DOI: 10.13656/j.cnki.gxkx.2005.01.003
广西科学 Guangxi Sciences 2005, 12(1): 8~9, 13

多项式 x^n-bx-a 的二次不可约因式*

The Irreducible Quadratic Factorizations of the Polynomial x^n-bx-a

何 波
He Bo

(四川省隆昌县响石中学,四川隆昌 642152)
(Longchang Xiangshi Middle School, Longchang, Sichuan, 642152, China)

摘要:设 $n>4$, $f_b(x)=x^n-bx-a\in \boldsymbol{Z}[x]$,其中 $a,b\neq 0$, $n\in \boldsymbol{N}$, $a,b\in \boldsymbol{Z}$.讨论 $b=\pm 1$ 时 $f_b(x)$ 的二次不可约因式.证明: x^6-x-a 在 $\boldsymbol{Z}[x]$ 中没有二次不可约因式;若 $f_{-1}(x)$ 在 $\boldsymbol{Z}[x]$ 中有二次不可约因式,除了 $n\equiv 2 \pmod 3$, $a=-1$, $g(x)=x^2+x+1$ 情况外,必有 $n=5$, $a=\pm 6$ 或 $n=13$, $a=\pm 90$,且 $g(x)=x^2\pm x+2$.

关键词:多项式 二次不可约因式 本原素因数 整系数 Lucas数
中图法分类号: O156.7 文献标识码: A 文章编号: 1005-9164(2005)01-0008-02

Abstract Let $n>4$, $f_b(x)=x^n-bx-a\in \boldsymbol{Z}[x]$ with $a,b\neq 0$, $n\in \boldsymbol{N}$, $a,b\in \boldsymbol{Z}$. We have discussed the irreducible quadratic factorizations of the polynomial $f_b(x)$ with $b=\pm 1$. We proved that: x^6-x-a has not irreducible quadratic factorizations in $\boldsymbol{Z}[x]$; $f_{-1}(x)$ has an irreducible quadratic factorization $g(x)$ in $\boldsymbol{Z}[x]$ witch is monic, then either $n\equiv 2 \pmod 3$, $a=-1$, $g(x)=x^2+x+1$, or $n=5$, $a=\pm 6$, or $n=13$, $a=\pm 90$, $g(x)=x^2\pm x+2$.

Key words polynomial, irreducible quadratic factorizations, primitive divisors, intergral coefficient, Lucas numbers

设 $\boldsymbol{Z}$, $\boldsymbol{Z}[x]$ 分别是整数及整系数多项式的集合, n 是大于4的整数,对于非零整数 a 和 b,三项式 $f_b(x)=x^n-bx-a$ 在 $\boldsymbol{Z}[x]$ 上的因式分解与工程技术中很多实际问题有着密切的联系[1].对此, Ribenbiom[2] 证明了:对于任意给定的 n, b,当 $|a|>C_1(n,b)$ 时, $f_b(x)$ 没有在 $\boldsymbol{Q}$ 上不可约且首项系数等于1的不可约二次整系数因式,这里 $C_1(n,b)$ 是与 n, b 有关的可有效计算的常数.陈宏基[3]证明了: $b=1$ 时,除了 $n\equiv 2 \pmod 6$ 且 $a=-1$ 外,若 $f_1(x)$ 有二次不可约因式,则必有 $n\leqslant 512880$.杨仕椿[4]证明了:若 $f_b(x)$ 有二次不可约因式,除去 $f_1(x)$ 中 $n\equiv 2 \pmod 6$, $a=-1$ 和 $f_{-1}(x)$ 中 $n\equiv 2 \pmod 3$, $a=-1$,必有 $n<\max(8|b|/7, 512870)$.

最近,乐茂华[5]给出当 $n>6$ 时 $f_1(x)$ 的精确结论.由于 Rabinowitz[6] 早已明确:当 $n=5$ 时, $f_1(x)$ 仅当 $a=\pm 15$, ± 22440 或 ± 2799640 有二次不可约因式.于是 $f_1(x)$ 的二次不可约因式仅剩下 $n=6$ 未解决.本文给出了 $n=6$ 时, $f_1(x)$ 的二次不可约因式以及 $f_{-1}(x)$ 的完整结论.

1 相关引理

设 $g(x)=x^2-sx+t$ 是 $\boldsymbol{Z}[x]$ 上的二次不可约因式,且 $g(x)$ 的根为 T, U,则

$$\mathrm{T}=(s+\sqrt{s^2-4t})/2,\ \mathrm{U}=(s-\sqrt{s^2-4t})/2, \tag{1}$$

其中, s^2-4t 为非平方数.

引理1[4] 多项式 $f_b(x)=x^n-bx-a$ 有二次不可约因式 $g(x)$ 的充要条件是:

$$b=\frac{\mathrm{T}^n-\mathrm{U}^n}{\mathrm{T}-\mathrm{U}},\ a=\frac{\mathrm{T}^n+\mathrm{U}^n}{2}-\frac{b(\mathrm{T}+\mathrm{U})}{2}. \tag{2}$$

引理2[4] 若多项式 $f_{-1}(x)=x^n+x-a$ 有二次不可约因式 $g(x)$,则

(i) $n\equiv 2 \pmod 3$, $a=-1$, $g(x)=x^2+x+1$;

(ii) $\gcd(s,t)=1$, T/U 不是单位根且 $\dfrac{\mathrm{T}^n-\mathrm{U}^n}{\mathrm{T}-\mathrm{U}}=-1$.

收稿日期: 2004-08-04
修回日期: 2004-10-12
作者简介:何 波(1978-),男,四川隆昌人,中学数学教师,业余从事数理研究。
* 四川省教育厅自然科学基金(2004B025)资助项目。

设 T和 U是代数整数.如果 T+ U和 TU都是互素的非零整数,而且 T/U不是单位根,则数组 (T,U)称为 1个 Lucas对.

又设 $a = T + U$, $c = TU$.此时,

$T = (a + \lambda\sqrt{b})/2$, $U = (a - \lambda\sqrt{b})/2$, (3)

其中, $b = a^2 - 4c$, $\lambda \in \{-1, 1\}$.如此的整数组 (a,b) 称为 Lucas对 (T,U) 的参数.当 2个 Lucas对 (T_1,U_1) 和 (T_2,U_2) 满足 $T_1/U_1 = T_2/U_2 = \pm 1$时,称 (T_1,U_1) 与 (T_2,U_2) 是等价的.

对于给定的 Lucas对 (T,U).整数

$$U_m = U_m(T,U) = \frac{T^m - U^m}{T - U}, m = 0, 1, 2, \cdots \quad (4)$$

统称为与 (T,U) 对应的 Lucas数.显然,当 Lucas对 (T_1,U_1) 与 (T_2,U_2) 等价时,对于任何非负整数 m都有 $U_m(T_1,U_1) = \pm U_m(T_2,U_2)$.

当 $m > 1$时,如果素数 p适合 $p \mid U_m$ 以及 $p \nmid bU_1 \cdots U_{m-1}$,则称 p是 Lucas数 U_m的本原素因数.

引理 3[7] 设 m是适合 $4 < m \leqslant 30$且 $m \neq 6$的正整数.如果 Lucas数 $U_m(T,U)$没有本原素因数,则 (T,U) 是下列参数的 Lucas对 (a,b) 或与其等价的 Lucas对:

(i) $m = 5$, $(a,b) = (1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, 1364)$;

(ii) $m = 7$, $(a,b) = (1, -7), (1, -19)$;

(iii) $m = 8$, $(a,b) = (1, -7), (2, -24)$;

(iv) $m = 10$, $(a,b) = (2, -8), (5, -3), 5, -47)$;

(v) $m = 12$, $(a,b) = (1, 5), (1, -7), (1, -11), (1, -15), (1, -9), (2, -56)$;

(vi) $m \in \{13, 18, 30\}$, $(a,b) = (1, -7)$.

引理 4[8] 当 $m > 30$时, Lucas数 $U_m(T,U)$都有本原素因数.

2 主要结果及其证明

定理 1 $x^6 - x - a$在 $\boldsymbol{Z}[x]$上没有二次不可约因式.

此外,利用 Lucas数的本原素因数的存在性的有关结果,对于 $f_{-1}(x)$,证明了:

定理 2 $f_{-1}(x) = x^n + x - a$ 在 $\boldsymbol{Z}[x]$上若有二次不可约因式,除去 $n \equiv 2 \pmod 3$, $a = -1$, $g(x) = x^2 + x + 1$情况外,仅当 $n = 5$, $a = \pm 6$或 $n = 13$, $a = \pm 90$时,有二次因式 $g(x) = x^2 \pm x + 2$.

定理 1的证明 设 $x^6 - x - a$在 $\boldsymbol{Z}[x]$上有二次不可约因式 $g(x) = x^2 - sx + t$, $s, t \in \boldsymbol{Z}$, 且 $g(x)$的根为 T,U,从引理 1可知存在适当的整数 s, t,使得

$$\frac{T^6 - U^6}{T - U} = 1 \quad (5)$$

成立.由于 $T + U = s$, $TU = t$,从 (5) 式可得

$$\frac{T^6 - U^6}{T - U} = (T + U)[(T + U)^4 - 4TU(T + U)^2 + 3T^2U^2] = s(s^4 - 4s^2t + 3t^2) = 1. \quad (6)$$

从 (6) 式知

$$s = (1 - t)(1 - 3t) = \pm 1, t \neq 0, \quad (7)$$

但 (7) 式无解.于是 $x^6 - x - a$在 $\boldsymbol{Z}[x]$上没有二次不可约因式.定理 1证毕.

定理 2的证明 从引理 2可知, T/U不是单位根, $\gcd(s, t) = 1$,且满足

$$\frac{T^n - U^n}{T - U} = -1, n \neq 2 \pmod 3. \quad (8)$$

于是 $T + U = s$, $TU = t$,可知 (T,U) 是参数为 $(s, s^2 - 4t)$ 的 Lucas对.从 (8)式知 Lucas数 $U_n(T,U)$满足 $U_n(T,U) = -1$.所以 Lucas数 $U_n(T,U)$没有本原素因数.根据引理 4,得到 $n \leqslant 30$.再由引理 3,故只须考虑 $n = 5, 7, 8, 10, 12, 13, 18$或 30的情形:

1) 当 $n = 5$, $(\pm s, s^2 - 4t) = (1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76)$或 $(12, 1364)$,分别有 $U_5 = 5, -1, 5, 1, 5, 1$或 1;

2) 当 $n = 7$, $(\pm s, s^2 - 4t) = (1, -7)$或 $(1, -19)$,分别有 $U_7 = \pm 7$或 1;

3) 当 $n = 8$, $(\pm s, s^2 - 4t) = (1, -7)$或 $(2, -24)$,分别有 $U_8 = \mp 3$或 ± 128;

4) 当 $n = 10$,由于 $(T + U) \mid \frac{T^{10} - U^{10}}{T - U} = -1$,由引理 3知 $T + U = \pm 2$或 ± 5,矛盾;

5) 当 $n = 12$, $(\pm s, s^2 - 4t) = (1, 5), (1, -7), (1, -11), (1, -15), (1, -19)$或 $(2, -56)$,分别有 $U_{12} = 0, \pm 45, \pm 160, \mp 231, \mp 3024$或 ∓ 23452;

6) 当 $n = 13, 18$或 30,此时 $(\pm s, s^2 - 4t) = (1, -7)$,由于 $U_{13} = -1$, $U_{18} = \pm 85$, $U_{30} = \mp 24475$.仅当 $n = 13$时 $a = \pm 90$,此时 $g(x) = x^2 \pm x + 2$.

此外,运用用类似于定理 1的方法,可知 $n = 6$时无解.定理 2证毕.

综上所述,除去 $n \equiv 2 \pmod 3$, $a = -1$, $g(x) = x^2 + x + 1$情况外, $f_{-1}(x)$仅当 $n = 5$, $a = \pm 6$或 $n = 13$, $a = \pm 90$时,有二次因式 $g(x) = x^2 \pm x + 2$.

致谢

衷心感谢西南民族大学付强教授对作者研究工作的热情鼓励!

(下转第 13页 Continue on page 13)

$c = 0$,

由(2.2),上式等价于

$$q_0 = \sum_{i=1}^{\infty} c_i.$$

显然这又等价于 Q 是保守的.定理证毕.

参考文献:

[1] Anderson W J. Continuous-Time Markov Chains. Springer, Series in Statistics [M]. New York: Springer-Verlag, 1991.

[2] Feller W. On the integro-differential equations of purely discontinuous Markov processes [J]. Trans Ann Math Soc, 1940, 48: 488-515.

[3] Reuter G E H. Denumerable Markov processes and the associated contraction semigroups on L[J]. Acta Math, 1957, 97: 1-46.

[4] 侯振挺,刘再明,张汉君,等.生灭过程 [M].长沙:湖南科学技术出版社,2000.

[5] Wu Q Y, Zhang H J, Hou Z T. An extended birth-death Q-matrix with instantaneous state (I) [J]. Chinese Journal of Contemporary Mathematics, 2003, 24(2): 159-168.

[6] 吴群英,张汉君,侯振挺.具有突变率、含瞬时态的广义生灭矩阵(I) [J].数学年刊(A辑),2003,24(2): 187-192.

[7] Wu Q Y, Zhang H J, Hou Z T. An extended birth-death Q-matrix with instantaneous state (II) [J]. Chinese Journal of Contemporary Mathematics, 2003, 24(4): 317-328.

[8] 吴群英,张汉君,侯振挺.具有突变率、含瞬时态的广义生灭矩阵(II) [J].数学年刊(A辑),2003,24(5): 555-564.

[9] 吴群英.广义全稳定生-灭过程 [J].系统科学与数学,2003,23(4): 517-528.

[10] 吴群英.广义生灭过程—强遍历性 [J].工程数学学报,2002,19(1): 104-108.

[11] Wu Qunying. The minimal Q-process and its properties for an extended birth-death Q-matrix [J]. Mathematica Applicata, 2002, 15(4): 79-84.

(责任编辑:黎贞崇)

(上接第 9页 Continue from page 9)

参考文献:

[1] 刘木兰.数学在密码学中的某些应用 [J].数学的实践与认识,1986,3: 47-55.

[2] Ribenboim. On the factorization of $x^n + Bx - A$ [J]. Enseign Math, 1991, 37: 191-200.

[3] 陈宏基.关于三项式 $x^n - x - a$ 的二次因式 [J].数学杂志,2002,22(3): 319-322.

[4] 杨仕椿.关于 $x^n - bx - a$ 的二次整系数因式 [J].长沙铁道学院学报,2003,(4): 77-81.

[5] 乐茂华. $x^n - x - a$ 的不可约二次因式 [J].黄岗师范学院学报,2003,(23)3: 1-2.

[6] Rabinowitz S. The factorizations of $x^5 \pm x + n$ [J]. Math Mag, 1968, 61: 191-193.

[7] Y Bilu, G Hanrot, P M Voutier. Existence of primitive divisors of Lucas and Lehmer numbers [J]. J Reine Angew Math, 2001, 529: 75-122.

[8] P M Voutier. Primitive divisors of Lucas and Lehmer numbers [J]. Math Comp, 1995, 64: 869-888.

(责任编辑:黎贞崇)