情報処理学会論文誌　Vol. 50　No. 8　1768–1774 (Aug. 2009)

円分体の相対類数計算 ——多倍長係数多項式の高速乗算の応用

谷　口　哲　也[†1]

2 次元 FFT を用いた多倍長整数係数多項式の高速乗算アルゴリズムを用いて，100,000 以下の素数導手 p を持つ虚アーベル体の相対類数をすべて求めた．本アルゴリズムの計算量は $O(p^2\log^2(p)\log\log(p))$ である．本手法は巡回終結式，巡回行列式の高速計算に応用することができる．

Computation of the Relative Class Number of Cyclotomic Fields —Applications of Fast Multiprecision Polynomial Multiplications

Tetsuya Taniguchi[†1]

We obtain a multiprecision polynomial multiplication algorithm using 2-dimensional FFT for computing the relative class numbers of imaginary abelian number fields with prime conductors p less than 100,000. The number of bit-operations of computation under our algorithm is $O(p^2\log^2(p)\log\log(p))$. Our algorithm can apply computation of cyclic resultants and determinants.

1. 序　　説

本論文では 100,000 以下のすべての素数 p に対して，導手 p を持つ円分体およびその虚の部分体の相対類数を求め，また $p-1$ が 7 以下の素因子のみを持つ $p \le 40{,}824{,}001$ に対する相対類数をすべて求める．既知の最新結果は，Shokrollahi [17] による 10,000 以下の素数導手 p を持つ虚アーベル体の相対類数の計算および，Yamamura [22] による同範囲の計算であり，Shokrollahi のアルゴリズムの計算量は ERH の下で $O(p^2\log^2(p)\log\log(p))$ である．

2 章では本アルゴリズムの要点である Galois 群の作用に関する反復平方法および多倍長整数係数多項式に関する 2 次元 FFT 乗算を提示する．3 章では計算量を評価し，ERH を仮定することなく $O(p^2\log^2(p)\log\log(p))$ で本アルゴリズムが動作することを示し，実装面でも十分に高速であることを報告する．本手法の応用として巡回終結式（cyclic resultant）や巡回行列式の高速計算をあげる．

なお，代数的整数論の諸概念については Washington [20]，Ireland ら[8]，高木[23),24)]，藤崎[27]，山本[26] などを参照されたい．

2. アルゴリズム

本アルゴリズムの概要を述べる．

まず，相対類数を円分体の整数の絶対ノルムの積として表現し，それぞれの絶対ノルムを相対巡回拡大の相対ノルムの合成として表現する．すなわち相対類数の計算を相対ノルムの計算に帰着する．これはメモリ使用量の削減のためである．また，高速化のために，

- Galois 群の作用に関する反復平方法，
- 多倍長整数係数多項式に関する 2 次元 FFT 乗算，

を用いる．反復平方法は積の回数を削減し，2 次元 FFT 乗算はそれぞれの積を高速化する．

2.1 相対ノルム計算への帰着

$\mathbb{N}$ を自然数全体，$\mathbb{Z}$ を整数全体，$\mathbb{Q}$ を有理数全体とする．p を素数，r を法 p の原始根，r_i を $r^i \equiv r_i \pmod p$, $0 < r_i < p$ を満たす整数とし，自然数 n に対して ζ_n を複素数体 $\mathbb{C}$ 上の 1 の原始 n 乗根とする．Kummer [11] は多項式 $f(x)=\sum_{i=0}^{p-2} r_{-i}x^i$ を用いて円分体 $\mathbb{Q}(\zeta_p)$ の相対類数 h_p^- を表現した：

$$h_p^- = \frac{1}{(2p)^{(p-3)/2}}\left|\prod_{k=0}^{(p-3)/2} f(\zeta_{p-1}^{2k+1})\right|. \tag{1}$$

まず，式 (1) の右辺を次のように変形する：

$$(2p)^{(p-3)/2}h_p^- = \prod_{\substack{de=p-1\\ 2\nmid d}} \left|\mathrm{N}_{\mathbb{Q}(\zeta_e)}\left(f(\zeta_e)\right)\right|. \tag{2}$$

ここに $\mathrm{N}_{\mathbb{Q}(\zeta_e)}$ は $\mathbb{Q}(\zeta_e)$ の絶対ノルムを表す．式 (2) は本質的に Lehmer [14] の Theorem 1 と

†1 東京理科大学理工学部
Tokyo University of Science

同じである．さらに，体の列 $\mathbb{Q} \subset K \subset L$ に対しノルム写像の連鎖律 $\mathrm{N}_{L/\mathbb{Q}} = \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{N}_{L/K}$ が成り立つから，相対類数の計算は相対巡回拡大に関する相対ノルムの計算に帰着される．

2.2　反復平方法

L/K を n 次巡回拡大，$\mathrm{Gal}(L/K) = \langle\sigma\rangle$ とし，$\alpha \in L$ とする．相対ノルム $\mathrm{N}_{L/K}(\alpha) = \alpha^{1+\sigma+\cdots+\sigma^{(n-1)k}}$ は反復平方法により効率的に計算することができる．

Proposition 2.1（反復平方法 1）**.** 次のアルゴリズムは $\alpha \in L$ の相対ノルム $\beta = \mathrm{N}_{L/K}(\alpha)$ を出力し，L の積の回数はたかだか $3[\log_2 n]$ 回である．ここに $[x]$ は x を超えない最大の整数を表す．

Require: n：正の整数，$\alpha \in L$.
Ensure: $\beta = \mathrm{N}_{L/K}(\alpha)$.
　$i = 0$, $\ell = [\log_2(n)]$.
　$e = 2^{\ell - i}$, $d = [n/e]$, $f = 0$.
　$\beta = \alpha$.
　while $i \leq \ell$ **do**
　　$f = f + (d \mod 2)e$.
　　$i \leftarrow i + 1$.
　　$e = 2^{\ell - i}$.
　　$d = [n/e]$.
　　$\beta \leftarrow \beta^{1+\sigma^e}(\alpha^{\sigma^f})^{(d \mod 2)}$.
　end while

Proposition 2.2（反復平方法 2）**.** 次のアルゴリズムは $\alpha \in L$ の相対ノルム $\beta = \mathrm{N}_{L/K}(\alpha)$ を出力し，L の積の回数はたかだか $3[\log_2 n]$ 回である．

Require: n：正の整数，$\alpha \in L$.
Ensure: $\beta = \mathrm{N}_{L/K}(\alpha)$.
　$k = [\log_2 n]$, $\beta \leftarrow \alpha$.
　while $k \geq 1$ **do**
　　$\beta \leftarrow \beta^{1+\sigma^{[n/2^k]}}$.
　　if $[n/2^{k-1}] \equiv 1 \pmod 2$ **then**
　　　$\beta \leftarrow \beta\alpha^{\sigma^{2[n/2^k]}}$
　　end if
　　$k \leftarrow k - 1$
　end while

上記の 2 つのアルゴリズムにおける L の積の回数はともに $O(\log n)$ である．両者を実装して比較したところ，$p < 10{,}000$ の相対類数計算においてほとんど差はなく，反復平方法 2 に対する反復平方法 1 の実行時間の比は約 1.003 倍であった．本番用の実装では反復平方法 2 を採用した．

2.3　2 次元 FFT 乗算

相対ノルムの計算をするためには円分体の元の加減乗算が必要となる．そこで，同型

$$\mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[x]/\Phi_n(x)\,\mathbb{Z}[x] \quad (\Phi_n(x) \text{ は } n\text{-円分多項式})$$

を用い，相対類数の計算を $\mathbb{Z}[x]$ の加減乗算と $\Phi_n(x)$ による剰余に帰着する．このうち最も重い演算は $\mathbb{Z}[x]$ の乗算，すなわち多倍長整数係数多項式の乗算である．なお，$\mathbb{Z}[\zeta_n]$ における複数回の乗算では次の工夫をした．相対類数計算においては n は偶数であることに注意し，乗算のたびに毎回 $x^{n/2} + 1$ で剰余をとった後に $\Phi_n(x)$ で剰余をとり，多項式の次数を $\varphi(n)$ 未満に保つ．これにより多項式の次数は $\varphi(n)$（$\leq n/2$）未満におさえられ，高速化とメモリ使用量の削減を実現した．

$M_{\mathrm{int}}(m)$ で m bit 整数どうしの乗算に必要な bit 演算の回数を表し，$M(m,n)$ で m bit 整数係数 n 次多項式の乗算に必要な bit 演算の回数を表す．m bit 整数どうしの乗算に必要な計算量は，筆算方式では $M_{\mathrm{int}}(m) = O(m^2)$ であり，Karatsuba 法[9),10)] では $M_{\mathrm{int}}(m) = O(m^{\log_2 3})$ となる．しかし FFT[25)] を用いた場合，$M_{\mathrm{int}}(m) = O(m\log(m)\log\log(m))$ である．以降の m bit 整数どうしの乗算の計算には FFT 乗算[10)] を用いる．多項式の乗算を筆算方式で計算した場合は $M(m,n) = O(mn^2\log(m)\log\log(m))$ であり，Karatsuba 法では $M(m,n) = O(mn^{\log_2 3}\log(m)\log\log(m))$ である．しかし 2 次元 FFT を用いた場合，$M(m,n) = O(mn\log(mn)\log\log(mn))$ となることを次で示す．

2.3.1　多倍長整数係数多項式の 2 次元 FFT 乗算

多倍長整数係数多項式の 2 次元 FFT 乗算とその計算量について述べる．

多倍長整数の基数を $R \in \mathbb{N}_{>1}$ で表し，各係数が R 進 m 桁以下であるような $n-1$ 次以下の多項式 $f(x), g(x) \in \mathbb{Z}[x]$ を

$$f(x) = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1} f_{ji}R^j\right)x^i, \quad (0 \leq f_{ji} \leq R-1),$$

$$g(x)=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}g_{ji}R^j\right)x^i,\quad (0\le g_{ji}\le R-1)$$

と表す．次数が $n-1$ より真に小さい場合は先頭に 0 を詰めて見かけの次数を $n-1$ 次に揃え，同様にして各係数の見かけの桁数を m 桁に揃える．$f(x)$ を次のように $2n\times 2m$ の 2 次元配列に変換する：

$$f=\begin{pmatrix} f_{0\,0} & f_{0\,1} & \cdots & f_{0\,n-1} & \\ f_{1\,0} & f_{1\,1} & \cdots & f_{1\,n-1} & \\ \vdots & \vdots & \ddots & \vdots & O \\ f_{m-1\,0} & f_{m-1\,1} & \cdots & f_{m-1\,n-1} & \\ & & O & & O \end{pmatrix}.$$

$g(x)$ も同様に 2 次元配列 g に変換する．離散フーリエ変換の畳み込み定理から

$$f*g=\frac{1}{4mn}\mathrm{DFT}^{-1}_{2n,2m}(\mathrm{DFT}_{2n,2m}(f)\cdot\mathrm{DFT}_{2n,2m}(g)),$$

が成立する．よって $f(x)g(x)$ は $f*g$ の係数から復元すればよい．以上が 2 次元 FFT 乗算の原理である．

次に計算量を見積もる．一般に，サイズ N の FFT の計算量は $O(N\log(N)\log\log(N))$ である．よって，内側の離散フーリエ変換に必要な計算量は $O(mn\log(mn)\log\log(mn)))$ となり，また成分ごとの積に必要な計算量は $O(mn)$ である．その外側の逆離散フーリエ変換に必要な計算量は $O(mn\log(mn)\log\log(mn)))$ となり，各成分を定数倍する操作の計算量は $O(mn)$ である．したがって，m-bit 整数係数の $n-1$ 次多項式に関する 2 次元 FFT 乗算全体の計算量は $O(mn\log(mn)\log\log(mn)))$ となる．

3. 計算量の評価，計算環境，計算結果

この章では，本アルゴリズムの計算量を評価し，使用計算機やソフトウェアなどについて述べ，得られた計算結果の分析をする．

3.1 計算量の評価

相対ノルム，絶対ノルム，相対類数計算の順に計算量の評価を行う．

3.1.1 相対ノルム計算の計算量

$a\in\mathbb{Z}$ に対し，$a\neq 0$ のとき $\ell(a):=[\log_2(|a|)]+1$，$a=0$ のとき $\ell(a)=0$ とおく．L/K が n 次巡回拡大，$L\subset\mathbb{Q}(\zeta_m)$ のとき，$\alpha=\sum_{i=0}^{m-1}a_i\zeta_m^i\in L$ に対し $\ell_\alpha=\max\{\ell(a_i)\mid 0\le i\le m-1\}$ とおけば，$\mathrm{N}_{L/K}(\alpha)$ における 1 回の乗算の計算量はたかだか $M(n(\log_2(m)+\ell_\alpha),m)=O(mn(\log_2(m)+\ell_\alpha)\log(mn(\log_2(m)+\ell_\alpha))\log\log(mn(\log_2(m)+\ell_\alpha))$ である．

反復平方法により，$\mathrm{N}_{L/K}(\alpha)$ における乗算の回数は $O(\log(n))$ である．一般に，1 回の反復の計算量が $M(n)$ であるような計算を $\log n$ 回繰り返すために必要な計算量は $M(n)\log n$ である．しかし $M(n/2)\le M(n)/2$ が成り立つ場合，実際の計算量は $M(n)(1+1/2+1/2^2+\cdots)=2M(n)$ でおさえられる．$M((n/2)(\log_2(m)+\ell_\alpha),m)\le M(n(\log_2(m)+\ell_\alpha),m)/2$ が成り立つため，$\mathrm{N}_{L/K}(\alpha)$ 全体を通じた計算量は $O(mn(\log_2(m)+\ell_\alpha)\log(mn(\log_2(m)+\ell_\alpha))\log\log(mn(\log_2(m)+\ell_\alpha))$ である．また Galois 群の作用の計算に必要な計算量は $O(m\ell_\alpha)$ であり，$(\bmod\ x^m-1)$ の剰余演算の計算量は $O(m\ell_\alpha)$ となる．まとめると，相対ノルム $\mathrm{N}_{L/K}(\alpha)$ の計算量は $O(mn(\log_2(m)+\ell_\alpha)\log(mn(\log_2(m)+\ell_\alpha))\log\log(mn(\log_2(m)+\ell_\alpha))$ である．

3.1.2 絶対ノルム計算の計算量

以降では簡単のため $K_n=\mathbb{Q}(\zeta_n)$ と表す．上記の結果を $L=K_n$，$K=\mathbb{Q}$ として適用すると，$\alpha\in K_n$ の絶対ノルム $\mathrm{N}_{K_n}(\alpha)$ の計算量は $O(\varphi(n)n(\log_2(n)+\ell_\alpha)\log(\varphi(n)n(\log_2(n)+\ell_\alpha))\log\log(\varphi(n)n(\log_2(n)+\ell_\alpha))$ である．

今回のプログラムでの絶対ノルムの計算は，K_{nq}/K_n（$n\in\mathbb{N}$，q：素数）の形をした巡回拡大をできるだけ多く経由するようにした．その理由はメモリ使用量削減のためである．この体の最小多項式は円分多項式なので多倍長演算は不要であり，これを求める時間は無視できる．$\gcd(n,q)=1$ のときは K_{nq}/K_n の真の中間体が存在し，さらに巡回拡大に分解することができるが，この分解は採用しない．その理由は最小多項式を求めるコストが大きいためである．また乗算回数は反復平方法により十分に削減されており，高速化が見込めないことも理由の 1 つである．

3.1.3 相対類数計算の計算量

式 (2) より，相対類数 h_p^- は $f(\zeta_{(p-1)/d})$ の絶対ノルムの積として表されている．簡単のため $e=(p-1)/d$ とおく．各 $f(\zeta_e)$ の係数の最大値 $\ell_{f(\zeta_e)}$ は $\ell_{f(\zeta_e)}<\log_2(d(p-1))=\log_2 d^2e$ を満たす．$\log e+\log d^2e=2\log(p-1)$ に注意すると，絶対ノルム $\mathrm{N}_{K_e}(f(\zeta_e))$ の計算には $O(e^2\log(p-1)\log(e\log(p-1))\log\log(e\log(p-1)))$ の計算量を必要とする．$\sum_{d|n}d^2=n^2\sum_{d|n}1/d^2<n^2\pi^2/6=O(n^2)$ より，相対類数 h_p^- を計算するために必

要な計算量は $O(p^2 \log^2(p) \log\log(p))$ である．

3.2 計算環境

今回の計算で用いたハードウェア，ソフトウェアはそれぞれ**表 1**，**表 2** のとおりである．

本プログラムは C 言語で記述し，Linux 上で開発した．多倍長整数係数多項式の演算の実装のために GMP [5] を用い，2 次元 FFT 乗算の実装のために FFTW [3] を用いた．GMP は多倍長演算を CPU アーキテクチャごとに最適化して実装した高速なライブラリであり，FFTW は多くのプロセッサにおいて高速なフーリエ変換ライブラリとして知られている．使用ソフトウェアの詳細は表 2 のとおりである．なお，本プログラムではマルチスレッド化や分散メモリ型の並列化は行っていない．

本プログラムを 1 台の Core2Duo E6700 2.66 GHz の機械で実行すると，$p < 10{,}000$ の範囲の相対類数は約 15 分ですべて求まった．一方，Shokrollahi [17] では Ultra SPARC 167 MHz を用いて約 1.5 日要しており，両者の速度比は 140 倍以上である．両 CPU の FFT の速度比は次のとおりである．http://www.matx.org/benchmark.html によると，Core2Duo E6700 2.66 GHz と Ultra SPARC 167 MHz の FFT の速度比は 40 倍程度である．また，Frigo ら [4] によると，UltraSPARC 167 MHz 上で FFTW の倍精度 1,024 点 FFT は約 150 MFlops で 65,536 点 FFT は約 70 MFlops であるのに対し，Core2Duo E6700 2.66 GHz 上で FFTW 3.2alpha3 付属のベンチマークプログラムを用いて実測したところ，倍精度 1,024 点 FFT は約 2,800 ∼ 3,400 MFlops で 65,536 点 FFT は約 2,100 ∼ 2,800 MFlops であった．本プログラムは $p \sim 10{,}000$ 付近で 8,388,608 ∼ 16,777,216 点程度の倍精度 FFT を用いるが，このあたりでは 600 ∼ 1,400 MFlops 程の性能である．したがって，両 CPU の FFTW における速度比はおおむね 40 倍以内だと考えることができる．以上により本プログラムは十分高速であるといえる．Shokrollahi [17] は有限体 $\mathbb{F}_q$ 上の計算，すなわち法 q の剰余演算を多用しているが，本アルゴリズムでは $\mathbb{F}_q$ は用いず $\mathbb{Z}$ 内で計算を完結させている．このことが速度差の一因ではないかと推測される．$p < 100{,}000$ の範囲の計算には表 1 の計算機資源を用いたが，他のユーザと共有しているため，正確な実行時間は計測できていないが全体を通しておおむね 1 カ月以内に完了した．

表 1　使用ハードウェア
Table 1　Hardware.

CPU	Memory	台数
Core2Duo E8400 3.00 GHz	8 GB	1 台
Core2Duo E8400 3.00 GHz	3 GB	1 台
Core2Duo E6700 2.66 GHz	4 GB	2 台
Pentium4 with HT 2.8 GHz	2 GB	2 台
PentiumD 2.8 GHz	2 GB	1 台

表 2　使用ソフトウェア
Table 2　Software.

コンパイラ	Intel Compiler 10.1.012
多倍長整数ライブラリ	GMP-4.2.2
高速フーリエ変換ライブラリ	FFTW 3.2alpha3
ソースコード	10,000 行弱

プログラム中ではすべての p に対してつねに 2 種類の検算を行った．1 つ目は，各相対ノルム $\mathrm{N}_{L/K}(\alpha)$ の計算結果が正しく K に入っていることの検証である．すなわち，反復平方法を抜けた後の値を K の最小多項式で割り，その剰余が K の整数環の基底で表されることを確かめた．2 つ目は，各絶対ノルム $\mathrm{N}_{K_{(p-1)/d}}(f(\zeta_{(p-1)/d}))$ の p 巾因子の個数が正しいことの検証である．

3.3 計算結果

Yamamura [22] には $p < 10{,}000$ の相対類数の計算結果が公開されており，さらにいくつかの相対類数を素因数分解した結果も公開されている．Shokrollahi [17] の計算結果も Web 上に掲載されていたが，彼の論文の中に記されている URL には 2009 年 3 月現在アクセスすることはできなかった．

今回，$p < 100{,}000$ の範囲すべての素数 p に対する h_p^- の計算を行った．また，$p-1$ が 7 以下の素因数のみを持つような 40,824,001 以下のすべての p に対して h_p^- を計算した．得られたデータの分析，とくに相対類数の偶奇性，小さい素数による整除性，正則性，大きさの評価について以下に述べる．

3.3.1 偶奇性および小さい素因数

Kummer [13] は $\mathbb{Q}(\zeta_p)$ の類数 h_p について $2 \mid h_p \Leftrightarrow 2 \mid h_p^-$ を示した．すなわち，h_p の偶奇性は h_p^- の偶奇性で判定することができる．

特殊な p に対する h_p^- の偶奇性の話題として，Sophie Germain 素数に関連したものがある．q が Sophie Germain 素数であるとは，q と $2q+1$ がともに素数であることをいい，h_{2q+1}^- の偶奇性について Hurrelbrink [7] は次の予想を述べた：

Conjecture 3.1. q が Sophie Germain 素数であると仮定し，$p = 2q+1$ とおく．このとき $2 \nmid h_p^-$ が成り立つ．

Stevenhagen [18] はこの予想に関して次の結果を得た．

表 3　2-整除性（$k = \mathrm{ord}_2(h_p^-)$）
Table 3　$k = \mathrm{ord}_2(h_p^-)$.

k	個数	最初の 3 個		
2	364	163	547	853
3	274	29	113	197
4	289	277	349	421
5	48	373	683	1,117
6	155	239	337	397
7	17	3,557	11,177	12,671
8	53	941	1,009	1,021
9	32	5,419	17,431	23,773
10	18	311	4,789	19,531
11	1	45,127		
12	8	11,677	18,661	29,581
13	3	7,687	8,191	45,823
14	5	14,407	18,859	31,751
15	2	3,067	85,933	

表 4　$p < 100{,}000$ で 100 以下の素因数を持つ h_p^- の個数
Table 4　Divisibility of small primes.

素数	個数	素数	個数	素数	個数
2	1,272	29	544	67	210
3	2,085	31	507	71	227
5	2,034	37	611	73	410
7	1,352	41	575	79	208
11	847	43	363	83	74
13	1,253	47	155	89	216
17	949	53	275	97	377
19	660	59	135		
23	376	61	484		

Theorem 3.2. $q \equiv 3 \pmod 4$ と $p = 2q + 1$ がともに素数であるとし，$2 \pmod q$ が有限体の乗法群 $\mathbb{F}_q^\times$ を生成すると仮定する．このとき $2 \nmid h_p^-$ である．

今回の計算データを基に，Hurrelbrink の予想が $p < 100{,}000$ で成立することを確認した．この範囲で h_p^- の 2 巾整除性のデータを**表 3** に示し，100 未満の素数による h_p^- の整除性のデータを**表 4** に示した．

3.3.2 正　則　性

素数 p が円分体 $\mathbb{Q}(\zeta_p)$ の類数 h_p を割り切るとき，p を非正則素数といい，割り切らないとき p を正則素数という．正則素数は整数論において重要な概念である．たとえば Fermat 予想「n が 3 以上の自然数のとき，$x^n + y^n = z^n$ は非自明な自然数解を持たない」の Wiles [19),21)] による解決に先立ち，Kummer は n が正則素数のときにこの予想が正しいことを示している．また，Kummer は $p \mid h_p \Leftrightarrow p \mid h_p^-$ を示している．

表 5　非正則素数
Table 5　Irregular primes.

範囲	非正則素数の個数	素数の個数
$p <$10,000	497	1,229
10,000 $< p <$ 20,000	403	1,033
20,000 $< p <$ 30,000	373	983
30,000 $< p <$ 40,000	404	958
40,000 $< p <$ 50,000	356	930
50,000 $< p <$ 60,000	352	924
60,000 $< p <$ 70,000	345	878
70,000 $< p <$ 80,000	371	902
80,000 $< p <$ 90,000	337	876
90,000 $< p <$ 100,000	351	879

非正則素数は無限に多く存在することが示されているが，正則素数の密度は $\exp(-1/2) = 0.6065306597\cdots$ であろうという予想は未解決であり，無限に多く存在するかどうかも分かっていない．非正則素数の実例の計算としては，2001 年の Buhler ら[1)] による $p < 12{,}000{,}000$ に対する計算がある．非正則素数についての詳細は Ribenboim [16)] を参照されたい．

今回の計算結果から非正則素数の個数を集計した結果を**表 5** に示した．$p - 1$ の素因数が 7 以下に限られる場合は，高速かつ少ない記憶領域で h_p^- を計算することができ，$p \le 40{,}824{,}001$ まで h_p^- が求まった．その結果，$p = 40{,}824{,}001$ が非正則素数であることが新たにわかり，またそのときの h_p^- の大きさは 10 進法で 61,384,565 桁であった．

3.4 大きさの評価式との関係

h_p^- の大きさは p の指数関数よりも速く増大し，きわめて大きな値となる．Kummer [12)] は h_p^- の大きさに関して

$$h_p^- \sim 2p\left(\frac{p}{4\pi^2}\right)^{(p-1)/4} =: G(p) \tag{3}$$

すなわち，$\lim_{p\to\infty} h_p^-/G(p) = 1$ が成り立つであろうと予想したが，Granville [6)] はこの予想は正しくないであろうと論じている．h_p^- の大きさの評価式としては

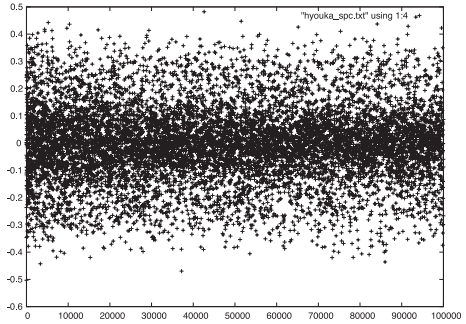

図 1　$\log(h_p^-/G(p))$
Fig. 1　$\log(h_p^-/G(p))$.

表 6　h_p^- が大きいもの
Table 6　Highest values of $h_p^-/G(p)$.

p	$\log(h_p^-/G(p))$	$h_p^-/G(p)$
42,611	0.482368	1.619907
93,371	0.462706	1.588366
51,503	0.447196	1.563921
5,231	0.442480	1.556562
84,131	0.437339	1.548581
10,313	0.436613	1.547457
91,529	0.428852	1.535493
65,171	0.425872	1.530925
99,551	0.422572	1.525882
9,689	0.421582	1.524372

$$-\frac{1}{2}\log(p) - 4\log\log(p) - 12.93 - \frac{4.66}{\log(p)} \leq \log\left(\frac{h_p^-}{G(p)}\right) \leq 5\log\log(p) + 15.49 + \frac{4.66}{\log(p)}$$

が Lepistö [15] によって与えられている．

今回の計算結果から $p < 100{,}000$ の範囲での $\log(h_p^-/G(p))$ の値の分布を計算し，**図 1** に示した．また，$\log(h_p^-/G(p))$ の値が大きいもの，小さいものから順に 10 個ずつ抜き出したものを，それぞれ**表 6**，**表 7** に示した．

表 7　h_p^- が小さいもの
Table 7　Lowest values of $h_p^-/G(p)$.

p	$\log(h_p^-/G(p))$	$h_p^-/G(p)$
3	−0.503189	0.604600
37,189	−0.469634	0.625231
3,331	−0.442499	0.642429
86,011	−0.435906	0.646678
73,309	−0.419938	0.657088
15,289	−0.419666	0.657266
78,367	−0.419378	0.657456
7,219	−0.418423	0.658084
82,189	−0.408841	0.664420
80,407	−0.406089	0.666251

3.5　本手法の応用

本アルゴリズムは円分体の絶対ノルムの高速計算を実現するものである．したがって，円分体の絶対ノルムで表現される量は本手法により高速に計算することができる：

- 巡回終結式 $\mathrm{Res}(f(x), x^n - 1)$,
- Skew 巡回終結式 $\mathrm{Res}(f(x), x^n + 1)$,
- 巡回行列の行列式,
- Skew 巡回行列の行列式.

4.　問題点および展望

本アルゴリズムの問題点は $p-1$ が大きな素因数を持つときにメモリ使用量が大きくなることであり，とくに $p = 2q+1$（p，q 素数）の形の場合，すなわち Sophie Germain 素数の場合で問題となる．この場合では計算に使える中間体がほとんど存在せず，相対ノルムの計算において多項式の次数が大きいまま係数の bit 長が増大し，メモリ使用量も増大する．たとえば $p \sim 100{,}000$ 付近では最大 250,000 bit 以上の係数を持つ約 50,000 次の多項式が現れ，これを 1 つメモリに格納するだけで 1.5 GB 以上の領域が必要となる．今回の実装では Karatsuba 法[9] で多項式の再帰分割を行って次数を縮小し，不必要な部分をディスクに退避させた．この方法ではメモリ使用量の最大値をおさえることはできるが，計算量が増大するという問題点がある．今後は Nussbaumer 法[2] などに切り替えるべきであると考える．

謝辞　有益な助言，ご指摘をくださった査読者の方々に感謝申し上げます．

参 考 文 献

1) Buhler, J., Crandall, R., Ernvall, R., Metsänkylä, T. and Shokrollahi, M.A.: Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comput.*, Vol.31, No.1-2, pp.89–96 (2001). Computational algebra and number theory (Milwaukee, WI, 1996).
2) Crandall, R. and Pomerance, C.: *Prime numbers*, 2nd edition, Springer, New York (2005). A computational perspective.
3) FFTW: The Fastest Fourier Transform in the West. http://www.fftw.org/
4) Frigo, M. and Johnson, S.G.: The Fastest Fourier Transform in the West, Technical ReportMIT-LCS-TR-728, Massachusetts Institute of Technology (1997).
5) GMP: the GNU MP library. http://gmplib.org/
6) Granville, A.: On the size of the first factor of the class number of a cyclotomic field, *Invent. Math.*, Vol.100, No.2, pp.321–338 (1990).
7) Hurrelbrink, J.: Class numbers, units and K_2, *Algebraic K-theory: Connections with geometry and topology*, Louise, A.B.L. (Ed.) (1987). NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Vol.279, Kluwer Acad. Pub., Dordrecht, pp.87–102 (1989).
8) Ireland, K. and Rosen, M.: A classical introduction to modern number theory, *Graduate Texts in Mathematics 2nd edition*, Vol.84, Springer-Verlag, New York, (1990).
9) Karatsuba, A.: Multiplication of multidigit numbers on automata, *Doklady Akad. Nauk SSSR*, Vol.145, pp.293–294 (1962).
10) Knuth, D.E.: The Art of Computer Programming Vol.2, 3rd edition, Seminumerical Algorithms, Vol.3, ASCII, 有沢　誠，和田英一（監訳），斎藤博昭ほか（訳）(2004).
11) Kummer, E.E.: Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ ten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben, *J. Reine Angew. Math.*, Vol.40, pp.43–116 (1850).
12) Kummer, E.E.: Mémoire sur la théorie des nombres complexes composées de racines de l'unité et de nombres entiers, *J. Math. Pure et Appliquees*, Vol.XVI, pp.377–498 (1851).
13) Kummer, E.E.: Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^{\lambda} = 1$ gebildeten complexen Zahlen und über den zweiten Faktor der Klassenzahl, *Monatsber. K. Akad. Wiss. Berlin*, pp.855–880 (1870).
14) Lehmer, D.H.: Prime factors of cyclotomic class numbers, *Math. Comp.*, Vol.31, No.138, pp.599–607 (1977).
15) Lepistö, T.: On the growth of the first factor of the class number of the prime cyclotomic field, *Ann. Acad. Sci. Fenn. Ser. A I*, No.577, p.21 (1974).
16) Ribenboim, P.（著），吾郷孝視（訳編）：素数の世界，第 2 版，共立出版 (2001).
17) Shokrollahi, M.A.: Relative class number of imaginary abelian fields of prime conductor below 10000, *Math. Comp.*, Vol.68, No.228, pp.1717–1728 (1999).
18) Stevenhagen, P.: Class number parity for the pth cyclotomic field, *Math. Comp.*, Vol.63, No.208, pp.773–784 (1994).
19) Taylor, R. and Wiles, A.: Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* (*2*), Vol.141, No.3, pp.553–572 (1995).
20) Washington, L.C.: *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, 2nd edition, Vol.83, Springer-Verlag, New York (1997).
21) Wiles, A.: Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (*2*), Vol.141, No.3, pp.443–551 (1995).
22) Yamamura, K. ftp://tnt.math.metro-u.ac.jp/pub/CDROM/rcn/
23) 高木貞治：初等整数論講義，第 2 版，共立出版 (1971).
24) 高木貞治：代数的整数論，第 2 版，岩波書店 (1971).
25) 佐川雅彦，貴家仁志：高速フーリエ変換とその応用，昭晃堂 (1992).
26) 山本芳彦：数論入門，岩波書店 (2003).
27) 藤崎源二郎：代数的整数論入門（上・下），裳華房 (1975).

(平成 20 年 10 月 27 日受付)
(平成 21 年 5 月 13 日採録)

谷口哲也（正会員）

昭和 50 年生．平成 11 年東京理科大学理工学部数学科卒業．平成 13 年同大学大学院理工学研究科修士課程修了．平成 19 年同大学院理工学研究科博士課程単位取得満期退学．博士（理学）．東京理科大学，日本工業大学，千葉県立野田看護専門学校，船橋情報ビジネス専門学校非常勤講師．代数的整数論および整数論的不変量の高速計算に関する研究に従事．日本応用数理学会会員．