1.

コンピュータ上での数学・数論

木村 巌（富山大学）

1.1　イントロダクション

本稿の目的は，サマースクールのテーマである計算機数論についてのより広い観点からの俯瞰を与えることにある．特に，サマースクールでは主題を楕円曲線とモジュラー形式に限ったため触れる機会のなかった，代数体の数論と計算機数論の関わりにより重点を置く．

1.2　数学的な対象のコンピュータ上での表現

現在広く持ちいられているコンピュータでは，情報は電荷の有無の 1bit の情報を連ねた形で表現される．CPU で直接サポートされるのは，

- 整数（32bit/64bit）の加減乗算
- 浮動小数点小数（32bit/64bit）の四則と初等関数

程度である[*1]．

それ以上のデータを表現したい時には，上記のデータを連ねた形で表現し，また演算もプログラムの形で定義しなければならない．例えば，

- 多倍長整数（整数の B 進表記），加減乗算は B 進表記の演算
- 多倍長有理数（多倍長整数の組として表す），加減乗算は分数の演算として

[*1] 最近の CPU は，動画や音声データの再生支援のため，また暗号計算の支援のために，より広いビット幅のデータに対する，並列計算のための機能を備えている（Intel の SSE や AVX など）．ここではこれ以上触れない．

- 多倍長の浮動点小数

こういった対象の初等関数，さらにはより複雑な関数がプログラムとして実現されている．（多倍長整数の乗算に関しては，FFT（高速 Fourier 変換を用いた巧妙な方法が用いられることがある．Crandall-Pomerance [CP 和 10] 参照)).

整数から有理数を構成する操作は，整域の分数体の構成として抽象化されるが，これはプログラミングでも同様である．結局，環の元の対に適切な同一視と演算を入れることにほかならない．多倍長整数が実現できれば，そこから多倍長の有理数が実現できる．

あるいは，環から多項式環を構成することも同様である．元の並び（配列）に，それが多項式の係数であるように演算を定義すれば，多項式環の構成がコンピュータの上で再現できる．したがって，有理数係数の多項式環を実現できる．

より抽象的な対象については，非自明な数学的議論によって，その対象を有限の情報で表現できるように規定しなければならない．例えば，有限（生成）Abel 群をコンピュータの上で実現したければ，その Smith Normal Form を行列として表す．準同型写像 $f\colon G \to G'$ は，生成元の像 $f(g_i)$ を G' の生成元で表示した係数として，やはり行列で表される（例えば木田 [木 07] 参照).

代数体をコンピュータ上で表すことも容易である．有理数体上の 1 変数多項式環の，既約元が生成するイデアルによる剰余環として実現できる．ここから，整数底や判別式，整数環のイデアル（2 元表示，整数底による表示），イデアル類群や類数，単数群を計算することも可能である．イデアル類群は生成元（イデアル類）と関係式（SNF）とで与えられる．（イデアル類群，単数群の計算アルゴリズムとしては，汎用のものとして Buchmann の subexponential アルゴリズムがある．Cohen [Coh93, Chap. 6], Pohst-Zassenhaus [PZ89] を参照されたい．また最近の進展については Biasse and Fieker [BF13] がある．Cohen 上掲書のアルゴリズムはほとんどが pari/gp [PAR17] に実装されている．）

注意 1.2.1. 代数体 K のイデアル類群を計算するにあたっては，「K に対して定まる正の実数 $B(K)$ があり，各イデアル類にはノルムが $B(K)$ 以下のものが存在する」という結果が重要である．例えば，$B(K)$ として Minkowski 定数 $M(K) = \sqrt{|D_K|}(4/\pi)^{r_2}(n!/n^n)$, D_K は K の判別式，r_2 は虚素点の個数，n は K の $\mathbb{Q}$ 上の次数 $[K\colon \mathbb{Q}]$ である．$M(K)$ は往々にして巨大すぎるが，GRH を仮定すれば Bach の定数 $12(\log|D_K|)^2$ といったより低い上限が取れる（E. Bach [Bac90]).

計算数論パッケージ（Pari/gp, Sagemath, Magma ほか）を用いて代数体の

イデアル類群などを計算する際には，何らかの仮定をおいて計算した結果ではないか意識して確認することが重要である．

Pari/gp では GRH を仮定した計算がデフォルト（特に設定を変更しない場合）の挙動である．Pari/gp の計算結果から GRH を取り除くには，`bnrcertify()` という組み込み関数を用いる．Sagemath は GRH ほか，証明されていない結果を一切仮定しないのがデフォルトである．

例 1.2.2. 比較的複雑な対象がコンピュータ上でどのように実現されているかの例として，イデアルを考えてみよう．

Pari/gp でのイデアルは，次のように表現されている．有限次代数体 K の整数環 O_K のイデアルを考える：

単項イデアル　代数的整数として整数底についての表示．

素イデアル $\mathfrak{p}$　$[p, a, e, f, m]$, p は $(p) = \mathfrak{p} \cap \mathbb{Z}$ なる素数，a は $\mathfrak{p}$ の 2 元表示 $\mathfrak{p} = pO_K + aO_K$ となる整数 $a \in O_K$, e は分岐指数，f は相対次数，m は $\mathfrak{p}^{-1} = O_K + \frac{m}{p}O_K$ となる m.

Pari/gp には，こういった量を求める関数が用意されている．

例 1.2.3. Pari/gp での有限 Abel 群は次のように表される：$[h, d]$ もしくは $[h, d, g]$ が群そのもので，h は群の位数，$d = [d_1, \ldots, d_n]$ は $d_{i+1} \mid d_i$ となる因子，$d_1 d_2 \ldots d_n = h$.

指標

$$\chi \colon G = \oplus_{j=1}^{n} (\mathbb{Z}/d_j\mathbb{Z}) g_j \to \mathbb{C}^\times$$

は整数の列 $[a_1, a_2, \ldots, a_n]$ で，

$$\chi\left(\prod_j g_j^{n_j}\right) = \exp\left(2\pi\sqrt{-1}\sum_j \frac{a_j n_j}{d_j}\right)$$

となるもので表される．

1.3 類体論

コンピュータ上に実装された数論の例として，類体論を取り上げる．主な参考文献は H. Cohen [Coh00] である．

有限次代数体 K, その ray $\mathfrak{m}$, ray class group $\mathrm{Cl}_m(K)$ に対して，法 $\mathfrak{m}$ の類体を $K(\mathfrak{m})$ と書くことにする．これは K 上の $\mathfrak{m}$ の外不分岐な Abel 拡大で，相互写像（ここでは $\mathrm{Art}(\cdot)$ と書く）により次の同型がある：

$$\mathrm{Cl}_{\mathfrak{m}}(K) \overset{\mathrm{Art}(\cdot)}{\cong} \mathrm{Gal}(K(\mathfrak{m})/K).$$

K の ray $\mathfrak{m}$ に対して，$K(\mathfrak{m})$ の K 上の，また $\mathbb{Q}$ 上の定義多項式を求める手続きが，Pari/gp には実装されている．類体の構成は，高木の存在定理の証明をたどることでなされ，

- 円分拡大（1 の冪根の付加）
- Kummer 拡大
- descent（降下，つまり Galois 群による固定体をとる操作）

を逐一実装している．

一方，特別な場合の類体は，解析関数の特殊値を付加することで得られることは古典的に知られている．$\mathbb{Q}$ の類体は指数関数の特殊値によって，また，虚 2 次体の類体は，モジュラー関数の特殊値によって生成される．また，証明はされていないが，実 2 次体の場合は，Stark 予想がある．

解析関数の値は，複素数として近似計算することになるが，そこから

- 定義多項式の候補を構成する
- その候補となる多項式から得られる拡大体 $K(\mathfrak{m})'$ が，$K(\mathfrak{m})$ であることを示す
  - 候補となる多項式から得られる $K(\mathfrak{m})'$ が K の Abel 拡大であり
  - Galois 群が ray class group と同型：$\mathrm{Gal}(K(\mathfrak{m})'/K) \cong \mathrm{Cl}_{\mathfrak{m}}(K)$
  - $K(\mathfrak{m})'/K$ は $\mathfrak{m}$ の外不分岐
  - 類体論の一意性定理

という議論を経て，類体の定義多項式を得ることができる．数値計算はあくまで解の候補を得るために行われるため，（Stark 予想を用いた実 2 次体の類体計算の場合も含めて）結果の正当性は担保される．

注意 1.3.1. 上の議論は，今回のサマースクールの主題の一つのである，「法 l-Galois 表現の計算」（Edixhoven-Couveignes ら）でも同様に用いられる．候補の構成を $\mathbb{C}$ 上の近似計算により行い，それが所望のものであることを，Serre 予想によって保証する（理論の概要については，本報告集の横山氏の論説 [横 18] を参照）．この場合では，計算量を評価するための「高さの評価」が議論を著しく複雑にする（Arakerov 幾何を援用する．内田氏の論説 [内 18] 参照）．類体論の場合に，計算量の評価が明示的に行われているか，筆者は知らない．

1.4 類体論の計算の例

簡単のため，K が虚 2 次体 $K = \mathbb{Q}(\sqrt{D})$, $D < 0$ で ray が自明な場合，つまり $\mathfrak{m} = (1)$ で $K(\mathfrak{m}) = K(1)$ が Hilbert 類体の場合を考える．（この節の記述は Cohen 上掲書 Chap. 6.3 に依る）．

古典的によく知られているのは，j 関数を使った

$$K(1) = K(j(O_k))$$

という関係であろう．しかし，この関係式を素朴に使って計算すると，得られる多項式の係数が増大しがちであるという観察がある．

例 1.4.1. Pari/gp で具体例を計算してみよう．まず，デフォルトの精度（十進で 28 桁）で $j(\frac{-1+\sqrt{-23}}{2})$ を計算する．Pari/gp では，`ellj()` が j 関数である．そして，その値の $\mathbb{Q}$ 上の代数関係式を推測する関数 `algdep()` にその値を渡す．しかし，推測された多項式の判別式（`poldisc()` で計算できる）の素因数分解（`factor()` で素因数分解ができる）をみても 23 があらわれておらず，計算は上手くいってないように見える（以下，クエスチョンマークは Pari/gp のプロンプトである）．

```
?\p
   realprecision = 28 significant digits
? j=ellj((-1+sqrt(-23))/2);
-3493225.699969933368205504739
? pol=algdep(j, 3);
? print(pol);
675*x^3 + 2357936127*x^2 + 30668842140*x - 13231708022
? f=factor(poldisc(pol));
? print(f);
[2, 2; 3, 7; 241, 1; 23321, 1; 120472360578334144019173565093, 1]
```

精度を 57 桁に挙げて計算し直してみると，代数関係式の判別式の素因数に 23 があらわれている．Pari/gp には，虚 2 次体の Hilbert 類体の定義多項式を計算する `quadhilbert()` という関数がある．答合わせとしてこの関数を使い，j 関数の値から求めた多項式，`quadhilbert()` で求めた多項式，それぞれが定義する代数体をもとめ（`bnfinit()`），それらの間に同型が存在するかを計算する（`nfisisom()`）．結果としてそれらの間には確かに同型が存在することが分かる．

```
?\p53
```

```
   realprecision = 57 significant digits (53 digits displayed)
? j=ellj((-1+sqrt(-23))/2);
? print(j)
-3493225.69996993336820550473854732970339618417972561 17
? pol=algdep(j, 3);
? print(pol);
x^3 + 3491750*x^2 - 5151296875*x + 12771880859375
? f=factor(poldisc(pol));
? print(f);
[-1, 1; 5, 18; 7, 12; 11, 4; 17, 2; 19, 2; 23, 1]
nfj = bnfinit(pol);
nfh = bnfinit(quadhilbert(-23));
print(nfisisom(nfj, nfh));
[-1084125*x^2 + 1904875*x - 1437500]
```

判別式 -23 の虚 2 次体の類数は 3 で，この場合の Hilbert 類体は 3 次多項式で定まる．絶対値のより大きい虚 2 次体では，更に精度を高く取らねばならないことが推測される．

そのため，実際の計算は Scherz のアルゴリズムを用いることが多い．

f をレベル 1, 重さ k のモジュラー形式とする（モジュラー形式については 6 章も参照のこと）．$\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ を K の整イデアル，$\omega_1/\omega_2 \in H$ とする（H は上半平面）．

$$f(\mathfrak{a}) = \left(\frac{2\pi\sqrt{-1}}{\omega_2}\right) f\left(\frac{\omega_1}{\omega_2}\right),$$

とすると，$\mathfrak{a}$ の底のとり方によらず，K のイデアル類の関数となる．

η 関数を導入する（$\tau \in H$, $q = \exp(2\pi\sqrt{-1}\tau)$）：

$$\begin{aligned}\eta(\tau) &= \exp\left(\frac{2\pi\sqrt{-1}}{24}\right)\prod_1^\infty(1-q^n)\\ &= q^{\frac{1}{24}}\left(1+\sum_1^\infty(-1)^n\left(q^{\frac{n(3n-1)}{2}}+q^{\frac{n(3n+2)}{2}}\right)\right).\end{aligned}$$

η は重さ $1/2$ のモジュラー形式である．適切な”multiplier system” v_η によって，

$$\eta(\gamma\tau) = v_\eta(\gamma)(c\tau+d)^{1/2}\eta(\tau), \quad \gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

このとき，$g_{p,q}(\tau)$ を次で定義する：

$$g_{p,q}(\tau) \coloneqq \frac{\eta(\tau/p)\eta(\tau/q)}{\eta(\tau/(pq))\eta(\tau)}.$$

$g_{p,q}(\tau)$ は

$$\Gamma^0(pq) \coloneqq \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; b \equiv 0 \pmod{pq} \right\}$$

に関する，適切な"multiplier system" v_g に対するモジュラー関数になる：

$$g_{p,q}(\gamma\tau) = v_g(\gamma) g_{p,q}(\tau), \quad \tau \in \Gamma^0(pq).$$

特に，整数 e が $24 \mid e(p-1)(q-1)$ を満たすなら，$g_{p,q}^e(\tau)$ は $\Gamma^0(pq)$ で不変になる．

定理 1.4.2. 整数 p, q, e のとり方に関する適切な仮定のもとで，$6pq$ と互いに素な $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_1/\omega_2 \in H$ に対して

$$g_{p,q,e}(\mathfrak{a}) \coloneqq g_{p,q}\left(\frac{\omega_1}{\omega_2}\right)^e$$

が well-defined．また，次の相互法則も成立する（$[c]$ は K の整イデアル c が代表するイデアル類，$\mathrm{Art}(\cdot)$ は相互写像）：

$$g_{p,q,e}(\mathfrak{a})^{\mathrm{Art}(\mathfrak{c})} = g_{p,q,e}(\mathfrak{a}\mathfrak{c}^{-1}).$$

定理 1.4.3 ([Coh00, Thm. 6.3.7])．定理 1.4.2 と同様の仮定のもとで，次の多項式

$$P_{p,q,e}(X) \coloneqq \prod_{[\mathfrak{a}] \in \mathrm{Cl}(K)} (X - g_{p,q,e}(\mathfrak{a})) \in \mathbb{Z}[X],$$

は K 上（また $\mathbb{Z}$ 上）既約で，その根の一つを K に添加した体が $K(1)$ に等しい．また，$P_{p,q,e}(X)$ の定数項は ± 1.

例 1.4.4. 例 1.4.1 と同様に，j 関数の値を計算して代数的な関係式を導くという方法で，虚 2 次体 $K = \mathbb{Q}(\sqrt{-199})$ の Hilbert 類体の定義多項式を計算できるか試してみよう．この K のイデアル類群は位数が 9 の巡回群である．

精度を挙げつつ計算すると，十進 832 桁の精度で

$$\begin{aligned}
&x^9 + 176561902797709386 60x^8 + 133130310018925681683743 4x^7 \\
&+ 311741055246397228842310784103371345424x^6 \\
&+ 239692998051174373263593885151882059812437 87x^5 \\
&+ 934682848803434155897358662478037099871861466271x^4 \\
&- 153618310508758956806228374670246699075188773087487 38x^3 \\
&+ 813115042133415857106312610566896644913264959146819654 78x^2 \\
&- 262648565634938630871054990973171108239996044803712751064 59x \\
&+ 607371299984970035446600042234842179599025402360813878527947 1
\end{aligned}$$

が得られる．この多項式の判別式は 199^4 で割り切れる（多項式の判別式が 199 で割れるまで精度を上げた）．

一方，上述の Scherz のアルゴリズムの実装である `quadhilbert()` を使うと，

$$x^9 + x^8 + 2x^7 + 8x^6 + 12x^5 + 5x^4 - x^3 - x^2 - x + 1$$

という小さな係数からなる多項式が得られる．

この二つの多項式は同じ代数体（K の Hilbert 類体）を与えることが，先の例と同じ方法で確認できる．

参考文献

[Bac90] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR 1023756

[BF13] Jean-François Biasse and Claus Fieker, *Improved techniques for computing the ideal class group and a system of fundamental units in number fields*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 113–133. MR 3207410

[Coh93] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[Coh00] ———, *Advanced Topics in Computational Number Theory*, Springer-Verlag, New York, 2000. MR 1 728 313

[CP 和 10] Richard E. Crandall, Carl Pomerance 著，和田秀男 監訳，素数全書：計算からのアプローチ, 朝倉書店, 2010.

[PAR17] PARI Group, Bordeaux, *PARI/GP, Version 2.9.4*, 2017, available from `http://pari.math.u-bordeaux.fr/`.

[PZ89] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1989. MR 1033013

[横 18] 横山俊一, 特別な楕円モジュラー形式の高速計算理論について, in 木村巌，横山俊一 [木横 18].

[内 18] 内田幸寛, 高さと *Arakelov* 理論，それらの *Galois* 表現の計算への応用, in 木村巌，横山俊一 [木横 18].

[木 07] 木田雅成, 数理・情報系のための整数論講義, 臨時別冊・数理科学, SGC ライブラリ; 58, サイエンス社, 2007.

[木横 18] 木村巌，横山俊一 (eds.), 第 *25* 回整数論サマースクール報告集「楕円曲線とモジュラー形式の計算」, 2018.