DOI:10.11721/cqnuj20170222

整数模 n 剩余类环上的准导数及分类*

邓　勇
(喀什大学 数学与统计学院,新疆 喀什 844006)

摘要:【目的】整数集 $\mathbf{Z}$ 上的准导数是一个将所有素数映到 1,并满足 Leibnitz 乘积法则的映射。为获得一个相似的数学对象并尝试在完全不同的环境中加深对它的认识。【方法】定义了在整数模 n 的环境下的准导数概念,即 $\mathbf{Z}_n$ 上的准导数是从 $\mathbf{Z}_n$ 到自身的、满足 Leibnitz 乘积法则 $\varphi(xy)=y\varphi(x)+x\varphi(y)$, $\forall x, y\in\mathbf{Z}_n$ 的一个映射 φ。【结果】研究了 $\mathbf{Z}_n$ 上准导数的性质并对 $\mathbf{Z}_n$ 上的所有准导数进行了分类。【结论】将整数集上的准导数概念推广到模整数 n 的剩余类环上,不仅丰富了准导数的内容,且使其成为讨论堆叠素数论各种猜想的一个强有力工具。

关键词:整数模 n; 剩余类环; 准导数
中图分类号:O156.2　　**文献标志码:**A　　**文章编号:**1672-6693(2017)02-0072-04

所谓整数集 $\mathbf{Z}$ 上的"准导数"是定义在 $\mathbf{Z}$ 上的一个函数。此概念虽然很早就已出现,但直到 1961 年,Barbeau 才对它进行了进一步细化[1]。表面上看,整数集上的准导数是用整数的唯一素数分解和微积分的乘积法则定义的简单函数。然而,作为与初等数论中某些最古老的猜想直接相关的"导数"行为,它具有很大的欺骗性[2]。

整数集 $\mathbf{Z}$ 上的准导数是将每一个素数映到 1 且满足 Leibnitz 乘积法则的唯一函数。具体地说,一个整数的准导数是满足如下 3 个条件的一个函数:1) $0'=0$;2) 对任何素数 p,有 $p'=1$;3) 对 $\forall a,b\in\mathbf{Z}$,都有 $(ab)'=a'b+ab'$(Leibnitz 乘积法则)成立。

受文献[1-2]的启发,本文首先在整数模 n 的剩余类环 $\mathbf{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$ 上定义准导数。然后,讨论它的基本性质。最后,对整数模 n 的所有准导数进行分类。

1 $\mathbf{Z}_n$ 上准导数的定义及基本性质

定义 1　设 $\varphi:\mathbf{Z}_n\to\mathbf{Z}_n$,即 φ 是 $\mathbf{Z}_n$ 上的一个映射。若:1) $\varphi(\bar{0})=\bar{0}$;2) 对任何小于等于 n 的素数 p,都有 $\varphi(\bar{p})=\bar{1}$;3) 对 $\forall\bar{x},\bar{y}\in\mathbf{Z}_n$,Leibnitz 乘法则 $\varphi(\bar{x}\cdot\bar{y})=\bar{x}\varphi(\bar{y})+\bar{y}\varphi(\bar{x})$ 成立。则称 φ 是 $\mathbf{Z}_n$ 上的准导数。

引理 1　若 φ 是 $\mathbf{Z}_n$ 上的准导数,则 $\varphi(\bar{0})=\varphi(\bar{1})=\bar{0}$,且对 $\forall\bar{x}\in\mathbf{Z}_n$, $m\geqslant1$,有 $\varphi(\bar{x}^m)=\overline{mx}^{m-1}\varphi(\bar{x})$。

证明　因 φ 是 $\mathbf{Z}_n$ 上的准导数,故由定义可直接验证:$\varphi(\bar{0})=\varphi(\bar{0}\cdot\bar{0})=\bar{0}\varphi(\bar{0})=\bar{0}$。$\varphi(\bar{1})=\varphi(\overline{1\cdot1})=\varphi(\bar{1}\cdot\bar{1})=\bar{2}\varphi(\bar{1})$,两边减去 $\varphi(\bar{1})$,可得 $\varphi(\bar{1})=\bar{0}$。

同理,由准导数的乘积法则和数学归纳法易证,$\varphi(\bar{x}^m)=\overline{m}\,\bar{x}^{m-1}\varphi(\bar{x})$ 成立。　证毕

设 $\bar{a}\in\mathbf{Z}_n$,用 $\bar{a}\mathbf{Z}_n$ 表示 $\mathbf{Z}_n$ 的 $\bar{a}$ 倍,即 $\bar{a}\mathbf{Z}_n=\{\bar{a}\cdot\bar{k}\mid\bar{k}\in\mathbf{Z}_n\}$。例如,$\bar{2}\mathbf{Z}_4=\{\bar{0},\bar{2}\}$。容易验证,表 1 中的每一个 $\varphi_i(i=1,2,3,4)$ 都是 $\mathbf{Z}_4$ 上的准导数。

2 模 2^e 的准导数

设 $e\in\mathbf{Z}^+$。现对 $\mathbf{Z}_{2^e}$ 上的所有准导数进行分类。首先,由引理 1 可知,$\mathbf{Z}_{2^1}$ 上的准导数只有零映射。当 $e=2$ 时,$\mathbf{Z}_{2^2}=\mathbf{Z}_4$ 上有 4 个准导数(表 1)。其次,考虑 $e\geqslant3$ 的情形。为此,需引入以下结论。

引理 2[3]　设 $e\in\mathbf{Z}^+$。1) 若 $\bar{x}\in\mathbf{Z}_{2^e}$,则存在 $i,k,m\in\mathbf{Z}$,$(0\leqslant i\leqslant e)$,使得 $\bar{x}=\overline{2^i\cdot5^k\cdot(-1)^m}$;

* **收稿日期:**2015-06-26　**修回日期:**2017-02-20　**网络出版时间:**2017-03-13 11:06
资助项目:国家自然科学基金(No. 11201411)
第一作者简介:邓勇,男,教授,研究方向为代数及其数值计算,E-mail:dengy-ks@sohu.com
网络出版地址:http://kns.cnki.net/kcms/detail/50.1165.N.20170313.1106.004.html

2) 设 $i,j,k,l,m,n\in\mathbf{Z}$。若 $0\leqslant i,j\leqslant e$,则:

$$\overline{2^i\cdot 5^k\cdot(-1)^m}=\overline{2^j\cdot 5^l\cdot(-1)^n}\Leftrightarrow$$

$$i=j \text{ 且 } 5^k\cdot(-1)^m\equiv 5^l\cdot(-1)^n(\bmod 2^{e-i});$$

3) 若 $e\geqslant 2$,则 $\overline{5^k\cdot(-1)^m}=\overline{5^l\cdot(-1)^n}\Leftrightarrow m\equiv n(\bmod 2)$ 且 $k\equiv l(\bmod 2^{e-2})$;

4) 若 $e\geqslant 2$,则 $\overline{5}^{2^{e-2}}=\overline{1}$。

注意到,4)是 3)在 $k=2^{e-2}$ 和 $m=l=n=0$ 时的特殊情况。并且引理 2 表明 $\mathbf{Z}_{2^e}$ 中的每个元都能写成 $2^r\cdot 5^s\cdot(-1)^t$ 的形式。此外,若 $\mathbf{Z}_{2^e}$ 的两个元素均能写成此形式,则引理 2 给出了如何准确判断它们是否相等的方法。进一步,设 φ 是 $\mathbf{Z}_{2^e}$ 上的任一准导数且 $\overline{x}=\overline{2^i\cdot 5^k\cdot(-1)^m}$。由引理 1 可得

$$\varphi(\overline{x})=\overline{i\cdot 2^{i-1}\cdot 5^k\cdot(-1)^m}\cdot\varphi(\overline{2})+\overline{k\cdot 2^i\cdot 5^{k-1}\cdot(-1)^m}\cdot\varphi(\overline{5})+\overline{m\cdot 2^i\cdot 5^k\cdot(-1)^{m-1}}\cdot\varphi(\overline{-1})。\quad(1)$$

由此可见,只要得到 $\varphi(\overline{2})$,$\varphi(\overline{5})$ 和 $\varphi(\overline{-1})$,利用(1)式就能完全确定 φ。

引理 3　设 $e\geqslant 3$。若 φ 是 $\mathbf{Z}_{2^e}$ 上的准导数,则 $\varphi(\overline{2})\in\overline{2}\mathbf{Z}_{2^e}$,$\varphi(\overline{5})\in\overline{4}\mathbf{Z}_{2^e}$,$\varphi(\overline{-1})\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$。

证明　由引理 1 可得,$\overline{2}\cdot\varphi(\overline{-1})=-\varphi(\overline{-1^2})=-\varphi(\overline{1})=\overline{0}$。因此,$\varphi(\overline{-1})$ 是 $\overline{2^{e-1}}$ 的倍数。类似地,由引理 1 和引理 2 可得,$\overline{0}=\varphi(\overline{1})=\varphi(\overline{5}^{2^{e-2}})=\overline{2^{e-2}}\cdot\overline{5^{2^{e-2}-1}}\cdot\varphi(\overline{5})$。因 $5^{2^{e-2}-1}$ 是奇数,故 $\varphi(\overline{5})$ 必为 $\overline{4}$ 的倍数。最后,若 e 是奇数,则 $\overline{0}=\varphi(\overline{0})=\varphi(\overline{2}^e)=\overline{e}\cdot\overline{2^{e-1}}\cdot\varphi(\overline{2})$。这表明,$\varphi(\overline{2})\in\overline{2}\mathbf{Z}_{2^e}$;若 e 是偶数,则

$$\varphi(\overline{2^{e-1}})=\varphi(\overline{2^e}+\overline{2^{e-1}})=\varphi(\overline{2^{e-1}\cdot 3})=\overline{3}\varphi(\overline{2^{e-1}})+\overline{2^{e-1}}\varphi(\overline{3})。\quad(2)$$

由引理 2 知,$\exists k,m\in\mathbf{Z}$,使得 $\overline{3}=\overline{5^k\cdot(-1)^m}$。于是

$$\varphi(\overline{3})=\overline{k\cdot 5^{k-1}\cdot(-1)^m}\cdot\varphi(\overline{5})+\overline{m\cdot 5^k\cdot(-1)^{m-1}}\cdot\varphi(\overline{-1})。$$

又因 $\varphi(\overline{5})\in\overline{4}\mathbf{Z}_{2^e}$,$\varphi(\overline{-1})\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$,故 $\varphi(\overline{3})$ 是偶数的剩余类。因此,(2)式中的项 $\overline{2^{e-1}}\varphi(\overline{3})$ 将消失。于是 $\varphi(\overline{2^{e-1}})=\overline{3}\varphi(\overline{2^{e-1}})$,即 $\overline{2}\varphi(\overline{2^{e-1}})=\overline{0}$。此外,$\overline{0}=\overline{2}\varphi(\overline{2^{e-1}})=\overline{e-1}\cdot\overline{2^{e-1}}\cdot\varphi(\overline{2})$。因为 $e-1$ 是奇数,所以 $\varphi(\overline{2})\in\overline{2}\mathbf{Z}_{2^e}$。　证毕

综上可知,由引理 1 和引理 2 就可完全定义 $\mathbf{Z}_{2^e}$ 上的所有准导数。然而,由于 $\mathbf{Z}_{2^e}$ 的同一个元素在表示为形式 $\overline{2^i\cdot 5^k\cdot(-1)^m}$ 时可能不同,所以还必须明确给出(1)式定义的函数,即当 i,k,m 取不同值时,它们表示 $\mathbf{Z}_{2^e}$ 中的相同元素。也就是说它们被(1)式定义的函数作用后结果相同。为此,给出引理 4。

引理 4　设 $\overline{a}\in\overline{2}\mathbf{Z}_{2^e}$,$\overline{b}\in\overline{4}\mathbf{Z}_{2^e}$,$\overline{c}\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$。若 $\overline{2^i\cdot 5^k\cdot(-1)^m}=\overline{2^j\cdot 5^l\cdot(-1)^n}$,$0<i,j<e$,则:

$$\overline{i\cdot 2^{i-1}\cdot 5^k\cdot(-1)^m\cdot a}+\overline{k\cdot 2^i\cdot 5^{k-1}\cdot(-1)^m\cdot b}+\overline{m\cdot 2^i\cdot 5^k\cdot(-1)^{m-1}\cdot c}=$$

$$\overline{j\cdot 2^{j-1}\cdot 5^l\cdot(-1)^n\cdot a}+\overline{l\cdot 2^j\cdot 5^{l-1}\cdot(-1)^n\cdot b}+\overline{n\cdot 2^j\cdot 5^l\cdot(-1)^{n-1}\cdot c}。$$

引理 4 表明,由(1)式的确可产生 $\mathbf{Z}_{2^e}$ 上的一个函数 φ,它规定 $\varphi(\overline{2})$,$\varphi(\overline{5})$,$\varphi(\overline{-1})$ 分别是 $\overline{2}$,$\overline{4}$,$\overline{2^{e-1}}$ 的倍数。因此,在 $\mathbf{Z}_{2^e}$ 上可定义如下函数。

定义 2　设 $e\geqslant 3$,$\overline{a}\in\overline{2}\mathbf{Z}_{2^e}$,$\overline{b}\in\overline{4}\mathbf{Z}_{2^e}$,$\overline{c}\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$。定义 $\varphi_{\overline{a},\overline{b},\overline{c}}:\mathbf{Z}_{2^e}\to\mathbf{Z}_{2^e}$ 为:

$$\varphi_{\overline{a},\overline{b},\overline{c}}(\overline{2^i\cdot 5^k\cdot(-1)^m})=\overline{i\cdot 2^{i-1}\cdot 5^k\cdot(-1)^m\cdot a}+\overline{k\cdot 2^i\cdot 5^{k-1}\cdot(-1)^m\cdot b}+\overline{m\cdot 2^i\cdot 5^k\cdot(-1)^{m-1}\cdot c}。$$

定理 1　若 $e\geqslant 3$,$\overline{a}\in\overline{2}\mathbf{Z}_{2^e}$,$\overline{b}\in\overline{4}\mathbf{Z}_{2^e}$,$\overline{c}\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$,则 $\varphi_{\overline{a},\overline{b},\overline{c}}$ 是 $\mathbf{Z}_{2^e}$ 上的准导数。反之,$\mathbf{Z}_{2^e}$ 上的任何一个准导数都具有 $\varphi_{\overline{a},\overline{b},\overline{c}}$ 的形式。

证明　由引理 2 和定义 2 容易验证,$\varphi_{\overline{a},\overline{b},\overline{c}}$ 满足 Leibnitz 乘积法则。因此,$\varphi_{\overline{a},\overline{b},\overline{c}}$ 是 $\mathbf{Z}_{2^e}$ 上的准导数。反之,由引理 3 可知,对 $\overline{a}\in\overline{2}\mathbf{Z}_{2^e}$,$\overline{b}\in\overline{4}\mathbf{Z}_{2^e}$,$\overline{c}\in\overline{2^{e-1}}\mathbf{Z}_{2^e}$,环 $\mathbf{Z}_{2^e}$ 上的任何一个准导数必须等于 $\varphi_{\overline{a},\overline{b},\overline{c}}$。　证毕

表 1　$\mathbf{Z}_4$ 上的准导数

Tab. 1　All quasi-derivatives on $\mathbf{Z}_4$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
φ_1	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
φ_2	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{0}$
φ_3	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{2}$
φ_4	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$

3 模奇素数幂的准导数

引理 5[4]　设 $e\in\mathbf{Z}^+$,p 是一个奇素数,$\overline{g}\in\mathbf{Z}_{p^e}$ 固定。于是,下列命题成立:

1) 对 $\forall\,\overline{x}\in\mathbf{Z}_{p^e}$,$\exists\,i,k\in\mathbf{Z}(0\leqslant i\leqslant e)$,使得 $\overline{x}=\overline{p^i\cdot g^k}$;

2) 设 $i,j,k,l\in\mathbf{Z}$ 且 $0\leqslant i,j\leqslant e$。$\overline{p^i\cdot g^k}=\overline{p^j\cdot g^l}\Leftrightarrow i=j$ 且 $g^k\equiv g^l(\bmod p^{e-i})$;

3) $\overline{g}^k=\overline{g}^l\Leftrightarrow k\equiv l(\mathrm{mod}(p^e-p^{e-1}))$;4) $(\overline{g})^{p^e-p^{e-1}}=\overline{1}$。

引理5表明,$\mathbf{Z}_{p^e}$中的单位乘法群$\mathbf{Z}_{p^e}^{\times}$是阶数为$p^e-p^{e-1}=p^{e-1}(p-1)$,生成元为$\overline{g}$的循环群。但通常生成元$\overline{g}$却很难确定。因此,参考引理5,可固定$e,p,\overline{g}$。这样$\mathbf{Z}_{p^e}$($p$是奇素数)上的准导数推导就与前一节类似了。

引理 6 若φ是$\mathbf{Z}_{p^e}$上的准导数,则$\varphi(\overline{g}),\varphi(\overline{p})\in\overline{p}\mathbf{Z}_{p^e}$,其中$p$是奇素数。

定义 3 设$\overline{a},\overline{b}\in\overline{p}\mathbf{Z}_{p^e}$。定义映射$\varphi_{\overline{a},\overline{b}}:\mathbf{Z}_{p^e}\to\mathbf{Z}_{p^e}$为$\varphi_{\overline{a},\overline{b}}(\overline{p^k\cdot g^i})=\overline{k\cdot p^{k-1}\cdot g^i\cdot a}+\overline{i\cdot g^{i-1}\cdot p^k\cdot b}$。

显然,$\varphi_{\overline{a},\overline{b}}$的定义依赖于生成元$\overline{g}$的选择。

定理 2 若$\overline{a},\overline{b}\in\overline{p}\mathbf{Z}_{p^e}$,则$\varphi_{\overline{a},\overline{b}}$是$\mathbf{Z}_{p^e}$的准导数。反之,$\mathbf{Z}_{p^e}$的任何一个准导数都具有$\varphi_{\overline{a},\overline{b}}$的形式。

例 1 求$\mathbf{Z}_9$上的所有准导数ψ。

解 因$\psi(\overline{2}^i\ \overline{3}^k)=\overline{i}\,\overline{2}^{i-1}\,\overline{3}^k\psi(\overline{2})+\overline{k}\,\overline{3}^{k-1}\,\overline{2}^i\psi(\overline{3})$,其中$\psi(\overline{2}),\psi(\overline{3})\in\overline{3}\mathbf{Z}_9=\{\overline{0},\overline{3},\overline{6}\}$,故$\mathbf{Z}_9$上有9个准导数。若令$\psi=\varphi_{\overline{6},\overline{3}}$,即$\psi(\overline{3})=\overline{6},\psi(\overline{2})=\overline{3}$。则:

$$\psi(\overline{6})=\psi(\overline{2}\cdot\overline{3})=\overline{2}\cdot\overline{6}+\overline{3}\cdot\overline{3}=\overline{3},$$
$$\psi(\overline{5})=\psi(\overline{2}^5)=\overline{5}\cdot\overline{2}^4\cdot\psi(\overline{2})=\overline{8}\cdot\overline{3}=\overline{6}。$$

其他准导数类似可求,结果见表2。

表2 $\mathbf{Z}_9$上的准导数

Tab. 2 All quasi-derivatives on $\mathbf{Z}_9$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\varphi_{\overline{0},\overline{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\varphi_{\overline{0},\overline{3}}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$
$\varphi_{\overline{0},\overline{6}}$	$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$
$\varphi_{\overline{3},\overline{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{0}$
$\varphi_{\overline{3},\overline{3}}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{0}$
$\varphi_{\overline{3},\overline{6}}$	$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{3}$	$\overline{0}$
$\varphi_{\overline{6},\overline{0}}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{0}$
$\varphi_{\overline{6},\overline{3}}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{3}$	$\overline{6}$	$\overline{0}$
$\varphi_{\overline{6},\overline{6}}$	$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{6}$	$\overline{3}$	$\overline{3}$	$\overline{3}$	$\overline{3}$	$\overline{0}$

4 模正整数的准导数

设$n\in\mathbf{Z}^+$。由孙子定理知,若n的素因子分解式为$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$,则$\mathbf{Z}_n\cong\mathbf{Z}_{p_1^{e_1}}\times\mathbf{Z}_{p_2^{e_2}}\times\cdots\times\mathbf{Z}_{p_k^{e_k}}$。其中,对应关系为$f(\overline{x})=(\overline{x},\overline{x},\cdots,\overline{x})$[5]。因此,找$\mathbf{Z}_n$上的准导数就等价于找$\mathbf{Z}_{p_i^{e_i}}$($i=1,2,\cdots,k$)上的准导数[6]。

引理 7 映射φ是$\mathbf{Z}_a\times\mathbf{Z}_b$上的准导数当且仅当存在$\mathbf{Z}_a$上的准导数$\varphi_1$和$\mathbf{Z}_b$上的准导数$\varphi_2$,使得对$\forall(\overline{x},\overline{y})\in\mathbf{Z}_a\times\mathbf{Z}_b$,都有$\varphi(\overline{x},\overline{y})=(\varphi_1(\overline{x}),\varphi_2(\overline{y}))$。

证明 充分性。设φ是$\mathbf{Z}_a\times\mathbf{Z}_b$上的准导数。若$v_1=(\overline{1},\overline{0}),v_2=(\overline{0},\overline{1})$,则$\varphi(v_1)=\varphi(v_2)=(\overline{0},\overline{0})$。因此,$v_1\varphi(\overline{x},\overline{y})=\varphi(v_1(\overline{x},\overline{y}))=\varphi(\overline{x},\overline{0})$。这说明$\varphi(\overline{x},\overline{y})$的第一个分量仅依赖于$\overline{x}$。同样,用$v_2$替换$v_1$可推出$\varphi(\overline{x},\overline{y})$的第二个分量仅依赖于$\overline{y}$。由此可见,必存在$\varphi_1:\mathbf{Z}_a\to\mathbf{Z}_a$和$\varphi_2:\mathbf{Z}_b\to\mathbf{Z}_b$,使得对$\forall(\overline{x},\overline{y})\in\mathbf{Z}_a\times\mathbf{Z}_b$,都有$\varphi(\overline{x},\overline{y})=(\varphi_1(\overline{x}),\varphi_2(\overline{y}))$。又因为:

$$(\varphi_1(\overline{x_1}\,\overline{x_2}),\varphi_2(\overline{y_1}\,\overline{y_2}))=\varphi(\overline{x_1}\,\overline{x_2},\overline{y_1}\,\overline{y_2})=\varphi((\overline{x_1},\overline{y_1})(\overline{x_2},\overline{y_2}))=$$
$$(\overline{x_1},\overline{y_1})\varphi(\overline{x_2},\overline{y_2})+(\overline{x_2},\overline{y_2})\varphi(\overline{x_1},\overline{y_1})=(\overline{x_1}\varphi_1(\overline{x_2})+\overline{x_2}\varphi_1(\overline{x_1}),\overline{y_1}\varphi_2(\overline{y_2})+\overline{y_2}\varphi_2(\overline{y_1}))。$$

所以,φ_1和φ_2分别是$\mathbf{Z}_a$和$\mathbf{Z}_b$上的准导数。

必要性。设φ_1和φ_2分别是$\mathbf{Z}_a$和$\mathbf{Z}_b$上的准导数。可以直接验证,映射$\varphi:\mathbf{Z}_a\times\mathbf{Z}_b\to\mathbf{Z}_a\times\mathbf{Z}_b$,即$\varphi(\overline{x},\overline{y})=(\varphi_1(\overline{x}),\varphi_2(\overline{y}))$,$\forall(\overline{x},\overline{y})\in\mathbf{Z}_a\times\mathbf{Z}_b$是$\mathbf{Z}_a\times\mathbf{Z}_b$上的准导数。 证毕

定理 3 映射φ是$\mathbf{Z}_n\cong\mathbf{Z}_{p_1^{e_1}}\times\mathbf{Z}_{p_2^{e_2}}\times\cdots\times\mathbf{Z}_{p_k^{e_k}}$上的准导数$\Leftrightarrow\varphi(\overline{x_1},\overline{x_2},\cdots,\overline{x_k})=(\varphi_1(\overline{x_1}),\cdots,\varphi_k(\overline{x_k}))$。其中$\varphi_i$($i=1,2,\cdots,k$)是$\mathbf{Z}_{p_i^{e_i}}$上的准导数。

利用引理7和数学归纳法易证定理3。

例 2 设ψ是$\mathbf{Z}_{144}\cong\mathbf{Z}_{16}\times\mathbf{Z}_9$上对应$(\varphi_1,\varphi_2)$的一个准导数,其中$\varphi_1=\varphi_{\overline{2},\overline{4},\overline{8}}$如定义2,$\varphi_2=\varphi_{\overline{3},\overline{6}}$如例1。试求$\psi(\overline{47})$。

解 因$\mathbf{Z}_{16}\times\mathbf{Z}_9$上对应于$\overline{47}$的元素为$(\overline{15},\overline{2})$,故$\psi(\overline{47})$是$\mathbf{Z}_{144}$对应于

$$(\varphi_{\overline{2},\overline{4},\overline{8}}(\overline{15}),\varphi_{\overline{3},\overline{6}}(\overline{2}))=(\varphi_{\overline{2},\overline{4},\overline{8}}(\overline{-1}),\varphi_{\overline{3},\overline{6}}(\overline{2}))=(\overline{8},\overline{6})$$

的元素。由孙子定理可知,$\overline{24}$也对应于$(\overline{8},\overline{6})$。因此,$\psi(\overline{47})=\overline{24}$。

如前所述,$\mathbf{Z}_2$的准导数仅有零映射。同样,由定理2可知,若p是奇素数,则$\mathbf{Z}_p$的准导数也只有零映射。若一个整数不能被任何素数的平方整除,则被称"无平方因子"。利用孙子定理及定理3可以证明,若$n\in\mathbf{Z}$无平方因子,则$\mathbf{Z}_n$的准导数只有零映射。更一般地,若$n\in\mathbf{Z}$的素因子分解为$\prod p_k^{e_k}$,则$\mathbf{Z}_n$恰有$\prod p_k^{2(e_k-1)}$个准

导数[7]。

参考文献：

[1] BARBEAU E. Remarks on an arithmetic derivative[J]. Canada Math Bull,1961(4):117-122.

[2] UFNAROVSKI V. How to differentiate a number[J]. Journal of Integer Sequences,2003(6):1-24.

[3] STILLWELL J. Elements of number theory[M]. New York: Springer-Verlag,2003.

[4] MURTY M R,ESMONDE J. Problems in algebraic number theory[M]. 2nd edition. New York: Springer-Verlag, 2005.

[5] 范德瓦尔登.代数学(Ⅰ)[M].北京:科学出版社,2009.
van der WAERDEN B L. Algebra(Ⅰ)[M]. Beijing:Science Press,2009.

[6] KOVIC J. The arithmetic derivative and anti-derivative[J]. Journal of Integer Sequences,2012,15:1-16.

[7] BUIUM A. Arithmetic analogues of derivations[J]. Journal of Algebra,1997,198:290-299.

The Quasi-derivative and Its Classification over the Residue Class Ring of Integers mod *n*

DENG Yong

(College of Mathematics and Statistics, Kashgar University, Kashgar Xinjiang 844006, China)

Abstract: [**Purposes**]An quasi-derivative on $\mathbf{Z}$ is a map that sending each prime to 1 and satisfying the Leibnitz product rule $(ab)'=a'b+ab'$. In the application, quasi-derivative has affected many other fields of mathematics. In order to obtain a familiar mathematical object and attempt to deepen understand of it in a completely different setting. [**Methods**]Here, the concept of quasi-derivative was given in the setting of the integer mod n. that is, an quasi-derivative on $\mathbf{Z}_n$ to be a map φ from $\mathbf{Z}_n$ to itself which satisfies the product rule $\varphi(xy)=\varphi(x)y+x\varphi(y)$ for all $x,y\in\mathbf{Z}_n$. [**Findings**]Further, all quasi-derivatives on $\mathbf{Z}_n$ were proceeded to classify. [**Condusions**]In particular, it is a very powerful tool to discuss the various unproven conjectures in additive prime number theory.

Keywords: the integer mod n; residual class ring; quasi-derivative

(责任编辑 黄 颖)