数理解析研究所講究録
第301巻 1977年 1-10

有限体に関するアルゴリズム

慶応大　工学部　高橋秀俊

概観　実数整数論の問題中には，有限体に関係した計算で多項式の既約分解，既約多項式の生成，整係数多項式に関するexactな計算，有限体の楕円関数の計算など，いろいろと興味あるものがたくさんあるように思われる．それらを実行するためには，通常の実数計算で必要ないろいろの数値アルゴリズムに対応した，有限体上のアルゴリズムが必要になる．加減乗の3則は自明だとして，有限体での除算，開方，一般の高次代数方程式の解法などが問題になる．

従来の純粋数学では，有限的なアルゴリズムが見つかれば解法の問題は解決されたと見做す習慣なので，有限体は元の数が有限だから，すべての元について試してみればよいという考えから，方程式の解法はあまり問題にされなかった．しかし体の指標 p が非常に大きいとき（具体的には計算機の1語で扱える上限に近い整数の場合など）には，この〝目の

子"的な方法は実際的でない．そこで，もし適当なアルゴリズムが存在して，問題が p の2を底とした対数またはその有限べきの程度の計算量で解けるならば，そのアルゴリズムは実行可能(feasible)であると定義し，前述のような基本的な問題に対する実行可能なアルゴリズムを考えることにする．

1．除法(逆数)

除算 b/a を行なうには，a の逆数 a^{-1} を求めて $b\cdot a^{-1}$ を計算すればよいから，逆数を求めるアルゴリズムがあればよい．標準的な逆数アルゴリズムは，不定方程式

$$ax+py=1$$

を Euclid 互除法によって解く方法であるが，計算機，特に Fortran のような言語を使う場合には，これを少し変更した次の方法が簡単である．

いま

$$ax\equiv 1 \mod p \qquad (1)$$

を解くために，適当に $y_1, y_2, \cdots$ を選んで，数列 $a_1\equiv ay_1$，$a_2\equiv a_1y_2, \cdots$ $a_k\equiv a_{k-1}y_k, \cdots$ をつくり，$a>a_1>a_2>\cdots$ となるようにして，最終的に $a_n\equiv 1$ となるようにするのである．すると $x\equiv y_1y_2\cdots y_n$ となる．そこで

初期値: $a_0 = a$, $x_0 = 1$

$$\text{ループ} \begin{cases} y_i = [p/a_{i-1}] + 1 \\ a_i = a_{i-1} \cdot y_i - p \\ x_i \equiv x_{i-1} \cdot y_i \mod p \end{cases}$$

$a_n = 1$ で脱出, $x = x_n$

というアルゴリズムになる. これは Euclid 互除法のように変数の順送りがないだけ, プログラムが簡単である.

もう一つの方法は, Fermat の定理によって

$$a^{-1} \equiv a^{p-2} \mod p \qquad (2)$$

であることを利用するのである. a を $p-2$ 回掛けるのでは実行可能でないが, a から a^2, a^4, a^8... と a^{2^m} をつくって, $p-2$ の2進表現の1のビットに相当するものを掛け合わせるという方法によれば, これも実行可能である.

2. 開方

$$x^n \equiv a \mod p \qquad (3)$$

を解く問題を考える. ここで n が素数である場合ができれば十分である. まず n が $p-1$ を割り切らないと仮定する. そのときは (3) の根はきっちり1個ある. 即ち $x^n \equiv 1$ の根は $x = 1$ だけである.

この場合

$$nq \equiv 1 \mod (p-1)$$

によって q を求めると，x は

$$x \equiv a^q \mod p$$

から得られる．

n が $p-1$ を割るときは，こんなに簡単に行かない．その場合は次節にのべる一般方程式の解法を用いるのがよい．

ただ，$n=2$ で $p-1$ が 4 の倍数でないときには，次のように簡単に求まる．

解が存在するように a は法 p の平方剰余であるものとする．すると

$$x \equiv a^{(p+1)/4} \mod p$$

である．証明は簡単なので省略する．

3. 一般の方程式の解法．

n 次方程式

$$f(x) \equiv 0 \mod p \qquad (4)$$

を解くこと，つまり (4) をみたす $GF(p)$ の元を求めることを考える．

いま，$x=\alpha \in GF(p)$ が (4) の根であることと，$x^{p-1}-1$ が $GF(p)$ において $x-\alpha$ で割り切れることとは同等である．そこで，$x=\alpha_1, \alpha_2, \cdots, \alpha_m$ が (4) の根のす

べてであるとすると　$x^{p-1}-1$ は m 次多項式

$$f_1(x) \equiv (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$$

で割り切れる. $f_1(x)$ はもちろん $f(x)$ を割り切るから,

$$f_1(x) \equiv GCM(x^{p-1}-1, f(x))$$

として, Euclid 互除法で求められる.

ここで $x^{p-1}-1$ を直接扱うことは実行可能でないが, a^{p-2} を求めたときと同様にして, まず $m-1$ 次多項式

$$g(x) \equiv x^{p-1} \mod p, f(x)$$

を求めることは $x, x^2, x^4, \cdots, x^{2^k}, \cdots$ を順次求めれば実行可能である. こうしてから $GCM(g(x)-1, f(x))$ を求めるようにすればよい.

問題は, こうして"実根"(GF(p) 中の根) ばかりを持つ $f_1(x)=0$ を解くことに帰着した. これが4次以下の方程式なら, 古典的な"代数的解法"が役立つ. しかし, もっと一般的な方法として, 上と同様にして今度は

$$f_1^+(x) \equiv GCM(x^{(p-1)/2}-1, f_1(x))$$

$$f_1^-(x) \equiv GCM(x^{(p-1)/2}+1, f_1(x))$$

を求める. $f_1(x)$ は $x^{p-1}-1=(x^{(p-1)/2}-1)(x^{(p-1)/2}+1)$ の因子なので, $f_1(x)$ の因子は $f_1^+(x)$ と $f_1^-(x)$ の二つに分配される. いうまでもなく

$$f_1(x) = f_1^+(x) f_1^-(x)$$

ここで $f_1(x) \equiv 0$ の根のうちの，何個がどちらの方に属することになるかは予知できない．しかし多くの場合，$f_1(x)$ はこうして二つの多項式に分解される．時には全部の根が一方にかたまってしまうこともあり得る．

ここまでで1次因子に分かれてしまえばよし，そうでなければ，x の原点をずらせて，再試行する．言いかえれば，$(x+1)^{(p-1)/2} \pm 1$ を用いて $f_1^+(x)$, $f_1^-(x)$ を更に分解する．更に $(x+h)^{(p-1)/2} \pm 1$ $h = 2, 3, 4, \cdots$ と，完全な分解ができるまで続ける．

ここで $f_1(x) = f_1^+(x) f_1^-(x)$ のように分解したのは，実は根 $\alpha_1, \alpha_2, \cdots \alpha_m$ を平方剰余であるものとないものとに分類したことにほかならない．次の分解は $\alpha_1+1, \alpha_2+1, \cdots$ が平方剰余であるかないかによる分類である．したがって，この方法は，それぞれの α_i の近傍における平方剰余と非剰余との配列パターンの違いによる分類を利用したものといえる．平方剰余の配列パターンが十分にランダムで，同じパターンの繰返しがないことは，Legendre記号 $\left(\frac{x}{p}\right)$ について

$$\sum_{x \in GF(p)} \left(\frac{x}{p}\right) \cdot \left(\frac{x+h}{p}\right) = -1 \quad (h \neq 0)$$

という直交関係に近い関係があることから，保証されている

と考えてよかろう．したがって，この方法で，比較的少数の k について試みるだけで，完全な因数分解ができる筈である．

4. 多項式の既約因子分解

多項式を $GF(p)$ で既約因子に分解することは，拡大体 $GF(p^k)$ における $f(x)=0$ の根を求めることと同等であるが，それには前述と全く同じようにやればよい．

$GF(p^k)$ における $f(x)=0$ の根の一つを α_i とすると，その共役は α_i^{p}, $\alpha_i^{p^2}$, $\alpha_i^{p^3}$, …, $\alpha_i^{p^{k-1}}$ であって，k 次式

$$\phi_i(x)=\prod_{j=0}^{k-1}(x-\alpha_i^{p^j})$$

がこれに対応する $f(x)$ の既約因子である．そして $\phi_i(x)$ は $x^{p^k-1}-1$ を割る．そこで，$f(x)$ の既約分解はまず

$$GCM(x^{p^2-1}-1,\ f(x)/f_1(x))=f_2(x)=\prod\phi_i(x)$$

をつくることからはじまる．ここで $\phi_i(x)$ は2次の既約因子であり，$f_2(x)$ はそれら全部の積である．以下同様にして

$$GCM(x^{p^k-1}-1,\ f(x)/f_1(x)f_2(x)\cdots f_{k-1}(x))=f_k(x)$$

によって，k 次の既約因子だけをまとめた積の式 $f_k(x)$ が得られる．

こうして求まった km 次多項式 $f_k(x)$ を更に個々の k 次既約因子にまで分解するには，前節と同様，α_i が平方剰余で

あるかないかに基いて分離する．それには $(x+h)^{\frac{p^k-1}{2}} \mp 1$ との最大公約式を求める手順を $h=0,1,2,\cdots$ と繰り返せばよい．

5. $GF(2^k)$ の場合

平方剰余を利用した上述の手法は，$p=2$ のときには使えない．$p=2$ だと x^2 は x の共役であり，したがってすべての数が平方数であって，平方剰余の概念が成立しないからである．$GF(2)$ の上の多項式は符号理論への応用などで重要で，これを既約因子に分解するためのアルゴリズムが確立されることは極めて望ましい．この場合に有効な方法として次の方法が考えられた．ここでは n の有限べきの程度の計算量でできるアルゴリズムを実行可能と定義することにする．

いま，$GF(2)$ の n 次多項式 $f(x)$ に対して，$f(\alpha)=0$ をみたす $GF(2^k)$ の元を求めたい．そこで，前と同様にして，$x^{2^k-1}-1$ との最大公約式を求めることによって，$GF(2^k)$ に根をもつ因子をまとめたもの，つまり k 次既約因子ばかりをまとめた積の多項式として，mk 次の式 $f_k(x)$ をつくることができる．

そこで次に，高々 $mk-1$ 次の多項式

$$A(x) \equiv x + x^2 + x^4 + \cdots + x^{2^k} \quad \mathrm{mod}\, 2,\ f_k(x)$$

をつくる．これは実行可能である．そして明らかに

$$(A(x))^2 \equiv A(x) \quad \mathrm{mod}\, 2,\ f_k(x)$$

をみたす．つまり

$$A(x)\left(A(x)-1\right) \equiv 0 \quad \mathrm{mod}\, 2,\ f_k(x)$$

で，$f_k(x)\equiv 0$ の根はすべて $A(x)\equiv 0$ か $A(x)\equiv 1$ のどちらかの根になっている．ここで $A(\alpha)$ は $GF(2^k)$ での α の共役和であるから，これは α をその共役和が 0 であるか 1 であるかにしたがって類別したことになる．言いかえれば，凡次の既約因子を，その x^{k-1} の係数が 1 であるか 0 であるかによって類別したとも言える．

そこで

$$GCM\left(A(x)-1,\ f_k(x)\right) = f_k^1(x)$$
$$GCM\left(A(x),\ f_k(x)\right) = f_k^0(x)$$

とすれば，$f_k(x) = f_k^1(x) f_k^0(x)$ で，こうして $f_k(x)$ の分解が得られる．なお，時には $A(x)\equiv 1$ あるいは $A(x)\equiv 0$ となってしまって分解が得られないこともある．それは全因子が片方の類に入ってしまう場合である．

いずれにせよ，分解がまだ完全でなければ次の試行を行なう．一般に，ある多項式 $P(x)$ を選んで

$$A(x) \equiv \sum_{j=0}^{k-1} P(x^{2^j}) \quad \mathrm{mod}\, 2,\ f_k(x)$$

を使うことによって，更に分解を進めることができる．

一般的に言って，有限体において方程式を解くことの困難さは，有限体には実数体のような位相が存在しないことにあると考えられる．実数体の場合のように一歩一歩接近して行くことができないのである．上述の方法の特徴は，平方剰余あるいは共役和という性質に着目して，有限体に一種の位相のようなものを導入したことにある．平方剰余のパターンの似ている数は近い数だと考えるのである．こうして，根の実際の値はわからないままに，それをグループ分けすることが可能になったのである．