doi: 10.3969/j.issn.0490-6756.2019.01.004

多项式 x^n-1 在有限域上的分解

唐　睿[1]，彭国华[2]
(1. 四川大学锦江学院，眉山，620860；2. 四川大学数学学院，成都 610064)

摘　要：多项式 x^n-1 在有限域 F_q 上的分解不仅在理论上有重要意义，在保密通信、纠错码等方面也有诸多应用. 本文在 $\mathrm{ord}_{\mathrm{rad}(n)}q=2w$($w$ 为奇素数)时得到了 x^n-1 的全部不可约因式，部分完善和推广了近期的相关研究.

关键词：有限域；不可约因式；分圆多项式；循环码
中图分类号：O156.2　　**文献标识码**：A　　**文章编号**：0490-6756(2019)01-0013-04

Factorization of polynomial x^n-1 over finite fields

TANG Rui[1], *PENG Guo-Hua*[2]
(1. Sichuan University Jinjiang College, Meishan 620860, China;
2. School of Mathematics, Sichuan University, Chengdu 610064, China)

Abstract: Factorization of the polynomial x^n-1 over finite fields is not only important theoretically, but also has many applications, especially in secure communication and error-correcting coding theory. In this paper, an explicit factorization of x^n-1 into irreducible factors over field F_q is given when $\mathrm{ord}_{\mathrm{rad}(n)}q=2w$, where w is an odd prime number. These results improve and generalize some recent progresses.

Keywords: Finite field; Irreducible factor; Cyclotomic polynomial; Cyclic code
(2010 MSC 11T06)

1　引　言

有限域上单变元多项式的分解无论在理论上还是在应用上都有重要价值[1-10]. 例如，设 n 为正整数，q 为某奇素数 p 的方幂，F_q 是 q 元有限域，F_q 上循环码的构造就归结为寻找多项式 x^n-1 在 F_q 上的因式. 这是因为，每一个长度为 n 的循环码都本质上对应于剩余类环 $F_q[x]/(x^n-1)$ 的一个理想，而该环的理想又与 x^n-1 的首项系数为 1 的因式一一对应. 理论上，$x^n-1=\prod_{d|n}\Phi_d(x)$，其中 $\Phi_d(x)$ 为 d 阶分圆多项式，因此 x^n-1 的分解也可归结为分圆多项式的分解.

对于分圆多项式 $\Phi_{2^k}(x)=x^{2^k}+1$，当 $q\equiv1\pmod 4$ 时，其因式分解是容易的[10]. 当 $q\equiv3\pmod 4$ 时，$\Phi_{2^k}(x)$ 的完全分解由 Meyn 于 1996 年给出[1]. 若 r 是奇素数并且 $q\equiv\pm1\pmod 4$，Fitzgerald 和 Yucas 在 2007 年得到了分圆多项式 $\Phi_{2^sr}(x)$ 的因式分解，并给出了 $\Phi_{2^r3}(x)$ 和 Dickson 多项式 $D_{2^r3}(x)$ 的精细分解[2]. 2012 年，王和王给出了 $\Phi_{2^r5}(x)$ 的分解[3]. 更一般地，当 $m>3$ 为奇数时，在假设 $\Phi_m(x)$ 的分解已知的情况下，2013 年 Tuxanidy 和王得到 $\Phi_{2^sm}(x)$ 的因式分解[4]. 同年，陈，李和 Tuerhong 分解了 $x^{2^sp^t}-1$，指出 $x^{2^sp^t}-1$ 的不可约因式都是二项式或者三项式，其中 $q\equiv1\pmod p$[5]. 2016 年，吴，朱，冯，杨指出 $\Phi_{p^s}(x)$ 和 $\Phi_{p^sr}(x)$ 的所有不可约因式都可以由比它们更低阶的分圆多项式的不可约因式导出[7].

以 $\mathrm{rad}(n)$ 记 n 的所有不同素因子的乘积，以

收稿日期：2018-04-18
基金项目：国家自然科学基金(11171150)
作者简介：唐睿(1988－)，男，四川成都人，硕士研究生，主要研究方向为数论. E-mail: 976040110@qq.com
通讯作者：彭国华. E-mail: peng@scu.edu.cn

$\mathrm{ord}_n a$ 记整数 a 作为乘法群 $(\mathbf{Z}/n\mathbf{Z})^\times$ 中元素的阶，即 $\mathrm{ord}_n a$ 是使得 $a^m \equiv 1 \pmod n$ 成立的最小正整数 m. 当 $\mathrm{rad}(n) \mid (q-1)$ 时，2015 年 Martinesz，Vergara 和 Oliveira 给出了 x^n-1 在 F_q 上的精细因式分解[6]. 他们首先分析了什么样的条件下二项式 x^t-a 为多项式 x^n-1 的不可约因式，再由该结论出发倒推得到 x^n-1 的不可约因式都是二项式的条件，最后给出了特定条件下 x^n-1 的精细因式分解. 当 $\mathrm{ord}_{\mathrm{rad}(n)} q$ 为素数时，2017 年吴，岳，范给出了 x^n-1 的因式分解[8]. 他们延续了 Martinesz，Vergara 和 Oliveira 的研究，先将 x^n-1 在 F_q 的一个扩域上分解为一系列的不可约二项式，再由域扩张理论给这些不可约二项式归类，属于 $F_q[x]$ 的二项式直接使其落入 $F_q[x]$ 中，不属于 $F_q[x]$ 的不可约因式通过伽罗瓦理论以 Frobenius 自同构找出所有与其共轭的不可约因式，它们的乘积正是 $F_q[x]$ 中的不可约多项式.

在本文中，我们讨论了 $\mathrm{ord}_{\mathrm{rad}(n)} q = 2w$（$w$ 为素数）时的情形. 基于 Martinesz 等人的结果[6]，利用伽罗瓦理论，并采用与吴等的研究类似的方法[8]，我们得到了更一般的结论.

2 预备知识

以下我们始终假设 $\mathrm{ord}_{\mathrm{rad}(n)} q = 2w$，$w$ 是一个奇素数. 为方便，本文记整数 $a_1,\cdots,a_k$ 的最大公因子为 $(a_1,\cdots,a_k)$，其中 k 为正整数. 对于素数 p 和正整数 n，以 $v_p(n)$ 记 p 在 n 的分解中的最高方幂. 若正整数 n 的素因子分解为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，则 $\mathrm{rad}(n) = p_1 p_2 \cdots p_s$，$v_{p_i}(n) = \alpha_i$. 由于 $\mathrm{rad}(n) \mid (q^{2w}-1)$，$(w, q^2-1, \frac{q^{2w}-1}{q^2-1}) = 1$，因此 n 有唯一分解式

$$n = w^{v_w(n)} n_1 n_2 \tag{1}$$

使得 $\mathrm{rad}(n_1) \mid q^2-1$，$\mathrm{rad}(n_2) \mid \frac{q^{2w}-1}{q^2-1}$. 对正整数 i,j，定义

$$l_{i,j} = \frac{q^j-1}{(i,q^j-1)}, m_{i,j} = \frac{i}{(i,q^j-1)} \tag{2}$$

设 θ,α,β,π 分别为循环群 F_q^*，$F_{q^2}^*$，$F_{q^w}^*$，$F_{q^{2w}}^*$ 的生成元，且

$$\theta = \alpha^{q+1} = \beta^{\frac{q^w-1}{q-1}} = \pi^{\frac{q^{2w}-1}{q-1}}.$$

根据文献[6]的结论，当 $\mathrm{ord}_{\mathrm{rad}(n)} q = 2w$ 时，x^n-1 在 $F_{q^{2w}}$ 中有如下的不可约分解

$$\prod_{t \mid m_{n,2w}} \prod_{\substack{1 \le u \le (n, q^{2w}-1) \\ (u,t)=1}} (x^t - \pi^{u l_{n,2w}}) \tag{3}$$

这里每个不可约因式都是二项式. 由伽罗瓦理论，对于 $\pi^{u l_{n,2w}} \in F_{q^{2w}}$，扩域 $F_q(\pi^{u l_{n,2w}})$ 必为中间域 $F_q, F_{q^2}, F_{q^w}, F_{q^{2w}}$ 之一. 据此，我们可以将如上的二项因式 $x^t - \pi^{u l_{n,2w}}$ 分为 4 类：S_1, S_2, S_w, S_{2w}，其中

$$S_i = \{x^t - \pi^{u l_{n,2w}} \mid F_q(\pi^{u l_{n,2w}}) = F_{q^i}\},$$
$$i = 1, 2, w, 2w.$$

Frobenius 自同构 $\sigma: F_{q^{2w}} \to F_{q^{2w}}$，$\pi \mapsto \pi^q$ 在多项式上诱导的作用可以定义等价关系 $\sim$：$f(x) \sim g(x)$ 当且仅当存在某个 $0 \le k \le 2w-1$，使得 $f(x) = g^{\sigma^k}(x)$. 我们分别记 S_2^*，S_w^*，S_{2w}^* 为 S_2, S_w, S_{2w} 在这个等价关系下的商集. 在这种分类下，x^n-1 在 $F_{q^{2w}}$ 上的因式分解为

$$x^n - 1 = \prod_{f(x) \in S_1} f(x) \prod_{g(x) \in S_2^*} g(x) g^\sigma(x) \cdot \prod_{h(x) \in S_w^*} \prod_{k=0}^{w-1} h^{\sigma^k}(x) \prod_{y(x) \in S_{2w}^*} \prod_{k=0}^{2w-1} y^{\sigma^k}(x) \tag{4}$$

根据文献[7]的引理 14 可知，$f(x)$，$g(x)g^\sigma(x)$，$\prod_{k=0}^{w-1} h^{\sigma^k}(x)$，$\prod_{k=0}^{2w-1} y^{\sigma^k}(x)$ 分别是 x^n-1 在 F_q 上的 $t, 2t, wt, 2wt$ 次不可约因式.

下面我们将分类精细刻画这些可约因式. 假设 $t \mid m_{n,2w}$. 我们首先来找出 x^n-1 在 F_q 上的所有 t 次不可约因式和 $2t$ 次不可约因式. 因为 $q^2 \equiv 3 \pmod 4$，$\mathrm{ord}_{\mathrm{rad}(n)}(q^2) = w$，所以根据文献[8]知 x^n-1 在 F_{q^2} 上可分解为一系列 t 次不可约二项式和 wt 次不可约多项式的积

$$\prod_{t \mid m_{n_1,2}} \prod_{\substack{1 \le u \le (n, q^2-1) \\ (u,t)=1}} (x^t - \alpha^{u l_{n,2}}) \prod_{t \mid m_{n,2w}} \prod_{v \in S} \prod_{k=0}^{w-1} (x^t - \pi^{q^{2k} v l_{n,2w}}) \tag{5}$$

其中 S 为满足如下条件的正整数 v 的集合：$1 \le v \le (n, q^{2w}-1)$，$(v,t) = 1$，$\frac{q^{2w}-1}{q^2-1} \nmid v l_{n,2w}$，$v = \min\{v, q^2 v, \cdots, q^{2w-2} v\}_{(n, q^{2w}-1)}$，这里 $\min\{a_1, a_2, \cdots, a_S\}_b$ 表示集合 $\{a_1, a_2, \cdots, a_S\}$ 中元素模 b 的最小非负剩余中的最小者. 根据伽罗瓦理论，若 $\alpha^{u l_{n,2}} \in F_q$，则 $x^t - \alpha^{u l_{n,2}}$ 也是 F_q 上的 t 次不可约因式. 反之，若 $\alpha^{u l_{n,2}} \notin F_q$，则 $(x^t - \alpha^{u l_{n,2}})(x^t - \alpha^{qu l_{n,2}})$ 为 F_q 上的 $2t$ 次不可约因式. 因为 $\alpha^{u l_{n,2}} \in F_q$ 当且仅当 $\alpha^{u l_{n,2}} = \alpha^{qu l_{n,2}}$，由计算可知这相当于 $\frac{(q^2-1, n)}{(q-1, n)} \mid u$. 令 $u = \frac{(q^2-1, n)}{(q-1, n)} v$. 由 $(u,t) = 1$ 可知 $\left(t, \frac{(q^2-1, n)}{(q-1, n)}\right) = 1$.

为了刻画同时满足 $t \mid m_{n_1,2}$ 和 $\left(t, \frac{(q^2-1, n)}{(q-1, n)}\right) = 1$ 这两个限制条件的 t，我们需要

分情况进一步讨论. 与 n 的分解 $n=w^{v_w(n)}n_1n_2$ 一样，由于 $\mathrm{rad}(n_1)\mid q^2-1$，我们有 n_1 的分解

$$n_1=2^{v_2(n_1)}n_{11}n_{12} \tag{6}$$

使得 $\mathrm{rad}(n_{11})\mid(q-1)$，$\mathrm{rad}(n_{12})\mid(q+1)$.

(i) 当 $v_2(n)=0$ 时，因为 $\left(t,\dfrac{(q^2-1,n)}{(q-1,n)}\right)=(t,q+1,n_{12})=1$，所以有 $t\mid m_{n_{11},1}$；

(ii) $v_2(n)\neq 0$ 时，同理有 $t\mid m_{n_{11},1}$.

所以，$x^t-\alpha^{ul_{n,2}}$ 为 x^n-1 在有限域 F_q 上的 t 次不可约二项式当且仅当 $t\mid m_{n_{11},1}$，$u=\dfrac{(q^2-1,n)}{(q-1,n)}v$，$(v,t)=1$，$1\leq v\leq(q-1,n)$. 特别地，此时有 $\alpha^{ul_{n,2}}=\theta^{vl_{n,1}}$. 于是我们找到了 x^n-1 在 F_q 上所有的 t 次不可约因式和 $2t$ 次不可约因式，得到如下两个结论.

引理 2.1　设 w 为奇素数，$\mathrm{ord}_{\mathrm{rad}(n)}(q)=2w$. 若 $t\mid m_{n_{11},1}$，$(t,v)=1$，$1\leq v\leq(q-1,n)$，则 $x^t-\theta^{vl_{n,1}}$ 是 x^n-1 在有限域 F_q 上的 t 次不可约因式.

引理 2.2　设 $t\mid m_{n_1,2}$，集合

$$S_{2,t}=\{1\leq u\leq(q^2-1,n)\mid (u,t)=1,\frac{(q^2-1,n)}{(q-1,n)}\nmid u,\ u=\min\{u,qu\}_{(n,q^2-1)}\} \tag{7}$$

若 $u\in S_{2,t}$，则多项式

$$f_{2,u}(x)=(x^t-\alpha^{ul_{n,2}})(x^t-\alpha^{qul_{n,2}}) \tag{8}$$

是 x^n-1 在有限域 F_q 上的 $2t$ 次不可约因式.

接下来，我们将找出 x^n-1 在 F_q 上所有的 wt 次不可约因式和 $2wt$ 次不可约因式. 根据前文中 x^n-1 在 F_{q^2} 上的因式分解，我们取 $\prod_{k=0}^{w-1}(x^t-\pi^{q^{2k}vl_{n,2w}})$ 为 x^n-1 在 F_{q^2} 上的 wt 次不可约因式. 由伽罗瓦理论，我们知道，若 $\pi^{vl_{n,2w}}\in F_{q^w}$，则 $\prod_{k=0}^{w-1}(x^t-\pi^{q^{2k}vl_{n,2w}})$ 也是 F_q 上的 wt 次不可约因式；反之，若 $\pi^{vl_{n,2w}}\notin F_{q^w}$，则 $\prod_{k=0}^{2w-1}(x^t-\pi^{q^kvl_{n,2w}})$ 为 F_q 上的 $2wt$ 次不可约因式. 因为 $\pi^{vl_{n,2w}}\in F_{q^w}$ 当且仅当 $\pi^{vl_{n,2w}}=\pi^{q^wvl_{n,2w}}$，由计算可知这相当于 $\dfrac{(q^{2w}-1,n)}{(q^w-1,n)}\mid v$. 不妨令 $v=\dfrac{(q^{2w}-1,n)}{(q^w-1,n)}u'$. 因为 $v\in S$ 满足 $\dfrac{q^{2w}-1}{q^2-1}\nmid vl_{n,2w}$，所以 $\dfrac{(q^w-1,n)}{(q^2-1,n)}\nmid u'$. 另一方面，由 $(v,t)=1$ 可得 $\left(t,\dfrac{(q^{2w}-1,n)}{(q^w-1,n)}\right)=1$.

为了刻画同时满足 $\left(t,\dfrac{(q^{2w}-1,n)}{(q^w-1,n)}\right)=1$ 和 $t\mid m_{n,2w}$ 这两个限制条件的 t，我们需要分情况进一步讨论. 由于 $\mathrm{rad}(n)\mid(q^{2w}-1)$，$(2,q^w-1,q^w+1)=1$，因此 n 有唯一分解式

$$n=2^{v_2(n)}n_3n_4 \tag{9}$$

使得 $\mathrm{rad}(n_3)\mid q^w-1$，$\mathrm{rad}(n_4)\mid(q^w+1)$.

(i) 假设 $q\equiv 1(\mathrm{mod}\ 4)$. 若 $v_2(n)\leq v_2(q^w-1)$，则

$$\left(t,\frac{(q^{2w}-1,n)}{(q^w-1,n)}\right)=(t,q^w+1,n_b)=1,$$

因此 $t\mid m_{n_3,w}$. 若 $v_2(n)\geq v_2(q^{2w}-1)$，同理有 $t\mid m_{n_3,w}$；

(ii) 若 $q\equiv 3(\mathrm{mod}\ 4)$，同理有 $t\mid m_{n_3,w}$.

所以，$\prod_{k=0}^{w-1}(x^t-\pi^{q^{2k}vl_{n,2w}})$ 为 x^n-1 在有限域 F_q 上的 wt 次不可约多项式当且仅当 $t\mid m_{n_3,w}$，$v=\dfrac{(q^{2w}-1,n)}{(q^w-1,n)}u'$，$1\leq u'\leq(n,q^w-1)$，$(u',t)=1(u,t)=1$，$\dfrac{(q^w-1,n)}{(q^2-1,n)}\nmid u'$. 特别地，此时有 $\pi^{vl_{n,2w}}=\beta^{u'l_{n,w}}$. 于是我们得到了 x^n-1 在 F_q 上所有的 wt 次不可约因式和 $2wt$ 次不可约因式，从而得到

引理 2.3　设 $t\mid m_{n_3,w}$，集合

$$S_{w,t}=\{1\leq u'\leq(q^w-1,n)\mid (u',t)=1,\frac{(q^w-1,n)}{(q-1,n)}\nmid u',\ u'=\min\{u',qu',\cdots,q^{w-1}u'\}_{(n,q^w-1)}\} \tag{10}$$

若 $u'\in S_{w,t}$，则多项式

$$f_{w,u'}(x)=\prod_{k=0}^{w-1}(x^t-\beta^{q^ku'l_{n,w}}) \tag{11}$$

是 x^n-1 在有限域 F_q 上的 wt 次不可约因式.

引理 2.4　设 $t\mid m_{n,2w}$，集合

$$S_{2w,t}=\{1\leq v'\leq(q^{2w}-1,n)\mid (v',t)=1,\frac{(q^{2w}-1,n)}{(q^w-1,n)}\nmid v',\frac{(q^{2w}-1,n)}{(q^2-1,n)}\nmid v',\ v'=\min\{v',qv',\cdots,q^{2w-1}v'\}_{(n,q^{2w}-1)}\} \tag{12}$$

若 $u'\in S_{2w,t}$，则多项式

$$f_{2w,v'}(x)=\prod_{k=0}^{2w-1}(x^t-\pi^{q^kv'l_{n,2w}}) \tag{13}$$

是 x^n-1 在有限域 F_q 上的 $2wt$ 次不可约因式.

将前面的 4 个引理整合起来，我们便得到了 x^n-1 在有限域 F_q 上的精细分解. 沿用引理 2.1 至引理 2.4 的记号，我们的主要结论是

定理 2.5　设 w 为奇素数，$\mathrm{ord}_{\mathrm{rad}(n)}(q)=2w$，那么 x^n-1 在有限域 F_q 中的因式分解为

$$x^n-1=\prod_{\substack{t\mid m_{n_{11},1}\\ 1\leq v\leq(q-1,n)\\ (v,t)=1}}(x^t-\theta^{vl_{n,1}})\cdot$$

$$\left(\prod_{t\mid m_{n_1,2}}\prod_{u\in S_{2,t}} f_{2,u}(x)\right)\cdot$$
$$\left(\prod_{t\mid m_{n_3,w}}\prod_{u'\in S_{w,t}} f_{w,u'}(x)\right)\cdot$$
$$\left(\prod_{t\mid m_{n,2w}}\prod_{v'\in S_{2w,t}} f_{2w,v'}(x)\right) \tag{14}$$

其中集合 $S_{2,t}$, $S_{w,t}$, $S_{2w,t}$ 分别由式(7),(10),(12)定义, $x^t-\theta^{vl_{n,1}}$, $f_{2,u}(x)$, $f_{w,u'}(x)$, $f_{2w,v'}(x)$ 均为 F_q 上的不可约多项式.

我们的定理推广了[6]和[8]中的相关结论.

3 实 例

下面给出利用我们主要定理的结论来分解多项式的例子.

例 3.1 设 $\theta=2\in F_5$, α 为 F_5 上不可约多项式 x^2-3 的根, π 为 F_5 上不可约多项式 $x^6+2x^5-x^4+3x^3+x^2+2x-1$ 的根. 构造 $F_{5^2}=F_5(\alpha)$, $F_{5^6}=F_5(\pi)$. 可以验证, θ,α,π 分别为 F_5^*, F_{25}^*, F_{15625}^* 的生成元,且 $\alpha^6=\pi^{3906}=\theta=2$.

因为 $\mathrm{ord}_{\mathrm{rad}(42)}(5)=6$,由我们的定理可以得到 $x^{42}-1$ 的完全分解式为

$$\begin{aligned}x^{42}-1=&\\&(x-\theta^2)(x-\theta^4)((x-\alpha^4)(x-\alpha^{20}))\\&((x-\alpha^8)(x-\alpha^{16}))\cdot\\&\left(\prod_{k=0}^{5}(x-\pi^{372\cdot 5^k})\right)\left(\prod_{k=0}^{5}(x-\pi^{744\cdot 5^k})\right)\cdot\\&\left(\prod_{k=0}^{5}(x-\pi^{1116\cdot 5^k})\right)\cdot\\&\left(\prod_{k=0}^{5}(x-\pi^{1488\cdot 5^k})\right)\left(\prod_{k=0}^{5}(x-\pi^{2232\cdot 5^k})\right)\cdot\\&\left(\prod_{k=0}^{5}(x-\pi^{4092\cdot 5^k})\right).\end{aligned}$$

这个分解式中有两个 1 次不可约因式,两个 2 次不可约因式,6 个 6 次不可约因式. 经过化简,我们得到 $x^{42}-1$ 在有限域 F_5 上的不可约因式分解为:

$$\begin{aligned}x^{42}-1=&\\&(x+1)(x-1)(x^2+x+1)(x^2-x+1)\cdot\\&(x^6+2x^4+2x^3+2x^2+1)\cdot\\&(x^6+2x^4+3x^3+2x^2+1)\cdot\\&(x^6+x^5+x^4+x^3+x^2+x+1)\cdot\\&(x^6-x^5+x^4-x^3+x^2-x+1)\cdot\\&(x^6+4x^5+3x^4+x^3+3x^2+4x+1)\cdot\\&(x^6+x^5+3x^4+4x^3+3x^2+x+1).\end{aligned}$$

参考文献:

[1] Meyn H. Factorization of the cyclotomic polynomials $x^{2^n}+1$ over finite fields [J]. Finite Fields Th App, 1996, 2: 439.

[2] Fitzgerald R W, Yucas J L. Explicit factorization of cyclotomic and Dickson polynomials over finite fields, arithmetic of finite [J]. Lect Notes Comput Sci, 2007, 4547: 1.

[3] Wang L, Wang Q. On explicit factors of cyclotomic polynomials over finite fields [J]. Design Code Cryptogr, 2012, 63: 87.

[4] Tuxanidy A, Wang Q. Composed products and factors of cyclotomic polynomials over finite fields [J]. Design Code Cryptogr, 2013, 69: 203.

[5] Chen B, Li L, Tuerhong R. Explicit factorization of $x^{2^m p^n}-1$ over a finite field [J]. Finite Fields Th App, 2013, 24: 95.

[6] Martinez F, Vergara C, Oliverira L. Explicit factorization of $x^n-1\in F_q[x]$ [J]. Design Code Cryptogr, 2015, 77: 277.

[7] Wu H, Zhu L, Feng R, *et al*. Explicit factorizations of cyclotomic polynomials over finite fields [J]. Design Code Cryptogr, 2016, 83: 197.

[8] Wu Y, Yue Q, Fan S. Further factorization of x^n-1 over a finite field [J]. arXiv: 1710.07943v1.

[9] Blake I F, Gao S, Mullin R C. Explicit factorization of $x^{2^k}+1$ over $F_q[x]$ with $p\equiv 3(\mathrm{mod}\ 4)$ [J]. Appl Algebra Eng Commun Comput, 1993, 4: 89.

[10] Lidl R, Niederreiter H. Finite fields [M]. New York: Addision-Wesley, 1983.

[11] 潘嘉堃, 张起帆. 有限交换环上的多项式置换群 [J]. 四川大学学报: 自然科学版, 2016, 53: 275.

引用本文格式:

中 文: 唐睿, 彭国华. 多项式 x^n-1 在有限域上的分解 [J]. 四川大学学报: 自然科学版, 2019, 56: 13.

英 文: Tang R, Peng G H. Factorization of the polynomial x^n-1 over the finite field F_q [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 13.