

# 有限域上插值多项式的两种构造方法

叶俊, 苏跃斌

(四川理工学院理学院, 四川 自贡 643000)

**摘要:** 在实数域上构造插值多项式, 由于计算机精度的限制和存在舍入误差与截断误差, 会使构造的插值多项式产生很大的误差。因此文章将问题限制在有限域上, 给出了有限域上存在唯一的插值多项式的定理, 且对定理进行了严格的证明。同时将 Lagrange 插值法与 Newton 插值法推广到有限域上, 形成有限域上构造插值多项式的两种方法, 最后通过算例验证了此方法的正确性。

**关键词:** Lagrange 插值多项式; Newton 插值多项式; 有限域; 存在; 唯一

**中图分类号:** TP309

**文献标识码:** A

## 引言

用多项式算子来逼近函数是数值逼近中十分有效的工具<sup>[1-3]</sup>。多项式插值用多项式对一组给定数据进行插值的过程, 换句话说就是, 对于一组给定的数据(如来自于采样的数据), 寻找一个恰好通过这些数据点的多项式, 即解决以下问题: 已知自变量  $x_0 < x_1 < \dots < x_n$  和它们的对应变量的值  $y_0, y_1, \dots, y_n$ , 求一个唯一的次数不超过  $n$  的多项式  $f(x)$ , 使得  $f(x_i) = y_i, i = 0, 1, \dots, n$ 。在文献[4]中有详细的定理和证明。

Lagrange 插值多项式与 Newton 插值多项式在数值逼近中更占有重要的地位, 虽然 Newton 和 Lagrange 插值多项式在表达的形式上是不同的, 两者其实是相同的同一个多项式, 而且, Lagrange 插值多项式可以直接从 Newton 插值多项式得到<sup>[5]</sup>, 但是两者并非对于任意的连续函数都一致收敛<sup>[6]</sup>。对此, Bernstein<sup>[7]</sup>提出了一类改进方法, 文献[8-9]给出了一些有意义的研究成果。

以上理论均建立在实数域基础上的, 在实数域上构造插值多项式在理论上是可行的, 但是在实际操作中, 由于计算机的精度限制和舍入误差与截断误差, 往往造成构造的插值多项式误差太大。

为了使构造的插值多项式在任何情况下都收敛, 且避免由计算机自身的问题所造成多项式的误差, 本文将论域限制在有限域上, 从而可以构造出在任何计算环境

下都没有误差的插值多项式, 并且结合 Lagrange 插值多项式与 Newton 插值多项式给出了在有限域上构造插值多项式的两种方法。

## 1 有限域上存在唯一插值多项式的定理及证明

**定理 1** 给定  $(x_1, y_1), (x_2, y_2) \dots (x_n, y_n), x_i \in F_p, y_i \in F_p, 1 \leq i \leq n$  且  $x_i \neq x_j, 1 \leq i < j \leq n$ , 则在有限域  $Z_p$  上通过  $(x_1, y_1), (x_2, y_2) \dots (x_n, y_n)$  的插值多项式  $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$  是存在且唯一的。

**证明** 将  $n+1$  个点  $(x_i, y_i), i = 0, 1, \dots, n$  代入多项式, 可得线性方程组

$$\begin{cases} a_0 + a_1x_0 + \dots + a_nx_0^n = y_0 \pmod{p} \\ a_0 + a_1x_1 + \dots + a_nx_1^n = y_1 \pmod{p} \\ \dots \\ a_0 + a_1x_n + \dots + a_nx_n^n = y_n \pmod{p} \end{cases}$$

及证明  $a_0, a_1, \dots, a_n$  存在且唯一并且  $a_i \in Z_p, i = 0, 1, \dots, n$  即可。

其系数行列式  $d = \begin{vmatrix} 1 & x_0 & \dots & x_0^n \\ 1 & x_1 & \dots & x_1^n \\ \dots & \dots & \dots & \dots \\ 1 & x_n & \dots & x_n^n \end{vmatrix}$  是范德蒙行列

式且  $x_i \neq x_j, i \neq j$  则  $d \neq 0$  由克莱姆法则知系数  $a_0$

$a_1, \dots, a_n$  存在且唯一,  $a_i = \frac{d_i}{d} \text{mod } p$  其中

$$d_i = \begin{vmatrix} \text{第 } i \text{ 列} \\ 1 & x_0 & \dots & y_0 & x_0^n \\ 1 & x_1 & \dots & y_1 & x_1^n \\ & & \dots & & \\ 1 & x_n & \dots & y_n & x_n^n \end{vmatrix}$$

只需证  $a_i \in Z/p, i = 0, 1, \dots, n$  即可。

由于是在有限域  $Z/p$  内的计算, 设  $Z/p$  的生成元为  $g$ , 则  $\forall x_i \in Z/p, x_i \neq 0 \exists m_i \in Z/p$ , 使得  $x_i = g^{m_i}$ , 又因为  $d \neq 0$  则  $d \text{mod } p$  可以表示成生成元的某个次方, 即

$\exists s \in Z/p$  使得  $d \text{mod } p = g^s$ . 而  $\frac{1}{d} = g^{-s} = (g^s)^{-1}$ , 即  $g^s$

得逆元, 因此  $a_i = \frac{d_i}{d} \text{mod } p = [(d_i \text{mod } p) \cdot (g^s)^{-1}] \text{mod } p \in$

$Z/p$ , 即定理 1 得证。

### 2 有限域上的 Lagrange 插值多项式

在实数域上构造 Lagrange 插值多项式已经是非常容易的事情了, 文献 [10] 提出了 lagrange 插值多项式的一种快速算法, 但是由于计算机精度的限制, 所构造的插值多项式存在一定的误差, 很多时候都不能通过检验。为此我们将 Lagrange 插值多项式的构造推广到有限域上, 构造一个有限域  $Z_p$  上的次数不超过  $n-1$  的 Lagrange 插值多项式  $f(x)$ ,

$$f(x) = \sum_{k=1}^{n-1} y_k \prod_{i=1, i \neq k}^{n-1} \frac{(x - x_i)}{(x_k - x_i)} \text{mod } p$$

即

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$$

其中,  $a_i \in F_p (i = 0, 1, 2, \dots, n-1)$ , 且  $f(x_i) = y_i (i = 1, 2, \dots, n)$ 。

### 3 有限域上的 Newton 插值多项式

拉格朗日插值的优点是插值多项式特别容易建立, 缺点是增加节点时原有多项式不能利用, 必须重新建立, 即所有基函数都要重新计算, 这就造成计算量的浪费。而 Newton 插值多项式是代数插值的另一种表现形式, 当增加节点时它具有所谓的“承袭性”, 即在增加节点时已构造的插值多项式可以继续使用, 只需加上一项新的多项式即可。文献 [11] 也给出了一些 Newton 插值多项式的快速算法。

在  $Z_p$  上构造次数不超过  $n-1$  的 Newton 插值多项式  $f(x)$ ,

$$f(x) = f(x_0) + f[x_0, x_1](x - x_0) +$$

$$f[x_0, x_1, x_2](x - x_0)(x - x_1) + \dots + f[x_0, x_1, \dots, x_{n-1}](x - x_0)(x - x_1) \dots (x - x_{n-2}) + f[x_0, x_1, \dots, x_n](x - x_0)(x - x_1) \dots (x - x_{n-1}) \text{mod } p$$

其中,

$$f[x_0, x_1, \dots, x_n] = \sum_{i=0}^n \frac{f(x_i)}{(x_i - x_0) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_n)} \text{mod } p$$

### 4 算例

如在  $Z/7$  中, 过点  $(1, 2), (2, 6), (4, 5)$ , 按照上述方法求得  $a_0 = 2, a_1 = 5, a_2 = 2$  即插值多项式为  $f(x) = 2 + 5x + 2x^2$ 。

在  $Z/7$  中, 过点  $(1, 5), (2, 3), (3, 1), (4, 6), (5, 2)$ , 按照上述方法求得  $a_0 = 5, a_1 = 1, a_2 = 0, a_3 = 2, a_4 = 4$  即插值多项式为  $f(x) = 5 + 1x + 2x^3 + 4x^4$ 。

在  $Z/17$  中, 过点  $(1, 2), (2, 5), (3, 6), (4, 11)$  按照上述方法求得  $a_0 = 8, a_1 = 0, a_2 = 10, a_3 = 1$  即插值多项式为  $f(x) = 8 + 10x^2 + 1 \cdot x^3$ 。

### 5 结束语

本文首先说明了插值多项式并非对任意的连续函数都收敛, 并且指出由于计算机精度的限制以及舍入误差与截断误差会使在实数域上构造的插值多项式出现很大的误差。为了避免误差的产生, 本文将问题限制在有限域上, 并且给出了有限域上存在唯一的插值多项式的一个定理, 且对此定理进行了严格的证明, 同时将 Lagrange 插值法与 Newton 插值法推广到有限域上来构造有限域上的插值多项式, 给出了有限域上构造插值多项式的两种方法。最后通过算例验证了定理的正确性。此结论得到的插值多项式克服了在实数域上由于计算机的精度和舍入误差与截断误差所产生的误差, 此插值多项式是一个精确的多项式, 在任何计算环境下都不会有任何的误差, 在密码学领域有着很好的用途。

### 参考文献:

[1] 刘强, 袁学刚. 关于 Lagrange 插值多项式的收敛性 [J]. 大连民族学院学报, 2007, 40(5): 128-129.

[2] 余海洋, 方世跃. 关于勒让德多项式递推公式的研究 [J]. 四川理工学院学报: 自然科学版, 2008, 21(4): 1-4.

[3] 孙慧娟, 赵小香. 有关雅可比多项式一些性质的研究 [J]. 四川理工学院学报: 自然科学版, 2009, 22(6): 37-41.

[4] 赵武超, 许文超. 插值多项式的存在性和唯一性 [J]. 洛阳师范学院学报, 2008, 29(2): 17-18.

[5] 凌征球. 函数逼近中的 Newton 和 Lagrange 插值多项式

- [ J]. 大学数学, 2006, 22( 5): 102-106
- [ 6] V am a A K. A new proof of A. E. T in an' s approximation theorem [ J]. Journal of Approx Theory, 1976( 18): 57-62
- [ 7] 沈燮昌. 多项式插值 ( I ) — Lagrange 插值 [ J]. 数学进展, 1983, 12( 12): 193-214
- [ 8] 袁学刚, 何甲兴. 关于  $|$  类插值多项式的最高收敛阶 [ J]. 工程数学学报, 2001, 18( 3): 117-120
- [ 9] Yuan Xue gang W ei Ping. On two revised nodes of S. N. Bernstein interpolation process [ J]. Le Mat em atic he, 2001 ( 17): 39-48
- [ 10] 林鹭, 黄旭东. 拉格朗日插值多项式的  $|$  种并行算法 [ J]. 厦门大学学报: 自然科学版, 2004, 43( 5): 592-595
- [ 11] 盛中平, 王晓辉, 孙雪楠. 多点多重 Newton 型插值公式 [ J]. 东北师大学报: 自然科学版, 2007, 40( 2): 136-137

## Two Construction Methods of Interpolation Polynomial in Finite Field

YE Jun<sup>1,2</sup>, SU Yue-bin<sup>1</sup>

(1. School of Science, Sichuan University of Science & Engineering, Zigong 643000, China)

2. School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin 541004, China)

**Abstract** Interpolation polynomials established in real number field may bring large error because of the accuracy limitations, rounding error and truncation error of computers. Problems of interpolation polynomials is considered in finite field in this paper; a theorem about the existence and uniqueness of interpolation polynomial in finite field is proposed, and then the theorem is proved strictly. Then two construction methods to gain the interpolation polynomials in finite field is also proposed by extending Lagrange interpolation and Newton interpolation to the finite field. At last, some examples are given to verify the correctness of the two methods.

**Key words** Lagrange interpolation polynomial; Newton interpolation polynomial; finite field; existence; uniqueness

(上接第 520 页)

## On the Diophantine Equation $x^3 \pm 1 = Dy^2$

LIANG Yong, HAN Yun-na

(Department of Mathematics, Northwest University, Xi'an 710127, China)

**Abstract** Using the properties of congruence, Legendre symbol and some other methods in number theory, the solutions of Diophantine equation  $x^3 \pm 1 = Dy^2$  are investigated, where  $D$  is square-free positive integer,  $D = D_1 p$ ,  $D_1$  cannot be divided by the prime number 3 or  $6k + 1$ , and  $p$  is an odd prime,  $p = 3(12r + 7)(12r + 8) + 1$ ,  $r$  is a positive integer. We prove that if  $D_1 \equiv 7 \pmod{12}$ , the equation  $x^3 + 1 = Dy^2$  has no positive integer solution, and if  $D_1 \equiv 5, 8 \pmod{12}$ , the  $x^3 - 1 = Dy^2$  has no positive integer solution.

**Key words** Diophantine equation; congruence; positive integer solution; Legendre symbol