文章编号:1000-2375(2010)04-0354-03

两个数论定理的群论证明

刘合国,吴佐慧

(湖北大学 数学与计算机科学学院,湖北 武汉 430062)

摘要:从群论的角度再次证明原根定理以及 Wilson 定理,并给出了 Wilson 定理的一个推广.

关键词:Wilson 定理;原根;循环群

中图分类号:O156;O152 文献标志码:A

本文中采用的术语和符号是标准的,按照文献[1-2].

原根定理以及 Wilson 定理是初等数论中著名的定理,在解决素数模的高次同余式问题,判断一个数是不是素数,证明同余式和整数的整除等问题上有重要的作用.同时也可以用来简化和解决许多难度较高的相关问题,它们的证明方法较多,如文献[2-3]中,主要是用整系数多项式、指数、既约剩余系等知识进行证明.其中 Wilson 定理在文献[1]中以习题的形式出现,它促使我们思考用群论的方法来解决一些数论中的问题.

本文中将用群论的语言再次给出原根定理以及 Wilson 定理的证明,并通过原根定理给出 Wilson 定理的一个推广.为叙述方便,先给出这两个定理.

原根定理[2] 模 m 有原根的充要条件是 $m=1,2,4,p^\alpha,2p^\alpha$,其中 p 是奇素数,$\alpha\geqslant 1$.

Wilson 定理[2] $(p-1)!\equiv -1(\mathrm{mod}\ p)$,其中 p 是素数.

我们用$\mathbb{Z}_m^*$表示模 m 的剩余类环$\mathbb{Z}_m$中所有单位组成的群,即环$\mathbb{Z}_m$的单位群.注意到模 m 有原根等价于$\mathbb{Z}_m^*$是循环群,故原根定理等价于

$$\mathbb{Z}_m^* \text{ 是循环群的充要条件是 } m=1,2,4,p^\alpha,2p^\alpha\text{,其中 } p \text{ 是奇素数},\alpha\geqslant 1 \tag{1}$$

引理 1 G 是偶阶循环群,则 G 有唯一的 2 阶元.

引理 1 的证明 设 $G=\langle a\rangle$ 是 $2n$ 阶循环群,则$|a|=2n$.于是 $a^n\in G$,且$|a^n|=2$.如果还存在 $a^m\in G$,且$|a^m|=2$,但 a^m 的阶为$\dfrac{2n}{(2n,m)}$,从而
$$\frac{2n}{(2n,m)}=2,n=(2n,m).$$
于是 n 整除 m,$a^m\in\langle a^n\rangle$,又因为$|a^n|=|a^m|=2$,故 $a^m=a^n$.即 G 有唯一的 2 阶元 a^n.

引理 2 群$\mathbb{Z}_{2^\alpha}^*$的结构为
$$\mathbb{Z}_{2^\alpha}^*\cong\begin{cases}1, & \text{如果 } \alpha=1,\\ C_2, & \text{如果 } \alpha=2,\\ C_2\times C_{2^{\alpha-2}}, & \text{如果 } \alpha\geqslant 3.\end{cases}$$

引理 2 的证明 当 $\alpha=1$ 时,模 2 的既约剩余系只有 1,所以$\mathbb{Z}_2^*\cong 1$;

当 $\alpha=2$ 时,模 4 的既约剩余系为 1 和 3,所以$\mathbb{Z}_4^*\cong C_2$;

当 $\alpha\geqslant 3$ 时,显然$\{\pm 1,2^{\alpha-1}\pm 1\}$是$\mathbb{Z}_{2^\alpha}^*$的子群,并且它同构于 $C_2\times C_2$,所以$\mathbb{Z}_{2^\alpha}^*$不是循环群,又因为$\langle 3\rangle$是$\mathbb{Z}_{2^\alpha}^*$的阶为 $2^{\alpha-2}$的子群,且$\langle -1\rangle\cap\langle 3\rangle=1$,$|\langle -1\rangle|\cdot|\langle 3\rangle|=2^{\alpha-1}$,所以此时$\mathbb{Z}_{2^\alpha}^*\cong C_2\times C_{2^{\alpha-2}}$.

引理 3[1] 设 G 是有限 Abel 群,其元素的最大阶为 m,则 G 中所有元素的阶都是 m 的因子.

引理 3 的证明 令 G 中元 g 的阶是 m,假如有一元素 g_1 的阶 n 不是 m,则存在素数 p 使得

收稿日期:2010-03-29
基金项目:国家自然科学基金(10971058)资助
作者简介:刘合国(1967-),男,博士,教授,Email:ghliu@hubu.edu.cn

$$m=p^i m_1,(p,m_1)=1;n=p^j n_1,(j>i).$$

令
$$g_2=g^{p^i},g_3=g_1^{n^1},$$

则
$$|g_2|=m_1,|g_3|=p^j,$$

又因为$(p,m_1)=1$,所以$|g_2g_3|=p^jm_1>m$,于是与 m 的最大性矛盾,故 G 中所有元素的阶都是 m 的因子.

令
$$n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots,$$

其中 p_i 为素数,且 $\alpha_i\geqslant 1$. 于是由中国剩余定理可得,模 n 的剩余类环同构于所有模 $p_i^{\alpha_i}$ 的剩余类环的直积,即
$$\mathbb{Z}_n\cong\mathbb{Z}_{p_1^{\alpha_1}}\times\mathbb{Z}_{p_2^{\alpha_2}}\times\mathbb{Z}_{p_3^{\alpha_3}}\times\cdots.$$

同样$\mathbb{Z}_n$的单位群$\mathbb{Z}_n^*$同构于所有$\mathbb{Z}_{p_i^{\alpha_i}}$的单位群$\mathbb{Z}_{p_i^{\alpha_i}}^*$的直积,即　$\mathbb{Z}_n^*\cong\mathbb{Z}_{p_1^{\alpha_1}}^*\times\mathbb{Z}_{p_2^{\alpha_2}}^*\times\mathbb{Z}_{p_3^{\alpha_3}}^*\cdots$.

下面我们将给出(1)式的证明

(1)式的证明　如果 m 不属于(1)式中列出的情形,那么必有
$$m=2^\alpha(\alpha\geqslant 3);2^\alpha p_1^{\alpha_1}\cdots p_r^{\alpha_r}(\alpha\geqslant 2,r\geqslant 1),$$

或者
$$2^\alpha p_1^{\alpha_1}\cdots p_r^{\alpha_r}(\alpha\geqslant 0,r\geqslant 2),$$

于是
$$\mathbb{Z}_m^*=\mathbb{Z}_{2^\alpha}^*(\alpha\geqslant 3);\mathbb{Z}_{2^\alpha}^*\times\mathbb{Z}_{p_1^{\alpha_1}}^*\times\cdots\times\mathbb{Z}_{p_r^{\alpha_r}}^*(\alpha\geqslant 2,r\geqslant 1),$$

或者
$$\mathbb{Z}_{2^\alpha}^*\times\mathbb{Z}_{p_1^{\alpha_1}}^*\times\cdots\times\mathbb{Z}_{p_r^{\alpha_r}}^*(\alpha\geqslant 0,r\geqslant 2).$$

又因为当 p 为奇素数时,$\mathbb{Z}_{p_i^{\alpha_i}}^*$ 是 $\varphi(p_i^{\alpha_i})$阶循环群,且
$$\mathbb{Z}_{2^\alpha}^*\cong\begin{cases}1, & \text{如果 }\alpha=1,\\ C_2, & \text{如果 }\alpha=2,\\ C_2\times C_{2^{\alpha-2}}, & \text{如果 }\alpha\geqslant 3.\end{cases}$$

所以无论那种情况均可得$\mathbb{Z}_m^*$中 2 阶元的个数大于 1,但$\mathbb{Z}_m^*$是循环群,于是与引理 1 矛盾,故当$\mathbb{Z}_m^*$是循环群时,$m=1,2,4,p^\alpha,2p^\alpha$,其中 p 是奇素数,$\alpha\geqslant 1$;

反之,当 $m=1,2,4$ 时,$\mathbb{Z}_m^*$ 显然是循环群;所以只用证明 $m=p^\alpha,2p^\alpha$ 的情形. 又因为此时$\mathbb{Z}_{2p^\alpha}^*=\mathbb{Z}_2^*\times\mathbb{Z}_{p^\alpha}^*=\mathbb{Z}_{p^\alpha}^*$,所以只用证明 $m=p^\alpha$ 的情形即可. 分以下几步来证.

(ⅰ)若$\mathbb{Z}_{p^\alpha}^*=\langle g\rangle$,其中 p 为奇素数且 $\alpha\geqslant 1$,则 g 在$\mathbb{Z}_{p^{\alpha+1}}^*$中的阶为 $\varphi(p^\alpha)$或者 $\varphi(p^{\alpha+1})$. 设 g 在$\mathbb{Z}_{p^\alpha}^*$与$\mathbb{Z}_{p^{\alpha+1}}^*$中的阶分别为 n 与 m,则 $n=\varphi(p^\alpha)$,m 整除 $\varphi(p^{\alpha+1})$. 又因为$\mathbb{Z}_{p^\alpha}^*$与$\mathbb{Z}_{p^{\alpha+1}}^*$均为循环群,所以 n 整除 m,因此 $m=\varphi(p^\alpha)$或者 $\varphi(p^{\alpha+1})$.

(ⅱ)当 $\alpha=1$ 时,$\mathbb{Z}_p^*$ 是循环群. 因为$\mathbb{Z}_p^*$是有限 Abel 群,令 $n=\max\{|a|\,|\,a\in\mathbb{Z}_p^*\}$且$|g|=n$,所以 $n\leqslant|\mathbb{Z}_p^*|$且由引理 3 可得对于$\mathbb{Z}_p^*$任一元 a 都有$|a|$整除 n,又因为 $x^n-1=0$ 在 F_p 中最多有 n 个解,所以$|\mathbb{Z}_p^*|\leqslant n$,故$|\mathbb{Z}_p^*|=n$,$\mathbb{Z}_p^*=\langle g\rangle$.

(ⅲ)$\mathbb{Z}_{p^2}^*$是循环群. 由(ⅱ)得$\mathbb{Z}_p^*=\langle g\rangle$. 下面证明$\mathbb{Z}_{p^2}^*=\langle g\rangle$或者$\mathbb{Z}_{p^2}^*=\langle g+p\rangle$即可. 令 g 与 $g+p$ 在$\mathbb{Z}_{p^2}^*$中的阶分别为 u 与 v,由(ⅰ)可得 $u=\varphi(p)$或者 $\varphi(p^2)$且 $v=\varphi(p)$或者 $\varphi(p^2)$. 如果 $u=v=\varphi(p)$,那么$(g+p)^{p-1}\equiv 1(\mathrm{mod}\ p^2)$,于是可得 p 整除 g,与 $g^{p-1}\equiv 1(\mathrm{mod}\ p^2)$矛盾,因此 u,v 中必有一个等于 $\varphi(p^2)$,故$\mathbb{Z}_{p^2}^*=\langle g\rangle$或者$\mathbb{Z}_{p^2}^*=\langle g+p\rangle$.

(ⅳ)由(ⅰ)和(ⅱ)并应用类似(ⅲ)的证明过程可得,在 $g+rp(r=0,1,2,\cdots,p-1)$中,定有一元 $g+ip$ 使得$\mathbb{Z}_{p^\alpha}^*=\langle g+ip\rangle$.

Wilson 定理的证明　考虑群$\mathbb{Z}_p^*$,不难发现它为偶阶循环群,由性质 1 可得有唯一 2 阶元 $p-1$,于是$(p-1)!=p-1\equiv -1(\mathrm{mod}\ p)$.

Wilson 定理也可以改写成:设$\mathbb{Z}_p^*=\{x_1,x_2,\cdots x_{\varphi_p}\}$,则 $x_1x_2\cdots x_{\varphi_p}\equiv -1(\mathrm{mod}\ p)$. 于是应用原根定理可以得到 Wilson 定理的一个推广结论. 这个结论是在文献[3]中以习题的形式出现的,其常规的证明都是用数论的方法来做的,现在我们将结合原根定理给出它的群论证明.

定理 1[3]　设$\mathbb{Z}_m^*=\{x_1,x_2,\cdots,x_{\varphi_m}\}$,其中 m 为大于 1 的正整数,则
$$x_1x_2\cdots x_{\varphi_m}\equiv\begin{cases}-1(\mathrm{mod}\ m), & m=2,2^2,p^\alpha,2p^\alpha,\\ 1(\mathrm{mod}\ m), & \text{其他}.\end{cases}$$

定理 1 的证明　当 $m=2,2^2,p^\alpha,2p^\alpha$ 时,由原根定理可得$\mathbb{Z}_m^*$是偶阶循环群,进而由引理 1 得$\mathbb{Z}_m^*$有唯

－2 阶元 $m-1$. 于是 $x_1x_2\cdots x_{\varphi_m}=m-1\equiv-1(\mathrm{mod}\ m)$;

当 $m\neq 2,2^2,p^\alpha,2p^\alpha$ 时,考虑$\mathbb{Z}_m^*$ 的所有 2 阶元生成的子群 $\Omega_2(\mathbb{Z}_m^*)$,则

$$\Omega_2(\mathbb{Z}_m^*)=\{g\in\mathbb{Z}_m^*\mid g^2=1\}=\underbrace{C_2\times C_2\times\cdots\times C_2}_{k},\text{其中 } k\geqslant 2,$$

令 $\Omega_2(\mathbb{Z}_m^*)=H\times K$,其中 $H=\underbrace{C_2\times C_2\times\cdots\times C_2}_{k-1}$,$K=\{1,a\mid a^2=1\}$. 则集合 $\Omega_2(\mathbb{Z}_m^*)$与集合 $H\cup aH$ 相同,且$|H|$为偶数. 于是 $x_1x_2\cdots x_{\varphi_m}=\prod_{h\in H}h\cdot\prod_{h\in H}ah=\prod_{h\in H}h^2\cdot a^{|H|}\equiv 1(\mathrm{mod}\ m)$.

参考文献:

[1] Robinson D J S. A course in the theory of groups[M]. Second edition. New York:Springer-Verlag,1996.
[2] 闵嗣鹤,严士健. 初等数论[M]. 北京:高等教育出版社,1982.
[3] 潘承洞,潘承彪. 初等数论[M]. 北京:北京大学出版社,2003.

A group-theoretic proof of two theorems in number theory

LIU Heguo, WU Zuohui
(School of Mathematics and Computer Science,Hubei University,Wuhan 430062,China)

Abstract:The primitive root theorem and Wilson theorem were proved again by using a new method from the viewpoint of group theorem, at the same time, it generalized the Wilson theorem.

Key words:Wilson theorem; primitive root; cyclic group

(责任编辑 肖铿)

(上接第350页)

参考文献:

[1] 北京大学数学系. 高等代数[M]. 3版. 北京:高等教育出版社,2008.
[2] 樊恽. 代数学词典[M]. 武汉:华中师范大学出版社,1994.
[3] 樊恽,郑延履,刘合国. 线性代数学习指导[M]. 北京:科学出版社,2003.
[4] Roger A Horn, Charles R Johnson. 矩阵分析(英文版)[M]. 北京:人民邮电出版社,2005.
[5] 杨艳,刘合国. Cayley-Hamilton 定理的有理证明[J]. 湖北大学学报:自然科学版,2009,31(2):109-112.
[6] 杨艳,刘合国. Cayley-Hamilton 定理的一个证明[J]. 数学的实践与认识,2009,39(9):235-238.

On the minimal polynomial of a vector

ZHENG Dabin, LIU Heguo
(School of Mathematics and Computer Science, Hubei University, Wuhan 430062,China)

Abstract:A proof of Cayley-Hamilton theorem was presented by the minimal polynomial of a vector. For a linear transformation A of a finite dimensional vector space, we also proved that it existed some vector such that its minimal polynomial with respective to A be equal to the minimal polynomial of A.

Key words:vector space; linear transformation; minimal polynomial; Cayley-Hamilton theorem

(责任编辑 肖铿)