

由组合的代数定义出发对其性质进行探讨

张少岩

泰莱学院, 马来西亚 梳邦再也

收稿日期: 2024年10月15日; 录用日期: 2024年11月15日; 发布日期: 2024年11月28日

摘要

本文回顾了 C_b^a 的定义并且由简单的定义出发, 采用初等办法证明了其一些基本性质以及一些整除性质, 在最后, 本文将提出证明费马小定理(Fermat's Little Theorem)的一种证明办法。

关键词

组合数学, 初等数论

Starting from the Algebraic Definition of Combination and Discussion on Its Properties

Shaoyan Zhang

Taylor's College, Subang Jaya, Malaysia

Received: Oct. 15th, 2024; accepted: Nov. 15th, 2024; published: Nov. 28th, 2024

Abstract

This article revises the definition of C_b^a and, starting from a simple definition, uses elementary mathematics to prove some of its basic properties as well as certain divisibility properties. In the final part, this article proposes a method to prove Fermat's Little Theorem.

Keywords

Combinatorics, Elementary Number Theory



1. 引言

组合数学是一门研究离散对象的科学，根据传说，其最早可以追溯到四千多年以前，最古老的组合数学问题是幻方问题，在大约 2200 年以前我国先民就已经独立发现了三阶幻方。中国历史在组合数学上最重要的进步之一是北宋数学家杨宪在其书《释锁算书》中提出了著名的杨宪三角(又称帕斯卡三角)，其中的第 n 行对应着 $(a+b)^n$ 展开后的系数，可以说，中国的组合数学曾比西方发达 500 余年。

在这篇文章中，我将先给出 C_b^a 的代数意义，随后我将接受几个定义并且根据我的定义证明 C_b^a 一定是整数以及一些引理，再之后我将提出几个相关的定理并且予以证明。

我将用初等的办法证明这些定理，这些定理的证明有些受到了[1]的启发，也有些是作者在过去学习的时候偶然发现的。

我在文章的最后一部分，将运用本文中讨论过的知识来证明费马小定理，证明的过程将会是简单易懂的。

费马小定理指的是 $r^p - r$ 可以被 p 整除，其中 r 是任意的整数， p 为一个质数。

这个定理最早在 1636 年由皮埃尔·德·费马(Pierre de Fermat)所发现，最早由数学家莱布尼茨(Gottfried Wilhelm Leibniz)和欧拉[2] (Leonhard Euler)给出证明。现在我们所熟知的利用模运算的方法[1]是由数学家詹姆斯·艾沃里于 1806 年发现，后来又被数学家狄拉克雷(Johann Peter Gustav Lejeune Dirichlet)于 1828 年重新发现。

2. 定义一

$$C_b^a = \frac{a \cdot (a-1) \cdot (a-2) \cdots (a-b+1)}{b!}, \text{ 其中 } b \text{ 是 } 0 \text{ 或者正整数, } a \text{ 是正整数, } b \text{ 不大于 } a.$$

接下来我们不要讨论 C_b^a 的任何其他意义，只遵从此处的定义来代数地理解。

3. 定义二

接下来当我们称 a 是 b 的 n 重因子，就是在说 b 至多可以被 a 的 n 次方整除，其中 a, b 都是正整数， n 是 0 或者正整数。

特别地，如果说 $n=1$ ，那么我们可以称 a 是 b 的单纯因子。

4. 定义三

设 m 个不同的正整数 $i_1, i_2, i_3, \dots, i_m$ 以及另一个正整数 k ，我们设 m_1 表示在序列 $i_1, i_2, i_3, \dots, i_m$ 中 k 至少作为单纯因子的次数； m_2 表示在序列 $i_1, i_2, i_3, \dots, i_m$ 中 k 至少作为二重因子的次数； m_3 表示在序列 $i_1, i_2, i_3, \dots, i_m$ 中 k 至少作为三重因子的次数；……以此类推。

并且我们定义 k 作为 $i_1 \cdot i_2 \cdot i_3 \cdots i_m$ 的因子的程度为 $m = m_1 + m_2 + m_3 + \dots$ ，显然 m 为正整数或 0。

为了更好地理解这个定义，让我试举一例：

设 m 个不同的正整数 3, 5, 25, 125, 310 以及另一个正整数 5，此时很显然，根据定义一，5 分别是 3, 5, 25, 125, 310 的 0 重因子，单纯因子，二重因子，三重因子，单纯因子。

所以此时 5 至少作为序列 3, 5, 25, 125, 310 中的单纯因子的次数 $m_1 = 0 + 1 + 1 + 1 + 1 = 4$ 。

而 5 至少作为序列 3,5,25,125,310 中的二重因子的次数 $m_2 = 0+0+1+1+0 = 2$ 。

而 5 作为序列 3,5,25,125,310 中的三重因子的次数 $m_3 = 0+0+0+1+0 = 1$ 。

我们可以知道 m_3, m_4, m_5, \dots 皆为 0, 所以根据定义 5 作为 $3 \cdot 5 \cdot 25 \cdot 125 \cdot 310 = 14531250$ 的因子的程度为 $4 + 2 + 1 = 7$ 。

事实上我们如果充分理解了以上的过程就应该不难明白如果 k 作为 $i_1 \cdot i_2 \cdot i_3 \cdot \dots \cdot i_m$ 的因子的程度为 m , 这实际上等价于在说 k 是 $i_1 \cdot i_2 \cdot i_3 \cdot \dots \cdot i_m$ 的 m 重因子。

5. 引理一

任意 $a \in \mathbb{N}^+$ 个连续的正整数之积皆可以被 $a!$ 整除(这等同于证明我定义一中的 C_b^a 一定是整数)。

证明: 让我们设 t 为一个正整数, 此时序列 $t+1, t+2, t+3, \dots, t+n$ 就是 $n \in \mathbb{N}^+$ 个连续的正整数且我们另外要求 n 不等于 1 (任何一个正整数都显然可以被 1! 整除, 所以说这样做仍然不失去本引理的一般性)。

让我们任取一个小于等于 n 的质数 p (这是一定能取到的因为 n 至少为 2), 并且让我们令

m_1 表示在序列 $t+1, t+2, t+3, \dots, t+n$ 中 p 至少作为单纯因子的次数;

m_2 表示在序列 $t+1, t+2, t+3, \dots, t+n$ 中 p 至少作为二重因子的次数;

m_3 表示在序列 $t+1, t+2, t+3, \dots, t+n$ 中 p 至少作为三重因子的次数。

以此类推。

现在再让我们考虑序列 $1, 2, 3, \dots, n$, 让我们令

s_1 表示在序列 $1, 2, 3, \dots, n$ 中 p 至少作为单纯因子的次数;

s_2 表示在序列 $1, 2, 3, \dots, n$ 中 p 至少作为二重因子的次数;

s_3 表示在序列 $1, 2, 3, \dots, n$ 中 p 至少作为三重因子的次数。

以此类推。

我们可以很明白地看到 p 作为 $(t+1) \cdot (t+2) \cdot (t+3) \cdot \dots \cdot (t+n)$ 的因子的程度为 $m = m_1 + m_2 + m_3 + \dots$, 而 p 作为 $1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$ 的因子的程度为 $s = s_1 + s_2 + s_3 + \dots$, 并且由 p 是一个小于等于 n 的质数这个性质, 我们可以确保 m 和 s 是正整数。

因为 p 作为 $(t+1) \cdot (t+2) \cdot (t+3) \cdot \dots \cdot (t+n)$ 的因子的程度为 $m = m_1 + m_2 + m_3 + \dots$, 所以在序列 $t+1, t+2, t+3, \dots, t+n$ 中可以被 p 整除的整数个数不小于 m_1 。

现在在序列 $t+1, t+2, t+3, \dots, t+n$ 中一定能选出 $t+p, t+2p, t+3p, \dots, t+s_1p$ 这些数, 因为在

$1, 2, 3, \dots, n$ 中一定有 $\left\lfloor \frac{n}{p} \right\rfloor$ 个数可以被 p 整除, 从而 $1, 2, 3, \dots, n$ 中 p 至少作为单纯因子的次数 s_1 一定不大于

$\left\lfloor \frac{n}{p} \right\rfloor$, 即 $s_1 \leq \left\lfloor \frac{n}{p} \right\rfloor$ 。而我们又知道 $\left\lfloor \frac{n}{p} \right\rfloor \leq \frac{n}{p}$, 故我们终得 $s_1 p \leq n$, 即证在序列 $t+1, t+2, t+3, \dots, t+n$ 中一

定能选出 $t+p, t+2p, t+3p, \dots, t+s_1p$ 这些数。 $\left\lfloor \frac{n}{p} \right\rfloor$ 意为 $\frac{n}{p}$ 向下取整。

既然在序列 $t+1, t+2, t+3, \dots, t+n$ 中一定能选出 $t+p, t+2p, t+3p, \dots, t+s_1p$ 这些数, 我们也能看出每个从 $t+kp$ 到 $t+(k+1)p$ 的区间 ($k=0, 1, 2, \dots, m_1-1$) 内至少有一个数可以被 p 整除, 因此这也就意味着 $s_1 \leq m_1$ 。

类似地我们可知 $s_2 \leq m_2, s_3 \leq m_3, \dots$

进而我们就得出了 $s \leq m$ 。这也就意味着 $n!$ 的每个质因子都是 $(t+1) \cdot (t+2) \cdot (t+3) \cdot \dots \cdot (t+n)$ 的因子, 于是我们得到了 $(t+1) \cdot (t+2) \cdot (t+3) \cdot \dots \cdot (t+n)$ 可以被 $n!$ 整除。

6. 引理二

设 $A \cdot \frac{B}{C} = I$, 其中 A, B, C 和 I 皆是整数且 A 和 C 互质, 那么 I 可以被 A 整除。

证明: 这个引理的证明是很简单的, 我们只需要将等式的两边同时乘以 C , 得到 $A \cdot B = I \cdot C$, 随后再同时除以 A , 我们得到

$$B = \frac{I \cdot C}{A}$$

因为 C 与 A 互质且 B 又由给定条件知一定是一个整数, 所以说 I 可以被 A 整除。

7. 引理三

设 $A \cdot \frac{B}{C} = I$, 其中 A, B, C 和 I 皆是整数, 如果 A 可以被 N 整除且 N 和 C 之间互质, 那么 I 必定可以 N 整除。

证明: 这个引理的证明也是很简单的, 由 A 可以被 N 整除我们可以知道 $A = N \cdot A_1$, A_1 是另一个整数。

此时我们就有 $\frac{A_1 \cdot N \cdot B}{C} = I$, 因为 I 是一个整数我们能够知道 $A_1 \cdot N \cdot B$ 可以被 C 整除, 而又因为 N 和 C 没有除了 1 以外的公因数, 所以说 C 必然能够整除 $A_1 \cdot B$, 进而 I 必然有 N 作为其因子, 这等价于 I 可以被 N 整除。

8. 定理一

$C_p^{p^2+i}$ 可以被 p 整除, 其中 p 是一个质数而 i 是 1 到 $p-1$ 之间的任何自然数。

证明:

设 $C_p^{p^2+i}$, p 为质数, 且 i 是 1 到 $p-1$ 之间的任何自然数。

那么此时我们有:

$$\begin{aligned} C_p^{p^2+i} &= \frac{(p^2+i) \cdot (p^2+i-1) \cdot \dots \cdot (p^2+1) \cdot p^2 \cdot (p^2-1) \cdot \dots \cdot (p^2+i-p+1)}{p!} \\ &= \frac{(p^2+i) \cdot (p^2+i-1) \cdot \dots \cdot (p^2+1) \cdot (p^2-1) \cdot \dots \cdot (p^2+i-p+1)}{(p-1)!} \cdot p \end{aligned}$$

根据引理一, 我们知道 $C_p^{p^2+i}$ 一定是一个整数, 而我们又发现 p 和 $(p-1)!$ 没有除 1 以外的公因数, 所以说根据引理二, 我们可以证明 $C_p^{p^2+i}$ 可以被 p 整除。

事实上, 依照相似的道理, 我们也可以证明 $C_p^{kp^2+i}$ 可以被 $k \cdot p$ 整除, k 是任意的正整数。

9. 定理二

设任意正整数 x , 我们有 $\frac{C_x^{kx^2}}{kx} = C_{x-1}^{kx^2-1}$, 其中 k 是另一个正整数。

证明: 因为 $\frac{C_x^{kx^2}}{kx} = k \cdot \frac{(kx^2-1) \cdot (kx^2-2) \cdot \dots \cdot (kx^2-x+1)}{(x-1)!} = C_{x-1}^{kx^2-1}$

所以由定理二我们显然可知 C_x^n 可以被 x^{n-1} 整除, 我们只需要令 $k = x^{n-2}$ 。

10. 定理三

设 n 为一个正整数, 那么我们有 $\frac{C_1^{n+1} \cdot C_2^{n+1} \cdot \dots \cdot C_{n-1}^{n+1} \cdot C_n^{n+1}}{C_1^n \cdot C_2^n \cdot \dots \cdot C_{n-2}^n \cdot C_{n-1}^n} = \frac{(1+n)^n}{n!}$

证明：因为

$$C_1^{n+1} \cdot C_2^{n+1} \cdot \dots \cdot C_{n-1}^{n+1} \cdot C_n^{n+1} = \frac{[(n+1)!]^{n-1}}{(1! \cdot 2! \cdot \dots \cdot n!)^2} \text{ 且 } C_1^n \cdot C_2^n \cdot \dots \cdot C_{n-2}^n \cdot C_{n-1}^n = \frac{(n!)^{n-1}}{[1! \cdot 2! \cdot \dots \cdot (n-1)!]^2}$$

$$\text{进而 } \frac{C_1^{n+1} \cdot C_2^{n+1} \cdot \dots \cdot C_{n-1}^{n+1} \cdot C_n^{n+1}}{C_1^n \cdot C_2^n \cdot \dots \cdot C_{n-2}^n \cdot C_{n-1}^n} = \frac{\frac{[(n+1)!]^{n-1}}{(1! \cdot 2! \cdot \dots \cdot n!)^2}}{\frac{(n!)^{n-1}}{[1! \cdot 2! \cdot \dots \cdot (n-1)!]^2}}$$

$$\text{化简得 } \frac{C_1^{n+1} \cdot C_2^{n+1} \cdot \dots \cdot C_{n-1}^{n+1} \cdot C_n^{n+1}}{C_1^n \cdot C_2^n \cdot \dots \cdot C_{n-2}^n \cdot C_{n-1}^n} = \frac{(1+n)^n}{n!}.$$

11. 定理四

设 n_1, n_2, \dots, n_r, n 和 r 皆为正整数，那么我们有

$$C_{n_1}^n \cdot C_{n_2}^{n-n_1} \cdot C_{n_3}^{n-n_1-n_2} \cdot \dots \cdot C_{n_r}^{n-n_1-n_2-\dots-n_{r-1}} = \frac{n!}{(n-n_1-n_2-\dots-n_r)! \cdot n_1! \cdot n_2! \cdot \dots \cdot n_r!}, \text{ 其中 } n \geq \sum_{i=1}^r n_i.$$

证明：

因为

$$\begin{aligned} & C_{n_1}^n \cdot C_{n_2}^{n-n_1} \cdot C_{n_3}^{n-n_1-n_2} \cdot \dots \cdot C_{n_r}^{n-n_1-n_2-\dots-n_{r-1}} \\ &= \frac{n!}{(n-n_1)! \cdot n_1!} \cdot \frac{(n-n_1)!}{(n-n_1-n_2)! \cdot n_2!} \cdot \frac{(n-n_1-n_2)!}{(n-n_1-n_2-n_3)! \cdot n_3!} \cdot \dots \cdot \frac{(n-n_1-n_2-\dots-n_{r-1})!}{(n-n_1-n_2-\dots-n_r)! \cdot n_r!} \\ &= \frac{n!}{(n-n_1-n_2-\dots-n_r)! \cdot n_1! \cdot n_2! \cdot \dots \cdot n_r!} \end{aligned}$$

写到这里，顺便提一下，如果 $n = \sum_{i=1}^r n_i$ ，那么 $\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!}$ 可以被记作 $\binom{n}{n_1, n_2, \dots, n_r}$

12. 定理五

设 p 是一个质数且 $1 < a \in N^+ < p$ ，那么 C_a^p 可以被 p 整除。

证明：

我们先来证明 $C_a^n \cdot \frac{n-a}{a+1} = C_{a+1}^n$ ，其中 n 是一个正整数且 $1 < a \in N^+ < n$ 。

事实上，我们根据定义一，就有 $C_b^a = \frac{a \cdot (a-1) \cdot (a-2) \cdot \dots \cdot (a-b+1)}{b!}$ ，进而：

$$\begin{aligned} & C_a^n \cdot \frac{n-a}{a+1} \\ &= \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-a+1)}{a!} \cdot \frac{n-a}{a+1} \\ &= \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-a+1) \cdot (n-a)}{(a+1)!} \\ &= C_{a+1}^n \end{aligned}$$

所以，当我们取 $n = p$ 时，我们先观察 $a = 1$ 时的情形，我们知道 $C_1^p = p$ 所以 C_1^p 显然可以被 p 整除，

而我们又知道 $C_1^p \cdot \frac{p-1}{2} = C_2^p$, 那么根据引理一, 我们明白 C_2^p 是整数, 而我们又明白 p 可以整除 C_1^p 且 p 和 2 互质, 那么根据引理三, 我们就能明白 C_2^p 必然可以被 p 整除。依照同样的道理, 由 $C_2^p \cdot \frac{p-1}{3} = C_3^p$ 就可以证明 C_3^p 可以被 p 整除。

如此递推下去, 我们就可以证明 C_a^p 可以被 p 整除, 其中 $1 < a \in N^+ < p$, p 是一个质数。

事实上我们由这个定理, 再意识到:

$$\frac{C_a^p}{p} = \frac{p \cdot (p-1) \cdot (p-2) \cdots (p-a+1)}{a!} = \frac{(p-1)!}{a! \cdot (p-1-a)!} \cdot \frac{1}{p-a} = \frac{(p-1) \cdot (p-2) \cdots (p-a)}{a!} = \frac{C_a^{p-1}}{p-a}$$

就可以发现 C_a^{p-1} 可以被 $p-a$ 整除。

13. 定理六(二项式定理)

设 x 为任意实数, n 为一个正整数, 那么我们有 $(1+x)^n = \sum_{k=0}^n C_k^n \cdot x^k$ 。

证明: 我们将采用数学归纳法, 不过在此之前为了流畅, 先证明 $C_r^n + C_{r-1}^n = C_r^{n+1}$, 其中 n 是一个正整数, 而 r 是一个正整数且 $0 \leq r \leq n$ 。

$$\text{由 } C_r^n + C_{r-1}^n = \frac{n!}{r! \cdot (n-r)!} + \frac{n!}{(r-1)! \cdot (n-r+1)!} = \frac{n![(n-r+1)+r]}{r! \cdot (n-r+1)!} = \frac{(n+1)!}{r! \cdot (n+1-r)!} = C_r^{n+1}, \text{ 即得。}$$

现在, 因为显然在 $n=1$ 时我们有 $1+x = C_0^1 + C_1^1 \cdot x$, 让我们假设 $(1+x)^r = \sum_{k=0}^r C_k^r \cdot x^k$, 对某正整数 r 成立, 那么 $(1+x)^{r+1} = (1+x)^r \cdot (1+x) = \left(\sum_{k=0}^r C_k^r \cdot x^k \right) + \left(\sum_{k=0}^r C_k^r \cdot x^{k+1} \right) = C_0^r + \sum_{k=0}^r C_k^{r+1} \cdot x^{k+1} = \sum_{k=0}^{r+1} C_k^{r+1} \cdot x^k$, 根据数学归纳法, 即证 $(1+x)^n = \sum_{k=0}^n C_k^n \cdot x^k$ 对任何实数 x 以及正整数 n 成立。

如果我们令 $x = \frac{a}{b}$, 随后再在等式两边乘以 b^n , 那么我们就可以得到 $(a+b)^n = \sum_{k=0}^n C_k^n \cdot a^k \cdot b^{n-k}$ 。

如果我们令 $x=1$, 那么我们就可以发现 $2^n = \sum_{k=0}^n C_k^n$ 。如果说再令 $n=p$, p 是一个质数,

那么我们可以发现 $2^p - 2 = \sum_{k=1}^{p-1} C_k^p$, 再根据定理五, 我们就能知道等式的右边可以被 p 整除, 从而 $2^p - 2$ 可以被 p 整除。可以认识到这实际上是费马小定理的特殊情况。这实际上给了我们一种启发, 是否我们能参考定理五和定理六的证明的过程来证明费马小定理。

14. 定理七(费马小定理)

设 r 是一个整数, p 是一个质数, 那么根据费马小定理(Fermat's Little Theorem), 就有 $r^p - r$ 可以被 p 整除。

现在让我们仔细回顾一下定理五和定理六, 我们会发现, 我们可以根据如下的步骤来证明费马小定理。

1) 让我们先证明 $\frac{p!}{n_1! \cdot n_2! \cdots n_r!}$ 是一个正整数且可以被 p 整除, n_1, n_2, \dots, n_r 都是不等于 p 的非负整数且满足条件 $n_1 + n_2 + \dots + n_r = p$, r 是一个正整数, p 是一个质数。

2) 之后我们来证明多项式定理, 并且通过多项式定理证明 $r^p = \sum_{n_1+n_2+\dots+n_r=p} \frac{p!}{n_1! \cdot n_2! \cdots n_r!}$, 其中 r 是

正整数, p 是质数, n_1, n_2, \dots, n_r 是非负的整数。

3) 最后我们再结合 1) 和 2), 就可以由 r 是一个正整数, n_1, n_2, \dots, n_r 都是非负的整数且均不等于 p , 知道等式 $r^p - r = \sum_{n_1+n_2+\dots+n_r=p} \frac{p!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!}$ 的右边必然可以被 p 整除, 进而等式的左边也可以被 p 整除。

而虽然此时的 r 是正整数, 但这丝毫不影响在 r 为整数的时候费马小定理还是成立的, 因为显然如果 $r^p - r$ 可以被 p 整除, 那么 $-(r^p - r) = (-r)^p - (-r)$ 也可以被 p 整除, 再加上 0 又能被任何非零的整数整除即可。对于 $p=2$ 的情形, 我们只需要记得 $(r+1) \cdot r = r^2 + r$, $r^2 + r$ 必然可以被 2 整除, 因为很明白两个连续的整数中必然有一个是偶数。

证明 1): 我们只需要回忆起定理四就可以发现

$$C_{n_1}^p \cdot C_{n_2}^{p-n_1} \cdot C_{n_3}^{p-n_1-n_2} \cdot \dots \cdot C_{n_r}^{p-n_1-n_2-\dots-n_{r-1}} = \frac{p!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!}, \quad p = \sum_{i=1}^r n_i。$$

因为等式的左边根据引理一我们知道是正整数之间的乘法, 所以他们的乘积依然是正整数, 进而等式的右边必然是一个正整数。

现在又由 $\frac{p!}{n_1! \cdot n_2! \cdot \dots \cdot n_i! \cdot \dots \cdot n_s! \cdot \dots \cdot n_r!} \cdot \frac{n_i}{n_s+1} = \frac{p!}{n_1! \cdot n_2! \cdot \dots \cdot (n_i-1)! \cdot \dots \cdot (n_s+1)! \cdot \dots \cdot n_r!}$, 其中 s 和 r 为不同的正整数且 $1 \leq s, i \leq r$ 。

所以我们只需要选取 $n_1 = p-1, n_2 = 1, n_3 = n_4 = \dots = n_r = 0$ 时, 我们就能够得到 $\frac{p!}{n_1! \cdot n_2! \cdot \dots \cdot n_i! \cdot \dots \cdot n_s! \cdot \dots \cdot n_r!} = p$, 其必然可以被 p 整除, 从而再结合引理三, 我们就证明了 1)。

证明 2): 如果我们采用组合数学中的方法来证明多项式定理那定然很好, 在很多书中[3]也有证明, 不过这里我还是希望使用数学归纳法来证明多项式定理。

$$\text{我们往证(多项式定理)} \quad (a_1 + a_2 + \dots + a_r)^k = \sum_{n_1+n_2+\dots+n_r=k} \frac{k!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!} \cdot a_1^{n_1} \cdot a_2^{n_2} \cdot \dots \cdot a_r^{n_r}$$

其中 a_1, a_2, \dots, a_r 是实数, n_1, n_2, \dots, n_r 和 k 是不为负的整数。

对于 $k=2$ 的情形, 多项式定理将退化为二项式定理, 我们已经讨论过了。

让我们假设有某大于等于 2 的正整数 $t-1$, 在 $r=t-1$ 时我们有

$$(a_1 + a_2 + \dots + a_{r-1})^k = \sum_{n_1+n_2+\dots+n_{r-1}=k} \frac{k!}{n_1! \cdot n_2! \cdot \dots \cdot n_{r-1}!} \cdot a_1^{n_1} \cdot a_2^{n_2} \cdot \dots \cdot a_{r-1}^{n_{r-1}}$$

那么对于 $(a_1 + a_2 + \dots + a_{r-1} + a_r)^k$, 我们由

$$\begin{aligned} & (a_1 + a_2 + \dots + a_{r-1} + a_r)^k \\ &= [(a_1 + a_2 + \dots + a_{r-1}) + a_r]^k \\ &= \sum_{n_r=0}^k \left[\frac{k!}{n_r! \cdot (k-n_r)!} \cdot \sum_{n_1+n_2+\dots+n_{r-1}=k-n_r} \frac{(k-n_r)!}{n_1! \cdot n_2! \cdot \dots \cdot n_{r-1}!} \cdot a_1^{n_1} \cdot a_2^{n_2} \cdot \dots \cdot a_{r-1}^{n_{r-1}} \right] \\ &= \sum_{n_1+n_2+\dots+n_r=k} \frac{k!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!} \cdot a_1^{n_1} \cdot a_2^{n_2} \cdot \dots \cdot a_r^{n_r} \end{aligned}$$

即证多项式定理。

现在, 我们只需要取 $a_1 = a_2 = \dots = a_r = 1$, 那么我们就有 $r^k = \sum_{n_1+n_2+\dots+n_r=k} \frac{k!}{n_1! \cdot n_2! \cdot \dots \cdot n_r!}$

接下来, 只需要取 $k=p$, p 是一个质数, 然后我们遵照 3) 中的说明, 证明费马小定理。

一个非常显然的推论是如果 r 不等于 p ，那么根据引理三，我们有 $r^{p-1} - 1$ 可以被 p 整除。

15. 结语

本文主要用代数方法讨论了 C_b^a 的诸多性质，最后我给出了一种办法证明费马小定理，这是在初等数论中极为重要的定理，它被广泛运用尤其是密码学当中。我的这种办法的优点在于是极便于理解的，学生不必学习同余和模运算的知识就能够了解证明费马小定理的办法，可是一个不可避免的缺点是，这种证明办法会比利用同余知识的办法的显得复杂一些，尽管过程都是初等的。

事实上，由代数方法我还能得出 C_b^a 的一些其他性质，读者大可以参照这里的思路进行研究。

致 谢

在写作时我曾得到很多人的帮助，在此向他们表达感谢。

参考文献

- [1] Shklarsky, D.O., Chentzov, N.N. and Yaglom, I.M. (1993) The USSR Olympiad Problem Book. English Edition, Dover Publications.
- [2] Euler, L. (1736) A Proof of Certain Theorems Regarding Prime Numbers.
<https://scholarlycommons.pacific.edu/euler-works/54/>
- [3] Brualdi, R.A. (2004) Introductory Combinatorics. Fourth Edition, Pearson Education.