2019 年 1 月 四川大学学报(自然科学版) Jan. 2019
第 56 卷 第 1 期 Journal of Sichuan University (Natural Science Edition) Vol. 56 No. 1

doi：10.3969/j.issn.0490-6756.2019.01.006

剩余类环上多项式的同余性质

朱朝熹[1]，李 懋[2]，谭千蓉[3]

(1. 四川大学数学学院，成都 610064；2. 西南大学数学与统计学院：重庆 400715；
3. 攀枝花学院数学与计算机学院，攀枝花 617000)

摘 要：设 $\mathbf{Z}/p^n\mathbf{Z}$ 是模 p^n 剩余类环. 本文证明了 $U=\{f(x)\in\mathbf{Z}/p^n\mathbf{Z}[x]\mid f(a)\equiv 0(\bmod p^n), \forall a\in\mathbf{Z}\}$ 是自由生成的 $\mathbf{Z}/p^n\mathbf{Z}$-模，给出了它的一组基，还证明了商环 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 是有限环，并通过这组基确定了商环 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 中的元素个数.

关键词：剩余类环；理想；商环；阶

中图分类号：O156.1 **文献标识码**：A **文章编号**：0490-6756(2019)01-0021-04

Congruence properties of polynomials over residue class ring

ZHU Chao-Xi[1], *LI Mao*[2], *TAN Qian-Rong*[3]

(1. School of Mathematics, Sichuan University, Chengdu 610064, China;
2. School of Mathematics and Statistics, Southwest University, Chongqing 400715, China;
3. School of Mathematics and Computer Science, Panzhihua University, Panzhihua 617000, China)

Abstract: Let $\mathbf{Z}/p^n\mathbf{Z}$ be the residue ring of module p^n. In this paper, we prove that $U=\{f(x)\in\mathbf{Z}/p^n\mathbf{Z}[x]\mid f(a)\equiv 0(\bmod p^n)\ \forall a\in\mathbf{Z}\}$ is a free generated $\mathbf{Z}/p^n\mathbf{Z}$-module. Consequently, we get a basis of U. Furthermore, we show that the quotient ring $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ is finite, and obtain a formula for the number of elements in $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$.

Keywords: Residue class ring; Ideal; Quotient ring; Order
(2010 MSC 11R09, 11R04)

1 引 言

在本文中，我们主要研究模 p^n 剩余类环 $\mathbf{Z}/p^n\mathbf{Z}$ 上多项式的个数问题[1-9]. 为了使计数有意义，我们视 $f(x)$ 和 $g(x)$ 为同一个多项式，如果 $f(x)$ 和 $g(x)$ 满足同余关系式 $f(a)\equiv g(a)(\bmod p^n), \forall a\in\mathbf{Z}/p^n\mathbf{Z}$. 为此，我们首先刻画 $\mathbf{Z}/p^n\mathbf{Z}[x]$ 以及它的零化多项式构成的理想 $U=\{f(x)\mid f(a)\equiv 0(\bmod p^n)\}$ (按理想定义即可证明 U 是 $\mathbf{Z}/p^n\mathbf{Z}[x]$ 的理想)，即 $U=\{f(x)\mid f(a)\equiv 0(\bmod p^n)\}$ 中的多项式诱导的从 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 到自身的映射全是零映射. 进而我们再考虑商环 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 的结构. 商环 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 的阶是有限的，因为从 $\mathbf{Z}/p^n\mathbf{Z}$ 到 $\mathbf{Z}/p^n\mathbf{Z}$ 的不同映射的个数不超过 p^{np^n}，并且每一个 $\mathbf{Z}/p^n\mathbf{Z}$ 上的多项式都直接诱导了一个 $\mathbf{Z}/p^n\mathbf{Z}$ 到自身的映射，商环中不同多项式诱导的映射不同，从而商环 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 的阶有限.

我们将证明 U 有一组生成元，进而 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 是一个有限生成 $\mathbf{Z}/p^n\mathbf{Z}$-模[1]，从而它存在一组基，使得它的任意元素均可用这一组基 $\mathbf{Z}/p^n\mathbf{Z}$-线性表示.

收稿日期：2018-04-18
基金项目：国家自然科学基金(11771304)；中央高校基本科研业务费专项基金
作者简介：朱朝熹(1992－)，男，重庆璧山人，博士研究生，主要研究方向为数论. E-mail：925011806@qq.com
通讯作者：李懋. E-mail：limao@swu.edu.cn

2 主要结果

我们首先给出一些基本定义.

定义 2.1 设 p 为素数,n 为正整数. 我们用 $\mathbf{Z}/p^n\mathbf{Z}$ 表示模 p^n 的剩余类环,$\mathbf{Z}/p^n\mathbf{Z}[x]$ 表示剩余类环上的多项式全体.

定义 2.2 对于任意 $r\in\mathbf{Q}$,若 $r=p^a\cdot\frac{c}{b}$,其中 $a,b,c\in\mathbf{Z}$ 且 $\gcd(p,bc)=1$,那么定义 $v_p(r):=a$.

关于赋值的更多内容,参见文献[6].

定义 2.3 算术函数 $\mu_p:\mathbf{Z}^+\to\mathbf{N}$ 定义如下:对任意正整数 n,有

$$\mu_p(n)=\min\{m\geqslant 0\mid v_p(m!)\geqslant n\}.$$

定义 2.4 对任意正整数 k,定义 $x^{\langle k\rangle}:=x(x-1)\cdots(x-k+1)$.

定义 2.5 定义 $\mathbf{Z}/p^n\mathbf{Z}[x]$ 中的零化多项式构成集合为

$$U:=\{f(x)\in\mathbf{Z}/p^n\mathbf{Z}[x]\mid f(a)\equiv 0(\bmod p^n),\ \forall a\in\mathbf{Z}\}.$$

现在我们叙述本文的主要结果.

定理 2.6 U 是自由 $\mathbf{Z}/p^n\mathbf{Z}$-模,并且 $\{p^{n-v_p(k!)}x^{\langle k\rangle}\mid 0\leqslant k\langle\mu_p(n)\}\cup\{x^{\langle k\rangle}\mid k\geqslant\mu_p(n)\}$ 是 U 的一组基.

定理 2.7 对任意 $\overline{f(x)}\in(\mathbf{Z}/p^n\mathbf{Z}[x])/U$,$\overline{f(x)}$ 可以唯一地表示成如下形式:

$$\overline{f(x)}=a_0+a_1\overline{x^{\langle 1\rangle}}+\cdots+a_{\mu_p(n)-1}\overline{x^{\langle\mu_p(n)-1\rangle}},$$

其中对于整数 k,

$$0\leqslant k\leqslant\mu_p(n)-1,a_k\in\mathbf{Z}/p^{n-v_p(k!)}\mathbf{Z}.$$

从而 $(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 是一个有限环,并且

$$|(\mathbf{Z}/p^n\mathbf{Z}[x])/U|=p^{\sum_{k=1}^{n}\mu_p(k)}.$$

3 定理的证明

在本节中,我们证明定理 2.6 和定理 2.7. 为此我们先证明一个引理.

引理 3.1 对任意正整数 n,我们有如下等式:

$$\sum_{k=0}^{\mu(n)-1}(n-v_p(k!))=\sum_{k=1}^{n}\mu_p(k).$$

证明 设

$$L_n:=\sum_{k=0}^{\mu_p(n)-1}(n-v_p(k!)),R_n:=\sum_{k=1}^{n}\mu_p(k).$$

我们对 n 作归纳法.

首先,显然有 $L_1=R_1$.

假设对于正整数 n 情形有 $L_n=R_n$. 下面考虑 $n+1$ 的情形. 由于 $\mu_p(n+1)-\mu_p(n)=0$ 或 p,因此我们分两种情况证明.

情形 1. $\mu_p(n)=\mu_p(n+1)$. 此时我们有

$$L_{n+1}=\sum_{k=0}^{\mu_p(n+1)-1}(n+1-v_p(k!))=\sum_{k=0}^{\mu_p(n)-1}(n+1-v_p(k!))=L_n+\mu_p(n).$$

另一方面,显然有 $R_{n+1}-R_n=\mu_p(n+1)$. 所以

$$R_{n+1}=R_n+\mu_p(n+1)=R_n+\mu_p(n).$$

于是,由归纳假设立即可知 $L_{n+1}=R_{n+1}$.

情形 2. $\mu_p(n)+p=\mu_p(n+1)$. 此时不难看出

$$L_{n+1}-L_n=\mu_p(n)+pn+p-\sum_{k=\mu_p(n)}^{\mu_p(n+1)-1}v_p(k!)=\mu_p(n)+pn+p-pn=\mu_p(n)+p.$$

上式中

$$v_p(k!)=n,\mu_p(n)\leqslant k\leqslant\mu_p(n+1)-1.$$

由 $\mu(n)$ 定义可知 $v_p(k!)\geqslant n$. 如果 $v_p(k!)\geqslant n+1$,那么 $k\geqslant\mu_p(n+1)$. 矛盾. 从而

$$v_p(k!)=n.$$

所以

$$L_{n+1}=L_n+\mu_p(n)+p.$$

另一方面,因为

$$\mu_p(n)+p=\mu_p(n+1),$$

所以

$$R_{n+1}=R_n+\mu_p(n+1)=R_n+\mu_p(n)+p.$$

故由归纳假设有 $L_{n+1}=R_{n+1}$,即对于 $n+1$ 情形,引理 3.1 成立. 证毕.

定理 2.6 的证明 设

$$S=\{p^{n-v_p(k!)}x^{\langle k\rangle}:0\leqslant k<\mu_p(n)\}\cup\{x^{\langle k\rangle}:k\geqslant\mu_p(n)\}.$$

首先证明 $S\subset U$. 考虑如下两种情形.

情形 1. $0\leqslant k<\mu(n)$. 对于任意 $x\in\mathbf{Z}_p$,有

$$v_p(p^{n-v_p(k!)}x^{\langle k\rangle})=n-v_p(k!)+v_p(x^{\langle k\rangle})=n-v_p(k!)+v_p(\binom{x}{k}k!).$$

由于对任意 $x\in\mathbf{Z}_p$,总有 $\binom{x}{k}\in\mathbf{Z}_p$(见文献[6]),所以 $v_p(\binom{x}{k})\geqslant 0$. 那么

$$n-v_p(k!)+v_p(\binom{x}{k}k!)\geqslant n-v_p(k!)+v_p(k!)=n.$$

这就是说,若 $x\in\mathbf{Z}_p$,则

$$p^{n-v_p(k!)}x^{\langle k\rangle}\equiv 0(\bmod p^n).$$

从而 $p^{n-v_p(k!)}x^{\langle k\rangle}\in U$.

情形 2. $k\geqslant\mu_p(n)$. 由 $\mu(n)$的定义可以推得

$$v_p(x^{\langle k\rangle})=v_p(\binom{x}{k}k!)\geqslant v_p(k!)\geqslant v_p((\mu_p(n))!)\geqslant n.$$

从而 $x^{\langle k\rangle}\in U$. 这就完成了 $S\subset U$ 的证明.

下面我们证明任意 $f(x)\in U$ 均可以唯一地写成S 中元素的 $\mathbf{Z}$-线性组合.

任取 $f(x)\in U$. 可设

$$f(x)=a_0+a_1x+\cdots+a_kx^k,a_i\in\mathbf{Z}/p^n\mathbf{Z}.$$

由于对任意 $j\in\mathbf{N}^*$，多项式 $x^{\langle j\rangle}$都是首项系数为 1 的 j 次多项式，所以存在 $b_i\in\mathbf{Z}/p^n\mathbf{Z}$，$0\leqslant i\leqslant k$，使得 $f(x)=b_0+b_1x^{\langle 1\rangle}+\cdots+b_kx^{\langle k\rangle}$.

当 $k\geqslant\mu_p(n)$时，由上述已证结果可知 $b_kx^{\langle k\rangle}\in U$. 如下我们设 $0\leqslant k\leqslant\mu_p(n)-1$. 下证对任意整数 i，$0\leqslant i\leqslant k$，有

$$v_p(b_i)\geqslant n-v_p(i!).$$

注意到对于任意正整数 $s\geqslant j$，有

$$v_p(j^{\langle j\rangle})=v_p(j!)\leqslant v_p(s^{\langle j\rangle}),$$

从而若有 $b_jj^{\langle j\rangle}\equiv 0(\bmod p^n)$，则有

$$b_js^{\langle j\rangle}\equiv 0(\bmod p^n).$$

于是，令 $x=0$ 有

$$0\equiv f(0)=b_0(\bmod p^n).$$

进而令 $x=1$，由上可推得

$$0\equiv f(1)=b_0+1!\ b_1\equiv b_1(\bmod p^n).$$

再令 $x=2$，我们又可以推得

$$0\equiv f(2)=b_0+b_12^{\langle 1\rangle}+b_22^{\langle 2\rangle}\equiv b_22^{\langle 2\rangle}(\bmod p^n).$$

如此继续下去. 最后我们令 $x=i$，则由上述同余式我们可以推得

$$0\equiv f(i)=b_0+i^{\langle 1\rangle}b_1+b_2i^{\langle 2\rangle}+\cdots+i^{\langle i-1\rangle}b_{i-1}+i^{\langle i\rangle}b_i\equiv i^{\langle i\rangle}b_i=i!\ b_i(\bmod p^n).$$

因此，对于任意的整数 i，$0\leqslant i\leqslant\mu_p(n)-1$，我们有

$$v_p(b_i)\geqslant n-v_p(i!).$$

故可设

$$b_i=\bar{b}_ip^{n-v_p(i!)},$$

其中 $\bar{b}_i\in\mathbf{Z}/p^n\mathbf{Z}$. 于是

$$b_ix^{\langle i\rangle}=\bar{b}_ip^{n-v_p(i!)}x^{\langle i\rangle}.$$

从而 $f(x)$可以表为 S 中的元素的 $\mathbf{Z}/p^n\mathbf{Z}$-线性组合. 所以 S 是 U 的一组 $\mathbf{Z}/p^n\mathbf{Z}$-基.

下面再证 U 是自由 $\mathbf{Z}/p^n\mathbf{Z}$-模. 首先，$\mathbf{Z}/p^n\mathbf{Z}$ 是一个幺环，且 U 是一个加法交换群. 对任意 $a\in\mathbf{Z}/p^n\mathbf{Z}$ 以及 $f(x)\in U$，定义映射$(a,f(x))=\alpha af(x)$. 则这样的映射显然满足两个分配率以及结合律，且 $1f(x)=f(x)$. 所以 U 是一个 $\mathbf{Z}/p^n\mathbf{Z}$-模. 并且由前面的证明可知，S 为 U 的一非空子集，且 U 中多有元素可由 $S\mathbf{Z}/p^n\mathbf{Z}$-线性表示. 所以 U 是自由 $\mathbf{Z}/p^n\mathbf{Z}$-模[1]. 综上所述，定理得证.

定理 2.7 的证明　由定理 2.1 知，U 是自由 $\mathbf{Z}/p^n\mathbf{Z}$-模，并且它有一组生成元$\{p^{n-v_p(k!)}x^{\langle k\rangle}\mid 0\leqslant k\langle\mu_p(n)\}\cup\{x^{\langle k\rangle}\mid k\geqslant\mu_p(n)\}$.

首先，由于 $x^{\langle i\rangle}$，$i\in\mathbf{N}$ 是首项系数为 1 的 i 次多项式，从而 $\mathbf{Z}/p^n\mathbf{Z}[x]$中所有多项式都可由 $x^{\langle i\rangle}$，$i\in\mathbf{N}$ 通过 $\mathbf{Z}$ 线性组合表示. 另一方面，假设

$$f(x)=b_0+b_1x+\cdots+b_kx^k.$$

当 $k\geqslant\mu(n)$时，我们有

$$f(x)+U=f(x)-b_kx^{\langle k\rangle}+U.$$

等式右端代表元的次数不超过 $k-1$. 于是总可以假设 $k\leqslant\mu(n)-1$. 若 $b_k\geqslant p^{n-v_p(k!)}$，那么

$$f(x)+U=f(x)-\bar{b}_kx^{\langle k\rangle}+U,$$

其中 $\bar{b}_k$ 为 b_k 在模 $p^{n-v_p(k!)}$剩余系中的代表元. 这样，$f(x)-\bar{b}_kx^{\langle k\rangle}+U$ 的代表元多项式的次数就不超过 k 次. 由归纳法可知 $f(x)$模 U 后的代表元形如

$$f(x)=\overline{f(x)}+U=a_0+a_1\overline{x^{\langle 1\rangle}}+\cdots+a_{\mu(n)-1}\overline{x^{\langle\mu_p(n)-1\rangle}},$$

其中

$$\overline{x^{\langle k\rangle}}=x^{\langle k\rangle}+U,a_k\in\mathbf{Z}/p^{n-v_p(k!)}\mathbf{Z}$$
$$\forall\, 1\leqslant k\leqslant\mu_p(n)-1.$$

由此可知

$$|(\mathbf{Z}/p^n\mathbf{Z}[x])/U|=p^{\sum_{i=0}^{\mu_p(n)-1}(n-v_p(i!))}.$$

由引理 2.6 知

$$|(\mathbf{Z}/p^n\mathbf{Z}[x])/U|=\sum_{k=1}^{n}\mu_p(k).$$

定理证毕.

4　例　子

作为定理 2.6 的应用，在环 $\mathbf{Z}/p^n\mathbf{Z}[x]$中，我们可得到$(\mathbf{Z}/p^n\mathbf{Z}[x])/U$ 中的子环

$$V_k:=\{f(x)\in(\mathbf{Z}/p^n\mathbf{Z}[x])/U\mid f(a+p^k)\equiv f(a)(\bmod p^n),\forall\, a\in\mathbf{Z}/p^n\mathbf{Z}\}$$

的阶. 特别地，在环 $\mathbf{Z}/2^2\mathbf{Z}[x]$中，我们给出如下例子.

例 4.1　对于环$(\mathbf{Z}/2^2\mathbf{Z}[x])/U$，由定理 2.6 可知$(\mathbf{Z}/2^2\mathbf{Z}[x])/U$ 中所有多项式具有如下形式：

$$f(x)=a_0+a_1x+a_2x^{\langle 2\rangle}+a_3x^{\langle 3\rangle},$$

其中 $a_0\in\mathbf{Z}/4\mathbf{Z}$，$a_1\in\mathbf{Z}/4\mathbf{Z}$，$a_2\in\mathbf{Z}/2\mathbf{Z}$，$a_3\in\mathbf{Z}/2\mathbf{Z}$.

若 $f(x)\in V_1$,那么

$$f(x)\equiv f(x+2)(\bmod 4),\ \forall x\in \mathbf{Z}/4\mathbf{Z},$$

也就是该多项式的系数满足同余式

$$a_1+2a_2x+a_2+3a_3x^2\equiv 0(\bmod 2),\ \forall x\in \mathbf{Z}/4\mathbf{Z},$$

即满足同余方程组

$$\begin{pmatrix}1 & 1 & 0\\ 1 & 1 & 1\end{pmatrix}\begin{bmatrix}a_1\\ a_2\\ a_3\end{bmatrix}\equiv 0(\bmod 2),$$

即

$$a_3\equiv 0(\bmod 2),a_1+a_2\equiv 0(\bmod 2).$$

所以,$|V_1|=4\times 4\times 1\times 1=16$. 同理可知 $|V_0|=8$.

最后,由定理 2.7 可知,

$$|V_2|=|(\mathbf{Z}/4\mathbf{Z}[x])/U|=64.$$

参考文献:

[1] Grillet P A, Abstract algebra [M]. Berlin: Springer, 2007.

[2] Hong S F, Additive characters and orthogonal systems of polynomials in several in determinates over residue class rings [J]. Chinese Sci Bull, 1998: 43, 275.

[3] Hong S F, Orthogonal system of multivariate polynomials over the ring $\mathbf{Z}/m\mathbf{Z}$ [J]. J Sichuan Univ: Natu Sci Ed, 1998, 35: 155.

[4] Hong S F. The p-adic proof of Eisenstein's congruence [J]. J Sichuan Univ: Natu Sci Ed, 2000, 37: 829.

[5] Hu S N, Hong S F, Zhao W. The number of rational points of a family of hypersurfaces over finite fields [J]. J Number Theory, 2015, 156: 135.

[6] Koblitz N. p-adic numbers, p-adic analysis, and zeta-functions [M]. Heidelberg: Springer-Verlag, 1984.

[7] Smith H J S. On systems of linear indeterminate equations and congruences [J]. Philos T R Soc A, 1861, 151: 86.

[8] Sun Q. Orthogonal systems of integral linear forms over the ring $\mathbf{Z}/(m)$ [J]. Chinese Ann Math A, 1993: 14: 328.

[9] Sun Q, Wan D Q. Orthogonal systems of polynomials in several in determinates modulo m [J]. J Sichuan Univ: Natu Sci Ed, 1994, 31: 439.

引用本文格式:

中 文:朱朝熹,李懋,谭千蓉. 剩余类环上多项式的同余性质 [J]. 四川大学学报:自然科学版,2019,56:21.

英 文:Zhu C X, Li M, Tan Q R. Congruence properties of polynomials over residue class ring [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 21.