科学版

大学数学习题精解系列

制胜数学奥林匹克

〔美〕E.洛桑斯基　C.鲁索　著

- 国际数学奥林匹克竞赛试题详解
- 阐述经典数学知识和思想
- 展示实用解题方法和技巧
- 培养解决数学问题的能力

科学出版社
www.sciencep.com

大学数学习题精解系列

制胜数学奥林匹克

〔美〕E. 洛桑斯基　C. 鲁索 著

侯文华　张连芳 译

刘嘉焜 校

科学出版社

北京

内 容 简 介

本书介绍数学奥林匹克竞赛有关的数学知识以及解题的方法与技巧，目的是培养广大青少年解决较难数学问题的能力. 主要内容包括：数，数学归纳法，同余，级数求和，丢番图方程，代数基本定理，代数方程，经典不等式，组合数学，容斥原理，鸽笼原理和极值问题等.

本书论述严谨，内容丰富. 书中有大量的例题和习题，其中有许多取自历届美国和国际数学奥林匹克数学竞赛. 通过习题的练习可使学生增加学习数学的兴趣和赢得数学奥林匹克竞赛的信心.

读者对象为广大青年学生、中学教师和数学爱好者.

Translation from the English language edition:
Winning Solutions by Edward Lozansky and Cecil Rousseau
Copyright © 1996 Springer Verlag New York, Inc.
Springer Verlag is a company in the Bertelsmann Springer publishing group
All Rights Reserved

图字：01－2001－0351 号
图书在版编目(CIP)数据

制胜数学奥林匹克/(美)E. 洛桑斯基，C. 鲁索著；侯文华，张连芳译；刘嘉焜校. —北京：科学出版社，2003. 3
(大学数学习题精解系列)
ISBN 7-03-010334-3

Ⅰ. 制… Ⅱ. ①洛…②鲁…③侯…④张…⑤刘… Ⅲ. 数学-竞赛题-解题

中国版本图书馆 CIP 数据核字(2002)第 020385 号

责任编辑：[illegible] / 责任校对：包志虹
责任印制：安春生 / 封面设计：黄华斌

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 3 月第 一 版 开本：B5 (720×1000)
2003 年 3 月第一次印刷 印张：11 3/4
印数：1—3 000 字数：222 000

定价：24.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

序

近年来，为有天赋的中学生举办的数学竞赛已经广泛地开展起来了．参加国际数学奥林匹克竞赛 (IMO) 的国家显著增加．在美国， IMO 代表队的成员是通过美国数学奥林匹克 (USAMO) 竞赛选拔出来的，这是和其他大多数参加国类似的选拔程序．因此，这类竞赛的数量不断增加，并进一步增长了培养有数学天才的年轻人的公众兴趣．

大多数高中数学的教学计划内容和参加 IMO 的要求有相当大的差距，本书就是为了缩小这一差距所做的努力．本书是为那些有数学天分但缺少解奥林匹克水平问题所必要的背景和经验的学生写的．我们通过给出有用的定理和技巧，提供适当的例题和习题来介绍这些背景和经验．

本书只包括美国数学奥林匹克和国际数学奥林匹克竞赛中常出现的一些分支．几何与一些其他特别的竞赛内容可参见其他书．书末我们给出了进一步学习的参考书目．

总而言之，本书读者对象是那些还不熟悉奥林匹克竞赛和此类竞赛中常出现的内容的人．直到现在，微积分还不是此类竞赛中的内容．奥林匹克竞赛常常需要使用 Ceva 定理， Chébyshev 不等式，中国剩余定理以及凸集等内容，但是没有微积分．应当指出，本书在选择内容上是有折衷的，我们是根据奥林匹克竞赛的传统与有数学天分的学生的需要来选材的．

在写这本书时，很多人提供了有价值的建议．我们特别要感谢 Basil Gordon (UCLA), Ian McGee (Waterloo 大学) 和 Ron Scoins (Waterloo 大学), 他们对前两章内容提出了很多建议．而 David Dwiggins (Memphis 大学) 仔细地阅读了最后的书稿．

本书前两章是 Cecil Rousseau 在 Waterloo 大学作学术访问期间完成的．他表示感谢 Ron Dunkley 邀请他访问 Waterloo 并感谢帮助他实现这一访问的所有的教职员．

作者 Cecil Rousseau 写这本书是因为有机会参加 USAMO 和 IMO 的工作很多年．该作者是由 Murray Klamkin 邀请加入的，并得到许多其他人包括 Dick Gibbs, Samuel Greitzer, Walter Mientka, Ian Richards, Leo Schneider, 以及数学奥林匹克暑期培训班成员 (Titu Andreescu, Anne Hudson, Gregg Patruno, Gail Ratcliff, Daniel Ullman, Elizabeth Wilmer) 的支持．很多出色的天才学生参加了 USAMO 和 IMO 竞赛及奥林匹克暑期培训班的学习．

最后我们要衷心感谢美国数学竞赛委员会允许我们使用 AIME(美国数学邀请赛) 和 USAMO 中的问题作为本书的例题与习题.

作　者

1996 年 1 月

此为试读,需要完整PDF请访问: www.ertongbook.com

目　录

第一章　数

§1.1　自　然　数

人类最早认识数是通过**计数**开始的，所以我们最先遇到的数集是计数的集合，或者是**自然数**$\{1,2,3,\cdots\}$. 后来，我们的知识扩展到**整数**、**有理数**、**实数**和**复数**. 甚至自然数系的正式的定义也需要仔细地思考，所以直到 1889 年才由意大利数学家 Giuseppe Peano 给出. 我们的方法是非正式的. 假定读者熟悉各种数系. 以下的定义在本书的习题和解答中是通用的.

我们用 $\mathbf{Z}$ 表示整数集 $\{\cdots,-2,-1,0,1,2,\cdots\}$, 用 $\mathbf{Z}^+$ 表示正整数集 $\{1,2,3,\cdots\}$. 我们用**自然数**表示正整数 (数学家不总是认同这一点的，有些人用自然数表示非负整数). 设 a 和 b 是整数，如果存在整数 c 使得 $b=ac$, 我们就说 a **整除** b, 用记号 $a\mid b$ 表示，称 a 是 b 的**除数**或**因数**. p 是大于 1 的自然数，如果 1 和 p 是其仅有的正除数，就称之为**素数**. 不是素数的自然数 $n>1$ 称为**复合数**. 素数列出来是 $2,3,5,7,11,13,\cdots$, 而且没有终点. 素数列没有终点的事实在 Euclid 的著作《几何原本》中证明， Euclid 给出的证明是数学家技巧的典范.

定理 1.1(Euclid)　素数无穷多.

Euclid 的证明是用反证法给出的. 若 $p_1,p_2,\cdots,p_N$ 是所有的素数，那么 $M=(p_1p_2\cdots p_N)+1$ 是不能被任意素数整除的数，而且它还比最大的素数还大，这是不可能的. 本节末第一个练习，读者可以用 Euclid 的证明方法去证明等差级数 $3,7,11,15,19,\cdots$ 中含有无穷多个素数.

a 和 b 是两个不同时为零的整数，它们的**最大公因数**用 (a,b) 表示，指的是满足 $d\mid a$ 和 $d\mid b$ 的最大的自然数 d. 如果 $(a,b)=1$, 就称 a 和 b 是互素的. 下面一个小小的事实是重要理论的基础.

引理 1.1　设 a 和 b 是两个不同时为零的整数，那么 $\{xa+yb\mid x,y\in\mathbf{Z}\}$ 是 (a,b) 的全体整数倍组成的集合. 特别的，(a,b) 是该集合中的最小正数.

为证此，令 M 表示所有形如 $xa+yb$ 的数的全体组成的集，这里 $x,y\in\mathbf{Z}$. 注意，如果 k 在 M 中，那么 k 的倍数也在 M 中，而且如果 k 和 l 在 M 中，那么 $k-l$ 也在 M 中. 易知 M 中包含某些正整数，于是 M 中必包含一个最小的正整数 (见 §1.2), 记该数为 d. 那么 M 恰好是 d 的所有整数倍的集. 因若不然，可找一数 $m\in M$, $\frac{m}{d}=q+\frac{r}{d}$, 这里 $0<r<d$, 由于 $r=m-qd\in M$ 这与 d 是 M 中最小正整数不合. 由于 $a,b\in M$, 我们有 $d\mid a$ 和 $d\mid b$. 另一方面，由于 $d=x_0a+y_0b$ 对某

$x_0, y_0 \in M$ 成立，任一同时整除 a 和 b 的数也一定能整除 d, 这就推出 $d = (a, b)$.

利用引理 1.1, 易证下面基本的结果.

引理 1.2(Euclid 引理) 若 $a \mid bc$ 且 a 和 b 互素，那么 $a \mid c$.

因 a 和 b 互素，故存在 x_0 和 y_0, 使得 $1 = x_0 a + y_0 b$, 于是 $c = x_0 ac + y_0 bc$. 由条件 $a \mid bc$ 可推得 $a \mid c$.

推出 Euclid 引理正确后，容易利用数学归纳法 (§1.2) 证明以下重要的结果.

定理 1.2(算术基本定理) 任一大于 1 的自然数，或者是素数，或者可以唯一(除去因数的次数以外) 写成两个或两个以上素数的乘积.

用符号表示，素因子分解可表示为

$$n = \prod_p p^{e_p(n)}, \quad n > 1,$$

这里 Π_p 表示乘积是依素数 p 进行的，$e_p(n)$ 是 n 的素因子分解中 p 的**指数**. 定理的重要部分是素因子分解的唯一性. 大于 1 的任意整数可以写成素因子的乘积是不难看出的，但只有一种方法表示却不是显然的. 但它的确是对的，而且素因子分解的唯一性的事实是解决许多问题的有力方法.

由于其显然的重要性，从 Euclid 时期到现在，很多研究者包括专业的和业余的数学家都把素数当作重要的研究对象. 许多**不可解问题**涉及素数，这些问题看起来很简单但实际上极其困难. 例如，在 1742 年给 Leonhard Euler 的一封信中，Christian Goldbach 猜想，每一个大于 2 的偶数都可以表示成两个素数的和. Goldbach 猜想至今没有被证明或者被否定，当然我们不去考虑这类问题，我们只限于去解决那些掌握了基本定义和定理可以正确的求解的那些问题.

作为如何应用基本定理的例子，我们考虑如下的简单的问题.

例 1.1 求所有的素数 p, 使得 $17p + 1$ 是完全平方.

解 设 $17p + 1 = n^2$, 于是 $17p = n^2 - 1 = (n-1)(n+1)$. 左端是确定的两个素数的乘积，而右端同样是两个因数的乘积. 如果 $n-1$ 或 $n+1$ 是复合数，那么 $(n-1)(n+1)$ 可进一步分解，最终将是三个或更多个素数的乘积，这与基本定理不合. 事实上由素因子分解的唯一性可推知 $17 = n+1$ 和 $p = n-1$ 或者 $17 = n-1$ 和 $p = n+1$. 前者推出 $p = 15$ 不是素数，而后者得出 $n = 18$, $p = 19$, 这是正确的. 所以 $p = 19$ 是使 $17p + 1$ 为完全平方的唯一解. □

我们经常要计算最大公因数，一个有力的方法很早以前由 Euclid 发现.

定理 1.3(Euclid 算法) 若 $a > b > 0$, $\frac{a}{b}$ 得到商 q 和余数 r, 即

$$\frac{a}{b} = q + \frac{r}{b}, \quad 0 \leqslant r < b,$$

那么 $(a, b) = (b, r)$.

为证此，把 a,b,q,r 的关系式写为 $a=qb+r$，注意到任一数整除 a 和 b 则也能整除 r，而任一数整除 b 和 r 则也能整除 a. 于是 a 和 b 的公因数的集合与 b 和 r 的集合是相同的. 特别的，最大公因数也相同.

为利用此定理计算 (a,b)，我们只要简单地继续使用这一算法，直到余数变为 0 为止. 这样得到一串等式 $(a,b)=(b,r)=\cdots=(d,0)=d$. 由于每个余数都是非负的，而且余数的序列是递减的，所以一定会在某一步余数变为 0.

作为一个例子，我们计算 5999 和 994 的最大公因数. 第一次除法得到 5999/994 =6+35/994，第二次得 994/35=28+14/35，第三次得 35/14=2+7/14，而最后得出 14/7=2 余数为 0，这样我们得到 $(5999,994)=(994,35)=(35,14)=(14,7)=(7,0)=7$.

例 1.2 证明若 a 和 b 是两个任意自然数，那么

$$(2^a-1,2^b-1)=2^{(a,b)}-1.$$

解 注意到 $a=qb+r(0\leqslant r<b)$，我们有

$$x^a-1=(x^b-1)(x^{a-b}+x^{a-2b}+\cdots+x^{a-qb})+x^r-1.$$

特别地，令 $x=2$ 有

$$2^a-1=(2^b-1)Q+2^r-1,$$

其中 $Q=2^{a-b}+2^{a-2b}+\cdots+2^{a-qb}$. 因此

$$(2^a-1,2^b-1)=(2^b-1,2^r-1).$$

现在我们发现 Euclid 算法中的等式串 $(a,b)=(b,r)=\cdots=(d,0)=d$ 在这里变成为 $(2^a-1,2^b-1)=(2^b-1,2^r-1)=\cdots=(2^d-1,0)=2^d-1$. 于是我们证明了 $(2^a-1,2^b-1)=2^{(a,b)}-1$. □

下面问题相当简单，但可让我们综合应用已讨论过的几个结果.

例 1.3 求一个 6 位数 (十进制)，该数的前 3 位和后 3 位数字 (整块) 互换后所得到的 6 位数是原数的 6 倍.

解 设所求的数为 $N=1000A+B$. 这里 A 和 B 都是 3 位数，前 3 位数和后 3 位数整块互换后得到 $1000B+A$. 由条件知 $1000B+A=6(1000A+B)$，由此推出 $5999A=994B$. 利用 $(5999,994)=7$，可得 $857A=142B$ 和 $(857,142)=1$. 由 Euclid 引理知 $857\mid B$，但由于 $0<B<10^3$，故知 $B=857$. 同理 $A=142$，所以 $N=142857$. □

回忆 n 阶乘的定义为对 $n>0$，

$$n!=n\cdot(n-1)\cdots2\cdot1,$$

定义 0!=1. 在许多问题中知道 $n!$ 的素因子分解是很有用的. 但面对这一问题时, 即使对不大的 n, 要解决它看起来都有好像是毫无希望的困难. 例如, 当你要求 $20! = 2432902008176640000$ 如此大的一个数的素因子分解时, 你当然希望要用一台计算机了. 所幸的是, Adrien-Marie Legendre 给出了一个求 $n!$ 素因子分解的精巧的公式, 这对求解很多问题都很有帮助. 为表达 Legendre 的公式我们要应用"取整"函数. 具体的, 取整函数 $\lfloor x \rfloor$ 表示不大于 x 的最大整数.

定理 1.4(Legendre) $n!$ 的素因子分解中, 素数 p 的指数为

$$e_p(n!) = \sum_{r \geqslant 1} \left\lfloor \frac{n}{p^r} \right\rfloor .$$

稍加思考, 这一公式是很显然的. 我们要求 $1 \cdot 2 \cdot 3 \cdots n$ 的素因子分解中 p 的因子个数, 首先在 1 和 n 之间有 $\lfloor \frac{n}{p} \rfloor$ 个 p 的倍数, 即 $p, 2p, \cdots, \lfloor \frac{n}{p} \rfloor p$. 它们中每一个都含有 p 的一个因子. 但其中有 $\lfloor \frac{n}{p^2} \rfloor$ 个 p^2 的倍数, 它们中每一个所含 p 的因子要多出 1 个. 类似的, 在 $\lfloor \frac{n}{p^3} \rfloor$ 个 p^3 的倍数中每一个中含 3 个 p 因子, 又多出 1 个, 如此继续下去, 直到 $\lfloor \frac{n}{p^r} \rfloor = 0$.

历史的注: 公式

$$n! = \prod_{p \leqslant n} p^{\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots}$$

通常被称为 Legendre 公式, 尽管它可能也被其他人独立地发现. 这一公式出现在 1808 年 Legendre 的著作《 Essai sur la théorie des nombres 》第二版上.

利用 Legendre 公式可以求 1000! 的素因子分解中 5 的指数, 有

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 200 + 40 + 8 + 1 = 249.$$

这一结果立刻给出下面问题的解.

例 1.4 求 1000! 的十进制表示中末端零的个数.

解 答案是 249. 由于 1000! 素因子分解中 2 的指数大于 249(如要求是精确值, 可用 Legendre 公式), 所以有一个 5 的因子就有一个 10 的因子. 由于 1000! 的素因子分解中 5 的指数是 249, 故 1000! 的十进制表示中末端零的个数是 249. □

例 1.5 若 m 和 n 是正整数, 则

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

是正整数.

解 由 Legendre 公式, 只需证明

$$\left\lfloor \frac{2m}{p^k} \right\rfloor + \left\lfloor \frac{2n}{p^k} \right\rfloor \geqslant \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor + \left\lfloor \frac{m+n}{p^k} \right\rfloor$$

此为试读,需要完整PDF请访问: www.ertongbook.com

对任意 p 和 k 成立. 更一般的, 只要证

$$\lfloor 2a\rfloor+\lfloor 2b\rfloor\geqslant\lfloor a\rfloor+\lfloor b\rfloor+\lfloor a+b\rfloor$$

对任意实数 a,b 成立即可. 为证此, 注意到对任意实数 x 我们可写 $x=\lfloor x\rfloor+\{x\}$, 这里 $\{x\}$ 表示 x 的**小数部分**, 满足 $0\leqslant\{x\}<1$. 将 $a=\lfloor a\rfloor+\{a\}$ 和 $b=\lfloor b\rfloor+\{b\}$ 代入上式, 要证的不等式可化为 $\lfloor 2x\rfloor+\lfloor 2y\rfloor\geqslant\lfloor x+y\rfloor$, 这里 $x=\{a\}$, $y=\{b\}$. 由于 $x+y<2$, 当 $x\geqslant\frac{1}{2}$ 或 $y\geqslant\frac{1}{2}$ 时等式显然成立. 当 $x<\frac{1}{2}$ 和 $y<\frac{1}{2}$ 同时成立时, 不等式两端都为 0, 不等式也成立. □

下面的例题来自 IMO, 是另一个应用 Legendre 公式的很好的例子. 作为预备, 先回忆非零整数集 $\{a_1,a_2,\cdots,a_k\}$ 的**最小公倍数**(LCM) 是可以被每一个 a_i 整除的最小自然数, 记做 $\mathrm{LCM}(a_1,a_2,\cdots,a_k)$. **二项式系数** 定义为

$$\binom{n}{k}=\frac{n!}{k!(n-k)!}.$$

$\binom{n}{k}$ 表示从 n 个不同的元素中选 k 个为一组的选法总数, 它是二项式 $(x+y)^n$ 展开式中 $x^{n-k}y^k$ 的系数.

例 1.6 证明 $\binom{2n}{n}$ 整除 $\mathrm{LCM}(1,2,\cdots,2n)$.

解 记 $\{1,2,\cdots,2n\}$ 的最小公倍数为 L, $M=\binom{2n}{n}$. 为证 $M\mid L$, 只要证对每一素数 p, $e_p(M)\leqslant e_p(L)$ 即可. 由于 L 是可以被 $1,2,\cdots,2n$ 中每一个数整除的最小的自然数, 可以推知 $e_p(L)$ 是满足 $p^m<2n$ 的最大整数 m, 即 $m=\lfloor\log(2n)/\log p\rfloor$. 由 Legendre 公式可知

$$e_p(M)=e_p((2n)!)-2e_p(n!)=\sum_{r=1}^{m}\left\{\left\lfloor\frac{2n}{p^r}\right\rfloor-2\left\lfloor\frac{n}{p^r}\right\rfloor\right\}.$$

(由于 $r>m$ 时 $p^r>2n$, 和式中已包括了所有消失为零的那些项了) 注意 $\lfloor 2x\rfloor-2\lfloor x\rfloor$ 或者是 0, 或者是 1(这依赖于 $x-\lfloor x\rfloor$ 是否小于 $\frac{1}{2}$). 由此上面和式中的项或者是 0 或者是 1, 所以有 $e_p(M)\leqslant M=e_p(L)$. □

上面结果可以用于 Chebyshev 关于素数的一个著名结论的一个初等的证明中. 令 $\pi(x)$ 表示不大于 x 的素数的个数. Chebyshev 用一个初等的论述证明了存在正常数 A 和 B, 使得

$$A\frac{x}{\log x}<\pi(x)<B\frac{x}{\log x}.$$

(这里 $\log x$ 表示 x 的自然对数.) 晚些时候, Hadamard 和 de la Vallée Poussin 各自独立的证明了当 x 无限增大时, $\pi(x)\log x/x$ 趋近于 1. 这就是著名的**素数定理**.

例 1.7 设 $\nu_p(n)$ 表示 n 的 p 进制表示中数字的和. $n!$ 的素因子分解中 p 的指数与 $\nu_p(n)$ 有以下关系:

$$e_p(n!)=\frac{n-\nu_p(n)}{p-1}.$$

解 设 $n = d_0 + d_1 p + \cdots + d_r p^r, 0 \leqslant d_i < p$. 则有

$$\begin{aligned}\left\lfloor \frac{n}{p} \right\rfloor &= d_1 + d_2 p + \cdots + d_r p^{r-1},\\ \left\lfloor \frac{n}{p^2} \right\rfloor &= d_2 + d_3 p + \cdots + d_r p^{r-2},\\ &\cdots\cdots\\ \left\lfloor \frac{n}{p^r} \right\rfloor &= d_r,\end{aligned}$$

于是由 Legendre 公式可得

$$e_p(n!) = d_1 + d_2(p+1) + d_3(p^2+p+1) + \cdots + d_r(p^{n-1} + \cdots + 1),$$

也就是

$$(p-1)e_p(n!) = d_1(p-1) + d_2(p^2-1) + \cdots + d_r(p^r - 1) = n - \nu_p(n). \qquad \square$$

下面记 $a(n) = e_2(n!)$, 而 $b(n)$ 表示 n 的二进制表示中 1 的个数.

例 1.8 令 $B(m)$ 表示整数 r 的集, 对这样的 r, m 的二进制表示中有 2^r 这样的项. 例如 $B(100) = \{2, 5, 6\}$. 证明 $\binom{n}{k}$ 是奇数的充要条件是 $B(k) \subseteq B(n)$.

解 例 1.7 中当 $p = 2$ 时的结果可推出 $a(m) + b(m) = m$ 对任意非负整数 m 都成立. 由此可知 $\binom{n}{k}$ 的素因子分解中 2 的指数为

$$e_2\left(\binom{n}{k}\right) = a(n) - a(k) - a(n-k) = b(k) + b(n-k) - b(n).$$

注意 $b(k)+b(n-k)-b(n) = 0$ 的充要条件是 k 和 $n-k$ 的二进制表示中做加法没有进位. 由此可知 $b(k)+b(n-k)-b(n) = 0$ 的充要条件是 $B(k) \subseteq B(n)$. 由上面的关系式, 若 $b(k)+b(n-k)-b(n) = 0$, 则 $\binom{n}{k}$ 是奇数; 反之, 若 $b(k)+b(n-k)-b(n) \geqslant 1$, 则 $\binom{n}{k}$ 是偶数. 我们将在 §1.3 中给出这一结论的另一个证明. $\square$

最后一个涉及素因子分解的例子将引进一个重要的数论函数.

例 1.9 若是 $n = p^r$, p 素数. 求满足如下条件的整数 k 的个数: $1 \leqslant k < n$ 且 $(n, k) = 1$.

解 先考虑 1 和 $n = p^r$ 之间与 n 不互素的那些数, 这样的数只有 p 的倍数, 即 $p, 2p, 3p, \cdots, p^r$, 共有 p^{r-1} 个这样的数. 去掉这些数, 剩下的数就是我们要求的数. 这样一来, 满足 $1 \leqslant k < p^r$ 和 $(p^r, k) = 1$ 的整数 k 的个数是

$$p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right).$$

这就是我们要求的数. $\square$

当 n 不是形如 p^r 的数时情况如何呢？对于 $n \geqslant 1$ 我们定义 $\phi(n)$ 是满足 $1 \leqslant k \leqslant n$ 和 $(n,k)=1$ 的整数 k 的个数. 如果发现 ϕ 有很好的性质，这使我们可以利用例 1.9 的结果计算出一般情形下 ϕ 的值. 可以证明，若 $(a,b)=1$，则 $\phi(a,b)=\phi(a)\phi(b)$. (一个函数 f，当 $(a,b)=1$ 时有性质 $f(ab)=f(a)f(b)$，就称是**可乘的**. 在数论中，可乘函数有重要的作用.) 由此可以推出，若

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

是 n 的素因子分解，则

$$\begin{aligned}\phi(n) &= p_1^{r_1}\left(1-\frac{1}{p_1}\right)\cdots p_m^{r_m}\left(1-\frac{1}{p_m}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_m}\right).\end{aligned}$$

这一函数就是 Euler 的 ϕ 函数，它将在 §1.3 中再次出现.

§1.1 的练习

1. 证明等差级数 $3,7,11,15,\cdots$ 中含有无穷多个素数.

提示：设 $p_1,p_2,\cdots,p_N$ 是该数列中的全部素数. 考虑 $M=4p_1p_2\cdots p_N-1$，显然，M 不能被 2 整除，也不能被任一个素数 $p_1,p_2,\cdots,p_N$ 整除. 又问 M 的每一个素因子能否属于级数 $5,9,13,17,21,\cdots$?

2. 求所有使 n^4+4 是素数的自然数 n.

3. 求所有使 $2^8+2^{11}+2^n$ 是完全平方的自然数 n.

4. 求所有形如 $aabb$ 的四位完全平方数.

5. 证明对一切 n, $(3n+4,2n+3)=1$.

6. 证明 5 个连续整数的平方和不是完全平方数.

7. 证明 3 个连续自然数的积不是完全乘方 (即完全平方，完全立方，$\cdots$). 提示：将乘积表示成 $(n-1)n(n+1)$.

8. 求十进制的四位完全平方数 N，它的每一位数字都小于 7，而且各位数字都加上 3 得到另一个完全平方数.

9. 如果存在整数 a 和 b 使得 $N=a^2+b^2$，就称 N 是二平方数之和. 证明若 N 是二平方数之和，则 $2N$ 也是. 并证明更一般的结果：若 M 和 N 都是二平方数之和，那么 MN 也是二平方数之和.

10. 在古罗马的拜占庭有一种类似于篮球的比赛，规定一次拦截得分记 a 分，一次直接投篮得分记 b 分. 在一份残存的手稿上没有记录下 a 和 b 的值. 但我们知道在这种比赛中恰有 14 个自然数是不可能的得分值，而且知道其中一个不可能得分值是 22. 假设 $a>b$，试确定 a 和 b 的值.

提示：先证明下面一般性的结论. 若 a 和 b 是互素的自然数，那么恰有 $(a-1)(b-1)/2$ 个自然数，不能表示为 $xa+yb$ 的形式，x 和 y 是非负整数.

11. 证明任意 n 个连续整数的乘积可被 $n!$ 整除.

12. 求所有的 n, 使 $2^{n-1} \mid n!$.

13. 求乘积 $1 \cdot 4 \cdot 7 \cdots 1000$ 中末尾零的个数.

14. 写出 20! 的素因子分解.

15. 证明第 n 个**调和数**

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

不是整数，$n > 1$.

§1.2 数学归纳法

我们常常希望证明一个确定的自然数集实际上就是全体自然数组成的集. 这可以利用下面重要的原理做到.

原理 1.1 (数学归纳法原理) 设 T 是满足以下条件的自然数集：(i) $1 \in T$, (ii) 若 n 是 T 中的一个元，那么 $n+1$ 也是 T 中的元，则可推知 $T = \mathbf{Z}^+$.

数学归纳法原理描述了自然数的一个基本性质. 在 Peano 的自然数理论中，它是公理之一. 它的一个逻辑等价的叙述是**良序原理**.

原理 1.2 (良序原理) 每一个 $\mathbf{Z}^+$ 的非空子集都有一个最小元.

在应用归纳法原理时，给定一列表述 $s_1, s_2, \cdots$，和使得 s_n 为真的所有自然数 n 的集合 T, 要证明对一切自然数 n, s_n 为真，换言之要证 $T = \mathbf{Z}^+$. 可以利用数学归纳法原理只需验证条件 (i) 和 (ii). 这样一来，为证明上列表述中的每一个表述均真，我们只要证明 (i)s_1 真和 (ii) 只要 s_n 真就可推出 s_{n+1} 也真.

在利用良序原理证明同样的事情时，令 F 是使 s_n 假的那些自然数 n 的集. 要证明 F 是空集. 用反证法，假设 F 不空，那么 F 必有最小元 (由良序原理，它是存在的). 最后的目的是要证明这一假设将导致矛盾.

作为一个说明，我们用良序原理来证明数学归纳法原理. 就是说我们给定一个集 T, 它满足 (i) 和 (ii), 要证明 $T = \mathbf{Z}^+$. 若不然，即设 F(在 $\mathbf{Z}^+$ 中，T 的余集) 非空，由良序原理可令 m 是 F 的最小元. 由 (i) 知 $1 \in T$, 故 $m > 1$,所以 $m-1$ 也是自然数. 由于 m 是 F 的最小元，于是可以断言 $m-1 \in T$. 这样一来，假设 F 非空就得出存在一个自然数 m, 使得 $m-1 \in T$, $m \notin T$. 这与 (ii) 矛盾，所以 F 非空不成立，因此 $T = \mathbf{Z}^+$.

在原理 1.1 中，(ii) 可换为 (ii)* 若 $1, 2, \cdots, n$ 是 T 中的元，那么 $n+1$ 也是 T 中的元. 我们称改动后的原理 1.1 为**强归纳法**. 例 1.13 中我们用这种形式的归纳法. 偶尔我们遇到从 $n = n_0 > 1$ 而不是 $n = 1$ 开始归纳. 原理 1.1 的 (i) 改为 (i)

T 包含 n_0, 而结论变为 T 是所有 $n \geqslant n_0$ 的整数全体组成的集. 例 1.14 就利用到归纳法的这一改动.

许多有趣的问题可以用数学归纳法原理求解. 我们从研究求和问题开始. 问题是要证明求和公式

$$\sum_{k=1}^{n} f(k) = F(n)$$

对每一自然数 n 成立. 设 T 为使公式真的自然数的集合. 若 $f(1) = F(1)$, 那么 T 满足数学归纳法原理中的 (i), 而若对每一自然数 n, 等式 $f(1)+f(2)+\cdots+f(n) = F(n)$ 可推出 $f(1) + f(2) + \cdots + f(n+1) = F(n+1)$, 那么 T 就满足条件 (ii). 换言之, 为用数学归纳法证明求和公式对每一自然数 n 都真, 我们只要简单的验证:

(a) $f(1) = F(1)$,

(b) $F(n+1) - F(n) = f(n+1)$,

后一条件对任意 n 都成立. 下面是一个简单的例.

例 1.10 证明对任意自然数 n,

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

解 令 $f(n) = n(n+1)$ 和 $F(n) = n(n+1)(n+2)/3$. 由于 $f(1) = F(1) = 2$, (a) 成立. 为验证 (b), 我们计算 $F(n+1) - F(n)$

$$\begin{aligned} F(n+1) - F(n) &= \frac{(n+1)(n+2)(n+3)}{3} - \frac{n(n+1)(n+2)}{3} \\ &= (n+1)(n+2) \\ &= f(n+1). \end{aligned}$$

于是 (b) 也成立. □

这一结果可以推广到更一般的情形. m 是一个非负整数. 那么

$$\sum_{k=1}^{n} k(k+1)\cdots(k+m) = \frac{n(n+1)\cdots(n+m+1)}{m+2} \tag{1.1}$$

对任一自然数 n 成立. 对 $n = 1$, 等式两端都等于 $(m+1)!$, 所以 (a) 成立. 为验证 (b), 我们计算 $F(n+1) - F(n)$, 这里 $F(n)$ 是 (1,1) 的右端. 化简

$$\frac{(n+1)(n+2)\cdots(n+m+2)}{m+2} - \frac{n(n+1)\cdots(n+m+1)}{m+2}$$

我们有

$$F(n+1) - F(n) = (n+1)(n+2)\cdots(n+m+1) = f(n+1).$$

于是 (1.1) 对所有的自然数 n 成立. 利用这一公式我们可以导出其他的和式. 例如, 由于

$$k^3 = k(k+1)(k+2) - 3k(k+1) + k,$$

前 n 个自然数的立方和可以由

$$\frac{n(n+1)(n+2)(n+3)}{4} - 3\frac{n(n+1)(n+2)}{3} + \frac{n(n+1)}{2}$$

给出. 化简后我们得到

$$\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

例 1.11 证明对任意自然数 n, $n(n-1)(n+1)(3n+2)$ 可以被 24 整除.

解 若 $n=1$,$n(n-1)(n+1)(3n+2)=0$ 显然可被 24 整除. 原理 1.1 中的 (i) 成立. 为证 (ii) 成立, 假设 $24 \mid n(n-1)(n+1)(3n+2)$, 那么由于

$$(n+1)n(n+2)(3n+5) = n(n-1)(n+1)(3n+2) + 12n(n+1)^2,$$

而 $n(n+1)^2$ 必是偶数, 故有 $24 \mid (n+1)n(n+2)(3n+5)$, 归纳法证完. □

涉及递推关系的问题最适于用数学归纳法解决, 下面是一个这方面的简单的例.

例 1.12 若 $a=3$, 且 $a_{n+1} = a_n(a_n+2), n \geqslant 1$. 求此序列的通项公式.

解 试算前三项, 我们有 $a_1 = 3 = 2^2 - 1, a_2 = 15 = 2^4 - 1, a_3 = 255 = 2^8 - 1$, 这显然启发我们猜想, 对任意自然数 n 有

$$a_n = 2^{2^n} - 1.$$

上面我们已经验证过了对 $n=1$ 真, 现假设序列的第 $n-1$ 项是真的, 对 $n>1$, 有

$$a_n = a_{n-1}(a_{n-1}+2) = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = 2^{2^n} - 1,$$

所以上面我们猜想的公式正确. □

例 1.13 假设 $a_1, a_2, \cdots$ 是一列自然数, 对每一个自然数 n, 满足等式

$$\sum_{k=1}^{n} a_k^3 = \left(\sum_{k=1}^{n} a_k\right)^2.$$

试问对任意 k, $a_k = k$ 是等式成立的必要条件吗?

解 答案是 "是". 首先对 $n=1$, 给定的等式推出 $a_1^3 = a_1^2$, 由 $a_1 \neq 0$ 可得 $a_1 = 1$. 现假设对 $k = 1, 2, \cdots, n$, $a_k = k$(强归纳) 成立, 要看是否有 $a_{n+1} = n+1$ 成立. 由归纳假设, 有

$$1^3 + 2^3 + \cdots + n^3 + a_{n+1}^3 = (1 + 2 + \cdots + n + a_{n+1})^2,$$

此为试读,需要完整PDF请访问: www.ertongbook.com