々の実験環境において 1 週間に約 1000 回程度数体篩法を実行できるような p は 75 ビットであったため，p を 75 ビットのある素数に固定して実験を行った．ここで，2.5 節の式 (2) から 2.2 節の代数体を定義する多項式 f の次数 n を 3 とし，式 (3) から 2.3 節の smoothness bound B を 7777 とした．篩区間 C は 389635 とした．また，以下の実験ではランダムな 3 次の f の生成法として，$[p^{1/3}, 2p^{1/3})$ の範囲からランダムに m を選び，3.1 節の多項式選択法に従い f を構成した．

4.2 good な多項式 f の確率

上記のように選択した 1045 個の多項式 f に対し，3.1.1 節の Algorithm 1 を適用した結果，good な f は 693 個であった．このとき，good な f の割合は 0.66 となり，[9, p.39] で予想された $[\mathcal{O}_K : \mathcal{O}] = 1$ となる確率 $6/\pi^2 \approx 0.61$ とほぼ一致した．

また，good な多項式 f を選択して数体篩法を行った場合，正しい離散対数が計算できるか (求められた全ての $\log_g q_i$ が正しいか) 実験を行った．ここで，p を 75 ビットとすると，693 個の good な f に対して上記の 1 コアで数体篩法を行うには約 5 日を要するため，1 日で約 10000 回程度数体篩法を行える 45 ビットの素数 p に対して実験を行った．この実験で得られた 6420 個の good な f を使用して数体篩法を行った結果，全ての f で正しい離散対数が計算できた．

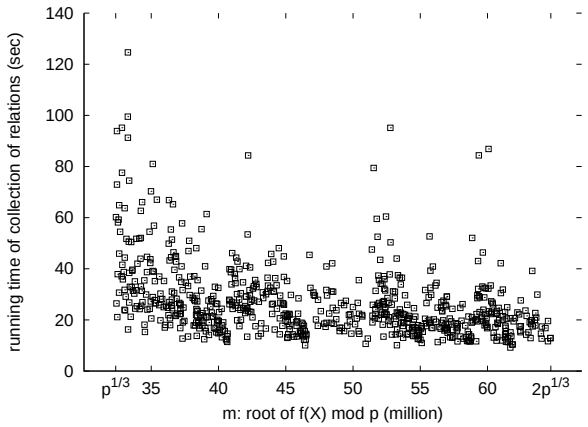

図 1: $B = 8000$ における関係探索時間

4.3 good な f に対する関係探索時間

4.2 節で得られた 693 個の good な多項式 f に対し，2.3 節の smoothness bound $B \in \{6000, 7000, 8000, 9000\}$ について，3.2.2 節の Schirokauer の指標 λ の計算を含む関係探索の実行時間を計測した．B の範囲は 2.5 節の式 (3) で見積もられた最適値 $B = 7777$ を含むように設定した．

最適値 $B = 7777$ に最も近い $B = 8000$ の場合の計測結果を図 1 に示す．横軸は f を選択する際に選ばれた $\bmod p$ の根 m の値である．$B = 8000$ では，最も速い f は 9.19 秒，最も遅い f は 124.62 秒，平均は 26.83 秒であった．最も速い f は最も遅い f に対して約 13 倍，平均に対しては約 3 倍 速かった．$B = 8000$ で最も速い (遅い)f は，$B \in \{6000, 7000, 9000\}$ においても最も速かった (遅かった)．

一方，B による関係探索時間の変化では，B を 8000 から小さくするほど速い f と遅い f の関係探索時間の差が大きくなり，B を大きくするほど差が小さくなる傾向があった．この実験で最も関係探索を速く終えた f と遅く終えた f は $B = 6000$ のときの f であった．最も速い f は 6.90 秒，最も遅い f は 318.62 秒であり，最も速い f は最も遅い f の約 46 倍 速かった．また，最も速い f 及び最も遅い f，平均的な f に対して篩区間 C を変化させても関係探索時間の比はほぼ変化しなかった．

5 まとめ

本稿では，GF(p) 上の離散対数問題に対する数体篩法の実装及び実験を行った．また，bad prime が有理側の因子基底に含まれないような代数体を定義する多項式 f(good な多項式) の判定法をクンマー・デデキントの定理を利用して実装した．この判定法を用いて，75 ビットの 1 つの素数 p に対して定まるランダムに選んだ多項式 f が good である確率が Lenstra 等によって予想された $[\mathcal{O}_K : \mathcal{O}] = 1$ である確率 $6/\pi^2 \approx 0.61$ とほぼ一致した．さらに，75 ビットの 1 つの素数 p に対して good な多項式 f による関係探索の実行時間の比較を smoothness bound $B \in \{6000, 7000, 8000, 9000\}$ について行った．この実験で最も速い f は $B = 6000$ のときの f で，$B = 6000$ のとき最も遅い f に対して約 46 倍速く，大きな差がみられた．この様な関係探索が速い f を選択する方法について考察することが今後の課題となる．

参考文献

[1] 青木和麻呂, 植田広樹, 木田佑司, 下山武司, 園田裕貴. “一般数体篩法実装実験 (1) - 概要,” SCIS 予稿集, pp.269-273, 2004.

[2] H. Cohen. “A Course in Computational Algebraic Number Theory,” Graduate Texts in Math., vol.138, 1993.

[3] D. Gordon. “Discrete Logarithms in GF(p) Using the Number Field Sieve,” SIAM J. Discrete Math., vol.6, pp.124-138. 1993.

[4] 伊豆哲也, 小暮淳, 下山武司. “近年の素因数分解について,” Fundamentals Review, vol.1, No.3, pp.58-70, 2008.

[5] A. Joux, and R. Lercier. “Improvements to the General Number Field Sieve for Discrete Logarithms in Prime Fields,” Math. Comp., vol.72, No.242, pp.953-967, 2003.

[6] T. Kleinjung. “On Polynomial Selection for the General Number Field Sieve,” Math. Comp., vol.75, No.256, pp.2037-2047, 2006.

[7] T. Kleinjung et al. “Discrete Logarithms in GF(p) - 160 digits,” Posting to the Number Theory List, available at `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0702&L=nmbrthry&T=0&P=194`, 2007.

[8] B. LaMacchia and A. Odlyzko. “Solving Large Sparse Linear Systems over Finite Fields,” CRYPTO ’90, LNCS 537, pp.109-133, 1991.

[9] A. Lenstra and H. Lenstra Jr. *The Development of the Number Field Sieve,* Lecture Note in Math., vol.1554, Springer-Verlag, 1993.

[10] R. Lercier. “Computations - Discrete Logarithms,” available at `http://perso.univ-rennes1.fr/reynald.lercier/plugins/getfilehtml/getfilehtml7d2c.html?lng=en&id=6`, 2009.

[11] B. Murphy. “Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm,” Ph.D. thesis, The Australian National University, 1999.

[12] C. Pomerance and J. Smith. “Reduction of Huge, Sparse Matrices over Finite Fields via Created Catastrophes,” Experiment. Math., vol.1, no.2, pp.89-94, 1992.

[13] O. Schirokauer. “Discrete Logarithms and Local Units,” Philos. Trans. Roy. Soc. London Ser. A, vol.345, pp.409-424, 1993.

[14] O. Schirokauer. “Virtual Logarithms,” J. Algorithms, vol.57, pp.140-147, 2005.

[15] P. Stevenhagen. “The Arithmetic of Number Rings,” Algorithmic Number Theory, pp.209-266, MSRI Publications, vol.44, 2008.

[16] C. Studholme. “The Discrete Log Problem,” available at `http://www.cs.toronto.edu/~cvs/dlog/`, 2002.

[17] 内山成憲. “有限体上の離散対数問題 -数体篩法, 関数体篩法-,” 日本応用数理学会論文誌, vol.13, No.2, pp.245-256, 2003.

[18] D. Weber, “An Implementation of the General Number Field Sieve to Compute Discrete Logarithms mod p,” EUROCRYPT ’95, LNCS 921, pp.95-105, 1995.