通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

정수계수위에서의 다항식의 인수분해

조인호* · 임종인** · 김창한***

Factorization of Polynomials With Integer Coefficients

In-ho Cho, Jong-In Lim, Chang-Han Kim

요 약

다항식 인수분해 문제는 정수론에서 뿐만 아니라 Discrete logarithm과 관련하여 암호학의 응용에도 중요한 문제이다. Hensel의 Lifting Lemma를 이용하여 유한체위에서 다항식을 인수분해하여 정수계수위에서 다항식의 인수를 찾는 방법으로 정수계수위에서 다항식의 인수분해를 실행하였다.

Abstract

The polynomial factorization problem is important not only number theory but chyptology with Discrete logarithm. We factorized polynomials with integer coefficients by means of factorizing polynomials on a finite field by Hensel's Lifting Lemma and finding factors of polynomial with integer coefficients.

1. 서 론

정수론에 있어서 다항식의 인수분해 문제는 중요한 문제중의 하나이다. 1707년에 I. Newton이 정수계수위에서 1, 2차의 인수를 찾는 방법을 제시하였고, 1793년에 F. von Schubert는 다항식의 모든 인수를 찾는 방법을 제시하였다. 약 90년 후에 L. Kronecker는 F. von Schubert의 방법을 독립적으로 만들었으나 불행히도 이 방법은 비효율적이다. Hensel의 Lemma를 이용하여 더 효율적인 방법이 제안되었으며, 1982년에 A.K. Lenstra[4]에 의해 polynomial time의 정수계수다항식 인수분해 알고리즘이 제안되었다. 그리고 1983년에 L.M.

* 고려대학교 이과대학 수학과 교수
** 고려대학교 자연과학대학 수학과 부교수
*** 세명대학교 수학과 전임강사

Adlemann[1]은 GRH(Generalized Riemann Hypothesis)하에서 다항식의 기약판정과 인수분해 문제는 정수의 솟수판정과 소인수분해 문제로 polynomial time내에서 전환할 수 있음을 보였다. 그러나 이것의 실행방법은 아직 발견되지 않았다.

이 논문은 유한체 위에서 Berlekamp's factorization algorithm과 Hensel's lifting lemma를 이용한 정수 계수위의 다항식 인수분해 알고리즘 제시와 이것의 실행을 목적으로 하고 있다. 알고리즘은 IBM PC 386에 Borland C^{++}을 이용하여 프로그램화 하였다. 다항식 f에 있어서 최고차의 계수를 lc(f)라 하고 pp(f)는 f의 primitive 다항식(정수 계수위에서 다항식의 계수들의 GCD가 1인 다항식)을 말한다.

2. 유한체에서의 다항식 인수분해 알고리즘

p를 솟수라하고 p의 잉여류의 집합을 $GF(p)=\{-\frac{(p-1)}{2}, \cdots, [p/2]\}$라 하면 GF(p)는 유한체가 된다. f를 GF(p)[x]에 있는 square-free 다항식이라 하고 n=deg(f)라 하면 i번째 행이 $x^{ip} \bmod f$인 n×n인 행렬을 M이라 하자.

보조정리 2.1

GF(p)[x] 내에 있는 다항식 $v=v_0+v_1x+\cdots+v_{n-1}x^{n-1}$라 하자. 그러면 다음과 같은 결과를 갖는다.

$$vM \equiv v^p \bmod f \qquad vM=v,$$

여기서, $v=(v_0, v_1, \cdots, v_{n-1})$

증명. $M=(m_{ij})$라 하자.

즉, $x^{ip} \equiv \sum_{j=0}^{n-1} m_{ij} \bmod f.$

그러면 $v(x)^p=v(x^p)$

$$=\sum_{i=0}^{n-1} v_i x^{ip}$$

$$=\sum_{i=1}^{n-1} v_i \left(\sum_{j=0}^{n-1} m_{ij}\, x^j\right) \bmod f$$

$$=vM \bmod f.$$

$V=\{v \in GF(p)[x] \mid \deg v<n\}$라 하면 이것은 GF(p) 위에서 선형공간이 되고 행렬 $M-I_n$은 V의 일차변환을 나타낸다.

보조정리 2.2

1) $n-\mathrm{rank}(M-I_n)$와 GF(p) 위에서 다항식 f의 기약인수의 수는 같다.

2) $\mathrm{kernel}(M-I_n)$의 기저를 $v_1, v_2, \cdots, v_r$라 하자. 그러면 모든 i에 대하여 $f=\prod_{s \in GF(p)[x]} (v_i-s, f)$.

3) $f=\prod_{i=1}^{r} g_i$과 같이 인수분해 된다면 $1 \le i<j \le r$과 s GF(p)에 대하여 $1 \le k \le r$, g_i는 (f, v_k-s)를 나누고 g_j는 (f, v_k-s)를 못 나누는 k가 존재한다.

알고리즘 2. 1(유한체 위에서의 다항식 인수분해 알고리즘)

Input : GF(p)[x]에 있는 다항식 f

Output : 기약다항식 $g_1, \cdots, g_r$와 $f=\Pi\, g_i^{ei}$인 e_i.

1. h:=f

만약 $(f, f')=1$ 이면 go to 3

2. g:=(f, f')

f:=f/g go to 1

3. $M-I_n$에 Gauss 소거법을 이용하여 $v_1, \cdots, v_r$을 구하여라.

4. 만약 r=1이면 f는 기약이다. go to 8

5. GF(p)에 있는 모든 s에 대하여 $\gcd(f, v_2-s)$를 계산 하여라.

6. $H_2=\{(f, v_2-s) \mid (f, v_2-s) \neq 1,\ s \in GF(p)[x]\}$의 원소의 갯수가 r이면 go to 8

7. $H_k=\{(h, v_k-s) \mid (h, v_k-s) \neq 1,\ h \in H_{k-1}$이고 $s \in GF(p)\}$을 계산하고 이 집합의 원소의 갯수가 r이면 go to 8

그렇지 않으면 k :=k+1 go to 7

8. GF(p)[x]에서 $f=\Pi g_i$와 같이 인수분해 된다고 하자.

h:=h/f, i:=1, e_i:=1

(*) 만약 g_i가 h를 나누면 e_i:=e_i+1, h:=h/g_i go to (*)

만약 i:=r이면 stop 아니면 i:=i+1 go to (*)

예제

$x^{32}+x^{15}+2x^3+2$는 Z[x]에서 기약이다. 그러나 GF(2)[x]에서는

$(x^{11}+x^9+x^7+x^2+1)(x^{21}+x^{19}+x^{15}+x^{13}+x^{12}+x^{10}+x^9+x^8+x^7+x^6+x^4+x^2+1)$와 같이 인수분해되고, GF(59)[x]에서는 $(x+4)(x^2+2x+8)(x^7-5x^6-8x^5-5x^4+9x^3-29x^2)(14x^{13}+28x^{12}-16x^9-14x^8-22x^7-3x^6-19x^5+17x^4+28x^3-6x^2+13x+14)$와 같이 인수분해된다.

3. 정수계수위에서의 다항식의 인수분해

f는 square-factor를 갖지 않는 정수를 계수로 갖는 다항식이라 하고 정수 p는 lc(f)·discr(f)를 못 나누는 솟수라하자. 그러면 f는 GF(p)[x]에서도 square-factor를 갖지 않는다.

보조정리 3.1

GF(p)[x]에서 $f=g_1h_1$이고 $(g_1, h_1)=1$이면 p-adic 환 Z_p에 대해서 $Z_p[x]$에 다음과 같은 g, h가 존재한다. 즉 $Z_p[x]$에서는 f=gh이고, GF(p)[x]에서는 $g=g_1$, $h=h_1$, $\deg(g)=\deg(g_1)$ 그리고 $\deg(h)=\deg(h_1)$이다.

증 명

모든 j=1, 2, …, n, …에 대하여 위 조건을 만족하는 $(Z/p^jZ)[x]$에 있는 g_j, h_j를 찾을 수 있으면 된다. 수학적 귀납법에 의하여 위의 사실을 증명해 보자.

먼저 j=1이면 명백하다. j<n에 대하여 g_j, h_j가 존재한다고 가정하자. 그러면 j=n-1에 대해서 $f=g_{n-1}h_{n-1}$이라하면, $(Z/p^nZ)[x]$에서 $f-g_{n-1}h_{n-1}=p^{n-1}c$이다. $(g_1, h_1)=1$이므로 GF(p)[x]에는 $g_1a+h_1b=1$이고 $\deg(a)<\deg(h_1)$인 a와 b가 존재한다. GF(p)[x]에서 $ac=sh_1+a_1$이고 $\deg(a_1)<\deg(h_1)$인 s와 a_1을 계산할 수 있고 $b_1=bc+sg_1$라 놓자.

그러면 GF(p)[x]에서 $a_1g_1+b_1h_1=c$이다. $g_n=g_{n-1}+p^{n-1}b_1$ 그리고 $h_n=h_{n-1}+p^{n-1}a_1$라 놓자. 그러면 $(Z/p^nZ)[x]$에서

$$f=g_nh_n$$
$$=(g_{n-1}+p^{n-1}b_1)(h_{n-1}+p^{n-1}a_1)$$
$$=g_{n-1}h_{n-1}+p^{n-1}c$$

이다. 또한 GF(p)[x]에서 $\deg(g_n)=\deg(h_{n-1})=\deg(g_1)$이고 $\deg(g_n)=\deg(g_{n-1})=\deg(h_1)$이다.

보조정리 3.2

Z[x]에 있는 $f(x)=a_nx^n+\cdots+a_1x+a_0$라 하자. $g=b_mx^m+\cdots+b_0$를 f의 한 인수라하면 모든 i=0, 1, …, m에 대하여 $|b_i|<|lc(f)|(a_0^2+\cdots+a_n^2)^{1/2}$ 이다. $\binom{[n/2]}{[n/4]}$

알고리즘 3.1. (정수계수 다항식의 GCD 알고리즘)

Input : Z[x]에 있는 primitive인 두 다항식 f와 g

Output : f와 g의 GCD

1. lc(f)·lc(g)를 나누지 못하는 소수 p를 찾아라.
2. GF(p)[x]에서 f와 g의 GCD를 구하여라.
   h:=gcd(f, g)
   prime:=p
3. H:=lc(f)f mod prime

만약 h가 lc(f)f를 나누고 pp(h)가 g를 나누면 GCD=pp(h) stop

4. lc(f)·lc(g)를 나누지 못하는 소수 q를 잡자. 그리고 GF(q)[x]에서 f와 g의 GCD를 구하자.
5. 그러면 다음과 같이 3가지 가능성이 있다.
   1) $\deg(h_q)<\deg(h)$이면 h:=h_q go to 3

2) $\deg(h_q) > \deg(h)$이면 go to 4

3) $\deg(h_q) = \deg(h)$이면 Chinese Remainder Theorem을 이용하여 $r = h \pmod{prime}$이고 $r = h_q \pmod{q}$인 r을 찾을 수 있다. h:=r, prime:=prime*q go to 3

위의 알고리즘은 GCD의 모든계수의 절대값이 prime/2 보다 작으면 끝난다.

알고리즘 3.2(정수계수위에서의 다항식 인수분해 알고리즘)

Input : Z[x]에 있는 다항식 f

Output : $f = \Pi\, g_i^{e_i}$인 기약다항식 g_i와 factor 수 e_i

1. F:=f
2. • Euclidean 알고리즘을 이용하여 f의 계수들의 GCD=d를 구하여라.
   • f:=f/d(f를 primitive로 만든다.)
   • 다항식의 Euclidean 알고리즘을 이용하여 GCD(f, f)를 구한다.
   • f:=f/GCD(f, f) (f를 square-free가 되도록 한다.)
   • n:=deg(f), $f = a_n x^n + \cdots + a_0$
3. • 행렬의 Gauss 소거법을 이용하여 다항식 f의 discriminant discr(f)를 구하여라.
   • lc(f) · discr(f)를 나누지 못하는 솟수 p를 찾자.
4. 다음조건을 만족하는 가장 작은 정수 k를 찾자.

$$p^k > 2 \mid lc(f) \mid (a_0^2 + \cdots + a_n^2)^{1/2} \qquad [n/2]$$

$$[n/4]$$

5. GF(p)[x]에서 알고리즘 2. 1을 이용하여 인수분해하여라.

$$f = \prod_{i=1}^{r} h_i$$

6. 보조정리 3.1을 이용하여 $(Z/p^kZ)[x]$에 있는 h_i^k들을 찾을 수 있다.

$$f = \prod_{i=1}^{r} h_i^k$$

7. • 모든 $\{1, 2, \cdots, n\}$의 부분집합 S에 대하여 $h := lc(f) \prod_{i \in S} h_i^k \pmod{p^k}$을 계산하라.

만약 h가 lc(f)f를 나누면 pp(h)는 f의 인수이다.

8. 이 과정은 알고리즘 2. 1의 8번 단계와 비슷하다.

4. 결 과

$2x^{80}+4x^{60}-6x^{50}-x^{31}+x^{30}-2x^{11}+2x^{10}+3x-3$
$=(x-1)(x+1)(x^4+x^3+x^2+1)$
$(x^4-x^3+x^2-x+1)(x^{20}+x^{10}+3)(2x^{50}-x+1)$

$x^{90}+7x^{80}-3x^{55}+2x^{47}-5x^{35}+10x^{30}-x+1$: 기약다항식

$12x^{90}+7x^{80}-3x^{55}+2x^{47}-5x^{35}+10x^{10}-x+1$: 기약다항식

$x^{90}+2x^{30}+3x^{10}-2$: 기약다항식

$6x^{90}-3x^{52}-2x^{30}-3x^{10}+2=(x-1)(x+1)(6x^{88}+6x^{86}+\cdots+6x^{52}+3x^{50}+3x^{48}+\cdots+3x^{30}+x^{28}+x^{26}+\cdots+x^{10}-2x^8-2x^6-\cdots-2)$

$6x^{90}-3x^{52}+2x^{30}-3x^{10}-2=(x-1)(x+1)(6^{88}+6x^{86}+\cdots+6x^{52}+3x^{50}+3x^{48}+\cdots+3x^{30}+5x^{28}+5x^{26}+\cdots+5x^{10}+2x^8+2x^6+\cdots+2)$

참 고 문 헌

1. L.M. Adleman, A.M.Odlyzko, Irreducibility testing and factorization of polynomials, Math. Com. 41 (1983), 669-709.

2. E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Com. 24(1970), 713-715.

3. H.Cohen, A course in algorithmic number theory. perprint.

4. A.K. Lenstra, Factorization of polymomials, Computational method in number theory, part 1,

Mathematical Centre Tracts, 154, 1982.

5. A.K. Lenstra, H.W.Lenstra, Jr. & L. Lovasz, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982) 515-534.

6. J.H. Loxton, Number theory and crytography, Cambridge University press, 1980.

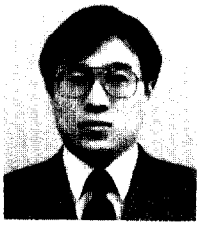
7. M.Mignotte, An equality about factors of polynomials, Math. Com. 28 (1974), 1153-1157.

8. R.Lidle, L. Niederreiter, Encyclopedia of mathematics and its applications, Vol. 20, (finite fields), Addison-Wesley, 1983.

□ 著者紹介

趙 寅 鎬(正會員)

高麗大學校 理科大學 數學科(學士)
高麗大學校 大學院 數學科(代數學 碩士)
高麗大學校 理科大學 講師/독일 뮌헨대학교 수학과(Dr. rer. nat)
서울大學校 大學院 講師/梨花女子大學校 數學科 助教授
大韓數學會 無任所 理事
大韓數學會 會誌 編輯委員/大韓數學會 監査
現 高麗大學校 理科大學 數學科 教授/韓國通信情報保護學會 副會長



임 종 인(正會員)

1980年 2月 高麗大學校 數學科 卒業(學士)
1986年 2月 高麗大學校 大學院 卒業(理學博士)
現 高麗大學校 自然科學大學 副教授
關心分野 : 정수론 및 관련응용분야

김 창 한(正會員)

1985年 2月 高麗大學校 數學科 卒業(學士)
1992年 2月 高麗大學校 大學院 卒業(博士)
現 : 세명대학 수학과 전임강사
關心分野 : 정수론 및 응용분야