现代数学译丛

组合数学

（附：组合矩阵论）

〔美〕H.J.赖瑟 著

科学出版社

现代数学译丛

组合数学

（附：组合矩阵论）

〔美〕H. J. 赖瑟 著

李乔 译

科学出版社

内 容 简 介

随着近代科学技术的发展，近几十年来组合数学的应用日趋广泛，本书简单扼要且又比较完整地阐述了组合数学的基本理论．正文分为九章，前三章主要讲计数问题方面的经典内容，后六章依次为 Ramsey 定理，相异代表组，(0，1)-矩阵，正交拉丁方，组合设计和完备差集．每章后都附有直到原书出版时为止所发表的详细的参考文献．

本书正文之后的"组合矩阵论"是作者于本书出版约十年之后完成的，是对(0，1)-矩阵的组合方面的研究的一个概述，由于内容与本书正文一脉相承且有所补充，故译出作为本书的附录．

本书曾经魏万迪、陶懋颀等同志审阅，最后由陶懋颀同志校订整理．

本书可供数学工作者、高等院校数学系师生、有关的科技人员阅读．

H. J. Ryser
COMBINATORIAL MATHEMATICS
The Mathematical Association of America, 1963

现代数学译丛
组 合 数 学
（附：组合矩阵论）
〔美〕H. J. 赖 瑟 著
李 乔 译

责任编辑 杜小杨 张鸿林
科学出版社 出版
北京朝阳门内大街 137 号

中国科学院印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*

1983年 8月第 一 版 开本：850×1168 1/32
1983年 8月第一次印刷 印张：4 1/2
印数：0001—12,900 字数：114,000

统一书号：13031·2336
本社书号：3197·13—1

定价： 0.86 元

序

本书并不要求对组合数学具备任何预备知识．在第一章中，我们讨论集合的一些基本性质，并定义排列、组合和二项式系数．当然，我们是从一种成熟的观点来处理这些概念的，而且从开始起，就设想读者能体味数学推理的精妙之处．把组合数学放在近世代数的体系中来研究最合适，因此，我们事先假定读者对少量代数概念有所了解．矩阵是真正重要的工具，它贯穿本书始终，并把很多章节沟通起来．开始时，矩阵主要是一些长方阵列，很少需要有关背景．以后它愈益重要，并用到一些矩阵演算的常见性质．数论用得很少，在大多数情况下懂一点整数同余式就够了．群和域只是顺便提到一下．此外，只在极个别的场合才涉及其它概念．

本书的证明大都用数数（shǔ shù）论证法、有限归纳法或其它一些久经考验的方法．这并不等于说组合数学容易掌握．事实上，这门学科研究起来固属不易，叙述起来亦颇费事．我们的定义和定理的证明都很简要，值得仔细推究．但勤学巧思出高艺，而得其要者定将收益匪浅．

我们对有些论题探讨得比较透彻，并达到目前研究的第一线．但为此也舍去了相当一部分有意义的内容．每章分别附有参考文献，它们是进一步研究的指南，并不求其完备无遗．我们还讨论了一些至今尚未解决的重要问题．现阶段组合数学非常活跃，我们相信，它的许多最重要的结果尚待揭示．

H. J. 赖　瑟

1963 年 2 月于锡拉丘兹大学

目　　录

第一章　组合数学的基础

§ 1. 何谓组合数学?

组合数学，也称作组合分析或组合学，是自古就有的数学分支．据传说，禹在公元前 2200 多年就观察到神龟背上的幻方

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}.$$

公元前 1100 多年，在中国已隐约产生了排列的概念．公元 1140 年 Rabbi Ben Ezra 似乎已知道从 n 个事物中同时取出 r 个的组合数的公式.古代有关这方面的知识大多联系着数的神秘主义;而近几个世纪来,许多作者又从数学游戏的角度接触这个课题．Bachet 的砝码问题，Kirkman 的女生问题和 Euler 的 36 名军官的问题等等,都是这方面有名的例子．这些问题很能推动人们去思索,它们的解答也常常是机智和精巧的.

过去为了娱乐或由于其美学上的魅力而被研究的很多这类问题,现在在纯粹和应用科学上都有重要的价值．不久以前,有限射影平面还只被当作一种组合的珍玩．今天，它在几何基础以及试验的分析和设计中都是基本的．由于离散性问题在现代技术中的极端重要性,过去的趣味数学也被赋予了新的严肃的目的.

更重要的是，现时代为组合数学展现了一系列有吸引力的新问题的广阔范围．这些问题出自抽象代数、拓扑学、数学基础、图论、博弈论、线性规划以及许多其它领域．组合学从来就很驳杂.在我们的时代,这种多样性更是大大地增加了.它的各种各样的问题不能在一个统一的理论中有效地着手解决．以上所述大部分对数论也同样适用．事实上，组合学和数论可以说是姐妹学科．它们在内容上有一定的共同部分,而且彼此真正地互相充实丰富.

组合数学与很多数学分支相交叉，因此很难对它下一个正式的定义．不过大体上可以说，组合数学从事于把一些元素安排成种种集合的研究．这些元素的个数通常是有限的，而这种安排必须服从所论问题提出的限制条件．文献中有两大类问题．在第一类问题中，所论组态 (configuration) 的存在尚待证实，而我们的研究在于对此作出明确的断言．这类问题称为存在问题．在第二类问题中，已知组态的存在，而我们的研究在于确定组态的数目或作出这些组态的分类．这类问题称为计数问题．本书侧重讨论存在问题，但许多计数问题也时常出现．

或许会认为，第二类问题不过是第一类问题的细致化或明显的推广．是有这种情形．但实际上，如果需要很费劲才能搞清楚组态的存在，则对相应的计数问题几乎一无所知．另一方面，如果计数问题容易处理的话，则相应的存在问题通常是不足道的．

我们用一个初等的例子来解释上述说明．在一个横竖各八格的正方形棋盘上，去掉对角上的两格．现有 31 张骨牌，每张骨牌正好能盖住棋盘的相邻两格．现在的问题是用这 31 张骨牌完全盖住这个去掉了对角上两格的棋盘．在这个问题中，解的存在尚待证实．事实上，我们说这种覆盖是不可能的．设想棋盘上全部 64 个格子黑白相间．如果去掉两个黑格或两个白格，则棋盘上留下的黑白格数不等．但一张骨牌在棋盘上一定同时盖住一黑格和一白格．由于棋盘的对角上的两格必同黑或同白．因此，所要求的覆盖是不可能的．如果对角上两格不去掉，则有许多种方法使 32张骨牌盖住整个棋盘．这时所要讨论的就是确定有多少种不同覆盖方法的计数问题了．

§2. 集合

设 S 是一个元素为 $a, b, c, \cdots$ 的任意集合．我们用 $s \in S$ 来表示 s 是 S 的一个元素．如果集合 A 的每一个元素都是集合 S 的元素，则称 A 为 S 的一个子集，记为 $A \subseteq S$．如果 $A \subseteq S$ 和 $S \subseteq A$ 都成立，则集合 A 与集合 S 等同，记为 $A=S$．如果 $A \subseteq S$，但 $A \neq S$，

则 A 是 S 的一个真子集，记为 $A\subset S$．S 的所有子集的集合记为 $P(S)$．为方便起见，空集或零集 $\varnothing$ 也算成 $P(S)$ 的一个成员．

设 S 和 T 是集合 M 的子集．M 中同时满足 $e\in S$ 和 $e\in T$ 的元素 e 的集合称为 S 和 T 的交，记为 $S\cap T$．更一般些，如果 T_1，T_2，$\cdots$，T_r 是 M 的子集，则 $T_1\cap T_2\cap\cdots\cap T_r$ 表示同时满足 r 个关系 $e\in T_i(i=1,2,\cdots,r)$ 的元素 e 的集合．如果 M 的子集 S 和 T 没有公共元素，则称 S 和 T 不交 (disjoint)．关系式 $S\cap T=\varnothing$ 表示 S 和 T 不交．M 中满足 $e\in S$ 或 $e\in T$ 的元素 e 的集合称为 S 和 T 的并，记为 $S\cup T$．更一般些，如果 $T_1,T_2,\cdots,T_r$ 是 M 的子集，则 $T_1\cup T_2\cup\cdots\cup T_r$ 表示元素 e 的集合，这种 e 至少满足 r 个关系 $e\in T_i(i=1,2,\cdots,r)$ 中的一个．M 的子集 $T_1,T_2,\cdots,T_r$ 如果满足 $M=T_1\cup T_2\cup\cdots\cup T_r$ 以及 $T_i\cap T_j=\varnothing(i\neq j;\ i,j=1,2,\cdots,r)$，则称 $T_1,T_2,\cdots,T_r$ 组成 M 的一个划分 (partition)．划分有有序及无序两种．M 的两个有序划分 $M=T_1\cup T_2\cup\cdots\cup T_r$ 和 $M=T_1'\cup T_2'\cup\cdots\cup T_r'$ 相等，表示 $T_i=T_i'(i=1,2,\cdots,r)$ 成立；M 的两个无序划分 $M=T_1\cup T_2\cup\cdots\cup T_r$ 和 $M=T_1'\cup T_2'\cup\cdots\cup T_r'$ 相等，表示每一个 T_i 分别等于某一个 T_j'．

只含有限个元素的集合称为有限集．如果一个有限集的元素个数是 n，则称它是 n 个元素的集合．用这个名词时，我们约定 $n>0$，即不包括零集 $\varnothing$．本书称 n 个元素的集合为 n-集．于是，一个 n-集的一个 r-子集，表示一个 n 个元素的集合中的一个有 r 个元素的子集．很多数数论证广泛使用下述初等原理．

设 S 是一个 m-集，T 是一个 n-集．如果 $S\cap T=\varnothing$，则 $S\cup T$ 是一个 $(m+n)$-集．此即所谓加法法则．推广的加法法则说：如果 T_i 是 n_i-集 $(i=1,2,\cdots,r)$，并且 $M=T_1\cup T_2\cup\cdots\cup T_r$ 是 M 的一个划分，则 M 是一个 $(n_1+n_2+\cdots+n_r)$-集．

设 S,T 是两个集合．对 $s\in S$ 和 $t\in T$，记 (s,t) 为一有序对．两个有序对 (s,t) 和 (s^*,t^*) 相等，当且仅当 $s=s^*,t=t^*$．所有这种有序对构成的集合称为 S 和 T 的积集，记作 $S\times T$．用

$M(S, T, n)$ 记形如 (s, t) 的有序对的一个集合，其中 s 可以是 S 的任意元素，但每个 $s \in S$ 恰好与 n 个元素 $t \in T$ 相配对. 这里 S 中的不同元素并不一定与 T 的同一个 n-子集的元素相配对. 上述记号表明 T 至少含有 n 个元素. 而且 $M(S, T, n) = S \times T$ 当且仅当 T 是 n-集. 现设 S 是一个 m-集，则 $M(S, T, n)$ 是一个 (mn)-集. 此即所谓乘法法则. 推广的乘法法则说: 如果 T_1 是 n_1-集，又记 $M_2 = M(T_1, T_2, n_2)$, $M_3 = M(M_2, T_3, n_3)$, $\cdots$, $M_r = M(M_{r-1}, T_r, n_r)$, 则 M_r 是 $(n_1 n_2 \cdots n_r)$-集.

§3. 样品

设 S 是一个集合，并设

$$(a_1, a_2, \cdots, a_r) \tag{3.1}$$

是一个有序 r-组，其中 $a_1, a_2, \cdots, a_r$ 是 S 的元素，但不一定互不相同. 两个这种 r-组 $(a_1, a_2, \cdots, a_r)$ 和 $(a_1^*, a_2^*, \cdots, a_r^*)$ 相等，当且仅当 $a_i = a_i^* (i = 1, 2, \cdots, r)$ 成立. 我们称(3.1)为 S 的一个样品. 样品(3.1)的大小是 r，故把(3.1)称为 S 的一个 r-样品.

定理 3.1. 一个 n-集的 r-样品的个数为 n^r.

证. 设 S 是 n-集. 本定理是当 $T_1 = T_2 = \cdots = T_r = S$ 和 $n_1 = n_2 = \cdots = n_r = n$ 时推广的乘法法则的特殊情形.

设 S 是 n-集，并设 S 的一个 r-样品(3.1)的各个分量 a_i 互不相同，则称这种 r-样品为 n 个元素的一个 r-排列. 对一个 r-排列来讲，必有 $r \leqslant n$. 我们称一个 n-排列为 n 个元素的一个排列.

定理 3.2. n 个元素的 r-排列的个数为

$$P(n, r) = n(n-1)\cdots(n-r+1). \tag{3.2}$$

证. 本定理是当 $T_1 = T_2 = \cdots = T_r = S$, $n_1 = n$, $n_2 = n-1$, $\cdots$, $n_r = n-r+1$ 时推广的乘法法则的特殊情形.

由(3.2)式可知，$P(n, n)$ 是头 n 个正整数的乘积. 称 $P(n, n)$ 为 n-阶乘，记作 $n!$. 即

$$P(n, n) = n! = n(n-1)\cdots 1. \tag{3.3}$$

推论 3.3. n 个元素的排列的个数为 $n!$.

集合 S 到集合 T 中的(单值)映射 α 是一种对应，在这种对应下,每一个 $s\in S$，必有唯一的一个 $t=s\alpha\in T$ 与之相结合．元素 $s\alpha$ 称为 s 在映射 α 作用下的象． S 到 T 中的两个映射 α 和 β 称为相等,如果 $s\alpha=s\beta$ 对所有 $s\in S$ 成立． 如果每个 $t\in T$ 都是某个 $s\in S$ 的像,映射 α 称为是 S 到 T 上的映射．如果 S 到 T 上的映射使 S 的不同元素有不同的象，则称这个映射是一一的． 现设 $G(S)$ 是 S 到自身上的所有一一映射的集合．如果 $\alpha\in G(S)$，$\beta\in G(S)$，则把 $s\in S$ 映为 $(S\alpha)\beta\in S$ 的映射也是一一映射，称它为映射 α 与 β 的乘积． 于是 $G(S)$ 是以上述乘积作为二元合成关系的代数系统,并可验证 $G(S)$ 满足群的公理．

设 S 是一个 n-集，其元素标记为 $1, 2, \cdots, n$，则 $G(S)$ 称为 n 级对称群,记作 S_n.设 α 是 S_n 的元素,并且 α 把 i 映为 $i\alpha(i=1, 2, \cdots, n)$，则一一映射 α 可以由排列

$$(1\alpha, 2\alpha, \cdots, n\alpha) \tag{3.4}$$

来刻划． 反之,n 个元素的每一个排列实际上是这个 n-集到自身上的一个一一映射．一个群的元素个数称为它的阶．我们可以用群论的语言来叙述推论 3.3.

推论 3.4. S_n 的阶是 $n!$.

例．(a) 3 个元素的 2-排列个数是 $P(3, 2)=3\cdot 2=6$． 如果元素标记为 1, 2, 3,这些 2-排列为

$$(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2).$$

(b) 用英文字母可以造出 26^5 个 5 个字母的字． 由 5 个不同的字母组成的字的个数为

$$26\cdot 25\cdot 24\cdot 23\cdot 22=7{,}893{,}600.$$

(c) S_{100} 约等于 $(9.3326\cdots)10^{157}$,照 Eddington 的估计,宇宙中电子的总数不过 $(136)2^{256}$.

(d) 设 A 是 m 行 n 列的矩阵,其元素都是整数 0 或 1，则这种矩阵共有 2^{mn} 个.当 $m=n=100$ 时,就有 $2^{10,000}$ 个这种矩阵.

§4. 无序选取

设 S 是一个集合,并设

$$\{a_1, a_2, \cdots, a_r\} \tag{4.1}$$

是一个无序 r-组,其中 $a_1, a_2, \cdots, a_r$ 是 S 的元素,但不一定互不相同. 一个元素在无序 r-组 (4.1) 中出现的次数称为此元素在 (4.1) 中的重数. 两个这种无序 r-组 $\{a_1, a_2, \cdots, a_r\}$ 和 $\{a_1^*, a_2^*, \cdots, a_r^*\}$ 相等,当且仅当每个元素在这两个无序 r-组中的重数相同. 我们称(4.1)式为 S 的一个无序选取. 无序选取 (4.1)式的大小是 r,故称(4.1)式为 S 的一个 r-选取. 如果在(4.1)式中,每个元素的重数都是 1,则此 r-选取是 S 的一个r-子集. 一个 n-集的 r-子集也称为 n 个元素的一个 r-组合.

当 n 是正整数时,(3.3) 式断言

$$n! = P(n,n). \tag{4.2}$$

为方便起见,可以规定

$$0! = 1, \tag{4.3}$$

于是对每个正整数 n,都有

$$n! = n(n-1)!. \tag{4.4}$$

现设 n 和 r 为正整数,并定义

$$C(n,r) = \binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!},$$

$$C(n,0) = \binom{n}{0} = 1, \tag{4.5}$$

$$C(0,r) = \binom{0}{r} = 0,$$

$$C(0,0) = \binom{0}{0} = 1,$$

再规定当 $r > n$ 时,$C(n,r) = 0$,则 (4.5) 式对所有非负整数 n 和 r 都定义了 $C(n,r)$. 这说明当 n 固定时,$C(n,r)$ 只取有限个不同的值. 由(4.5)式所定义的数 $C(n,r)$ 正是熟知的二项系数.

它们在计数问题中非常重要.

定理 4.1. 一个 n-集的 r-子集的个数为$\binom{n}{r}$.

证. 由定理 3.2 可知, n 个元素的 r-排列的个数为 $P(n, r)$. 每个 r-排列可以用 $r!$ 种方法安排次序. 如果不计次序, 即得不同的 r-子集的个数为

$$C(n, r)=\frac{P(n, r)}{r!}. \tag{4.6}$$

设 S 是一个 n-集,又设 $P(S)$ 表示 n-集 S 的所有子集的集合. 设 T 表示元素为整数 0, 1 的一个 2-集的所有 n-样品的集合, 则有 $P(S)$ 到 T 上的一个自然的一一映射: 设 $X=\{a_{i_1}, a_{i_2}, \cdots, a_{i_r}\}\in P(S)$, X 的像是一个 n-样品,这个 n-样品的第 $i_1, i_2, \cdots, i_r$ 个分量为 1,其余 $n-r$ 个分量都为 0. 现在我们可以用定理 4.1 来数出 $P(S)$ 的元素个数, 又可以用定理 3.1 来数出 T 的元素个数. 它们应当相等,故得

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}=2^n. \tag{4.7}$$

当然 (4.7) 不过是一个初等恒等式. 但它的上述证明方法说明了一种在很多组合研究中有效的数数论证法.

定理 4.2. 一个 n-集的 r-选取的个数为

$$\binom{n+r-1}{n-1}=\binom{n+r-1}{r}. \tag{4.8}$$

证. 取 n-集 S 为由正整数 $1, 2, \cdots, n$ 所组成的集合 S',则 S' 的每个 r-选取可以表为

$$\{a_1, a_2, \cdots, a_r\}, \tag{4.9}$$

其中

$$a_1\leqslant a_2\leqslant\cdots\leqslant a_r. \tag{4.10}$$

令 S^* 为正整数 $1, 2, \cdots, n+r-1$ 组成的 $(n+r-1)$-集, 则

$$\{a_1+0, a_2+1, \cdots, a_r+r-1\} \tag{4.11}$$

是 S^* 的一个 r-子集. 而且对应

$$\{a_1, a_2, \cdots, a_r\} \longleftrightarrow \{a_1 + 0, a_2 + 1, \cdots, a_r + r - 1\} \tag{4.12}$$

是从 S' 的所有 r-选取到 S^* 的所有 r-子集上的一一映射．由定理 4.1 可知，S^* 的 r-子集个数为

$$\binom{n+r-1}{r}.$$

故定理得证．

设

$$S = T_1 \cup T_2 \cup \cdots \cup T_k \tag{4.13}$$

是 n-集 S 的一个划分，这里 T_i 是 r_i-子集 $(i = 1, 2, \cdots, k)$，则

$$n = r_1 + r_2 + \cdots + r_k. \tag{4.14}$$

我们称划分 (4.13) 为 S 的一个 $(r_1, r_2, \cdots, r_k)$-划分．

定理 4.3．一个 n-集的有序 $(r_1, r_2, \cdots, r_k)$-划分的个数为

$$\frac{n!}{r_1!r_2!\cdots r_k!}. \tag{4.15}$$

证．根据定理 4.1 以及推广的乘法法则，可知一个 n-集的有序 $(r_1, r_2, \cdots, r_k)$-划分的个数等于

$$\binom{n}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_1-\cdots-r_k}{r_k} = \frac{n!}{r_1!r_2!\cdots r_k!}. \tag{4.16}$$

数 (4.15) 是所谓的多项式系数．从定理 4.3 可以推得 n-集的有序$(1,1,\cdots,1)$-划分的个数为 $n!$，这时定理 4.3 即化为推论 3.3．n-集的有序 $(r, n-r)$-划分个数为

$$\frac{n!}{r!(n-r)!},$$

这时定理 4.3 即化为定理 4.1．

定理 4.3 中的多项式系数还有另一种很有用的组合解释．设 S 是元素为 $a_1, a_2, \cdots, a_k$ 的 k-集，并设

$$n = r_1 + r_2 + \cdots + r_k, \tag{4.17}$$

其中 r_i 都是正整数．设 $(a_{i_1}, a_{i_2}, \cdots, a_{i_n})$ 是 S 的一个 n-样品，其中 a_i 正好出现 r_i 次 $(i = 1, 2, \cdots, k)$．记 T 为所有这种样品的集合，则 T 的元素个数是

$$\frac{n!}{r_1!r_2!\cdots r_k!}. \tag{4.18}$$

因为在每个样品中，r_1 个 a_1 可以换成 r_1 个彼此不同并与样品中其它元素也不同的元素．这 r_1 个新元素可以按 $r_1!$ 种方法在原来都是 a_1 的位置上排列，故每个样品产生出 $r_1!$ 个新样品．在如此产生的新样品的集合中，同样可把每个样品中的 r_2 个 a_2 换成 r_2 个彼此不同并与样品中其它元素也不同的元素，这时每个样品产生出 $r_2!$ 个新样品．继续这种替换手续，最终得到 n 个元素的 $n!$ 个排列．所以 T 的元素个数正如(4.18)所示．

例．(a) 从一副 52 张扑克牌中任取 13 张得一手牌，在每一手牌中不考虑这 13 张牌的次序，则总共有

$$\binom{52}{13}=635,013,559,600$$

手不同的牌．

(b) 把一副 52 张扑克牌分给 4 个人，每人得 13 张，则总共有

$$\frac{52!}{(13!)^4}=(5.3645\cdots)10^{28}$$

种不同的牌局．

(c) 由 4 个 a，4 个 b，2 个 c 和 2 个 d 这 12 个字母能组成

$$\frac{12!}{4!4!2!2!}=207,900$$

个具有 12 个字母的字．

(d) 用字母 a，b，c 组成 5 个字母的字，每个字中 a 至多出现 2 次，b 至多 1 次，c 至多 3 次．这种字的个数为

$$\frac{5!}{2!0!3!}+\frac{5!}{2!1!2!}+\frac{5!}{1!1!3!}=60.$$

(e) 将 r 个骰子掷一次，可以看成一个 6-集的 r-选取．所以总共可能掷出

$$\binom{r+5}{5}=\binom{r+5}{r}$$

种不同结果.

§5. 二项式系数

设 n 和 r 是正整数，则

$$\binom{n}{r}=\binom{n-1}{r}+\binom{n-1}{r-1}. \tag{5.1}$$

公式(5.1)是定义(4.5)的直接推论，它提供了关于二项式系数的一个基本递推公式. §4 的推论告诉我们二项式系数是整数，现在直接用归纳法来证明这个断言. 当 $n=0$ 或 $r=0$ 时，由(4.5)易知结论为真. 如果 n 和 r 都是正整数，由归纳法假设已知(5.1)式右边两项都是整数，所以左边也必为整数. 这个结论可以更醒目地重述为： r 个相继的正整数的乘积可被 $r!$ 整除.

我们把只能被自身以及 1 整除的正整数称作素数.

定理 5.1. 如果 p 是素数，则

$$\binom{p}{1},\binom{p}{2},\cdots,\binom{p}{p-1} \tag{5.2}$$

都能被 p 整除.

证. 设 r 是区间 $1\leqslant r\leqslant p-1$ 中的一个整数，则 $r!$ 可整除

$$p(p-1)\cdots(p-r+1). \tag{5.3}$$

但 $r!$ 与 p 互素，因而 $r!$ 可整除

$$(p-1)(p-2)\cdots(p-r+1). \tag{5.4}$$

所以

$$\binom{p}{r}=p\frac{(p-1)(p-2)\cdots(p-r+1)}{r!} \tag{5.5}$$

能被 p 整除.

公式 (5.1) 指出了一种计算二项式系数的有效程序. 它可以图示如下