数理解析研究所講究録
1038巻 1998年 183-189

p進近似を利用した代数的数の取り扱い

NTT CS研 関川 浩 (Hiroshi Sekigawa) [1)]

1. はじめに

本稿では，p進近似を利用した代数的数の取り扱いについて述べる．

最初に，復習の意味で，p進近似を利用した有理数の取り扱いの例を挙げる．

例 1 *([2], pp. 141–142)* 以下の $A(x)$, $B(x)$ に対し，$\gcd(A(x), B(x))$ を求めよ．

$$A(x) = x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5,$$
$$B(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21.$$

各係数を mod 5で見て，$\mathbf{Z}/5\mathbf{Z}$ 上の多項式として計算を行う．ただし，$\mathrm{remainder}(f, g)$ は，多項式 f を多項式 g で割った余りを表す．

$$A_5(x) = x^8 + x^6 + 2x^4 + 2x^3 + x^2 + 2x,$$
$$B_5(x) = 3x^6 + x^2 + x + 1,$$
$$C_5(x) = \mathrm{remainder}(A_5(x), B_5(x)) = 2x^2 + 3,$$
$$D_5(x) = \mathrm{remainder}(B_5(x), C_5(x)) = x,$$
$$E_5(x) = \mathrm{remainder}(C_5(x), D_5(x)) = 3.$$

Gaussの補題より，$\gcd(A(x), B(x)) = G(x) \in \mathbf{Z}[x]$ をモニックに取ることができ，$A(x) = P(x)G(x)$, $B(x) = Q(x)G(x)$, ただし，$P, Q \in \mathbf{Z}[x]$ と書ける．G, P, Q を mod 5で見た多項式を G_5, P_5, Q_5 と書くと，$A_5(x) = P_5(x)G_5(x)$, $B_5(x) = Q_5(x)G_5(x)$ となる．すなわち，G_5 は $\gcd(A_5, B_5)$ を割り切る．ところが，$\gcd(A_5, B_5) = 1$ なので，Gがモニックであることに注意して，$G = 1$ となる．

この例を有理数のままで計算すると，A, Bが互いに素であることを示す最後の余りが，

$$\frac{17722579277662042}{7972349896225}$$

となり，係数膨張が起きていることがわかる．

以下，代数的数に対してもp進近似を利用した取り扱いが可能であること，とくに，どのような性質を満たす素数pを取ればよいか，そのような素数pはどれくらいあって，どうやって探すか，について述べる．

[1)] E-mail: sekigawa@cslab.kecl.ntt.co.jp

なお，p進近似とは，代数的整数論の言葉でいえば，以下のようになる．代数体Kが与えられたとせよ．まず，素数pと素イデアル$\mathfrak{p}$を，pが生成するKの整数環の単項イデアルを$\mathfrak{p}$が割り切り，かつ，$\mathfrak{p}$進付値によるKの完備化がp進体$\mathbf{Q}_p$と同型であるように選ぶ（一般には，$\mathbf{Q}_p$と同型ではなく，$\mathbf{Q}_p$の拡大体となる）．次に，うまく選んだ$p, \mathfrak{p}$を用いて，Kでの計算を$\mathbf{Q}_p$（あるいは，その整数環であるp進整数環$\mathbf{Z}_p$）で，$\bmod p^e$による近似を用いて行う，ということである．p進体，完備化，素イデアルと付値との対応などついては，たとえば，[4], [7]を参照されたい．

2. p進近似を利用した代数的数の取り扱い

まず最初に，簡単な例を示す．

例 2 αを$x^2-2=0$の根とする．以下の$A(x)$, $B(x)$に対し，$\gcd(A(x), B(x))$を求めよ．

$$A(x) = x^3 + \alpha x^2 + x + 1,$$
$$B(x) = 3x^2 + 2\alpha x + 2.$$

$3^2 - 2 \equiv 0 \pmod 7$なので，$\alpha \mapsto 3 \bmod 7$として$\mathbf{Z}/7\mathbf{Z}$で計算する．

$$A_7(x) = x^3 + 3x^2 + x + 1,$$
$$B_7(x) = 3x^2 + 6x + 2,$$
$$C_7(x) = \mathrm{remainder}(A_7(x), B_7(x)) = 3x + 5,$$
$$D_7(x) = \mathrm{remainder}(B_7(x), C_7(x)) = 5.$$

$\mathbf{Q}(\sqrt{2})$の整数環$\mathbf{Z}[\sqrt{2}]$はUFDなので，例1と同様な議論で$\gcd(A(x), B(x)) = 1$である（だだし，一般には，代数体の整数環はUFDとは限らないので，注意が必要である）．

必要なら，$\alpha \mapsto a \bmod 7^e$の$e$を大きくする（近似精度を上げる）ことも可能である．

$$\alpha \mapsto 10 \bmod 7^2 \ (10^2 \equiv 2 \pmod{7^2},\ 10 \equiv 3 \pmod 7),$$
$$\alpha \mapsto 108 \bmod 7^3 \ (108^2 \equiv 2 \pmod{7^3},\ 108 \equiv 10 \pmod{7^2}),$$
$$\alpha \mapsto 2166 \bmod 7^4 \ (2166^2 \equiv 2 \pmod{7^4},\ 2166 \equiv 108 \pmod{7^3}),$$
$$\vdots$$

合同式の解の持ち上げに関しては，[8]を参照のこと．

p進近似でできることを，いくつか挙げておく．

- 非ゼロ判定．あるeで$\alpha \mapsto a \not\equiv 0 \pmod{p^e}$ならば$\alpha \neq 0$である．
- ゼロ判定．近似的にゼロになった場合，すなわち，あるeで$\alpha \mapsto a \equiv 0 \pmod{p^e}$になった場合，Mahler measureを援用することにより，αが真にゼロであるか否かの判定が可能である[6]（ただし，[6]で定義した，拡張されたMahler measureは，通常のMahler measureに一致する）．αを代数的数，$M(\alpha)$をαのMahler measureとする．このとき，以下が成り立つ．

$$\alpha \mapsto a \equiv 0 \pmod{p^e} \text{ かつ } M(\alpha) < p^e \Longrightarrow \alpha = 0$$

とくに，$\alpha \in \mathbf{Z}$の場合，$M(\alpha) = |\alpha|$なので，上の主張は以下の通りとなる．

$$\alpha \equiv 0 \pmod{p^e} \text{ かつ } |\alpha| < p^e \Longrightarrow \alpha = 0$$

- 適当な付加情報の下で，p進近似から元の値の復元（[1]など）．
- gcdの計算（[9]など）．
- 因数分解（[5]など）．

3. p進近似のpの取り方

3.1. 理論的な準備

$f(x) \in \mathbf{Z}[x]$を，$\mathbf{Q}$上既約かつ$\deg(f) \geq 2$とし，αを$f(x) = 0$の根としよう．αを$\bmod p^e$で近似するとは，$\mathbf{Z}[\alpha] \to \mathbf{Z}/p^e\mathbf{Z}$なる準同型を構成することである．この構成は，まず，$\mathbf{Z}[\alpha] \to \mathbf{Z}/p\mathbf{Z}$なる準同型を構成し，次に，$p$の巾を上げる，という手順による．今，$\mathbf{Z}[\alpha] \to \mathbf{Z}/p\mathbf{Z}$による$\alpha$の像が$a \bmod p$であるとしよう．このとき，$f(a) \equiv 0 \pmod{p}$となること，すなわち，$f \bmod p$が一次因子$x - a$を持つことが必要である．

以下に示すように，$f \bmod p$が一次因子を持つ素数pは無限に存在する．この事実のよりどころとなるFrobeniusの定理を述べるために，cycle patternとdecomposition typeの定義をしておく．

定義 1 (cycle pattern) Gをn次対称群の部分群とする．Gの元σを，$\sigma = \sigma_1\sigma_2 \ldots \sigma_t$, ただし，$\sigma_i$は長さが$l_i$の巡回置換，$1 \leq l_1 \leq \cdots \leq l_t$, $l_1 + \cdots + l_t = n$, と書いたとき，σの*cycle pattern*は$l_1, l_2, \ldots, l_t$である，と定義する．

定義 2 (decomposition type) $f \in \mathbf{Z}[x]$をモニックかつ，判別式が0ではない，とする．fの判別式を割らない素数pに対して，fを$\bmod p$で因数分解した結果が，

$$f \equiv f_1 f_2 \ldots f_t \pmod{p}, \qquad \deg(f_i \bmod p) = d_i, \qquad d_1 \leq d_2 \leq \cdots \leq d_t,$$

ただし，$f_i \bmod p$は$\mathbf{Z}/p\mathbf{Z}[x]$で既約，となったとする．このとき，$f \bmod p$の*decomposition type*は$d_1, d_2, \ldots, d_t$である，と定義する．

以上の準備によって，Frobeniusの定理を述べることができる．

定理 1 (Frobeniusの定理) *[3]* $f \in \mathbf{Z}[x]$がモニックかつ，判別式が0ではない，とし，fの*Galois*群をGとする．Gは，$f = 0$の根$\alpha_1, \ldots, \alpha_n$の置換群なので，$n$次対称群の部分群と見なせる．$G$の元で*cycle pattern*が$n_1, n_2, \ldots, n_t$なるものが存在するならば，$f \bmod p$の*decomposition type*が$n_1, n_2, \ldots, n_t$となる素数$p$は無限に存在する．

この定理から，以下が成り立つことがわかる．

系 1 定数ではない$f \in \mathbf{Z}[x]$に対し，$f \bmod p$が一次因子を持つ素数pは無限に存在する．

証明 fが$\mathbf{Z}$上既約の場合に証明すれば十分である．

fがモニックの場合，定理1より，$f \bmod p$が完全に一次式の積に分解する素数pだけでも無限にあることがわかる（単位元のcycle patternは$1, 1, \ldots, 1$だから）．

fがモニックではない場合，fの主係数をc, 次数をnとする．$p|c$なる素数pは有限個であることに注意して，$c^{n-1}f(x/c)$を考えることにより，モニックの場合に帰着する． ■

注意 1 以下の例*3*に示すように，特別な場合は，*Dirichlet*の算術級数定理：

> $m \geq 1$を整数とする．このとき，$(a, m) = 1$となる整数aに対し，$p \equiv a \pmod{m}$となる素数は無限に存在する．

によっても示すことができる．

なお，上記の*Frobenius*の定理と*Dirichlet*の定理は簡略版であり，実際は，無限の程度（密度）まで述べている．*Dirichlet*の定理と*Frobenius*の定理の関係や，その*"least common generalization"*である*Chebotarev*の密度定理に関しては*[10]*を参照のこと．

例 3 $f(x) = x^2 - 2$とする．このとき，平方剰余の相互法則（の第二補充法則）から以下が成り立つ．

$$f \bmod p\text{が一次因子を持つ} \Longleftrightarrow p = 2\text{あるいは}\ p \equiv 1, 7 \pmod{8}$$

したがって，*Dirichlet*の定理より，$f \bmod p$が一次因子を持つ素数pは無限に存在する．

以上の準備の下，まず，現れる代数的数が，すべてある一つの代数的数αの$\mathbf{Q}$係数多項式で表されている場合，すなわち，単純拡大$\mathbf{Q}(\alpha)$の形で代数体が与えられた場合を考える．$f \in \mathbf{Z}[x]$ $(\deg(f) \geq 2)$を，αの最小多項式とする．$f \bmod p$が一次因子を持つ素数pのうち，以下の条件1のをすべての項目を満たすものをp進近似に用いることができる．

条件 1

1. $\deg(f \bmod p) = \deg(f)$.
2. $f \equiv 0 \pmod{p}$が重根を持たない．
3. $f \bmod p$は，$x - a$ $(a \neq 0)$なる一次因子を持つ．

条件を説明する．一番目の条件は結局，fの主係数を割る素数は避ける，ということである．二番目の条件が満たされているとき，$f(a) \equiv 0 \pmod{p}$であれば，すべての自然数eに対して，$f(x) \equiv 0 \pmod{p^e}$かつ$x \equiv a \pmod{p}$に解が存在する（たとえば，[8]を参照のこと）．すなわち，近似精度をいくらでも上げることができることを保証する．三番目の条件は，0ではない数の近似値が0になって欲しくない，ということである．

定理 2 fは上記の通りとする．$f \bmod p$が一次因子を持つ素数p（系*1*より無限に存在する）は，有限個の例外を除いて条件*1*の三項目をすべて満たす．

証明 $f \bmod p$が一次因子を持つ素数pのうち，項目1を満たさないものは，fの主係数を割り切る素数だから，有限個．

項目2を満たさない素数は，fの判別式を割り切るものだから有限個．

xが$f \bmod p$の一次因子となる素数pは，fの定数項を割り切るものだから有限個． ■

以下，現れる代数的数が複数の代数的数 $\alpha_1, \ldots, \alpha_m$ の $\mathbf{Q}$ 係数多項式として表されている場合，すなわち，逐次拡大の形で代数体が与えられた場合を扱う．$K_0 = \mathbf{Q}$, $K_i = K_{i-1}(\alpha_i)$, $(i = 1, \ldots, m)$ とし，$f_i(x) \in \mathbf{Z}[\alpha_1, \ldots, \alpha_{i-1}][x]$ を，K_{i-1} 上の α_i の最小多項式とする．K_m は単純拡大としても書けるが，実用上は，逐次拡大のまま扱う方がよい場合がある．

$\alpha_i \mapsto a_i \bmod p$ と近似できるための条件を考えよう．今，$a_1, \ldots, a_m$ を整数とし，$\tilde{f}_i$ を，f_i の係数に現れる α_j 達を a_j 達に置き換えたもの，とする．以下の条件 2 のすべての項目を満たすものを p 進近似に用いることができる．

条件 2

1. $\deg(\tilde{f}_i \bmod p) = \deg(f)$.
2. $\tilde{f}_i \equiv 0 \pmod p$ が重根をもたない．
3. $a_i \not\equiv 0 \pmod p$, $\quad 1 \le i \le m$.
4. $a_i \not\equiv a_j \pmod p$, $\quad 1 \le i < j \le m$.

新たに増えた最後の項目は，α_i 達が $\bmod p$ で異なる近似値を持つことを要請するものである．このとき，以下の定理が成り立つ．

定理 3

1. 以下の条件を満たす素数 p は無限に存在する．

   ある整数 $a_1, \ldots, a_m$ が存在して，$\tilde{f}_1(a_1) \equiv \cdots \equiv \tilde{f}_m(a_m) \equiv 0 \pmod p$.
2. 上記の素数は，有限個の例外を除いて条件 2 のすべての項目を満たす．

証明のために，まず，以下の補題を準備しておく．

補題 1 $f, g \in \mathbf{Z}[x]$, $(f, g) = 1$, かつ，f は定数ではないとする．このとき，「ある整数 a が存在して，$p|f(a)$ かつ $p \not| g(a)$」となる素数 p は無限に存在し，「ある整数 a が存在して，$p|f(a)$ かつ $p|g(a)$」となる素数 p は有限個である．

証明 系 1 より，$p|f(a)$ なる素数 p は無限に存在する．$(f, g) = 1$ より，適当な $A, B \in \mathbf{Z}[x]$ をとると，$Af + Bg = c \in \mathbf{Z}$ となる．したがって，$p|f(a)$ かつ $p|g(a)$ となる素数 p は c の素因数に限られるので有限個． ■

定理 3 の証明 $K = Q(\theta)$ と単純拡大で書き，$g \in \mathbf{Z}[x]$ を θ の $\mathbf{Q}$ 上の最小多項式とする．このとき，$\alpha_i = g_i(\theta)$, ただし，$g_i \in \mathbf{Q}[x]$, $\deg(g_i) < \deg(g)$, と書ける．必要なら θ を適当な整数で割ったものと置き換えることにより，$g_i \in \mathbf{Z}[x]$ と仮定してよい．

系 1 より，「ある整数 a が存在して，$p|g(a)$ となる素数 p」は無限に存在する．g は $\mathbf{Q}$ 上既約であることと，$\deg(g_i) < \deg(g)$ であることに注意すれば，$(g, g_i) = 1$ がわかるので，「ある整数 a が存在して，$p|g(a)$ となる素数 p」のうち，「ある整数 a が存在して，ある i $(1 \le i \le m)$ について $p|g_i(a)$」となる素数 p は有限個である． ■

3.2. 素数 p の取り方

この節では，素数 p の取り方を考察する．単純拡大の場合，正功法として，$f \bmod p$ を因数分解する方法がある．ただし，特別な場合（たとえば，以下の例 4），一次因子の有無を調べるだけならは，因数分解は不必要である．

例 4 a を平方数ではない整数とする．このとき，以下が成り立つ．

$$x^2 - a \bmod p \text{ が一次因子を持つ} \iff \left(\frac{a}{p}\right) = 1$$

ただし，$\left(\frac{a}{p}\right)$ は *Legendre* 記号である．したがって，因数分解は不必要である．

さらに，たとえば，$p \equiv 3 \pmod 4$ かつ $\left(\frac{a}{p}\right) = 1$ のとき，以下の通り，簡単に因数分解できる．

$$x^2 - a \equiv (x - a^{(p+1)/4})(x + a^{(p+1)/4}) \pmod p.$$

単純拡大の場合，先に α の像 $a \bmod p$ を与えて，$f(a)$ を素因数分解する方法もある．ただし，f の次数が大きいときは $|f(a)|$ は巨大となり，効率的とは限らないし，この方法は，逐次拡大には適用できない．

以下，逐次拡大の場合を考える．

定理 3 の証明の手順に沿って，単純拡大に書き直す（すなわち，原始元を求める）方法は，以下の通りとなる．

方法 1 (単純拡大に直してから求める方法)

1. $K_m = \mathbf{Q}(\theta)$ となる θ と，θ の $\mathbf{Q}$ 上の最小多項式 $g(x) \in \mathbf{Z}[x]$ を求める．
2. $\alpha_i = g_i(\theta)$ となる $g_i \in \mathbf{Q}[x]$ $(\deg(g_i) < \deg(g))$ を求める．$g_i \notin \mathbf{Z}[x]$ となる g_i 達の係数の分母の *lcm* を d として，θ を θ/d に置き換えることにより，すべての i に対して $g_i \in \mathbf{Z}[x]$ とする．
3. 素数 p を一つ取る．
4. $g(a) \equiv 0 \pmod p$ となる $a \bmod p$（有限個）に対して，$a_1 = g_1(a), \ldots, a_m = g_m(a)$ として，条件 *2* のすべての項目を満たすものを探す．
5. $(p, a_1, \ldots, a_m)$ がすべての項目を満たせば，それを返す．
   すべての項目を満たすものがなければ，p を取り直して，*4* へ．

ただし，この方法は，事実上，単純拡大に直しているので，拡大次数が大きい場合，実効性に問題がある．したがって，以下に示す通り，逐次拡大のまま扱う方法が考えられる．

方法 2 (逐次拡大のまま扱う方法)

1. 素数 p を一つ取る．
2. $\tilde{f}_1(a_1) \equiv \cdots \equiv \tilde{f}_m(a_m) \equiv 0 \pmod p$ となる $(a_1 \bmod p, \ldots, a_m \bmod p)$（有限個）の中から，条件 *2* のすべての項目を満たすものを探す．
3. $(p, a_1, \ldots, a_m)$ がすべての項目を満たせば，それを返す．
   すべての項目を満たすものがなければ，p を取り直して，*2* へ．

4. 計算例

どれくらいの拡大次数のものが扱えるのか確かめる意味で，以下の二つの例を挙げる．実験は，DEC Alpha Server 4100/5/400 (400MHz) 上の C で書いたプログラムで，逐次拡大のまま扱う方法（方法 2）を使用した．

例 5 $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{47})$ （$\mathbf{Q}$ に 50 以下の素数 15 個の平方根を添加した体）.

拡大次数 $[K : \mathbf{Q}]$ は，$2^{15} = 32768$ である．この場合，因数分解は不必要であり，Legendre 記号の計算ですむ．具体的には，$q = 2, 3, \ldots, 47$ のすべてに対して，$\left(\frac{q}{p}\right) = 1$ となる素数 p を求めることになる．なお，実際には，Legendre 記号は Jacobi 記号と見て計算する．$p = 9257329$ がすべての条件を満たす最小の素数であって，1 秒強で求まった．

例 6 $L = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{97})$ （$\mathbf{Q}$ に 100 以下の素数 25 個の平方根を添加した体）.

拡大次数 $[L : \mathbf{Q}]$ は，$2^{25} \sim 3 \times 10^7$ である．今度は，$q = 2, 3, \ldots, 97$ のすべてに対して，$\left(\frac{q}{p}\right) = 1$ となる素数 p を求めることになる．$p = 7979490791$ がすべての条件を満たす最小の素数であって，20 分弱で求まった．

5. おわりに

逐次拡大の形で与えられた代数体において p 進近似を利用しようとする場合，都合よく計算するために素数 p が満たすべき十分条件を確認し，その条件を満たす p が無限に存在することを示した．さらに，そのような p の求め方を提案した．

今後の課題として，gcd, 因数分解などのアルゴリズムにおいて p 進近似を用いたとき，拡大次数が大きい場合でも実用的な意味で計算可能かどうかを調べることが挙げられる．

参 考 文 献

[1] J. Abbott, Recovery of Algebraic Numbers from their p-adic Approximations, *Proc. ISSAC'89*, pp. 112–120, 1989.

[2] J. H. Davenport, Y. Siret and E. Tournier, *Computer Algebra (2nd ed.)*, Academic Press, 1993.

[3] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitzungsberichte Königl. Preußisch. Akad. Wissenschaft. Berlin*, pp. 689–703, 1896.

[4] 彌永昌吉（編），数論，岩波書店，1969.

[5] A. K. Lenstra, Factoring Polynomials over Algebraic Number Fields, *Proc. EUROCAL'83*, Springer Lec. Notes Comp. Sci. **162**, pp. 245–254, 1983.

[6] 関川 浩，拡張された Mahler の measure による代数的数のゼロ判定，京都大学数理解析研究所講究録 986「数式処理における理論と応用の研究」，pp. 83–91，1997.

[7] J.-P. Serre, *Corps Locaux*, Hermann, 1962.（英訳: *Local Fields*, Springer-Verlag, 1979.）

[8] J.-P. Serre, *Cours d'Arithmétique*, Presses Univ. de France, 1970.（英訳：*A Course in Arithmetic (2nd ed.)*, Springer-Verlag, 1978, 和訳：数論講義，岩波書店，1979.）

[9] T. J. Smedley, A New Modular Algorithm for Computation of Algebraic Number Polynomial Gcds, *Proc. ISSAC'89*, pp. 91–94, 1989.

[10] P. Stevenhagen and H. W. Lenstra, Jr., Chebotarëv and his Density Theorem, *The Mathematical Intelligencer*, Vol. 18, No. 2, pp. 26–37, 1996.