DOI:10.19789/j.1004-9398.2015.02.003

首都师范大学学报(自然科学版)
第36卷 第2期 Journal of Capital Normal University No. 2
2015年4月 (Natural Science Edition) Apr., 2015

费尔马小定理的一种奇特证明

邓 勇

(喀什师范学院数学系,新疆 喀什市 844006)

摘 要

给出了费尔马小定理的一种不借助欧几里得算法、群论和二项式系数等概念或性质的奇特证明方法.

关键词: 费尔马小定理,形式幂级数,无穷乘积,对数导数,归纳法.

中图分类号: O156

1 文献回顾

1636年,法国数学家皮埃尔·德·费尔马提出了一个命题,即对任意素数 p 和 $a \in \mathbb{Z}$,有 $p \mid (a^p - a)$. 该命题被后人称为费尔马小定理,而且成为数论中一个重要的基本定理. 它与 Wilson 定理、Euler 定理、中国剩余定理构成初等数论的四大定理. 该定理在数论中有着广泛而重要的应用. 比如,借助它可以得到 F_p 上有限域 F_{p^n} 的 Frobenius 同构等等.

费尔马虽然提出了上述定理,但他并没有证明. 直到1736年,欧拉在其出版的一本名为《一些与素数有关定理的证明》(拉丁文: Theorematum Quorundam ad Numeros PRIMOS Spectantium Demonstratio)的书中才第一次给出证明. 从莱布尼兹未发表的手稿中发现,他在1683年左右已经得到几乎与欧拉相同的证明. 关于这段历史的描述可查阅相关的数学史.

围绕费尔马小定理有许多有趣的、甚至是意想不到的证明[1]. 例如,基于二项式系数性质的证明就是其中一个经典. 具体来说,因 $(d+1)^p - d^p - 1 = \sum_{i=1}^{p-1} C_p^i d^i$. 而对每一个 $1 \leqslant i \leqslant p-1$,都有 $p \mid C_p^i = \frac{p!}{i!(p-i)!}$,故得 $p \mid [(d+1)^p - d^p - 1]$,$(d = 1, 2, \cdots, a-1)$. 由整除的性质可知,$p$ 整除上面 $a-1$ 个式子右端的和,即得 $p \mid (a^p - a)$.

另一个经典证明基于拉格朗日定理,即有限群中元素的阶整除群的阶[2]. 若将这个定理应用到有限域 F_p 的乘法群上,费尔马小定理立即就可获证. 除此之外,文献[3]还列举了许多其他证明方法.

在费尔马小定理的众多证明中,其推导过程大都要借助于欧几里得算法. 本文将不用欧几里得算法、群论和二项式系数等概念或性质,而是巧妙地借助两个形式幂级数项之间的恒等式,得到了费尔马小定理的一种新的证明方法.

2 定理证明

命题1 若 $f(x) = 1 - x - dx^2 + \sum_{k \geqslant 3} a_k x^k$ 是 $f(x)$ 在 $\mathbb{Q}$ 上的任意一个形式幂级数,其中系数取自于 $\mathbb{Z}$,则该幂级数能够唯一地表成如下乘积形式

$$f(x) = \prod_{k \geqslant 1} (1 - m_k x^k),$$

其中系数 m_k 是整数.

证明 当 $k = 1$ 和 $k = 2$ 时,我们只能唯一地选择 $m_1 = 1$ 和 $m_2 = d$,此时命题1显然成立. 假设 $N \geqslant 3$ 且已经选定了使上式成立的 m_k,$(k \leqslant N-1)$,则

$$\prod_{k=1}^{N-1} (1 - m_k x^k) = 1 - x - dx^2 + \sum_{k=3}^{N-1} a_k x^k - cx^N + \text{“更高阶项”},$$

其中 c 是仅依赖于 m_k,$(1 \leqslant k \leqslant N-1)$ 的某个整数. 因此,m_N 的唯一选择是 $m_N = c - a_N$. 由数学归纳法可知,命题1成立.

命题2 若 $1/f(x) = 1 + x + (d+1)x^2 + \sum_{k \geqslant 3} b_k x^k$ 是 $1/f(x)$ 在 $\mathbb{Q}$ 上的任意一个形式幂级数,其中系数取自于 $\mathbb{Z}$,则该幂级数能够唯一地表成如

收稿日期: 2013-12-17

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

下乘积形式

$$1/f(x) = (1+x)(1+(d+1)x^2)\prod_{k\geqslant 3}(1-n_k x^k),$$

其中系数 n_k,$(k\geqslant 3)$ 均是整数且 $n_1 = -1$,$n_2 = -(d+1)$.

证明 利用数学归纳法同上可证.

由数学分析可知,函数 $g(x)$ 的对数导数 $(\lg(x))'$ 的幂级数为 $g'(x)/g(x)$ 的幂级数. 而对任何两个可微函数 $g(x)$ 和 $h(x)$,有 $[\ln(g(x)\cdot h(x))]' = (\lg(x))' + (\ln h(x))'$ 成立[4]. 所以对 $f(x)$ 的对数求导数,可以得到

$$-x(\ln f(x))' = \sum_{k\geqslant 1}\frac{km_k x^k}{1-m_k x^k} = \sum_{N\geqslant 1}x^N\sum_{s\mid N}m_{N/s}^s\frac{N}{s}.$$

类似地,也可以得到

$$-x\left(\ln\frac{1}{f(x)}\right)' = x(\ln f(x))' = \sum_{N\geqslant 1}x^N\sum_{s\mid N}n_{N/s}^s\frac{N}{s}.$$

从上面两个无穷级数的项之间可以得到如下恒等式:

$$\sum_{s\mid N}m_{N/s}^s\frac{N}{s} = -\sum_{s\mid N}n_{N/s}^s\frac{N}{s},(N\in\mathbb{N}). \qquad (1)$$

由关系式(1),用数学归纳法容易证明: 当 k 为奇数时,有 $m_k = -n_k$,但对偶数下标的项则不成立! 为此,我们可以得出如下命题.

命题3　任何系数为 $\{m_1 = \pm 1, m_k, 2\leqslant k\in\mathbb{N}\}$ 的无穷整数序列都对应一个系数为 $\{n_1 = \mp 1, n_k, 2\leqslant k\in\mathbb{N}\}$ 的"逆"无穷整数序列. 进一步,所有这种无穷序列可分成互逆对.

例如,取 $m_k = 1$,$(k\in\mathbb{N})$,可得乘积 $(x,x)_\infty = \prod_{k=1}^{\infty}(1-x^k)$. 同时,$(x,x)_\infty^{-1} = \sum_{n=0}^{\infty}p(n)x^n$,其中 $p(n)$ 是 Ramanujan's 分割函数[3]. 使用递推关系(1),能够计算出序列 $\widetilde{n_k} = -n_k$. 正如前面提到的,对奇数 k,$\widetilde{n_k} = 1$,并且这个序列的偶数下标项为

2,4,0,14,−4,−8,−16,196,−54,−92,−184,144,−628,−1040,−2160,41102,…

因此,

$$\sum_{n=0}^{\infty}p(n)x^n = \prod_{k=1}^{\infty}(1+\widetilde{n_k}x^k).$$

费尔马小定理的证明　由命题1与命题2,因为 $m_2 = d$ 和 $n_2 = -(d+1)$,所以当 $N = 2p$ 时($p>2$ 是素数),(1)式就成为

$$2p\cdot m_{2p} + p\cdot m_p^2 + 2d^p + 1 = -2p\cdot n_{2p} - p\cdot n_p^2 + 2(d+1)^p - 1,$$

由此可得,$p\mid[(d+1)^p - d^p - 1]$,$(d = 1,2,\cdots,a-1)$,从而推出 $p\mid(a^p - a)$. 证毕.

3　补充说明

设 $f(x) = \dfrac{1-(d+1)\cdot x}{1-d\cdot x}$. 同样,若把函数 $f(x)$ 表成标准无穷乘积,即

$$f(x) = 1 - x - \sum_{n=1}^{\infty}d^n x^{n+1} = \prod_{n=1}^{\infty}(1-a_n x^n),$$

则求其对数的导数,可得

$$-x(\ln f(x))' = \sum_{N=1}^{\infty}((d+1)^N - d^N)x^N = \sum_{N\geqslant 1}x^N\sum_{s\mid N}a_{N/s}^s\frac{N}{s}.$$

特别地,作为上式的一个直接结果,我们可以得到 $a_p = \dfrac{(d+1)^p - d^p - 1}{p}$,这意味着 $\dfrac{(d+1)^p - d^p - 1}{p}$ 是一整数.

众所周知,素数 p 称为 Wieferich 素数当且仅当 $2^{p-1}\equiv 1(\mathrm{mod}p^2)$. 例如 $p = 1093$ 和 $p = 3511$,而且在范围 $p < 4\cdot 10^{12}$ 内没有其他素数. 若在 $f(x) = \dfrac{1-(d+1)\cdot x}{1-d\cdot x}$ 中取 $d = 1$,则所有的数 $a_p = \dfrac{2^p - 2}{p}$ 将同时出现在 $\dfrac{1-2x}{1-x}$ 的无穷乘积中. 因此,如果读者对 $\dfrac{1-2x}{1-x}$ 的标准无穷乘积做更深入的研究,那么它可能会帮助我们进一步厘清对这些特殊 Wieferich 素数性质的理解,甚至获得一些新的有益结果.

参　考　文　献

[1] 邓勇. 关于费尔马小定理的一个初等证明[J]. 高等数学研究, 2013, 16(1): 10.

[2] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta Functions [M]. (2nd ed) New York: Springer-Verlag New York Inc, 1984: 85.

[3] Wikipedia, the Free Encyclopedia, several classical and less known proofs of Fermat's little theorem [OL]. [2008-5-4]. http://en.Wikipedia.org/wiki.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[4] 常庚哲,史济怀. 数学分析教程[M]. 北京:中国科学技术大学出版社,2012:8.

A Peculiar Proof on Fermat's Little Theorem

Deng Yong

(Department of Mathematics, Kashgar Teacher's College, Kashgar, Xinjiang 844006)

Abstract

We presented a peculiar method to prove the Fermat's little theorem without using the conception or property of Euclidean algorithm, group theory and binomial coefficients.

Key words: Fermat's little theorem, formal power series, infinite product, logarithmic derivative, inductive approach.

作者简介 邓勇(1967 -),男,四川遂宁人,喀什师范学院数学系,教授,主要从事高等代数教学研究.

(上接第 7 页)

Generalized Correlation Coefficient Among Multi-variable Groups and Its R-program with R-language

Dong Xiaomeng

(Department of Math and Information Science, Weinan Teachers University, Weinan, Shannxi 714000)

Abstract

The recearch was done in order to complete generalized correlation coefficient theory system among multi-variable groups and provide the non-linear correlation method for operator. A kind of new generalized correlation coefficient based on the four rank moments was built with linear regression model, which could describe the correlation of different multi-variable groups, give its function package with R-language, enrich the R-language's function package.

Key words: multi-dimentional random vector; vector groups, generalized correlation coefficient, R-language.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net