# 何谓数论

关于数论流传着多种说法：成千上万的人们在网上研究共同关心的数论问题．PBS 电视系列节目 NOVA 报道了一个著名数论问题被解决的新闻．人们研究数论是为了理解信息加密系统．这门学问到底是什么？今天为何有那么多人对它感兴趣？

数论是数学的一个分支，研究一类特殊数的性质和相互关系．在数论所研究的数当中，最重要的是正整数集合．更具体地说，特别重要的是*素数*，即那些没有大于 1 并且小于自身的正因子的正整数．数论的一个很重要的结果表明，素数是正整数的乘法结构的基石．这个叫做*算术基本定理*的结果告诉我们，每个正整数可以按递增顺序唯一地写成素数的乘积．对于素数的兴趣要追溯到 2500 年前古希腊数学家的研究工作．人们思考的第一个问题可能是：素数是否有无穷多个．在《几何原本》(The Elements)中，古希腊数学家欧几里得(Euclid)对于素数的无穷性给出了证明．这个证明被认为是所有数学证明中最漂亮的证明之一．17 和 18 世纪研究素数的热情之火被重新点燃，数学家费马(Fermat)和欧拉(Euler)证明了许多重要结果，并且对素数的生成提出许多猜想．素数的研究在 19 世纪取得重大进展，其结果包括：在等差数列中有无穷多素数，对不超过正数 $x$ 的素数个数作了精细的估计等．最近 100 年来发明了研究素数的许多强大的技术方法，但是许多问题用这些方法仍不能解决．比如说，一个未解决的问题是：孪生素数(即相差为 2 的两个素数)是否有无穷多对？下一个十年里肯定还会有新的结果，因为专家们仍在致力于研究与素数有关的许多悬而未决的问题．

现代数论的发展始于德国数学家高斯(Gauss)，他是历史上最伟大的数学家之一，在 19 世纪初期发明了同余的语言．我们称两个整数 $a$ 和 $b$ 是模 $m$ 同余的(其中 $m$ 为正整数)，是指 $m$ 整除 $a-b$．这种语言使我们在研究整除性关系的时候变得像研究方程那样容易．高斯提出了数论中的许多重要概念．例如，他证明了最具智慧和美感的一个结果：*二次互反律*．这个定律把素数 $p$ 是否为模另一个素数 $q$ 的完全平方与 $q$ 是否为模 $p$ 的完全平方联系起来．高斯给出二次互反律的许多不同的证明，其中有些证明开启了数论的一些新领域．

将素数从合数中区分出来是数论的一个关键问题．这方面的工作发展出了大量的*素性检验法*．最简单的素性检验是检查一个正整数是否被不超过此数平方根的每个素数所整除．不幸的是，对于非常大的正整数，这个试验方法效率很低．多种方法被用于确定某个整数是否为素数．例如，在 17 世纪，费马证明了若 $p$ 为素数，则 $p$ 整除 $2^p-2$．一些数学家考虑反过来是否也对(即若 $n$ 整除 $2^n-2$，则 $n$ 必为素数)．但这是不成立的，在 19 世纪初期人们找到反例：对于合数 $n=341$，$n$ 整除 $2^n-2$．这样的整数叫做*伪素数*．尽管存在伪素数，但是多数合数都不是伪素数，基于这个事实给出的素性检验现在仍可用来快速找到一些非常大的素数．然而这种方法并不能用来确定一个整数为素数。寻求有效算法来证明一个整数为素数是一个有几百年历史的问题，但令数学界惊讶的是在 2002 年，这个问题已经由三位印度计算机科学家 Manindra Agrawal，Neeraj Kayal 和 Nitin Saxena 解决。他们

的算法能在多项式时间内证明一个整数 $n$ 是素数(即 $n$ 的位数的多项式时间).

将正整数进行素因子分解是数论中的另一个核心问题. 可以用试除法把一个正整数分解,但是这种方法非常费时间. 费马、欧拉和许多其他数学家提出了一些富有想象力的分解算法,这些算法在过去的 30 年中扩展成一大批因子分解方法. 用目前已知的最先进技术,我们可以很容易地找到几百位甚至几千位长的素数,但是要把同样位长的整数进行因子分解,目前最快的计算机还不能胜任.

找出大素数和分解大数在时间上的强反差是当今一种非常重要的称为 RSA *密码系统*的基础. RSA *系统*是一种公钥密码系统,在此类系统中,每个用户有公私两把密钥. 每个用户可以用别人的公钥来加密信息,但只有拥有相应私钥的用户才能解密. 要明白 RSA 密码系统的工作机制就必须要懂得一些数论的基础知识,现代密码学的其他分支也要求这一点. 数论在密码学上的极端重要性推翻了早期许多数学家的看法,那就是数论在现实世界的应用中并不重要. 具有讽刺意味的是历史上的一些著名的数学家(像哈代(G. H. Hardy))还为数论没有像今天这样得到广泛应用而沾沾自喜.

寻求方程的整数解是数论的又一个重要内容. 一个方程若要求解仅为整数,则称为*丢番图方程*,以纪念古希腊数学家丢番图(Diophantus). 人们研究了许多不同类型的丢番图方程,其中最著名的是*费马方程* $x^n+y^n=z^n$. *费马大定理*说:若 $n$ 是大于 2 的整数,则这个方程没有整数解 $(x, y, z)$,其中 $xyz\neq 0$. 费马在 17 世纪猜想这个定理是对的. 在随后的 300 多年里数学家们(和其他人)一直在努力地寻求证明,直到 1995 年才由怀尔斯(Andrew Wiles)给出第一个证明.

正像怀尔斯的证明中所显示的,数论不是一个静止的对象! 新的发现不停地产生,研究人员经常得到重大的理论结果. 今天计算机联网所产生的巨大威力使数论在计算方面的研究步伐大大提高. 每个人都能加入这项研究的队伍中,比如说,你可以一起来寻找新的*梅森*(Mersenne)*素数*,即形为 $2^p-1$ 的素数,其中 $p$ 也是素数. 2008 年 8 月,第一个超过 1000 万位的素数被发现,即梅森数 $2^{43\,112\,609}-1$,该发现获得了由电子前沿基金颁发的十万美元大奖. 大家正在协同努力去寻找超过一亿位的素数,这个素数奖金有 15 万美元. 在学过本书的某些内容之后,你也能够决定是否涉猎于这项活动,使你的计算资源用于有益的事业.

**何谓初等数论?** 你可能会想,为什么书名上冠以"初等"二字. 这本书只考虑数论的一部分,即称为*初等数论*的那部分,它不依赖于诸如复变函数、抽象代数或者代数几何等高等数学. 有志于继续学习数学的学生会学到数论的更高深内容,如解析数论(使用复变函数)和代数数论(用抽象代数的概念证明代数数域的有趣结果).

**一些建议** 在你开始学数论的时候,要记住数论是一门具有几千年历史的经典学科,也是很现代的学科,新的发现不断快速地涌现. 它是最富含人类智慧的一个纯数学分支,也是应用数学,它在密码学和计算机科学以及电子工程方面有重要的应用. 我希望你能捕捉到数论的多种面孔,就像在你之前的许多数学迷那样,在离开学校之后仍旧对数论保持浓厚的兴趣.

动手实验和探索是研究数论所不可缺少的部分. 本书的所有成果都是数学家们不断考

察大量的数值计算现象、寻找规律并作出猜测而得到的. 他们努力地工作以证明他们的猜测，一些猜想被证明而成为定理，另一些由于找到反例而被否定，还剩下一些未被解决. 在你学习数论的时候，我建议你考察大量的例子，从中寻找规律，形成你自己的猜测. 你可以自己动手研究一些小的例子，就像数论的奠基者所做的那样，但与这些先行者不同的是，你可以利用当今强大的计算能力和计算工具. 通过手工或借助计算机来研究这些例子，会帮助你学习这门学科，甚至你也会得到自己的一些新结果.

# 第1章 整 数

在最一般的意义下，数论研究各种数集合的性质. 在本章中我们讨论某些特别重要的数的集合，包括整数、有理数和代数数集合. 我们将简单介绍用有理数逼近实数的概念，也介绍序列(特别是整数序列)的概念，包括古希腊人所研究的一些垛积数序列. 一个常见问题是如何由一些初始项来判定一个特别的整数序列. 我们将简单讨论一下如何解决这种问题.

利用序列概念，我们定义可数集合并且证明有理数集合是可数的. 我们还引进了求和符号和求积符号，并建立一些有用的求和公式.

数学归纳法是数论(和许多数学分支)中最重要的证明方法之一. 我们讨论数学归纳法的两种形式，说明如何用它们来证明各种结果，并且解释数学归纳法为什么是一种有效的证明手段.

然后我们介绍著名的斐波那契(Fibonacci)数序列，讲述引出这种数的原始问题. 我们将建立与斐波那契数有关的一些恒等式和不等式，其中有些证明就使用了数学归纳法.

本章最后一节讲述数论的一个基本概念：整除性. 我们将建立整数除法的基本性质，包括“带余除法”，还将解释如何用最大整数函数来表示一个整数去除另一个整数的商和余数. (也讲述了最大整数函数许多有用的性质.)

## 1.1 数和序列

本节将介绍一些基础知识，它们在本书中通篇使用. 特别地，我们将涉及数论中所研究的重要的数集合、整数序列的概念、求和与求积符号.

### 数

首先，我们介绍一些不同类型的数. 整数是集合{…，－3，－2，－1，0，1，2，3，…}中的数. 整数在数论的研究中扮演着重要的角色. 关于正整数的一个性质是值得关注的.

**良序性质**(The Well-Ordering Property) 每个非空的正整数集合都有一个最小元.

良序性质看起来是显然的，但是在1.3节中我们将看到这是能够帮助证明关于整数集合的许多结果的一个基本性质.

良序性质可以作为定义正整数集合的公理，或者由一组公理推导出来. (附录A列出了整数集合的这组公理.)我们说正整数集合是良序的. 但是所有整数的集合不是良序的，因为在有些整数集合中没有最小的元素，例如负整数的集合、小于100的偶数集合和全体整数的集合.

在数论学习中的另一类重要的数是那些可以被写为整数的比的数的集合.

**定义** 如果存在整数 $p$ 和 $q\neq 0$，使得 $r=p/q$，则称实数 $r$ 是**有理数**. 如果 $r$ 不是有理的，则称为**无理数**.

**例 1.1** $-22/7$，$0=0/1$，$2/17$ 和 $1111/41$ 都是有理数. ◀

注意每个整数 $n$ 都是有理数，因为 $n=n/1$. 无理数的例子有$\sqrt{2}$，$\pi$ 和 e. 我们可以用正整数集合的良序性质证明$\sqrt{2}$是无理数. 我们给出的证明尽管技巧性较强，但却不是证明$\sqrt{2}$是无理数的最简单的方法. 读者可以参考我们在第 4 章给出的证明，该证明基于第 4 章中所给出的概念.（e 是无理数的证明作为习题 44. 关于 $\pi$ 是无理数的证明并不容易，请参考[HaWr08].）

**定理 1.1** $\sqrt{2}$是无理数.

**证明** 假设$\sqrt{2}$是有理数，那么存在正整数 $a$ 和 $b$ 使得$\sqrt{2}=a/b$. 因此，$S=\{k\sqrt{2}\mid k$ 和 $k\sqrt{2}$为正整数$\}$是一个非空的正整数集合(非空是因为 $a=b\sqrt{2}$是 $S$ 的一个元素). 因此，由良序性质，$S$ 有最小元，比如 $s=t\sqrt{2}$.

$s\sqrt{2}-s=s\sqrt{2}-t\sqrt{2}=(s-t)\sqrt{2}$. 由于 $s\sqrt{2}=2t$ 和 $s$ 都是整数，故 $s\sqrt{2}-s=s\sqrt{2}-t\sqrt{2}=(s-t)\sqrt{2}$也必是整数. 进一步，这个数是正的，这是因为 $s\sqrt{2}-s=s(\sqrt{2}-1)$并且$\sqrt{2}>1$. 而这个数又小于 $s$，这是因为$\sqrt{2}<2$，从而$\sqrt{2}-1<1$. 这与 $s$ 是 $S$ 中的最小元矛盾. 因此$\sqrt{2}$是无理数. ■

整数集合、正整数集合、有理数集合和实数集合通常分别记为 $\mathbb{Z}$，$\mathbb{Z}^+$，$\mathbb{Q}$ 和 $\mathbb{R}$. 我们也用 $x\in S$ 来表示 $x$ 属于集合 $S$. 在本书中我们偶尔会使用这些记号.

这里我们简要地提及几种其他类型的数，之后在第 12 章才会再涉及它们.

**定义** 数 $\alpha$ 称为**代数数**，如果它是整系数多项式的根；也就是说，$\alpha$ 是代数数，如果存在整数 $a_0$，…，$a_n$ 使得 $a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0$. 如果数 $\alpha$ 不是代数数，则称为**超越数**.

**例 1.2** 无理数$\sqrt{2}$是代数数，因为它是多项式 $x^2-2$ 的根. ◀

注意每个有理数都是代数数，这是因为数 $a/b$ 是多项式 $bx-a$ 的根，其中 $a$，$b$ 是整数且$b\neq 0$. 在第 12 章中，我们将给出超越数的一个例子. e 和 $\pi$ 也是超越数，但是这些事实的证明超出了本书的范围(可参看[HaWr08]).

## 最大整数函数

在数论中我们用一个特别的符号来表示小于或等于一个给定的实数的最大整数.

**定义** 实数 $x$ 中的**最大整数**(greatest integer)记为$[x]$，是小于或等于 $x$ 的最大整数，即$[x]$是满足

$$[x]\leqslant x<[x]+1$$

的整数.

**例 1.3** $[5/2]=2$，$[-5/2]=-3$，$[\pi]=3$，$[-2]=-2$，$[0]=0$. ◀

**注记** 最大整数函数也被称为取整函数(floor function). 在计算机科学中通常用记号$\lfloor x\rfloor$来代替$[x]$. 上整数函数(ceiling function)是在计算机科学中常用的相关函数. 一个实数 $x$ 的上整数函数记为$\lceil x\rceil$，是大于或等于 $x$ 的最小整数. 例如$\lceil 5/2\rceil=3$，$\lceil -5/2\rceil=-2$.

最大整数函数出现在许多情况下. 除了在数论中有重要应用之外，我们在这本书中也会看到，它在计算机科学的一个分支——算法分析中也扮演着重要角色. 下面的例子体现了这个函数的一个非常有用的性质. 最大整数函数的其他性质可参看本节后的习题和[GrKnPa94].

**例 1.4** 证明：如果 $n$ 是整数，则对于任意实数 $x$，都有 $[x+n]=[x]+n$. 为了证明这个性质，设 $[x]=m$，则 $m$ 是整数，即 $m\leqslant x<m+1$. 我们在这个不等式上加上 $n$ 得到 $m+n\leqslant x+n<m+n+1$. 这说明 $m+n=[x]+n$ 是小于或等于 $x+n$ 的最大整数，从而 $[x+n]=[x]+n$. ◀

**定义** 实数 $x$ 的**分数部分**(fractional part)记为 $\{x\}$，是 $x$ 与 $[x]$ 的差，即 $\{x\}=x-[x]$.

由于 $[x]\leqslant x<[x]+1$，从而对任意实数 $x$，有 $0\leqslant\{x\}=x-[x]<1$. 因为 $x=[x]+\{x\}$，所以 $x$ 的最大取整也叫做 $x$ 的整数部分.

**例 1.5** $\{5/4\}=5/4-[5/4]=5/4-1=1/4$. $\{-2/3\}=-2/3-[-2/3]=-2/3-(-1)=1/3$. ◀

## 丢番图逼近

我们知道一个实数和与之最接近的整数的距离不超过 1/2. 但是我们可否证明一个实数的前 $k$ 个倍数中的某一个一定更接近某个整数？数论中一个很重要的部分称为丢番图逼近，它正是研究这类问题的. 特别地，丢番图逼近着重研究用有理数逼近实数的问题. (丢番图这个词来自古希腊数学家丢番图(Diophantus)，他的传记见 13.1 节.)

这里我们将要证明在实数 $\alpha$ 的前 $n$ 个倍数中至少有一个实数与最接近它的整数的距离小于 $1/n$. 这个证明是基于德国数学家狄利克雷(Dirichlet)提出的鸽笼原理[⊖](pigeonhole principle). 简单地说，这个原理告诉我们，如果有比盒子多的物体，那么当要把这些物体放进盒子中时，至少有两个物体被放入同一个盒子里. 尽管这个想法看起来特别简单，但是它在数论和组合数学中非常有用. 我们现在陈述并证明这个重要的事实. 如果你所拥有的鸽子数多于鸽笼数，那么必有两只鸽子栖息在同一个鸽笼中，因此我们把它称为鸽笼原理.

**定理 1.2**(鸽笼原理) 如果把 $k+1$ 个或者更多的物体放入 $k$ 个盒子中，那么至少有一个盒子中有两个或者更多的物体.

**证明** 如果 $k$ 个盒子中的任何一个中都没有多于一个的物体，那么所有物体的总数至多为 $k$. 这个矛盾说明有一个盒子中至少有两个或者更多的物体. ■

现在我们来叙述并证明狄利克雷逼近定理，它能够保证一个实数的前 $n$ 个倍数之一必定在某个整数的 $1/n$ 邻域内. 我们给出的证明说明了鸽笼原理很有用. (关于鸽笼原理的更多应用参见[Ro07].)(注意在证明中我们用到了绝对值函数(absolute value function). 在这里我们先回顾一下，$x$ 的绝对值 $|x|$ 当 $x\geqslant 0$ 时等于 $x$，当 $x<0$ 时等于 $-x$. $|x-y|$ 给出了 $x$ 与 $y$ 之

⊖ 狄利克雷并未把定理 1.2 称为鸽笼原理，而是用德语称为 Schubfachprinzip，译为英语是抽屉原理(drawer principle). 狄利克雷的传记见 3.1 节.

间的距离.)

**定理 1.3**(狄利克雷逼近定理)　如果 $\alpha$ 是一个实数，$n$ 是一个正整数，则存在整数 $a$ 和 $b$，$1\leqslant a\leqslant n$，使得 $|a\alpha-b|<1/n$.

**证明**　考虑 $n+1$ 个数 $0$，$\{\alpha\}$，$\{2\alpha\}$，…，$\{n\alpha\}$. 这 $n+1$ 个数是数 $j\alpha(j=0,1,\cdots,n)$的分数部分，所以 $0\leqslant\{j\alpha\}<1$，$j=0,1,\cdots,n$. 这 $n+1$ 个数中的每一个都位于 $n$ 个互不相交的区间 $0\leqslant x<1/n$，$1/n\leqslant x<2/n$，…，$(j-1)/n\leqslant x<j/n$，…，$(n-1)/n\leqslant x<1$ 中的一个. 由于我们考虑的是 $n+1$ 个数，但是仅有 $n$ 个区间，因此由鸽笼原理可知至少有两个数位于同一个区间中. 由于这些区间的长度都等于 $1/n$，并且不包含右端点，所以位于同一区间中的两个数的距离小于 $1/n$，从而存在整数 $j$ 和 $k$，$0\leqslant j<k\leqslant n$，使得 $|\{k\alpha\}-\{j\alpha\}|<1/n$. 现在证明 $a=k-j$ 时，乘积 $a\alpha$ 位于一个整数的 $1/n$ 邻域内，即 $b=[k\alpha]-[j\alpha]$. 由于 $0\leqslant j<k\leqslant n$，可见 $1\leqslant a=k-j\leqslant n$. 而且

$$\begin{aligned}|a\alpha-b| &= |(k-j)\alpha-([k\alpha]-[j\alpha])|\\ &= |(k\alpha-[k\alpha])-(j\alpha-[j\alpha])|\\ &= |\{k\alpha\}-\{j\alpha\}|<1/n.\end{aligned}$$

这样我们就找到了想要的整数 $a$ 和 $b$，满足 $1\leqslant a\leqslant n$ 且 $|a\alpha-b|<1/n$. ■

**例 1.6**　假定 $\alpha=\sqrt{2}$ 且 $n=6$. 我们发现 $1\cdot\sqrt{2}\approx1.414$，$2\cdot\sqrt{2}\approx2.828$，$3\cdot\sqrt{2}\approx4.243$，$4\cdot\sqrt{2}\approx5.657$，$5\cdot\sqrt{2}\approx7.071$，$6\cdot\sqrt{2}\approx8.485$. 在这些数中 $5\cdot\sqrt{2}$ 的分数部分最小. 我们看到 $|5\cdot\sqrt{2}-7|\approx|7.071-7|=0.071\leqslant1/6$. 所以如果 $\alpha=\sqrt{2}$，$n=6$，那么可以取 $a=5$，$b=7$，从而使得 $|a\alpha-b|<1/n$. ◀

对于定理 1.3 我们采取的是狄利克雷 1834 年的原始证明. 把定理 1.3 中的 $1/n$ 替换为 $1/(n+1)$，可以得到一个更强的结论. 它的证明并不困难(见习题 32). 进一步，在习题 34 中我们展示如何用狄利克雷逼近定理来证明对于一个无理数 $\alpha$，存在无数多个不同的有理数 $p/q$ 使得 $|\alpha-p/q|<1/q^2$，这是丢番图逼近定理中的一个重要结果. 我们将在第 12 章再回到这个话题.

## 序列

序列 $\{a_n\}$ 是一列数 $a_1$，$a_2$，$a_3$，…. 我们在研究数论时会考虑一些特殊的整数序列. 在下面的例子中我们将介绍一些有用的序列.

**例 1.7**　序列 $\{a_n\}$(其中 $a_n=n^2$)由 1，4，9，16，25，36，49，64，…开始. 这是整数平方序列. 序列 $\{b_n\}$(其中 $b_n=2^n$)由 2，4，8，16，32，64，128，256，…开始. 这是 2 的乘方序列. 序列 $\{c_n\}$(当 $n$ 是奇数时 $c_n=0$；当 $n$ 是偶数时 $c_n=1$)由 0，1，0，1，0，1，0，1，…开始. ◀

有一些序列每个后继的项都是由前一项乘一个公共因子得到的. 例如，在 2 的乘方序列中每一项都是由前一项乘 2 得到的. 这导出了下面的定义.

**定义**　**等比数列**(geometric progression)是形如 $a$，$ar$，$ar^2$，$ar^3$，…的序列，其中**初始项**(initial term)$a$ 和**公比**(common ratio)$r$ 都是实数.

**例 1.8**　序列 $\{a_n\}$(这里 $a_n=3\cdot5^n$，$n=0,1,2,\cdots$)是一个等比数列，初始项是 3，

公比为5.（注意这个序列是由项 $a_0$ 开始的．项的下标可以从0或者我们选择的其他任何整数开始.）◀

数论中的一个常见问题是如何寻找构造序列的通项公式或者规则，即使仅有很少的几项是已知的(例如寻找第 $n$ 个三角数 $1+2+3+\cdots+n$ 的公式)．尽管一个序列的几个初始项不能确定这个序列，但是知道前几项有助于我们猜测通项公式或规则．考虑下面的例子.

**例 1.9** 猜测 $a_n$ 的公式，这里序列$\{a_n\}$的前8项是4，11，18，25，32，39，46，53．我们注意由第二项开始的每一项都是由前一项加7得到的．因此第 $n$ 项应该为初始项加 $7(n-1)$．一个合理的猜测是 $a_n=4+7(n-1)=7n-3$．◀

例1.9中给出的序列是一个等差数列(arithmetic progression)，即形如 $a$，$a+d$，$a+2d$，…，$a+nd$，…的序列．例1.9中的序列是 $a=4$，$d=7$ 的特殊形式.

**例 1.10** 猜测 $a_n$ 的公式，这里序列$\{a_n\}$的前8项是5，11，29，83，245，731，2189，6563．我们注意到每一项都接近前一项的3倍，暗示着在 $a_n$ 的通项公式中有项 $3^n$．对于 $n=1$，2，3，…，整数 $3^n$ 分别为3，9，27，81，243，729，2187，6561．比较这两个序列，我们会发现生成这个序列的公式为 $a_n=3^n+2$．◀

**例 1.11** 猜测 $a_n$ 的公式，这里序列$\{a_n\}$的前10项是1，1，2，3，5，8，13，21，34，55．从不同的角度观察这个序列，我们注意到这个序列中前两项之后的每一项都是它之前两项的和．也就是说，我们发现 $a_n=a_{n-1}+a_{n-2}$，$3\leqslant n\leqslant 10$．这是一个递归定义序列的例子，将在1.3节中讨论．在这个例子中列出的项是斐波那契序列的前几项，这个序列将在1.4节中讨论．◀

整数序列在数论中的许多地方出现．在这些序列中我们将会研究斐波那契数、素数(第3章)和完全数(在3.7节中介绍)．除了数论外，整数序列还出现在很多其他学科中．尼尔·斯劳恩(Neil Sloane)在他的《在线整数序列百科全书》(On-Line Encyclopedia of Integer Sequences)中搜集了超过170 000个整数序列(截至2010年年初)，此书现可网上查阅(2010年年初，由OEIS基金会接手维护该书)．(参考文献[SlPl95]是早期的只包含了目前该书一小部分内容的印刷版.)该书所在的网址中提供了一个程序，用于寻找与输入的几个起始项匹配的序列．你会发现在你今后的数论(和其他学科)学习中这是一个很有价值的资源.

我们现在定义什么是可数集，并且证明一个集合可数当且仅当它的元素可以被列为一个序列.

**定义** 一个集合**可数**(countable)，如果它是有限的或者是无穷的但与正整数集合之间存在一个一一映射．如果一个集合不是可数的，则称为**不可数**(uncountable)．

一个无穷集合是可数的当且仅当其中的元素可以被列为一个由正整数标记的序列．为了看到这一点，只需注意从正整数集合到一个集合 $S$ 的一一映射 $f$ 其实就是把集合中的元素列成序列 $a_1$，$a_2$，…，$a_n$，…，其中 $a_i=f(i)$.

**例 1.12** 整数集合是可数的，因为整数可以被列出来，由0开始，接下来是1和$-1$，2和$-2$，如此继续下去．这样产生一个序列0，1，$-1$，2，$-2$，3，$-3$，…，这里 $a_1=0$，$a_{2n}=n$，$a_{2n+1}=-n$，$n=1$，2，….◀

有理数集合是否可数？对于这个问题，第一眼看上去，似乎在正整数集合与有理数集合之间不存在一一映射．然而，其中确实存在一个映射，如下述定理所述．

**定理 1.4**　*有理数集合是可数的．*

**证明**　我们可以将有理数作为一个序列的项列举如下：首先，将全部有理数排列成一个二维阵列，如图 1.1 所示．将第一行放置分母为 1 的所有分数，它们的分子按照例 1.12 的顺序放置．接下来，按照图 1.1 的顺序，将所有分数序列列举在连续的对角线上．最后，从列表中将所有用来表示已经列举过的有理数的分数删除．（例如，并不列举 2/2，因为已经列举了 1/1.）

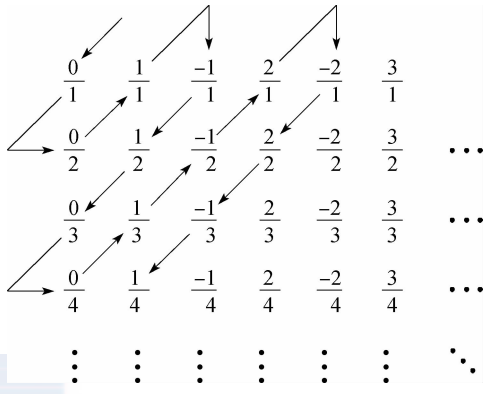


图 1.1　列举有理数

所得序列的初始几项是 $0/1=0$，$1/1=1$，$-1/1=-1$，$1/2$，$1/3$，$-1/2$，$2/1=2$，$-2/1=-2$，$-1/3$，$1/4$，等等．此过程将全部有理数列举为一个序列的项，请读者自行补充证明细节．■

我们已经证明了有理数集合是可数的，但并没有给出不可数集合的例子．本节的习题 45 将会证明实数集合不可数．

## 1.1 节习题

1. 确定下列集合是否是良序的．或者使用正整数集合的良序性质给出一个证明，或者给出集合的一个没有最小元的子集作为反例．
   a) 大于 3 的整数集合
   b) 偶正整数集合
   c) 正有理数集合
   d) 能够写成 $a/2$ 形式的正有理数集合，其中 $a$ 为正整数
   e) 非负有理数集合

☞ 2. 证明：如果 $a$ 和 $b$ 为正整数，则在所有形如 $a-bk(k\in\mathbb{Z})$ 的正整数中有一个最小元．

3. 证明两个有理数的和与积都是有理数．

4. 证明或推翻下列命题．
   a) 有理数与无理数之和为无理数．　　b) 两个无理数的和是无理数．
   c) 有理数与无理数之积是无理数．　　d) 两个无理数的积是无理数．

* 5. 用良序性质证明$\sqrt{3}$是无理数．

6. 证明每个非空的负整数集合都有一个最大元．

7. 求下列最大整数函数的值．
   a) $[1/4]$　b) $[-3/4]$　c) $[22/7]$　d) $[-2]$　e) $[[1/2]+[1/2]]$　f) $[-3+[-1/2]]$

8. 求下列最大整数函数的值．
   a) $[-1/4]$　b) $[-22/7]$　c) $[5/4]$　d) $[[1/2]]$　e) $[[3/2]+[-3/2]]$　f) $[3-[1/2]]$

9. 求下列各数的分数部分．
   a) 8/5　b) 1/7　c) $-11/4$　d) 7

10. 求下列各数的分数部分．

a) $-8/5$ b) $22/7$ c) $-1$ d) $-1/3$

11. $[x]+[-x]$的值是什么？其中 $x$ 为实数.

12. 证明当 $x$ 为实数时$[x]+[x+1/2]=[2x]$.

13. 证明对于所有实数 $x$ 和 $y$，都有$[x+y]\geqslant[x]+[y]$.

14. 证明当 $x$ 和 $y$ 为实数时，$[2x]+[2y]\geqslant[x]+[y]+[x+y]$.

15. 证明：如果 $x$ 和 $y$ 是正实数，则$[xy]\geqslant[x][y]$. 当 $x$ 和 $y$ 都是负实数时结果如何？当 $x$ 和 $y$ 一个为正一个为负时结果又如何？

16. 证明当 $x$ 为实数时，$-[-x]$是大于或等于 $x$ 的最小整数.

17. 证明$[x+1/2]$是最接近 $x$ 的整数(当有两个整数与 $x$ 等距时，这是其中比较大的那个).

18. 证明：如果 $m$ 和 $n$ 是整数，则当 $x$ 为实数时，$[(x+n)/m]=[([x]+n)/m]$.

* 19. 证明当 $x$ 为非负实数时，$[\sqrt{[x]}]=[\sqrt{x}]$.

* 20. 证明：如果 $m$ 为正整数，则当 $x$ 为实数时，$[mx]=[x]+[x+(1/m)]+[x+(2/m)]+\cdots+[x+(m-1)/m]$.

21. 如果一个序列的前十项如下，猜测序列$\{a_n\}$的第 $n$ 项公式.

a) 3，11，19，27，35，43，51，59，67，75

b) 5，7，11，19，35，67，131，259，515，1027

c) 1，0，0，1，0，0，0，0，1，0

d) 1，3，4，7，11，18，29，47，76，123

22. 如果一个序列的前十项如下，猜测序列$\{a_n\}$的第 $n$ 项公式.

a) 2，6，18，54，162，486，1458，4374，13 122，39 366

b) 1，1，0，1，1，0，1，1，0，1

c) 1，2，3，5，7，10，13，17，21，26

d) 3，5，11，21，43，85，171，341，683，1365

23. 找出序列$\{a_n\}$的三个不同通项公式或规则，其中序列的前三项分别是 1，2，4.

24. 找出序列$\{a_n\}$的三个不同通项公式或规则，其中序列的前三项分别是 2，3，6.

25. 证明由大于 $-100$ 的所有整数构成的集合是可数的.

26. 证明所有形如 $n/5$ 的有理数集合是可数的，其中 $n$ 是整数.

27. 证明所有形如 $a+b\sqrt{2}$的数的集合是可数的，其中 $a$ 和 $b$ 是整数.

* 28. 证明两个可数集合的并是可数的.

* 29. 证明可数多个可数集合的并是可数的.

30. 如果必要，使用一些计算辅助方法，求整数 $a$ 和 $b$ 使得 $1\leqslant a\leqslant 8$ 且 $|a\alpha-b|<1/8$，其中 $\alpha$ 为

a) $\sqrt{2}$ b) $\sqrt[3]{2}$ c) $\pi$ d) e

31. 如果必要，使用一些计算辅助方法，求整数 $a$ 和 $b$ 使得 $1\leqslant a\leqslant 10$ 且 $|a\alpha-b|<1/10$，其中 $\alpha$ 为

a) $\sqrt{3}$ b) $\sqrt[3]{3}$ c) $\pi^2$ d) $e^3$

32. 证明下面的强狄利克雷逼近定理. 如果 $\alpha$ 是实数，$n$ 是正整数，则存在整数 $a$ 和 $b$ 使得 $1\leqslant a\leqslant n$ 且 $|a\alpha-b|\leqslant 1/(n+1)$. (提示：考虑 $n+2$ 个数 0，…，$\{j\alpha\}$，…，1 和 $n+1$ 个区间$(k-1)/(n+1)\leqslant x<k/(n+1)$，$k=1$，…，$n+1$.)

33. 证明：如果 $\alpha$ 是实数，$n$ 是正整数，则存在整数 $k$，使得 $|\alpha-n/k|\leqslant 1/2k$.

34. 使用狄利克雷逼近定理证明：如果 $\alpha$ 为无理数，则存在无穷多个正整数 $q$，对于每个 $q$ 存在一个整数 $p$，使得 $|\alpha-p/q|\leqslant 1/q^2$.

35. 求四个有理数 $p/q$，使得 $|\sqrt{2}-p/q|\leqslant 1/q^2$.

36. 求五个有理数 $p/q$，使得 $|\sqrt[3]{5}-p/q|\leqslant 1/q^2$.

37. 证明：如果 $\alpha=a/b$ 是有理数，则只有有限多个有理数 $p/q$，使得 $|p/q-a/b|<1/q^2$.

实数 $\alpha$ 的**谱序列**(spectrum sequence)是第 $n$ 项为 $[n\alpha]$ 的一个序列.

38. 求下列各数的谱序列的前十项.

a) 2　b) $\sqrt{2}$　c) $2+\sqrt{2}$　d) e　e) $(1+\sqrt{5})/2$

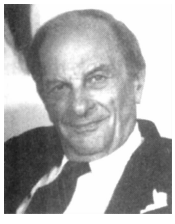
39. 求下列各数的谱序列的前十项.

a) 3　b) $\sqrt{3}$　c) $(3+\sqrt{3})/2$　d) $\pi$

40. 证明：如果 $\alpha\neq\beta$，则 $\alpha$ 的谱序列与 $\beta$ 的谱序列不同.

** 41. 证明：每个正整数仅在 $\alpha$ 的谱序列或 $\beta$ 的谱序列中出现一次，当且仅当 $\alpha$ 和 $\beta$ 是正无理数且 $1/\alpha+1/\beta=1$.

定义**乌拉姆数** $u_n$($n=1, 2, 3, \cdots$)如下：我们规定 $u_1=1$ 且 $u_2=2$. 对接下来的每个整数 $m$，$m>2$，这个整数是乌拉姆数当且仅当它可以唯一地写成两个不同的乌拉姆数之和. 这些数是以斯坦尼斯诺·乌拉姆的名字命名的，他于 1964 年第一个描述了它们.



**斯坦尼斯诺·乌拉姆**(Stanislaw M. Ulam，1909—1984)出生于波兰的 Lvov 市. 从 12 岁收到叔叔送给他的一架望远镜的时候起，他开始对天文学和物理学感兴趣. 乌拉姆决心去学一些必要的数学知识来读懂相对论，并且在 14 岁的时候，他开始从课本上学习微积分和其他数学知识.

在 Lvov 的理工学院学习期间，乌拉姆在数学家巴拿赫(Banach)的指导下，于 1933 年获得了实分析专业的博士学位. 1935 年，他应邀在高等研究院进行了几个月的高级研究. 1936 年，乌拉姆作为 Society of Fellows 的成员进入哈佛大学工作一直到 1940 年. 其间，每年夏天他都会回到波兰，在苏格兰咖啡厅之类的地方与他在这里的数学家伙伴们深入研讨数学.

乌拉姆是幸运的，他于 1939 年离开波兰，而一个月后第二次世界大战就爆发了. 1940 年，他在美国威斯康星大学做助理教授. 1943 年，他在 Los Alamos 从事第一颗原子弹的研究工作，这是曼哈顿计划的一部分. 在 Los Alamos，乌拉姆还发展了蒙特卡罗(Monte Carlo)方法. 这是用随机数抽样技术寻找数学问题的解的一种方法.

第二次世界大战后，乌拉姆在 Los Alamos 一直待到 1965 年. 他在南加州大学、科罗拉多大学、佛罗里达大学的学院工作过. 乌拉姆有超强的记忆力，而且口才极好. 他的头脑是汇集轶闻、笑话、智力游戏、语录、公式、问题和许多其他信息的宝库. 他写了许多书，包括《Sets, Numbers, and Universes》和《Adventures of a Mathematician》. 他对包括数论、实分析、概率论和生物数学在内的很多数学领域感兴趣，并做出了贡献.

42. 求前十个乌拉姆数.

* 43. 证明存在无穷多个乌拉姆数.

* 44. 证明 e 是无理数. (提示：使用 $e=1+1/1!+1/2!+1/3!+\cdots$ 这一事实.)

* 45. 证明实数集不可数。(提示：假定可将 0，1 之间的实数进行排列. 构造一个实数如下：

如果第 $i$ 个实数的第 $i$ 位是 5 其小数点后的第 $i$ 位取值为 4，若第 $i$ 个实数的第 $i$ 位非 5，则它的第 $i$ 位取值为 5. 证明如此构造的实数不在前述排列之中.)

## 计算和研究

1. 求 10 个有理数 $p/q$ 使得 $|\pi-p/q|\leqslant 1/q^2$.

2. 求 20 个有理数 $p/q$ 使得 $|e-p/q|\leqslant 1/q^2$.

3. 尽可能多地求出$\sqrt{2}$的谱序列中的项(谱序列的定义参看习题 38 前面的导言).
4. 尽可能多地求出 $\pi$ 的谱序列中的项(谱序列的定义参看习题 38 前面的导言).
5. 求前 1000 个乌拉姆数.
6. 你能找到多少对都是乌拉姆数的连续整数?
7. 除了 1 和 2，其他任意两个相继的乌拉姆数之和是否可以为另外一个乌拉姆数? 如果是，你能找到多少个这样的例子?
8. 相继的乌拉姆数之间的差有多大? 你认为这些差可以是任意大吗?
9. 关于小于整数 $n$ 的乌拉姆数的个数，你有什么猜想? 你的计算是否支持你的猜想?

**程序设计**

1. 给定一个数 $\alpha$，求有理数 $p/q$ 使得 $|\alpha-p/q|\leqslant 1/q^2$.
2. 给定一个数 $\alpha$，求它的谱序列.
3. 求前 $n$ 个乌拉姆数，这里 $n$ 是正整数.

## 1.2 和与积

由于和与积在数论的研究中频繁出现，我们现在就来介绍和与积的记号. 下面的记号表示数 $a_1$，$a_2$，…，$a_n$ 的和：

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n.$$

字母 $k$ 称为求和下标(index of summation)，是一个“虚变量”，可以用任意字母代替. 例如

$$\sum_{k=1}^{n} a_k = \sum_{j=1}^{n} a_j = \sum_{i=1}^{n} a_i, \text{等等.}$$

**例 1.13** $\sum_{j=1}^{5} j=1+2+3+4+5=15$，$\sum_{j=1}^{5} 2=2+2+2+2+2=10$，$\sum_{j=1}^{5} 2^j=2+2^2+2^3+2^4+2^5=62$.

我们还注意到，在求和的记号中，求和下标可以在任意两个整数之间变动，只要求和下界不超过上界. 如果 $m$ 和 $n$ 是整数且满足 $m\leqslant n$，则 $\sum_{k=m}^{n} a_k=a_m+a_{m+1}+\cdots+a_n$. 例如，$\sum_{k=3}^{5} k^2=3^2+4^2+5^2=50$，$\sum_{k=0}^{2} 3^k=3^0+3^1+3^2=13$，$\sum_{k=-2}^{1} k^3=(-2)^3+(-1)^3+0^3+1^3=-8$. ◀

我们经常需要考虑一些和，其中的求和下标是取遍所有具有某种特殊性质的整数. 可以使用求和记号来标记在和式中出现的单项的下标所必须满足的特殊的一条或多条性质. 下面的例子说明了这个记号的作用.

**例 1.14** 我们有

$$\sum_{\substack{j\leqslant 10 \\ j\in\{n^2\mid n\in\mathbb{Z}\}}} 1/(j+1) = 1/1+1/2+1/5+1/10 = 9/5,$$

和式中的项是所有那些与不超过 10 的完全平方数 $j$ 对应的项. ◀

下面的三个和式的性质通常是很有用的. 我们把它们的证明留给读者.

$$\sum_{j=m}^{n} ca_j = c\sum_{j=m}^{n} a_j \tag{1.1}$$

$$\sum_{j=m}^{n}(a_j+b_j)=\sum_{j=m}^{n}a_j+\sum_{j=m}^{n}b_j \tag{1.2}$$

$$\sum_{i=m}^{n}\sum_{j=p}^{q}a_ib_j=\Big(\sum_{i=m}^{n}a_i\Big)\Big(\sum_{j=p}^{q}b_j\Big)=\sum_{j=p}^{q}\sum_{i=m}^{n}a_ib_j \tag{1.3}$$

接下来，我们给出几个有用的求和公式．我们经常需要求一个等比数列的相继若干项的和．下面的例子说明了如何推导这样的和的公式．

**例 1.15** 求等比数列 $a$，$ar$，…，$ar^k$，…的前 $n+1$ 项的和

$$S=\sum_{j=0}^{n}ar^j.$$

我们把上式两边同时乘以 $r$ 并对求和结果进行处理：

$$\begin{aligned}
rS&=r\sum_{j=0}^{n}ar^j\\
&=\sum_{j=0}^{n}ar^{j+1}\\
&=\sum_{k=1}^{n+1}ar^k && \text{（平移求和下标，取 } k=j+1\text{）}\\
&=\sum_{k=0}^{n}ar^k+(ar^{n+1}-a) && \text{（移出第 } k=n+1 \text{ 项，并添加第 } k=0 \text{ 项）}\\
&=S+(ar^{n+1}-a).
\end{aligned}$$

这说明

$$rS-S=(ar^{n+1}-a).$$

当 $r\neq1$ 时求解 $S$，

$$S=\frac{ar^{n+1}-a}{r-1}.$$

注意当 $r=1$ 时，我们有 $\sum_{j=0}^{n}ar^j=\sum_{j=0}^{n}a=(n+1)a$. ◀

**例 1.16** 在例 1.15 得到的公式中取 $a=3$，$r=-5$ 和 $n=6$，我们得到 $\sum_{j=0}^{6}3(-5)^j=\frac{3(-5)^7-3}{-5-1}=39\,063$. ◀

下面的例子说明 2 的前 $n$ 个连续方幂之和比 2 的下一个方幂小 1.

**例 1.17** 设 $n$ 为正整数．求和

$$\sum_{k=0}^{n}2^k=1+2+2^2+\cdots+2^n,$$

利用例 1.15，并取 $a=1$，$r=2$，得到

$$1+2+2^2+\cdots+2^n=\frac{2^{n+1}-1}{2-1}=2^{n+1}-1.$$ ◀

形如 $\sum_{j=1}^{n}(a_j-a_{j-1})$ 的和被称为是叠进的(telescoping)，其中 $a_0$，$a_1$，$a_2$，…，$a_n$ 是一

数列．叠进和是很容易计算的，因为

$$\sum_{j=1}^{n} a_j - a_{j-1} = (a_1 - a_0) + (a_2 - a_1) + \cdots + (a_n - a_{n-1}) = a_n - a_0.$$

古希腊人对排列规则等间距的点组成的数列很有兴趣．下面的例子说明了这样的一个数列．

**例 1.18** 三角数 $t_1$，$t_2$，$t_3$，…，$t_k$，…是一个数列，其中 $t_k$ 为第 $j$ 行有 $j$ 个点的 $k$ 行三角阵列中点的个数． ◀

图 1.2 表示 $k=1$，2，3，4，5 时，相继增大的正三角形中点的个数 $t_k$．

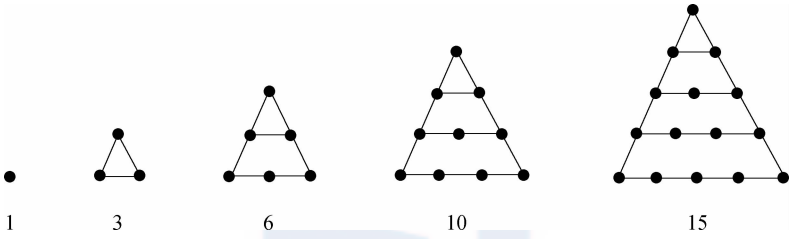



图 1.2 三角数

接下来，我们将要确定第 $n$ 个三角数 $t_n$ 的表达公式．

**例 1.19** 我们怎么能够找到第 $n$ 个三角数的表达式呢？一种方法是使用恒等式 $(k+1)^2 - k^2 = 2k+1$．当我们把因子 $k$ 分离出来时，得到 $k = ((k+1)^2 - k^2)/2 - 1/2$．把这个表达式关于 $k$ 求和，其中 $k=1$，2，…，$n$，我们得到

$$\begin{aligned}
t_n &= \sum_{k=1}^{n} k \\
&= \left(\sum_{k=1}^{n} ((k+1)^2 - k^2)/2\right) - \sum_{k=1}^{n} 1/2 \quad (\text{用 } ((k+1)^2 - k^2)/2 - 1/2 \text{ 取代 } k) \\
&= ((n+1)^2/2 - 1/2) - n/2 \quad (\text{化简叠进和}) \\
&= (n^2 + 2n)/2 - n/2 \\
&= (n^2 + n)/2 \\
&= n(n+1)/2.
\end{aligned}$$

第二个等式由叠进级数 $a_k = (k+1)^2 - k^2$ 的求和公式得出．我们推出第 $n$ 个三角数 $t_n = n(n+1)/2$．($t_n$ 的另一种求法见习题 7.) ◀

与求和类似，我们也给乘积定义一个记号．数 $a_1$，$a_2$，…，$a_n$ 的积记为

$$\prod_{j=1}^{n} a_j = a_1 a_2 \cdots a_n.$$

上面的字母 $j$ 是“虚变量”，可以用任意字母代替．

**例 1.20** 为了说明求积符号，我们有

$$\prod_{j=1}^{5} j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120,$$

$$\prod_{j=1}^{5} 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32,$$

$$\prod_{j=1}^{5} 2^j = 2 \cdot 2^2 \cdot 2^3 \cdot 2^4 \cdot 2^5 = 2^{15}.$$

◀

阶乘函数(factorial function)在数论中通篇出现.

**定义**　设 $n$ 为正整数，则 $n!$（读为“$n$ 的阶乘”)是整数 1，2，…，$n$ 的积. 我们还特别定义 $0! = 1$. 采用乘积符号，我们有 $n! = \prod_{j=1}^{n} j$.

**例 1.21**　$1! = 1$，$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$，$12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 479\,001\,600$. ◀

## 1.2 节习题

1. 求下列和式的值.

   a) $\sum_{j=1}^{5} j^2$　　b) $\sum_{j=1}^{5} (-3)$　　c) $\sum_{j=1}^{5} 1/(j+1)$

2. 求下列和式的值.

   a) $\sum_{j=0}^{4} 3$　　b) $\sum_{j=0}^{4} (j-3)$　　c) $\sum_{j=0}^{4} (j+1)/(j+2)$

3. 求下列和式的值.

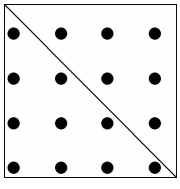
   a) $\sum_{j=1}^{8} 2^j$　　b) $\sum_{j=1}^{8} 5(-3)^j$　　c) $\sum_{j=1}^{8} 3(-1/2)^j$

4. 求下列和式的值.

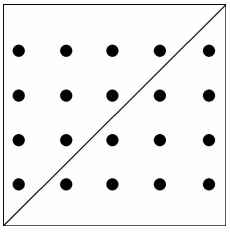
   a) $\sum_{j=0}^{10} 8 \cdot 3^j$　　b) $\sum_{j=0}^{10} (-2)^{j+1}$　　c) $\sum_{j=0}^{10} (1/3)^j$

* 5. 用 $n$ 以及 $[\sqrt{n}]$ 表达求和公式 $\sum_{k=1}^{n} [\sqrt{k}]$，并加以证明.

6. 把两个三角阵列组合在一起，其中一个是 $n$ 行而另外一个是 $n-1$ 行，形成一个正方形阵列(下图所示为 $n=4$ 的情形)，证明 $t_{n-1} + t_n = n^2$，这里 $t_n$ 是第 $n$ 个三角数.



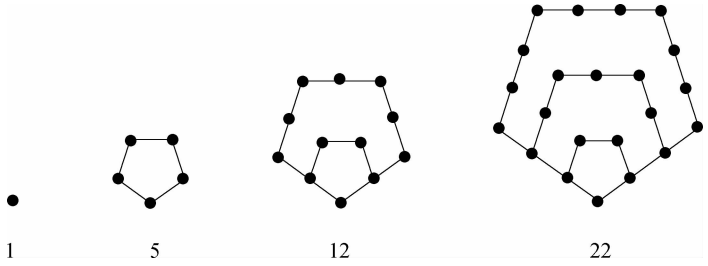
7. 把两个三角阵列组合在一起，每个都是 $n$ 行，形成一个有 $n$ 乘 $n+1$ 个点的矩形阵列(下图所示为 $n=4$ 的情形)，证明 $2t_n = n(n+1)$，从而得到 $t_n = n(n+1)/2$.



8. 若 $t_n$ 是第 $n$ 个三角数，证明 $3t_n+t_{n-1}=t_{2n}$.

9. 若 $t_n$ 是第 $n$ 个三角数，证明 $t_{n+1}^2-t_n^2=(n+1)^3$.

*五边形数*(pentagonal numbers)$p_1$，$p_2$，…，$p_k$，…记录的是 $k$ 个嵌套在一起的五边形中点的个数，如下图所示.




10. 证明 $p_1=1$，而对 $k\geqslant 2$，$p_k=p_{k-1}+(3k-2)$. 从而有 $p_n=\sum_{k=1}^{n}(3k-2)$，计算这个和，以求出 $p_n$ 的简单公式.

11. 证明第$(n-1)$个三角数与第 $n$ 个平方数之和为第 $n$ 个五边形数.

12. a) 用与三角数、平方数、五边形数类似的方法定义六边形数 $h_n$，其中 $n=1$，2，…. (注意六边形是个有六个边的多边形.)

    b) 求六边形数的公式.

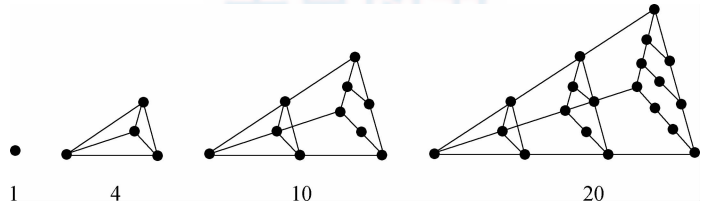
13. a) 用与三角数、平方数、五边形数类似的方法定义七边形数. (注意七边形是有七个边的多边形.)

    b) 求七边形数的公式.

14. 证明 $h_n=t_{2n-1}$ 对所有的正整数 $n$ 成立，其中 $h_n$ 是习题 12 中定义的六边形数，$t_{2n-1}$ 是第 $2n-1$ 个三角数.

15. 证明 $p_n=t_{3n-1}/3$，其中 $p_n$ 是第 $n$ 个五边形数，$t_{3n-1}$ 是第 $3n-1$ 个三角数.

*四面体数*(tetrahedral number)$T_1$，$T_2$，$T_3$，…，$T_k$，…记录的是 $k$ 个嵌套在一起的四面体的面上点的个数，如下图所示.




16. 证明第 $n$ 个四面体数是前 $n$ 个三角数之和.

17. 求第 $n$ 个四面体数的公式并证明之.

18. 当 $n$ 分别等于前十个正整数时求 $n!$.

19. 把整数 $100!$，$100^{100}$，$2^{100}$ 和$(50!)^2$ 按从小到大的顺序排列. 证明你的结果是正确的.

20. 把下面各乘积用 $\prod_{i=1}^{n}a_i$ 表达，其中 $k$ 为一个常数.

    a) $\prod_{i=1}^{n}ka_i$　　b) $\prod_{i=1}^{n}ia_i$　　c) $\prod_{i=1}^{n}a_i^k$

21. 使用恒等式$\frac{1}{k(k+1)}=\frac{1}{k}-\frac{1}{k+1}$计算 $\sum_{k=1}^{n}\frac{1}{k(k+1)}$.

22. 使用恒等式$\frac{1}{k^2-1}=\frac{1}{2}\left(\frac{1}{k-1}-\frac{1}{k+1}\right)$计算 $\sum_{k=2}^{n}\frac{1}{k^2-1}$.

23. 用类似于例 1.21 的方法和公式求 $\sum_{k=1}^{n}k^2$ 的公式.

24. 用类似于例 1.19 的方法以及该例与习题 21 的结果求 $\sum_{k=1}^{n}k^3$ 的公式.

25. 不用计算各项的乘积，证明下列等式成立.

a) $10!=6!\,7!$　　b) $10!=7!\,5!\,3!$　　c) $16!=14!\,5!\,2!$　　d) $9!=7!\,3!\,3!\,2!$

26. 设 $a_1$，$a_2$，…，$a_n$ 为正整数. 设 $b=(a_1!\,a_2!\cdots a_n!)-1$，$c=a_1!\,a_2!\cdots a_n!$. 证明 $c!=a_1!\,a_2!\cdots a_n!\,b!$.

27. 求所有满足 $x!+y!=z!$ 的正整数 $x$，$y$ 和 $z$.

28. 求下面各乘积的值.

a) $\prod_{j=2}^{n}(1-1/j)$　　b) $\prod_{j=2}^{n}(1-1/j^2)$

**计算和研究**

1. 使得 $n!$ 少于 100 位数字的 $n$ 的最大值是什么？使得 $n!$ 少于 1000 位数字的 $n$ 的最大值是什么？使得 $n!$ 少于10 000位数字的 $n$ 的最大值是什么？
2. 找出尽可能多的同时是完全平方数的三角数.（我们将在 13.4 节的习题中研究这个问题.）
3. 找出尽可能多的同时是完全平方数的四面体数.

**程序设计**

1. 给定序列 $a_1$，$a_2$，…，$a_n$ 的各项，计算 $\sum_{j=1}^{n}a_j$ 和 $\prod_{j=1}^{n}a_j$.
2. 给定一个等比数列的各项，求它的各项之和.
3. 给定一个正整数 $n$，找出第 $n$ 个三角数、第 $n$ 个完全平方数、第 $n$ 个五边形数和第 $n$ 个四面体数.

## 1.3　数学归纳法

对于比较小的 $n$ 值，观察前 $n$ 个正奇整数的和，可以猜想这个和的公式. 我们有

$$\begin{aligned}1&=1,\\1+3&=4,\\1+3+5&=9,\\1+3+5+7&=16,\\1+3+5+7+9&=25,\\1+3+5+7+9+11&=36.\end{aligned}$$

从上面的值可以猜想对于正整数 $n$，有 $\sum_{j=1}^{n}(2j-1)=1+3+5+7+\cdots+2n-1=n^2$.

我们如何才能证明这个公式对所有的整数 $n$ 都成立？

*数学归纳原理*(The principle of mathematical induction)是证明与整数有关的结果的一个有效工具——例如上面关于前 $n$ 个正奇整数和的公式的猜想. 首先，我们叙述这个原理，然后说明如何应用. 接下来，我们使用良序原理来说明数学归纳法是一个有效的证明方法. 在关于数论的研究中，将要多次使用数学归纳原理以及良序性质.

使用数学归纳法证明一个特定命题对所有正整数都成立必须实现两步. 第一，设 $S$ 为我们认为命题成立的那个正整数集合，必须说明 1 属于 $S$；即命题对整数 1 为真. 这叫做

基础步骤.

第二，必须证明对每个正整数 $n$，如果 $n$ 属于 $S$ 则 $n+1$ 也属于 $S$；即如果这个命题对 $n$ 为真，则对 $n+1$ 也为真. 这被称为归纳步骤. 一旦这两步都完成了，我们就可以由数学归纳原理得到结论：命题对所有正整数为真.

**定理 1.5**(数学归纳原理) 一个包含整数 1 的正整数集合如果具有如下性质，即若其包含整数 $k$，则其也包含整数 $k+1$，那么这个集合一定是所有正整数的集合.

下面用几个例子来说明如何应用数学归纳法，首先我们证明本节开始给出的猜想.

**例 1.22** 使用数学归纳法来证明

$$\sum_{j=1}^{n}(2j-1)=1+3+\cdots+(2n-1)=n^2$$

对所有正整数 $n$ 成立.（顺便指出，如果我们关于上述和式的值的猜想是错误的，那么数学归纳法将不能给出证明!）

我们从基础步骤开始，由于

$$\sum_{j=1}^{1}(2j-1)=2\cdot 1-1=1=1^2,$$

所以这一步成立.

对于归纳步骤，我们的归纳假设为公式对于 $n$ 成立，即假定 $\sum_{j=1}^{n}(2j-1)=n^2$. 使用归纳假设，我们有

$$\begin{aligned}\sum_{j=1}^{n+1}(2j-1)&=\sum_{j=1}^{n}(2j-1)+(2(n+1)-1) \quad (\text{把 } j=n+1 \text{ 的项分出来})\\ &=n^2+2(n+1)-1 \quad (\text{使用归纳假设})\\ &=n^2+2n+1\\ &=(n+1)^2.\end{aligned}$$

由于基础步骤和归纳步骤都完成了，我们知道结果成立. ◀

下面我们用数学归纳法证明不等式.

**数学归纳法的起源**

已知的数学归纳法的使用最早出现在 16 世纪数学家 Francesco Maurolico(1494—1575)的工作中，在他的著作《Arithmeticorum Libri Duo》中，Maurolico 给出了整数的各种性质以及证明. 为了完成一些证明，他发明了数学归纳法. 在他的书中，数学归纳法首次出现在证明前 $n$ 个正奇数的和是 $n^2$ 中.

**例 1.23** 我们可以用数学归纳法证明 $n!\leqslant n^n$ 对任意正整数 $n$ 成立. 基础步骤中，也就是当 $n=1$ 时，由于 $1!=1\leqslant 1^1=1$，故命题成立. 现在假定 $n!\leqslant n^n$；这就是归纳假设. 为了完成证明，我们必须证明在上述归纳假设成立的条件下，$(n+1)!\leqslant(n+1)^{n+1}$. 应用归纳假设，我们有

$$(n+1)!=(n+1)\cdot n!$$

$$\begin{aligned}&\leqslant (n+1)n^n\\&< \ (n+1)(n+1)^n\\&= (n+1)^{n+1}.\end{aligned}$$

这样就结束了归纳步骤，并且完成了整个证明. ◀

现在我们根据良序性质证明数学归纳原理.

**证明** 设 $S$ 是包含整数 1 的正整数集合，并且如果它包含整数 $n$，则一定包含 $n+1$. 假定(为了推出矛盾)$S$ 不是所有正整数的集合. 因此有某个正整数不包含在集合 $S$ 中. 由良序性质，由于不包含在 $S$ 中的正整数集合是非空的，所以不包含于 $S$ 中的所有正整数中存在一个最小的正整数，记为 $n$. 注意由于 1 在 $S$ 中，故 $n\neq 1$.

现在，由于 $n>1$(因为不存在正整数 $n$ 满足 $n<1$)，故 $n-1$ 是小于 $n$ 的正整数，并且一定在集合 $S$ 中. 但是因为 $S$ 包含 $n-1$，从而一定包含 $(n-1)+1=n$，这与假定 $n$ 为不包含于 $S$ 中的最小整数矛盾. 这说明 $S$ 一定是所有正整数的集合. ■

数学归纳原理的另一形式有时在证明中也很有用.

**定理 1.6**(第二数学归纳原理) 对于包含 1 的正整数集合，如果它具有下述性质：对每一个正整数 $n$，如果它包含全体正整数 1，2，…，$n$，则它也包含整数 $n+1$，那么这个集合一定是由所有正整数构成的集合.

为了区别于数学归纳原理，第二数学归纳原理有时也称为强归纳，而数学归纳原理也称为弱归纳.

在证明第二数学归纳原理的有效性之前，我们先给出一个例子说明如何使用它.

**例 1.24** 我们要证明任何超过 1 分的邮资都可以仅仅由 2 分和 3 分的邮票构成. 对于基础步骤，注意 2 分的邮资可以使用一张 2 分的邮票，3 分的邮资可以使用一张 3 分的邮票.

对于归纳步骤，假定所有不超过 $n(n\geqslant 3)$ 分的邮资都可以由 2 分和 3 分的邮票构成. 则 $n+1$ 分的邮资可以由 $n-1$ 分的邮资和一张 2 分的邮票构成. 这就完成了证明. ◀

现在证明第二数学归纳原理是正确的.

**证明** 设 $T$ 是一个包含 1 的整数集合，并且对任意正整数 $n$，如果它包含 1，2，…，$n$，则它也包含 $n+1$. 设 $S$ 是所有使得小于等于 $n$ 的正整数都在 $T$ 中的正整数 $n$ 的集合. 则 1 在 $S$ 中，并且，根据假设，我们看到如果 $n$ 在 $S$ 中，则 $n+1$ 在 $S$ 中. 因此，由数学归纳法原理，$S$ 必为所有正整数的集合，故显然 $T$ 也是所有正整数的集合，因为 $S$ 是 $T$ 的一个子集. ■

## 递归定义

数学归纳原理提供了一种方法来定义函数在正整数处的值. 我们不用明确给出函数在 $n$ 处的值，而是给出其在 1 处的值，并且给出对于任意正整数 $n$，从函数在 $n$ 处的值来寻找在 $n+1$ 处的值的规则.

**定义** 我们说函数 $f$ 是**递归定义的**，如果指定了 $f$ 在 1 处的值，而且对于任意正整数 $n$，都提供了一个规则来根据 $f(n)$ 确定 $f(n+1)$.

数学归纳原理可以用来证明递归定义的函数在每个正整数上都是唯一定义的(参看本

节末尾的习题 25). 我们用下面的例子说明如何来递归定义一个函数.

**例 1.25** 我们将递归定义阶乘函数 $f(n)=n!$. 首先，给定

$$f(1)=1.$$

然后对每个正整数给出一个根据 $f(n)$求 $f(n+1)$的规则，即

$$f(n+1)=(n+1)\cdot f(n).$$

这两个公式对正整数集合唯一定义了 $n!$.

根据递归定义来求 $f(6)=6!$ 的值，连续应用第二个公式如下：

$$f(6)=6\cdot f(5)=6\cdot 5\cdot f(4)=6\cdot 5\cdot 4\cdot f(3)=6\cdot 5\cdot 4\cdot 3\cdot f(2)=6\cdot 5\cdot 4\cdot 3\cdot 2\cdot f(1)$$

然后应用定义中的第一个公式使用 $f(1)$的值 1 来代替它，得到

$$6!=6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1=720.$$ ◀

第二数学归纳原理也可以作为递归定义的基础. 我们可以如下定义一个定义域为正整数集合的函数：首先指定它在 1 处的值，并且对每个正整数 $n$，给定一个根据 $f(j)(1\leqslant j\leqslant n-1)$的值求 $f(n)$的规则. 这将是在 1.4 节中讨论的斐波那契数序列的定义的基础.

## 1.3 节习题

1. 用数学归纳法证明对任意正整数 $n$，有 $n<2^n$.
2. 猜想前 $n$ 个正偶数的和的公式. 用数学归纳法证明你的结果.
3. 用数学归纳法证明对任意正整数 $n$，有 $\sum_{k=1}^{n}\frac{1}{k^2}=\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{n^2}\leqslant 2-\frac{1}{n}$.
4. 对较小的整数 $n$，猜测 $\sum_{k=1}^{n}\frac{1}{k(k+1)}=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}$的公式. 用数学归纳法证明你的猜测是正确的.（与 1.2 节习题 17 比较.）
5. 猜测 $A^n$ 的公式，其中 $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. 用数学归纳法证明你的猜测.
6. 用数学归纳法证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}j=1+2+3+\cdots+n=n(n+1)/2$.（与 1.2 节例 1.19 比较.）
7. 用数学归纳法证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}j^2=1^2+2^2+3^2+\cdots+n^2=n(n+1)(2n+1)/6$.
8. 用数学归纳法证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}j^3=1^3+2^3+3^3+\cdots+n^3=[n(n+1)/2]^2$.
9. 用数学归纳法证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}j(j+1)=1\cdot 2+2\cdot 3+\cdots+n\cdot(n+1)=n(n+1)(n+2)/3$.
10. 用数学归纳法证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}(-1)^{j-1}j^2=1^2-2^2+3^2-\cdots+(-1)^{n-1}n^2=(-1)^{n-1}n(n+1)/2$.
11. 求 $\sum_{j=1}^{n}2^j$ 的公式.
12. 证明对任意正整数 $n$，都有 $\sum_{j=1}^{n}j\cdot j!=1\cdot 1!+2\cdot 2!+\cdots+n\cdot n!=(n+1)!-1$.

13. 证明大于 11 分的任意整数分值的邮资都可以仅仅由 4 分和 5 分的邮票构成.
14. 证明大于 53 分的任意整数分值的邮资都可以仅仅由 7 分和 10 分的邮票构成.

设 $H_n$ 是调和级数的前 $n$ 项和，即 $H_n=\sum_{j=1}^{n}1/j$.

* 15. 用数学归纳法证明 $H_{2^n}\geqslant 1+n/2$.

* 16. 用数学归纳法证明 $H_{2^n}\leqslant 1+n$.

17. 用数学归纳法证明：如果 $n$ 为正整数，则 $(2n)!<2^{2n}(n!)^2$.
18. 用数学归纳法证明 $x-y$ 是 $x^n-y^n$ 的因子，其中 $x$ 和 $y$ 是变量.
19. 应用数学归纳原理证明，包含整数 $k$ 的整数集合如果满足只要包含 $n$ 就包含 $n+1$，则这个集合包含大于等于 $k$ 的整数集合.
20. 应用数学归纳法证明对于 $n\geqslant 4$，有 $2^n<n!$.
21. 应用数学归纳法证明对于 $n\geqslant 4$，有 $n^2<n!$.
22. 应用数学归纳法证明：如果 $h\geqslant -1$，则对于任意非负整数 $n$，有 $1+nh\leqslant(1+h)^n$.
23. 七巧板问题就是把它的每一块按照正确的方式组合在一起. 证明解决 $n$ 片七巧板问题恰需要移动 $n-1$ 步，其中移动一步表示把两块放在一起，而每一块包含一个或多个装配好的片.（提示：用第二数学归纳原理.）
24. 解释下面利用数学归纳法证明所有马都是同色的过程错在哪里：显然只有一匹马的集合中所有马都是同色的，这就是基础步骤. 现在假定任何 $n$ 匹马的集合中所有马都是同色的. 考虑有 $n+1$ 匹马的集合，分别标记为整数 1，2，…，$n+1$. 由归纳假设，标号为 1，2，…，$n$ 的马为同色的，标号为 2，3，…，$n$，$n+1$ 的马也为同色的. 由于这两个集合有公共成员，即 2，3，4，…，$n$ 号马，所以所有的这 $n+1$ 匹马一定是同色. 这就完成了归纳步骤.
25. 应用数学归纳原理证明递归定义的函数在每个正整数处的值都是唯一确定的.
26. 由 $f(1)=2$ 和 $f(n+1)=2f(n)(n\geqslant 1)$ 递归定义的函数 $f(n)$ 是什么？用数学归纳法证明你的结论.
27. 如果 $g$ 是由 $g(1)=2$ 和 $g(n)=2^{g(n-1)}(n\geqslant 2)$ 递归定义的，那么 $g(4)$ 是多少？
28. 应用第二数学归纳原理证明：如果指定 $f(1)$ 的值，且给定了根据 $f$ 在前 $n$ 个正整数处的值求 $f(n+1)$ 的规则，则 $f(n)$ 对每个正整数 $n$ 都是唯一确定的.
29. 我们对所有正整数 $n$ 递归地定义函数如下：$f(1)=1$，$f(2)=5$，且对 $n\geqslant 2$，$f(n+1)=f(n)+2f(n-1)$. 用第二数学归纳原理证明 $f(n)=2^n+(-1)^n$.
30. 证明当 $n$ 为大于 4 的整数时，$2^n>n^2$.
31. 假定 $a_0=1$，$a_1=3$，$a_2=9$，且对 $n\geqslant 3$，$a_n=a_{n-1}+a_{n-2}+a_{n-3}$. 证明对每个非负整数 $n$，有 $a_n\leqslant 3^n$.

* 32. 河内塔是在 19 世纪末流行的难题. 这个题目包括三个木桩和八个不同尺寸且按照尺寸大小放置的圆环，这些圆环最大的在底部，全都套在一个木桩上. 题目要求每次移动一个圆环，并且不能把尺寸大的圆环放在尺寸小的圆环上面，利用第三个辅助木桩，把所有的圆环从第一个木桩移动到第二个木桩.

a) 应用数学归纳法证明，按照前述规则把 $n$ 个圆环从一个木桩移动到另外一个木桩上的最小移动次数为 $2^n-1$.

b) 一个古代传说讲述的是在一个有 64 个金环和三个钻石桩子的塔中的一些僧侣. 当世界被创立之初，他们以每秒钟移动一个环的速度开始移动金环. 当他们把所有的环都移动到第二个桩子上时，就是世界的末日. 那么这个世界将会存在多久？

* 33. 正实数 $a_1$，$a_2$，…，$a_n$ 的算术平均和几何平均分别为 $A=(a_1+a_2+\cdots+a_n)/n$ 和 $G=(a_1a_2\cdots a_n)^{1/n}$. 用数学归纳法证明对任意正实数的有限序列，$A\geqslant G$. 等式何时成立？

34. 用数学归纳法证明缺一个小方格的 $2^n\times 2^n$ 的棋盘可以被 $L$-形的片覆盖，其中每个 $L$-形片包括三个小

方格.

* 35. 单分数是形为 $1/n$ 的分数，其中 $n$ 为正整数. 由于古埃及人把分数表示为不同的单分数的和，因此这样的和被称为埃及分数. 证明任意有理数 $p/q$(其中 $p$ 和 $q$ 为整数，且 $0<p<q$)可以被写为不同的单分数的和，即写为埃及分数.(提示：对分子 $p$ 用强归纳来证明在每一步加上一个可能的最大单分数的算法是可以终止的. 例如，运行这个算法证明 $5/7=1/2+1/5+1/70$.)

36. 用习题 35 的算法把下面这些数写为埃及分数.

a) 2/3 b) 5/8 c) 11/17 d) 44/101

**计算和研究**

1. 使用数值和符号计算两种方法，完成基础和归纳步骤，对所有正整数 $n$，证明 $\sum_{j=1}^{n} j=n(n+1)/2$.

2. 使用数值和符号计算两种方法，完成基础和归纳步骤，对所有正整数 $n$，证明 $\sum_{j=1}^{n} j^2=n(n+1)(2n+1)/6$.

3. 使用数值和符号计算两种方法，完成基础和归纳步骤，对所有正整数 $n$，证明 $\sum_{j=1}^{n} j^3=(n(n+1)/2)^2$.

4. 利用 $n=1$，2，3，4，5，6 时 $\sum_{j=1}^{n} j^4$ 的值来猜测这个和的表达式是一个关于 $n$ 的 5 次多项式，并从数值和符号计算两种途径用数学归纳法证明你的猜测.

5. Paul Erdös 和 E. Strauss 曾经猜测分数 $4/n$ 可以被写为三个单分数的和，即对任意满足 $n>1$ 的整数 $n$，$4/n=1/x+1/y+1/z$，其中 $x$，$y$ 和 $z$ 是不同的正整数. 对尽量多的正整数 $n$ 求这样的表示.

6. 设 $p$ 和 $q$ 是满足 $0<p<q$ 的整数，且 $q$ 为奇数，猜想有理数 $p/q$ 可以表示为埃及分数，即奇数分母的单分数之和. 使用下述算法研究这个猜想，即在每一步逐步地加上具有最小正奇数分母 $q$ 的单分数.(例如，$2/7=1/5+1/13+1/115+1/10\,465$.)

**程序设计**

* 1. 列出河内塔问题(见习题 32)中的移动步骤. 如果可以，动画显示这些移动步骤.

** 2. 用 $L$-形片覆盖缺一个小方格的 $2^n\times 2^n$ 棋盘(见习题 34).

3. 给定有理数 $p/q$，用习题 35 中描述的算法把 $p/q$ 表示为埃及分数.

## 1.4 斐波那契数

数学家斐波那契在他写于 1202 年的书《算经》(Liber Abaci)中提出了一个涉及某特定地区中兔子的生长数量的问题. 这个问题可以如下叙述：一对年轻的兔子，每种性别一只，被放在一个岛上. 假定兔子到两个月大才开始繁殖，两个月后每对兔子每个月生一对兔子，问 $n$ 个月后有多少对兔子?

设 $f_n$ 为 $n$ 个月后兔子的对数. 我们有 $f_1=1$，因为一个月后在岛上只有原始的那对兔子. 由于这对兔子在第二个月不繁殖，故 $f_2=1$. 为了求 $n$ 个月后的兔子对数，把岛上上个月兔子的数目 $f_{n-1}$ 加上新出生的兔子对数，即为 $f_{n-2}$，因为每一对新出生的兔子都来自至少两个月大的兔子. 这就导出了下面的定义.

**定义** **斐波那契序列**有如下递归定义：$f_1=1$，$f_2=1$，且对 $n\geqslant 3$，$f_n=f_{n-1}+f_{n-2}$. 这个序列中的项被称为**斐波那契数**.

**斐波那契**(Fibonacci，1180—1228)(filus Bonacci，Bonacci之子的简称)也称为比萨的里昂纳多，生于意大利的商业中心比萨．斐波那契是一个商人，经常往来于中东．在那里他接触了一些阿拉伯世界的数学工作．在他的著作《算经》中，斐波那契将阿拉伯数字的记法及其算法引入了欧洲．该书中就提到了这个著名的兔子繁殖问题．斐波那契还写过一本关于几何学与三角几何学的专著《Practica geometriae》以及一本关于丢番图方程的书《Liber quadratorum》.

数学家爱德华·卢卡斯于19世纪给出了这个序列的许多性质，并以斐波那契命名这个序列．斐波那契问题的答案是 $n$ 个月后岛上有 $f_n$ 对兔子.

在研究斐波那契序列的性质时，检查它的初始几项是十分有用的.

**例 1.26** 我们计算前十个斐波那契数如下：

$$\begin{aligned}
f_3 &= f_2 + f_1 = 1 + 1 = 2\\
f_4 &= f_3 + f_2 = 2 + 1 = 3\\
f_5 &= f_4 + f_3 = 3 + 2 = 5\\
f_6 &= f_5 + f_4 = 5 + 3 = 8\\
f_7 &= f_6 + f_5 = 8 + 5 = 13\\
f_8 &= f_7 + f_6 = 13 + 8 = 21\\
f_9 &= f_8 + f_7 = 21 + 13 = 34\\
f_{10} &= f_9 + f_8 = 34 + 21 = 55.
\end{aligned}$$

◀

我们可以定义 $f_0 = 0$，从而 $f_2 = f_1 + f_0$．还可以对负数 $n$ 定义 $f_n$，使其满足递归定义(见习题37).

斐波那契数显示出了多得令人惊讶的应用．例如，在植物学中植物的螺旋线的数目(就是我们所知的叶序)总是斐波那契数．它们在大量计数问题的解答中出现，例如在没有两个连续的1的比特串数目的计数问题中[Ro07].

斐波那契数还满足相当多的恒等式．例如，我们可以容易地找到一个关于前 $n$ 个斐波那契数的和的恒等式.

**例 1.27** 对于 $3 \leqslant n \leqslant 8$，前 $n$ 个斐波那契数的和等于1，2，4，7，12，20，33和54．观察这些数，可以看到它们恰比斐波那契数 $f_{n+2}$ 小1．故可以猜想

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1.$$

我们是否能证明这个恒等式对所有正整数 $n$ 成立？

我们将要用两个不同的方法证明这个恒等式对于所有整数 $n$ 成立．我们提供两个不同的实例来说明：常常有多种方法来证明一个恒等式是正确的.

首先，利用事实 $f_n = f_{n-1} + f_{n-2}$ ($n = 2, 3, \cdots$)得出 $f_k = f_{k+2} - f_{k+1}$，其中 $k = 1, 2, 3, \cdots$．这意味着

$$\sum_{k=1}^{n} f_k = \sum_{k=1}^{n} (f_{k+2} - f_{k+1}).$$

我们很容易计算这些和，因为它们是叠进和. 利用 1.2 节中的叠进和的公式，我们得到

$$\sum_{k=1}^{n} f_k = f_{n+2} - f_2 = f_{n+2} - 1.$$

这就证明了上述结果.

还可以用数学归纳法证明这个恒等式. 因为 $\sum_{k=1}^{1} f_k = 1$，且 $f_{1+2} - 1 = f_3 - 1 = 2 - 1 = 1$，故基础步骤成立. 归纳假设是

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1.$$

我们必须在这个假设下证明

$$\sum_{k=1}^{n+1} f_k = f_{n+3} - 1.$$

为了证明这个结果，注意到根据归纳假设有

$$\begin{aligned}\sum_{k=1}^{n+1} f_k &= \left(\sum_{k=1}^{n} f_k\right) + f_{n+1} \\ &= (f_{n+2} - 1) + f_{n+1} \\ &= (f_{n+1} + f_{n+2}) - 1 \\ &= f_{n+3} - 1.\end{aligned}$$

◀

本节末的习题要求你去证明许多关于斐波那契数的其他恒等式.

**斐波那契数增长有多快**

下面的不等式说明斐波那契数比公比为 $\alpha = (1+\sqrt{5})/2$ 的等比数列增长得快，这一结论将在第 3 章中应用.

**例 1.28** 我们可以用第二数学归纳原理证明对 $n \geqslant 3$，有 $f_n > \alpha^{n-2}$，其中 $\alpha = (1+\sqrt{5})/2$. 基础步骤包括对于 $n=3$ 和 $n=4$ 验证这个不等式. 我们有 $\alpha < 2 = f_3$，所以定理对 $n=3$ 成立. 由于 $\alpha^2 = (3+\sqrt{5})/2 < 3 = f_4$，故定理对 $n=4$ 成立.

归纳假设假定对满足 $k \leqslant n$ 的所有整数 $k$，都有 $\alpha^{k-2} < f_k$. 由于 $\alpha = (1+\sqrt{5})/2$ 是 $x^2 - x - 1 = 0$ 的一个解，故 $\alpha^2 = \alpha + 1$. 因此

$$\alpha^{n-1} = \alpha^2 \cdot \alpha^{n-3} = (\alpha+1) \cdot \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}.$$

由归纳假设，我们得到不等式

$$\alpha^{n-2} < f_n, \qquad \alpha^{n-3} < f_{n-1}.$$

把这两个不等式加起来，得到

$$\alpha^{n-1} < f_n + f_{n-1} = f_{n+1}.$$

这就完成了证明. ◀

我们用第 $n$ 个斐波那契数的一个显式计算公式来结束本节. 我们在正文中不给出证明，但是在本节末的习题 41 和习题 42 中概述了如何分别利用线性齐次递归关系和母函数来求这个公式. 进一步，习题 40 要求通过说明这些项满足与斐波那契数相同的递归定义来证明这个恒等式，习题 45 要求用数学归纳法来证明. 前两个方法的优点是它们可以用来发现公

式，而后两个方法却不能.

**定理 1.7**　设 $n$ 是正整数，$\alpha=\dfrac{1+\sqrt{5}}{2}$，$\beta=\dfrac{1-\sqrt{5}}{2}$. 则第 $n$ 个斐波那契数 $f_n$ 由下式给出：

$$f_n=\frac{1}{\sqrt{5}}(\alpha^n-\beta^n).$$

我们已经给出了关于斐波那契数的几个重要结果. 有大量关于这些数以及它们在植物学、计算机科学、地理学、物理学以及其他领域的应用的文献(参见[Va89]). 甚至有一个学术刊物《斐波那契季刊》(The Fibonacci Quarterly)专门报道关于它们的研究.

## 1.4 节习题

1. 求下列斐波那契数.
   a) $f_{10}$　b) $f_{13}$　c) $f_{15}$　d) $f_{18}$　e) $f_{20}$　f) $f_{25}$
2. 求下列斐波那契数.
   a) $f_{12}$　b) $f_{16}$　c) $f_{24}$　d) $f_{30}$　e) $f_{32}$　f) $f_{36}$
3. 证明当 $n$ 为正整数时，$f_{n+3}+f_n=2f_{n+2}$.
4. 证明当 $n$ 为正整数时，$f_{n+3}-f_n=2f_{n+1}$.
5. 证明当 $n$ 为正整数时，$f_{2n}=f_n^2+2f_{n-1}f_n$. (注意 $f_0=0$.)
6. 证明当 $n$ 为满足 $n\geqslant 2$ 的整数时，$f_{n-2}+f_{n+2}=3f_n$. (注意 $f_0=0$.)
7. 对正整数 $n$，求前 $n$ 个奇数下标的斐波那契数的和的简单公式，并且给出证明. 即求 $f_1+f_3+\cdots+f_{2n-1}$ 的一个公式.
8. 对正整数 $n$，求前 $n$ 个偶数下标的斐波那契数的和的简单公式，并且给出证明. 即求 $f_2+f_4+\cdots+f_{2n}$ 的一个公式.
9. 对正整数 $n$，求表达式 $f_n-f_{n-1}+f_{n-2}-\cdots+(-1)^{n+1}f_1$ 的一个简单公式.
10. 证明当 $n$ 为正整数时，$f_{2n+1}=f_{n+1}^2+f_n^2$.
11. 证明当 $n$ 为正整数时，$f_{2n}=f_{n+1}^2-f_{n-1}^2$. (注意 $f_0=0$.)
12. 证明当 $n$ 为满足 $n\geqslant 3$ 的正整数时，$f_n+f_{n-1}+f_{n-2}+2f_{n-3}+4f_{n-4}+8f_{n-5}+\cdots+2^{n-3}=2^{n-1}$.
13. 证明对任意正整数 $n$，$\sum_{j=1}^{n}f_j^2=f_1^2+f_2^2+\cdots+f_n^2=f_nf_{n+1}$.
14. 证明对任意正整数 $n$，$f_{n+1}f_{n-1}-f_n^2=(-1)^n$.
15. 证明对任意正整数 $n$，$n>2$，有 $f_{n+1}f_n-f_{n-1}f_{n-2}=f_{2n-1}$.
16. 证明：如果 $n$ 是一个正整数，则 $f_1f_2+f_2f_3+\cdots+f_{2n-1}f_{2n}=f_{2n}^2$.
17. 证明当 $m$ 和 $n$ 为正整数时，$f_{m+n}=f_mf_{n+1}+f_nf_{m-1}$.

卢卡斯数以 François-Eduoard-Anatole Lucas(见第 7 章的人物传记)命名，递归定义如下：

$$L_n=L_{n-1}+L_{n-2},n\geqslant 3$$

其中 $L_1=1$，$L_2=3$. 它们满足与斐波那契数相同的递归关系，但是初始的两项是不同的.

18. 求前 12 个卢卡斯数.
19. 当 $n$ 为正整数时，求前 $n$ 个卢卡斯数的和的公式，并证明之.
20. 当 $n$ 为正整数时，求前 $n$ 个奇数下标的卢卡斯数的和的公式，并证明之.
21. 当 $n$ 为正整数时，求前 $n$ 个偶数下标的卢卡斯数的和的公式，并证明之.
22. 证明当 $n$ 为满足 $n\geqslant 2$ 的整数时，$L_n^2-L_{n+1}L_{n-1}=5(-1)^n$.

23. 证明当 $n$ 为满足 $n\geqslant 1$ 的整数时，$L_1^2+L_2^2+\cdots+L_n^2=L_nL_{n+1}-2$.

24. 证明第 $n$ 个卢卡斯数是第 $n+1$ 个斐波那契数 $f_{n+1}$ 和第 $n-1$ 个斐波那契数 $f_{n-1}$ 之和.

25. 证明对满足 $n\geqslant 1$ 的所有整数 $n$，有 $f_{2n}=f_nL_n$，其中 $f_n$ 是第 $n$ 个斐波那契数，$L_n$ 是第 $n$ 个卢卡斯数.

26. 证明当 $n$ 为正整数时，$5f_{n+1}=L_n+L_{n+2}$，其中 $f_n$ 是第 $n$ 个斐波那契数，$L_n$ 是第 $n$ 个卢卡斯数.

* 27. 证明当 $m$ 和 $n$ 为正整数且 $n>1$ 时，$L_{m+n}=f_{m+1}L_n+f_mL_{n-1}$，其中 $f_n$ 是第 $n$ 个斐波那契数，$L_n$ 是第 $n$ 个卢卡斯数.

28. 证明第 $n$ 个卢卡斯数 $L_n$ 由下式给出：

$$L_n=\alpha^n+\beta^n,$$

其中 $\alpha=(1+\sqrt{5})/2$，$\beta=(1-\sqrt{5})/2$.

正整数的**泽肯朵夫(Zeckendorf)表示**是把整数写成不同的斐波那契数的和的唯一表示，其中这些斐波那契数中没有任何两个是斐波那契序列中的连续项，并且其中不使用 $f_1=1$ 这一项(但是可能会用到 $f_2=1$ 这一项.)

29. 求整数 50，85，110 和 200 的泽肯朵夫表示.

* 30. 证明每个正整数都有唯一的泽肯朵夫表示.

31. 证明对每个满足 $n\geqslant 2$ 的正整数 $n$ 都有 $f_n\leqslant\alpha^{n-1}$，其中 $\alpha=(1+\sqrt{5})/2$.

32. 证明

$$\binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots=f_{n+1},$$

其中 $n$ 为非负整数，$f_{n+1}$ 为第 $n+1$ 个斐波那契数. $\left($关于二项式系数请参看附录 B. 这里这个和结束于项$\binom{1}{n-1}$.$\right)$

33. 证明当 $n$ 为非负整数时，$\sum_{j=1}^{n}\binom{n}{j}f_j=f_{2n}$，其中 $f_j$ 是第 $j$ 个斐波那契数.

34. 设 $\boldsymbol{F}=\begin{pmatrix}1&1\\1&0\end{pmatrix}$，证明当 $n\in\mathbb{Z}^+$ 时 $\boldsymbol{F}^n=\begin{pmatrix}f_{n+1}&f_n\\f_n&f_{n-1}\end{pmatrix}$.

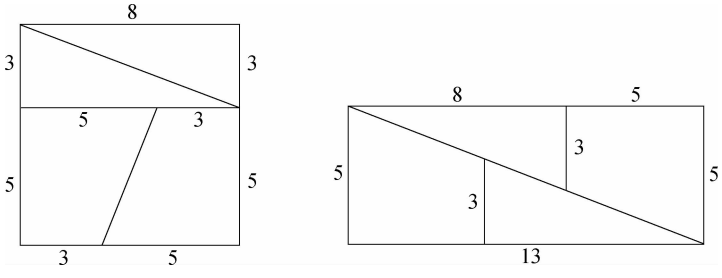
35. 通过对习题 34 的结果两边同时取行列式来证明习题 14 中的恒等式.

36. 递归定义广义斐波那契数如下：$g_1=a$，$g_2=b$，$g_n=g_{n-1}+g_{n-2}$，$n\geqslant 3$. 证明 $g_n=af_{n-2}+bf_{n-1}$，$n\geqslant 3$.

37. 当 $n$ 为负整数时，给出斐波那契数的一个递归定义. 用该定义对 $n=-1$，$-2$，$-3$，…，$-10$ 求出 $f_n$.

38. 当 $n$ 为正整数时，利用习题 37 的结果给出一个刻画 $f_{-n}$ 和 $f_n$ 的关系的公式的猜想. 用数学归纳法证明你的猜想.

39. 指出下面陈述中的错误：8×8 的正方形能够分割成几片，在重新安置之后形成一个如下图所示的 5×13 长方形.



（提示：观察习题 14 中的恒等式．哪里多出了一个平方单元?）

40. 证明：如果 $a_n=\frac{1}{\sqrt{5}}(\alpha^n-\beta^n)$，其中 $\alpha=(1+\sqrt{5})/2$，$\beta=(1-\sqrt{5})/2$，则 $a_n=a_{n-1}+a_{n-2}$，且 $a_1=a_2=1$. 从而得到 $f_n=a_n$，其中 $f_n$ 是第 $n$ 个斐波那契数.

一个常系数的 2 次线性齐次递归关系是一个形如

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

的方程，其中 $c_1$ 和 $c_2$ 为实数且 $c_2\neq 0$．不难证明(见[Ro07])如果方程 $r^2-c_1 r-c_2=0$ 有两个不同的根 $r_1$ 和 $r_2$，则序列 $\{a_n\}$ 是线性齐次递归关系 $a_n=c_1 a_{n-1}+c_2 a_{n-2}$ 的解当且仅当 $a_n=C_1 r_1^n+C_2 r_2^n$，其中 $n=0$，1，2，…，且 $C_1$ 和 $C_2$ 是常数．这些常数的值可以通过这个序列的前两项求得.

41. 通过解初始条件为 $f_0=0$ 和 $f_1=1$ 的递归关系 $f_n=f_{n-1}+f_{n-2}$(其中 $n=2$，3，…)求 $f_n$ 的显式公式，从而证明定理 1.7.

序列 $a_0$，$a_1$，…，$a_k$，…的母函数是无穷级数

$$G(x) = \sum_{k=0}^{\infty} a_k x^k.$$

42. 用母函数 $G(x)=\sum_{k=0}^{\infty} f_k x^k$ 来求 $f_k$ 的一个显式公式，证明定理 1.7，其中 $f_k$ 是第 $k$ 个斐波那契数．(提示：使用事实 $f_k=f_{k-1}+f_{k-2}$($k=2$，3，…)来证明 $G(x)-xG(x)-x^2G(x)=x$．解这个方程证明 $G(x)=x/(1-x-x^2)$，然后像在微积分中一样把它写成部分分式的形式.)(关于应用母函数的信息请参看[Ro07].)

43. 用习题 41 中的技巧求卢卡斯数的显式公式.

44. 用习题 42 中的技巧求卢卡斯数的显式公式.

45. 用数学归纳法证明定理 1.7.

**计算和研究**

1. 求斐波那契数 $f_{100}$，$f_{200}$ 和 $f_{500}$.
2. 求卢卡斯数 $L_{100}$，$L_{200}$ 和 $L_{500}$.
3. 考察尽可能多的斐波那契数，判断它们是否是完全平方数，并依此提出相关的猜想.
4. 考察尽可能多的斐波那契数，判断它们是否是三角数，并依此提出相关的猜想.
5. 考察尽可能多的斐波那契数，判断它们是否是完全立方数，并依此提出相关的猜想.
6. 分别找出不超过 10 000 的最大的斐波那契数、不超过 100 000 的最大的斐波那契数和不超过 1 000 000 的最大的斐波那契数.
7. 一个令人惊讶的定理表明斐波那契数是当 $x$ 和 $y$ 取遍所有非负整数时多项式 $2xy^4+x^2y^3-2x^3y^2-y^5-x^4y+2y$ 的全部正值．对满足 $x+y\leqslant 100$ 的非负整数 $x$ 和 $y$，验证这个猜想.

**程序设计**

1. 给定一个正整数 $n$，求斐波那契序列的前 $n$ 项.
2. 给定一个正整数 $n$，求卢卡斯序列的前 $n$ 项.
3. 给定一个正整数 $n$，求其泽肯朵夫表示(习题 29 前有定义).

## 1.5　整除性

一个整数可以被另一个整数整除的概念在数论中处于中心地位.

**定义**　如果 $a$ 和 $b$ 为整数且 $a\neq 0$，我们说 ***a* 整除 *b*** 是指存在整数 $c$ 使得 $b=ac$．如果 $a$ 整除 $b$，我们还称 ***a* 是 *b* 的一个因子**，且称 ***b* 是 *a* 的倍数**.

如果 $a$ 整除 $b$，则将其记为 $a\mid b$，如果 $a$ 不能整除 $b$，则记其为 $a\nmid b$．(小心不要弄混

了记号 $a|b$ 和 $a/b$，前者表示 $a$ 整除 $b$，后者表示 $a$ 被 $b$ 除所得的商.)

**例 1.29** 下面是说明整数的整除性概念的例子：$13|182$，$-5|30$，$17|289$，$6\nmid 44$，$7\nmid 50$，$-3|33$，$17|0$. ◀

**例 1.30** 6 的因子是 $\pm1$，$\pm2$，$\pm3$，$\pm6$. 17 的因子是 $\pm1$，$\pm17$. 100 的因子是 $\pm1$，$\pm2$，$\pm4$，$\pm5$，$\pm10$，$\pm20$，$\pm25$，$\pm50$，$\pm100$. ◀

在后面几章中，需要一些关于整除性的简单性质，现在我们来叙述并证明它们.

**定理 1.8** *如果 $a$，$b$ 和 $c$ 是整数，且 $a|b$，$b|c$，则 $a|c$.*

**证明** 因为 $a|b$，$b|c$，故存在整数 $e$ 和 $f$，使得 $ae=b$，$bf=c$. 因此 $c=bf=(ae)f=a(ef)$，从而得到 $a|c$. ■

**例 1.31** 因为 $11|66$，$66|198$，故由定理 1.8 可知 $11|198$. ◀

**定理 1.9** *如果 $a$，$b$，$m$ 和 $n$ 为整数，且 $c|a$，$c|b$，则 $c|(ma+nb)$.*

**证明** 因为 $c|a$ 且 $c|b$，故存在整数 $e$ 和 $f$，使得 $a=ce$，$b=cf$. 因此，$ma+nb=mce+ncf=c(me+nf)$. 从而，$c|(ma+nb)$. ■

**例 1.32** 由于 $3|21$，$3|33$，故由定理 1.9 可知 3 能够整除

$$5\cdot 21-3\cdot 33=105-99=6.$$ ◀

下面的定理是一个关于整除性的重要结论.

**定理 1.10(带余除法)** *如果 $a$ 和 $b$ 是整数且 $b>0$，则存在唯一的整数 $q$ 和 $r$，使得 $a=bq+r$，$0\leqslant r<b$.*

在带余除法给出的公式中，我们称 $q$ 为商，$r$ 为余数. 我们还称 $a$ 为被除数，$b$ 为除数.(注意：这个定理采用了传统的名字，尽管带余除法实际上不是一个算法. 我们将在 2.2 节中讨论算法.)

我们注意到 $a$ 能被 $b$ 整除当且仅当在带余除法中的余数为 0. 在证明带余除法之前，先考虑下面的例子.

**例 1.33** 如果 $a=133$，$b=21$，则 $q=6$，$r=7$，因为 $133=21\cdot 6+7$ 且 $0<7<21$. 类似地，如果 $a=-50$，$b=8$，则 $q=-7$，$r=6$，因为 $-50=8(-7)+6$ 且 $0<6<8$. ◀

我们现在用良序性质证明带余除法.

**证明** 考虑形如 $a-bk$ 的所有整数集合 $S$，其中 $k$ 为整数，即 $S=\{a-bk\,|\,k\in\mathbb{Z}\}$. 设 $T$ 是 $S$ 中的所有非负整数构成的集合. $T$ 是非空的，因为当 $k$ 是满足 $k<a/b$ 的整数时，$a-bk$ 是正的.

由良序性质，$T$ 中有最小元 $r=a-bq$.($q$ 和 $r$ 的值如定理中所述.)根据 $r$ 的构造可知 $r\geqslant 0$，且容易证明 $r<b$. 如果 $r\geqslant b$，则 $r>r-b=a-bq-b=a-b(q+1)\geqslant 0$，这与我们选择 $r=a-bq$ 为形如 $a-bk$ 的整数中的最小元矛盾. 因此 $0\leqslant r<b$.

为了证明 $q$ 和 $r$ 的值是唯一的，我们假定有两个方程 $a=bq_1+r_1$ 和 $a=bq_2+r_2$，满足 $0\leqslant r_1<b$，$0\leqslant r_2<b$. 把第二个方程从第一个方程中减去，可得

$$0=b(q_1-q_2)+(r_1-r_2).$$

因此，

$$r_2-r_1=b(q_1-q_2).$$

由此可知 $b$ 整除 $r_2-r_1$. 因为 $0\leqslant r_1<b$，$0\leqslant r_2<b$，故 $-b<r_2-r_1<b$. 因此 $b$ 可以整除 $r_2-r_1$ 只有当 $r_2-r_1=0$，或者，换句话说，当 $r_1=r_2$ 时. 因为 $bq_1+r_1=bq_2+r_2$，且 $r_1=r_2$，我们还得到 $q_1=q_2$. 这说明商 $q$ 与余数 $r$ 是唯一的. ■

我们现在应用最大整数函数(在 1.1 节中定义的)来给出带余除法中商和余数的显式公式. 因为商 $q$ 是满足 $bq\leqslant a$ 和 $r=a-bq$ 的最大整数，因而

$$q=[a/b],\qquad r=a-b[a/b]. \tag{1.4}$$

下面的例子展示了除法中的商和余数.

**例 1.34** 设 $a=1028$，$b=34$，则 $a=bq+r$，$0\leqslant r<b$，其中 $q=[1028/34]=30$，$r=1028-[1028/34]\cdot 34=1028-30\cdot 34=8$. ◀

**例 1.35** 设 $a=-380$，$b=75$，则 $a=bq+r$，$0\leqslant r<b$，其中 $q=[-380/75]=-6$，$r=-380-[-380/75]\cdot 75=-380-(-6)75=70$. ◀

我们可以使用等式(1.4)来证明关于最大整数函数的一个有用的性质.

**例 1.36** 证明：如果 $n$ 是正整数，则当 $x$ 为实数时 $[x/n]=[[x]/n]$. 为了证明这个等式，假定 $[x]=m$. 由带余除法，我们有整数 $q$ 和 $r$ 使得 $m=nq+r$，其中 $0\leqslant r\leqslant n-1$. 根据(1.4)，我们有 $q=[[x]/n]$. 因为 $[x]\leqslant x<[x]+1$，故 $x=[x]+\varepsilon$，其中 $0\leqslant\varepsilon<1$. 我们看到 $[x/n]=[([x]+\varepsilon)/n]=[(m+\varepsilon)/n]=[((nq+r)+\varepsilon)/n]=[q+(r+\varepsilon)/n]$. 因为 $0\leqslant\varepsilon<1$，所以有 $0\leqslant r+\varepsilon<(n-1)+1=n$. 因此 $[x/n]=[q]$. ◀

给定一个正整数 $d$，可以根据整数被 $d$ 除的余数把它们分类. 例如，当 $d=2$ 时，我们从带余除法中看到任意整数被 2 除所得的余数或为 0，或为 1. 这引出了下面一些常见术语的定义.

**定义**　如果 $n$ 被 2 除的余数为 0，则对某个整数 $k$，有 $n=2k$，我们称 $n$ 为**偶数**；而如果 $n$ 被 2 除的余数为 1，则对某个整数 $k$，有 $n=2k+1$，我们称 $n$ 为**奇数**.

类似地，当 $d=4$ 时，我们从带余除法中看到当整数 $n$ 被 4 除时，余数为 0，1，2 或者 3. 因此，每个整数都形如 $4k$，$4k+1$，$4k+2$ 或 $4k+3$，其中 $k$ 为正整数.

我们将在第 4 章继续讨论这个问题.

### 最大公因子

如果 $a$ 和 $b$ 为不全为零的整数，则它们的公因子的集合是一个有限的整数集，通常包括 $+1$ 和 $-1$，我们对其中最大的那个公因子感兴趣.

**定义**　不全为零的整数 $a$ 和 $b$ 的**最大公因子**是指能够同时整除 $a$ 和 $b$ 的最大整数.

$a$ 和 $b$ 的最大公因子记作 $(a,b)$. (有时也记作 $\gcd(a,b)$，特别是在非数论的著作中. 我们将一直沿用传统的记号 $(a,b)$，虽然有时候这种记法也表示有序数对.)注意当 $n$ 为正整数时，$(0,n)=(n,0)=n$. 虽然所有的正整数都能整除 0，我们还是定义 $(0,0)=0$. 这样可以确保关于最大公因子的相关结论在所有情况下均成立.

**例 1.37** 24 和 84 的公因子有 $\pm1$，$\pm2$，$\pm3$，$\pm4$，$\pm6$，$\pm12$，因此 $(24,84)=12$. 类似地，通过查看公因子集合，我们有 $(15,81)=3$，$(100,5)=5$，$(17,25)=1$，$(0,44)=44$，$(-6,-15)=3$，以及 $(-17,289)=17$. ◀

我们特别关注那些所有公因子均不超过 1 的整数对，这样的数对被称为**互素**.

**定义** 设 $a$，$b$ 均为非零整数，如果 $a$ 和 $b$ 的最大公因子$(a, b)=1$，则称 $a$ 与 $b$ **互素**.

**例 1.38** 因为$(25, 42)=1$，所以 25 和 42 互素. ◀

我们将在第 4 章中详细研究最大公因子，并给出计算最大公因子的算法. 同时也将证明许多相关的结论，而这些结论能导出很多数论中的重要定理.

## 1.5 节习题

1. 证明 $3 \mid 99$，$5 \mid 145$，$7 \mid 343$，$888 \mid 0$.
2. 证明 1001 可以被 7，11 和 13 整除.
3. 确定下面整数中哪个可被 7 整除.
   a) 0　b) 707　c) 1717　d) 123 321　e) −285 714　f) −430 597
4. 确定下面整数中哪个可被 22 整除.
   a) 0　b) 444　c) 1716　d) 192 544　e) −32 516　f) −195 518
5. 求带余除法中的商和余数，其中除数为 17，被除数为
   a) 100　b) 289　c) −44　d) −100
6. 求出能整除下列整数的所有正整数.
   a) 12　b) 22　c) 37　d) 41
7. 求出能整除下列整数的所有正整数.
   a) 13　b) 21　c) 36　d) 44
8. 通过求整除下列数对中每个整数的所有正整数并选取最大的那个来求下列数对的最大公因子.
   a) (8，12)　b) (7，9)　c) (15，25)　d) (16，27)
9. 通过求整除下列数对中每个整数的所有正整数并选取最大的那个来求下列数对的最大公因子.
   a) (11，22)　b) (36，42)　c) (21，22)　d) (16，64)
10. 求出所有与 10 互素且小于 10 的正整数.
11. 求出所有与 11 互素且小于 11 的正整数.
12. 求出不超过 10 且互素的正整数对.
13. 求出介于 10 与 20 之间(包括 10 与 20)的互素的正整数对.
14. 如果 $a$ 和 $b$ 是非零整数，且 $a \mid b$，$b \mid a$，你能得到什么结论?
15. 证明：如果 $a$，$b$，$c$ 和 $d$ 是整数，$a$ 和 $c$ 非零，且满足 $a \mid b$，$c \mid d$，则 $ac \mid bd$.
16. 是否有整数 $a$，$b$ 和 $c$，使得 $a \mid bc$，但是 $a \nmid b$，且 $a \nmid c$?
17. 证明：如果 $a$，$b$ 和 $c \neq 0$ 都是整数，则 $a \mid b$ 当且仅当 $ac \mid bc$.
18. 证明：如果 $a$ 和 $b$ 是正整数且 $a \mid b$，则 $a \leqslant b$.
19. 证明：如果 $a$ 和 $b$ 是整数且满足 $a \mid b$，则对任意正整数 $k$，有 $a^k \mid b^k$.
20. 证明两个偶数或两个奇数的和是偶数，而一个奇数和一个偶数的和是奇数.
21. 证明两个奇数的积是奇数，而如果两个整数中有一个为偶数，则这两个整数的积是偶数.
22. 证明：如果 $a$ 和 $b$ 是正奇数且 $b \nmid a$，则存在整数 $s$ 和 $t$ 使得 $a=bs+t$，其中 $t$ 是奇数，且 $|t|<b$.
23. 当整数 $a$ 被整数 $b$ 除时，其中 $b>0$，带余除法给出一个商 $q$ 和一个余数 $r$. 证明：如果 $b \nmid a$，则当 $-a$ 被 $b$ 除时，带余除法给出商为 $-(q+1)$，余数为 $b-r_j$，而如果 $b \mid a$，则商为 $-q$，余数为 0.
24. 证明：如果 $a$，$b$ 和 $c$ 为整数，$b>0$，$c>0$，使得当 $a$ 被 $b$ 除时商为 $q$，余数为 $r$，且 $q$ 被 $c$ 除的商为 $t$，余数为 $s$，则当 $a$ 被 $bc$ 除时，商为 $t$，余数为 $bs+r$.

25. a) 通过允许除数为负来扩展带余除法. 特别地，证明当 $a$ 和 $b\neq 0$ 为整数时，存在唯一的整数 $q$ 和 $r$ 使得 $a=bq+r$，其中 $0\leqslant r<|b|$.

b) 求 17 除以 $-7$ 的余数.

☞ 26. 证明：如果 $a$ 和 $b$ 为正整数，则存在唯一整数 $q$ 和 $r$ 使得 $a=bq+r$，其中 $-b/2\leqslant r\leqslant b/2$. 这个结果被称作**改良型带余除法**(modified division algorithm).

27. 证明：如果 $m$ 和 $n>0$ 为整数，则

$$\left[\frac{m+1}{n}\right]=\begin{cases}\left[\dfrac{m}{n}\right] & \text{如果对某整数 } k,\text{有 } m\neq kn-1;\\ \left[\dfrac{m}{n}\right]+1 & \text{如果对某整数 } k,\text{有 } m=kn-1.\end{cases}$$

28. 证明整数 $n$ 为偶数当且仅当 $n-2[n/2]=0$.

29. 证明小于等于 $x$ 且能够被正整数 $d$ 整除的正整数个数等于 $[x/d]$，其中 $x$ 为正实数.

30. 求不超过 1000 且能够被 5，25，125 和 625 整除的正整数个数.

31. 在 100 和 1000 之间有多少整数能够被 7 整除？被 49 整除？

32. 求不超过 1000 且不能被 3 或 5 整除的正整数个数.

33. 求不超过 1000 且不能被 3，5 或 7 整除的正整数个数.

34. 求不超过 1000 且能够被 3 整除但不能被 4 整除的正整数个数.

35. 2010 年年初，在美国邮寄一封一等信件，一盎司内需花费 44 美分，而后每增加一盎司(不足也按一盎司计)，需要多花费 17 美分. 求一个用最大整数函数来表示的 2010 年年初的邮资的公式. 在 2010 年年初的美国是否可能花费 1.81 美元或 2.65 美元来邮寄一封一等信件？

36. 证明：如果 $a$ 为整数，则 3 整除 $a^3-a$.

37. 证明两个形如 $4k+1$ 的整数之积仍然是这种形式，而两个形如 $4k+3$ 的整数的积的形式为 $4k+1$.

38. 证明每个奇数的平方都形如 $8k+1$.

39. 证明每个奇数的四次方都形如 $16k+1$.

40. 证明两个形如 $6k+5$ 的整数的积形如 $6k+1$.

41. 证明任意三个连续的整数的积都能被 6 整除.

42. 用数学归纳法证明对任意正整数 $n$，$n^5-n$ 可以被 5 整除.

43. 用数学归纳法证明三个连续的整数的立方和能够被 9 整除.

在习题 44～48 中，$f_n$ 表示第 $n$ 个斐波那契数.

44. 证明 $f_n$ 为偶数当且仅当 $n$ 可被 3 整除.

45. 证明 $f_n$ 能被 3 整除当且仅当 $n$ 可被 4 整除.

46. 证明 $f_n$ 能被 4 整除当且仅当 $n$ 可被 6 整除.

47. 证明当 $n$ 为满足 $n>5$ 的正整数时，$f_n=5f_{n-4}+3f_{n-5}$. 应用这个结果证明当 $n$ 能被 5 整除时，$f_n$ 能被 5 整除.

* 48. 证明当 $m$ 和 $n$ 为正整数，且 $m>1$ 时，$f_{n+m}=f_m f_{n+1}+f_{m-1}f_n$. 应用这个结果证明当 $m$ 和 $n$ 为正整数且满足 $n\mid m$ 时 $f_n\mid f_m$.

设 $n$ 为正整数，我们定义

$$T(n)=\begin{cases}n/2 & \text{如果 } n \text{ 为偶数;}\\ (3n+1)/2 & \text{如果 } n \text{ 为奇数.}\end{cases}$$

则可以通过迭代 $T$ 来得到一个序列：$n$，$T(n)$，$T(T(n))$，$T(T(T(n)))$，…. 例如，从 $n=7$ 开始，我们得到 7，11，17，26，13，20，10，5，8，4，2，1，2，1，2，1，…. 一个著名的猜想(有时被称为 Collatz 猜想)宣称无论由哪个正整数 $n$ 开始，由迭代 $T$ 得到的序列总是会达到整数 1.

49. 求从 $n=39$ 开始通过迭代 $T$ 所得到的序列.

50. 证明从 $n=(2^{2k}-1)/3$ 开始通过迭代 $T$ 所得到的序列总是会达到整数 1，其中 $k$ 为大于 1 的正整数.

51. 证明：如果可以证明对于任意整数 $n$，$n\geqslant 2$，在通过迭代 $T$ 得到的序列中总存在一项小于 $n$，那么 Collatz猜想为真.

52. 验证对于所有满足 $2\leqslant n\leqslant 100$ 的正整数 $n$，由正整数 $n$ 开始，通过迭代 $T$ 得到的序列中存在一项小于 $n$.（提示：从容易证明这个结论正确的正整数集合开始考虑.）

* 53. 证明：当 $n$ 为非负整数时，$[(2+\sqrt{3})^n]$为奇数.

* 54. 确定满足$[a/2]+[a/3]+[a/5]=a$ 的正整数 $n$ 的个数，其中$[x]$是通常的最大整数函数.

55. 用第二数学归纳原理证明带余除法.

### 计算和研究

1. 求 111 111 111 111 被 987 654 321 除所得的商和余数.

2. 对于不超过 10 000 的所有整数 $n$，验证习题 49 前的导言中描述的 Collatz 猜想.

3. 考察一些数据，对于在迭代 $T(n)$得到的序列达到 1 之前所需的迭代步数，你能做出什么样的猜测？其中 $n$ 为给定的正整数.

4. 考察一些数据，推导出关于斐波那契数对于 7，8，9，11 和 13 等数的可除性的猜测.

### 程序设计

1. 确定一个整数是否能被一个给定的整数整除.

2. 求带余除法中的商和余数.

3. 求在习题 26 中给出的特殊带余除法中的商、余数和符号.

4. 对给定的正整数 $n$，计算习题 49 前的导言中定义的序列 $n$，$T(n)$，$T(T(n))$，$T(T(T(n)))$，…中的项.