数理解析研究所講究録
第520巻 1984年 47-57

多項式の因数分解について

アブストラクト

Sin Hitotumatu

京都大学数理解析研究所　　一松　信

多項式の因数分解は、永らく計算機にとって、難しい仕事と考えられていた。　原理的には、整数係数の多項式が、もしも因数分解できるものならば、その因子の係数は、有限の可能性の中から捜せばよい。　実際、２次式については、中学においてそのような方法が教えられている。　しかしこのような素朴な方法では、次数ｎとともに手数が急増する、いわゆるＮＰ問題になり、実用的ではない。

近年、素数ｐを法としてＨｅｎｓｅｌの補題を利用する算法により、かなりの多項式の因数分解が、人間よりも速くできるようになったが、まだすべての多項式の因数分解が、完全に自動的にできるというわけにはゆかないようである。　そのような例と、それに対する工夫をいくつかあげてみたい。

多変数の場合も、Ｈｅｎｓｅｌの補題の拡張を利用して、かなりの因数分解が可能であるが、対称式や交代式などの特性を活用した方法は、まだこれからの仕事として残された部分が多いようである。　そのほか経験上いくつかの特別な型を判定して、それらに対する算法をプログラムに加えることが、能率を高めるために不可欠なようである。

A few remarks on the factorization of polynomials

By

Sin Hitotumatu

(Res. Inst. for Math. Sci., Kyoto Univ.)

0. Introduction

For long time, it has been considered that the factorization of polynomials in computer algebra is a difficult task. At least, in principle, if a polynomial of one variable with integer coefficients is reducible in the rational field, then its factors are all of integer coefficients and their possibilities are finite. Indeed, this procedure is effective for quadratic polynomials, which is taught in the secondary schools.

However, such primitive procedure is not useful for polynomials of higher degree, since the number of possibilities rapidly increases as the degree does.

Recent computer can factorize polynomials much faster than human's work, using efficient procedures based on modulo p arithmetic and Hensel's lemma (see e.g. [1]). However, there still remain serious problems for complete automatic factorizations by computer algebra. Here I shall give a few examples and remarks.

1. Hensel's Lemma

Theorem 1 (Hensel's lemma). Assume that a polynomial of one variable with integer coefficients

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0$$

is factorized to the product of two relatively prime polynomials $G_1(x)$ and $H_1(x)$ with respect to modulo p, where p is a prime which does not divide the leading coefficient a_n. Then, for each integer $m=2,3,\dots$ there exist relatively prime polynomials $G_m(x)$, $H_m(x)$ (not necessarily unique) with the following properties:

$$\text{(i)} \quad P(x) \equiv G_m(x) \cdot H_m(x) \qquad \text{mod } p^m$$

$$\text{(ii)} \quad G_m(x) \equiv G_1(x), \quad H_m(x) \equiv H_1(x) \quad \text{mod } p$$

Outline of the proof. Use induction in m. If such $G_m(x)$ and $H_m(x)$ have been determined, we have by assumption

$$P(x) - G_m(x) \cdot H_m(x) = p^m \cdot R(x).$$

We can take suitable polynomials $U_m(x)$ and $V_m(x)$ such that

$$U_m(x) \cdot G_m(x) + V_m(x) \cdot H_m(x) \equiv R(x) \quad \text{mod } p.$$

Then the polynomials

$$G_{m+1}(x) = G_m(x) + p^m V_m(x), \quad H_{m+1}(x) = H_m(x) + p^m U_m(x)$$

satisfies the conditions for $m+1$. □

If the original polynomial $P(x)$ is actually reducible and $G_1(x)$ and $H_1(x)$ are the correct factors reduced in modulo p, then we may arrive at the correct factors of $P(x)$ up to constant factors, after finite steps of iterations.

As for the first factorization in modulo p, we know Berlekamp's algorithm, see [2].

2. An extension to the polynomial of several variables.

For polynomials of several variables, one can generalize Hensel's lemma in the following manner. First we arrange the given polynomial as a polynomial of one main variable x whose coefficients are polynomials of auxiliary variables $y_1,\ldots, y_\ell$. We assume that the leading coefficient $a_n(y_1,\ldots,y_\ell)$ does not vanish at $y_1=\cdots=y_\ell=0$. This assumption gives no restriction in generality, at least in principle, because if $a_n(y_1,\ldots,y_\ell)$ is not identically zero, there must be constant values $c_1,\ldots, c_\ell$ with $a_n(y_1-c_1,\ldots,y-c_\ell) \neq 0$. Hence we may change the variables $y_1,\ldots,y_\ell$ by $Y_1 = y_1-c_1,\ldots, Y_\ell=y_\ell-c_\ell$ as parallel displacement. However, in the actual computation, this transformation may cause usually serious explorsion of terms. Hence, we recommend several abbreviated algorithms, as in [3].

Now we have the following generalization of Theorem 1.

Theorem 2. Under the assumptions as above, we assume that $P(x;0)$ is decomposed into a product of two mutually prime factors $G_1(x)$ and $H_1(x)$. Then for each integer

$m=2,3,\ldots,$ there are polynomials $G_m(x;y)$ and $H_m(x;y)$ satisfying the following conditions:

(i) $P(x;y) \equiv G_m(x;y)\cdot H_m(x;y) \mod y^m$

(ii) $G_m(x;0) = G_1(x), \quad H_m(x;0) = H_1(x).$

Here $A \equiv B \mod y^m$ means that all coefficients in $A - B$ consist of polynomials in $y_1,\ldots, y_\ell$ with degree at least m. In this notation, the first assumption $P(x;0) = G_1(x)\cdot H_1(x)$ is equivalent to

$$P(x;y) \equiv G_1(x)\cdot H_1(x) \mod y^1.$$

The proof is completely similar to that of theorem 1.

The following classical theorem is sometimes useful.

Theorem 3. A quadratic polynomial of two variables x and y:

$$P(x,y) = ax^2 + 2h\,xy + by^2 + 2gx + 2fy + c$$

is decomposed into a product of two linear factors if and only if the coefficient determinant

$$\det \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix}$$

vanishes. If this condition is fulfilled, then we factorize $P(x,y)$ by the following procedure.

(i) First decompose the quadratic term into $(Ax+By)(Dx+Ey)$.

(ii) If these two factors are different, we solve the linear equations: $AF+DC=2g$, $BF+EC=2f$ in F and C.

Then $(Ax+By+C)(Dx+Ey+F)$ gives the factorization, where $CF=c$ is a check.

(ii') If $A:B = D:E$, then the original polynomial is reduced to a quadratic polynomial in $w=Ax+By$, which is readily factorized as a polynomial in w.

3. Examples.

Exp. 1. $P(x) = 54x^3 + 57x^2 + 28x + 15$.

We take $p=11$. $P(x)$ reduces to

$$-x^3 + 2x^2 - 5x + 4$$

which is easily factorized to

$$(-x+1)(x^2-x+4).$$

We have

$$P(x) - G_1(x)\cdot H_1(x) = 11(5x^3+5x^2+3x+1),$$

and

$$5x^3+5x^2+3x+1 = G_1(x)\cdot(5x+7)+H_1(x)\cdot(5x+4) \quad \text{mod } 11.$$

Hence we have

$$G_2(x) = G_1(x)+11\cdot(5x+4) = 54x+45 = 9(6x+5)$$

$$H_2(x) = H_1(x)+11\cdot(5x+7) = x^2+54x+81 = x^2+27(2x+3).$$

Now we see that $3^5 = 243 = 2\times 11^2 +1 = 0 \pmod{11^2}$, so that $9=3^2$ and $27=3^3$ are mutually reciprocal in mod 11^2. Transfering the numerical factor 9 from G_2 to H_2, we have

$$\tilde{G}_2(x) = 6x+5, \quad \tilde{H}_2(x) = 9x^2+2x+3$$

which are the correct factors of $P(x)$. In this case, we can avoid automatically the problem of distribution of the leading coefficients.

Exp. 2. $P(x,y) = x^4 - 2x^3y - x^2y^2 - 2xy^3 + y^4$

$$+ 4x^2y + 4xy^2 - 3x^2 - 3y^2 + 1.$$

In fact, this is the determinant of the 4th order matrix

$$\begin{bmatrix} 1 & x & y & y \\ x & 1 & x & y \\ y & x & 1 & x \\ y & y & x & 1 \end{bmatrix} .$$

We arrange $P(x,y)$ in a polynomial of x, say

$$x^4 - 2yx^3 + (-y^2 + 4y - 3)x^2 + (-2y^3 + 4y^2)x + (y^4 - 3y^2 + 1).$$

For $y=0$, it is

$$x^4 - 3x^2 + 1 = (x^2 - x - 1)(x^2 + x - 1),$$

(see next section). We have

$$P(x,y) - G_1(x) \cdot H_1(x) \equiv y(-2x^3 + 4x^2) \mod y^2$$

where

$$-2x^3 + 4x^2 = G_1(x) \cdot (-3x+1) + H_1(x) \cdot (x-1),$$

and hence

$$G_2(x,y) = G_1(x) + y(x-1) = x^2 + xy - x - y - 1,$$

$$H_2(x,y) = H_1(x) + y(-3x+1) = x^2 - 3xy + x + y - 1.$$

Then we have

$$P(x,y) - G_2(x,y)\cdot H_2(x,y) = y^2(2x^2-2yx+y^2-2)$$

where

$$2x^2 - 2yx + y^2 - 2 \equiv G_2(x,y) + H_2(x,y) \quad \mathrm{mod}\ y^2.$$

Hence we have

$$G_3(x,y) = G_2(x,y) + y^2 = x^2 + xy + y^2 - x - y - 1,$$
$$H_3(x,y) = H_2(x,y) + y^2 = x^2 - 3xy + y^2 + x + y - 1,$$

which given the correct factors of $P(x,y)$. □

Here the second term $H_3(x,y)$ is still reducible, if we extend the coefficient field algebraically. Using Theorem 3, we can factorize it as follows:

$$H_3(x,y) = (\tau x - \tau^{-1}y - 1)(\tau^{-1}x - \tau y + 1),$$

where $\tau = (\sqrt{5}+1)/2$, $\tau^{-1} = (\sqrt{5}-1)/2$.

Alternative method. Since the original polynomial $P(x,y)$ is symmetric in x and y, we can rewrite it as

$$5t^2 + (-6s^2+4s+6)t + s^4 - 3s^2 + 1,$$

if we put $s=x+y$ and $t=xy$. This is easily factorized to

$$(5t - s^2 - s + 1)(t - s^2 + s + 1)$$

which gives the same factors as above $G_3(x,y)$, $H_3(x,y)$, up to the signatures. □

But remember that a aymmetric polynomial does not always factorized into symmetric factors.

4. An unsuccessful example.

Exp. 3. $P(x) = x^4 - 3x^2 + 1$.

This appears in the first step in Exp. 2. We take $p=11$. The reason of this selection will be explained later. In modulo 11, we have

$$P(x) = (x^2 - 5)(x^2 + 2) \quad \text{mod } 11, \tag{1}$$

where

$$P(x) - G_1(x) \cdot H_1(x) = 11.1, \quad 1 \equiv 3(G_1 - H_1) \quad \text{mod } 11,$$

and hence

$$\left.\begin{aligned} G_2(x) &= G_1(x) - 11.3 = x^2 - 38, \\ H_2(x) &= H_1(x) + 11.3 = x^2 + 35. \end{aligned}\right. \tag{2}$$

Though this satisfies the condition in modulo 11^2 as

$$P(x) - G_2(x) \cdot H_2(x) = 1331 = 11^3 \equiv 0 \quad \text{mod } 11^2,$$

it is obvious that they are not correct factors of $P(x)$. Repeating the process, we always have a factorization $(x^2 + a_m)(x^2 - a_m - 3)$ in mod 11^m for each m, where a_m is a constant satisfying

$$a_m(a_m + 3) \equiv -1 \quad \text{mod } 11^m.$$

However, we never arrive at correct factors.

The reason of this failure is evident, as we have started from wrong factors. If we consider the original polynomial $P(x)$ as a quadratic polynomial in X^2, the discriminant is $3 \times 3 - 4 = 5$. Since 11 is the least prime for which 5 is the quadratic residue, we have had (1) in modulo 11. But this is not the ultimate factorization; 5 and -2 are again quadratic residues in modulo 11. The ultimate factorization is

$$P(x) = (x-4)(x+4)(x-3)(x-3).$$

Here we make an "arrangement of factors" say

$$P(x) = [(x-4)(x+3)][(x+4)(x-3)] = (x^2-x-12)(x^2+x-12).$$

Reducing the factors in modulo 11, we have the following correct factors

$$P(x) = (x^2 - x - 1)(x^2 + x - 1).$$

In the factorization of a quadratic polynomial in x^2, similar procedure is effective. But, actually we recommend to introduce the following elementary theorem in the factorization program.

<u>Theorem 4</u>. Under the assumption that the quadratic form $x^2 - bx + c$ is irreducible in the rational field, x^4-bx^2+c is reducible if and only if $c=u^2$ (perfect square; u may be negative) and $b+2u=v^2$. If this is fulfilled, x^4-bx^2+c is factorized to $(x^2-vx-u)(x^2+vx-u)$.

Example. $x^4 + x^2 + 1$, $x^4 + 4$, $x^4 - 3x^2 + 9$.

References

[1] E. Kaltofen, Factorization of polynomials, Computer Algebra; Symbolic and algebraic computation, Computing Supplementrum 4, Springer 1982, p.95-113.

[2] E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. 24(1970) p.715-735.

[3] D.R. Musser, Multivariant polynomial factorization, J. ACM 22 (1976), p.291-308.