所有你一直想知道的数学知识*

(但是甚至不知道要问)

一次引导进入抽象数学世界和证明写作之旅

布伦丹·W·沙利文
bwsulliv@andrew.cmu.edu
与约翰·麦基教授

数学科学系 卡内基梅隆大学 匹兹堡
，宾夕法尼亚州

2013年5月10日

This work is submitted in partial fulfillment of the requirements for the degree of Doctor of Arts in Mathematical Sciences.

Contents

Part I

Learning to Think Mathematically

Chapter 1

What Is Mathematics?

1.1 Truths and Proofs

您如何知道某事是真是假？当然，你肯定被告知过，例如，三角形的角之和为180°，但你是如何确信无疑的呢？如果你遇到了一个从未学习过基本几何的外星人呢？你如何向他/她/它证明这个事实是真实的呢？从某种意义上说，这就是数学的本质：制定新的陈述，以某种方式判断它们是对是错，并向其他人（或者外星人，视情况而定）解释这些发现。不幸的是，似乎很多人认为数学家整天都在做的是将大数相乘；然而，实际上，数学是一门比其广泛认知的更复杂算术角色更具创造性和写作基础的学科。这本书的一个目标就是让你相信这个事实，但这仅仅是一个额外的好处。这本书的主要目标是向你展示数学思维、问题解决和证明写作的真正内容，向你展示如何做这些事情，以及这些事情有多么有趣！

作为旁注，你可能甚至会想，“什么是真实的东西意味着什么？”对这个问题的全面讨论将涉及哲学、心理学，也许还有语言学，而我们并不真的想深入那个领域。然而，在数学的背景下，主要思想是{v*}。我们知道1 {v*} 1 {v*} 2始终如一。无论它是午夜还是中午，我们都可以放心，这个等式将始终成立。（你有没有想过如何证明这样一个事实？这实际上相当困难！一本名为{v*} {v*} 的书从“第一原理”开始这样做，作者们需要许多许多页才能到达1 {v*} 1 {v*} 2！）这与其他科学，也许，大不相同。如果我们进行10次物理实验并且得到相同的结果，我们是否知道这将会{v*}发生？如果我们做这个实验一百万次呢？十亿次呢？我们实际上在什么时候{v*}了什么？在数学中，重复实验不是有效的证明！我们需要

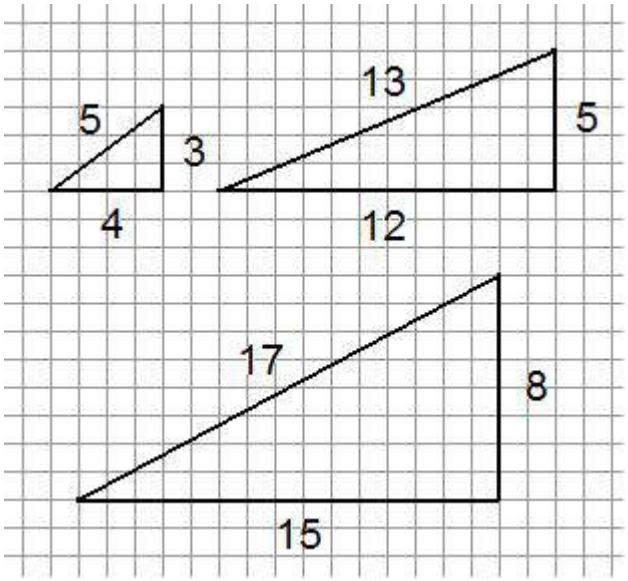
找到一个论证来说明为什么这种现象会发生 *always*。例如，数学中有一个著名的未解问题，称为 *Goldbach Conjecture*。到目前为止，尚不清楚它是否为真，尽管它已经被计算机模拟验证到大约 10^{18} 的值。这是一个 *huge* 数，但它仍然不足以知道猜想是 True 还是 False。你看到区别了吗？我们数学家喜欢 *prove* 事实，而检查一大堆值但不是 *all* 的它们并不能构成证明 *not*。

1.1.1 Triangle Tangle

我们通过讨论我们希望证明能完成的事情以及为什么我们会如此关注它们，引入了**proof**的概念。那么，你可能想知道，一个人如何*define*一个证明。这实际上是一个难以解决的问题！为了接近这个想法，我们将提出几个不同的数学论证。我们希望你能跟随它们阅读，并思考它们是否具有说服力。它们*prove*了什么？它们正确吗？它们容易理解吗？它们让你有什么感觉？自己思考它们，形成一些观点，然后跟随我们的讨论阅读。

这里我们将要提出的数学论证都是关于三角形的。具体来说，它们涉及**Pythagorean Theorem.**

Theorem 1.1.1 (勾股定理)**.** *If a right triangle has base lengths a, b and hypotenuse length c, then these values satisfy $a^2 + b^2 = c^2$.*



我们如何知道这一点？这是一个非常有用的事实，你可能在你的数学课上（甚至在生活中，甚至没有意识到）多次使用过。

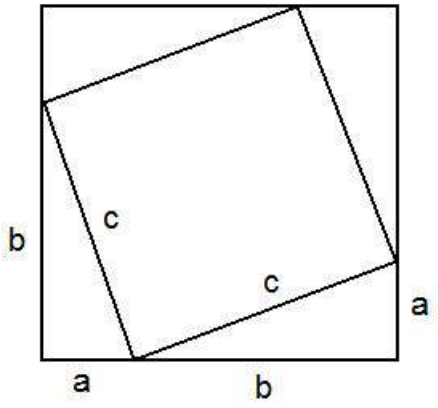
你有没有想过为什么这是真的？你将如何向一个怀疑的朋友解释？这正是**mathematical proof**努力实现的目标：对一个事实的清晰简洁的解释。要求证明背后的推理也很有道理，并且是双重的：知道我们认为是真的确实是真的，这让人感到欣慰，而且每次我们想使用这个事实时，不必每次都解释它，这也很好。在证明了勾股定理（令人满意地）之后，我们只需在出现相关情况时提及定理的名称；我们已经完成了证明，所以没有必要再次证明。

现在，究竟什么是证明？我们如何知道一个解释是否足够清晰和简洁？回答这个问题通常相当困难，这也是为什么数学可以被视为一种艺术，而不仅仅是科学的一部分。我们处理的是冷酷、坚硬的事实，是的，但能够用这些事实进行推理并满意地向他人解释它们本身也是一种艺术形式。

Examples of "Proofs"

让我们看看一些样本"证明"并看看它们是否足够有效。（我们现在称之为"证明"，直到我们后来给出一个更精确的定义。）下面是第一个：

"Proof" 1. 画一个边长为 $a+b$ 的正方形。在这个正方形内，绘制四个直角三角形，形成一个边长为 c 的正方形，位于大正方形内部。



大正方形的面积可以通过两种方式计算：将面积公式应用于大正方形或加上小正方形的面积和四个三角形的面积。因此，必须成立{v*}

$$(a+b)^2 = c^2 + 4 \cdot \frac{ab}{2} = c^2 + 2ab$$

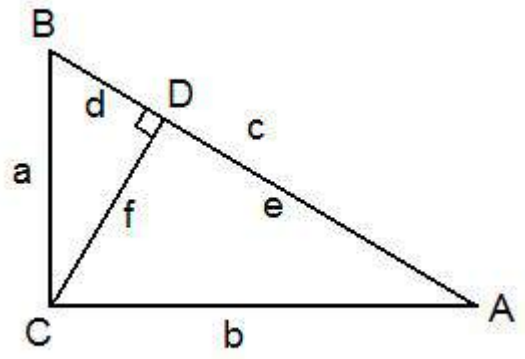
展开左侧的表达式并在两边消去一个公共项得到

$$a^2 + \cancel{2ab} + b^2 = c^2 + \cancel{2ab}$$

因此，$a^2 + b^2 = c^2$ 是正确的。 □

你信服了吗？每一步都合理吗？也许你还没有确定，那么让我们看看定理的另一个“证明”。

“Proof” 2. 假设勾股定理成立，并从对应直角的顶点画出高，如下图中所示，标记点和长度：



由于勾股定理成立，我们可以将其应用于图中所有的三个直角三角形，即 ABC, BCD, ACD。这告诉我们（定义 $e = c - d$）

$$a^2 = d^2 + f^2$$
$$b^2 = f^2 + e^2$$
$$c^2 = a^2 + b^2$$

将前两个方程相加，并用这个和替换第三个方程，我们得到

$$c^2 = d^2 + e^2 + 2f^2$$

注意，角度 $\angle ABC$ 和 $\angle ACD$ 相等，因为它们都是与角度 $\angle CAB$ 补角，所以我们知道三角形 $\triangle CDB$ 和 $\triangle ADC$ 是 *similar triangles*。(我们现在假设对平面几何有所了解。) 这告诉我们 $\frac{e}{f} = \frac{f}{d}$，因此 $f^2 = ed$。我们可以用这个来替换上面一行中的 f^2 并进行因式分解，如下所示：

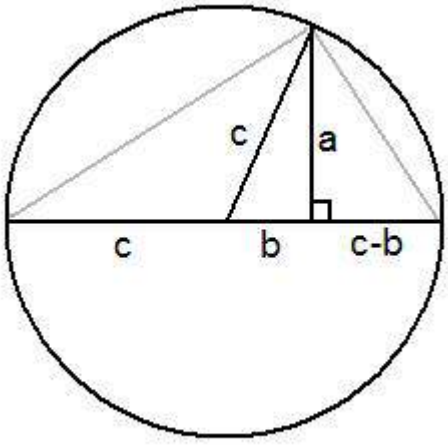
$$c^2 = d^2 + e^2 + 2de = (d + e)^2$$

两边取平方根（并且知道c, d, e都是正数）告诉我们$c = d + e$，根据长度d和e的定义，这是正确的。因此，我们关于勾股定理正确的假设是有效的。

□

这个证明怎么样？它有说服力吗？它清晰吗？在我们决定什么构成“正确”或“良好”的证明之前，让我们再考察一个“证明”。

“Proof” 3. 观察发现



因此$\frac{a}{c+b} = \frac{c-b}{a}$，从而 $a^2 + b^2 = c^2$。 □

这对你来说有意义吗？最后，这里有一个需要考虑的“证明”。

“Proof” 4. 勾股定理必须是正确的，否则我的老师一直在骗我。

□

Discussion

在继续阅读之前，我们鼓励您思考这四个“证明”，甚至与另一个学生或朋友讨论它们。您认为什么构成了一个“正确的”证明？清晰度和易读性重要吗？它会影响证明的“正确性”吗？

从历史角度来看，数学证明写作在多年中不断发展，关于什么是“正确”的证明有一个良好、普遍的共识：

- 每个证明中的 *step*，每个逻辑推理和主张，从数学角度来说，都是 *valid* 的重要。
- 也很重要，证明编写者要（合理地）说明一个陈述是如何从先前的工作或外部知识中得出的。

关于 $truth$ 要求的优点在于，数学已经被构建起来，我们可以阅读一个论点并验证每个主张是否为 True 或 False。难以定义的是 $clear$ 写作。从某种意义上说，它很像美国最高法院大法官波特·斯图尔特对淫秽的定义：“当我看到它时，我知道它”。

给定这四个比较论点，让我们评估它们的清晰度和正确性：

Clarity:

- “证明”1和2解释得相当清楚。有关于作者在做什么以及为什么做的明确陈述。它们指出了任何方程的来源，甚至包括一些图片来向读者说明他们的想法。

  注意，“证明1”确实依赖于一些基本先验知识，如变量的代数操作和三角形、正方形的面积公式，但这没关系。

  同样，“证明2”依赖于对相似三角形的理解以及这对其边长意味着什么。至少证明的作者指出了这一点，所以感兴趣的读者可以查找一些相关想法。如果他们没有说这一点，读者可能会感到困惑，不知道他们缺少什么！

- “证明”3表述非常糟糕！它根本没有任何解释。这使得很难确定他们的说法是否实际上正确。是的，包括了一张图片，但没有说明他们为什么选择围绕三角形画圆，或者为什么所说的方程式从图中得出。

- “证明”4是一个语法正确的英语句子，但它没有任何$ex\text{-}\ plain$!

已经，我们可以看到“证明”4无疑是成为一个良好且适当的$proof$的可行候选人。“证明”1和2仍在竞争中，因为它们至少是清晰书写的。“证明”3按照现在的写法，可能不是一个好的候选人；然而，也许它确实包含了一些正确但需要更好解释的想法。也许它可以被改写为一个良好且适当的$proof$。

让我们分析这四个论点的逻辑正确性：

Correctness:

- “证明”1大部分良好。正方形和三角形的面积公式应用正确，相应的代数操作也正确。但我们如何知道他们描述的过程——将给定的三角形放入一个更大的正方形内，四份——在内部创建了一个边长为c的正方形？他们只是这样说了$does$，所以没有

实际上说的是 why。尽管如此，这个证明既写得很好，又正确无误。

(你能证明这个事实吗，里面的形状实际上是一个正方形？只需看看它的角度：你能说明为什么它们都是 $right$ 角吗？)

- 很遗憾，“证明”2 完全无效！它所进行的每一个逻辑步骤都确实是从前一步推导出来的。例如，假设我们以这种方式建立了三角形，我们可以正确地推断出 ΔCDB 和 ΔADC 是相似三角形。然而，为什么我们一开始就能 $assume$ 该定理是 True 呢？难道这不是我们试图在证明中实现的目标吗？这是一个关键的缺陷。**Assuming a fact and deducing something True from it does *not* allow us to conclude the original assumption was valid.**

  如果这种方法有效，我们就可以“证明”我们想要的几乎所有事情！以下是一个例子：你认为以下证明 $0 = 1$ 的方法怎么样？

  “Proof”. 假设 $0 = 1$。然后，根据 $=$ 的对称性质，$1 = 0$ 也成立。将这两个方程相加告诉我们 $1 = 1$，这是 True。因此，$0 = 1$ 是一个有效的假设，所以它必须是 True。 □

  您是否看到这与上面“证明”2之间的相似性？使用了相同类型的错误推理：我们假设了一个事实，做了一些工作以得到我们知道是 True 的其他东西，然后说假设的事实必须是 True，同样。

- 关于“证明”3，大多数数学家会说这是一个“糟糕的证明”，尽管它似乎声称的一切都是正确的。我们说“似乎”，因为没有任何文字来解释正在发生的事情，我们实际上并不知道证明作者试图说什么！然而，我们将说一个完美的证明的核心包含在其中。

  从图中，你可以证明所给的方程 $\frac{a}{c+b} = \frac{c-b}{a}$ 必须成立。（提示：使用相似三角形！）从那里，通过简单的操作可以推导出 $a^2 + b^2 = c^2$。

  你能写一些与图表相符的句子，使这成为一个完整的证明吗？

- 最后，几乎所有合乎逻辑的合理人（我们希望如此！）都会说，“证明”4甚至不能算是一个证明，尽管这样说可能很方便。

这个讨论表明，“证明”1 实际上是一个很好的证明。在所有四个中，它写得最清楚，也是逻辑正确的。现在我们可以将其称为 **proof**。“证明”2 虽然表述清晰，但完全是错误的。“证明”3 包含了正确想法，但表述不清。“证明”4 与证明相去甚远，我们甚至不想讨论它。

Question

在继续其他主题之前，我们先给你一个问题：如果我们给你三个满足 $a^2+b^2=c^2$ 的正数 a, b, c，是否必然存在一个边长为 a, b 和斜边长度为 c 的直角三角形？如果是这样，你将如何构建它？如果不是，为什么不是？

1.1.2 Prime Time

当我们在讨论证明时，让我们看看另一个证明，针对不同的定理。作为提醒（或简要介绍），让我们谈谈 *prime numbers*。

Definition, Examples, and Uses

Definition 1.1.2. *A positive integer p that is larger than 1 is called a* **prime** *number if the only positive divisors of p are 1 and p. A non-prime positive integer is called a* **composite** *number.*

素数在数学的所有分支中都显示出了极其重要的作用，不仅在于对整数及其性质的研究，这被称为**number theory**。在所有数学中，最著名的**conjectures** (一个尚未被证明或证伪的定理的猜测)是*Riemann Hypothesis*。其结论已被证明与整数中素数的分布密切相关。关于这个主题已经写了许多书籍。此外，大多数现代密码方案都是基于将巨大的素数相乘，依赖于这样一个事实：给定它们的乘积，要撤销这个过程并找出两个巨大的素数因子相当困难。所以现在你知道了：每次你用信用卡在iTunes上购买歌曲时，某台计算机就只是将两个大素数相乘了！

前几个质数是2, 3, 5, 7, 11, 13, 17, 19, 23, . . . (记住，1不符合我们的定义)。有多少个质数？它们之间相隔多远？是否存在某种规律？回答这些问题既有趣又好玩，但也很困难（有时甚至不可能！）在这里，我们将回答其中一个问题：是否存在无穷多个质数？

Theorem and Proof

Theorem 1.1.3 (无穷的素数)**.** *There are infinitely-many prime numbers.*

"Proof". 假设只有有限个素数，并将它们按升序列出：$p_1, p_2, p_3, \ldots, p_k$，使得 p_k是这些素数中最大的。定义新的数字

$$N = (p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k) + 1$$

它必须是真的，N能被某个质数整除。然而，它不能被p_1或p_2或...或p_k整除，因为那样会留下余数1,

基于我们如何定义 N。因此，N 可以被列表中的某个其他质数整除，该质数是 *not*。

如果 N 本身是合数（即不是素数），那么我们就找到了一些新的素数 $p < N$，这些素数不在我们可能拥有的 *all* 素数列表中。如果 N 本身是素数，那么我们就找到了一个新的素数 $N > p_k$，因此 p_k 实际上不是最大的素数。无论如何，我们都保证有一个新的素数不在给定的 k 素数列表中。因此，必须有无穷多个素数。 □

你觉得这个“证明”怎么样？你信服了吗？它似乎与我们之前看到的论点有点不同，不是吗？试着向同学解释一下这个证明与上一节中勾股定理的“证明1”有何不同。虽然如此，我们将揭示这一点：这里的“证明”实际上是一个完全正确的 *proof*，不带引号！

1.1.3 Irrational Irreverence

让我们谈谈一种不同类型的数字，现在：**rational**数字。你可能知道有理数被称为“分数”、“商”或“比率”。

Definition and Examples

这里是对 *rational* 个数的精确定义：

Definition 1.1.4. *A real number r is a* **rational** *number if and only if it can be expressed as a ratio of two integers $r = \frac{a}{b}$, where a and b are both integers (and $b \neq 0$).*

A real number that is not rational is called **irrational**.

此定义并未说明有理数必须只有一个这样的表示；它仅仅要求有理数至少有一个这样的表示。例如，1.5是有理数，因为$1.5 = \frac{3}{2} = \frac{12}{8} = \frac{30}{20}$等等。不是有理数的实数称为**irrational**数，这就是整个定义：*not*有理，即该数不能表示为整数的比。你可能知道$\sqrt{2}$是无理数，但你如何*prove*这样的事情？自己试试。我们实际上会在稍后重新审视这个问题（参见例4.9.4）。你可能已经知道的其他无理数包括e, π, φ和$\sqrt{n}$，其中n是任何不是完全平方的正整数。

Questions

给定这个有理/无理的定义，我们可能会想知道我们如何将无理数结合起来得到一个有理数。试着独立回答以下问题。如果你的答案是“是”，试着找一个例子，如果你的答案是“否”，试着解释为什么期望的情况不可能发生。

(1) 是否存在无理数 a 和 b，使得 $a \cdot b$ 是有理数？

(2) 是 存在不合理的数 a 和 b，使得 $a+b$ 是一个有理数 al 编号?

(3) 是否存在无理数 a 和 b，使得 a^b 是有理数?

你找到了任何例子吗？结果是，所有三个问题的答案都是“是”！前两个问题不太难想出来，但第三个问题有点棘手。

这里，我们将通过一个证明来说明第三个问题的答案是“是”。然而，有趣的是，我们实际上不会找到使 a 成为有理数的确定数字 b 和 a^b；我们只会将其缩小到两种可能的选择，并展示其中一种选择 $must$ 是可行的。听起来很有趣，对吧？让我们试试。

Proof. 我们知道 $\sqrt{2}$ 是一个无理数。考虑数字 $x=\sqrt{2}$ $\sqrt{2}$.
有两种可能性需要考虑:

- 如果 x 是有理数，那么我们可以选择 $a=\sqrt{\wedge}2$ 和 $b=\sqrt{\wedge}2$，并得到我们的答案。
- 然而，如果 x 是无理数，那么我们可以选择 $a=\sqrt{2}^{\sqrt{2}}$ 和 $b=\sqrt{2}$，因为那时

$$a^b=\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}=\left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}}=\left(\sqrt{2}\right)^2=2$$

  2 是一个有理数。

在任何情况下，我们都可以找到无理数 a 和 b，使得 a^b 是一个有理数。因此，这样的一对数字必须存在。 □

你对这个证明有什么看法？它有说服力吗？它以上面的第三个问题给出了一个明确的“是”，但它并没有告诉我们 $which$ 对 a,b 实际上是正确的，而只是说其中一对会起作用。（结果发现 $\sqrt{2}^{\sqrt{2}}$ 也是无理数，但证明这个事实需要更多的工作。）

有许多其他具体的例子可以回答这个问题，尽管如此。你能想出任何吗？（提示：尝试使用 $\log_{10}$ 函数...）

1.2 Exposition Exhibition

1.2.1 Simply Symbols

Mathematics is a Language

尽管表面上看（以及一些内容繁多的教科书），数学不仅仅是我们在纸上推来推去的符号集合。英语语言基于一组固定的符号（字母表中的26个字母加上常见的标点符号，如句号、逗号和括号），但我们以特定的方式将这些符号组合在一起，同时遵循一些标准

协议的惯例，以创造有意义的词语、短语、句子、段落等；本质上，英语，就像任何语言一样，是通过一组符号及其符号的规则集合来传达意义的一种方式。同样的概念也适用于 *language of mathematics*：存在一组符号和一套应用于这些符号的规则。

一个区别是，我们用于数学中的符号集合可能相当大，这取决于当前正在讨论的数学分支。数学的结构灵活性很大一部分在于我们总能创建和定义新的符号来使用。很多时候，这样做甚至是为了使事物更简短、更容易阅读。

另一个数学与其他语言的主要区别在于我们精心选择如何*define*我们的词汇以及它们所代表的概念。通常，数学家们的大部分争论都围绕着定义。这可能让你感到惊讶；也许你会认为数学家们争论的是证明和猜想更有意义，或者也许这是一个新颖的想法，即数学家们甚至还会争论！为新发现的概念选择正确的定义和术语是数学发现和表述的关键组成部分，因为它有助于发现者/发明者向其他感兴趣的人解释他的/她的想法。（如果没有这个过程，数学就不会进步，只会有一群人试图独自发现真理。）

情况与口语相似，但似乎不那么极端。例如，如果你对你的朋友说，“我饿了”，或者“我有点饿”，或者“哦我的天，我快要饿死了”，他们听到的基本上是同样的信息，并且会以大致相同的方式回应。然而，在数学中，我们的定义要精确得多，并且不包含口语所允许的那种细微差别。当然，这两种哲学都有利弊，但在数学中，我们尽可能追求精确性，所以我们喜欢我们的定义要准确无误。然而，尽管如此，我们控制着这些定义的内容！这就是为什么在数学界，关于定义的辩论如此普遍：为手头概念选择正确的定义可以使未来对这些概念的工作更加容易和方便。

Choosing Definitions Properly

作为一个具体例子，让我们回到前一小节中看到的*prime number*的定义1.1.2。它说：

Definition. *A positive integer p that is larger than 1 is called a* **prime** *number if the only positive divisors of p are* 1 *and p. A non-prime positive integer is called a* **composite** *number.*

这里对这个定义似乎没有什么可疑之处，是吗？也许你会用不同的措辞，或者更加简洁，或者使用不同的变量字母，等等，但最终的信息会是相同的：素数是一定类型的数，具有某种特性

属性。然而，无论你如何写出那种特定类型的数（一个大于1的正整数）以及那个属性（除了它自己和1之外没有正除数），你都会得到一个等效的定义。

存在这个定义背后的某些微妙问题：为什么是那种特定类型的数字？为什么我们如此关注那个特定属性——只能被1和它本身整除——呢？如果定义稍有不同会怎样？事情真的会改变很多吗？我们将用另一个问题来回答这些问题：你认为以下关于素数的替代定义怎么样？

Definition 1.2.1. *An integer p that is less than -1 or greater than 1 is called a* 原点 *number if the only positive divisors of p are 1 and p.*

你注意到细微的差别了吗？所有符合“素数”之前定义的数字仍然符合这个定义，但现在负数也符合了！具体来说，给定任何在旧定义下是素数的数字 p，现在在新的定义下也是素数。这是一个合理的想法吗？负素数有什么问题？

关于这个素数的第三个定义怎么样？

Definition 1.2.2. *A positive integer p is called a* 素数 *number if the only positive divisors of p are 1 and p.*

(记住，0既不是正数也不是负数，这是惯例。) 现在，负数超出了范围，但1符合这个定义。这合理吗？1的唯一正除数是1和...本身，对吧？

这可能是一个有争议的地方：你可能不介意将1视为一个质数，但你的朋友却强烈反对。好吧，无论哪一方都没有充分的理由，都无法说你们中的任何一方是 *wrong*，实际上；你们只是对术语的选择不同，而且它们都没有改变1的唯一正除数是1和它本身的固有属性。作为一个类似的想法，考虑这一点：无论你称它们为凉鞋、拖鞋还是人字拖，事实仍然是这些类型的鞋子是海滩上合适的鞋子。

从历史的角度回顾，并考虑到新的愿望，但往往有一个特定的定义被证明更为合适。在未来，我们将探讨 **prime factorizations**，一种将每个（正）整数仅表示为质数乘积的方法。例如，$15 = 3 \cdot 5$ 和 $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ 以及 $14285 = 3^3 \cdot 11 \cdot 13 \cdot 37$ 都是质因数分解。

这些分解也有一个特殊性质：一般来说，一个正整数的素数分解是 **unique**！也就是说，将一个正整数写成素数乘积的方式只有一种（因为我们认为因子的不同排列是相同的东西，所以 $105 = 3 \cdot 5 \cdot 7$ 和 $105 = 7 \cdot 3 \cdot 5$ 是相同的分解）。这是我们将会严格使用上面给出的第一个定义来证明的。如果我们使用第二个定义，或者第三个定义呢？这个唯一性性质是否仍然成立？为什么你认为这个唯一性性质如此重要？最终，这里的教训是

定义应由逻辑和实用性共同驱动，并且这可能会随时间而变化，引发一些争议。

Mathematicians Study Patterns

另一个明确和精确定义的好处是作为思考者所获得的知识和理解；建立逻辑基础对未来可能会有所帮助。人类学习的一个重要方面是通过日常经验识别模式，然后将想法、概念、词语和事件与这些模式联系起来。然后，一个人可以使用这些模式来预测和理论化关于抽象想法、概念和事件。

例如，已经研究和证明人类婴儿最初缺乏，但随着时间的推移会发展出*object permanence*的概念。如果你向一个孩子展示一个他们微笑并喜欢的彩色玩具，然后把它藏在纸箱下面，孩子并不完全理解玩具仍然存在，只是看不见了。他/她会表现得好像这个物体不再存在。然而，在某个时候，我们了解到这并不真实，并且我们视野之外的对象仍然存在。这究竟是如何发生的呢？也许我们认识到许多此类事件中物体“消失”然后我们后来又找到它的模式。

更好的例子可以在自然科学中找到，它们展示了模式识别和抽象思维的一个额外方面，这在数学和科学中尤为重要。人们可以想象，尼安德特人可能以某种方式知道，每次他们拿起一块石头，将其伸直手臂并放手，石头就会落到地上。这种情况可能反复发生，所以他们“理解”这种现象是自然的一个必然产物。在足够多的发生之后，他们可能理解这总会发生，或者至少，任何没有发生的情况都会引起极大的困惑和恐惧。（正是这种情绪反应可能有助于解释为什么火山爆发等不常见但强大的事件导致古代文明将这些事件归咎于“愤怒的神明”）。

这些对事件的观察并没有让这些史前人类更接近理解*why*石头总是会落到地上，或者能够*explain*为什么它每次都会发生。在许多个千年之后，人们才开始思考为什么以及如何发生这种现象，而在艾萨克·牛顿最终提出一个试图解释重力行为（最终被赋予这种现象的名字）的模型之前，还要更长的时间。即使现在，有些人说，我们仍然没有确切地弄清楚它是如何工作的。（上网谷歌“环量子引力”，如果你好奇的话，试着理解一下。）

这是从对模式的观察到一个模式的认识论理解中的抽象跳跃，这标志着真正的好奇和有思想的人，一个真正的**scientist**，在最好的意义上。你认为哪个昆虫学家更好：那个贪婪的读者，他已经记住了并能列出目前所知的所有甲虫种类的人

世界，或者那位检验过多种物种并能将新样本归类为甲虫或非甲虫的实验室科学家？这是一个有点引导性的问题，但主要观点是：了解一个定义及其背后的动机，远比仅仅知道满足某个定义的一堆*instances*更有益。

这可以说是数学中更为重要的部分。你能想象一个不知道素数是什么的数学家吗？但他却能仅凭记忆列出前100个素数，并且对此感到满足？当然不能！数学研究的美丽、多功能性和吸引力之一在于，我们研究模式和现象，然后选择如何为这些模式制定适当的定义。然后，我们利用对这些模式的新理解，对其他模式和现象做出严格精确的预测。彻底理解一个定义或概念可以增强预测能力，这比仅仅知道该定义/概念的一些例子要有效得多。

1.2.2 Write Right

另一个有趣的数学方面是，尽管它本身是一种语言，但我们仍然依赖于外部语言来表达我们所拥有的数学思想和洞察。尝试用任何我们之前看过的定义和证明来重写，而不使用任何词语。这很难，不是吗？因此，我们希望我们用来传达数学思想的书面语言遵循与我们对所写的数学“句子”应用的标准相同：我们希望它们是 *precise*，*logical* 和 *clear*。

现在，为这三个词中的每一个制定一个精确、逻辑和清晰的定义本身是一项艰巨的任务。然而，我们可以一致认为，一个证明应该是：

- **precise:** 每个个体陈述都不应是不真实的或可以有多种解释，从而使得真相变得可疑；
- **logical:** 每一步都应该从前一步中合理地推导出来，并附有适当的动机和解释；并且，
- **clear:** 步骤应连接并使用正确的英语语法和用法进行描述，帮助读者了解正在发生的情况。

让我们考察几个忽视这些标准并且 somehow 无法符合我们迄今为止所定义的 *proof* 的“证明”。

Bad “Proof” #1

首先，我们有一个“证明”1=2，因此我们知道这个肯定有问题。你能找到错误吗？它违反了哪个标准？精度、逻辑还是清晰度？

"Proof". 假设我们有两个实数 x 和 y，并考虑以下等式链：

$$\begin{aligned} x &= y \\ x2 &= xy \text{ 两边同时乘以 } x \\ x^2 - y^2 &= xy - y^2 \text{ 从两边减去 } y^2 \\ (x+y)(x-y) &= y(x-y) \text{ 两边同时因式分解} \\ x + y &= y \text{ 消去 } (x-y) \text{ 两边} \\ y + y &= y \text{ 记住 } x = y, \text{ 从第一行} \\ 2y &= y \\ 2 &= 1 \text{ 两边同时除以 } y \end{aligned}$$

□

这里的问题是 *precision*。在第四行进行因式分解后，似乎方便且明智地除以公因数（$x - y$）以获得第五行；然而，第一行告诉我们 $x = y$ 因此 $x - y = 0$，并且 **division by zero is not allowed**！使用变量 x 和 y 只是为了让你偏离线索并伪装除以零。（说到这个话题，为什么除以零是不允许的？你能想到一个合理的解释吗？从乘法的角度来考虑。）

Bad "Proof" #2

这是另一个类似"事实"的证明，即$0 = 36$。

"Proof". 考虑方程 $x^2 + y^2 = 25$。重新排列以隔离 x 告诉我们

$$x = \sqrt{25 - y^2}$$

然后两边加3再平方得到

$$(x+3)^2 = \left(3 + \sqrt{25 - y^2}\right)^2$$

注意，$x = -3$ 和 $y = 4$ 是原始方程的解，因此最终方程也应该成立。将这些值代入 x 和 y 告诉我们

$$0 = (-3+3)^2 = \left(3 + \sqrt{25-16}\right)^2 = (3+3)^2 = 36$$

因此，$0 = 36$。 □

这里发生了什么？你能找出这个不合理的步骤吗？也许如果我们用变量的具体值重新写出证明的步骤会有帮助

x 并且我们在结尾处选择的 y:

$$\begin{aligned}(-3)^2 + 4^2 &= 25\\ -3 &= \sqrt{25 - 4^2}\\ (-3+3)^2 &= \left(3 + \sqrt{25-4^2}\right)^2\\ 0 &= 36\end{aligned}$$

现在很明显，不是吗？在等式的两边应用平方根运算存在问题，并且它依赖于$(-x)^2 = x^2$这一事实。

当我们试图解一个如 $z^2 = x^2$ 的方程时，我们必须记住这个方程有两个根：$z = -x$ 和 $z = x$。因此，从一个方程开始，对两边进行平方是完全合乎逻辑的一步（结果方程 *follows* 的真实性源于原始方程的真实性），但反过来操作则是不合逻辑的（平方方程的真实性并不能告诉我们开平方的方程也是真实的）。这是 **conditional statements** 或 **logical implications** 的问题，我们将在后面详细讨论（在第 4.5.3 节）。现在，我们可以用以下这句话来概括这个想法:

$$\text{If } a = b \text{ then } a^2 = b^2, \text{ but if } a^2 = b^2 \text{ then } a = b \text{ or } a = -b.$$

这表明为什么从 $x^2 + y^2 = 25$ 移动到 $x = \sqrt{25 - y^2}$ 在上面的“证明”中是一个不合逻辑的步骤：我们立即假设了一个特定的平方根选择，而实际上有两个可能的选择。如果我们选择了负平方根会怎样呢？尝试用第二步读作 $-x = \sqrt{25 - y^2}$ 重新编写证明，然后在最后使用相同的 x 和 y 值。会发生什么？如果你使用 $x = 3$ 和 $y = -4$ 呢？或者 $x = -5$ 和 $y = 0$ 呢？你能描述如何确定我们应该使用正根 x 和负根 $-x$ 吗?

Mathematics Uses the “Inclusive Or”

自这个词刚刚出现，让我们提及上面句子中 *or* 的用法。当我们说“$a = b$ 或 $a = -b$”，我们指的是两个陈述中的一个是真的，可能两个都是真的。现在，如果 $a \neq 0$ 和 $b \neq 0$，那么只有结论中的一个可以是真实的；也就是说，在那个上下文中，只有根（正或负）中的一个将是正确的，而不是两个。然而，如果 $b = 0$，那么两个结论都说了同样的事情，$a = 0$，因此，规定 *or* 只意味着一个陈述可以是真实的，不允许它们同时都是真实的，这是不合理的。在其他情况下，这种区别会产生更明显的差异。

例如，如果你在餐馆点了一份三明治，服务员问：“你想要薯条还是土豆沙拉作为配菜？”这表示你可以选择这两种选项之一，但不能两者都要。这是一个 **exclusive *or*** 的例子，因为

它排除了你选择两个选项。或者，如果你忘记带笔到课堂上，正在寻找任何旧方法来记笔记并问你的朋友，“你有我可以借的铅笔或钢笔吗？”，那么可以理解你真的不在乎提供的两个选项中的哪一个，只要至少有一个可用。也许你的朋友两者都有，任何一个都行。这是一个**inclusive *or***的例子，这也是所有数学例子中假设的解释。

Unclear Arguments

最后两个糟糕的“证明”失败是因为精度和逻辑正确性问题。我们对一个好的证明的第三个要求是它必须是 *clear*：我们希望写作能够解释证明者在每一步中完成了什么，以及为什么这个成就是相关的。换句话说，我们不希望读者在任何地方停下来问，“这句话是什么意思？”或者“这从哪里来的？”或者类似的问题，这些问题源于困惑。如果有帮助，想想用向你的同学解释证明的方式去写证明，或者阅读你的作业的评分者，或者一个具有相似智力水平的家庭成员。重新阅读你自己的写作，并尝试预测可能出现的任何问题或可能向你提出的任何澄清，然后通过重写来解决这些问题。

有几种方式可能导致证明不满足这个条件，显得不清楚。首先，单词和句子可能无法正确解释证明的步骤和动机，这实际上可能是因为单词太多（通过让读者负担过重而使证明变得模糊）或因为单词太少（没有给读者提供足够的信息来处理）或因为选用的单词令人困惑（没有正确解释证明）。这些都是证明的 *language* 的问题。

数学上，可能会出现许多问题，尤其是在清晰度方面。也许证明作者突然引入一个变量，但没有说明它是什么类型的数（整数、实数等），或者跳过了一些算术/代数步骤，或者在没有先定义其含义的情况下使用新的符号，或者...这些行为在技术上并不错误或不合逻辑，但它们确实可能会让读者感到困惑。你能想到其他证明可能不清楚的方式吗？试着想出一个基于语言的一个和一个数学的。

Bad “Proof” #3

让我们陈述一个关于多项式函数的简单事实，然后考察关于该事实的一个“证明”。仔细阅读论点，并尝试找出一些句子或数学步骤是 *unclear*。

Fact: 考虑多项式函数 $f(x) = x^4 - 8x^2 + 16$。此函数对于任何 x 的值都满足 $f(x) \geq 0$。

“Proof”. 无论我们将什么值插入到 x 的函数 f 中，我们都可以通过因式分解多项式来写出函数输出的值，

像这样：

$$f(x) = x^4 - 8x^2 + 16 = (x-2)^2(x+2)^2$$

现在，任何数 z 必须小于 −^2，或者大于 2，或者严格介于 −^2 和 2 之间，或者等于它们中的一个。当 $z >$^2 时，z −^2 和 z +^2 都大于 0，所以 $f(z) >$ = 0 。当 $z <$ −^2 时，两个项都是负数，负数的平方是正数，所以 $f(z) >$ 也等于 0 。当 −^2 $< x <$^2 时，发生类似的情况，当 $x =$^2 或 $x =$ −^2 时，其中一个项是 0，所以 $f =$ = 0。因此，我们试图证明的东西必须是正确的。 □

在这份证明中有什么可以批评的地方？首先，它是正确的吗？它是精确的吗？逻辑的吗？清晰的吗？哪里不清楚？尝试识别那些哪怕稍微不清楚的语言和数学陈述，并尝试适当地修正它们。在不指出任何个别错误的情况下，我们下面提供了一个关于上述事实的更好、*clearer*证明。

Proof. 我们首先通过将其视为变量 x^2 中的二次函数来分解函数 $f(x)$。

$$f(x) = (x^2)^2 - 8x^2 + 16 = (x^2-4)^2$$

接下来，我们因式分解 x^2 −4= $(x$ +2$)(x$ −2$)$并重写原始f 函数作为

$$f(x) = \big((x+2)(x-2)\big)^2 = (x+2)^2(x-2)^2$$

现在，对于任何实数 x，$(x$ +^2$)^2 \geq \geqslant$ 0 和 $(x$ −^2$)^2 \geq \geqslant$ 0，因为平方的量总是非负的。两个非负项的乘积也是非负的，所以 $f(x) = (x$ +^2$)^2(x$ −^2$)^2 \geq \geqslant$ 0，对于 x 的任何值。 □

什么是第一个“证明”和这个第二个证明之间的区别？你重写的证明看起来也像这个第二个证明吗？

一个对第一个“证明”的批评是，它没有完全解释$-2 < x < 2$的情况；相反，它只是说发生了“类似”的事情，并没有实际执行任何细节。这在数学中是一个常见的情况（其中证明的一些步骤“留给读者”），这是一种有时可以避免繁琐的算术/代数，使阅读证明更容易、更快、更愉快的方便技术。然而，应该谨慎使用。作为一个证明者，确保这些步骤确实有效是很重要的，即使你不会在你的证明中展示它们；你应该考虑为读者提供一个简短的摘要或提示，说明这些步骤实际上是如何工作的。此外，证明者应尽量避免在证明最终结果至关重要的步骤上使用这种技术。

在这个特定情况下，因式分解的实际步骤被完全跳过，而关于 −^2 $< x <$^2 的情况只是简单提及，但这些是证明中的关键组成部分！无论如何，这个证明如此简短，展示这些步骤并不代表在简洁或清晰度上做出了巨大的牺牲。再次，这提出了证明写作作为一门艺术，就像是一门科学一样的问题：

选择何时将一些细节的验证留给读者可能很棘手。在这个特定情况下，展示所有步骤很重要。

尽管如此，我们在这里展示的第二个证明要清晰得多。此外，它完全避免了第一个“证明”中出现的案例分析！第一个“证明”中的一个案例存在清晰度问题，但与其在修订版本中简单地阐述细节，我们选择完全放弃那种技术，并使用更简短、更直接的证明。现在，这并不是说第一个证明的技术是错误的。如果我们填补第一个“证明”论点的空白，我们将得到一个完全正确的证明。然而，该技术中的一些步骤是多余的。请注意，当$-$^2 $< x <$^2和$x >$^2时的情况实际上是相同的，从某种意义上说：因子满足$(x -^{2})^2 >$^0和$(x +^{2})^2 >$^0在这两种情况下。事实上，这在第一个案例中也是正确的，其中$x < -$^2！那么为什么将这个论点分成三个单独的案例，当相同的最终观察适用于所有三个案例时？在这种情况下，最好将它们合并为一个（也利用当$x =$^2或$x = -$^2时，其中一个因子为0的知识）。再次强调，使用那种扩展技术当然不是错误的；相反，它只是给证明增加了一些不必要的长度。

我们上文提到了“案例”一词和“案例分析”这个短语，但没有对其定义或解释我们所说的意思。现在，我们想将这些术语的讨论推迟到第4章彻底讨论逻辑之后。尽管如此，如果你对这个问题迫不及待地想要得到满足，你可以跳到1.4.4节，查看“匈牙利朋友”问题，其中包含一些复杂的案例分析。

1.2.3 Pick Logic

我们已经多次使用“逻辑”这个词及其相关形式，而没有完全解释我们对其含义的理解。我们意识到这似乎与我们迄今为止一直强烈倡导的精确性和清晰度相矛盾，但我们也必须承认，不幸的是，为$logic$提供一个详尽的定义极其困难。

Games

如果您正在寻找对逻辑的合理启发式理解，尝试将其视为“逻辑谜题”如数独或卡库罗。这些谜题/游戏围绕非常具体的规则构建，这些规则从一开始就被确立并达成一致，然后解题者会得到一个起始板，并期望以严谨的方式应用这些规则，直到谜题被解决。例如，在数独中，记住每个数字从1到9必须在每个行、列和3×3个格子中恰好出现一次的条件，允许解题者系统地放置更多的数字在网格中，不断缩小大量可能的“解决方案”，以找到起始数字网格提供的唯一答案。这个解决过程中的一个重要方面是，在任何时候都不需要（或明智地）$guess$;

每个步骤都应该由当前情况和谜题的既定规则所指导的理性选择来引导，在这个框架内，谜题保证可解（当然，前提是有足够的时间）。

数学逻辑在某些方面略有不同，但本质上是相同的：有既定的游戏规则，每一步都应该遵循这些规则和当前的知识，没有其他。这就是我们说写数学证明应该受制于*logic*的意思：从一条真理到另一条真理的每一步，都应该遵循约定的规则，并且只参考这些规则或已经证明的事实。我们在证明（以及在数学中，一般而言）所玩的游戏，并不像数独游戏那样清晰明了。然而，更令人困惑的是，有时我们开始玩一个无法取胜的游戏，却没意识到这一点！

这个“不可胜游戏”的想法是20世纪奥地利逻辑学家库尔特·哥德尔工作的一个令人震惊、令人惊讶且极具影响力的结论。他的*Incompleteness Theorems*指出了强大逻辑系统的一个固有问题：存在True陈述，这些陈述在该系统中不是*provable*的。我们无法在这里提供某些术语的详细解释（特别是*logical system*和*provable*），但希望你能看出这里有些奇怪的事情发生。这怎么可能呢？如果某件事在数学上是True的，我们难道不能以某种方式证明它是真实的吗？否则我们怎么知道它是真实的呢?

Some Mathematical History

要开始回答这些自然问题，让我们稍微回顾一下时间，讨论逻辑作为数学一个完整分支的起源。在整个讨论中，有一点需要记住的是，我们无法完全解决出现的每一个话题，这可能会让人感到不满意，我们理解这一点。数学之美的一部分在于，了解任何一个话题都会引发许多其他问题和概念来思考，而且这些也可以通过更多的数学来解决这个问题。然而，上下文很重要，对于这本书的上下文来说，我们并没有时间和空间来解决所有这些相关的话题。我们并不是试图隐瞒任何事情或把一些问题掩盖起来；相反，我们只是在处理确保我们不是强迫你阅读1万页关于整个数学历史的书籍，只是为了传达我们的观点的现实！

您可能会在数学生涯的后期进一步研究我们下面提到的人（以及他们所做的工作）。在那个阶段，您将通过对材料的实际操作经验，对主题有更深入的理解和欣赏，并且将更好地准备应对其中存在的问题。目前，我们只是出于兴趣介绍这些人。数学有着丰富而有趣的历史，了解它很有帮助！在这里，我们将尝试提供一个简洁而又有意义的逻辑解释——它的历史、动机和意义——这与当前的环境相吻合。

19世纪中后期研究演变为现代逻辑的思想的数学家和哲学家们对以下内容感兴趣

许多我们在这里试图调查的相同问题：我们如何知道某物是 True？我们如何表达这个真理？我们甚至可以声明哪些“某物”是 True 或不是？将这些数学语言分解到其最根本的根源，这些数学家研究了以非常具体的方式组合一组固定符号以创建更复杂的陈述的方法，但在整个大局中，这些陈述仍然相当简单。这并不是要贬低他们的努力；毕竟，每个人都要从某个地方开始，而这些人是从基础开始的。

第一个主要努力是研究算术的基础，或者说研究**natural numbers** (1, 2, 3, 4, . . .)。这与欧几里得试图通过建立一组被接受为真理的简短列表，或者说**axioms**，然后从这些给定假设中推导出真理，非常相似。意大利数学家朱塞佩·佩亚诺为自然数建立了一套公理，而其他人则从略微不同的角度来探讨这个主题。同时，这种对严谨和明确地关于真理以及证明这些真理的新认识，导致大卫·希尔伯特和其他人提出了关于欧几里得公理的一些问题，特别是平行公设。

这项关于几何和算术的工作自然地引申到对其他数学领域的深入研究，以及对像实数分析这样的领域的公理化热情尝试。在研究这个主题时，Karl Weierstrass产生了一些具有奇特性质的函数的令人震惊的例子。例如，尝试定义一个在任何地方都不可微分的连续函数。（如果你对微积分中的这些术语不熟悉，不必担心；只需说，这很困难。）最后，Richard Dedekind能够建立完全基于自然数的严格、逻辑的实数定义，不依赖于一些模糊的物理观念，即必须存在一个数字的连续体。

稍后，这项研究略微转向了对**sets**或对象集合的研究。这一领域的许多基础工作是由乔治·康托尔在19世纪末奠定的。他是第一个真正研究无限集理论的人，提出了有争议的观点，即存在不同的“无限大小”。也就是说，他证明了有些无限集比其他无限集严格更大。在当时，这个观点如此有争议，以至于他遭到了许多其他数学家的憎恨！如今，我们认识到康托尔是正确的。（这也让你对我们在第7.6节后面将要讨论的内容有所了解。以这个有趣的事例为例：奇数集合和偶数集合的大小相同，当然，它们也与al整数集合的大小相同。然而，所有实数集合要大得多$strictly$！）

确实，一些数学家对康托尔的发现感到非常震惊，甚至伟大的伯恩哈德·黎曼也认为集合论的发展将是数学的灾难（至少最初是这样）。然而，情况并非如此，它自那时起就蓬勃发展起来，许多数学家致力于寻找以恰当的方式表示所有数学的方法，并理解数学的“基础”。从某种意义上说，你可以将集合论视为研究所有数学家都在使用的最基本对象的研究，最终，这与所有化学都是通过适当组合的方式完成的相似。

ele元素周期表的表述越来越复杂 d 种方式。

这些主题的进一步发展是符号逻辑的研究，这比我们之前提到的抽象概念更为具体，我们将在本书的前几章中频繁研究其基本思想。这一领域涵盖了如何将数学方程和符号与基于语言的符号和连接词结合起来，形成有意义的数学陈述，这些陈述可以通过证明被确认为真。这在数学的一般性和本书的特定性中都是一个极其重要的组成部分。个别观点当然比这更为细腻和具体，但总的来说，大多数数学家都持有这样的观点：有许多数学真理等待被发现，我们花费时间学习我们已经发现的真理，希望揭示更多这样的真理。这就像一场巨大的考古挖掘，通过研究我们已经挖掘出的骨骼和文物，将帮助我们预测我们将找到哪些类型的其他宝藏以及在哪里，这告诉我们在哪里寻找以及如何挖掘，一旦到达那里。从某种意义上说，逻辑是从挖掘中抽象出来的一步：逻辑是挖掘过程的研究。它告诉我们如何实际上利用我们的数学知识并从中学习，将其与其他知识相结合，以证明更多的真理。

现在，请注意，这并不是一个精确的类比，抽象逻辑的研究要复杂和错综得多。然而，就我们的目的而言，在这本书中，这是一种足够合理的逻辑思考方式。我们将学习一些符号逻辑的基本原理和基本操作，并将这些知识应用于我们对证明的研究。这将帮助我们真正理解什么是证明*is*，它将帮助我们指导我们想要编写的证明的构建，它将使我们能够批评可能不正确的证明，并最终帮助我们理解数学是如何作为一个整体运作的。

Applications of Logic: Theoretical Computer Science

逻辑的思想和结果在计算机科学，尤其是理论计算机科学和可计算理论的发展和研究中有非常重要的应用。这个数学分支最初是由大卫·希尔伯特的二十三个问题之一所激发的：这是一份在1900年出版时数学界著名的未解猜想列表。第十个问题涉及解决**Diophan- tine Equations**，这些是形如的方程

$$a_1x_1^{p_1} + a_2x_2^{p_2} + a_3x_3^{p_3} + \cdots + a_nx_n^{p_n} = c$$

在 $a_1, a_2, \ldots, a_n$ 和 c 为固定常数，$p_1, \ldots, p_n$ 为固定自然数，$x_1, x_2, \ldots, x_n$ 为待确定的变量，以便使方程成立的情况下。

给定一个这样的方程，人们可能会想知道是否真的存在解，以及如果存在，究竟有多少个。此外，如果我们知道固定的常数 a_i 和 c 都是理性数，我们可能会想知道

我们能否确保存在一个解，其中所有变量 {v*} 都是理性数。关于这个特定问题已经建立了一些理论结果，但希尔伯特在1900年提出的第10个问题，询问是否存在“一个过程，通过这个过程可以在有限次操作中确定”给定方程是否有解，其中所有变量 x_i 都是理性数。当时他们没有这个术语的适当概念或定义，但希尔伯特所要求的是一个 **algo- rithm**，它会接受常数 a_i 和 c 的值，并根据是否存在具有所需性质的解输出 True 或 False。他问题的一个重要部分是，这个“过程”在输出答案之前需要经过有限步。

剑桥大学英国的一名学生，名叫艾伦·图灵，在多年后通过思考一种物理机器来执行输出所提出问题的步骤，开始研究这个问题。他的一些后续出版物描述了他的发明，我们现在称之为*Turing Machine*，这是一个有趣的理论装置，可以用来解决形式逻辑中的一些问题，但也代表了构建现代计算机的许多想法。我们称之为*theoretical device*，因为其定义的本质确保了它在物理上无法构建和运行，但它处理一些理论问题相当好，包括上述希尔伯特的第十个问题。更具体地说，这台机器为当我们说某物是可计算的，或能在有限步骤中确定时，我们所说的含义提供了一个适当的定义，这有助于确立一个适当的**algorithm**概念。如果我们不提及同时也在研究类似问题的阿隆佐·丘奇，那么讨论这些主题将是不公平的。他们的名字一起被放在*Church-Turing thesis*上，这把图灵机的作品与更理论化、基于形式逻辑的计算可及性概念联系起来。

What Will *We* Do with Logic?

虽然集合论和逻辑中的所有这些主题在本质上都很有趣，对数学来说极其重要，但总的来说，我们并没有足够的时间和空间来详细讨论它们。相反，让我们更多地关注我们在撰写和评论数学证明时将使用的逻辑概念。

我们将考虑以下内容：（1）我们实际上可以陈述和证明哪些“事物”，（2）我们如何将已知为真的“事物”结合起来产生更复杂的真理，（3）我们如何解释我们得出那些“事物”确实是True的结论。由于没有更好的术语，我们称之为“事物”，因为我们还没有对**mathematical statement**给出正式的定义，而**mathematical statement**实际上是我们将要证明的“事物”的类型。本质上，一个数学陈述是数学和英语（至少在这本书中）中的符号和句子的组合，可以验证为True或False之一，但不能同时或都不是。因此，证明就是安排一系列步骤和解释，这些步骤和解释使用了真实的数学陈述

将连接这些真理的句子放在一起，以得出特定陈述的预期真理。我们研究逻辑将涉及我们如何组合这些步骤，并保证我们的证明最终导致对真理的正确评估。

更具体地说，我们将探讨一个数学陈述真正是什么，以及我们如何将它们结合起来产生更复杂的陈述。单词 *and* 和 *or* 在那里尤其重要，因为这两个单词允许我们以新的和有意义的方式将两个数学陈述结合起来。我们还将研究 **conditional** 个数学陈述，这些陈述的形式是“如果 A，那么 B”或“A 蕴含 B”。这些实际上是数学陈述的精髓，大多数重要的数学定理都是这种形式。这些陈述涉及在陈述 A) 中做出某些 *assumptions* 或 *hypotheses* (，并使用这些假设的真理来推导出陈述 B) 中的 *conclusion* (。回顾一下第 1.1.1 节中勾股定理的陈述，注意它是以条件陈述的形式出现的。（能否用另一种方式写？尝试用非条件形式写出定理的陈述，并思考它是否是以那种形式本质上不同的陈述。找到另一个以条件陈述形式出现的著名数学定理，并尝试进行同样的格式更改。）

另一个在数学中非常重要的概念，在证明写作中会经常出现，就是**variable**的概念。有时我们想要泛泛地谈论一种数学对象，而不给它指定一个特定的值，这是通过引入一个变量来实现的。你很可能在之前对数学的学习中经常看到这种情况发生，我们在这本书中也已经这样做过了。再次看看1.1.1节中勾股定理的陈述。字母a, b, c代表什么？嗯，我们没有明确地陈述它，但我们知道这些是代表直角三角形三边长度的正实数。什么三角形？我们没有提到一个特定的三角形或指向一个特定的图形或类似的东西，但你一直都知道我们在谈论什么。此外，我们考察的证明并不依赖于这些值实际上是什么，只是它们是具有某些性质的积极实数。这非常有用且重要，从某种意义上说，它节省了时间，因为我们不必单独考虑宇宙中（其中有无穷多个！）可能的all个直角三角形，而可以将整个想法简化为一个紧凑的陈述和证明。

我们可以用变量进行 {v*}。这涉及到对语句是否对变量的 *any* 可能值成立，或者可能只对 *one* 特定值成立的断言。例如，在勾股定理中，我们无法断言 $a^2 + b^2 = c^2$ 对任何正实数 a, b, c 成立；我们必须对变量施加额外的假设才能得到我们得到的结果。这是一个 **universal** 量化的例子：“对于具有这些属性和那些属性的 *all* 数，我们可以保证 ...” 同样，我们可以量化 **existentially**：“有一个具有这个属性的 n 数。”

你能想到我们已经考察过的使用存在量词的定理/事实吗？再次看看存在无理数的证明

数字 a 和 b，使得 a^b 是有理数。注意，我们已证明的这个命题是存在性的：我们声称存在两个具有所需性质的数字 *there are*，然后我们继续证明确实存在这样的数字。现在，那个证明的有趣之处在于它 *nonconstructive*；也就是说，我们能够在不明确说出数字 a 和 b 实际是什么的情况下证明我们的命题。我们将选择范围缩小到两个，但从未声称哪个是正确的选择，只是说其中一对 *must* 是有效的。

1.2.4 Obvious Obfuscation

作为我们稍后将在数学细节中检验这些逻辑概念的预览，让我们来看一些基于现实世界、语言相关的例子来阐述这些想法。

Conditional Statements

首先，让我们研究 **conditional statements**。数学定理通常以条件语句的形式出现，但这类语句也经常出现在日常语言中，有时是隐含的（这只会增加混乱）。例如，人们有时会谈论他们会如何使用他们的彩票奖金，说一些像这样的事情

> 如果我中彩票，那么我将买一辆新车。

想法是，在“那么”之后的语句的第二部分依赖于语句的第一部分，该部分与“如果”相关。当“如果”部分中概述的条件得到满足时，“那么”部分中概述的行动将得到保证。

条件语句中与“如果”相关的部分被称为**hypothesis** (，有时，更正式地，被称为**antecedent**)。与“那么”相关的部分被称为**conclusion** (，或者，更正式地，被称为**consequent**)。

有时条件句的结论更为微妙，或者句子的动词时态如此，以至于甚至不包含“如果”这个词。以下是从电影 *Top Gun* 中引用的例子：

> 它已被分类。我可以告诉你，但那样我就不得不杀了你。

这里的思想是，第一部分“我可以说”，实际上是一个伪装的假设。句子 *“If I told you, I would have to kill you”* 应该具有与实际电影台词相同的逻辑意义；然而，它并没有传达出同样的强烈、戏剧性的含义。在条件语句的结论中实际上不包含“然后”这个词是很常见的；在阅读句子时，你甚至可能在心里加上这个词，而自己都没有意识到。以下是从乐队The Barenaked Ladies的一首歌中的歌词，比如说：

> 如果我有一百万美元，我们就不必走到储藏室 e. 如果我有100万美元，我们会开一辆豪华轿车，因为它的价格更高。

两个语句都是条件语句，但都没有包含“然后”这个词；它被认为是句子的一部分。

与以下句子进行比较，看看有什么不同：{v*}

> 我只在下雨时才带伞。

这里的思想是，说话者不愿意没有理由地随身携带雨伞，更愿意确保它会有用。这个句子和以下类似的句子意思相同吗?

> 如果我在撑伞，那么正在下雨。

在现代语言使用中，条件概念可能有点模糊。第一句话可以理解为有时可能会下雨，但说话者忘记带伞，比如说。第二句话是一个明确的条件语句的断言：看到我打着伞走来走去，你必然可以推断这是因为下雨。在数学中，我们将这两句话联系起来，说它们具有相同的逻辑意义。

这激发了短语“仅当”的含义，进而激发了短语“当且仅当”的含义。考虑以下两个句子：

> 如果我中彩票，我将买一辆新车。我将买一辆新车 *only if* 我中彩票。

第一个说赢得彩票保证我会买一辆新车，而第二个说买新车的行为保证是因为我刚刚赢得了彩票。如果这两个句子都是真的，那么“赢得彩票”和“买新车”这两个事件在某种意义上是等价的，因为每个事件的发生 *necessarily guarantees*等同于另一个事件的发生。

相应地，数学定义通常使用短语 **“if and only if”**。例如，我们可能会写出“一个整数是偶数，当且仅当它能被2整除。”这表明知道一个数具有该属性允许我们称其为“偶数”，并且知道一个数是偶数允许我们得出其可整除的性质。（有时，定义将仅使用 *if*，其中 *only if* 部分未明确说明但被理解。你可能已经注意到我们在第1.1.2节中定义素数时就是这样做的。）

Creating More Conditional Statements from Others

从条件语句开始，我们可以稍作修改，从而产生三个具有相同内容但结构不同的其他条件语句。继续使用“彩票/汽车”的例子，让我们考虑以下四个原始句子的版本：

> 1. 如果我中了彩票，那么我会买一辆新车。2. 如果我买了一辆新车，那么我中了彩票。3. 如果我没有中彩票，那么我不会买新车。

4. 如果我没有买一辆新车，那么我就没有赢得彩票 y.

这些句子如何比较？它们之间是否有相同的逻辑意义？在第一个句子为真的假设下，它们都是True，必然的吗？我们可能会争辩说，在这种情况下，第二个句子可能是False，即使第一个句子是True。也许我在工作中得到了丰厚的加薪或者继承了些钱，决定买一辆新车。那么第三和第四个句子呢？它们能否以某种方式与其他句子相关联？我们将把这个留给你自己讨论和探索。也许向一些我们之前看过的其他条件语句提出同样的问题会很有趣，看看你的答案是否也不同。

一个我们将提到的条件语句的最终例子来自喜剧演员Demetri Martin的一个笑话。

> 我走进了一家服装店，一位女士走过来对我说：“如果你需要什么，我是Jill。”我以前从未遇到过有条件身份的人。“如果我什么都不需要呢！你是谁？”

这应该让你对现代语言中条件语句可能不精确或微妙的方式有所了解，有时甚至可能存在歧义。在数学中，我们希望这些类型的陈述是严谨的、定义良好的且无歧义的。这是我们将在第4.5.3节稍后进一步探讨的内容。然而，现在，考虑这些类型陈述的严谨方式，就像计算机算法解释一个 `if...then` 陈述的方式可能会有所帮助。当 `if` 部分的条件得到满足时，子程序将被执行，否则它们将被忽略。同样，一个 `while` 循环只是将一系列 `if...then` 陈述压缩成一种简洁的形式。

Quantifiers

接下来，让我们考察一些 **quantifiers** 的例子。当存在一个未知变量，该变量意味着从可能的值或表示的集合中抽取对象时，我们将使用量词。例如，当我们对勾股定理陈述中的变量 a, b, c 进行量化时，它们是从代表直角三角形边长的实数集合中抽取的。对于一个非数学的例子，考虑以下句子：

> 每个人都被某人爱着。

这里有哪些变量？它们是如何量化的？请注意，是的，这个句子中实际上有两个量化，分别对应两个不同的变量。在两种情况下，变量代表世界上所有人的集合中的一个成员，第一个变量是全称量化，而第二个变量是存在量化。这可能会听起来很困惑，所以让我们尝试更详细地重写这个句子：

> 对于世界上每个人 x，都存在另一个人 y，具有这样的属性：第一个人 y 爱上第二个人 x。

你看到这一点与第一句话有相同的逻辑意义吗？当然，这句话在对话中显得过于冗长和精确，但我们在这里提出它，是为了向您展示潜在的变量和量词。量词的关键短语是 *"for every"* (全称) 和 *"there exists"* (存在)。

The Order of Quantification Matters!

现在，让我们看看一个与上一个例子类似的句子：

> 每个人都被爱着。

这句话与上面那一句非常相似；它甚至有所有相同的单词！单词顺序的改变对句子的逻辑意义有何影响？嗯，仍然有两个变量和两个量词，一个是全称量词，一个是存在量词，但应用这些量词的顺序已经交换了。这个句子的冗长版本是：

> The Translated Text: The 存在一个具有以下属性的人 x，即对于每个 pe rson y 在世界上，人y爱着人x。

这完全不同于第一句话的意思！第一句看起来可信，但这句话几乎是荒谬的。这应该让你意识到保持量词顺序的重要性，以确保你实际上所说的就是你想说的。

Nested Quantifiers

以下示例说明了我们的大脑有时可以相当快速和容易地处理基于语言的句子中的量词，即使相互关联性可能使其难以理解。当量词一个接一个地出现时，我们称它们为 $nested$。

分析和理解此类句子的能力可能取决于句子的上下文以及它试图传达的信息。如果信息有意义且我们相信它，那么理解起来可能更容易。我们已知此现象的最佳例子体现在以下引用中，该引用归功于伟大的总统演说家亚伯拉罕·林肯：

> 你可以永远欺骗一部分人，也可以在某个时期欺骗所有人，但你不能永远欺骗所有人。

这里到处都是量词！我们正在讨论所有人的集合以及某些人被愚弄的实例的集合，并在这些集合上进行量化。试着用几种不同的措辞来写这句话，看看是否可以听起来更“简单”或更简洁。

可能还有其他方式来表达这个句子，从而去除一些（或全部）量词而不改变其含义吗?

最后，出于个人兴趣和增添一点幽默，我们将提到一句来自鲍勃·迪伦的歌曲《谈论第三次世界大战布鲁斯》，收录在他1963年的专辑 *The Freewheelin' Bob Dylan*中的一句类似的话:

> 一半的人可以一直部分正确，一些人可以在一段时间
> 内全部正确，但所有人不可能一直全部正确。我认为
> 亚伯拉罕·林肯说过这样的话

我们将稍后更详细地讨论这些主题，届时我们将探讨它们的数学动机、意义和用途。目前，我们无法强调这些问题在撰写证明中的重要性。将一些句子连在一起，却无法知道它们是如何相互关联的，这并不是证明，而是一个结构良好的逻辑陈述和推论的系列，这正是我们所寻求的。

1.3 Review, Redo, Renew

迄今为止，我们试图从逻辑角度激发和解释数学推理和证明写作，但在过程中，我们使用了一些你可能熟悉或不熟悉的数学概念和技术。当然，在做数学时进行逻辑和理性的思考是很重要的，但这只是更大图景的一部分。我们试图解释如何组织数学思想并以有意义的方式构建它们，以使他人相信某个特定事实，但这些思想必须包含与该事实相关的某些数学概念!

例如，如果我们没有对几何学有基本的了解，我们就无法查看勾股定理的任何证明：什么是三角形，三角形、线和角度的一些基本性质等。我们还假设读者会理解什么？许多步骤涉及算术，如通过乘以相同的因子来操作多个方程，或者减去两个方程等。这些想法现在可能对你来说很自然，但你在某个时候必须学习这些知识，了解为什么以及它们是如何实际工作的，这样你才能在将来安全、恰当地使用它们。

回顾一下我们在前几节中看过的其他证明。我们使用了哪些数学思想？尽量写下一些，并思考你是何时以及如何了解它们的。尽量写下一些我们可能没有明确说明但我们可能使用过的具体事实，并思考我们为什么会这样做。此外，尽量找出一些我们提出了一个主张但并没有必要完全解释为什么它必须是 True 的情况，并尝试这样做。例如，在勾股定理的“证明1”中，我们在一个正方形内画了四个相同的三角形，然后说正方形内的图形也将是一个正方形。这真的是 True 吗？我们怎么能这么肯定呢？尽量证明它!

Presumed Knowledge

主要观点是我们实际上无法在不赋予它们一些有意义的数学内容的情况下写出证明。因此，本书的主要目标之一就是与您分享一些有趣的数学事实。有时，这涉及到处理您已经了解并见过（如三角形或素数）的对象，并尝试用它们做些新的事情。其他时候，我们可能会向您介绍一些全新的数学对象（如等价关系或二项式系数）并与之合作。我们现在想讨论一些我们将非常频繁使用且您可能之前见过的一些数学对象和概念。我们并不一定假设您已经见过所有这些，但这些想法都不难学习/快速重学，并且它们将在本书的剩余部分以及您数学生涯的剩余部分中非常有用！我们为您准备了一些问题，让您在本书的这一部分以及结束部分进行练习。

1.3.1 Quick Arithmetic

我们不会期望你在脑海中乘以六位数或类似的东西，但能够通过加法、减法和乘法操作“小”数是一项重要的技能。当然，计算器和计算程序可能会有所帮助，但我们希望在我们需要加几个四位数时，不必立刻跑到`Maple`或`Mathematica`或你的`TI-89`那里。技术以准确性和时间效率的形式为我们提供了许多便利，但当我们过度依赖这些设备时，我们就会削弱验证我们得到答案的能力（例如，在输入错误或按键遗漏的情况下），而且当我们过于频繁地使用它们时，我们实际上可能根本不会节省任何时间！

我们鼓励你不断地尝试在脑海中或在一张废纸上完成我们遇到的任何算术步骤。涉及“大数”的算术问题/谜题相对较少，即使它们确实涉及，也可能有一个特殊的技巧可以将问题简化为更容易处理的形式。例如，尝试解决以下一系列问题，看看你注意到了什么。

Problem 1.3.1. 对于以下每个乘法，尝试确定结果的最后一位数字。如果你的答案是“0”，那么尝试确定结果末尾有多少个*many*零。

1. $1 \cdot 2 \cdot 3 \cdot 4 \cdot 52.\ 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 103.\ 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 254.\ 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 1005.\ 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 1000$

6. $1 \cdot 2 \cdot 3 \cdot \cdots \cdot 10000$
7. $1 \cdot 2 \cdot 3 \cdot \cdots \cdot 10^9$

尝试写下几句话，向朋友解释你上面使用的程序。也就是说，给定任何数字 n ，解释如何识别乘以 $1{\cdot}2{\cdot}3{\cdot}\cdots{\cdot}n$ 后得到的数字末尾的零的数量。

你注意到了什么？你用计算器做了前几个吗？当然，那应该会起作用，或者你也可以手动完成前两个或三个，但那后来又帮了你什么忙呢？那又是如何帮助你解释你的方法的呢？当然，你需要找到一种更通用的方法来解决这个问题，在某些情况下，求助于计算器或电脑可能有所帮助，但它不会给你提供任何关于答案的见解。

如果您还没有想出一个通用程序，我们将提供这个：

Hint考虑在乘法中有多少个2的倍数和多少个5的倍数出现。尝试将它们配对在一起。（你为什么要这样做呢？）

1.3.2 Algebra Abracadabra

该术语 **algebra** 在数学世界中具有几种含义，每种含义都有一些细微差别。通常，这个术语让人联想到处理带有变量的方程，并试图找到它们的数值解。这可能是你在高中代数课上处理文字问题的方式。然而，更普遍地，**abstract algebra** 是数学的一个分支，研究具有特定性质的某些数学结构，这些结构通常与整数或实数无关。

许多这个领域的准备工作是在19世纪之前由寻求多项式方程根的数学家们完成的，其中变量被提升到三次、四次甚至更高的幂。对于一个二次方程（包含被提升到二次幂的变量），你可能还记得寻找方程根的公式（即变量值，使得表达式评估为零）；这就是著名的 *Quadratic Formula*。

你也知道有一个用于求解涉及立方变量或四次幂变量的表达式的根的步骤吗？有趣的是，研究这个一般问题的数学家发现，对于更高的幂，有*no*种可能的步骤！他们所使用的许多概念和结构发展成了一些固有的有趣数学，人们一直在研究这些对象，最终分支出来并研究这些对象的潜在属性，剥离了求解方程根的数值背景。这就是当数学家说“代数”时通常所指的。

在这个特定语境中，尽管如此，我们将使用“代数”这个词，就像你很可能想到的那样：操作多个方程和变量

为了获得使表达式求值得到满足所有方程的数字的变量的数值。实际上，解决线性方程组的背后有一个丰富而精彩的原理，但这种深入的研究更适合矩阵代数（也称为线性代数）的课程。现在，我们将看看一些实用的技巧，然后让您练习它们。

Solving Systems of Linear Equations

一个线性方程组只是包含一定数量的变量（所有变量都乘以1次方，因此是*linear*）的方程集合，乘以系数并相加，然后设为某些常数。系数和常数存在特定条件，可以保证是否存在解（以及是否存在无限多个或只有一个，实际上）但我们不会深入这些特定细节。只需说，在这本书中我们将要处理的方程组将有唯一解，这意味着我们拥有的方程数量将与涉及的变量数量相同。提前知道这一点，我们如何操作一个方程组来找到那个唯一解呢?

在实际情况中，解决一个系统最有效的方法不仅取决于系数和常数，还可能需要找到我们即将解释的方法的特定应用方式。尽管如此，简单地遵循这些方法在任何情况下都将在短时间内有效，所以不必过于担心在特定情况下找到绝对最短的方法。

Method 1: 第一种方法涉及一个包含两个方程和两个未知数的系统。在这种情况下，我们可以使用其中一个方程将一个变量用另一个变量表示，然后将这个表达式代入第二个方程，得到一个方程和一个未知数。从那里，我们可以找到一个变量的特定值，然后将这个值代入第一个方程以找到另一个变量的特定值，从而得到我们想要的解。让我们通过一个具体的例子来看这个过程。考虑以下方程组:

$$\begin{aligned} 7x + 4y &= -2 \\ -2x + 3y &= 13 \end{aligned}$$

按照我们刚才描述的方法，我们将重新排列第一个方程，用 y 表示 x

$$y = \frac{1}{4}(-2 - 7x)$$

然后将此代入第二个方程

$$-2x + 3 \cdot \frac{1}{4}(-2 - 7x) = 13$$

解这个新方程以求解 x:

$$\begin{aligned} -2x - \frac{3}{2} - \frac{21}{4}x &= 13 \\ -\frac{29}{4}x &= \frac{29}{2} \\ x &= -2 \end{aligned}$$

然后，我们将在第一个方程中使用这个值，并解出 y:

$$\begin{aligned} 7 \cdot (-2) + 4y &= -2 \\ 4y &= -2 + 14 = 12 \\ y &= 3 \end{aligned}$$

因此，我们寻求的解是 $(x, y) = (-2, 3)$。

如果我们用第二个方程中找到的 x 的值代替第一个方程中的值呢？嗯，它会产生与 y 相同的值，但也许计算会稍微快一点。或者，如果我们反过来操作，用 y 来表示 x，解出 y，然后回过头来解出 x 呢？我们还是会找到相同的解，但也许数字会更容易处理，并为我们节省几秒钟的草稿工作。这就是我们不担心找到最“有效”的方法的意思。当然，有多种方法可以处理这个方程组，但它们最终都源于相同的方法（代入求解）并得到相同的解。

Method 2: 一种处理两个方程和两个未知数的替代方法是，将两个方程都乘以特定的值，然后将它们相加，适当地选择这些乘数，以便消除一个变量。使用上面的例子，我们可以将第一个方程乘以2，第二个方程乘以7，使得两个方程中x的系数相等但符号相反；然后，相加方程将系统简化为一个方程和一个未知数，即y。观察:

$$\begin{aligned} 2 \cdot \big(7x + 4y = -2\big) \\ 7 \cdot \big(-2x + 3y = 13\big) \\ 14x + (-14x) + 8y + 21y &= -4 + 91 \\ 29y &= 87 \\ y &= 3 \end{aligned}$$

从那里，我们可以将此值代入第一个或第二个方程，并解出 x。

您可以使用这两种方法中的任何一种来处理任何包含两个未知数的二元方程组。可能其中一种方法会稍微快一点，这取决于涉及的数字，但无论如何您也节省不了超过一分钟，所以我们鼓励您只选择一种方法并完成它。

Method 3: 有时将这些方程组图形化解释可能很方便；这通常不是识别系统特定解的高效方法，但它可以给出是否存在解的指示以及解的值的大致估计。

两个未知数时，我们可以通过重新排列来解释平面上的方程如 $ax + by = c$，即 $y = -\frac{a}{b}x + \frac{c}{b}$。这是斜率为 $-\frac{a}{b}$ 且 y 截距为 $\frac{c}{b}$ 的直线。给定两个这样的方程，我们可以在平面上画出两条直线并直观地找到它们的交点。该点的 (x, y) 坐标正是我们通过上述方法解方程组所得到的解。

此视觉方法也适用于三个方程和三个未知数的系统，但需要在三维空间中绘制线条。这在实践中可能很困难，但在技术上是可以实现的。这些相同的概念也适用于更多方程和未知数，但对于我们人类来说，在四维或更多维度中绘制“线条”是无法可视化的!

More than two variables: Reduce! 下一段该方法基于第一部分，通过取一个包含两个以上方程（和未知数）的系统，并不断将其简化为更小的系统，最终获得一个包含两个方程和两个未知数的系统，在那里我们可以应用该方法的第一部分。我们将通过考虑一个包含三个方程和三个未知数的系统来阐述该方法，如下所示：

$$\begin{aligned} 6x - 3y + z &= -1 \\ -3x + 4y - 2z &= 12 \\ 5x + y + 8z &= 6 \end{aligned}$$

第一个目标是消除三个变量中的一个。本质上，这可以通过两种方式之一来完成，就像两个方程和两个未知数的方法一样。假设我们要尝试从系统中消除 z；我们可以尝试用 x 和 y 来表示 z 并进行某种替换，或者我们可以将某些方程相乘并相加以消除 z 的系数。这里唯一的区别是，无论我们选择哪种选项，我们都需要做两次。让我们用第一个方程来写

$$z = -6x + 3y - 1$$

在将此表达式代入第二个和第三个方程中的 z 之后，我们将得到一个包含两个方程和两个未知数的方程组。

一种思考方式是，我们需要从所有三个方程中获取信息才能最终得出答案，而在将系统简化为两个方程时，我们需要以某种方式保留原始三个方程中的所有信息。我们得到的 z 表达式来自第一个方程，因此我们需要将其代入其他两个方程中，以保留所需的所有信息。

与以下步骤进行比较：将第一个方程式重新排列以隔离 z，并将其代入第二个方程式，然后重新排列第二个方程式以隔离 z，并将其代入第一个方程式。

发生什么了？直观的感觉是我们以某种方式“丢失”了第三个方程的信息，是的，我们将得到一个包含两个方程和两个未知数的系统，但它将信息不足，无法为 x 和 y 提供唯一解。如果您实际执行我们刚才描述的步骤（尝试这样做以检查我们的工作），在最小化简化后，您将得到以下“系统”的两个方程：

$$\begin{aligned} 9x - 2y &= 10 \\ \frac{9}{2}x - y &= 5 \end{aligned}$$

这些实际上是完全相同的方程！因此，我们实际上无法为 x 和 y 的唯一值求解。

让我们回到我们之前的位置，并将上面关于 z 的表达式代入第二个和第三个方程中

$$\begin{aligned} -3x + 4y - 2 \cdot (-6x + 3y - 1) &= 12 \\ 5x + y + 8 \cdot (-6x + 3y - 1) &= 6 \end{aligned}$$

然后简化

$$\begin{aligned} 9x - 2y &= 10 \\ -43x + 25y &= 14 \end{aligned}$$

应用第一个问题中的方法之一将给我们解决方案$(x, y) = (2, 4)$。有了这些值中的*both*，我们现在可以回到原始的三个方程中的任何一个并求解z；更好的是，我们可以直接使用我们从第一个方程中已经找到的孤立表达式z：

$$z = -6x + 3y - 1 = -6 \cdot (2) + 3 \cdot 4 - 1 = -12 + 12 - 1 = -1$$

More than two variables: Reduce another way! 另一种将系统从三个方程减少到两个方程的方法与之前提到的“乘法和加法”方法有关，但我们仍然必须小心确保我们保留了所有三个方程的信息。使用上面相同的三个方程组，我们可能会注意到，在将第一个方程乘以8和第二个方程乘以4之后，所有三个方程中z的系数要么是± 8。这使我们能够以方便的方式加减方程，将系统减少到两个方程和两个未知数。具体来说，让我们做我们刚才提到的乘法

$$\begin{aligned} 48x - 24y + 8z &= -8 \\ -12x + 16y - 8z &= 48 \\ 5x + y + 8z &= 6 \end{aligned}$$

然后，将第一个方程加到第二个方程上

$$\begin{aligned} (48x - 12x) + (-24y + 16y) + (8z - 8z) &= -8 + 48 \\ 36x - 8y &= 40 \end{aligned}$$

并且第二个方程到第三个

$$(-12x + 5x) + (16y + y) + (-8z + 8z) = 48 + 6$$
$$-7x + 17y = 54$$

这产生了只涉及 x 和 y 的两个方程；此外，我们还结合了所有三个原始方程的信息来生成这些方程，因此我们可以确信我们没有“丢失”任何东西。求解这个新系统

$$36x - 8y = 40$$
$$-7x + 17y = 54$$

通过我们之前讨论的任何一种方法都可以得到解 $(x, y) = (2, 4)$。将这些值代入任意一个原始方程中并解出 z，就能得到我们寻求的最终答案。

我们可以执行类似的步骤从三个方程组中消除 y，例如，我们可以将第一个方程乘以4加到第二个方程乘以3上，并将第三个方程乘以4从第二个方程中减去。这些方法中的任何一种都会产生相同的最终答案，但其中一些可能会缩短算术步骤或涉及“更漂亮”的数字（即更少的分数、更小的乘法等）。解具有更多方程的方程组相当于相同的通用程序：将方程相乘并相加以消除系统中的一个变量，然后继续这样做，直到只剩下两个方程和两个未知数；然后，求解这两个变量的值，并反向替换这些值以求解已消除的变量的值。

Algebra Practice

Problem 1.3.2. 解以下方程组以求解 (x, y, z):

$$x + y + z = 15$$
$$2x - y + z = 8$$
$$x - 2y - z = -2$$

现在，解这个类似的系统 (x, y, z):

$$x + y + z = 15$$
$$2x - y + z = 9$$
$$x - 2y - z = -2$$

比较两个系统中 $x, y,$ 和 z 值的变化。

哪个变量变化最大？最小？这些变化的比率是多少？

您可以通过改变系统第二个方程右侧的常数来使这个比率变得多大或多小？

Problem 1.3.3. 一位父亲、一位母亲和一个儿子坐在餐馆里吃晚餐，这时他们被另一家由一位父亲、一位母亲和一个儿子组成的一家接近。第二家注意到他们与第一家非常相似，所以第二位父亲问第一位，“你们三个人多大了？我猜我们都差不多大”。第一位父亲碰巧是一位数学家，不想轻易透露他家庭成员的年龄，因此以巧妙的方式“揭示”给其他人。他说：“嗯，我们现在的年龄加起来是72岁，我碰巧是我的儿子年龄的六倍。然而，在未来当我只是他年龄的两倍时，我们的总年龄将是现在总年龄的两倍。你们认为我们现在是多少岁？”

三个家庭成员多大了?

1.3.3 Polynomnomnomials

有时我们需要处理平方、立方或更高次幂的变量。一般来说，**polynomial**是我们用来表示一个或多个变量被整数次幂提升，乘以系数，然后相加的函数的术语。以下是一些多项式的例子：

$$x^2 - 7x + 1, \quad 7p^6 + 5p^4 + 3p^2 + 2p, \quad \frac{1}{2}z^2 + 9y^2z - 2y + z^3y^2 - 7z$$

这些类型的函数在数学中相当常见且受欢迎，部分原因是它们方便的性质，部分原因是它们在自然界中的普遍存在。我们将看到它们贯穿整本书。然而，现在让我们专注于只有 *one input variable* 的多项式。

Roots of Polynomials

有时，我们将在谜题的背景下定义一个多项式函数，并想知道是否存在任何输入变量的值使得输出值为0。这些输入值被称为多项式的 **roots**。

一种识别多项式根的方法是将 **factor** 它分解为线性项；也就是说，我们试图将函数表示为一系列乘法而不是加法，因为我们可以说（至少）一个因子必须是0以得到0值。这种技术背后的动机基于以下事实：

> **Fact**如果 a 和 b 是实数且 $ab =$ 不等于 0，则 $a =$ 等于 0 或 $b =$ 等于 0（或者可能两者都等于）。

Example 1.3.4. 让我们看看一个具体的例子。让我们尝试分解以下多项式：

$$p(x) = x^2 + 6x + 8$$

(这是一个常见的表示法，将多项式定义为 $p(x)$，其中 p 表示多项式，x 是输入变量，$p(x)$ 是对应于输入值 x 的输出值。但这并不一定如此。)

您可能会注意到

$$p(x) = x^2 + 6x + 8 = (x + 4) \cdot (x + 2) = (x + 4)(x + 2)$$

(它也很常见，当有括号分隔的因子时省略 $\cdot$，因此从现在开始我们将采用这个惯例。)

这个因式分解之所以有效，是因为我们多次应用了分配律，并且是反向应用。如果我们展开我们刚刚找到的因式分解，明确地展示每一步，它看起来会像这样：

$$\begin{aligned} p(x) &= (x + 4)(x + 2) \\ &= x(x + 2) + 4(x + 2) \\ &= (x^2 + 2x) + (4x + 8) \\ &= x^2 + 2x + 4x + 8 = x^2 + 6x + 8 \end{aligned}$$

所有我们真正做的是注意到项 $+4$ 和 $+2$ 的乘积是 $+8$，这是常数项，它们的和是 $+6$，这是 x 项的系数。知道这些因子的后续展开会如何进行，使我们能够写下这个分解，而实际上并不需要检查它。

Factoring Quadratics

让我们将我们在那个特定例子中所做的方法推广到任何二次函数。如果我们想分解一个像{v*}

$$p(x) = x^2 + bx + c$$

我们寻求值 r 和 s 以便 $r \cdot s = c$ 和 $r + s = b$。通常，我们可以“通过观察”来做这件事，或者只是盯着这两个方程看一分钟，想出适当的值。（这正是我们刚才在最后一个例子中所做的！）

如果我们发现 x^2 的系数不是 1 而是某个其他数字 a，我们该怎么办呢？嗯，注意，如果我们能分解多项式 $\frac{p(x)}{a} = x^2 + \frac{b}{a}x + \frac{c}{a}$，那么我们也可以通过乘以 a 来找到原始多项式 $p(x)$ 的一个分解。这不会影响我们找到多项式根的能力（我们的原始目标），因为我们假设 $a \neq 0$（否则我们一开始根本就没有二次多项式，也就不需要分解它了）。一旦我们找到了这个分解，就很容易识别 $p(x)$ 的根；既然我们想知道 $p(x) = 0$ 的时候，我们只需使用分解和上面提到的那个事实，就可以得出结论：

$$\begin{aligned} 0 = p(x) = (x + r)(x + s) \quad &\text{implies} \quad x + r = 0 \text{ or } x + s = 0 \\ &\text{which implies} \quad x = -r \text{ or } x = -s \end{aligned}$$

这意味着根必须是 $-r$ 和 $-s$。

如果我们有一个形如 $p(x) = x^2 - a^2$ 的多项式？这种特殊类型的函数被称为**difference of squares**，并且有一个快速的分解技巧。这是一个二次多项式，因此，根据上面的方法，我们会寻找满足 $rs = -a^2$ 和 $r + s = 0$（因为 $p(x)$ 中没有 x 项）的值 r, s。第二个约束告诉我们 $r = -s$，将这个值代入第一个约束中，我们得到 $r^2 = a^2$。因此，使用 $r = a$ 和 $s = -a$ 实现分解 $p(x) = (x - a)(x + a)$，因此根是 $\pm a$。（注意，使用 $r = -a$ 和 $s = a$ 也满足这两个约束，但实际上它产生了相同的分解 $p(x)$。）

类似的小技巧有时可以应用于更高次的**degree** (多项式。记住，“次数”是指输入变量的最高次幂)。例如，以下多项式的次数为4

$$p(x) = 4x^4 - x^2 - 3$$

但是，如果我们定义 $y = x^2$ 并将其写成二次多项式，我们就可以轻松地分解它

$$p(y) = 4y^2 - y - 3 = (4y + 3)(y - 1)$$

注意，你可以考虑 y^2、y 和常数项的分解，直接跳到我们找到的分解，或者遵循我们提到的除法技巧。在这里，我们想要分解 $\frac{p(y)}{4} = y^2 - \frac{1}{4}y - \frac{3}{4}$，因此需要 $rs = -\frac{3}{4}$ 和 $r + s = -\frac{1}{4}$；使用 $r = -1$ 和 $s = +\frac{3}{4}$ 有效，所以我们得到分解

$$\frac{p(x)}{4} = (y + (-1))\left(y + \frac{3}{4}\right)$$

这可以简化为

$$p(x) = 4(y - 1)\left(y + \frac{3}{4}\right) = (y - 1)(4y + 3)$$

这正是我们之前所拥有的。

A Root Yields A Factor

当然，这个识别根的技巧也可以反过来用：如果我们能轻易地找到一个多项式的根，这可以帮助我们识别一个因子。例如，看看下面的三次多项式，看看你是否能通过观察找到一个根；也就是说，看看你是否能找到一个输入值，使得 x 的值使得 $p(x)$ 评估为零：

$$p(x) = x^3 - 3x + 2$$

如果您还没有注意到，您可能想尝试插入一些“简单值”，比如前几个整数（正数和负数），看看会发生什么。如果您这样做，您会发现 $p(1) = 1 - 3 + 2 = 0$。因此，我们

知道多项式 p 的一个分解应包括因子 $(x-1)$，因为这与根 $x=1$ 对应。了解这一点后，我们想要将 $p(x)$ 除以因子 $(x-1)$，以便我们可以进一步分解这个商并识别 p 的所有根。

Polynomial "Division"

我们如何除多项式呢？我们寻求另一个多项式 $q(x)$，使得 $p(x)=q(x)\cdot(x-1)$，换句话说，我们需要找到 $\frac{p(x)}{x-1}$。识别此类函数的一种方法是通过使用你在中学时学习除整数时学到的相同原理。这些概念同样适用于多项式函数！回想一下长除法是如何工作的，并尝试解决一些基本示例——比如 $22\div 7$，以刷新你对它是如何工作的记忆。

现在，让我们尝试将这些相同的原理应用到多项式上。以下是将长除法思想应用于 $\frac{x^3-3x+2}{x-1}$ 的一个例子：

$$\begin{array}{r|l} & x^2+x-2 \\ \hline x-1 & x^3\quad -3x+2 \\ & -x^3+x^2 \\ \hline & \quad x^2-3x \\ & \quad -x^2+x \\ \hline & \quad\quad -2x+2 \\ & \quad\quad\ 2x-2 \\ \hline & \quad\quad\quad\ 0 \end{array}$$

在方法的每次迭代中，我们试图找到可以“进入”较大项的最大的“因子”。在这种情况下，这些只是x的幂的倍数；我们识别出可以“进入”当前所讨论项的最大的x的幂。由于被除数有x^3，除数有x，我们在除法线上方写上x^2。然后，我们将$(x-1)$乘以x^2，将这个结果写在被除数下方，并相减以找到余数。

我们重复相同的过程，直到我们在除法线上方得到一个常数项（即 x^0 的倍数）并看到余数。由于这里的余数是 0，我们知道我们有一个没有余数的因式分解。然后我们可以通过注意到 $r+=$^2 和 $s=-$^1 满足 $r+s=$^1 和 $rs=-$^2，所以我们最终可以写出

$$p(x)=(x-1)(x-1)(x+2)=(x-1)^2(x+2)$$

相应地，$p(x)$ 的根是 $x=1$ 和 $x=-2$。对于这个函数，多项式的次数是 3，但函数只有 2 个根。这让你觉得奇怪吗？你能想到一个次数为 3 但只有一个根的多项式吗？一个次数为 3 没有根的多项式呢？或者 4 个根、5 个或更多呢？这些可能吗？为什么或为什么不呢？如果我们处理的是一个次数为 4 的多项式呢？次数为 n 的多项式呢？关于多项式的根的数量与其次数之间的关系，你能肯定地说些什么呢？

Expanding Factors

有时，当我们解决一个谜题时，我们从一个多项式的分解开始，并希望完全展开这些因子，以便我们可以识别特定项的系数。我们如何快速简单地相乘多项式？本质上，我们正在尝试反复应用分配律，而不必写出所有步骤（尽管这种彻底的、逐步的程序是保证有效的，所以如果你不确定你的答案，总是一个好的主意回到并彻底检查每个步骤）。

一个可以减少涉及步骤数量的特定实例是在我们需要展开一个如$(a+b)^n$的分解式时，其中a和b代表任何常数或变量，n是一个整数。在这种情况下，有一种方便的方法可以识别展开多项式的系数，这些值来自**Pascal's Triangle**。

这是一个将整数排列成三角形的安排，其中每一行对应于这种扩展中 n 的特定值。生成帕斯卡三角形的技巧是将前两行写为全1，并将三角形的“腿”写为全1。在三角形的内部，任何一项都是通过找到该项上方左侧和右侧两个项的和来填充的。试着自己生成三角形的几行，并与下面的一行进行比较，以确保你正确地执行了程序。

$$
\begin{array}{lccccccccc}
n=0: & & & & & 1 & & & & \\
n=1: & & & & 1 & & 1 & & & \\
n=2: & & & 1 & & 2 & & 1 & & \\
n=3: & & 1 & & 3 & & 3 & & 1 & \\
n=4: & 1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

我们在左侧写下了n值以指示与原问题扩展$(a+b)^n$的对应关系。一般来说，展开式中的任何一项都将是一个系数（从三角形中取出）乘以$a^k b^{n-k}$，对于某个在0和n之间的k值；也就是说，在展开式的每一项中，a和b的幂的和必须是n。三角形中任何一行的数字都是按照a的降幂顺序书写的，因此第一个1是a^n的系数，下一个数字是$a^{n-1}b$的系数，依此类推。

如果我们面对展开$(a+b)^2$，我们会读取帕斯卡三角形的第$n=$行，看到系数应该是1, 2, 1，并且这些分别是a^2, ab, b^2的系数。因此，

$$(a+b)^2 = a^2 + 2ab + b^2$$

我们也可以通过手动展开相当容易地完成。如果我们面临展开 $\left(x^2+2\right)^4$，会怎样呢？这手动展开并不快，所以让我们看看如果我们使用帕斯卡三角形会发生什么。$n=4$ 行

告诉我们$a^4, a^3b, a^2b^2, ab^3, b^4$的系数分别为1, 4, 6, 4, 1，其中$a = x^2$和$b = 2$。因此，我们可以写出

$$\begin{aligned}\left(x^2+2\right)^4 &= 1\cdot\left(x^2\right)^4 + 4\cdot\left(x^2\right)^3\cdot 2 + 6\cdot\left(x^2\right)^2\cdot(2)^2 \\ &\quad + 4\cdot x^2\cdot(2)^3 + 1\cdot(2)^4 \\ &= x^8 + 4\cdot x^6\cdot 2 + 6\cdot x^4\cdot 4 + 4\cdot x^2\cdot 8 + 16 \\ &= x^8 + 8x^6 + 24x^4 + 32x^2 + 16\end{aligned}$$

尝试逐步进行此展开并比较。实际上，帕斯卡三角形的某些非常有趣的性质深深植根于其他数学概念中，这些性质在**combinatorics**领域尤其有用。实际上，我们将在稍后更详细地检查这些性质中的许多！例如，你可能想知道*why*为什么这个程序——添加上面的两个条目——会产生与这种展开因子相对应的条目。当我们讨论**Binomial Theorem**及其相关思想时，我们将证明它是有效的！（如果你好奇，请参阅第8.4.4节。）

Completing the Square

在推导重要结果之前，我们还需要提到一个与多项式相关的技巧。有时，将多项式重写为一个平方项加上一个常数项是有用的，这样我们就可以方便地分离变量和常数。这相当于添加和减去一个特定的项，使得整体上我们对多项式添加了0，但这个项被选择得可以方便地重写多项式的项。这个过程被称为**completing the square**，即我们添加一个项来创建一个平方因子，并通过减去相应数量的项来完成多项式。

让我们用一个例子来尝试这个程序，然后尝试进行推广。从以下多项式开始：{v*}

$$p(x) = x^2 + 8x + 9$$

一个因式分解在这里并不立即明显，所以让我们尝试完成平方。我们希望看到一个像 $(x + a)^2$ 这样的项，因为我们知道 x 的系数是 1，因为多项式有 $1 \cdot x^2$。展开这样的项给出 $x^2 + 2ax + a^2$。由于我们需要出现 $8x$，我们应该使用 $a = 4$。这个展开给出 $x^2 + 8x + 16$，但我们实际上想看到 $+9$ 作为常数项，所以让我们从原始多项式中加上和减去 7:

$$p(x) = x^2 + 8x + 9 + 7 - 7 = (x^2 + 8x + 16) - 7 = (x + 4)^2 - 7$$

这看起来熟悉吗？确切地说，这是一个平方差，我们知道如何

要分解的:

$$\begin{aligned} p(x) = x^2 + 8x + 9 = (x+4)^2 - 7 = (x+4)^2 - \left(\sqrt{7}\right)^2 \\ = \left(x + 4 + \sqrt{7}\right)\left(x + 4 - \sqrt{7}\right) \end{aligned}$$

相应地，此多项式的根为 $x = -4 - \sqrt{7}$ 和 $x = -4 + \sqrt{7}$。

让我们推广！假设我们从形如的二次多项式开始

$$p(x) = ax^2 + bx + c$$

并且，为了完成平方，我们需要添加和减去一个特定的项。我们之前是如何找到这个项的？嗯，像$(rx+s)^2$这样的项的展开得到$r^2x^2 + 2rsx + s^2$，为了使这些系数与原始多项式的系数相匹配，我们看到我们需要$r^2 = a$，所以我们应该使用$r = \sqrt{a}$。（注意，这当然需要$a \geq 0$！如果$a < 0$我们应该怎么办？）然后，为了得到$2rs = b$，我们需要$s = \frac{b}{2r} = \frac{b}{2\sqrt{a}}$。然后，当这个展开时，我们添加了$s^2 = \frac{b^2}{4a}$，所以我们应该从多项式中减去它。

以下步骤在下面执行，进行了一些额外的代数清理，以使项看起来“更漂亮”：Translated Text: 这些步骤在下面执行，进行了一些额外的代数清理，以使项看起来“更漂亮”：{v*}

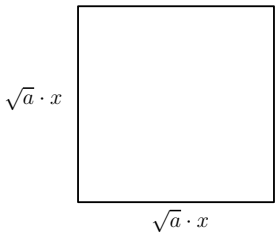
$$\begin{aligned} p(x) = ax^2 + bx + c = ax^2 + bx + \frac{b^2}{4a} + c - \frac{b^2}{4a} \\ = \left(\sqrt{a}x + \frac{b}{2\sqrt{a}}\right)^2 + \left(c - \frac{b^2}{4a}\right) \\ = \left(\sqrt{a} \cdot \left(x + \frac{b}{2a}\right)\right)^2 + \left(c - \frac{b^2}{4a}\right) \\ = a\left(x + \frac{b}{2a}\right)^2 + \left(c - \frac{b^2}{4a}\right) \end{aligned}$$

这现在告诉我们如何完成任何二次多项式的平方！

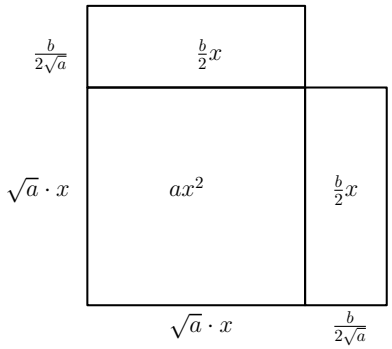
Visualizing Completing the Square

这是一个记住如何进行此过程的有用方法。它基于正方形和矩形面积的可视表示。

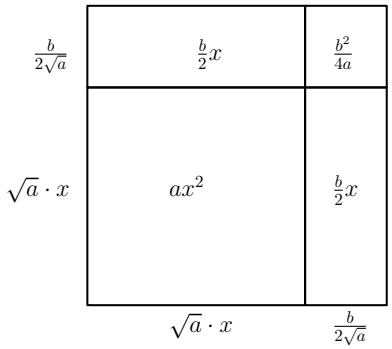
让我们假设 $a, b > 0$，这样我们可以从几何上解释 $ax^2 + bx$ 为矩形的面积。具体来说，让我们将 ax^2 项视为正方形的面积。这意味着每条边的长度为 $\sqrt{a} \cdot x$:



如何表示 bx 项？我们希望把这个正方形建成一个更大的正方形；这就是完成平方的含义。因此，我们应该在这个正方形周围构建一些矩形，这将帮助我们实现这个目标。让我们将 bx 项贡献的面积分成两个矩形，每个矩形的面积都是 $\frac{b}{2}x$。由于我们必须有一边长度为 $\sqrt{a} \cdot x$，并且我们希望总面积为 $\frac{b}{2}x$，那么我们可以看到我们需要另一边的长度为 $\frac{b}{2\sqrt{a}}$：



我们需要添加什么才能使这个图形成为正方形？我们看到右上角只剩下一小块正方形需要填充。每边的长度是 $\frac{b}{2\sqrt{a}}$，所以它的面积——我们需要添加的项——是 $\frac{b^2}{4a}$。



看看这个！这是我们上面通过代数推导得到的相同术语。通过添加这个，我们能够将项因式分解为完全平方。我们只需要确保减去它，这样对原始表达式的净变化为零。

这是一个值得记住的有用技巧。它可以提醒你完成平方的动机过程以及如何实现它。不过，你需要注意一件事：为什么这种视觉表示有效？我们必须假设 $a, b > 0$ 来绘制这些图表，那么为什么通用公式无论 a 和 b 是什么都有效呢？

The Quadratic Formula

让我们回到识别多项式根的问题。具体来说，让我们回忆一下 **quadratic formula**。你可能已经把这个公式当作“解二次方程”的方法来记忆，但你知道它实际上是如何工作的吗？让我们试着弄清楚！一般来说，我们从形式为的二次多项式开始

$$p(x) = ax^2 + bx + c$$

在 $a \neq 0$（否则，它实际上不是二次的），并且我们想要识别 x 的值，使得 $p(x) = 0$。（你尝试回答我们上面关于这种类型的多项式可以有多少个根的问题了吗？在整个以下推导过程中，请记住这些概念。）我们无法轻易地将多项式分解为线性因子，所以让我们利用上面使用的过程：完成平方。这种程序的优点是，我们可以在完成平方后设置 $p(x) = 0$ 并重新排列项来解决 x。观察：

$$0 = p(x) = ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 + \left(c - \frac{b^2}{4a}\right)$$

简化为：

$$\frac{b^2}{4a} - c = a\left(x + \frac{b}{2a}\right)^2$$

现在，我们想要“撤销”这里的进程来解决 x，这需要取两边的平方根。但是，如果 $\frac{b^2}{4a} - c <$ 为 0 呢？我们根本不能取那个平方根！或者，如果 $\frac{b^2}{4a} - c =$ 为 0 呢？这是问题吗？当 $\frac{b^2}{4a} - c >$ 为 0 时，我们有什么要担心的吗？这些问题与我们之前关于多项式可能有多少个根的问题有关。你可能已经推断出（正确地）一个二次多项式可以有 *at most* 两个根，但在这里我们发现了一个可能性（以及原因），即二次多项式可能有一个或零个根！

- 在 $\frac{b^2}{4a} - c <$ 为 0 的情况下，*no* 的 x 值可能满足上述推导中的最后一行。因此，在实数集中不存在 $p(x)$ 的根。

- 在 $\frac{b^2}{4a} - c =$ 为 0 的情况下，对上面最后一行的两边取平方根是完全有效的，但它会产生 *exactly one* 值

x 的:

$$\begin{aligned}\frac{b^2}{4a} - c = 0 &= a\left(x + \frac{b}{2a}\right)^2 \\ 0 &= x + \frac{b}{2a} \\ x &= -\frac{b}{2a}\end{aligned}$$

剩余的情况是当 $\frac{b^2}{4a} - c > 0$。在这种情况下，我们可以预期 two 个 $p(x)$ 的根，因为对两边取平方根引入了两个可能的解。一般来说，当我们有类似 $s^2 = t$ 的情况时，我们可以说唯一的可能解是 $s = \sqrt{t}$ 和 $s = -\sqrt{t}$，但我们必须考虑两者（我们通常写成 $s = \pm\sqrt{t}$）。在这种情况下求解 x 得到

$$\begin{aligned}\frac{b^2}{4a} - c &= a\left(x + \frac{b}{2a}\right)^2 \\ \pm\sqrt{\frac{b^2 - 4ac}{4a}} &= \sqrt{a}\left(x + \frac{b}{2a}\right) = \sqrt{a}x + \frac{b}{2\sqrt{a}} \\ -\frac{b}{2\sqrt{a}} \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a}} &= \sqrt{a}x \\ -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} &= x\end{aligned}$$

现在，我们需要注意之前做的平方根观察。一般来说，$\sqrt{4a^2} = \pm 2a$，但我们已经知道涉及该平方根的分数项已经有一个相关的 ± 1 因子，所以这个因子不会改变它。因此，我们可以得出结论

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Voilà，二次公式!

记住，推导的最后一步是在假设 $\frac{b^2}{4a} - c > 0$ 的情况下进行的。当 $\frac{b^2}{4a} - c = 0$ 时，这个公式仍然适用吗？我们能否在那种假设下执行上面立即进行的相同步骤？为什么或为什么不?

Problems

Problem 1.3.5. 找出所有可能的 a 值，使得 $x-a$ 是 $x^2+2ax-3$ 的因数。

Problem 1.3.6. 找出所有可能的 b 值，使得 $x^3 + b$ 能被 $x + b$ 整除，且没有余数。

Problem 1.3.7. 因子 $x^n - 1$ 对于任何自然数 n。

Problem 1.3.8. 确定由 x 定义的价值

$$x = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots}}}}$$

Hint尝试使用 x 及其自身来表示无限嵌套的平方根。

Problem 1.3.9. 使用配方法证明一个正数 n 和它的倒数之和总是大于或等于2，并且唯一使和等于2的数是 $n = 1$。

Hint取和，加2减2，并重新排列。

Problem 1.3.10. 我们如何找到形如 $ax^4 + bx^2 + c$ 的四次多项式的根?

1.3.4 Let's Talk About Sets

我们已经提到了一些特定的数字类型，但我们要特别定义我们将在未来使用的数字集合。这些数字集合中的每一个都由 `blackboard bold` 字体中的特定字母表示。**natural numbers** (，也称为整数或计数数)，之所以被称为“自然”，是因为当我们开始计数物体时，它们听起来“自然”。我们可以写出

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

(存在一个更具体和技术的定义，我们将在稍后解释。) 我们用 $\mathbb{N}$ 来表示“自然”。

使用 $\mathbb{N}$，我们可以定义一个相关的数字集合：所有 **inte- gers** 的集合，它结合了自然数、0 和负自然数。我们可以写成

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

信件 $\mathbb{Z}$ 来自德语单词 *Zahlen*，意为“数字”。

从这个集合中，我们可以定义集合 **rational numbers**。这些数字可以用整数比表示，但它们似乎没有像 $\mathbb{N}$ 和 $\mathbb{Z}$ 这样的自然“列表”，因此我们无法以上述方式写出这个集合。为此，我们使用一个非常常见的集合表示法，如下所示：

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

我们将其读作：

> 有理数集是所有形式为 $\frac{a}{b}$ 的数的集合，其中 a 和 b 都是整数，且 b 不为零。

这传达了有理数是一个分数的必要信息，其中分子和分母是整数（但分母不能

因为除以0是不允许的，所以b等于0。我们使用字母$\mathbb{Q}$表示有理数的原因是$\mathbb{R}$已经被保留用于*real*数，而$\mathbb{Q}$是下一个可用的字母。此外，$\mathbb{Q}$包含所有整数的*quotients*，这也很有道理！

real numbers $\mathbb{R}$有一个非常技术性的定义，我们很遗憾地无法在这本书中完全深入探讨。（这正好说明了数学上定义该集合是多么困难！）目前，一种思考实数的方法是通过一个**number line**。实数是所有位于直线上的数，而$\mathbb{N}, \mathbb{Z}$和$\mathbb{Q}$的数是位于直线上的特定数，但它们并不构成直线的全部。从某种意义上说，$\mathbb{R}$是$\mathbb{Q}$的“完善”，即在有理数之间“填补空缺”。

1.3.5 Notation Station

一个流行的方便的写和积的方法是使用简化的符号，将许多项或因子收集到一个共同的形式中。例如，如果我们想谈论前500个自然数的和呢？写出所有500项的和会很麻烦，所以通常写成类似$1 + 2 + 3 + \cdots + 499 + 500$的形式。（实际上，我们已经使用了这样的省略号。你明白我们的意思了吗？）这种方法很流行，确实能传达要点，但一些数学家对中间不必要的省略号使用表示反感。我们推迟讨论这个问题直到现在，因为通常情况下**notation**可能难以学习和理解。我们不是一开始就向你轰炸新的符号，而是诉诸于我们对“...”能完成什么的直观理解。

现在，既然我们已经提到了这一点，让我们看看如何避免使用省略号。要写出我们上面提到的和，我们会使用以下符号：

$$1 + 2 + 3 + \cdots + 499 + 500 = \sum_{i=1}^{500} i$$

大西格玛 $\sum$ 来自于代表“和”的希腊字母S，而 **index** i 告诉我们要找到和的各个项的值。在 $\sum$ 符号下方写1，上方写500，意味着我们让 i 假设所有介于1和500（包括）之间的自然数。使用这些值，我们将它们代入项的一般表达式，在这种情况下就是 i。因此，我们发现项是$1, 2, 3, \ldots, 500$，正如所期望的那样。尝试通过改变项的一般表达式和/或索引的值来找到写这个和的几种其他方法。如果我们想找到前500个偶数自然数的和呢？关于（包括）500的所有偶数自然数呢？尝试用上面的符号风格写出这些和。

与此相关的是 $\prod$ 符号。如果我们想查看前500个自然数的乘积，我们将遵循相同的识别约定

索引和通项的值:

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot 499 \cdot 500 = \prod_{i=1}^{500} i$$

大π ∏ 来自于对应于 P 的希腊字母，表示“乘积”。再次，尝试用不同的方式表达，通过改变通项和/或索引值。如果我们想找到前500个 $even$ 自然数的乘积呢？又或者所有偶数自然数 $up\ to$ (以及包括) 500 的乘积呢？尝试用上述的符号风格写出这些乘积。

Problems

Problem 1.3.11. 编写一个英文句子，描述以下方程的含义:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Problem 1.3.12. 表达，用适当的符号，从$2^0 =$ 开始的2的n 次幂的和与积。你能证明这个公式吗？积的公式?

Problem 1.3.13. 考虑17和33（含）之间所有奇数的和。用求和符号表示这个和，其中索引从0开始。现在尝试将其索引从1开始写。现在尝试将其索引从8开始写，然后再从9开始写。哪一个感觉“更自然”？ 为什么?

1.4 Quizzical Puzzicles

让我们将迄今为止讨论的一些原则付诸实践。具体来说，让我们考察一些有趣的数学谜题，并解释如何解决它们。这些谜题都不需要了解超出基础代数和算术的知识，但这并不意味着它们是“基础”或“简单”，因为它们都涉及批判性思维技能和敏锐的洞察力来解决和理解。在这个过程中，我们将运用我们已经提出的一些逻辑思想。我们可能需要处理多项式函数，或者用代数方法解一些方程。我们可能需要仔细思考我们论点的顺序和流程，确保一切都能从先前的知识或推论中得出。总的来说，我们也应该思考构成我们所发现事实的良好和有效 *proof* 的要素!

1.4.1 Funny Money

Problem Statement

这个经典谜题包含在一个关于一些朋友支付共享酒店房间费用的故事中:

三位朋友在深夜的一次旅行中在一家酒店停下，想找个房间休息一下。当值的职员说当晚只有一个房间空着，三个人一起住需要支付30美元。朋友们决定他们急需睡眠，同意平分房间，每人把10美元放在柜台上预付。职员感谢他们，递给他们钥匙，他们就去车里拿行李。与此同时，另一位职员出现在现场开始他的班次，并意识到之前的职员犯了一个错误，多收了三位朋友房费：实际上只需25美元。他从收银机里拿出5美元，递给当值的行李员，说：“把这个带给29号房间。那里的客人被多收了费。”行李员点头，然后前往他们的房间。当三位朋友开门时，他们惊讶而高兴地发现他们得到了退款。为了公平分配钱，一位朋友用五张1美元的纸币找零，然后每人拿1美元，剩下的2美元作为小费给了行李员。行李员友好地感谢他们，然后回去工作。

现在，三个朋友每人向房间贡献了9美元，再加上2美元的小费，总共29美元。但他们原本给了收银员30美元... 那丢失的1美元去哪了？！

仔细思考这个问题，然后再翻页阅读我们的解决方案。

Solution: Keeping Careful Track of the Money

你弄懂了吗？你意识到实际上根本没有什么“缺失”的吗？这个谜题旨在迷惑读者，并误导他们去寻找实际上并不存在的东西。所涉及的数字被选择得如此之小，以至于读者会认为发生了某种神秘的事情，但仔细和逻辑的分析事件应该会让你意识到，最后的提问实际上并不公平；它是基于对情况的误解，而试图忽略其推理是解开这个谜题的关键。当数字被大幅度改变，以至于最终差异的值要大得多时，读者就不再有那种情感投资去寻找那个“缺失的一美元”。

首先，让我们分析一下在这个特定案例中实际上发生了什么。关键是仔细解释钱实际上流向了哪里。忘记涉及的个人，考虑两个不同的实体有助于思考：我们称之为 F 的朋友圈，以及我们称之为 H 的酒店服务员/门童组合。现在，让我们回顾故事中的步骤，并描述在每一步中钱从何而来以及去向何方：

(1) F 到达并给 H（房间原始成本 $30

(2) H退还$5给$F$ (退款超收) (3) F退还$2给$H$（给行李员的小费) (4)净变化：$F$退还$30-$5+$2=$27给$H$

现在更有意义了，不是吗？退款是5美元，所以房间实际上花费了25美元，说三个朋友每人付了9美元是不合理的，还要加上给行李员的的小费。他们三人共贡献的27美元$includes$包括了小费。故事之后的问题暗示我们应该$adding$将小费算在朋友们的贡献里，但实际上，小费是他们贡献的一部分。通过将朋友们和行李员/职员放在一起，我们实际上可以追踪资金的流动。

Generalizing: Changing The Numbers

让我们以上述提到的方式改变问题；具体来说，让我们尝试改变问题的数字，以消除对“丢失的美元”的情感依恋，并使差异更大。首先，我们将定义一些变量来表示上述步骤中使用的美元金额。我们可以尝试通过“测试”这些美元金额的特定值来看会发生什么，但通过引入变量并在稍后为它们替换特定值，基本上“一次尝试所有事情”会更有效率。

我们将用$3n$表示酒店房间的原始成本（三位朋友首次到达时支付的金额），对于某个n的值。我们选择这样做是因为我们希望成本由朋友们平均分担。接下来，我们希望

为了定义一个变量来表示他们收到的退款。知道他们想要将这笔金额平均分给三个人，并留一些小费给行李员，让我们假设退款的形式为$3r+2$。变量r代表每个朋友从酒店单独收到的金额，而2代表给行李员的小费。现在，让我们用这些变量而不是原始值来重新表述这个谜题。

> 三位朋友在深夜的一次旅行中在一家酒店停下，想找个房间休息一下。当值的职员说，当晚只有一个房间空着，三个人一起住需要支付$3n$美元。朋友们决定他们急需睡眠，同意平摊房间费用，每人将$\$n$放在柜台上预付。职员感谢他们，递给他们钥匙，他们去车里拿行李。与此同时，另一位职员出现，开始他的班次，意识到之前的职员犯了一个错误，多收了三位朋友房费：实际上应该是$3n-(3r+2)$美元。他从收银机里取出$3r+2$美元，交给当值的行李员，说：“把这个带给29号房间。那里的客人被多收了费。”行李员点头，前往他们的房间。当三位朋友开门时，他们惊讶而高兴地发现他们得到了退款。为了公平分配钱，每位朋友拿$\$r$，剩下的2美元作为小费给了行李员。行李员友好地感谢他们，然后回去工作。
>
> 现在，三个朋友每人向房间贡献了 $\$n-r\$$，再加上2美元的小费，总共是 $\$3(n-r)+2\$$。但他们原本给了服务员 $\$3n\ldots\$$，那3美元去哪了？$[3(n-r)+2]=\$3r-2$？！

你现在看到发生了什么吗？差异发生，正如我们之前解释的，因为这个问题考虑了*adding*的$2小费作为退还的房间费用，并将其与$3n$的原始成本进行比较。实际的比较应该是朋友退还的贡献，即$\$3(n-r)=\$3n-3r$，以及退还的房间费用和小费的总和，即$\$3n-(3r+2)+2=\$3n-3r$。那里没有差异！

Generalizing: Questions For You

在谜题的原表述中，数值是 $n=10$ 和 $r=1$，因此“缺失的金额”神奇地变成了 $\$3r-2=\$1$。如果我们选择了更大的数值——比如说 $n=100$ 和 $r=10$——那么实际的 $300 房间实际上应该花费 $268，行李员会给朋友们 $32，他们每人会拿走 $10，他会保留 $2，差异变成了 $28。有人真的会相信在这笔交易中丢失了 $28 吗？如果我们使用更大数值的 n 和 r 呢？差异可以有多大？有多小？给定

期望的差额（美元），你能找到n和r的值来实现这个差额吗？有多少种方法可以实现？

Lessons From This Puzzle

逻辑和理性思维在解决谜题时很重要，因为有时很容易被情绪所误导。如果我们最初将谜题表述为“丢失28美元的问题”，你会以同样的方式反应吗？在尝试回溯并发现真正发生的事情之前，你会不会感到暂时困惑？

1.4.2 Gauss in the House

Problem Statement

有一个在数学家之间广为流传的轶事，可能或可能不是伪史，但我们中的一些人愿意相信它是真实的，因为它涉及到了有史以来最伟大的数学家/物理学家之一，卡尔·弗里德里希·高斯。他在18世纪末和19世纪初到中期工作，并在广泛的领域证明了基本而强大的结果。他研究数论、复变函数、光学、几何学、天文学等等！阅读下面的故事，思考你会在那种情况下做什么——作为一个小孩和现在——然后继续阅读以进行讨论。

> 早上很早，在一间小学教室里，学生们很吵闹，让老师感到非常沮丧，他感到非常累，字面上，对他们的行为感到非常累。他需要一种方法让他们暂时忙碌起来，这样他就可以在办公桌旁放松并恢复体力。他大声喊道，让他们拿出石板和粉笔。经过几次催促，每个人都照做了。然后他告诉他们把从1到100的所有数字加起来，第一个做到的人将获得当天的老师助手的特权。他回到办公桌前坐下，松了一口气，因为他们将会花很长时间进行大数计算。然而，仅仅一分钟过后，一个男孩走到办公桌前，向老师展示了他石板上的答案。老师惊讶了，不得不花几分钟时间自己进行计算来检查答案，但最终，这个小男孩是正确的，他这么快就完成了这个壮举。他是怎么做到的？

仔细思考这个问题，然后再翻页阅读我们的解决方案。记住，这个故事“发生”在计算器出现之前，所以你只能使用你的大脑、铅笔和纸。

Solution: Reducing Computations

也许你已经想明白了这个问题。实际上，有几种不同的方法来解决这个问题，但它们基本上都归结于同样的洞察：尝试减少所需的计算量。

简单地逐个将这100个数加到之前得到的和中，需要99次加法，涉及的数字越来越大。当然，这里的技巧不仅仅是比其他人更快地完成这些加法，而是要更高效地完成所需的计算。记住，乘法可以看作是一个数对自己重复相加，所以也许我们可以将这些所有的加法都减少到一次乘法，前提是我们找到正确的数，让它不断地对自己相加。

另一个需要记住的重要事实是，加法是 **associative** 和 **commutative**，这意味着我们可以以任何顺序进行加法，并确保我们得到相同的答案。具体来说，我们可以将所有从100到1的数字相加，并得到相同的总和，称之为 S。让我们以方便的方式在这里写下这个事实：

$$\begin{array}{ccccccccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & 98 & + & 99 & + & 100 & = & S \\ 100 & + & 99 & + & 98 & + & \cdots & + & 3 & + & 2 & + & 1 & = & S \\ \hline 101 & + & 101 & + & 101 & + & \cdots & + & 101 & + & 101 & + & 101 & = & 2S \end{array}$$

注意，我们已经以两种不同的方式写下了所需的和，逐项相加这两个和，并得到了$2S$的表达式，即所需和的两倍。这个新表达式可以写成乘法，因为这里有100个项，每个项都是数字101。因此，

$$2S = 101 \cdot 100 \quad \text{and therefore,} \quad S = 101 \cdot 50 = 5050$$

这比进行99次加法运算要快得多，实际上，如果我们仔细思考，我们可能能够在脑海中完成整个过程！

Alternate Solution: Pairing Terms

现在，看待这个问题的另一种非常相似的方法是跳过添加上面我们写的两条线，只需将原始求和中的数字配对，如下所示：

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 98 + 99 + 100 \\ &= (1 + 100) + (2 + 99) + (3 + 98) + \cdots + (49 + 52) + (50 + 51) \\ &= 101 + 101 + \cdots + 101 = 50 \cdot 101 = 5050 \end{aligned}$$

这种方法本质上等同于我们上面描述的方法；它仍然利用加法的结合性质将求和转换为乘法，只是跳过了我们找到$2S$的表达式然后除以两步的中间步骤。

Generalizing: Even n

如果老师要求他的学生把从1加到1000的数字相加，他们会抗议吗？高斯能否像那样快速找到答案？你会怎么做？我们不确定前两个问题的答案，但我们认为你同样可以轻松地处理这个求和问题。这里唯一不同的是，我们将创建的配对数量将是500（而不是50），并且每一对的总和将是1001（而不是101），因此结果将是

$$1 + 2 + 3 + \cdots + 998 + 999 + 1000 = 1001 \cdot 500 = 500500$$

看起来那里有一个模式吗？你认为你能立刻说出从1到100万的数字总和，而不进行乘法运算吗？

Generalizing: Odd n

如果老师要求计算前99个数的和呢？配对过程还会起作用吗？让我们看看：

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 97 + 98 + 99 \\ &= (1 + 99) + (2 + 98) + (3 + 97) + \cdots + (48 + 52) + (49 + 51) + 50 \\ &= (49 \cdot 100) + 50 = 4950 \end{aligned}$$

注意我们总共有 *odd* 个项，所以不能配对每个数字，不得不将乘积的结果加上50。我们能否以不同的方式配对数字？

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 97 + 98 + 99 \\ &= (1 + 98) + (2 + 97) + (3 + 96) + \cdots + (48 + 51) + (49 + 50) + 99 \\ &= (49 \cdot 99) + 99 = 50 \cdot 99 = 4950 \end{aligned}$$

这 *seems* 更接近原始谜题的结果，因为我们最终执行了 *one* 乘法。这现在可能看起来像是一种奇怪的巧合，但试着用一些其他的奇数和按照上面的步骤进行。前7个整数的和是多少？前29个？前999个？前999999个？

Generalizing: Any n

让我们从我们在这里考察的个别案例中退一步，尝试更一般性地解决这个问题。让我们假设老师向学生提出了以下问题：

> 找到一个公式来求前 n 个数的和。我希望一个 *specific* 公式，这样如果有人告诉我 n 是什么，我可以通过插入那个特定的值来快速找到答案。

第二句话的注意事项排除了我们上面调查给出的形式解决方案。我们已经有了一些简单的 *algorithms* 来寻找这个问题的解决方案，但现在我们被要求找到一个 *forumla*，它将产生一个解决方案。我们如何开始着手解决这个问题呢？好吧，基于我们上面做出的某些观察，通过分别处理 n 为偶数和 n 为奇数的情况来解决这个问题是有意义的。我们看到在这些情况下配对略有不同，所以让我们先研究一个，然后再研究另一个。在每种情况下，我们都在寻找 $S(n)$ 的公式，即由 $1+2+3+\cdots+(n-2)+(n-1)+n$ 表示的和。我们使用这个新的符号 $S(n)$ 来表示在 n 的特定值上的和 *depends*。

如果 n 是偶数，我们知道我们可以配对每个数字，没有剩余项：

$$\begin{aligned} S(n) &= 1+2+3+\cdots+\left(\frac{n}{2}-1\right)+\frac{n}{2}+\left(\frac{n}{2}+1\right)+\cdots \\ &\quad +(n-2)+(n-1)+n \\ &= (1+n)+(2+(n-1))+(3+(n-2))+\cdots \\ &\quad +\left(\left(\frac{n}{2}-1\right)+\left(\frac{n}{2}+2\right)\right)+\left(\left(\frac{n}{2}\right)+\left(\frac{n}{2}+1\right)\right) \\ &= (n+1)\cdot\frac{n}{2}=\frac{n^2+n}{2} \end{aligned}$$

尝试使用我们上面考察的 n 的某些偶数值（如100、1000、1000000等）来使用这个公式。它有效，不是吗？请注意，我们之所以可以写出涉及 $\frac{n}{2}$ 的项并确信它们是总和的一部分，是因为 n 是 *even*，所以 $\frac{n}{2}$ 也是一个整数。

好的，现在假设 n 是奇数会发生什么？我们知道我们无法配对每个数字，所以我们需要在这里做得更聪明。记得我们求前99个数的和的方法吗？通过省略和的最后一项，我们可以将所有其他项配对，没有任何剩余，而且每一对的总和都等于那个最后的数字 *same value*。让我们尝试在这里使用那种方法：

$$\begin{aligned} S(n) &= 1+2+3+\cdots+\left(\frac{n-1}{2}-1\right)+\frac{n-1}{2}+\left(\frac{n-1}{2}+1\right)+\cdots \\ &\quad +(n-2)+(n-1)+n \\ &= (1+(n-1))+(2+(n-2))+\cdots+\left(\left(\frac{n-1}{2}\right)+\left(\frac{n-1}{2}+1\right)\right)+n \\ &= n+n+\cdots+\left(\frac{2n-2}{2}+1\right)+n=(n+n+\cdots+n)+n \end{aligned}$$

这表明每一对术语的总和为 n，这是我们配对过程之前移除的最终数字。现在，让我们仔细思考我们有多少对 *many*。注意，我们可以通过查看每一对的第一数字来编号：第一对是 $(1, n-1)$，第二对是 $(2, n-2)$，以此类推，最后一对的第一数字是 $\frac{n-1}{2}$。因此，我们有

确切地有那么多对：$\frac{n-1}{2}$。记住n是奇数，所以我们有信心$n-1$是偶数，因此$\frac{n-1}{2}$是一个整数。我们并没有每次都提到这一点，所以请务必回顾我们迄今为止所做的一切，并确信我们写的每一步和每个项都是有效的。对于这些对，我们在它们后面添加了一个最终的数字n，因此我们可以将求和的乘法写成以下形式：

$$S(n) = \left(\frac{n-1}{2} + 1\right) \cdot n = \left(\frac{n-1}{2} + \frac{2}{2}\right) \cdot n = \frac{n+1}{2} \cdot n = \frac{n^2+n}{2}$$

哇，这正是我们在 n 为偶数时找到的相同公式！这让你感到惊讶吗？我们最终得到相同的公式并不明显，即使我们的解题方法相似。这对你有什么启示？一个数学家会看到这样的“巧合”并想知道是否有一条更 *simpler* 和 *direct* 的路线到达这个结果；也就是说，我们能否以某种方式解决这个问题，同时回答 *both* 奇数和偶数的情况？既然我们得到了相同的答案，可能存在一种方法可以实现这一点。在继续阅读之前，请花一分钟时间思考一下。

Generalizing: Any n, *without* separate cases

结果显示，我们在之前对这个谜题的讨论中已经暗示了这种方法。记得我们当时把求和向前写在第一行，向后写在另一行，然后把它们加在一起吗？当我们处理这里的奇偶情况时，我们决定避免那种方法，因为它似乎增加了几个额外的步骤；“配对项”的过程似乎更快，所以我们遵循了那个方法。如果我们回过头来重新审视“两次求和”的方法呢？我们会发现类似以下的内容：

$$\begin{array}{ccccccccccc} 1 & + & 2 & + & \cdots & + & (n-1) & + & n & = & S(n) \\ n & + & (n-1) & + & \cdots & + & 2 & + & 1 & = & S(n) \\ \hline (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) & = & 2S(n) \end{array}$$

在这种情况下，我们在第三行的和中具有 n 项，每一项是 $(n+1)$。因此，

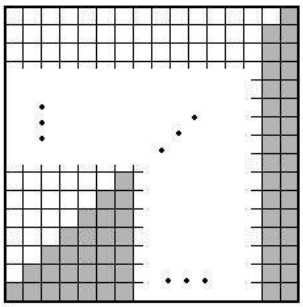
$$(n+1) \cdot n = 2S(n) \quad \text{and therefore,} \quad S(n) = \frac{1}{2}(n+1) \cdot n = \frac{n^2+n}{2}$$

这是我们已经获得的公式，我们发现它在这里的方式不依赖于n是奇数还是偶数！（回顾我们刚才执行的步骤，并亲自验证n的奇偶性确实无关紧要。）

Alternate Solution: Visual Diagram

在我们结束这个谜题之前，我们想提及一种解决这个问题的几何方法。我们将把和 $S(n)$ 与一个正方形的面积联系起来，并找到一种方法

绘制求和公式（$1, 2, 3, \ldots, n-1, n$）的各个项作为正方形面积的组成部分。具体来说，让我们考虑一个 $n \times n$ 正方形，并将求和公式的各项绘制为高度递增的矩形，每个矩形的宽度为1个单位。请参见下面的图片：



现在，要求一个得到和 $S(n)$ 的公式等同于询问所有我们在方形内画出的矩形覆盖了什么 *area*。试图将各个面积加起来只是重申了谜题，因此我们需要想一种方法将这个面积与方形的总面积联系起来。为此，让我们考虑剩余的部分；也就是说，我们如何描述被矩形覆盖的方形面积 *not*? 看看严格位于第一个 1 $\times$ 1 矩形上方的面积：它也是一个矩形，尺寸为 $(n-1) \times 1$。

查看2 $\times$ 1矩形上方的区域：它是一个$(n-2) \times 1$矩形。这种模式继续！最终，我们在$(n-1) \times 1$矩形上方有一个1 $\times$ 1矩形，然后最后一个$n \times 1$矩形上方没有区域。所有这些矩形的总面积是多少？嗯，它看起来很像我们正在考虑的求和$S(n)$，但它只是缺少最后一个项，n。现在，我们可以通过将它们与$S(n)$相关联，然后与正方形的面积相关联来求出所有矩形的面积：

$$n^2 = S(n) + (S(n) - n) = 2S(n) - n$$

因此，

$$S(n) = \frac{n^2 + n}{2}$$

之前我们有的相同公式！

Lessons From This Puzzle

有时，解决谜题的方法有几种完全合理的途径，并获得解决方案。其中一些可能首先出现在脑海中，但执行起来需要更长的时间，一些可能更难找到，但更容易找到解决方案，或者一些可能根本走不通！通常很难事先知道任何特定方法会发生什么，所以只需开始尝试解决谜题，看看会发生什么，并记录下你所做的

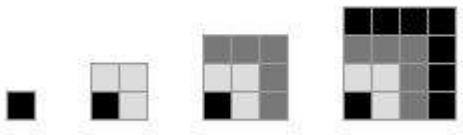
尝试过并发生了什么，这样你可以在以后重新评估这种方法。这是我们随着数学生涯的推进需要记住的事实。我们不可能总是立即知道该做什么。有时我们难免会遇到困境，或者尝试最终成为死胡同的道路。这不应该让人气馁；这只是事情本来的样子！

作为一个子谜题，尝试重新做奇数 n 情况下的“配对项”，但不是省略求和的最后一项，而是尝试分离中间项，并从外侧向内侧配对数字。这给你同样的结果吗？这看起来是否比我们使用的方法更容易/更快/不同？或者，如果我们通过说 $n = 2k$ 对于某个数字 k 来处理偶数 n 情况，我们会怎么做奇数 n？这种符号是否改变了程序？这使它更容易处理吗？现在，你能想到任何完全不同的方法来解决这个问题吗？

1.4.3 Some Other Sums

Summing Odd Numbers: Observing a Pattern

当我们在讨论评估整数和的话题时，让我们看看一些相关的问题。首先，我们将探讨一种有趣的几何方法来解释 *odd* 整数的和：让我们将 1 表示为一个 1×1 块，然后每个依次更大的奇数作为一个 1×1 块的直角角落，这个角落完美地围绕前一个这样的图形。我们为什么要这样做呢？嗯，因为这些全是奇数，连续项的大小相差两个，每次将角落块的一边加长一个，使我们能够紧密地围绕彼此放置角落，并依次构建更大的正方形！



这个模式会继续吗？如果我们相信它会，我们如何证明这样的事情？这个几何模式在数值总和方面意味着什么？这是一个很好的问题，首先要回答，因为尽管几何模式很漂亮，但它很难处理和操作，最终，*prove*明显如此。本质上，指出模式的最初几个项并说，“看，它起作用了！”这难道构成一个正式的、数学上的证明吗？因此，我们必须找到一种更好的方式来制定这个问题。这并不是要贬低我们注意到的模式的含义和美丽；它确实以那种方式起作用，并且确实为我们提供了对可能正在数学上发生的事情的一些有价值的见解，但最终，这就是它能为我们做的所有事情。

Summing Odd Numbers: Proving Our Findings

让我们尝试用数值术语写出上面图中表示的求和。角落的部件由1 × 1块组成，每个角落比前一个多两个块，因此我们看到的每个正方形图形都由如下求和表示

$$1 \quad \text{or} \quad 1+3 \quad \text{or} \quad 1+3+5 \quad \text{or} \quad 1+3+5+7$$

等等。我们从这些项中注意到，确实，它们的和是平方数:

$$1 = 1^2 \qquad 1+3 = 4 = 2^2 \qquad 1+3+5 = 9 = 3^2 \qquad 1+3+5+7 = 16 = 4^2$$

This 这是我们要证明的真正模式；它与我们之前注意到的几何模式等价，但现在是以我们可以操作的方式来表达的。让我们现在思考一下我们如何做到这一点。这个模式与之前见过的任何东西相似吗？我们是否证明了关于整数和的任何结果？当然！回顾之前的谜题；我们实际上证明了（实际上是以几种方式证明了）

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

这可能在这个谜题中有什么用？我们证明的求和公式涉及从1到n的*all*个连续整数，但对于当前所需的公式，我们只想考虑连续的*odd*个整数。

之前，我们使用函数 $S(n)$ 来表示前 n 个自然数的和，所以让我们定义一个函数 $T(n)$ 来表示前 n 个奇数自然数的和。现在，我们首先需要确定这个和的项，然后将它们与 $S(n)$ 以某种方式联系起来。下面，我们已将 $n = 1, 2, 3$ 和 4 的和写出来。你能找到一种方法来识别这个和中的最大项，并用 n 来表示它吗？

$$n=1: \quad 1, \quad n=2: \quad 1+3, \quad n=3: \quad 1+3+5, \quad n=4: \quad 1+3+5+7$$

注意，和的最后一项总是$2n-1$。这与一个一般事实有关，即任何 *even* 整数都可以表示为$2k$，对于某个特定的整数 k，任何 *odd* 整数都可以表示为$2n-1$，对于某个特定的整数 n。（我们也可以将奇数表示为某个整数$2n+1$，对吧？在这个上下文中，使用$2n-1$形式更方便。）因此，我们想要找到一个公式来表示前 n 个奇自然数的和，给定如下

$$T(n) = 1+3+5+7+\cdots+(2n-3)+(2n-1)$$

我们可以将这个和与$S(n)$或类似的东西联系起来吗？嗯，注意这个和

$$S(2n) = 1+2+3+\cdots+(2n-3)+(2n-2)+(2n-1)+2n$$

包含从1到2n的自然数中的*all*，而$T(n)$只包含该范围内的奇数自然数。也许从这两个和中减去，并尝试找到一个剩余项之和的表达式是有意义的：

$$\begin{aligned} S(2n) - T(n) &= \big(1 + 2 + 3 + \cdots + (2n-1) + 2n\big) \\ &\quad - \big(1 + 3 + 5 + \cdots + (2n-3) + (2n-1)\big) \\ &= 2 + 4 + 6 + \cdots + (2n-2) + 2n \end{aligned}$$

这些术语都是从2到2n的所有*even*自然数。我们如何找到一个这个和的公式？我们需要做额外的工作吗，或者我们可以应用一个之前证明的结果？嗯，因为所有的项都是*even*，我们可以将所有东西除以2并写为

$$\begin{aligned} \frac{1}{2}\left(S(2n) - T(n)\right) &= \frac{1}{2}\big(2 + 4 + 6 + \cdots + (2n-2) + 2n\big) \\ &= 1 + 2 + 3 + \cdots + (n-1) + n = S(n) \end{aligned}$$

我们确实可以保证右侧求和中的所有项都是整数。不仅如此，它们是连续整数从1到n的*all*，而且我们还有一个求这个和的公式！现在，
everything is written in terms of formulas we already know，即$S(n)$和$S(2n)$，以及我们正在寻找的一个公式，即$T(n)$。现在的最后一步是将方程重新排列以隔离$T(n)$，然后代入我们关于涉及S的公式的已知信息：

$$\begin{aligned} \frac{1}{2}\left(S(2n) - T(n)\right) &= S(n) \\ S(2n) - T(n) &= 2S(n) \\ S(2n) - 2S(n) &= T(n) \\ \frac{(2n)^2 + 2n}{2} - \frac{2 \cdot (n^2 + n)}{2} &= T(n) \\ \frac{4n^2 + 2n - 2n^2 - 2n}{2} &= T(n) \\ \frac{2n^2}{2} &= T(n) \\ n^2 &= T(n) \end{aligned}$$

这个看起来相当不错，不是吗？尽管我们需要通过一些代数步骤来解决问题，但我们得出了我们希望证明的一个结论：连续奇数之和是一个完全平方数。不仅如此，我们还成功地证明了那个平方数与求和项数之间的关系。具体来说，总结我们刚刚证明的结果的简洁方式是可以说“前n个奇数之和是n^2。”

Alternate Solution: An Inductive Argument

我们能否用另一种方式证明这一点？如果我们还没有证明上一节的结果，或者我们没有想到以那种方式使用它呢？我们是否能够利用我们最初注意到的求和的几何结构呢？

让我们以稍微不同的方式回顾并思考这个问题。具体来说，让我们看看为什么在求和中添加一个额外的项会产生另一个平方数。假设我们已经知道其中一个求和产生了平方数；我们知道这是对第一个求和（$1 = 1^2$）成立的，但让我们假设这发生在一些任意数量的项上，n。也就是说，让我们假设*assume*

$$1 + 3 + 5 + \cdots + (2n - 3) + (2n - 1) = n^2$$

对于某个值 n。给定这个事实，我们接下来可以推断出关于下一个和的什么？当我们向和中添加一个额外的项时，我们添加下一个奇数整数，$2n + 1$，那么让我们看看这如何影响和的值：

$$1 + 3 + 5 + \cdots + (2n - 3) + (2n - 1) + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$$

这似乎证实了我们的信念，不是吗？知道一个和的行为方式符合我们的预期（“如果前n个奇数的和是n^2...”）使我们能够推断下一个和必须*also*以相同的方式行为（“...那么前$n+$个1的奇数的和是$((n + 1)^2)$”）。这也证明了结果吗？你怎么想？这感觉奇怪吗？我们本质上是在假设我们的结果来进一步证明关于它的东西？我们真的就是这样做的吗？

这个证明策略，使用结果的一种形式来证明关于“后续”形式的结果，被称为 **mathematical induction**。（一般来说，“后续”一词的含义取决于上下文；在这里，它指的是下一个包含一个额外项的求和。）我们将在下一章更详细地考察这种策略。现在，我们将指出，这是一个完全合理的策略，但它高度依赖于 *first* 求和的行为是否适当：$1 = 1^2$。这样，我们之前所做的努力使我们能够推断出第二个求和的行为是这样的（$1 + 3 = 2^2$），然后我们可以推断出第三个求和的行为是这样的（$1 + 3 + 5 = 3^2$），依此类推... 如果我们只能证明第二部分，但第一个求和没有按照我们想要的方式工作呢？我们还能证明这个结果吗？这对你关于归纳策略的一般性有什么启示？我们将在稍后更普遍地解决这些问题。

Generalizing: Arithmetic Series

一个我们想要提到的最终求和问题与迄今为止我们看到的两个问题密切相关，实际上，如果我们首先证明了下一个结果，我们就不必再对前两个结果做任何事情了！从这个意义上说，这个下一个结果比前两个更重要：这个结果的正确性比前两个结果的正确性更重要。（这在数学术语中是一个常见的概念，将结果标记为比其他结果更重要或更次要。）

对于这个结果，我们想检验一个一般的 **arithmetic series**。这个短语意味着我们在添加一系列数字，其中相邻项之间的值差是一个固定值。另一种思考方式是，每个项都是通过在前面一个项上加上一个固定的常数得到的。请注意，我们在前两个谜题中检查的和是算术级数：在第一个和中，每个项相差1（或者，我们给每个项加1得到下一个项），在第二个和中，每个项相差2（或者，我们给每个项加2得到下一个项）。

如何表示一个一般的算术数列？知道连续项必须相差一个固定的常数，让我们用一个变量来表示这个值，比如说 c，作为常数。现在，在和中也必须有一个首项，所以让我们用一个变量来表示这个值，比如说 a，因为它是最先的字母。我们只需要一个额外的变量来告诉我们和中有多少个 $many$ 项，所以我们将使用 k，因为我们之前已经用这个变量表示过同样的意思。现在，我们只需要这三个变量就可以表示整个和：

$$A(a,c,k) = a + (a+c) + (a+2c) + (a+3c) + \cdots + (a+(k-2)c) + (a+(k-1)c)$$

我们可以使用每个相邻项之间相差 c 的事实，用第一项 a 来表示第二项，然后我们可以用这个方法来表示第三项，以此类推，通过不断加上 c。我们总共想要 k 项，所以把第一项看作 $a + 0 \cdot k$，最后一项将是我们在第一项 $k-1$ 次加上 c 后得到的结果（从 0 到 $k-1$ 共有 k 个数，包括 0 和 $k-$）。注意，我们还引入了 $A(a,c,k)$ 这个符号，表示“首项为 a，公差为 c，项数为 k 的等差数列之和”。现在，我们如何计算这个和呢？

让我们采用之前有效的方法：在第一个求和谜题中，我们将求和项正向和反向书写并相加。这使我们能够创建许多具有相同和的项对，将求和简化为乘法。当我们这样做时会发生什么？我们看到

$$\begin{array}{ccccccccc}
a & + & (a+c) & + \cdots + & (a+(k-1)c) & = & A(a,c,k) \\
(a+(k-1)c) & + & (a+(k-2)c) & + \cdots + & a & = & A(a,c,k) \\
\hline
(2a+(k-1)c) & + & (2a+(k-1)c) & + \cdots + & (2a+(k-1)c) & = & 2A(a,c,k)
\end{array}$$

再次，我们发现每一对项的和都相同，在这种情况下，这个和是 $2a+(k-1)c$。这样的对有多少个？当然恰好有 k 个项！（这就是我们选择使用那个变量的原因，甚至。）将和表示为乘法，我们现在可以推断出

$$2A(a,c,k) = k \cdot (2a + (k-1)c)$$

因此，

$$A(a,c,k) = \frac{k}{2} \cdot (2a + (k-1)c)$$

这看起来是你预期的结果吗？你有什么期望吗？有时尝试“猜测”可能会发生什么，然后看看结果是否以及如何与你的直觉相符，这有时会有帮助。

Applying the General to the Specific

我们之前提到，我们之前考察的数列都是算术数列，那么这个公式是否为这些数列提供了正确的值？在第一个谜题中，变量的值分别是 $a = 1$，$c = 1$，和 $k = n$；将这些值代入后得到

$$A(1, 1, n) = \frac{n}{2} \cdot (2 + (n - 1)) = \frac{n}{2} \cdot (n + 1) = \frac{n^2 + n}{2}$$

这确实是我们推导出的结果。第二个求和项呢？变量的值是多少？公式正确吗？我们将留给你去验证这个结果。

Another Representation

作为这个谜题的最后一句话，我们想讨论另一种表示我们刚刚推导出的公式的办法。看看括号中的项，并稍作改变：$a+(a+(k-1)c)$。这些项看起来特别有趣吗？嗯，它们分别是和的第一个和最后一个项。这给了我们另一种陈述我们推导出的和公式的办法：$A(a, c, k) = \frac{k}{2}(a + b)$，其中 a 是和的第一个项，b 是最后一个项。这种公式的版本可能更方便，并让我们更快地验证一些和。

例如，如果我们让你找到一个首项为12、末项为110且总共有14项的等差数列的和，你就不必费心去计算常数差c；相反，你只需找到和：$\frac{14}{2} \cdot (12 + 110) = 854$。这要快得多，对吧？那个等差数列的$c$值是多少？给定$a$、$b$和$k$，有没有简单的方法找到$c$?

Lessons From This Puzzle

有意识地了解以往的结果可能会有所帮助，因为它们可以使其他证明更简短、更容易。有时，很难认识到某个特定结果何时有用，即使你认识到它的用途，也可能难以想出如何应用它。在这种情况下，我们认识到我们之前已经证明了一个求和公式，因此至少尝试弄清楚它在证明不同的求和公式中可能有用是有意义的。然而，有一个完全不同的方法来证明奇数求和公式，这并不依赖于我们之前的结果。这暗示了一个更一般的结果，一个好奇的数学家会试图更一般地探索这个问题，我们通过观察一个任意的算术级数做到了这一点。然而，最后我们使用了多种策略来解决前两个求和公式，并将其中之一应用于一般级数问题。我们能否在其他环境中使用这些策略？我们能否通过归纳法证明第一个求和公式？我们能否使用前后写法技术证明第二个求和公式？尝试使用这些策略并看看会发生什么。这可能对你来说似乎很奇怪或不必要，因为我们已经有了结果，但看到不同的技术在不同的环境中是如何工作的是一个宝贵的教训。在数学中，这通常就像

难以（甚至更难）确定在证明中要使用哪种策略，就像确定要证明的结果一样。考虑到这一点，练习特定的策略以培养对何时它们会起作用以及何时需要尝试其他方法的直觉是有帮助的。

1.4.4 Friend Trends

Problem Statement

这个谜题基于以下关于一位匈牙利社会学家及其对儿童朋友圈观察的轶事。

> 在20世纪50年代，一位匈牙利社会学家S. Szalai研究了儿童之间的友谊关系。他观察到，在约20个孩子的任何一组中，他都能找到四个互为朋友的孩子，或者四个孩子，其中没有两个孩子是朋友。在得出任何社会学结论之前，Szalai咨询了当时匈牙利的三位著名数学家：Erd s、Turan和Sos。简短的讨论揭示了这确实是一种数学现象，而不是社会学现象。对于至少有18个元素的任何对称关系R，存在一个包含4个元素的子集S，使得R要么包含S中的所有配对，要么不包含任何配对。这一事实是1930年证明的Ramsey定理的特殊情况，它是后来发展成为丰富组合学领域的Ramsey理论的基石。

(引用自麻省理工学院Jacob Fox教授的讲义。)

我们现在提出的谜题遵循同样的思路，但使用了一些更小的数字。具体来说，我们感兴趣的是研究一组人的最小规模，其中包含一个由三个人组成的子组，这三个人要么都是互相朋友，要么都是互相敌人。

> 假设在一组人中，任何两个人要么是朋友，要么是敌人，并且这些是唯一可能的关系（即没有熟人、半朋友或其他类似关系）。取一组四个人，并尝试为每一对分配朋友/敌人的标识，使得有 no 个三人组要么都是朋友，要么都是敌人。你能用五个人做到这一点吗？六个人呢？七个人呢？十个人呢？二十个人呢？尝试确定一个截止人数，使得你可以 $guaranteed$ 找到一个三人组，他们要么都是朋友，要么都是敌人。

仔细思考这个问题，然后再翻页阅读我们的解决方案。

Representing The Problem Effectively

你弄懂了吗？这是一个非常棘手的谜题，所以如果你在寻找解决方案时遇到了困难，请不要感到难过。事实上，我们认为研究这个谜题和找到答案一样重要，因为有多种方法可以解决这个问题，看到不同的人如何解读这个谜题总是很有趣的。

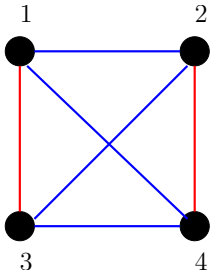
让我们首先讨论如何写下/画出/谈论这种情况。对于这个谜题提出的任何问题，我们都需要考虑一个具有一定规模的人群，并思考该群体中任何两个人之间的关系。为了解决这个谜题，我们需要一种方法来有效地表示所有这些关系，以便我们可以验证关于三个人的子群所期望的性质。具体来说，我们希望轻松地识别是否存在任何三个人的子群是 *homogeneous*，即这三个人是 *all* 朋友或 *all* 敌人。从现在起，我们将称之为 **"homegeneity property"**。

我们如何做到这一点？我们如何表示人和他们之间的关系？我们可以给组内的人编号，然后列出所有数字对的列表，并用 F (朋友) 或 E (敌人) 标记每一对。让我们尝试为四个人组做这件事：

$$12F\,13E\,14F\,23F\,24E\,34F$$

这个朋友/敌人群体是否满足同质性属性？验证并不容易，对吧？首先，编号使得找到三个人的子群变得困难，为了验证这个属性，我们需要检查*all*这样的子群以确保它们不是EEE或FFF。也许在尝试解决方案之前，我们应该找到一种更好的方式来*representing*谜题的信息。你能想到一种更直观的方式来表示在群体中所有可能的配对中两个人是朋友还是敌人吗？具体来说，我们希望有一种相对高效的方式来寻找三个人的子群并识别它们是否都是朋友或都是敌人。

让我们尝试将组中的每个人表示为一个单独的点，并根据这两个人是否是朋友或敌人，用不同类型的线将他们连接起来。例如，让我们用蓝色线条连接朋友，用红色线条连接敌人（记住，任何两个人要么是朋友，要么是敌人，没有其他情况，因此每对点之间必须有一条彩色线条）。例如，以下图表描述了上面线条中分配的关系，使用以下其他符号：



现在，我们要寻找什么来验证同质性属性？我们想要三个点（三个人），使得它们之间的所有线要么是蓝色（都是朋友）要么是红色（都是敌人）。没错——我们正在寻找**monochromatic triangles**！（注意：我们希望三角形的顶点是我们最初画的点之一；也就是说，我们不希望顶点是一个两条线交叉的地方。此外，*monochromatic*来自希腊单词*monos*和*khroma*，分别表示“一个”和“颜色”。）这种表示法在视觉上更容易理解，并且使检查解决方案变得更快。

基于上图，我们解决了关于四个人群的问题：我们找到了一种特定的朋友和敌人的排列方式，使得没有三个人的子群要么全是朋友要么全是敌人。也就是说，没有三个人的子群具有同质性属性。这表明这种情况可以用四个人实现，所以我们不认为在四个人中会有具有同质性属性的群体。

你能找到另一种这样的排列吗？你怎么确定它比我们之前看到的 *different* 排列更好？有多少不同的排列满足同质性属性？现在，尝试画出一个排列，其中 *does* 有一个大小为三的子群具有同质性属性。那会是什么样子？有多少这样的排列？

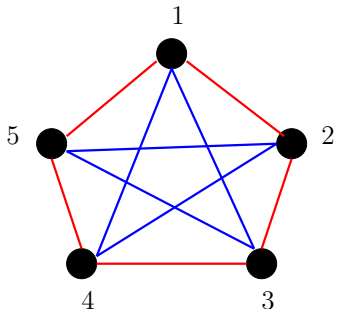
Restating the Problem for $n = 5$

让我们继续思考一组五个人。我们的图示发生了变化，因为我们现在有五个点，这意味着需要绘制更多的线条。尽管如此，我们仍然希望用蓝色或红色线条填满所有连接，并确保没有单色三角形。这是否可能？（提示：尝试将点排列成正五边形形状，然后填充线条。）尝试绘制几次，看看你的任何排列是否可行。也可以尝试随机绘制一些线条，然后确保在添加新线条时不会创建任何三角形，从而引导你的选择。

你弄懂了吗？翻到下一页看看我们是怎么做到的 . . .

Solution for $n = 5$

这里是我们对五个点之间红色/蓝色线的安排，完全避免了均匀性属性：



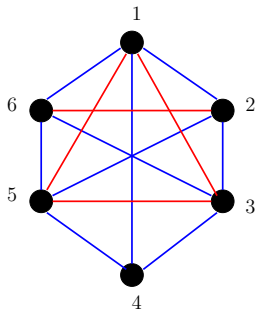
注意这个图形的优雅对称性：所有的红色线条都在五边形的外面，所有的蓝色线条都在形状的内部。这个方法之所以有效，是因为任何以三个点为顶点的三角形必须使用两条外部线条和一条内部线条，或者两条内部线条和一条外部线条。（想想看：为什么我们不能使用三条内部线条或三条外部线条来构成三角形呢？）这个 {v*} 任何我们画出的三角形都将使用两种不同颜色的线条，所以这个图形确实具有 {v*} 同质性属性！当然，我们可以查看图中的所有可能的三角形，并确保它们没有使用一种颜色。有多少这样的三角形？你能够多快用手检查它们？这样做更容易，还是注意到我们上面提到的内部/外部属性更容易？

可能你找到了一个看起来不像我们有的图纸的解决方案。你怎么能判断它实际上是不是一个不同的图形呢？在你的图中有多少条蓝色和红色线条？在我们的图中呢？尝试通过移动点来重新绘制你的图形，但保持点之间的关系（即连接任意两个点的线条颜色）。你能让你的图形看起来像我们的吗？你认为这说明了这个谜题有多少个解？

What about $n = 6$?

好的，现在我们准备思考当我们有六个人时会发生什么。在点与线的方面，我们要画出六点之间所有可能的蓝色或红色线条连接，并确保没有相同类型的线条构成的三角形。在你开始画之前，试着思考一下当我们用四个和五个点工作时这个谜题的解决方案。那些解决方案看起来是什么样子？我们需要填入多少条线？这次我们需要画多少条？我们能否尝试使这个图形看起来像五个点的解决方案？有时思考当前谜题的解决方案可能与之前的工作相似会有所帮助。现在，试着画出这个图形，看看会发生什么。

它工作了吗？为什么不呢？你在哪里遇到了麻烦？在你能够画出一个单色三角形之前，你能画出多少条线？也就是说，在画下一条线之前，你能将多少条线放入图中，无论它是蓝色还是红色，都会形成一个单色三角形？这些问题在某种程度上是解决这个特定谜题的旁枝末节，但它们值得思考，因为它们本身很有趣，并且可能引导我们找到这个谜题或其一般化的解决方案。为了说明，这里是我们尝试在图中分配红色和蓝色线的其中一个尝试。我们为什么在这里停下来？还需要添加多少条线？我们能添加其中任何一条吗？

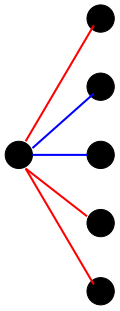


我们现在面临的情况很有趣，因为它与我们之前遇到的情况性质相反。用四个和五个点，我们想表明，要安排所有线条以形成没有单色三角形的结构是 *possible* 的。为了证明这一点，我们只需要做到这一点！展示一个具有所需性质的 *particular* 图形就足以证明实现我们想要的性质是可能的。然而，用六个点，似乎有可能安排线条，使得没有单色三角形。我们如何证明这是一个事实？我们可能会说，我们应该只看看所有可能的线条排列，并论证在每个排列中都有一个 *at least* 单色三角形。这是可行的吗？有多少种线条排列？我们如何轻松地在任何给定的图形中找到一个单色三角形？记得我们是如何用五个点的图形做到这一点的吗？我们注意到，任何三角形都必须至少使用一条外线和一条内线，这立即保证了任何三角形都有两种类型的线条。我们能否在这里做同样的事情，并识别出一些 *guarantees* 三角形的性质？

问题在于，图中有六个点，有 *too many* 种可能的线条排列方式，我们需要手动检查所有这些排列！需要绘制 15 条线，每条线可以是蓝色或红色，所以看起来有 2^{15} 种可能的排列。这是一个很大的数字！（实际上，可能性稍微少一些，因为其中一些在某种意义上是等效的；更技术地说，它们被称为“*isomorphic*”。）

Solution: Working with an *Arbitrary* Diagram

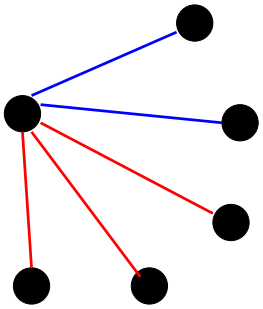
我们需要在论据上更加巧妙，以便我们可以在不绘制特定图形的情况下证明关于*any*图形的一个性质。也就是说，我们需要找到一些事实，一些性质，这些性质对所有可能的六个点的图形都成立，同时仍然允许我们推断出必须存在一个三角形。一种方法是考虑在图形的一个小部分中绘制线条。具体来说，我们可以取六个点中的任何一个，并考虑从这个点发出的五条线。例如，我们可能会有如下情况：



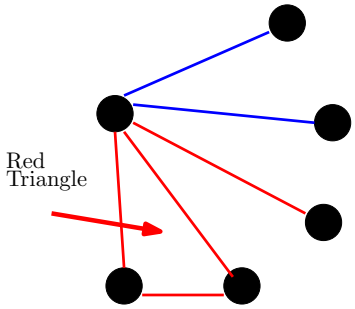
有多少是蓝色的，有多少是红色的？这个问题部分是一个技巧性问题：我们实际上并没有考虑任何*particular*图（如上面的图），而是在试图找到一个关于所有可能图的事实。因此，我们无法太具体地回答这个问题。假设我们面前有一个**arbitrary**图，我们必须提出一个无论那个图是什么都能成立的论点。

这里是我们 *can* 要说的：至少有三条蓝色线条 *or* 至少有三条红色线条。你明白为什么这是真的吗？这个 *wouldn't* 为真的唯一方式是如果有两条（或更少）蓝色线条 *and* 两条（或更少）红色线条离开这个特定的点，总共四条（或更少）线条。然而，我们知道必须画出所有可能连接，所以应该有五条！（这个论点是被称为 **Pigeonhole Principle** 的概念的一个例子。这个想法是我们不能将五个不同颜色的物体放入两个不同的盒子中，而不将三种颜色的物体放入一个盒子中。这是一种在处理这类问题时极其有用的策略，我们将在第8.6节中更详细地探讨这个原则。）

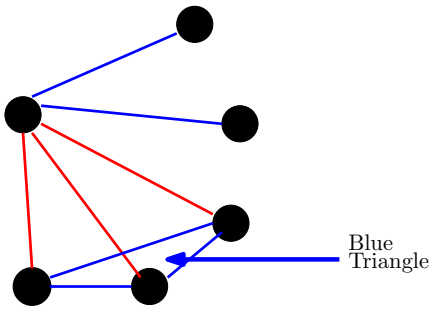
所以我们的立场是什么？我们从六个点全部填充线的*any*个图形开始，专注于一个特定的点；从这个点出来，必须有三条蓝色线*or*三条红色线。它可以是任何一种颜色，所以我们不能仅仅假设它是红色并据此进行论证；我们可以这样做，但之后我们必须回到这个点并看看如果三条线是蓝色会发生什么变化。所以让我们这样做：让我们检查所有有三条红色线从这个特定点出来的图形。从这里我们可以去哪里？我们还没有对图形中的其他线条做出任何假设，所以让我们看看它们可能是什么。查看下面的图片以了解我们迄今为止假设存在的线条颜色：



现在，可以向这张图添加哪些线条，以避免在三个点之间形成同色三角形？我们无法必然地对图中孤立的两个点发出的线条做出任何假设，所以让我们专注于底部的三个点。这些点之间的线条可能是什么颜色？嗯，如果其中任何一条是红色，那么它就会在原点与我们关注的那个点之间形成一个单色的三角形！这将是一个问题。

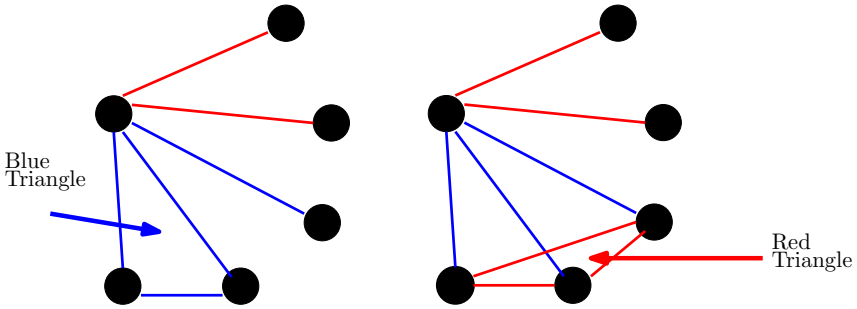


好的，避免这种情况的唯一方法是让所有这些线条都变成蓝色。但那样就会在这三个点之间形成一个蓝色三角形！哇，看起来不管我们怎么做，都在形成一个单色三角形！



让我们回到我们的鸽巢论证并重新评估情况。如果论证保证的三条同类型的线是蓝色而不是红色呢？好吧，实际上没有什么会改变，对吧？我们仍然

无法在图底部的三个点之间添加新行：



如果我们包含任何蓝色线条，那么它就与原始点形成一个单色三角形，如果我们将它们全部变成红色，那么那里就形成一个单色三角形！在这个意义上，我们在鸽巢论证之后遵循的两个论点是 *identical*；如果我们把“蓝色”这个词的每一个实例都替换成“红色”，反之亦然，我们就会得到相同的论点。有时，数学家会利用这种情况来缩短证明，只说“不失一般性，这三条线是红色的。”这通常意味着如果我们选择其他选择（即如果线条是蓝色的），那么进一步的论证在数学上会有相同的结构，因此我们可以通过不重复写相同的词来节省空间和时间。事实上，这种情况如此普遍，有时你可能会看到这个短语“不失一般性”，缩写为 **WOLOG** 或 **WLOG**。

Solution: Summarizing Our Results

我们迄今为止取得了什么成果？我们制作了 *specific* 个图表，展示了我们可以在四个和五个点之间排列线条，以避免单色三角形，并且我们论证了六点线条的 *any* 图表 *must* 具有单色三角形。就这个谜题的朋友/敌人公式而言，这意味着任何六人群体都必须有一个由三个都是朋友或都是敌人的人组成的小组。

注意将谜题重新构思成这种点/线公式是多么有帮助；这使得我们完全忘记了问题的社会背景（这在某种程度上可能会分散注意力）并让我们简化了我们的术语和符号（我们从将一对人标记为“朋友”或“敌人”简化为在两个点之间画一条线）。这是一个非常有用的策略：提取谜题的固有 *structure* ——其运作方式、元素之间的关系、它们如何相互作用等——并以这些部分为依据重新编写一切。这可以使谜题更容易理解和解决，并可以指导我们设计更好的符号。如果我们继续用 $13F, 23E, \ldots$ 符号来解决这个谜题会怎样？这最终可能奏效，但会困难得多！

这个问题的一个原始问题是确定一个截止数，使得任何更大的群体必然具有这个子群属性。你认为我们做到了吗？我们找到了一个截止点吗？六是不是那个数字？为什么是或不是？在七个人的任何群体中，都有一个更小的六人群体，然后我们上面的工作证明了那个群体中必然有三对互相的朋友/敌人！当然，这对任何大于六人的群体都适用，所以这必须是我们要找的那个精确的截止点。这与谜题原始陈述中提到的结果类似，匈牙利社会学家注意到了大小为四的子群中的这种现象。那个问题要难得多，所以我们处理了一个更小、更简单的情况。这两个结果都与一个更大的问题类别相关，称为**Ramsey Theory**。组合数学和图论的这个分支与识别这类“截止点”有关，在这些点上，随着某些结构（如人群）的规模不断增长，最终会有一个点，我们可以找到具有某种属性（三对互相的朋友/敌人）的子群！最初被认为是一种社会学现象，结果却是一个严格的数学事实。怎么样！

Generalizing: Questions for You

在继续之前，让我们提出一些有趣且相关的问题。如果我们寻找的是不同规模的同质群体，比如四个、五个或十二个呢？当然，为了保证找到这样的子群，我们总体上需要更多的人。我们能否总是做到这一点？也就是说，给定任何期望的子群大小，我们能否像这里所做的那样确定一个截止点？你能想出如何证明这样的截止点 *must* 存在，即使不找到特定的数字？此外，如果我们允许第三种可能性：朋友、敌人、不熟悉的人。我们能否对同质群体提出类似的问题？这些都是与拉姆齐理论相关的问题，其中一些问题相当难以回答，数学家们花费了许多年才解决。许多这类简单陈述的问题仍然是开放的和未解决的问题！如果你在这些问题上没有取得任何进展，请不要气馁。我们相信，即使尝试回答这些问题并思考其中存在的问题，本身就足够有意义和有益。

Lessons From This Puzzle

这个谜题提出了几个难题。首先，我们必须找到一种有意义的解释谜题的方法，以便我们甚至可以回答它提出的问题，这涉及到提出适当的 *notation* 来表示谜题的元素。这是数学问题解决的重要部分，尤其是对于像这样的谜题，它没有将符号和可视化作为问题陈述的一部分。

其次，为了将六作为组截断大小，我们必须以某种方式证明

某些 *is not* 是可能的，但需要检查的可能配置数量太大，以至于无法逐个检查。这种情况经常发生，尤其是在与计算机科学和算法相关的问题中。为了解决这个问题，我们不得不采用比单纯的暴力更聪明的策略，而且并不总是清楚应该采用什么策略。在这里，我们基本上开始尝试填充线条，就像它将要成功一样，然后意识到我们已经达到了一个无法修复的点。证明某事是可能的可能只是展示该现象的一个例子（我们用四个和五个大小的组做到了这一点），但证明某事是 *impossible* 可能要复杂得多，需要一些依赖于上下文的巧妙方法。

最后，我们看到了思考与当前谜题紧密相关的问题，只需简单调整一个或多个问题条件，这可能很有趣。如果我们寻找更大的子群呢？如果我们允许更多类型的线条呢？这会如何改变结果？通过改变条件如这种方式探索谜题的边界可以导致新的数学发现和技术，并使数学家们积极寻找新的知识和分享这些知识的方式。

1.4.5 The Full Monty Hall

Problem Statement

这个谜题只涉及基本的概率和算术，然而多年来它一直让一些非常聪明的人感到困惑。事实上，当玛丽莲·沃斯·萨万特在1990年将这个谜题及其解决方案发表在她的《*Parade*》杂志专栏时，引发了一场辩论，许多人（包括数学家）给她写信同意或不同意她的（正确，我们应该这么说）答案。让我们看看你的看法！

> 假设你在参加一个游戏节目，你面前有三个门可以选择。其中一扇门后面有一辆车，其余的后面都是山羊。在节目开始之前，车和山羊被随机放在了门后面。游戏节目的规则如下：在你选择了一个门之后，这个门暂时保持关闭。游戏节目主持人蒙提·霍尔，他知道门后面是什么，现在必须打开剩下的两扇门中的一扇，而他打开的门后面必须是一只山羊。如果剩下的两扇门后面都是山羊，他将随机选择一扇。蒙提·霍尔打开一扇有山羊的门后，他会问你，你是否想坚持你的第一个选择，还是切换到最后剩下的那扇门。想象一下，你选择了门1，主持人打开了门3，门3后面是一只山羊。然后他问你：“你想切换到门2吗？”改变你的选择对你有利吗？

当然，我们假设您宁愿赢得一辆车而不是一只山羊，并且您希望最大化赢得那辆车的机会。此外，我们

应提及这个谜题的名字来源于一档名为 *Let's Make a Deal* 的电视游戏节目的主持人（蒙提·霍尔）。

那么你认为呢？想象一下你自己站在舞台上，面对电视观众，当蒙提霍尔问你，“你想换到另一扇门吗？”时，你会怎么做？

仔细思考这个问题，然后再翻页阅读我们的解决方案。

Solution: *Always* Switch

我们立即陈述答案，因为它可能会让你震惊：你绝对应该改变你的选择！推理出这个答案并获取这个解决方案是棘手且令人困惑的部分，而确定正确解读谜题的方法是长期以来困扰解谜者的一部分。

Analyzing an Incorrect Argument

让我们先向您展示一个声称切换无关紧要的 $incorrect$“解决方案”。想象一下，你和你的朋友听到了这个谜题，他/她给出了这个解释。你会如何回应？你会同意吗？为什么？如果不，你会如何告诉他们他们错了？他们的解释有什么问题?

> 嗯，在我选择一扇门后，蒙提霍尔向我展示另一扇门后的山羊，那么只剩下两扇未打开的门。其中一扇有山羊，另一扇有车，所以车在我选的门后和另一扇门后的概率都是50/50。因此，无论我是否换门，概率都是一样的，所以我最好坚持我已做的选择。

你被这个说服了吗？让我们试着找出这个论点的问题所在。解决这个谜题我们需要解决的主要问题包括找出两个数字：坚持我们的第一个选择赢得汽车的概率，以及切换到另一扇门赢得汽车的概率。我们需要确定这两个值并比较它们；只有$then$我们才能最终解决这个谜题的问题。

现在，上述论点似乎通过说它们都是50%来同时解决这两个概率，但论者对情况的理解存在一个问题。你认为通过坚持第一个选择赢得汽车的机会有多大？本质上，这相当于甚至不让蒙提·霍尔向我们展示另一扇门后面有山羊。如果我们打算坚持我们的第一个选择，那么我们甚至没有必要看到另一扇门后面是否有山羊，因为那并不$affect$我们最初选择的那扇门后面的对象。让我们重申这个观点，以强调其重要性：

> 自有三扇门，第一次选中正确的一扇的概率为 $\frac{1}{3}$，看到另一扇门后面有山羊的概率为 $doesn't\ change\ that\ fact$。

这是上述论点的错误所在，实际上，这是在“解决”这个谜题时最常犯的错误之一。

下一步是弄清楚汽车$after$开关切换的概率，并将其与$\frac{1}{3}$进行比较。实际上，有几种方法可以完成这个任务。一种简洁的方法是推理，当我们第一次选择一个恰好有山羊的门时，切换会导致成功（赢得汽车）。在这些情况下，两个未选择的门隐藏着山羊和汽车，以某种顺序，游戏主持人被迫向我们展示山羊；因此，汽车隐藏在

剩余的门，切换结果为胜利。由于我们将在 $\frac{2}{3}$ 的时间选择一个后面有山羊的门，我们得出结论，切换在 $\frac{2}{3}$ 的时间会导致胜利。

Enumerating the Possibilities

这些解释可能让你觉得不满意，所以让我们实际列举（明确计数）山羊和车门后面汽车的可能排列，并写下在每种情况下我们交换会发生什么。首先要注意的是，门的编号是 *irrelevant*，因为所有选择都是随机做出的；也就是说，无论汽车是否在印有“#1”的门后面，还是“#2”或“#3”，结果都会相同：我们仍然有 $\frac{1}{3}$ 的机会识别出那扇有汽车的门。相应地，我们可以假设 WOLOG（记住这个缩写代表“不失一般性”）汽车在门 #1 后面，山羊在门 #2 和 #3 后面。当然，这是我们对问题的强加，我们不能说游戏玩家知道这一点（否则他/她会每次都选择门 #1！）。有了这个安排，让我们检查我们最初可以做出的所有 3 个选择，并看看在每个情况下交换或留下会取得什么成果：

Door #1	Door #2	Door #3
Car	Goat	Goat

Our choice	Host shows	Result of switching	Result of staying
Door #1	Door #2 or Door #3	Goat	Car
Door #2	Door #3	Car	Goat
Door #3	Door #2	Car	Goat

一个重要的观察是，当我们最初选择有车的那扇门时，主持人可以选择剩下的任何一扇门来向我们展示一只山羊，他做出这个选择 *randomly*。然而，无论哪种选择，我们换门就会输，坚持就会赢。尽管如此，这些情况只发生 $\frac{1}{3}$ 的时间，即在我们最初选择了有车的那扇门之后。由于上表中的每一行都是等可能的，我们可以得出结论，$\frac{2}{3}$ 的时间我们通过换门获胜，而 $\frac{1}{3}$ 我们赢的时间是保持。

这个谜题现在更有意义了吗？试着把这个谜题告诉你的朋友和家人，观察他们的反应。有多少人给出了正确答案？有多少人能正确解释它？有多少人错误地说“这没关系”？有多少人已经听说过这个谜题了？

Generalizing to Many Doors and Cars

让我们看看这个游戏节目情景的推广，并尝试证明在那里切换是否也是一个好主意。具体来说，假设总共有 n 个门和 m 辆车，因此有 $n - m$ 只山羊。为了分析这个问题，我们需要指定 $m \leq n - 2$。想想为什么这是必要的：

- 如果 $m = n$ 为真，那么我们总是能赢，无论我们是否切换。因此，在这种情况下没有什么需要证明的。
- 如果 $m = n - 1$ 为真，那么无论我们第一次选择门时是否恰好选择了门后有 *only* 只山羊的门，主持人都会 *unable* 向我们展示一个有山羊的门。因此，游戏被破坏，是否换门的疑问也就没有意义了。

现在，有了这些变量，这里是游戏的新规则：我们选择n扇门中的一扇。主持人识别所有隐藏山羊的门，并随机选择其中一扇门并打开它。然后我们有选择坚持我们的原始选择或切换到我们选择的另一扇*any*门的机会。现在的策略是什么？我们应该切换吗？我们应该留下吗？答案是否依赖于m和n？如何？

我们将以与上述版本第一次方法相同的方式处理这个修改后的谜题。在这个版本中，我们不可能枚举所有情况，因为 m 和 n 是未知变量。相反，我们需要运用逻辑推理来推断停留和切换时获胜的概率。第一个关键观察与之前我们做出的观察完全相同：当 *staying* 精确时获胜的概率与第一次选择隐藏汽车的门的概率相同。当我们第一次选择一个后面有汽车的门时，无论主持人揭示哪个门，坚持我们的当前选择都会导致获胜。此外，当我们第一次选择一个隐藏山羊的门时，坚持会导致失败。因此，坚持我们的第一次选择获胜的唯一方式是从总共 n 个门中选择一个有汽车在后面的 m 个门之一。这个概率恰好是 $\frac{m}{n}$.

为了确定在 *switching* 后获胜的概率，我们需要仔细考虑每个步骤相关的概率。注意，由于 $m \geq$^2 是一种可能性，我们可能一开始选择了有车的门，然后改变了选择，并且 *still won*。考虑到这一点，我们应该检查两种不同的情况，这里：（a）当我们首先选择有山羊的门时会发生什么，以及（b）当我们首先选择有车的门时会发生什么。每种情况都会给主持人留下不同数量的选择，从而给我们留下不同数量的换门并获胜的方式，因此我们应该分别处理它们。

(a) 假设我们首先选择了一扇有山羊的门。现在还剩下 $n - m - 1$ 扇门隐藏着山羊，主持人随机打开其中一扇。从我们的角度来看，换门后我们剩下 $n-2$ 种选择（我们不能换到已经打开的门或我们的第一次选择），其中 m 是汽车。因此，在这种情况下，换门后获胜的概率是$\frac{m}{n-2}$。

因此，这种情况对切换后总获胜概率的贡献为

$$\frac{n-m}{n} \cdot \frac{m}{n-2} = \frac{nm - m^2}{n(n-2)}$$

(考虑一下为什么我们要 *multiplied* 这些概率。为什么我们非得这么做？我们为什么不直接相加呢？我们接下来会做什么

将此概率与下一个案例相关的概率相结合？)

(b) 然后，假设我们首先选择了一扇有车的门。现在还有 $n-m$ 扇门隐藏着山羊，主持人随机打开其中一扇。从我们的角度来看，换门后我们剩下 $n-$ 个选项，其中 $m-$ 个是车。因此，在这种情况下，换门后获胜的概率是 $\frac{m-1}{n-2}$。

因此，此情况对切换后总获胜概率的贡献为

$$\frac{m-1}{n-2}\cdot\frac{m}{n}=\frac{m^2-m}{n(n-2)}$$

自这两个情况分别发生（即它们不能同时发生）以来，我们应该将这些概率相加。这将告诉我们从我们的原始选择切换到另一个随机门后赢得汽车的总概率：

$$\begin{aligned}\frac{nm-m^2}{n(n-2)}+\frac{m^2-m}{n(n-2)}&=\frac{nm-m^2+m^2-m}{n(n-2)}\\&=\frac{nm-m}{n(n-2)}\\&=\frac{m(n-1)}{n(n-2)}\\&=\frac{m}{n}\cdot\frac{n-1}{n-2}\end{aligned}$$

现在，我们选择这样写分数是有原因的。我们想将这个概率与坚持我们最初选择的大门后获胜的机会进行比较，最初选择的大门是 $\frac{m}{n}$。我们发现，在切换后获胜的概率实际上确实是另一个概率的倍数，并且因子 $\frac{n-1}{n-2}>$ 为 1 因为 $n-1>n-2$。用不等式形式表示：

$$\frac{m}{n}<\frac{m}{n}\cdot\underbrace{\frac{n-1}{n-2}}_{>1}$$

因此，切换后的获胜概率为 *strictly better* (，即不等于，始终优于留在原位的获胜概率)。我们应该始终切换到另一个随机门！

Applying the General to the Specific

原始版本的这个谜题是 $n=3$ 和 $m=1$ 的特例，因此我们可以检查我们的结果是否合理。我们推导出的公式告诉我们，换牌后获胜的概率是 $\frac{1}{3}$，正如我们之前所发现的，而继续持有牌获胜的概率是 $\frac{1(3-1)}{3(1)}=\frac{2}{3}$，正如我们之前所发现的。真 neat！

Generalizing: Questions for You

其他 m 和 n 的值会发生什么？能否使“始终切换”策略比“始终停留”策略显著更好？也就是说，我们能在两种策略的获胜概率之间获得多大的差异？我们能使它有多小？能否使它们相等？

另一个这个谜题的修改版本是基于主持人打开超过1扇门，揭示多只山羊。具体来说，假设有n扇门，其中m扇有车，在你第一次选择之后，主持人随机识别p扇有山羊的门并打开它们，之后你可以选择切换到剩余的$n-p-$扇1号门，或者坚持你的第一次选择。在这个游戏中最佳策略是什么？你需要对m, n和p施加什么条件才能确保我们甚至可以玩游戏？你应该总是切换，还是这取决于p？我们可以将“总是切换”和“总是保持”策略赢得机会的差异做得有多大/多小？

Lessons From This Puzzle

直观和快速决策有时有助于我们找到解决方案，但始终重要的是要检查这些瞬间判断，以确保它们基于合理的理性论据。在这个谜题中，最初说机会是“50/50”可能是有道理的，但经过更仔细的思考和重新评估情况后，我们意识到论据中存在缺陷。具体来说，这个缺陷与正确解读谜题和按照游戏节目中的适当顺序遵循游戏步骤有关。最好按照游戏进行时出现的顺序评估概率，而不是从结束位置开始向后看。

一般来说，涉及概率的谜题相当棘手，需要仔细分析，因此这一点很重要。这里还有一个更大的教训，那就是很多时候，最简单表述的谜题往往是最难解决的。永远不要被误导，认为一个谜题会因为表述简短或容易理解而容易解决！

关于蒙提霍尔问题的更多信息以及相关的心理学，请查看以下论文链接：Krauss, Stefan 和 Wang, X. T. (2003)。“蒙提霍尔问题的心理学：揭示解决顽固智力游戏的心理机制”，*Journal of Experimental Psychology*：通用 132(1)。

1.5 It's Wise To Exercise

我们将以一些练习结束本章，这些练习结合了我们迄今为止讨论的一些想法，或者给你一个练习以前知识的机会，或者只是让你保持精神集中。尽可能多地尝试，并与一些朋友讨论可能的解决方案，看看他们的看法。在

一天结束时，尽管如此，只需将其视为保持大脑肌肉灵活的一种方式!

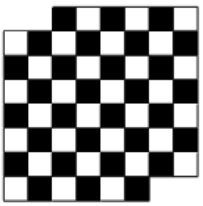
Problem 1.5.1. 一只苍蝇停在以每小时60公里的速度向前飞驰的火车的前端。在同一轨道上，前方300公里处，另一列火车以每小时60公里的速度向第一列火车飞驰。在那个时刻，当两列火车相距300公里时，苍蝇以每小时90公里的速度起飞。他不断地在两列火车之间来回飞行，飞行在轨道上方，并在到达火车时瞬间转身。在两列火车相撞并在这个过程中将苍蝇压扁之前，苍蝇总共飞行了多少距离？你是如何得出这个结论的？尝试将这种情况推广到一列火车以a公里/小时的速度行驶，另一列以b公里/小时的速度行驶，苍蝇以c公里/小时的速度飞行的情况。

Problem 1.5.2. 一家政府造币厂被委托生产金币。造币厂有20台机器，每台机器生产的金币重量均为5克。有一天，造币厂的工头发现有些金币较轻，在检查机器后，他发现其中一台机器正在生产4克重的金币，而其他19台机器工作正常。他决定利用这种情况来为自己谋利，并找出最聪明的员工，以便晋升。他告诉工人，恰好有一台机器正在生产4克重的金币，他们需要确定哪台机器是坏的。作为员工，你可以取一枚金币，*only*一枚，在秤上称重。你可以从任何机器中取出任意数量的金币，但必须将它们放在一起，你只能看到所有金币的总重量，以克为单位。你该如何做才能准确地确定哪台机器是坏的?

Problem 1.5.3. 在一盘棋棋中，皇后可以垂直、水平或斜向移动，任何方向，任何数量的空间。尝试在一个标准的8×8棋盘上放置8个皇后，使得 *none* 的皇后正在攻击其他任何皇后（也就是说，没有皇后可以移动一步并立即捕获另一个皇后）。展示一种方法来做这件事，或者证明这是不可能的。如果你找到了一种方法，你认为有多少种不同的方法可以做到这一点？如果你证明了这是不可能的，那么找到一个更小的皇后数量，使得放置是可能的。你能在棋盘上以这种方式放置的最大皇后数量是多少?

Problem 1.5.4. 从标准的8×8棋盘开始，移除相对角落的2个方格，比如说右上角和左下角。你能用2×1个多米诺骨牌覆盖剩余的方格，使得没有任何一个多米诺骨牌 *overlap*? （注意：这被称为棋盘的 *tiling*。）为什么或为什么不呢？在一般情况，一个 $n \times n$ 棋盘呢？你的答案是否依赖于 n？如何?

Problem 1.5.5. 考虑一个标准的8×8格棋盘，从每个角落移除两个相邻的方块。（见图。）你能用T形四联体来铺满这个棋盘吗？（见图。）如果可以，怎么做？如果不可以，为什么?



关于一般情况，有一个 $n \times n$ 板怎么办？你的答案是否完全依赖于 n？如何依赖？

Problem 1.5.6. 给定一个实数 x，我们让 $\lfloor x \rfloor$ 表示小于（或等于）x 的最大整数，并让 $\lceil x \rceil$ 表示大于（或等于）x 的最小整数。例如，$\lfloor 6.02 \rfloor = 6$ 和 $\lfloor 6.99999 \rfloor = 6$ 和 $\lfloor 6 \rfloor = 6$ 和 $\lfloor -6.5 \rfloor = -7$。

确定以下表达式的值时，尽可能找到一个更具体、更简洁的表示。（可能需要根据x找到几个不同的表达式。）

1. $\lfloor x \rfloor + \lfloor 1 - x \rfloor$
2. $\lceil x \rceil + \lceil 1 - x \rceil$
3. $\lfloor x \rfloor + \lceil x \rceil$ 4. $\frac{\lfloor x \rfloor}{x}$ 5. $\lfloor x^2 \rfloor - \lfloor x \rfloor^2$ 6. $\lceil x^2 \rceil - \lceil x \rceil^2$

Problem 1.5.7. 找出三个自然数 a, b, c，使得没有任何子集的和能被3整除。也就是说，找出 a, b, c，使得以下任何和都不能被3整除：
$a, b, c, a + b, a + c, b + c, a + b + c$。这是可能的吗？为什么或为什么不呢？

尝试用4个数字做同样的事情：找到a, b, c, d，使得没有任何子集的和能被4整除。这是可能的吗？为什么或为什么不呢？

尝试推广。你能说些什么关于找到 n 个自然数，使得没有任何子集的和能被 n 整除吗？

Problem 1.5.8. 回想一下我们是如何通过点和彩色线来解决 *Friend Trends* 问题的。对于这个问题，我们想要解决一个类似的情况，即我们有一定数量的点，需要画出所有可能的线，使得任意两点恰好由一条线连接，但在这个情况下，我们不在乎颜色，所以我们可以说所有线都是黑色，比如说。你能用3个点画出这个图形，使得没有任何一条线交叉吗？用4个点呢？或者5个？或者6个？为什么或为什么不呢？尝试解释为什么那些图形是不可能实现的。如果你不能实现0交叉，你能实现的最小交叉数是多少？

Problem 1.5.9. 让我们使用来自 *Friend Trends* 问题中的相同假设：任何两个人要么是朋友，要么是敌人，没有其他关系。取一组 n 个人，并假设没有一个人有超过 k 个朋友。我们想要将 n 个人分成一些俱乐部，使得每个人恰好在一个俱乐部中。我们需要多少个俱乐部，总共，才能分配 n 个人，使得没有人能与朋友在同一俱乐部中？给定所有人的关系（即给定两个人，我们知道他们是否是朋友）以及俱乐部的数量，我们如何进行人员分配以实现这一属性?

Problem 1.5.10. 画一个圆。在圆周上放置3个点。我们想要给点之间的部分上色（每个部分恰好一种颜色），使得没有点被两种颜色的部分接触。我们需要多少种颜色？如果我们在圆周上放置4个点呢？或者5个？尝试推广到n个点。你能说些什么关于所需颜色的数量?

Problem 1.5.11. 假设你有一个装满袜子的抽屉。里面包含2双蓝色袜子，3双红色袜子，和4双绿色袜子。（也假设左右袜子无法区分。）一天早上，你非常匆忙，开始随机抓取袜子，一次一只，直到你抓到一双袜子。你需要从抽屉里取出多少只袜子才能*guarantee*手里有一双袜子?

如果现在每种颜色的袜子数量是之前的两倍，你的答案会如何变化？如果我们有红色、绿色、蓝色、黄色和棕色各3双袜子怎么办？如果我们有 n 种颜色中每种颜色有 m 双袜子怎么办?

Problem 1.5.12. 四个朋友晚上走在回家的路上，发现自己在一座桥的一侧。这座桥又旧又摇摇晃晃，不适合一群人过桥。他们之间只有一个手电筒，而且光线只能照亮两个朋友的路。每个朋友对这座桥的舒适度不同，所以他们过桥的速度也不同。一个朋友需要5分钟过桥，一个需要10分钟，一个需要15分钟，一个需要20分钟。如果两个朋友一起过桥，他们将以*slower*朋友的速度过桥。四个人过桥需要多长时间？你能找到产生最短时间的最佳方法吗?

Problem 1.5.13. 考虑美国美元的常见硬币面值：分币（1分）、五分镍币（5分）、一角硬币（10分）和25分硬币。你需要在口袋里携带哪些硬币，以便可以用这些硬币支付0分到100分之间的任何价格并找零？是否存在多个可能的硬币组合可以实现这一点？具有这种特性的硬币的最小总价值是多少？是否存在多个具有相同最小总价值的硬币组合?

Problem 1.5.14. 设 a, b, c 为实数，且 $a \neq 0$。以下“欺骗”中，如果有的话，$-\frac{b}{2a}$ 是方程 $ax^2 + bx + c = 0$ 的解，有什么问题?

“Spoof”: 设 x 和 y 是方程的解。减去 $ay^2+by+c = 0$

从 $ax^2+bx+c=0$ 得到 $a(x+y)(x-y)+b(x-y)=0$。因此，$a(x+y)+b=0$，并且 $x+y=-\frac{b}{a}$。由于 x 和 y 是 *any* 的解，我们可以用 $x=y$ 重复这个计算。因此，$2x=-\frac{b}{a}$，因此 $x=-\frac{b}{2a}$ 是一个解。“□”

Problem 1.5.15. 解释为什么 $(-1)(-1)=1$. 假设你是在为一个与你智力相当、对此事实持怀疑态度的同学写作，他需要被说服。仅仅说“因为它就是！”是不够的。试着提出一个有帮助的 *geometric* 或 *physical* 解释，某种易于记忆的论点。

Problem 1.5.16. 对于以下每个提出的方程，找出所有满足它们的实数：

(1) $|x-2|=|x-3|2)$ $|2x-1|=|2x-3|3)$ $|2x-2|=|3x-3|4)$ $|x+1|=|x-5|5)$ $|x-1|+|x-2|=$

((((

Problem 1.5.17. **The First Rule Of Logic Club Is** ...**:** 要加入逻辑俱乐部，你必须决定要 *always* 说出真相还是 *always* 说谎。逻辑俱乐部的成员知道谁在说谎，谁在撒谎。我不属于逻辑俱乐部，但在街上遇到了三位成员，他们发表了以下陈述：

- 杰克：“我们三个人都是骗子。”
- 泰勒：“我们中恰好有两个是骗子。”
- Chuck:“杰克和泰勒是骗子。”

我应该相信谁，如果有人呢?

Problem 1.5.18. 解 $\sqrt{x-1}=x-3$ 对于满足方程的所有实数 x。解释你的工作，并尽量指出你的答案/是/否是 *only* 答案/。

Problem 1.5.19. 你有两根导火线。每根导火线都会燃烧正好一个小时。虽然导火线不一定相同，燃烧速度也不一定恒定。你只有一根打火机和这两根导火线。你能精确测量45分钟吗？如果能，请解释如何操作。如果不能，请解释原因。

Problem 1.5.20. 这个问题是一种标准谜题的变体，其中一种形式最早出现在1926年的《周六晚间邮报》上!

三位朋友一起买了一袋M&M巧克力豆。他们把盒子带回公寓，决定等到第二天派对上再一起分享这袋巧克力豆。

在夜间，第一个朋友醒来，想吃点东西。他

决定现在只吃他那份糖果，第二天不再吃。他打开袋子，把M&Ms分成三等份，但发现还剩下一个。他想一个多出来也无妨，于是吃了自己的那份和那个多出来的，然后把剩下的放回袋子里。

夜间较晚时，第二个朋友做了完全相同的事情。他醒来感到饥饿，把包里剩下的东西分成三堆，吃了他那份以及剩下的额外一份。

甚至更晚的时候，第三个朋友也做了完全一样的事情，包括剩下的额外M&M。

第二天在他们的派对上，朋友们把剩下的糖果分成三个 *equal* 份额并享用了它们。（当然，没有人承认他们所做的一切）。

一开始袋子里有多少个M&Ms？最小可能的数量是多少？

Problem 1.5.21. 给定一个实数列表，它们的 *arithmetic mean* 定义为它们的和除以项数，它们的 *geometric mean* 定义为它们的乘积乘以项数的倒数。也就是说，假设我们有 $x_1, x_2, \ldots, x_n$ 个实数，那么算术平均数是

$$\frac{x_1 + x_2 + \cdots + x_n}{n}$$

并且几何平均数是

$$\sqrt[n]{x_1 \cdot x_2 \cdots x_n}$$

(注意：一个数的 n 次方根等于这个数被提升到 $\frac{1}{n}$ 次幂.)

您能找出两个数，使得它们的算术平均数和几何平均数都是 *equal* 吗？您能找出两个数，使得它们的算术平均数严格大于几何平均数吗？反过来又如何？

重复这个操作，用三个数字，四个数字等。你能识别出一个一般模式吗？

Problem 1.5.22. 考虑变量方程 $6x + 15y = 93$。我们想要找到一些 *integral* 解；也就是说，我们想要找到满足方程的 x 和 y 的值，这些值都是 *integers* (自然数、零和负自然数)。

1. 找到一个解，其中 x 和 y 都是正整数。用几句话描述你是如何得到这个解的。2. 找到一个解，其中一个值，x 或 y，是正数，另一个是负数。再次描述你是如何得到这个解的。3. 你认为有多少个解？尝试写下所有可能解的特征，或者描述你如何找到所有解。

Problem 1.5.23. 一个 **magic square** 是一个包含从 1 到 n^2 的每个数字恰好一次的 $n \times n$ 数组，并且具有每一行和每一列（以及两条主对角线）之和相同的性质。

例如，这里是一个3 × 3 魔方：

8	1	6
3	5	7
4	9	2

注意，在这种情况下，每行/列/对角线所谓的 **magic sum** 是 15。

你能找到一个公式来表示一个 $n \times n$ 魔方的神奇数之和吗?

(*Hint:* Th 这里是我们在本章中发现的一个结果，它将 u seful.)

Problem 1.5.24. 小于或等于1000的整数中，有多少个整数至少有一个数字是1?例如，我们想要计算1和12和511各一次。

Problem 1.5.25. 我们有几堆考拉。为了分散它们，我们从每一堆中移除一只考拉，并将所有这些考拉放入一个新堆中。例如，如果我们开始时有大小为1、4和4的考拉堆，我们最终将得到大小为3、3和3的考拉堆；或者，如果我们开始时有大小为3和4的堆，我们最终将得到大小为2、3和2的堆。

它 **is** 可能我们执行这个操作 *exactly once* 并以与开始时相同的 *exact same pile sizes* 结束（它们的顺序无关紧要；只有 *sizes* 有关）。

识别所有具有此属性的堆叠集合，并解释为什么它们是唯一的。

Hint: 一个具有此属性的开始情况示例是当我们只有一个大小为1的堆时。我们进行操作，再次获得一个大小为1的堆。 bingo。

Hint 2: 确保也要解释为什么你的情况是那些有效的 *only* 之一。我们如何确保你没有遗漏一些答案?

1.6 Lookahead

这一章的目的是让你思考什么是 **mathe- matics**，我们如何 **solve problems**，以及撰写 **proof** 的意义。在本书的其余部分，我们将越来越详细地讨论这三个想法。在这样做的同时，我们将探索数学宇宙的几个不同领域。我们有一个贯穿整个旅程的总体规划，所以不要认为我们只是在森林中随意摸索。我们的主要

目标是要（a）将我们对数学对象的某些直观想法形式化，（2）看到许多好的证明的例子，并培养创造和撰写好证明的能力，（3）培养解决问题的技能和运用数学知识的能力，以及（4）培养对数学的艺术和科学的欣赏。

查看书籍开头的目录，以了解我们的旅程将走向何方。短语和术语现在可能对你来说很陌生，但到书结束时，我们都会说同一种语言：**mathematics**。

Chapter 2

Mathematical Induction: "And so on ..."

2.1 Introduction

这一章节标志着我们迈向更深入地研究数学证明和学会构建自己证明的第一大步。它也是对我们将看到的第一个重要**proof technique**的介绍。正如我们下面所描述的，这一章节旨在成为一份开胃菜，一份**mathematical induction**是什么以及如何使用它的第一口品尝。在接下来的几章中，我们将能够严格定义归纳和*prove*，证明这种技术是数学上有效的。没错，我们将实际证明它是如何以及为什么有效！然而，现在，我们将继续研究一些有趣的数学谜题，这些特定问题是我们精心挑选的，因为它们使用了归纳技术。

2.1.1 Objectives

以下本引言中的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作将如何有所帮助，它们将激励我们为什么要关注本章中出现的主题，并且它们将告诉您我们的目标和在阅读过程中您应该牢记什么以实现这些目标。现在，我们将通过一系列声明为您总结本章的主要目标。以下各节将更详细地重申这些观点，但这将为您提供一份供未来参考的简要清单。当您完成本章的学习后，请回到这份清单，看看您是否理解了所有这些目标。您明白为什么我们将它们列为重要吗？您能定义我们使用的所有术语吗？您能应用我们描述的技术吗？

By the end of this chapter, you should be able to ...

- 定义什么是归纳论证，以及将一个提出的论证分类为归纳论证或非归纳论证。
- 决定何时使用归纳论证，取决于你正在解决的问题的结构。
- 通过类比启发式地描述数学归纳法。
- 识别并描述不同类型的归纳论证，通过比较和对比它们，以及确定相应问题背后的结构，这些结构会产生这些相似性和差异性。

2.1.2 Segue from previous chapter

如前一章所述，我们不会假设读者对超出基础代数和算术的更高级数学有任何了解，也许还有一些视觉和几何直觉。然而，我们将会相当频繁地使用求和和乘积符号，所以如果你觉得你的符号技能有所欠缺，请回顾第1.3.5节。

2.1.3 Motivation

回顾1.4.3节中的谜题，我们证明了前n个奇自然数的和正好是n^2。我们首先通过将求和（奇数）的项排列成平方的依次更大的“角落块”来几何地观察到这个模式。然而，我们证明这个结果的第一种方法似乎并不依赖于这个观察，而只是以一种*algebraic*的方式利用了之前的结果（关于偶数和奇数之和）；也就是说，我们对一些方程进行了一些巧妙的操作（乘法、减法等），然后——voilà！——出现了我们预期的结果。你对这种方法有什么看法？感觉满意吗？从某种意义上说，它并不完全符合我们最初所拥有的几何解释，所以它如此顺利地工作可能会让人惊讶。（也许这种方法有一个*different*几何解释。你能找到一个吗？）

我们的第二种方法是模拟那个初始几何观察。我们将视觉元素转化为代数元素；具体来说，一个和与一个正方形的面积相关，而这个和的项与该正方形的特定部分相关。我们建立了一个*correspondence*，用于不同问题的同一解释之间，找到了一种将一个与另一个相关联的方法，这样我们就可以使用任何一种解释，并知道我们正在证明关于整体结果的一些事情。视觉解释的好处是它使我们能够利用一种称为**mathematical induction**的通用证明策略，有时简称为**induction**。（单词*induction*也有一些非数学含义，例如在电磁学或哲学论点中，但在这本书的上下文中，当我们说*induction*时，我们指的是

mathematical induction.) 什么 exactly 是归纳？它是如何工作的？我们何时可以使用这种策略？我们如何将策略适应特定的谜题？在某些情况下，策略的变体是否更有用？这些都是我们希望在本章中回答的问题。

第一个我们想讨论的主题是一个问题，我们不仅在上一段中提出了这个问题，即，“*Why*归纳？*Why*麻烦去处理它？”基于1.4.3节中的这个谜题，似乎数学归纳法并非完全必要，因为可能存在其他证明某种东西的方法，而不是通过归纳。根据上下文，这完全可能是正确的，但我们从一开始就想明确指出，*induction is incredibly useful!* 在许多情况下，归纳证明是最简洁、最清晰的方法，这是一种众所周知的一般策略，可以在各种此类情况下应用。此外，将归纳应用于问题需要问题存在某种*structure*，即结果的一个“部分”依赖于“先前部分”。（“部分”和“依赖”当然取决于上下文。）认识到归纳适用性，并实际进行后续的证明过程，通常会*teach*让我们对问题的内在结构有所了解。即使归纳失败，这也是正确的！也许问题的一个特定部分“破坏”了归纳过程，而识别这个特定部分可能会有所帮助和启发。

我们希望通过一些示例首先激发这些观点，之后我们将提供一个相当详尽的*definition*数学归纳法，以展示该方法在一般性上的工作原理。（一个完全的*rigorous*定义将不得不推迟到稍后，在我们定义并研究了一些相关概念，如集合论、逻辑语句和蕴涵之后。现在，尽管如此，我们给出的定义将足以解决一些有趣的谜题，并允许我们讨论归纳作为一种一般的证明策略。）

2.1.4 Goals and Warnings for the Reader

请记住，我们仍在朝着数学严谨性的目标迈进，或者尽可能在本书和课程的范畴和时间范围内做到这一点。我们在这章中提出的一些主张将在适当讨论自然数和一些基本数学逻辑之后得到阐明和技术证明。一切都会在适当的时候！

尽管如此，这一章仍然非常重要，因为我们正在继续向您介绍解决数学问题的过程，将我们现有的知识和技能应用于发现新事实并向他人解释。此外，数学归纳法是一种基本的证明技术，你将在你学习的每一门数学课程中都会遇到！这是因为它的有用性和数学世界中归纳性质的普遍性。Translated Text: 尽管如此，这一章仍然非常重要，因为我们正在继续向您介绍解决数学问题的过程，将我们现有的知识和技能应用于发现新事实并向他人解释。此外，数学归纳法是一种基本的证明技术，你将在你学习的每一门数学课程中都会遇到！这是因为它的有用性和数学世界中归纳性质的普遍性。

2.2 Examples and Discussion

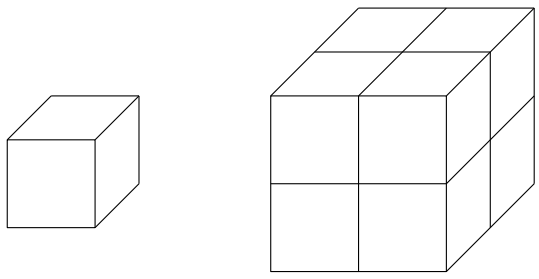
2.2.1 Turning Cubes Into Bigger Cubes

为了激发数学归纳法的整体方法，让我们考察一个几何谜题并共同解决它。这个例子被精心挑选出来，以说明当谜题具有特定类型结构时，**mathematical induction**的相关性；具体来说，某些真理或事实或观察*depends*或*relies*或可以从“之前”的事实中*derived*。这种对先前情况（或情况）的依赖性使得过程*inductive*，当我们观察到这种现象时，应用*induction*几乎总是好主意。

1-Cube into a 2-Cube

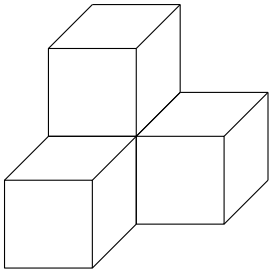
让我们来研究立方数，特别是，让我们尝试描述一个立方数 *in terms of* 之前的立方数。想象一个 $1 \times 1 \times 1$ 立方体，只是一个建筑块。我们如何通过添加 $1 \times 1 \times 1$ 建筑块来构建“下一个最大的”立方体，大小为 $2 \times 2 \times 2$？我们需要添加多少？从算术上讲，我们知道答案：$2^3 = 8$ 和 $1^3 = 1$，所以我们需要添加 7 块才能达到正确的体积。好吧，这是一个具体的答案，但它并没有完全告诉我们 *how* 如何排列这 7 块来形成一个立方体，也没有给我们任何关于如何回答这个问题 *larger* 立方体的见解。最终，我们希望说明构建一个 $100 \times 100 \times 100$ 立方体到 $101 \times 101 \times 101$ 立方体需要多少块，而不必进行大量的繁琐计算；也就是说，我们希望最终找到这个问题的答案：给定一个 $n \times n \times n$ 立方体，我们需要添加多少块才能将其构建成 $(n+1) \times (n+1) \times (n+1)$ 立方体？考虑到这一点，让我们仔细思考这个初始情况，并尝试用一般的论点来回答它。

给定这个单个建筑块，并且知道我们必须向其中添加7个块，让我们尝试确定这7个块应该放置在哪里才能形成一个$2 \times 2 \times 2$ 立方体。（为了简化，我们将大小为 $n \times n \times n$ 的立方体称为 n-立方体，对于任何 n 的值。我们只需要使用在这个例子中是 *natural numbers* 的 n 的值，即非负整数。）看看下面的1-立方体和2-立方体的图片，并尝试解释如何从一个构建到另一个。

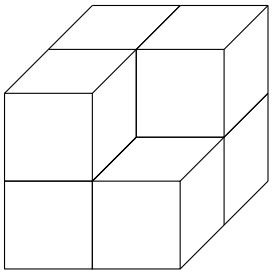


这里有一个合理的解释，我们想使用它，因为它将指导我们从 n-立方体构建 $(n+1)$-立方体的总体解释，并且因为

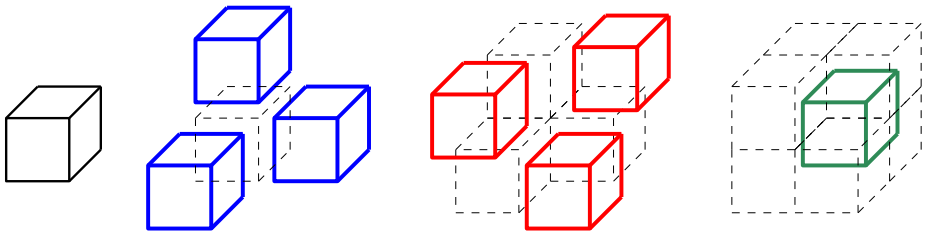
这是一个数学上 *elegant* 且简单的解释。从上面放置的 1-立方体开始，“扩大”3 个暴露的面，在这种情况下，扩大一个方块。这解释了 7 个方块中的 3 个：$2^3 = 1^3 + 3 +$ 。现在“空洞”在哪里?



我们刚刚添加的方块在它们之间创造了“间隙”，每个“间隙”都可以用一个方块填满。这解释了7个总方块中的3个：$2^3 = 1^3 + 3 + 3 +$。现在怎么办?



仅剩一个方块需要填充，它正是最顶部的角落。添加这个方块完成2-立方体，并告诉我们如何用以下图片和方程式从数学上描述我们的构建过程:

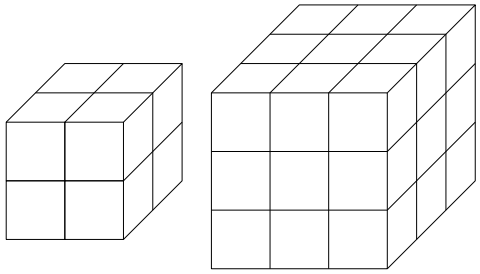


$$2^3 = 1 + 3 + 3 + 1$$

2-Cube into a 3-Cube

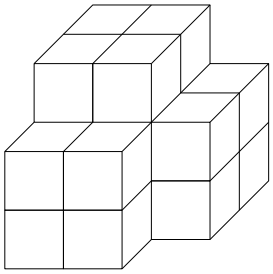
好的，我们现在可能对如何一般描述这个过程有了更好的理解，但让我们再考察一两个案例，以确保我们完全理解。

让我们从一个2-立方体开始，并从中构建一个3-立方体。（如果你恰好拥有各种大小的鲁比克魔方，甚至可以亲手尝试！）我们可以遵循与之前案例中使用的步骤类似的过程，只需适当地更改数字。从一个类似的图形开始



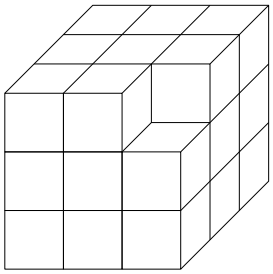
我们注意到，我们需要“扩大”2-立方体的三个暴露的面，但在这个情况下，我们需要扩大的量比之前（与1-立方体）多了*different*，因为我们正在处理一个更大的初始立方体。具体来说，每个面必须扩大2×2 *square*个方块（而在上一个案例中，我们添加了1×1个方块的平方）。因此，一个用于解释这种增加的方程是

$$3^3 = 2^3 + 3 \cdot 2^2 + \_\_\_$$

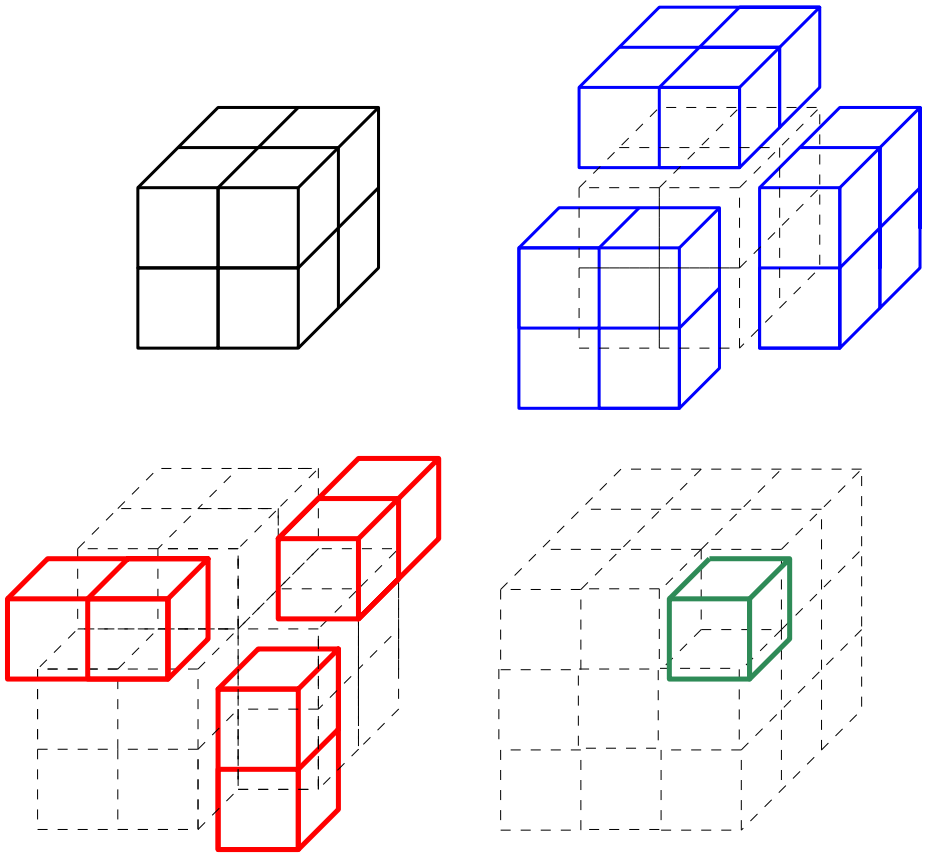


在完成这项工作后，我们发现需要在那些放大的人脸之间填充2×1个方块（而在上一个例子中，我们添加了1×1行方块）。到目前为止，一个用于解释这些增加的方程是

$$3^3 = 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + \_\_\_$$



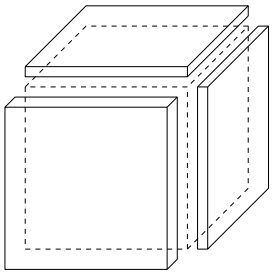
在完成这项工作后，我们发现只剩下一个顶角需要填写。因此，我们可以描绘我们的构建过程及其相应的方程：



$$33 = 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + 1$$

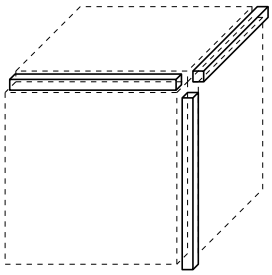
n-Cube into an $(n+1)$-Cube

你现在看到这个过程如何推广了吗？如果我们从一个 n-立方体开始呢？我们如何构造一个 $(n+1)$-立方体？让我们遵循之前两个案例中使用的相同步骤。首先，我们会通过添加三个 *squares* 的块来扩大三个暴露的面。每个正方形有多大？嗯，我们希望每个正方形与暴露的面大小相同，所以它们将是 $n \times n$ 个正方形，每个面有 n^2 个块：



$$(n+1)^3 = n^3 + 3n^2 + \_\_\_$$

接下来，我们将在这些放大的人脸之间用一排排的方块填满空隙。这些排有多长？嗯，它们各自沿着我们刚才添加的方块平方的边缘排列，所以它们各自的大小将是$n \times 1$，每个空隙将占用n个方块：



$$(n+1)^3 = n^3 + 3n^2 + 3n + \_\_\_$$

最后，只剩下一个顶角需要填写！因此，

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1$$

“等一下！”你可能会突然说，“我们早就知道了，对吧？”从某种意义上说，是的；上面的等式是一个代数恒等式，我们也可以通过简单地展开左边的乘积并合并同类项来轻松看出：

$$\begin{aligned}(n+1)^3 &= (n+1)\cdot(n+1)^2 \\ &= (n+1)\cdot(n^2+2n+1) \\ &= (n^3+2n^2+n)+(n^2+2n+1) \\ &= n^3+3n^2+3n+1\end{aligned}$$

所以我们真正取得了什么成就呢？嗯，以这种几何和视觉方式推导出这个恒等式的主要目的是，它展示了这个恒等式如何代表某种*inductive*过程。我们试图解释如何从一个已知的“事实”（下一个最小的立方数，n^3）推导出一个“事实”（一个立方数，$(n+1)^3$），并正确地解释了如何做到这一点。将此与我们所使用的方法之一来调查奇数之和产生完全平方数的事实进行比较。那个观察也揭示了

归纳过程，尽管当时我们没有将其描述为这样的，但我们现在鼓励你思考这一点。回顾我们的讨论，尝试写出如何通过观察方块平方来表示 $(n+1)^2$ 关于 n^2 的形式。这看起来像是一个“显而易见”的代数恒等式吗？（如果你感到有挑战性，思考一下在 $n+1)^4$ 关于 n^4 的表示中会发生什么。这背后有什么几何直觉？更高次幂呢？）

该方法的好处是我们现在知道如何用较小的立方数来描述立方数，*all the way down to* 1；也就是说，每次我们看到表达式中有一个立方数，我们都能精确地知道如何用较小的立方数和一些剩余项来写出那个值。此外，每个这样的表达式和剩余项都有一种固有的 *structure*，这取决于所讨论的立方数。因此，通过迭代地用我们上面推导出的表达式替换任何立方数，如 $(n+1)^3$，并继续进行，直到我们不能再替换为止，应该会产生一个具有一些内置 *symmetry* 的等式。这个想法最好通过实际操作来展示，让我们看看会发生什么。让我们从一个任意值 n 的表达式开始推导，

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1$$

然后认识到我们现在知道一个类似的表达式

$$n^3 = (n-1)^3 + 3(n-1)^2 + 3(n-1) + 1$$

我们证明了当我们对 n^3 上的表达式给出一个一般论证时，这个等式成立，因为那只依赖于 $n \geq 1$。我们可以遵循相同的逻辑步骤，在整个过程中用 $n-1$ 替换 n 1，并最终得到上面的第二个表达式，对于 $(n-1)^3$。(这会一直持续下去，对于 *any* 的 n 值吗？花一分钟想想这个问题。当 $n \leq$ 为 0 时，我们的论证有意义吗？谈论从不同的立方体中构建一个 $(-2) \times (-2) \times (-2)$ 立方体在物理上是否有意义？)

因此，我们可以替换上面一行中的 n^3 项

$$\begin{array}{rccccccc} (n+1)^3 = & & \cancel{n^3} & + & 3n^2 & + & 3n & + & 1 \\ & + & (n-1)^3 & + & 3(n-1)^2 & + & 3(n-1) & + & 1 \end{array}$$

这是也是一个代数恒等式，但绝对不是我们仅仅通过展开左侧的乘积并分组就能轻易想到写下来的那种。在这里，我们利用我们结果中的 *structure* 重复应用它，从而获得我们原本不会想到写下来的新表达式。让我们继续这个过程，看看它会带我们到何处！接下来，我们将 $(n-1)^3$ 替换为相应的表达式，并找到

$$\begin{array}{rccccccc} (n+1)^3 = & & & & 3n^2 & + & 3n & + & 1 \\ & & \cancel{(n-1)^3} & + & 3(n-1)^2 & + & 3(n-1) & + & 1 \\ & + & (n-2)^3 & + & 3(n-2)^2 & + & 3(n-2) & + & 1 \end{array}$$

也许你已经看到了这个趋势？我们可以反复进行这个过程，上面排列的列将继续增长，表明这里正在进行着某种深刻且数学上对称的事情。但这个过程何时停止呢？我们希望写下这个迭代过程的简洁版本，并能够解释所有出现的术语，因此我们需要知道它何时结束。还记得我们研究立方数时的第一步吗？我们找到了如何写出$2^3 = 1^3 + 3 + 3 + 1$的方法。由于这是我们*first*步骤在*building*这个归纳过程中的步骤，它应该是我们在现在这种反向构建时应用的*last*步骤。因此，我们可以写出

$$\begin{array}{rcccccccc}
(n+1)^3 = & & & & 3n^2 & + & 3n & + & 1 \\
& & + & & 3(n-1)^2 & + & 3(n-1) & + & 1 \\
& & + & & 3(n-2)^2 & + & 3(n-2) & + & 1 \\
& & + & & 3(n-3)^2 & + & 3(n-3) & + & 1 \\
& & & & \vdots & + & \vdots & + & \vdots \\
& & + & & 3 \cdot 2^2 & + & 3 \cdot 2 & + & 1 \\
& + & 1^3 & + & 3 \cdot 1^2 & + & 3 \cdot 1 & + & 1
\end{array}$$

这是*definitely*一个我们不可能凭空想出来的恒等式！除了在这个页面上看起来相对美观之外，它还允许我们应用一些之前的知识并简化表达式。为了了解我们如何做到这一点，让我们将求和符号应用于上面的列并将许多项收集到一些简单的表达式中：

$$(n+1)^3 = 1^3 + 3 \cdot \sum_{k=1}^{n} k^2 + 3 \cdot \sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$$

在最后一章中，我们看到了几个不同的证明，它们告诉我们

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

让我们在上面的行中使用这个事实，并简化最右边的项，以写出

$$(n+1)^3 = 1 + 3 \cdot \sum_{k=1}^{n} k^2 + \frac{3n(n+1)}{2} + n$$

这告诉我们什么？经过所有这些代数操作后，我们取得了什么成果？嗯，我们之前已经证明了关于前 n 个自然数之和的一个结果，所以在此之后的一个自然问题是：前 n 个自然数之和 *squared* 是多少？我们如何开始回答这个问题？这是一个陷阱问题，因为 *we already have*！让我们通过隔离求和项在上面的方程中再进行一步或两步代数操作。

然后除以:

$$(n+1)^3 - 1 - n - \frac{3n(n+1)}{2} = 3 \cdot \sum_{k=1}^{n} k^2$$

$$\frac{1}{3}(n+1)^3 - \frac{1}{3}(n+1) - \frac{n(n+1)}{2} = \sum_{k=1}^{n} k^2$$

This 我们已经取得的成果是：我们推导出了一个求前 n 个平方自然数之和的公式！当然，上面一行中左边的表达式看起来并不特别美观，我们可以进行一些进一步的简化，我们将留给你来验证这会产生下面的表达式:

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

"And so on" is not rigorous!

有几个"教训"我们想指出，基于所有这些工作。第一个教训是，将一个论点推广是一种发现新的有趣的数学思想和结果的好方法。你考虑过这个谜题与奇自然数的和有什么关系吗？如果没有，我们强烈建议你现在尝试一下，同时思考将这个推广到四维或五维"立方体"等。除了给你一些其他有趣的结果外，它还将对学习抽象思考和应用归纳过程有极大的指导意义。第二个教训更像是一种承认：我们在技术上*not proven*上面公式给出了前n个平方自然数的和。我们的推导似乎是有效的，并告诉我们"正确答案"，但有一个明显的问题：省略号！在展开$(n+1)^3$的方程并得到那些项的列时

我们收集到特定的总和，在那些列的中间写上...有助于引导我们的直觉，但 *this is not a mathematically rigorous technique*。我们如何 *know* 中间的所有项确实是我们所期望的？我们如何如此确信我们所有的立方体图像完美地转化为我们写下的数学表达式？我们所说的"一直持续到1"究竟是什么意思?

例如，考虑以下内容:

$$1, 2, 3, 4, \ldots, 100$$

这是那个数字列表吗？你可能把它理解为"1到100之间的所有自然数，包括100"。这似乎是合理的。但如果我们*actually*的意思是这个列表呢?

$$1, 2, 3, 4, 7, 10, 11, 12, 14, \ldots, 100$$

当然，我们指的是从1到100的自然数列表，它们的英文名称中没有"i"！这不是很明显吗?

这个要点是：和朋友交谈时，如果有一些想法，写“1, 2, 3, . . . , 100”可能没问题，并确保听的人知道*exactly*你的意思。不过，一般来说，我们不能假设读者会自然而然地*intuit*我们试图传达的内容；我们应该尽可能*explicit*和*rigorous*。

它现在可能看起来像我们在吹毛求疵，但更大的问题是，有一种数学方法可以使这个论点更加*precise*，使其成为一个完全有效的*proof*。到目前为止我们所做的一切都有助于引导我们的直觉，但我们需要做更多的工作来确保我们的论点完全令人信服。为了使这种类型的论点在一般情况下更加严谨，还需要一些其他概念，我们将在下一章中探讨这些概念，并在之后立即回到这个主题。然而，在此期间，让我们再考察一个例子来练习这种直观论证风格，并识别归纳何时是一个适用的技术。

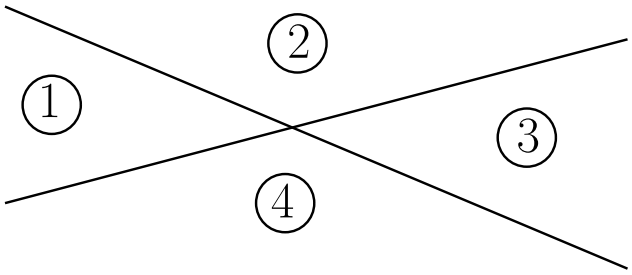
2.2.2 Lines On The Plane

拿一张干净的纸、一支笔和一把尺子。你的纸上有多少个区域？只有一个，对吧？在纸上画一条直线。现在有两个区域。再画一条直线，使其与第一条直线相交。有多少个区域？你应该总共数出四个。画第三条直线，使其与前两条直线相交，但*not*在第一条和第二条相交的点处。（也就是说，总共有三个交点。）有多少个区域？在计数之前你能预测答案吗？当有4条线、5条线或100条线时会发生什么？我们如何解决这个问题，最终找到答案？让我们给出一个更正式的陈述，以确保我们思考的方式相同：

考虑在无限平面（二维表面）上的 n 条线，使得没有任何两条线是 *parallel*，并且不超过两条线 *intersect* 在一个点上。这些线创建了多少个不同的区域？

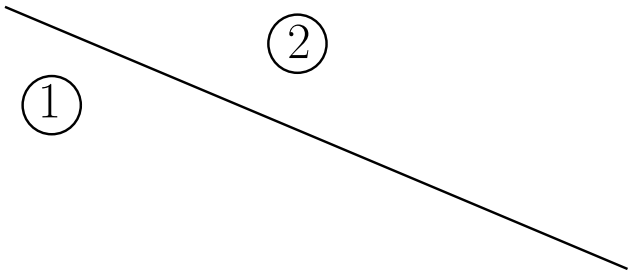
我们可以手动绘制一些例子，当 n 很小（比如，说到 $n = 5$ 是合理的）时，并让我们用这个来引导我们的直觉，为 *arbitrary* 的 n 值做出一般性的论证。（注意，这种策略与我们之前在谜题中做的事情非常相似：识别小案例中的模式，识别可以推广的那些案例的相关组成部分，然后抽象到任意案例。）具体来说，我们想要尝试识别一个绘制中的区域数 *depends* 与一个线条更少的绘制中的区域数之间的关系。当我们绘制一条新线时会发生什么？我们能确定这如何改变已经存在的区域吗？我们能以某种方式计算这创造了多少区域吗？在继续阅读之前，先自己对这个谜题做一些调查。如果你发现了一些结果，比较你的工作与我们下面遵循的步骤。

让我们从一个小的例子开始，比如说 $n = 2$。我们知道一条线可以将平面分成两个区域；当我们添加第二条线时会发生什么？我们知道我们会得到四个区域，因为我们只需看看并数一数：

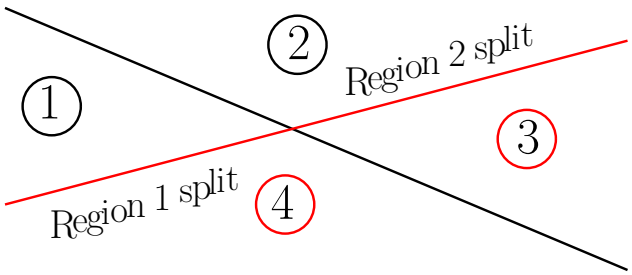


然而，我们只观察两条相交直线的 *one specific case*。我们如何知道无论我们如何适当地绘制这两条线，我们都会找到四个区域？也就是说，我们能否以某种方式描述 *how* 这发生的情况，从而包含这样一个事实，即线的数量是 $n = 2$？想想看！

这里是我们的方法。注意，当我们添加第二行时，每个已经存在的区域都被分成两个，而且这是真的 *no matter how you choose to draw the lines*；只要我们确保两条线不平行，它们总是会这样表现。也就是说，如果我们取一条将平面分成两个区域的线，

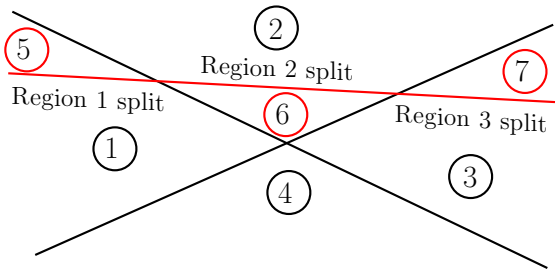


然后添加一个新行将把每个现有区域分成两个。这为整个平面增加了两个新区域，总共四个区域：

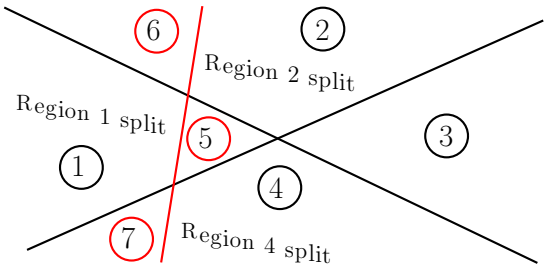


关于当 $n = 3$ 时怎么办？在这种情况下，我们想要考虑向一个由两条线和四个区域组成的图中添加第三条线。我们想要提出一个不依赖于线的 *particular* 安排的论点，因此最终我们唯一应该使用的事实是没有任何线是 *parallel* 的，并且 *intersection* 的任何一点只位于两条线上（不是三条或更多）。然而，目前，

它有助于查看特定的线条排列，以便我们谈论的是同一张图；我们可以用我们对这个特定图的观察来指导我们的总体论证。让我们从一个两行图开始，如下左图，并添加第三行，但让我们选择第三行，使得所有交点都“靠近”或在该图的范围内，这样我们就不必重新缩放图片：

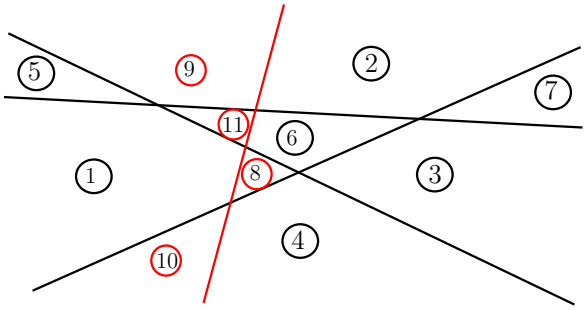


我们当然现在有7个区域，但我们把第三行变成了另一种颜色，这样我们就可以识别出“新”区域出现在哪里：一个区域（下象限，区域4）保持不变，但其他三个区域被分成两部分，每个“分割”都使我们的计数增加1（原本有一个区域，现在有两个）。如果我们把线放在不同的地方会怎样?



相同的现象发生，其中一个象限保持不变，但其他三个象限被分成两部分。（我们如何知道在我们的图表尺度内没有其他未被描绘的区域? 这个问题并不像你最初想象的那么容易回答，值得思考。）尝试其他三条线的排列，并试图说服自己这总是发生的；同时，考虑*why*这种情况，我们可以解释为什么必须发生这种情况。然而，在给出一般解释之前，让我们先考察另一个小案例。

当 $n = 4$ 时，我们开始时有三条线和 7 个区域，并添加一条不与任何现有线平行的第四条线，且不穿过任何现有交点。同样，我们希望提出一个不受特定线条排列约束的论点，但查看以下特定图将有助于引导我们的直觉来提出这个论点：

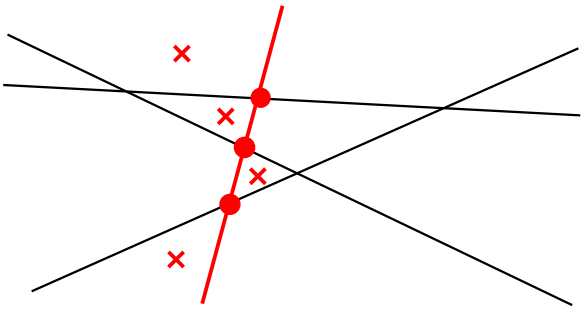


注意，原始的三个区域保持不变（区域3、5和7），其他四个区域被分成两部分。你注意到这里的模式了吗？似乎对于我们所检查的每个n，添加第n行恰好使$n-$个区域保持不变，其余区域被分成两部分。让我们试着解释为什么会这样。记住，我们正在尝试确定当我们画n条线时会出现多少个区域，所以让我们给这个值起一个“名字”，这样我们就可以引用它；让我们说$R(n)$代表在平面上画n条线所创建的区域数，这样没有任何两条线是平行的，并且没有交点属于超过两条线。在这些例子中，当我们考虑n的小值时，我们已经研究了当我们添加一条新线时的$changes$；也就是说，我们已经通过已经知道$R(n-1)$来确定了$R(n)$。让我们尝试调整我们的观察，使它们适用于任何$arbitrary$的n值。

假设我们已经知道 $R(n)$。(为什么我们可以这样做？我们是否确实知道某些特定的 $R(n)$ 值，对于某些特定的 n？哪个？如何？) 假设我们在平面上有一个 $arbitrary$ 图，它包含 n 条线，这些线满足上述谜题陈述中给出的两个条件。这些线创造了多少区域？是的，正好是 $R(n)$。现在，当我们添加第 $(n+1)$ 条线时会发生什么？关于这条线及其如何改变图，我们能说些什么 $for\ sure$？好吧，我们真正拥有的唯一信息是：(a) 这条新线不与任何现有的 n 线平行，并且(b) 这条新线不与任何已经存在的交点相交。现在，条件(a)告诉我们，这条新线必须与现有的 n 条线中的 all 条相交；平行线不相交，非平行线必须在某处相交。因此，我们必须在图上创建 n 个新的交点。这些交点中的任何一个能与现有的交点重合吗？不！这正是条件(b)告诉我们的。这两条信息共同告诉我们，无论我们如何绘制这条新线，只要它满足谜题的要求，我们就能识别 n 沿这条线的“特殊”点。这些特殊点正是新线与现有线相交的点。

我们现在想利用这些特殊点来识别图中的新区域。回顾我们上面考察的案例：识别新的交点，看看你是否能将它们与新的区域联系起来。也许用大圆点标记这些交点，并用X标记新区域，使它们都突出出来会有所帮助。下面我们将展示一个例子，其中$n=4$。你注意到什么了？你能用这些点来

帮助识别添加那条 n-th 行后创建了多少新区域？思考一下，然后继续阅读。



确切！在任意两个新的交点之间，我们有一条线 *segment* 将区域一分为二！剩下的只是确定我们创建了多少这样的新段。由于每个都对应于恰好 *one* 个现有的区域被一分为二，这将告诉我们我们创建了多少个新区域。我们已经计算出这条 $(n+1)$-th 线创建了 n 个新的交点。想想这些点是如何排列在直线上的。任何两个“连续”的点都形成一个段，但极端点也形成了无限段（这些极端点永远延伸过去）。总共有多少个？恰好 $n+1$.（看上面的图，对于 $n=3$.我们看到有3个新的交点和4个新的段，其中两个是无限射线。）这意味着有 $n+1$ 个线段将区域一分为二，因此我们恰好创建了 $n+1$ 个新区域！这使得我们可以说

$$R(n+1) = R(n) + n + 1$$

哇，多么观察！需要一点时间来尝试例子和进行一些几何论证，但我们终于做到了。我们为这个谜题识别了一些 *inductive structure*；我们找到了一个案例如何依赖于另一个案例。也就是说，我们找到了 $R(n+1)$ 如何依赖于 $R(n)$。这还没有解决谜题，但我们现在更接近了。剩下的只是用类似的表达式替换 $R(n)$，并不断这样做，直到我们达到一个已知值，$R(1)=2$。观察：

$$\begin{aligned}
R(n+1) &= & & & & & \cancel{R(n)} & + & n+1 \\
&= & & & \cancel{R(n-1)} & + & n & + & n+1 \\
&= & & \cancel{R(n-2)} & + & (n-1) & + & n & + & n+1 \\
&\vdots & & & & & & & & \\
&= & & \cancel{R(2)}+3 & + & \cdots & + & n & + & n+1 \\
&= & R(1)+2 & + & 3 & + & \cdots & + & n & + & n+1
\end{aligned}$$

自我们知道 $R(1)=2$，我们可以说

$$R(n+1) = 2 + (2+3+\cdots+n+(n+1)) = 2 + \left(\sum_{k=1}^{n+1} k\right) - 1 = 1 + \sum_{k=1}^{n+1} k$$

并且这是我们之前研究过的和！（注意，由于括号中缺少第一个求和项，我们不得不减去1。）回忆一下 $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$，为了表示上面方程中的和，我们只需将 n 替换为 $n+1$。因此，

$$R(n+1) = 1 + \frac{(n+1)(n+2)}{2}$$

最后，我们希望进行的一个简化是将方程中的 $n+1$ 替换为 n，因为对于 $R(n)$ (，这样的表达式更有意义。对于哪些 n 的值这是有效的？)

$$R(n) = 1 + \frac{n(n+1)}{2}$$

最后，我们解决了最初提出的谜题！为此，我们采用了*inductive*技术：我们解释了如何将一个“事实”，即$R(n+1)$，*depends*与一个“先前事实”的值，即$R(n)$联系起来，并利用这些迭代依赖关系反向工作，直到我们达到一个特定的、*known*值，即$R(1)$。

我们再次指出，本节中我们遵循的推导和做出的观察引导我们的直觉得出答案，但这并没有*rigorously proven*任何东西。问题是“$\cdots$”，这并不是一个具体的、“官方”的数学方法来捕捉我们技术背后的归纳过程。此外，我们的“平面上的线”问题方法让我们*starting*了一个$n-1$条线的图和*building*一个有n条线的新的图；这可以吗？这实际上告诉我们关于一个*arbitrary*有n条线的图的什么？所有这样的图是否都来自一个少一条线的更小的图？

我们将在接下来的两章中学习描述我们迄今为止所做事情所需的工具，以全面描述一种 *rigorous* 的方法，然后在下一章中，我们将使用这些工具来使 **mathematical induction** 正式严谨。然而，现在我们想要给出归纳的启发式定义，并继续研究依赖于归纳技术的有趣谜题和观察。练习这些类型的谜题——学习何时识别归纳过程，如何与之合作，如何使用该结构解决问题等——将在未来非常有帮助，我们不需要深入研究技术数学细节。（至少，现在还不必！）

2.2.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 哪些特性定义了一个 *inductive* 流程?

(2) 我们是如何证明 $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ 是正确的? 我们的方法是如何归纳的? （如果你忘记了，请重新阅读第1.4.2节！）

(3) 为什么我们可以将前一个问题中提到的求和公式中的 n 用 $n+1$ 替换，并且知道它仍然成立? 我们也可以将 n 替换为 $n-1$ 吗?

(4) 通过代数步骤求解，得到前 n 个平方和的最终表达式；即验证

$$\frac{1}{3}(n+1)^3 - \frac{1}{3}(n+1) - \frac{n(n+1)}{2} = \frac{1}{6}n(n+1)(2n+1)$$

(5) 尝试回忆添加平面上的第 $(n+1)$ 行创建 $exactly\ n+1$ 个新区域的论点。你能为朋友解释这个论点并说服他/她这是有效的吗?

(6) 要找到前 n 个平方数的和，为什么我们不能直接对前 n 个数的和的公式进行平方? 为什么这是错误的?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 在平面上画出5条线（满足谜题的两个条件）并验证是否有16个区域。你也能验证6条线会产生22个区域吗?

(2) 想出一个描述序列的另一种方法，该序列为1, 2, 3, 4, . . . , 100，它只是从1到100的所有数字。*not*（回想我们给出的例子：从1到100的所有数字，它们的英文名称中没有“i”。）

(3) 想出一个代数表达式，将 $(n+1)^4$ 与 n^4 相关联，就像我们处理立方体时那样。 (**Challenge:** 你能为你刚才推导出的表达式提供一个 *geometric* 解释吗?)

(4) **Challenge:** 让我们将“平面上的线条”谜题提升一个维度！想象一下在三维空间中有 n 个平面。会创建多少个区域? 假设没有任何两个平面是平行的，并且没有任何三个平面在一条直线上相交。（想想这两个条件如何直接类似于“线条”谜题的指定条件。）

2.3 Defining Induction

为了正确地激励即将对 **mathematical induction** 作为证明技术的定义，我们想强调上述例子使用了关于谜题结构的某些直观概念来发展一个“解决方案”，其中我们在 *solution* 的周围使用引号来表示我们尚未正式证明它。从这个意义上讲，我们提出以下问题：如果我们已经推导出公式并要求验证它呢？如果我们没有经过任何直观步骤来推导公式，而是有人告诉我们它是正确的呢？我们如何检查他们的说法？我们之所以提出这个问题，是因为我们确实面临着这种情况，只是告诉我们公式的人是……上面发现的那个非常直观的论证 *we*!

假设你有一个怀疑的朋友说：“嘿，我听说了一个求前 n 个自然数平方和的公式。有人告诉我，它们加起来是 $\frac{1}{6}n(n+1)(2n+1)$。我检查了前两个自然数，它确实如此，所以它肯定是对的。传下去吧！”作为一个逻辑思维者，同时也是好朋友，你点头附和，说：“我确实听说了，但让我们先验证它对 *every* 个数是否正确。”你会怎么进行？你的朋友是对的，前几个值“确实”很完美：

$$\begin{aligned} 1^2 = 1 &= \frac{1}{6}(1)(2)(3) \\ 1^2 + 2^2 = 5 &= \frac{1}{6}(2)(3)(5) \\ 1^2 + 2^2 + 3^2 = 14 &= \frac{1}{6}(3)(4)(7) \\ 1^2 + 2^2 + 3^2 + 4^2 = 30 &= \frac{1}{6}(4)(5)(9) \end{aligned}$$

等等。如果我们想的话，甚至可以手动检查一个很大的n值：

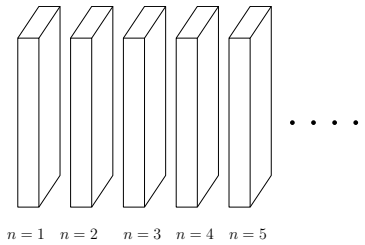
$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2 + 8^2 + 9^2 + 10^2 = 385 = \frac{1}{6}(10)(11)(21)$$

记住，尽管如此，这个公式据说对于*any*的n值是有效的。手动检查个别结果会花费很长时间，因为自然数有*infinite*个。无论我们检查多少个n的个别值，总会存在更大的值，我们如何确保公式对于某个大值*know*不会失效？从数学和时间上讲，我们需要一个更*efficient*的程序，以某种方式在几步之内验证公式对所有n值的正确性。我们当然有一个想法（它是数学归纳法的严格版本），在这里我们将从广义上解释这个程序是如何工作的。

2.3.1 The Domino Analogy

假设我们有一组多米诺骨牌。这是一组特殊的多米诺骨牌，因为我们有无限多个（！）并且我们可以想象任何我们想要的东西

它们上写着，而不是标准的点阵。让我们还假装它们被设置在一个无限长的桌面上，并且我们从侧面观察多米诺骨牌，我们可以在每个下面看到一个标签，这样我们就可以知道我们在哪条线上：{v*}



对于这个特定示例，为了验证公式

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

我们将想象每个多米诺骨上写有一个特定的“事实”。具体来说，我们将想象第一个多米诺骨上写有表达式 {v*}。

$$\sum_{k=1}^{1} k^2 = \frac{1}{6}(1)(2)(3)$$

它上面写着，第二个多米诺有表达式

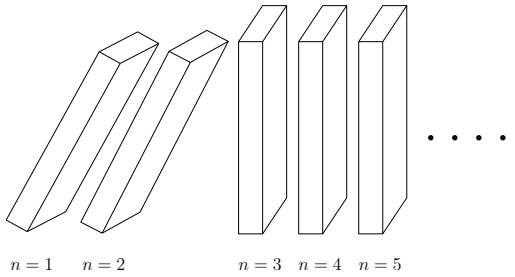
$$\sum_{k=1}^{2} k^2 = \frac{1}{6}(2)(3)(5)$$

它上面写着。一般来说，我们想象在无限行中的第 n- 个多米诺骨牌上写着以下“事实”：

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

因为我们处理的是要相互跌倒并推倒对方的骨牌，所以让我们假设每当一个骨牌跌倒，就意味着它上面写的相应“事实” *is a true statement*。这就是我们将如何将我们对骨牌的物理解释与我们所推导出的公式的数学解释的有效性联系起来。

我们手动检查了 $n = 1$ 的总和：$1^2 = \frac{1}{6}(1)(2)(3)$。因此，第一个多米诺骨牌上写的事实是正确的陈述，所以我们知道第一个多米诺骨牌确实会倒下。我们还手动检查了 $n = 2$ 的总和，所以我们知道第二个多米诺骨牌也会倒下：



然而，继续这样下去会让我们回到之前的问题：我们不想检查*every individual*多米诺以确保它会倒下。我们真的希望封装我们对多米诺骨牌线的物理概念——即当一个多米诺倒下时，它会倒向下一个并推倒它，以此类推——并且以某种方式关联相邻多米诺上写着的“事实”。

让我们先看看前两个多米诺骨牌的情况。知道多米诺1倒下后，我们能否保证多米诺2也会倒下，而无需重写求和的所有项？两个多米诺骨牌上的陈述是如何相关的？每个陈述都是平方自然数的和，第二个多米诺骨牌上恰好多一个项。因此，知道多米诺1已经倒下，即知道*already*，我们可以使用多米诺1上的*true statement*来*verify*多米诺2上陈述的真实性：

$$\sum_{k=1}^{2} k^2 = 1^2 + 2^2 = 1 + 2^2 = 5 = \frac{1}{6}(2)(3)(5)$$

现在，这可能会显得有些愚蠢，因为我们所节省的唯一“工作”就是不必“做算术”来写出$1^2 = 1$。让我们用一个更大的数字的例子来使用这个程序，这样我们就能更有说服力地说明这种方法的好处。让我们*assume*多米诺10已经倒下了。（如果你对这个假设感到担忧，我们之前几段已经写出了完整的总和，你可以在那里验证。）这意味着我们*know*

$$\sum_{k=1}^{10} k^2 = \frac{1}{6}(10)(11)(21) = 385$$

这是一个 *true statement*。让我们用这个来验证Domino 11上写下的陈述，它是

$$\sum_{k=1}^{11} k^2 = \frac{1}{6}(11)(12)(23)$$

The sum written on Domino 11 has 11 terms, and the first 10 are exactly the sum written on Domino 10! Since we know something about that sum, let’s just separate that 11th term from the sum and apply our knowledge of the other

术语:

$$\begin{aligned}\sum_{k=1}^{11} k^2 &= \left(1^2+2^2+\cdots+10^2\right)+11^2\\ &= \left(\sum_{k=1}^{10} k^2\right)+11^2\\ &= 385+121\\ &= 506\\ &= \frac{1}{6}3036 = \frac{1}{6}(11)(12)(23)\end{aligned}$$

看看我们节省了多少努力！如果我们已经了解一些关于它们的，为什么还要费心去读求和的前10项呢?

现在，想象一下如果我们能对 n 的 *simultaneously* 个值进行这个程序！也就是说，想象一下我们能够证明每次多米诺 n 倒下时，我们都是多米诺 $(n+1)$ 倒下的。这会告诉我们什么？好吧，再想想那无限长的多米诺线。我们知道多米诺 1 会倒下，因为我们手动检查了那个值。然后，因为我们已经验证了“多米诺 n 推倒多米诺 $(n+1)$”这一步对于 n 的 *all* 个值，所以我们知道多米诺 1 会倒进多米诺 2，多米诺 2 又会倒进多米诺 3，多米诺 3 又会倒进多米诺 4，依此类推，整个多米诺线都会倒下！本质上，我们可以将整个多米诺线倒下的过程简化为仅仅 *two* 步:

(a) 确保第一个多米诺骨牌倒下;

(b) 确保 每个多米诺骨牌都会撞倒紧随其后的一个 在同一行。

仅用这两步，我们就可以 *guarantee* 每个多米诺骨牌都会倒下，因此，*prove* 所有写在上面的事实都是真实的。这将证明我们推导出的公式对 *every* 自然数 n 是有效的。

我们已经完成了步骤（a），所以现在我们必须完成步骤（b）。我们在前面的段落中已经对特定情况进行了处理（多米诺1推倒多米诺2，多米诺10推倒多米诺11），所以让我们尝试跟随这些案例的步骤并将它们推广到n的任意值。对于某些n的*specific but arbitrary*值，多米诺n会倒下，这告诉我们方程

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

这是一个 *true statement*。现在，我们想将此与Domino上写明的陈述 $(n+1)$ 相关联，并应用上面方程中给出的知识。让我们做之前做过的事情，将 $n+1$ 项的和写成 n 项的和加上最后一项:

$$\sum_{k=1}^{n+1} k^2 = 1^2+2^2+\cdots+n^2+(n+1)^2 = \left(\sum_{k=1}^{n} k^2\right)+(n+1)^2$$

接下来，我们可以应用我们的假设，多米诺 n 已经倒下（这告诉我们它上面写的事实是真的），然后写下

$$\sum_{k=1}^{n+1} k^2 = \frac{1}{6}n(n+1)(2n+1) + (n+1)^2$$

这是否与Domino上写的事实相同（$n+1$）？我们先看看那是什么，然后再进行比较。Domino上的“事实”$(n+1)$与Domino上的事实 n 类似，除了我们随处可见的“n”都被替换成了“$n+1$”：

$$\sum_{k=1}^{n+1} k^2 = \frac{1}{6}(n+1)((n+1)+1)(2(n+1)+1) = \frac{1}{6}(n+1)(n+2)(2n+3)$$

目前尚不清楚我们迄今为止推导出的表达式实际上是否等于这个。我们可以尝试简化我们推导出的表达式并将其分解，使其“看起来”像这个新表达式，但直接展开两个表达式并比较所有项可能更容易。（这源于这样一个普遍观点：展开一个分解的多项式远比识别一个多项式可以分解要容易。）对于第一个表达式，我们得到

$$\begin{aligned}\frac{1}{6}n(n+1)(2n+1) + (n+1)^2 &= \frac{1}{6}n(2n^2+3n+1) + (n^2+2n+1)\\ &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n + n^2 + 2n + 1\\ &= \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{13}{6}n + 1\end{aligned}$$

并且对于第二个表达式，我们得到

$$\begin{aligned}\frac{1}{6}(n+1)(n+2)(2n+3) &= \frac{1}{6}(n+1)(2n^2+7n+6)\\ &= \frac{1}{6}\left[(2n^3+7n^2+6n) + (2n^2+7n+6)\right]\\ &= \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{13}{6}n + 1\end{aligned}$$

看看那个；它们是相同的！另外，注意这比尝试重新排列其中一个表达式并将其“变形”为另一个要容易得多。我们通过操纵它们两个并最终找到相同的表达式来证明它们是相同的。现在，让我们回顾一下我们所取得的成果：

1. 我们将证明公式的有效性比作

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

对于 *all* 的 n 值，到推倒无限多米诺骨牌线。

2. 我们通过手动检查对应情况的公式，验证了多米诺1将会倒下。3. 我们证明了多米诺n将会倒进多米诺(n+1)，并通过$assuming$多米诺n上写的事实是真实的，以及利用这一知识来证明多米诺($n+1$)上写的事实也必须是真实的。4. 这保证了all个多米诺将会倒下，因此对于n的所有值，该公式都是正确的!

你被这种技术说服了吗？你认为我们已经证明了该公式对所有自然数 $rigorously\ proven$ 都成立吗？如果存在一个值 n 使得该公式不成立，那会意味着什么，从我们的多米诺方案的角度来看？

记住，这个多米诺类比是理解归纳工作原理的一个很好的直观指南，但它并非建立在数学严谨的基础上。这将是下一章的目标。现在，让我们回顾一下本节中我们考察的另一个例子：平面上的直线。同样，我们在公式 $R(n)$ 的推导中使用 $ellipses$ 是有问题的，我们希望避免它。让我们尝试在这个谜题的背景下遵循多米诺方案。

想象一下，我们已将表达式 $R(n)$ 定义为表示由 n 条线在平面上创建的不同区域的数量，其中没有任何两条线是平行的，也没有三条线在一点相交。同样，想象一下，在多米诺 n 上我们写下了“事实”，“$R(n) = 1 + \frac{n(n+1)}{2}$”。我们能否遵循上述相同的步骤并验证所有多米诺骨牌都会倒下？

首先，我们需要检查多米诺1确实会倒下。这相当于验证以下陈述：“$R(1) = 1 + \frac{1(2)}{2} = 1+1 = 2$”。这是一个正确的陈述吗？当然，我们之前已经看到了；一条线将平面分成两个区域。其次，我们需要证明对于任何$arbitrary$的n值，多米诺n都会倒向多米诺($n+1$)。也就是说，让我们假设“$R(n) = 1 + \frac{n(n+1)}{2}$”是某个$n$和$show$值的$true$陈述，并且“$R(n+1) = 1 + \frac{(n+1)(n+2)}{2}$”也必须是一个正确的陈述。我们如何做到这一点？好吧，让我们跟随之前用过的论点，将$R(n+1)$与$R(n)$联系起来。通过考虑向具有n条线（也符合我们的线规则）的any图添加额外线的几何后果，我们证明了$R(n+1) = R(n)+n+1$。利用这个知识，结合我们对多米诺n倒下的假设，我们可以说

$$R(n+1) = R(n) + n + 1 = 1 + \frac{n(n+1)}{2} + n + 1$$

这是否与写在多米诺上（$n+1$）的表达式相同？再次，让我们简化 $both$ 表达式以验证它们是否相同。我们有

$$1 + \frac{n(n+1)}{2} + n + 1 = 2 + n + \frac{n^2+n}{2} = \frac{1}{2}n^2 + \frac{3}{2}n + 2$$

和

$$1 + \frac{(n+1)(n+2)}{2} = 1 + \frac{n^2+3n+2}{2} = \frac{1}{2}n^2 + \frac{3}{2}n + 2$$

看看那个；它们是相同的！因此，我们已经证明多米诺n会以$guaran\text{-}\ teed$的方式落入多米诺$(n+1)$，对于any的n值。相应地，我们可以宣布all个多米诺会倒下！

考虑一下我们使用这种“多米诺技术”所做的工作与我们之前推导出我们刚刚证明的表达式所做的工作之间的区别。我们在本节中使用了省略号吗？为什么用这种方式证明公式更好？我们能否使用多米诺归纳技术来 $derive$ 这些公式本身？

2.3.2 Other Analogies

多米诺类比相当流行，但它并不是对归纳工作方式的唯一描述。根据你所阅读的内容或你所交谈的人，你可能会了解到不同的类比，或者完全是另一种类型的描述。在这里，我们将描述我们之前听说的一些类比。思考这些类比都是如何从根本上都是 $equivalent$ 的，这将有助于巩固你对归纳的理解（至少就我们所发展的而言）。

Mojo the Magical, Mathematical Monkey

想象一个无限高的梯子，笔直地向上延伸到天空。这个梯子上有无限多的梯级，按顺序编号：1，2，3，以此类推向上。我们的朋友Mojo恰好站在这个梯子旁边。他是一只聪明的猴子，对数学非常感兴趣，而且有点神奇，因为他实际上可以爬上这个无限高的梯子！

如果Mojo到达了梯子上的某个等级，那么对应这个数字的事实就是True。我们如何确保他爬上整个梯子？逐个检查每个等级将非常低效。想象一下：我们不得不站在地上确保他到达了第1个等级，然后我们得抬头确保他到达了第2个等级，然后是第3个等级，以此类推……相反，让我们在Mojo开始爬之前确认两个细节。他会开始爬吗？也就是说，他会到达第1个等级吗？如果是的话，太好了！另外，等级之间的距离足够近，以至于无论他在哪里都能$always$到达下一个等级吗？如果是的话，那就更好了！这些条件与我们建立的多米诺类比中的条件完全一样。为了确保Mojo到达$every$等级，我们只需要知道他到达了第一个等级，并且他总能到达下一个等级。

Doug the Induction Duck

认识道格。他是一只鸭子。他也喜欢面包，他将去每个人的院子里寻找更多的面包。这些院子都在数学镇的电感街上，房子编号为1、2、3等等，排列成一行。

Doug从房子#1的院子里开始寻找面包。他没有找到任何，所以他还饿着。他还能在哪里找？隔壁的房子#2有一

后院，也！道格朝那个方向走去，他的肚子咕咕叫。他在那里也没有找到面包，所以还得继续找。他已经知道1号房子没有面包，所以唯一能去的地方就是3号房子的隔壁。我们认为你已经知道接下来会发生什么了……

如果我们跟踪Doug的进度，我们可能会想知道他最终是否能到达*every*码。假设我们事先也知道*no- body*有面包。这意味着无论他在谁的院子里，他肯定会去下一家，继续寻找食物。这意味着他肯定会到达每一家！也就是说，无论我们住在哪一家，无论我们前门上的数字有多大，我们最终都会看到Doug在我们后院里徘徊。（不幸的是，他在这段时间里会饿着肚子！可怜的Doug。）

2.3.3 Summary

让我们重新考虑到目前为止我们所取得的成就，包括我们看到的两个示例谜题和我们所给出的类比。在我们对每个谜题的初步考虑中，我们确定了一些关于谜题的 *structure* 的方面，其中“事实”依赖于“先前的事实”。在立方数的例子中，我们找到了一种方法来表达 $(n+1)^3$ 在 *terms* 的 n^3 中；在平面上的线的例子中，我们描述了当向具有 n 条线的图中添加额外线条时，添加了多少个区域。从这些观察中，我们反复应用这种封装的知识，直到我们到达了一个“事实”，我们知道，在两种情况下，对于“小”的 n (值，这里 $n = 1$)。这使我们能够推导出一个公式、方程或表达式，以适用于 *any* 的 n 值的一般事实。

这项工作有趣且对推导这些表达式至关重要，但它对表达式的有效性从 *not enough* 到 *prove* 进行了验证。在完成上述工作中，我们识别出存在一个归纳过程，并利用其结构推导出所讨论的表达式。这实际上有两个好处；我们实际上找到了我们想要证明的表达式，并且通过识别谜题的归纳行为，我们意识到通过 *mathematical induction* 证明这些表达式将是谨慎且高效的。

对于实际的“归纳证明”，我们遵循了两个主要步骤。首先，我们确定了一个“起始值”，我们可以手动检查该公式/方程。其次，我们*assumed*，n的一个特定值使得相应的公式成立，然后利用这一知识来证明对于值$n+1$的相应公式也必须成立。在这两个步骤之间，我们可以放心“所有的多米诺骨牌都会倒下”，因此，这些公式对于所有相关的n值都将是正确的。

One Concern: What's at the "top" of the ladder?

您可能对某事感到担忧，我们在这里尝试预测您的问题。（我们之所以提出这一点，是因为这是一个常见的观察。如果您在思考这个问题，试着想象这个想法从何而来。）您可能会说：“嘿，我现在觉得我明白了Mojo是如何爬上梯子的，

但实际上他怎么能够得到 *all the way to the top* 呢？这是一个无限高的梯子，对吧？他永远到不了那里……对吧？”

从某种程度上说，你是对的。因为这个神奇的梯子确实延伸到 *forever*，所以它确实没有 *end*，Mojo 永远不会到达“那里”。然而，这并不是重点；我们不在乎梯子的任何“尽头”（不仅仅是因为有 *isn't*）。我们只需要知道 Mojo 真的到达了 *every possible* 级。他不必超越所有这些并站在梯子的顶端，俯瞰他来的地方。那不是目标！

想象一下：假装你对我们要证明的某个特定事实有利益关系。比如说，它是第18,458,789,572,311,000,574,003号事实。（一个巨大的数字。实际上并不重要。）它对应的梯级在梯子上非常高，而你唯一关心的是Mojo在他的旅途中是否能到达那里。他会吗？……当然会！可能需要很长时间（需要多少步？），但在这个猴子梯子的神奇世界中，谁在乎时间呢！你知道他最终会到达那里，这让你感到高兴。现在，想象一下，在神奇世界中，对于每个事实，都有人在乎那个事实。当然，每个人都会因为知道Mojo会在他的旅途中到达他们的梯级而感到高兴。没有人关心他是否能到达顶端；这不是他们的关注点。与此同时，在我们这个普通、非神奇的世界里，我们非常高兴地发现*that*世界中的每个人最终都会感到快乐。整个无限的过程，即梯子攀登，被压缩成仅仅两步，而且只有这两步，我们可以确信梯子上的每一个梯级都会被触及。每个编号的事实都是真实的。

考虑这一点时，也可以用多米诺骨牌类比。我们是否关心这条多米诺骨牌线是否有某个“终点”，以至于它们都撞到某处的墙上？当然不；这条线永远继续下去。每个骨牌最终都会倒下，我们甚至不关心这需要多“长时间”。同样，我们知道道格会到达每个人的院子里；我们不在乎他何时到达任何*individual*院子，只在乎他到达了*all*中的多少。

2.3.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 如何将多米诺、魔力和道格的类比都转化为 *equivalent*？你能想出一个描述它们之间关系的“函数”，将一个类比转化为另一个类比吗？

(2) 找一个之前没有学过数学归纳法的朋友，并尝试描述它。你是否发现自己使用了其中一个类比？这有帮助吗？

(3) 为什么我们用立方体进行的工作没有 *prove* 求和公式？为什么我们仍然需要经历所有这些工作?

(4) 考虑多米诺类比。多米诺骨牌的行列永远延伸下去是问题吗？这难道意味着有些多米诺骨牌永远不会倒下吗？试着用这个类比来描述这意味着什么。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 通过归纳步骤证明公式

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

(2) 通过归纳步骤证明公式

$$\sum_{k=1}^{n} (2k-1) = n^2$$

(3) 通过归纳步骤证明公式

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

(4) 假设我们有一系列按自然数索引的事实。让我们用表达式“$P(n)$”来表示第 n 个事实。

(a) 如果我们要证明 *every* 实例是 True，对于每一个自然数 n，我们该如何做呢？(b) 如果我们想要证明只有 n 的每一个 *even* 值才构成一个 True 陈述，我们能这样做吗？你能提出修改我们给出的类比之一来描述你的方法吗？(c) 如果我们想要证明只有大于或等于 4 的每一个 n 值才构成一个 True 陈述，我们能这样做吗？你能提出修改我们给出的类比之一来描述你的方法吗?

2.4 Two More (Different) Examples

这个简短的部分有几个目的。首先，我们不想让你立刻产生这样的想法，即归纳就是用数字和多项式证明一个 *numerical formula*。归纳比这有用得多！以下例子中，特别是关于证明某个抽象性质对于给定情况中的任何“大小”都是正确的。你将看到它仍然属于“归纳”的范畴，但也会注意到它与前面的例子有所不同。此外，这些例子将说明有时我们需要知道“更多信息”才能推翻一些多米诺骨牌。在前面的例子中，我们只需要知道多米诺骨牌 n 倒下了，多米诺骨牌 $n+1$ 将会倒下。然而，在这里，我们可能需要了解几个之前的多米诺骨牌。在这两个例子之后，我们将总结这与上面给出的多米诺骨牌定义的不同之处，并预览一个更广泛的归纳技术定义，它适用于这些例子。

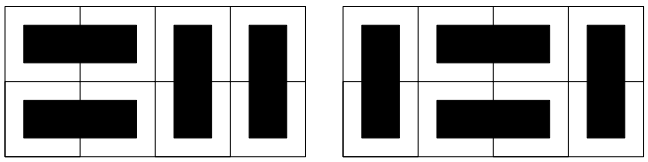
2.4.1 Dominos and Tilings

这个下一个例子比前两个稍微复杂一些。我们最终仍然会证明某个数值 *formula*，但问题显然比仅仅操作代数表达式更具视觉性。此外，我们还会注意到起始步骤中有一个有趣的“曲折”，在那里我们必须解决几个“小情况”才能将我们的方法推广。这将是我们的第一次考虑如何将归纳技术推广和适应其他情况。

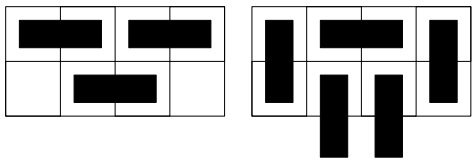
我们想要回答的问题是如下所述：

> 给定一个$2 \times n$ 的方块数组，我们有多少种不同的方式用多米诺骨牌铺满这个数组？一个 *tiling* 必须由一个多米诺骨牌覆盖每一个方块，并且 *only* 只有一个。

例如，以下都是正确的镶嵌

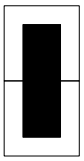


而以下为 *not* 正确的镶嵌

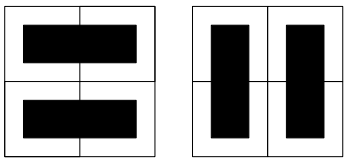


像之前一样，让我们检查前几个情况——其中 $n = 1, 2, 3$，以此类推——看看我们是否注意到任何模式。在继续阅读之前，甚至尝试自己解决这个问题吧！

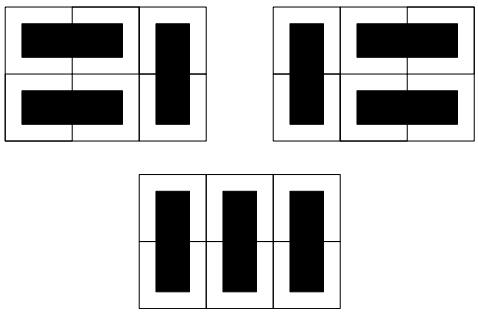
当 $n = 1$ 时，我们有一个正好是一个多米诺形状的数组，所以当然只有一种方法来做这件事。让我们用符号 $T(n)$ 来表示一个 $2 \times n$ 数组上的铺砖数量。因此，$T(1) = 1$。



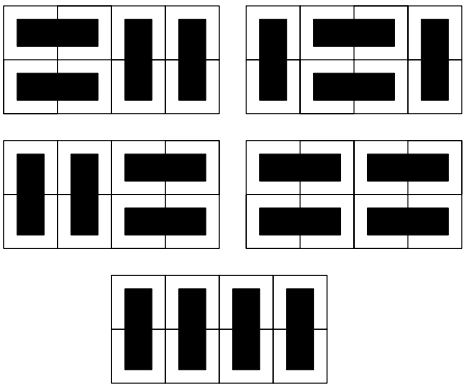
当 $n = 2$ 时，我们有一个 2×2 的数组。由于数组的方向很重要，我们有以下不同的铺砖方式。因此，$T(2) = 2$。



关于当 $n = 3$ 时怎么办？再次，我们可以手动枚举这些镶嵌，并确保我们没有遗漏任何。我们看到 $T(3) = 3$。

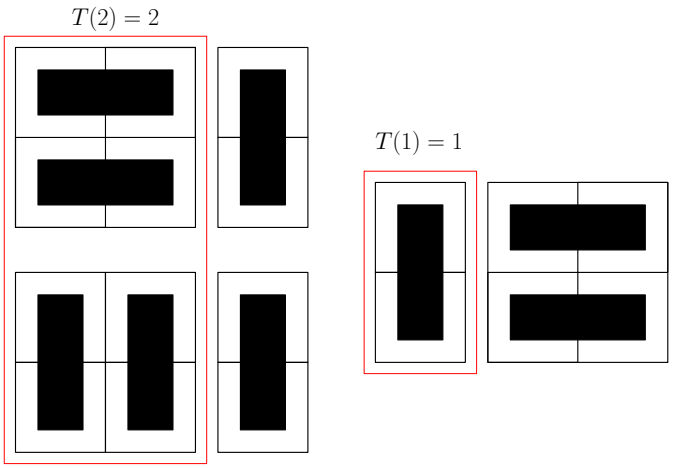


好的，再举一个例子，当 $n = 4$。我们看到 $T(4) = 5$。



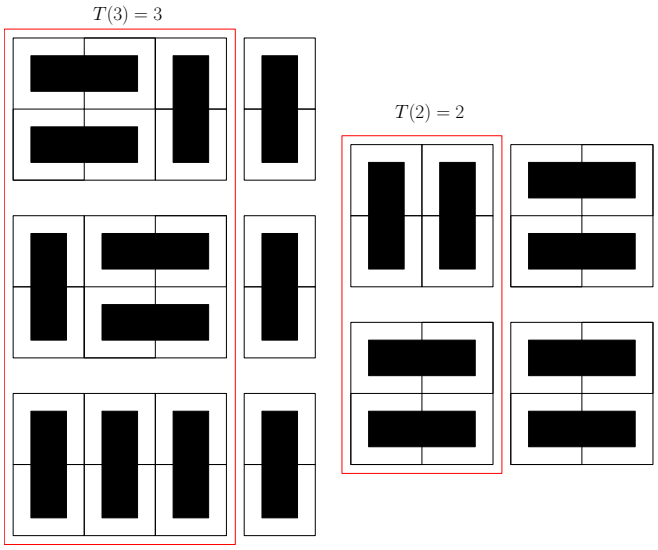
我们现在可以开始寻找规律了吗？写下更大的数组只会让人感到疲倦！让我们思考一下，我们如何利用 $T(1) = 1$ 这个事实来推断 $T(2)$ ... 的某些信息。嗯，等等，... 我们做不到，对吧？这两个情况在本质上有所不同。具体来说，因为多米诺骨牌的大小是 2×1，我们只给数组添加了一行并没有帮到我们。

好的，让我们考虑 $n = 3$，然后。我们能否使用 $T(2) = 2$ 的这个事实？在这种情况下，是的！知道有 2×2 数组的两种铺砖方式，我们就可以立即构建 2×3 数组的两种铺砖方式，无需太多思考。具体来说，我们只需将 *append a vertical domino* 应用到之前的每一种铺砖方式上。但现在我们知道 $T(3) = 3$。第三个铺砖方式是从哪里来的？再次看看那个铺砖方式，以及它与另外两个铺砖方式的比较。在那个第三个铺砖方式中，右侧的骨牌是水平的，而其他两个铺砖方式中的骨牌是垂直的。如果我们移除那两个平行的水平骨牌，我们就剩下 $n = 1$ 的精确情况。换句话说，我们可以通过将 *appending a square of two horizontal dominoes* 向右侧移动来构建一个 2×3 数组的铺砖方式。因此，总的来说，我们已经用更小尺寸的板来描述了 2×3 花园的所有铺砖方式，即 2×2 和 2×1：



$$T(3) = 3 = 2 + 1 = T(2) + T(1)$$

现在你可能看到模式是如何发展的了！让我们展示当 $n = 4$ 时会发生什么，以及我们如何通过在每个组成 $T(3)$ 的铺砖中附加一个垂直多米诺骨牌，或者在每个组成 $T(2)$ 的铺砖中附加两个水平多米诺骨牌来构造 *all* 的组成 $T(4)$：



注意，也没有以这种方式生成2 × 4数组的平铺 *twice*。 (仔细思考一下为什么这是真的。我们如何以保证它们完全不重叠的方式描述两种类型的平铺？) 有了这个信息，我们就可以立即得出结论 $T(4) = T(3) + T(2)$。

此外，我们可以推广这个论点；$n = 4$ 没有什么特殊之处，对吧？对于任何特定的 n，我们只需考虑所有可能的铺砖方式，并观察数组中的 *far right-hand side* 发生了什么：要么我们有一个垂直的骨牌（这意味着铺砖来自一个 $2 \times (n-1)$ 数组），要么有两个水平的骨牌（这意味着铺砖来自一个 $2 \times (n-2)$ 数组）。在这个论点的信心下，我们可以得出结论：

$$T(n) = T(n-1) + T(n-2)$$

对于所有使此表达式有意义的 n 的值。这些值是什么？记住，我们不得不单独识别 $T(1)$ 和 $T(2)$；此论证不适用于这些值。因此，为了使上述方程成立，我们必须添加限制 $n \geq 3$。

使用这些信息，我们就可以轻松地计算出$T(n)$，对于n的任何值，只要给足够的时间。甚至可以相当容易地编写一个计算机程序。然而，正是这个 *inductive*论点——我们注意到的模式和我们对为什么它发生的详细描述——使我们最初得出了结论。在这种情况下，恰好每个项的值$T(n)$都依赖于前*two*个项的值，$T(n-1)$和$T(n-2)$。这种情况在我们的上一章的例子中确实发生了，并且暗示这里正在进行更深入的事情。你看到我们之前对归纳的定义和多米诺骨牌类比在这里不再完全适用了吗？你如何尝试修改我们的类比来解释这种情况？思考

关于这些问题讨论一下，然后继续阅读。在下一个例子之后，我们将更深入地讨论它们。

顺便问一下，你注意到我们这个例子解决方案的有趣之处了吗？你知道其他类似行为的数字序列吗？想想看……

2.4.2 Winning Strategies

这个例子将成为我们第一个需要用 *doesn't* 证明数值公式的归纳谜题！这听起来可能有些奇怪，但事实确实如此，您很快就会看到。实际上，这在数学中比您想象的更常见：一个问题或数学对象可能具有某种潜在的归纳结构，而不依赖于代数或算术。

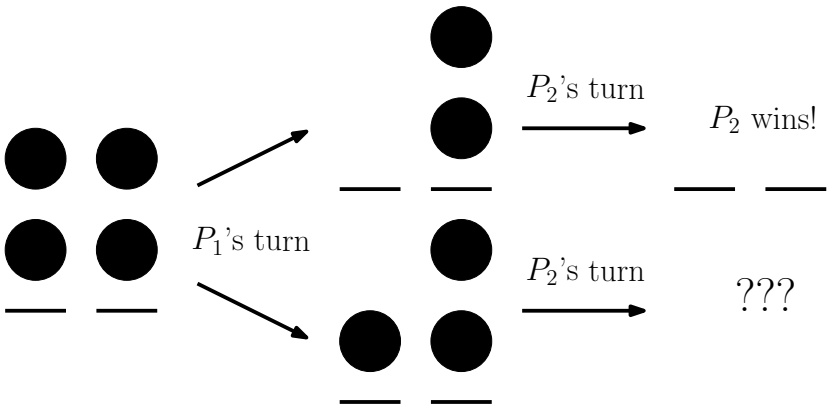
实际上，我们将讨论一个 *game*。在通常意义上，它是一场游戏——有两个玩家需要遵循规则，并且有一个明确的胜者和败者——但它在数学意义上也是一场游戏，我们可以使用数学符号来制定规则和比赛情况，并以抽象的方式讨论正式的 *strategies*。我们甚至可以 *solve* 这场游戏。这与棒球等游戏非常不同。

让我们讨论这个游戏的规则，我们先称它为“Takeaway”。有两个玩家，分别称为 P_1 和 P_2。玩家 P_1 每次都先走。玩家从桌子中间开始，各有两堆石头，每堆恰好有 n 颗石头，其中 n 是某个自然数。（为了区分不同版本的游戏，当每堆有 n 颗石头时，我们说玩家正在“玩 T_n”）。在每位玩家的回合中，他们可以从 *either* 堆中移除 *any* 颗石头。但是，一次从两堆中移除石头是非法的。从堆中移除 *final* 颗石头的玩家是 *winner*。

尝试和一些朋友玩“外卖”游戏。用便士或糖果或硬糖作为棋子。尝试不同的n值。尝试切换角色，让自己成为P_1和P_2。尝试想出一个获胜的*strategy*，一种最大化你获胜机会的玩法。尝试对不同n值的情形做出猜想。谁“应该”获胜？你能*prove*你的主张吗？认真地说，玩这个游戏，尝试在继续阅读我们的分析之前证明一些东西。你可能会对你能取得的成就感到惊讶！

与其他示例一样，让我们使用一些小的 n 值来弄清楚真正发生的事情，然后尝试推广。当 $n =$ 为 1 时，这个游戏相当愚蠢。P_1 必须清空其唯一的石头堆，然后 P_2 获得另一堆中唯一的剩余石头。因此，P_2 获胜。（请注意，P_1 从哪一堆中选择并不重要，P_2 总是会得到另一堆。我们可能会说 P_1 选择左边的堆“不失一般性”，因为两种情况都不重要；情况是等效的，所以我们不妨说它是左边的堆，以便有具体的东西可以说。我们将在讨论数学逻辑时进一步探讨“不失一般性”这一概念。）

当 $n = 2$ 时，我们现在有几个可能出现的情况。考虑 P_1 的可能移动。再次，它们可能作用于左堆或右堆，但由于它们最终是相同的，我们可以交换这两堆，所以我们不妨（不失一般性）说 P_1 从左堆移除了一些石头。有多少？可能是一块或两块石头。让我们分别检查每种情况。

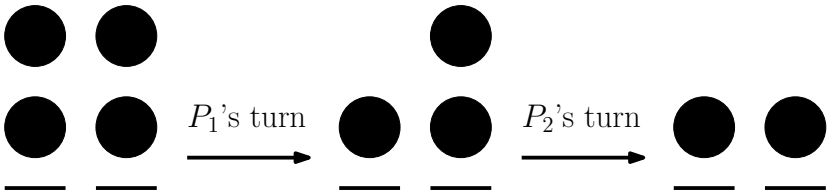


如果 P_1 移除两颗石头，P_2 应该如何反应？ 哎呀，他们应该拿另一堆，所以 P_1 可能一开始就不应该那样走。然而，P_1 可能没有想清楚或者出了什么问题，而且我们还需要考虑所有可能的情况，以全面分析这场比赛。因此，在这种情况下（上图中的最上面一行）P_2 赢了。好吧，这是简单的情况。

如果 P_1 只从左边的一堆（上面的底线）移走一块石头怎么办？P_2 应该如何反应？我们现在有一些选择：

- 如果 P_2 从左边的堆 . . . 中很好地移除其他石头，P_1 拿起另一堆，P_1 获胜。
- 如果 P_2 从右堆 . . . 中很好地移除两块石头，P_1 就会从左堆中取走最后一块石头，P_1 就会获胜。

- 然而，如果 P_2 只从右边一堆中移走一块石头 ...



现在我们遇到了与T_1相同的情况，我们已经分析过了！又是P_1先走，所以我们知道会发生什么：无论怎样P_2都会赢。如果你是玩家P_2，这显然是最好的走法：你赢了*no matter how* P_1 *responds*!

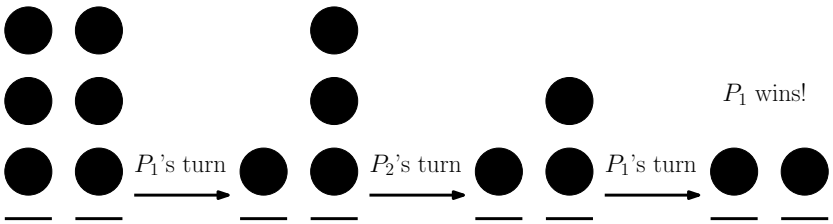
退后一步，让我们思考一下这展示了什么：无论 P_1 首先做什么（从任一堆中移除一块或两块石头），*some possible response* 都可以做出 P_2，这将使 P_2 获胜，无论 P_1 的后续反应如何。哇，P_2 看起来很美！让我们看看这是否适用于 n 的其他值。

当 $n = 3$ 时，我们再次假设（不失一般性）玩家 P_1 在左边的一堆上行动。他们可以移除一个、两个或三个石头：

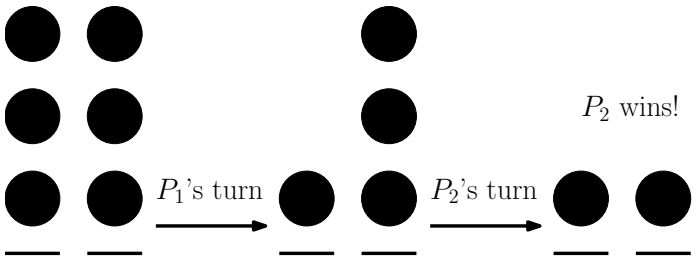
- 如果 P_1 移除所有三个，P_2 通过拿走另一堆完全获胜。

- 如果 P_2 顺利移除两个石子 ...，玩家 P_2 应该怎么做?

完成左边那一堆是愚蠢的（因为 P_1 可以拿走整个右边一堆并获胜），同样地，拿走整个右边一堆也是愚蠢的（因为 P_1 可以拿走整个左边一堆并获胜），所以需要在这两者之间找到一个平衡。现在，如果 P_2 只从右边一堆移走一块石头，请注意 P_1 可以用同样的动作回应；这会在两堆中留下正好一块石头，但角色相反。在这种情况下，如果 P_2 首先行动，根据我们之前的分析，他们现在注定会输。糟糕的举动，P_2!



让我们再试一次。如果 P_2 从右边一堆移除两块石头的话...看吧！现在每堆正好有一块石头，P_1 先手，所以我们知道 P_1 要输了。P_2 再次出击!



考虑一下当 $n = 4$ 的情况，一分钟内你会发现发生着完全相同的分析。你还会考虑另一种可能性：玩家 P_1 可以从左边的一堆中移除一个、两个、三个或四个石头。尽管如此，你会发现 P_2 可以在另一堆上 *mimic that action*，将整个游戏简化为之前的一个，*smaller* 游戏版本，其中 P_2 被证明是必胜的！看起来 P_2 整个时间都在掌控全局，因为他们可以回应 P_1 的任何动作，在另一堆上做出相同的动作。无论 P_1 做什么，总有一个对 P_2 的回应意味着他们获胜，无论 P_1 的后续动作如何。从这个意义上说，我们说“P_2 有一个必胜的策略”。有一个明确且可描述的方法来评估 P_2 的游戏情况并选择一个特定的动作来 *guarantee a win*。

我们如何证明这一点？这如何与本章关于归纳的章节相符？目前可能很难看出。我们实际上在这里证明的是什么？我们这个问题的类比中的多米诺骨牌或阶梯是什么？在理解这个例子时，你可能会意识到以下内容：归纳始终与代数公式有关；归纳代表某种“构建”结构，其中较大情况依赖于较小情况；我们必须证明某个初始事实，然后论证一个任意较大的事实如何被简化，使其依赖于一个先前的事实。这正是多米诺骨牌类比旨在实现的目标。碰巧这个类比对于某些归纳问题（但并非所有）特别具有说明性，并且是可视觉化和容易记忆的。尽管如此，它并不完美地适用于*all*情况。

回顾本章中的这四个例子，思考它们之间的相似之处和不同之处。尝试用更精确、更数学化的术语，甚至可能是你自己创造的术语，来描述数学归纳法。通过这种方式，我们指的是比我们直观类比更好的东西。你会惊讶于你可能会多么成功地描述归纳法，即使你并不真正知道你“应该”说什么，在这个过程中你实际上会学到很多东西！在适当的时候，我们将有一个关于数学归纳法及其各种形式的严格陈述和证明。在此期间，我们需要在其他数学领域进行一次旅行，以建立必要的语言、符号和知识，以便回来解决这个问题。在我们出发之前，我们应该提到一些数学归纳法的有用应用。

2.4.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 这两个例子 *inductive* 怎么样？它们与之前的例子，即立方体和线条，有哪些相似之处？有哪些不同之处？

(2) 在多米诺铺砖中，我们需要知道多少个 *many* 之前的值来计算 $T(n)$？

(3) 写$T(n) = T(n-1) + T(n-2)$和$T(n+2) = T(n+1) + T(n)$有什么区别？

(4) 在Takeaway游戏中，获胜策略是什么？试着和一个不知道这个游戏的朋友一起玩，并使用该策略作为玩家P_2。每次你获胜时，他们会多么沮丧？他们开始明白了吗？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 什么是 $T(5)$？你能画出所有这些镶嵌吗？

(2) 通过两堆4个石子的取走可能性进行操作。你能确保玩家P_2总是有必胜的一步吗？

(3) **Challenge:** 如果你用大小相等的 *three* 堆玩 Takeaway 会发生什么？你能找到任何一方的获胜策略吗？试着和朋友一起玩，看看会发生什么！

(4) 查找 *Fibonacci numbers*。它们与我们找到的多米诺铺砖示例中的数字序列 $T(n)$ 有何关联？

2.5 Applications

2.5.1 Recursive Programming

数学归纳法背后的概念在计算机科学中也得到了广泛的应用。回想一下我们是如何首次推导出 $\sum_{k=1}^{n} k^2$ 的公式的。

一旦我们找到了一种用较小的立方体和一些剩余项来表示立方数的方法，我们就反复进行这种替换过程，直到我们到达“最简单”的情况，即我们在开始问题时首先观察到的那个：$2^3 = 1+3+3+1$。递归编程利用了这种技术：为了解决一个“大”问题，确定问题如何依赖于“小”的情况，并将问题简化到一个简单、已知的情况。

一个此类技术的经典例子是编写计算 *factorial* 函数的代码，$n!$，它定义为前 n 个自然数的乘积：

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$$

这是一个简单的定义，我们人类可以直观理解，但告诉计算机如何执行这个乘积并不完全相同。（试试看！你如何在计算机代码中说“一直继续直到你达到 n”？）更有效的方法是编程函数，并且实际上是通过一个程序 *recursively call itself* 直到它达到那个“简单”的情况。对于阶乘函数，那个情况是 $1! = 1$。对于 n 的任何其他值，我们只需应用以下知识：

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

反复计算 $n!$。考虑以下 *pseudocode* 来表示这个想法：

```
 factorial(n):

if n = 1
   return 1
else
   return n * factorial(n-1)
end
```

我们知道$1! = 1$，所以如果程序被要求计算这个值，它会立即返回正确的值。对于任何更大的n值，程序会参考*itself*并说，“回去为我计算$(n-1)!$，然后我在最后添加一个因子n，我们就会知道答案。”为了计算$(n-1)!$，程序再次询问，如果输入是1；如果不是，它会调用自己并说，“回去为我计算$(n-2)!$，然后我在最后添加一个因子$n-1$。”这个过程会一直持续到程序返回$1! = 1$。从那里，它就知道如何找到$2! = 1 \times 2$，然后$3! = 2! \times 3$，以此类推，直到$n! = (n-1)! \times n$。

另一个涉及递归编程的例子与*Fibonacci numbers*有关。你可能之前在数学课程中见过这个数字序列。事实上，我们甚至在上一节中提到了它们，与多米诺骨牌铺地有关！你也可能听说过它们以一些有趣和奇怪的方式出现在自然界中。（这个序列最初是由意大利数学家莱昂纳多·皮萨诺在研究兔子种群增长时“发现”的。）序列中的前两个数字被指定为1，并且任何

序列中的数定义为前两个数的和。也就是说，如果我们说 $F(n)$ 代表第 n 个斐波那契数，那么

$F(1) = 1$ 和 $F(2) = 1$ 和 $F(n) = F(n-1) + F(n-2)$ 对于每个 $n \geq 3$

现在，$F(5)$是什么？或者$F(100)$？或者$F(10000)$？这可以通过一个递归程序轻松处理。思路是相同的：如果程序引用了“简单情况”之一，即$F(1)$或$F(2)$，那么它将立即知道返回正确的1。否则，它将调用自身来计算前两个数字，然后将它们相加。看看下面的伪代码，想想它是如何工作的。如果我们用这个程序来计算$F(10)$会发生什么？它会如何找出答案?

```
 Fibonacci(n):

if n = 1 or n = 2
   return 1
else
   return Fibonacci(n-1) + Fibonacci(n-2)
end
```

这与上面提到的 `factorial` 程序遵循相同的思路（让程序调用自身来计算函数“较小”情况下的值，直到达到已知值），但这里有一些更深入的东西。如果我们向程序输入 $n = 10$，它会认识到它还不知道输出值，并将调用自身来计算 `Fibonacci(9)` 和 `Fibonacci(8)`。在每个对程序的调用中，它都会再次认识到该值尚不明确。因此，它会再次调用自身来计算 `Fibonacci(8)` 和 `Fibonacci(7)`，但也会计算 `Fibonacci(7)` 和 `Fibonacci(6)`。没错，程序多次使用 *same input value* 调用自身。为了计算 $F(9)$，我们需要知道 $F(8)$ 和 $F(7)$，但与此同时，为了计算 $F(8)$，我们也需要知道 $F(7)$ 和 $F(6)$。这样，我们最终会调用程序 `Fibonacci` 多次。

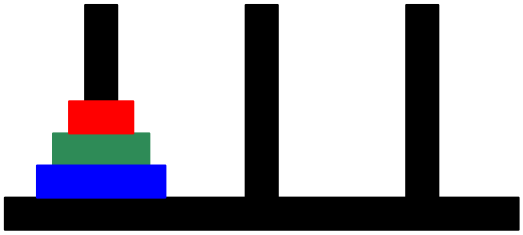
尝试比较程序 `Fibonacci` 和 `factorial`，特别是关于我们在本章中一直在研究的归纳过程。它们是否使用了类似的想法？它们如何与我们所概述的数学归纳法的“多米诺”类比相关？将多米诺 n 上写下的“事实”视为对 n 或 $F(n)$ 正确值的计算！思考每个案例中的类比是如何工作的？所有的多米诺骨牌都会倒下吗？在继续阅读时牢记这些问题。所有这些想法背后都隐藏着一些非常强大的数学。

2.5.2 The Tower of Hanoi

让我们短暂休息一下，玩个游戏。嗯，这并不完全算休息，因为这在某种程度上是一个 *inductive* 游戏，所以它非常相关。但是它确实是一个

游戏，尽管如此！*Tower of Hanoi*是一个非常受欢迎的谜题，部分原因是因为它涉及如此简单的设备和规则。解决它则是另一回事了！

想象我们有三根垂直的杆和三个不同大小的圆盘（蓝色、绿色和红色），像这样堆叠在一起：



目标是将所有三个圆盘移动到另一个杆上（无论是中间的还是右边的，都无所谓）并遵循以下规则：

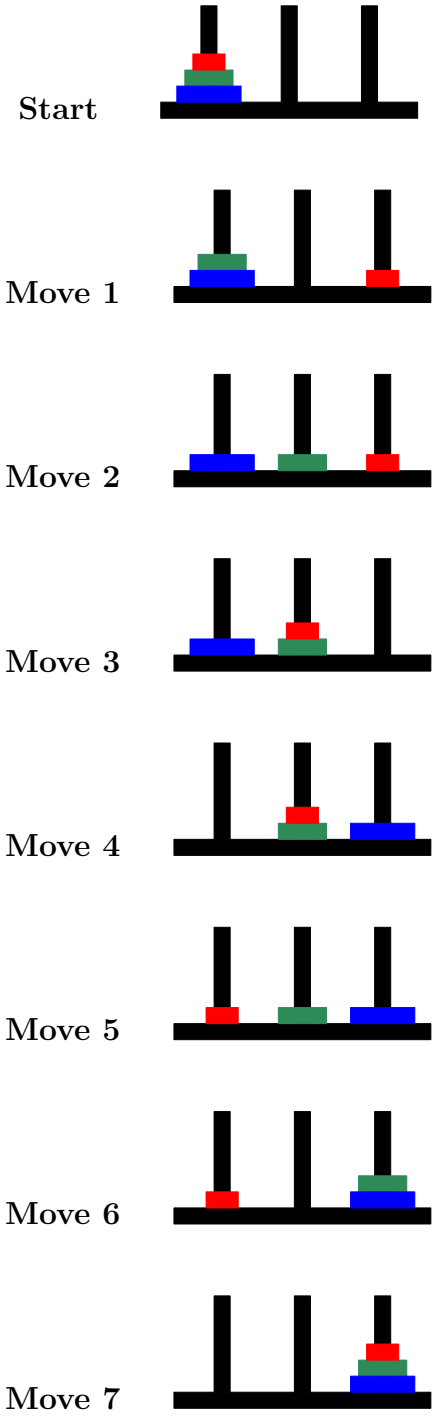
1. 一次移动包括将一个（以及 *only* 一个）磁盘从任何杆的栈顶移动到另一个杆的栈顶。

2. 磁盘不能放在比它小的磁盘上面。

这就是全部！只有两条简单的规则，但玩起来却很难。试着用几枚硬币或扑克牌或你手头上的任何东西来模拟这个游戏。（你甚至可以在一些游戏店买到汉诺塔套装。）你能解决它吗？你用了多少步？你的解决方案是“最佳”的吗？为什么是或不是？

我们提到这是一个 *inductive* 游戏，所以现在让我们来探讨一下这个想法。我们想要考虑解决这个谜题需要多少 *moves*（其中每一个 *move* 代表将一个盘子从一个柱子移动到另一个柱子），更具体地说，确定解决这个谜题所需的 *smallest possible number of moves*。要解决三个盘子的谜题，我们可以不断地将最小的盘子在两个柱子之间来回移动，如果我们想的话，可以生成100次移动，然后解决它，但这当然不是最好的方法，对吧？假设我们找到了一种在特定次数的移动中解决这个谜题的方法；我们如何证明我们使用的移动次数是 *smallest possible* 移动的次数？

为了解决这个问题，我们希望分解解决谜题 *recursively* 的方法。在这个过程中，我们实际上将回答一个更加普遍的问题：使用 n 个盘子在 3 根柱子上解决汉诺塔谜题所需的最小移动次数是多少？我们以上只使用 3 个盘子来提出这个问题，以便给你一个具体的版本来思考和操作，但我们可以通过仔细思考来回答这个更普遍的问题。为了确保我们处于同一页面上，我们将向您展示我们如何解决 3 个盘子的版本：


Start
Move 1
Move 2
Move 3
Move 4
Move 5
Move 6
Move 7

注意，最大的磁盘在大多数解决方案中基本上是“无关紧要”的。因为我们可以在它上面放置任何其他磁盘，所以我们只需要通过将其他磁盘移动到不同的杆上来“揭示”该磁盘，然后将最大的磁盘移动到唯一的空杆上，最后将其他磁盘放在大磁盘上。本质上，我们执行了相同的程序（将两个较小的磁盘从一个杆移动到另一个杆）两次，在这两次之间，我们将大磁盘从一个杆移动到另一个杆。如果最大的磁盘根本不存在，我们实际上解决的是2个磁盘的谜题版本，但却是两次！（仔细思考这一点，并确保你明白为什么这是真的。按照上图中的移动步骤进行，假装大蓝色的磁盘不存在。）

这表明解决3盘拼图的方法涉及两次解决2盘拼图的迭代，中间增加一步（移动最大的盘子）。这表明了一种通用的 *recursive* 程序来解决拼图。为了最优地解决 n-盘拼图，我们只需遵循最优解决 $(n-1)$-盘拼图的程序，使用一步移动最大的 n-号盘子，然后再次解决 $(n-1)$-盘拼图。

现在我们已经对 *how* 有了一些了解，可以优化地解决这个谜题，让我们确定这个程序需要多少个 *moves*。认识到解决这个谜题使用了一个 *recursive* 算法，我们意识到了解关于最优解的任何内容都需要 *proving*。相应地，我们需要确定我们多米诺骨牌的“起点”，它应该对应于谜题的“最小”或“最简单”版本。对于汉诺塔，这是1个盘子的谜题。当然，这几乎不是一个“谜题”，因为我们只需移动一个盘子，从一个柱子移到任何其他柱子即可解决它。如果我们让 $M(n)$ 代表解决 n-盘子谜题所需的最优 *moves* 的数量，那么我们刚刚确定了 $M(1)=1$。为了确定 $M(2)$，我们可以使用上一段中的观察结果，并说

$$\underbrace{M(2)}_{\text{solve 2-disk}} = \underbrace{M(1)}_{\text{solve 1-disk}} + \underbrace{1}_{\text{shift largest disk}} + \underbrace{M(1)}_{\text{solve 1-disk}} = 1+1+1=3$$

然后它必须是

$$M(3) = M(2)+1+M(2) = 3+1+3 = 7$$

和

$$M(4) = M(3)+1+M(3) = 7+1+7 = 15$$

并且如此。你注意到模式了吗？这些数字都是2的幂次减1，特别是，我们注意到对于迄今为止我们看到的每个情况，$M(n)=2^n-1$，指出观察这个模式并不*prove*这个模式；仅仅因为它在前4个情况中有效，并不意味着趋势会继续，这正是归纳证明要完成的。此外，认识到这个模式和“观察”到$M(n)=2^n-1$是一个非平凡的事情，本身。我们碰巧知道答案，并且没有问题为你识别出公式。你可能应该自己尝试“解决”以下关系

$$M(n) = 2M(n-1)+1 \quad \text{and} \quad M(1)=1$$

并且看看你是否可以推导出公式 $M(n) = 2^n - 1$。这种公式之所以比上面的关系 *nicer*，是因为现在 $M(n)$ 只依赖于 n，而不是依赖于之前的项（例如 $M(n-1)$）。这种关系以及类似的关系被称为 *recurrence relations*，通常很难解决！

我们知道如何解决这个问题，尽管如此，它产生了 $M(n) = 2^n - 1$。我们将把它留给你来验证。你可以通过检查方程上的一些值来做这件事，但我们都知道那不是 *proof*。试着通过归纳步骤来实际证明它！我们已经做了大部分工作，但将取决于你仔细清楚地安排一切。记住，你应该确定每个多米诺骨牌上的“事实”，确保多米诺1倒下，然后对多米诺 n 倒入多米诺 $(n+1)$ 进行一般论证。试着写出这个证明。细节对你来说有意义吗？试着向朋友展示你的证明，看看他们是否理解。你需要告诉他们其他什么吗或引导他们通过它？考虑最好的方法来 *explain* 你的方法和步骤，以便书面版本足够，你不必添加任何口头解释。

2.5.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 如何证明递归程序是归纳的?

(2) 汉诺塔的归纳结构是什么？我们在解决3盘拼图问题时，在哪里解决了2盘拼图问题?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 按照伪代码 `factorial` 的步骤计算 5!。 (2) 按照伪代码 `Fibonacci` 的步骤计算 $F(5)$。 (3) 用 4 个盘子解决汉诺塔问题。确保你能

o

在 *optimal* 次移动中 it，$2^4 - 1 = 15$。

2.6 Summary

我们现在已经看到了一些**inductive arguments**的例子。我们意识到，我们解决的一些谜题使用了类似的论证风格，并探讨了几个例子，以了解这种论证中可能出现的不同问题。具体来说，我们看到了归纳论证总是关于证明一个求和公式或方程：归纳论证可以应用于*any*的情况，其中某个事实依赖于该事实的“先前实例”。这使我们开始发展一个关于归纳如何工作的类比，从数学的角度来说。我们现在对用“多米诺类比”来思考归纳感到很舒服，但我们向前推进的主要目标之一是严格地*stating*和*proving*归纳原理。现在，让我们大量练习使用这类论证。这就是本章练习想要达到的目的。稍后，一旦我们形式化了归纳，我们会从中受益，并对这个概念有一个深入的理解！

2.7 Chapter Exercises

这里有一些问题，可以帮助你熟悉归纳式论证。我们在这里不是寻找完全严格的证明，只是对正在发生的事情进行良好描述，并记录你的步骤。一旦我们确立了数学归纳法原理（PMI）和相应的证明策略，我们将回头对其中一些进行严格证明。

Problem 2.7.1. 证明以下求和公式对每个自然数以及 $n = 0$ 都成立：

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

后续问题：使用这个结果来表示在2^n支队伍的单败淘汰赛制比赛中需要多少场比赛才能确定胜者。（例如，NCAA疯狂三月锦标赛采用这种格式，有$n = 6$支队伍。）

Problem 2.7.2. 证明对于每个大于或等于2的自然数n，都有$3^n \geq 2^{n+1}$。

Problem 2.7.3. 对于哪些自然数 n 以下不等式成立？先陈述一个命题，然后证明它。

1. $2^n \geq (n+1)^2$ 2. $2^n \geq n!$
3. $3^{n+1} > n^4$ 4. $n^3 + (n+1)^3 > (n+2)^3$

Problem 2.7.4. **The December 31 Game:** 两位玩家轮流从日历中命名日期。在每一轮中，玩家可以增加月份或日期，但不能同时增加。起始位置是1月1日，说出12月31日的人获胜。确定第一玩家的获胜策略。

例如，一个导致玩家1获胜的移动序列如下:

(1) 1月10日，(2) 3月10日，(1) 8月10日，(2) 8月25日，(1) 8月28日，
(2) 11月28日，(1) 11月30日，(2) 12月30日，(1) 12月31日

通过 *winning strategy*，我们指的是玩家1遵循的一种玩法，无论玩家2做什么，都能确保 *guar- antees* 胜利。

Problem 2.7.5. 找到一个公式并证明一个 *geometric series* 的和，它是一个形如的级数

$$\sum_{i=0}^{n-1} q^i$$

对于某些实数 q 和某些自然数 n。(提示：当 $q =$ 为 1 时请小心。)

Problem 2.7.6. 编写一个句子，该句子依赖于n，使得当n的值从1到99（包括99）时，该句子为真，但当$n =$为100时，该句子为假。

Problem 2.7.7. 以下关于 $a^n = 1$ 对于每个 n 的“伪造”声明有什么问题?

“Spoof”: 设 a 为一个非零实数。注意 $a^0 = 1$。此外，注意我们可以递归地写出

$$a^{n+1} = a^n \cdot a = a^n \cdot \frac{a^n}{a^{n-1}} = 1 \cdot \frac{1}{1} = 1$$

“□”

Problem 2.7.8. 在一个未来社会中，只有两种货币面额：一枚值3布伦丹的硬币和一枚值8布伦丹的硬币。还有一项全国性法律规定，店主只能收取可以用这两种硬币支付的价格。

咖啡店老板可能会向你收取多少法律费用?

Hint: 尝试一些小的值并看看会发生什么。

Problem 2.7.9. 考虑一个大小为 $2^n \times 2^n$ 的棋盘，对于某个任意的自然数 n。从棋盘上移除 **any** 个方块。是否可以用 L-形的三连形来铺满剩余的方块?

如果你的答案是 Yes，请证明它。

如果你的答案是 No，请提供一个反例论证。（也就是说，找到一个 n，使得没有任何 *possible* 方式可以铺满棋盘，并说明为什么这是这种情况。）

Problem 2.7.10. 考虑一个 $n \times n$ 格的方块。在这个网格中存在多少个子方块，无论大小？例如，当 $n = 2$ 时，答案是 5：有 4 个 1×1 的方块和 1 个 2×2 的方块。为你的答案找到一个公式，并尝试证明它是正确的。

Problem 2.7.11. 证明，在至少有2个人的队伍中，如果第1个人是女性且最后一个人是男性，那么队伍中某处有一个男性站在一个女性后面。

Problem 2.7.12. 证明对于每一个自然数 n，$n^3 - n$ 是 3 的倍数。

Problem 2.7.13. 一个 **binary n-tuple** 是由 0 和 1 组成的有序字符串，字符串中总共有 n 个数字。提供一个 *inductive argument* 来解释为什么有 2^n 个可能的二进制 n-元组。

Problem 2.7.14. 回想一下，**Fibonacci Numbers** 是通过将 $f_0 =$ 设置为 0 和 $f_1 =$ 设置为 1 来定义的，然后对于每个 $n \geq 2$，设置 $f_n = f_{n-1} + f_{n-2}$。这产生了序列 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, . . .

您可能不知道斐波那契数列也有一个 *closed form*；也就是说，除了上面给出的常规递归定义外，还有一个特定的 *formula* 来定义它们。这里就是：

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

证明该公式对所有 $n \geq 0$ 的值都正确。

Problem 2.7.15. 再次，考虑斐波那契数列 f_n，证明以下：

1. $\sum_{i=0}^{n} f_i = f_{n+2} - 1$
2. $\sum_{i=0}^{n} f_i^2 = f_n \cdot f_{n+1}$
3. $f_{n-1} \cdot f_{n+1} - f_n^2 = (-1)^n$
4. $f_{m+n} = f_n \cdot f_{n+1} + f_{m-1} \cdot f_n$
5. $f_n^2 + f_{n+1}^2 = f_{2n+1}$

Problem 2.7.16. 尝试提供一个归纳论证，解释为什么每个自然数 $n \geq 2$ 都可以写成素数的乘积。你也能证明这个乘积是 *unique* 吗？也就是说，你也能解释为什么有 *exactly one way* 将自然数分解为素数的必要性吗？

Problem 2.7.17. 证明

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

Problem 2.7.18. 以下“欺骗”有什么问题，所有的笔都有相同的颜色。

“Spoof”: 考虑一组尺寸为1的钢笔。由于只有1支钢笔，它当然与自己颜色相同。

假设任何一组 n 支笔在组内只有一种颜色。（注意：我们已解释为什么这个假设对于 $n = 1$ 是有效的，因此我们可以做出这个假设。）取任意一组 $n + 1$ 支笔。将它们在桌子上排成一排，并从 1 到 $n + 1$ 编号，从左到右。看看它们中的前 n 支，即看看笔 $1, 2, 3, \ldots, n$。这是一组 n 支笔，所以根据假设，组内只有一种颜色。（我们还不确定那是什么颜色。）然后，看看这些笔中的最后 n 支；即看看笔 $2, 3, \ldots, n + 1$。这也是一组 n 支笔，所以根据假设，这个组中也只有一种颜色。现在，笔 #2 恰好属于这两个组。因此，无论笔 #2 是什么颜色，那也是 *both* 组中每支笔的颜色。因此，所有 $n + 1$ 支笔都有相同的颜色。

通过归纳，这表明任何尺寸的钢笔组都只有一种颜色被代表。因此，观察世界上有限的钢笔集合，我们只应找到一种颜色。“□”

Problem 2.7.19. ⋆ 此问题分析起来很*extremely difficult*，并摘自著名数学家陶哲轩的博客（链接在此）。

有一个岛上居住着一个部落。这个部落由1000人组成，有着各种眼睛颜色。然而，他们的宗教禁止他们知道自己的眼睛颜色，甚至讨论这个话题；因此，每个居民都可以（并且确实）看到其他居民的眼睛颜色，但无法发现他或她的自己的（没有反射表面）。如果一个部落成员发现了自己的眼睛颜色，那么他们的宗教会迫使他们第二天中午在村庄广场上当众进行仪式性自杀。所有部落成员都非常逻辑和虔诚，他们都知道彼此也非常逻辑和虔诚（他们也都知道他们都知道彼此非常逻辑和虔诚，以此类推）。

（为了这个逻辑谜题的目的，“高度逻辑”意味着任何可以从岛民可用的信息和观察中逻辑推导出的结论，岛民都会自动知道。）

在1000个岛民中，结果发现其中100人有蓝眼睛，900人有棕眼睛，尽管岛民最初并不了解这些统计数据（他们当然只能看到1000个部落成员中的999个）。

一天，一位蓝眼睛的外国人来到岛上，赢得了部落的完全信任。

一个晚上，他向整个部落致谢，感谢他们的款待。

然而，由于不了解习俗，外国人错误地在问候中提及眼睛颜色，评论道
how unusual it is to see another
blue-eyed person like myself in this region of the world。

这个失态对部落有什么影响，如果有影响的话?

2.8 Lookahead

在这一章中，我们向您介绍了**mathematical in- duction**的概念。我们探讨了几个通过归纳过程引导我们解决问题的谜题示例，然后描述了如何通过 *proof by induction*来遵循*rigorously verify*该解决方案。到目前为止，我们拥有的数学技术和概念，我们必须依赖非技术性的类比来向您描述这个过程。想象一排无限长的多米诺骨牌，上面写着“事实”，相互碰撞，这是对这个过程的完美合理解释，但它未能代表归纳的完整数学范围。从某种意义上说，这就像一个朋友向你描述如何挥高尔夫球杆，尽管你以前从未打过高尔夫。当然，他们可以给你一些挥杆“感觉”的心理图像，但如果没有亲自出去练习，你如何真正理解高尔夫挥杆的力学呢？你如何学习如何调整你的挥杆，或者区分使用球杆和五号铁杆以及沙坑杆的差异呢？通过研究潜在的力学并练习这些概念，我们希望更好地理解数学归纳法，以便在未来，我们可以适当地使用它，识别出它有用的场合，并最终学会如何*adapt*它到其他场合。当然，记住多米诺比类可以帮助我们引导直觉，但我们也应该记住，它不是严谨的数学。它也没有完美地描述我们讨论的其他例子，其中倒下的多米诺不仅依赖于它后面的一个，还依赖于它前面的几个。

在下章節中，我們將探討一些有關的概念，這些概念用於謹慎地陳述和證明數學歸納作為證明技術。具體而言，我們將研究一些 *mathematical logic* 的想法，並調查如何將複雜的數學陳述和定理分解為其構成部分，以及如何從基本構建塊中構建有趣和複雜的陳述。在這過程中，我們將介紹一些新的符號和縮寫，這將使我們能夠將我們所說的一些冗長陳述縮短為簡潔（並精確）的數學語言。有了這些，我們將探討一些更基礎的證明策略，然後將其應用於本課程的 *ev- erything else we do*，包括歸納技術本身！我們還將研究 *set theory* 的某些想法，這是構成所有其他分支的基礎的數學分支。這對於未來組織我們的思路將非常有益，但它也將幫助我們嚴謹地定義 *natural numbers*。在我們集體掌握這兩個數學分支的某些概念和知識後，我們將能夠在堅實的基礎上建立數學歸納，並繼續正確地使用它。

Chapter 3

Sets: Mathematical Foundations

3.1 Introduction

现在是集合教育的时候了！在上一章之后，这样的跳跃可能看起来有些奇怪。当我们说这实际上是非常自然且最终是必要的时，您必须相信我们。我们在数学中所做的一切都是建立在**sets**的基础上的，所以我们最好开始谈论它们并习惯它们。

3.1.1 Objectives

以下本引言中的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作将如何有所帮助，它们将激励我们为什么要关注本章中出现的主题，并且它们将告诉您我们的目标和在阅读过程中您应该牢记什么以实现这些目标。现在，我们将通过一系列声明为您总结本章的主要目标。以下各节将更详细地重申这些观点，但这将为您提供一份供未来参考的简要清单。当您完成本章的学习后，请回到这份清单，看看您是否理解了所有这些目标。您明白为什么我们将它们列为重要吗？您能定义我们使用的所有术语吗？您能应用我们描述的技术吗?

By the end of this chapter, you should be able to ...

- 定义什么是集合，并识别几个常见例子。
- 使用适当的符号定义一个集合并引用其元素。

- 定义和描述几种操作集合的方法；即确定如何从两个或更多集合中创建新集合的方法。

- 描述如何比较两个集合，以及应用适当的技术来证明这些主张。

- 解释自然数与集合的关系，并将其与数学归纳法联系起来。

3.1.2 Segue from previous chapter

我们正在构建一个形式化的数学归纳法声明作为 *theorem*，然后我们将对其进行证明。为了达到这个目标，我们需要一些基本的对象来进行工作和讨论，逻辑上。集合就是那些对象！从历史上讲，数学是在20世纪初的转折点相对较晚地建立在 *set theory* 基础上的。在此之前，数学家们往往对他们的工作下面真正发生的事情“挥挥手”；他们做出了很多“直观”的假设，并且还没有尝试严格和 *axiomatically* 描述他们所做的一切。在数学家 **Georg Cantor** 的工作展示了令人惊讶的、反直觉的结果，这些结果是完全正确且与我们假设一致之后……我们意识到我们最好决定我们一直在谈论什么。当然，这并不是要贬低1900年以前的数学家的工作！我们只是意味着他们一直在玩一个游戏，在这个游戏中，他们还没有真正就一套规则达成一致。这就是集合论 **axioms** 的意义。

3.1.3 Motivation

当然，我们被我们持续想要了解**proofs**的愿望所驱动，发现它们是什么以及它们是如何工作的，特别是，使数学归纳法更加严谨。然而，更普遍的是，我们对了解数学家真正在做什么感兴趣，我们确信世界上任何一位数学家都能告诉你**sets**在他们工作中有多么重要。他们可能会不情愿地这样做，并说他们自己永远无法从事纯*set theory*的工作，但我们怀疑你找不到任何否认集合重要性的任何人。

所有我们之后所做的一切都将涉及对一组对象提出某种主张；也就是说，我们将尝试说出（并随后证明）某些事实是关于某些特定对象的 True。我们指定这些对象的方式涉及 **sets**。我们表达此类事实的方式将涉及数学逻辑，我们很快就会达到这一点。现在，我们首先需要学习如何表达许多类型的数学对象，在我们甚至可以对它们提出主张之前。

3.1.4 Goals and Warnings for the Reader

本章可能涉及一些对你来说是新的数学概念，与之前章节我们专注于仅依赖于数字、代数和算术以及批判性思维的谜题不同。这些新概念需要仔细阅读和思考。当我们介绍这些概念和结果时，我们希望你能仔细阅读，并在旁边进行思考。数学表述比报纸文章对读者要求更高；它期望一个 *engaged* 读者，即一个会仔细思考每一句话，有时需要暂停几分钟以确保完全理解到目前为止所说内容的读者。在继续阅读时请记住：阅读数学可能很困难，但这是可以预料的！不要让它让你气馁；只需把每一句话都看作是一个更大的待解谜题中的一个单独的拼图块。

特别地，如果这一章的阅读时间（如果不是更长）与前面两章的总和相当，请不要感到惊讶！多年来，我们观察到最令人困惑的部分是集合的 **notation**。这可能是你数学生涯中第一次被期望在写作中尽可能 **precise** 和 **rigorous**。在书面工作中，仅仅"有正确的想法"不再足够；我们真的很关心你确切地表达了你想要说的，没有其他内容。当你阅读我们所写的内容时，问问自己，"为什么这比其他东西更有意义？"在你写下对一个问题或作业问题的答案之后，再次阅读它并问自己，"这实际上有意义吗？它是否表达了我想要说的，我头脑中的想法？别人是否一定会以与我写作相同的方式阅读它？"

此外，本章将涉及比您典型的数学课程更多的 **abstract** 思考。这可能对您来说是个冲击，也可能不是。无论如何，这绝对不是您可以匆匆浏览并期望一眼就能抓住的材料。现在，比以往任何时候，您都应该花时间和精力来消化这些材料。读一些页面，然后在吃饭、洗澡或打篮球时思考这些材料。尝试在现实生活中找到例子。和你的朋友们讨论集合。现在这听起来可能很傻，但最终，这会帮到您。相信我们。

3.2 The Idea of a "Set"

A "Collection of Objects" with a Common Property

集合的直观概念可能对你来说并不完全陌生。如果你是棒球卡收藏家，拥有一套"完整收藏"意味着拥有来自卡制造商特定印刷系列的每一张卡片。如果你和朋友玩桌面游戏，在开始玩之前会商定一套"规则"，以避免之后出现未解决的争议。如果你在生物、化学或物理课上进行了实验室实验，你会收集信息到一个"数据集"中，并分析这些结果来检验一个假设。

这些是三个不同的情况，每个都涉及到单词 **set**，那么这个词究竟有什么关联这些上下文并赋予其适当意义的地方呢？本质上，一个集合指的是一些具有某种共同属性的物体的集合。在第一个例子中，1995年Topps生产的每张棒球卡的副本都属于那个特定的集合。在第二个例子中，任何达成的约定都属于你的规则集合。在第三个例子中，你在实验中收集到的任何数据点都属于你的数据集。在每种情况下，都有一个共同属性，使我们能够将特定的物体相互关联，并将它们称为一个集合。

Sets in Mathematics

集合在数学中非常常见、流行、有用且基本。由于数学家处理抽象对象以及这些对象之间的关系，如果不能引用数学对象的集合，就很难准确地描述自己在想什么。实际上，我们已经在这样做过了！

例如，在研究多项式和二次公式时，我们提到，一个判别式为负的二次多项式 $p(x) = ax^2 + bx + c$（当 $\frac{b^2}{4a} - c < 0$ 时）将没有根 *in the set of real numbers*。我们这是什么意思？你理解这句话了吗？我们试图传达的想法是，无论我们从所有实数的集合中选择什么实数 x，都可以保证 $p(x) \neq 0$。但实数集到底是什么？它是如何定义的？我们如何能如此确信它甚至存在？这些问题实际上相当难以回答，试图回答这些问题将使我们偏离课程，进入集合论的世界。

在数学的语言中，我们希望我们的句子和陈述是 *precise* 和 *unambiguous*，并且我们寻求基于某些基本假设建立真理。我们需要将这些假设作为起点，否则我们就没有任何依据来建立我们的真理。这些在“玩数学游戏”之前大家都同意作为“规则集”一部分的假设，被称为 **axioms**。

也许，如果你研究过一些几何学或者阅读过关于古希腊数学家欧几里得及其著作《几何原本》的内容，那么你之前可能已经听说过“公理”这个词。欧几里得*proved*所提出的所有基本几何学结果都是建立在一些基本假设之上的：任何两点都可以由一条线段连接，给定一个中心点和半径的圆必须存在，非平行线相交，等等。这些陈述在最初只是*agreed upon*被True。

另一个我们发现公理的地方是在被称为**set theory**的数学分支中。这个分支的公理将所有涉及集合的结果建立在坚实的基础上，并且使用这些公理以及从它们推导出的结果，我们可以在数学宇宙中继续发现新的真理。然而，研究这些公理及其后果更适合于一门专门研究集合论的课程，我们将探讨集合论中的许多后果。

公理未经严格证明就被接受。这并不是因为这样的证明不可能，只是因为在这个书中完成它们会花费太多时间和空间。

我们所 *will* 做的是提供一个“集合”的定义，这个定义在我们在这本书中使用集合的上下文中是令人满意的。我们还将定义一些集合的基本属性，分享一些说明性示例，并讨论我们可以对集合执行的不同操作以创建新的集合。

3.3 Definition and Examples

3.3.1 Definition of “Set”

让我们从一个定义开始。正如我们上面解释的那样，我们通常认为集合是由组合到该集合中的对象以及使这种组合有意义的属性来表征的。以下定义试图尽可能精确地表达这个概念，同时引入一些相关的符号和术语。

Definition 3.3.1. *A* **set** *is a collection of all objects that have a common, well-defined property. The objects contained in a set are called* **elements** *of the set. The mathematical symbol “$\in$” represents the phrase “is an element of” (and “$\notin$” represents “is not an element of”).*

3.3.2 Examples

让我们直接从一些集合（甚至非集合）的具体例子开始，以说明这个定义。在数学中，通常用大写字母来指代 *sets*，用小写字母来指代 *elements* 的集合，我们将经常遵循这个惯例（但不总是）。为了定义或描述一个集合，我们需要确定那个将集合的元素相互联系起来的共同、明确的属性。例如，我们可以定义 B 为所有大联盟棒球队的集合。这是一个明确的属性吗？如果我们给你一个物体，你能给出一个明确的 Yes/No 答案来回答“这个物体有这个定义属性吗？”是的，情况就是这样，这是一个表征集合的属性。（为了避免未来读者的混淆，让我们更具体地说，B 指的是2012赛季的MLB球队。）在数学的语言中，我们会写成

$$B = \{\text{Major League Baseball teams from the 2012 season}\}$$

“花括号”——{和}——表示它们之间的描述将标识一个集合，其中的文本是对对象及其共同、明确属性的描述。现在可以说匹兹堡海盗$\in B$和匹兹堡企鹅$\notin B$是有意义的。

常见的将数学符号 $\in$ 译成英文的方法是 **“is an element of”** 或 “是...的成员” 或 “属于...” 或 “在...中”。我们将主要

使用“是……的元素”因为它在这些表达中是最不模糊的，并且适当地使用了数学术语 **element**。根据上下文，可以使用这些其他等效的表达，但它们不太可取。（特别是，“是……的”可能会与其他集合关系混淆，因此我们将完全避免使用它，并鼓励您也这样做。）

我们已经看到一些常用的数字集合。你知道它们是什么，因为之前对这些数字的工作，但你可能通常不会把它们当作集合，而它们正是集合！

$$\begin{aligned}
\mathbb{N} &= \{\text{ natural numbers }\} = \{1, 2, 3, \ldots\} \\
\mathbb{Z} &= \{\text{ integers }\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\
\mathbb{Q} &= \{\text{ rational numbers }\} \\
&= \{\text{numbers of the form } \frac{a}{b} \text{ , where } a, b \in \mathbb{Z} \text{ and } b \neq 0\} \\
\mathbb{R} &= \{\text{real numbers}\}
\end{aligned}$$

考虑一下上面 $\mathbb{Q}$ 的第二个定义是如何有意义的。我们很快就会看到一个更简洁的方式来写出像“形式为……blah blah……的数字，以及额外的信息是……blah blah”这样的短语。另外，我们实际上无法真正定义 $\mathbb{R}$，除了说它们是实数。你甚至如何定义实数呢？你尝试过吗？

3.3.3 How To Define a Set

另一种定义或描述集合的方法是简单地列出其所有元素。当集合中的元素数量较少时，这样做很方便。例如，以下对集合 V 的定义都是 *equivalent*：

$$\begin{aligned}
V &= \{\text{A,E,I,O,U}\} \\
V &= \{\text{vowels in the English language}\} \\
V &= \{\text{U,E,I,A,O}\}
\end{aligned}$$

通过“等价”，我们指的是上面的每一行都定义了*same*集合V，使用不同的术语。（注意：我们采用了y是辅音的惯例，所以$y \notin V$。）与对象A、E、I、O和U相关联的常见、定义明确的属性是它们都是元音（如第二定义所示），由于只有五个这样的对象，因此简单地列出它们（如第一定义所示）既简单又方便。

Order and Repetition Don’t Matter

为什么你认为第三个定义与其他定义相同？它指的是同一组对象，任何集合都完全由其元素来表征，因此我们写入元素 *does not matter* 的 *order* 是 U$\in V$吗？无论 U 是否在元素列表中排在首位或末位，这个问题的答案都是“是”。

不仅集合中元素的顺序无关紧要，元素的 {v*} 也不重要！也就是说，集合 $A = \{a, a, a\}$ 和集合 $A = \{a\}$ 完全相同。再次提醒，集合完全由其元素来表征；我们只关心集合中“有什么”。（我们将在第 3.4.4 节再次提及这一点，当我们讨论集合的“袋类比”时。）写 $A = \{a, a, a\}$ 只是一种三重冗余的说法，即 $a \in A$ 和 *only* a 是 A 的一个元素。因此，$A = \{a\}$ 是表达相同信息的最简洁方式。

The Common Property Might Be Being an Element of That Set

现在，仍然遵循我们可以通过写出所有元素来定义一个集合的想法，考虑以下集合的定义 A:

$$A = \{2, 7, 12, 888\}$$

当然，这是一个集合，因为我们只是通过列举其元素来定义它的。但是，将它的元素联系起来的共同、明确的属性是什么呢？对于元音的集合 V，我们可以列举元素 *and* 提供一个语言定义，但对于这个集合 A，似乎我们只能列举元素而不知道如何 *describing* 它们的共同属性。然而，从数学的角度来看，2, 7, 12, 888 这几个数的共同属性是它们都是这个集合 A 的元素！在数学宇宙中，我们有抽象思维的自由，仅仅通过讨论这个集合 A 和它的元素，我们就赋予了它们这个共同属性。这对你来说满意吗？你能想出一个共同、明确的属性，它能产生恰好是 A 的元素吗？（提示：找到一个多项式 $p(x)$，其 *roots* 是 2, 7, 12 和 888。）如果一个集合的元素有多个将它们联系起来的属性，你认为我们在提到集合时考虑哪个属性重要吗？你对集合 $S := \{2, 7, \text{M}, \text{波士顿红袜队}\}$ 有何看法？除了我们在这里列举的事实之外，可能还有其他共同属性吗？

Ellipses Are Sometimes Okay, But Informal

有时，当关于所讨论的集合没有混淆，或者它已经以另一种方式定义，并且我们希望列出一些元素作为示例时，使用省略号来浓缩集合元素的列举是方便的。例如，我们可能会写

$$E = \{\text{even natural numbers}\} = \{2, 4, 6, 8, 10, \dots\}$$

这个集合是 *infinitely large*，实际上，即使我们尝试，也无法列出其所有元素，但从列出的前几个元素中可以清楚地看出，我们指的是偶数，尤其是因为我们已经将 E 称为“偶自然数集合”。然而，我们无法强调这一点是 *not* 对所讨论集合的精确定义。在非正式场合，这已经足够，但它不是数学上严谨的，这一点在我们讨论以下定义集合的正确方法时将变得清晰。

Set-Builder Notation

最佳定义或描述集合的方法是将其元素识别为具有特定属性的另一个集合中的特定对象。例如，如果我们想引用包含1到100（含）之间所有自然数的集合S，我们可以列出所有这些元素，但这需要大量的不必要的书写。我们还可以使用省略号表示法$S = \{1, 2, 3, \ldots, 100\}$，但同样，如果没有已经正式定义$S$，这仍然不够精确。（有人可能会以不同的方式误解省略号。）更精确、更简洁的方法是写出

$$S = \{x \in \mathbb{N} \mid 1 \leq x \leq 100\}$$

我们将其读作“S是自然数集合$such\ that$ $1 \leq x \leq 100$中的所有对象集合x”。

条形符号 | 读取为 **“such that”**，表示左侧的信息告诉我们对象来自哪个“更大的集合”，而右侧的信息告诉我们这些对象应该具有的特定属性。

注意：不要在其他上下文中使用 not 和 | 来表示“使得”。这仅在定义集合的上下文中是可接受的。它仅用作占位符，以将左侧——我们用来抽取元素的集合——与右侧——描述这些元素应具有的属性——分开。

这是一个非常流行且有用的**set-builder notation**的例子。我们之所以这样称呼它，是因为我们是通过从“更大的”可能性集合中抽取元素来构成一个 $building$，并且只包括那些具有特定属性的元素。为此，我们需要向读者说明（1）更大的集合是什么，以及（2）共同属性是什么。让我们通过几个例子来说明这个概念：

$$\begin{aligned}
S &= \{x \in \mathbb{N} \mid 1 \leq x \leq 100\} = \{1, 2, 3, \ldots, 100\} \\
T &= \{z \in \mathbb{Z} \mid \text{we can find some } k \in \mathbb{Z} \text{ such that } z = 2k\} \\
&= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\
U &= \left\{x \in \mathbb{R} \mid x^2 - 2 = 0\right\} = \left\{-\sqrt{2}, \sqrt{2}\right\} \\
V &= \left\{x \in \mathbb{N} \mid x^2 - 2 = 0\right\} = \{\ \}
\end{aligned}$$

最后两个例子显示了**context**的极端重要性。当我们改变从中抽取元素的 $larger\ set$时，相同的共同属性（满足$x^2 - 2 = 0$）可以通过一组不同的元素来满足。两个实数满足该属性，但没有任何自然数满足它！任何有理数满足该属性吗？你怎么想？

这是因为指定更大的集合绝对必要。像“$U = \left\{x \mid x^2 - 2 = 0\right\}$ 是 $meaningless$ 因为它是模糊的，可能会产生完全不同的解释。

Reading Notation Aloud

我们在这里真正学习了一个新的 **language**，这些都是一些基本的单词和语法规则。我们需要练习翻译这些句子。

将句子翻译成英语（在我们的脑海中和大声说出）以及相反。例如，我们可以将上面S的定义说成以下任何一种，都是合理的:

S 是所有自然数 x 的集合，其中 x 在 1 和 100 之间，包括 1 和 100。

S 是包含1到100之间所有自然数的集合，包括100。

S 是满足不等式 1 {v*} 100 的所有自然数 x 的集合。

S 自然数集 x 满足 $1 \leq x \leq 100$ 的性质。

注意，它们都识别了更大的集合和共同属性；它们之间的唯一区别是语言/语法上的，它们并没有改变数学意义。

尝试为其他定义编写类似的句子。尝试从朋友那里得到一个集合的口头定义，并用数学符号写下他们所说的话。

考虑我们之前看到的有理数 $\mathbb{Q}$ 的定义，并注意我们可以将其重写为:

$$\begin{aligned}\mathbb{Q} &= \left\{ \frac{a}{b} \text{ , where } a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\} \\ &= \left\{ x \in \mathbb{R} \mid \text{we can find } a, b \in \mathbb{Z} \text{ such that } \frac{a}{b} = x \text{ and } b \neq 0 \right\}\end{aligned}$$

注意这两个定义之间的细微差别。上面的一个告诉我们所有有理数都是**of the form** $\frac{a}{b}$，然后告诉我们 a 和 b 必须满足的特定假设。下面一个告诉我们所有有理数都是具有特定属性的 *real* 数，即我们可以将那个实数表示为整数的比。我们强烈倾向于下面的定义，因为它告诉我们更多信息。

一般来说，如果 $P(x)$ 代表一个句子（涉及英语和/或数学语言）来描述一个特定、定义明确的 *property*，并且 X 是一个给定的集合，那么该符号

$$S = \{x \in X \mid P(x)\}$$

是读作

“S 是集合 X 中所有满足属性 $P(x)$ 为真的元素 x 的集合”。

在符号 $P(x)$ 中，字母 x 代表一个变量对象，并且根据我们用作 x 的特定对象，属性 $P(x)$ 可能成立（即 $P(x)$ 为真）或失败（即 $P(x)$ 为假）。如果属性成立，那么我们将 x 包含在 S (so $x \in S$) 中，如果它失败，我们不在 S (so $x \notin S$) 中包含 x。

返回到我们关于偶数自然数集合 E 的例子，更精确地写法是

$$\begin{aligned}E &= \{\text{even natural numbers}\} \\ &= \{x \in \mathbb{N} \mid \text{there is a natural number } n \text{ such that } x = 2n\}\end{aligned}$$

注意这里有两个“层”的属性。如果一个自然数包含在我们的集合 E 中，那么我们可以找到一个自然数 *another*，使得它是一个自然数 n，并且具有额外的属性 $x = 2n$。试着为奇数集合或完全平方数集合写下类似的定义。那么质数集合呢？回文数集合呢？完全数集合呢？你能使用集合表示法为这些集合写出定义吗？

3.3.4 The Empty Set

如果没有元素满足属性 $P(x)$，会发生什么？例如，考虑以下定义

$$S = \left\{x \in \mathbb{N} \mid x^2 - 2 = 0\right\}$$

我们知道，具有该属性的我们要“寻找”的数 x 是 $\sqrt{}2$（以及 $-\sqrt{}2$，也是）但 $\sqrt{}2 \notin \mathbb{N}$。因此，无论我们让 $\mathbb{N}$ 的哪个元素代表 x，由“$x^2 - 2 = 0$”给出的属性 $P(x)$ 实际上 *fails*。因此，这个集合中没有元素。这真的是一个集合吗？

记住，一个集合完全由其元素来定义，一个包含*no elements*的集合，例如这个集合，就由这个事实来定义。如果我们尝试列出其元素，我们将得到{}。实际上，这个集合非常特殊，以至于我们给它一个名称和符号：

Definition 3.3.2. *The* **empty set** *is the set which has no elements. It is denoted by the symbol* $\varnothing$.

存在许多使用集合构造符号定义空集的方法。（是的，我们指的是 *the* 空集；只有一个没有元素的集合！）我们上面看到了一个例子，我们相信你能想出很多其他的。例如，考虑以下集合：

$$\{a \in \mathbb{N} \mid a < 0\}$$
$$\{r \in \mathbb{R} \mid r^2 < 0\}$$
$$\{q \in \mathbb{Q} \mid q^2 \notin \mathbb{Q}\}$$

你看到为什么这些都定义了同一个集合，即空集吗？

Context Matters

我们应该再次注意指定较大的集合 X 的重要性，我们从该集合中抽取变量元素 x，在上述类似集合定义中。例如，考虑以下两个集合：

$$S_1 = \{x \in \mathbb{N} \mid |x| = 5\} = \{5\}$$
$$S_2 = \{x \in \mathbb{R} \mid |x| = 5\} = \{-5, 5\}$$

(注意：使用上文中看到的下标表示法，**index** 集合也非常常见，这使得我们可以多次使用相同的字母。)

这个规范显然很重要，在这种情况下，因为它产生了两个完全不同的集合！因此，在以这种方式定义集合时，我们必须精确且清晰。像 $S = \{x \mid |x| = 5\}$ 这样的定义应被视为含糊不清且不理想的，因为它会导致上述问题。

3.3.5 Russell's Paradox

也许这看起来像是在吹毛求疵，但我们对这种激烈态度的推理根植于集合论的一些基本思想。我们希望避免在没有这项政策的情况下可能出现的某些复杂问题和悖论。有一个特别著名的涉及集合的悖论例子，说明了为什么我们必须在上文所述段落中指定一个更大的集合，即当我们使用集合构造符时。这个例子被称为*Russell's Paradox* (，以英国数学家伯特兰·罗素)的名字命名，我们将在本节中介绍和讨论它。

Sets Whose Elements Are Sets

首先，我们应该指出，这次讨论将引入一个概念，即集合也可以是其他集合的*elements*。现在这听起来可能是一个奇怪且抽象的想法，但在数学中这是一个基本概念。

对于一个具体的例子，回想一下我们所有的美国职业棒球大联盟球队集合 B 。我们也可以将每个球队视为一个集合，其元素是球队中的球员。因此，可以说

$$\text{德里克·杰特} \in \text{纽约洋基} \in B$$

自从德里克·杰特是集合*New York Yankees*的一个元素，而这个集合本身又是集合B的一个元素。（然而，请注意德里克·杰特$\notin B$。由“$\in$”表示的关系不是**transitive**。我们将在稍后定义这个术语。现在，我们将指出，在实数集合is上由“$\leq$”表示的关系是传递的。如果我们知道$x \leq y \leq z$，那么我们可以推断出$x \leq z$。这种情况与“$\in$”关系也是一样的。）

另一个例子是 $S = \{1, 2, 3, \{10\}, \varnothing\}$。是的，空集本身也可以是另一个集合的元素，就像集合 $\{10\}$ 一样。为什么不能呢？作为一个思维练习，我们建议思考 $\varnothing$、$\{\varnothing\}$、$\{\{\varnothing\}\}$ 等之间的区别。为什么它们是不同的集合？

一个最终的例子涉及自然数 $\mathbb{N}$。让我们用 $\mathbb{O}$ 和 $\mathbb{E}$ 分别表示自然数 *odd* 和 *even*。那么，集合 $S = \{\mathbb{O}, \mathbb{E}\}$ 是什么，它与 $\mathbb{N}$ 有何不同，如果有不同的话？这是一个微妙的问题，所以请仔细思考。

The Paradoxical "Set"

花些时间在旁边思考这个概念：集合的元素也是集合的集合。然而，现在让我们继续解释罗素悖论。考虑以下“集合”的定义。我们称之为“集合”，因为它是

实际上 not 是一个定义良好的集合，但还需要弄清楚为什么是这样。当明确这不是一个集合时，这将是我们使用集合构造符号时指定更大集合以从中抽取的论据；这是因为下面的定义没有指定更大的集合。以下是该定义：

$$\mathcal{R} = \{x \mid x \notin x\}$$

这是！这是一个集合吗？$\mathcal{R}$ 的元素是什么？想想上面定义的内容：$\mathcal{R}$ 的元素是那些恰好也是 not 的元素的集合。你能识别出 $\mathcal{R}$ 的任何元素吗？你能识别出不是 $\mathcal{R}$ 元素的对象吗？

第一个问题更容易回答：我们迄今为止讨论的任何集合都将是 $\mathcal{R}$ 的元素。例如，空集 $\varnothing$ 包含 no 个元素，所以它肯定不包含 $itself$ 作为元素。因此，$\varnothing \in \mathcal{R}$。另外，请注意$\mathbb{N} \notin \mathbb{N}$ (，因为自然数集本身不是自然数)，因此 $\mathbb{N} \in \mathcal{R}$ 。

识别是 not 的元素的对象是一个非常棘手的问题，我们将通过以下问题来帮助你：$\mathcal{R}$ 是它自己的元素吗？$\mathcal{R} \in \mathcal{R}$ 是真的还是假的？在继续阅读之前仔细思考这个问题。我们将引导你考虑适当的因素。

- 假设 $\mathcal{R} \in \mathcal{R}$ 是 True。

  定义属性 $\mathcal{R}$ 告诉我们，它的任何元素都是一个不包含自身作为元素的集合。因此，我们可以推断出 $\mathcal{R} \notin \mathcal{R}$。

  等一下！知道 $\mathcal{R} \in \mathcal{R}$ 让我们得出结论，事实上，$\mathcal{R} \notin \mathcal{R}$。当然，这些矛盾的事实不可能同时成立。因此，我们的原始假设一定是错误的，所以必须是 $\mathcal{R} \notin \mathcal{R}$，而不是这样。

- 现在，假设 $\mathcal{R} \notin \mathcal{R}$ 是 True。

  定义属性 $\mathcal{R}$ 告诉我们，任何是 $not\,\mathcal{R}$ 的元素的对象必须是其自身的元素。（否则，它将被包括为 $\mathcal{R}$ 的元素。）因此，我们可以推断出 $\mathcal{R} \in \mathcal{R}$。

  等一下！知道 $\mathcal{R} \in \mathcal{R}$ 让我们推断出，事实上，$\mathcal{R} \notin \mathcal{R}$。这也有矛盾。

无论我们选择哪个选项——$\mathcal{R} \in \mathcal{R}$或$\mathcal{R} \notin \mathcal{R}$——我们都会发现另一个也必须为真，但当然，这些相互矛盾的选项不可能同时为真。

其中包含 **paradox**。这不是一个定义良好的集合。如果是的话，我们就会陷入我们刚才看到的两种情况，而且这两种情况都不可能成立。也不是 $\mathcal{R}$ 简单地等于 $\varnothing$；不，它必须是 $\mathcal{R}$ $does$ 和 not $exist$ 作为集合。

The "Set of all Sets" is *Not* a Set

能否以某种方式修改 $\mathcal{R}$ 的定义，以产生定义试图传达的"集合"？我们应该从哪个"更大的集合"中抽取我们的对象 x，以便定义有意义并正确识别一个集合?

回顾我们在定义之后写的英文解释："{v*}的元素是集合，碰巧这些集合也是它们的元素。" 我们希望测试的具有所需属性($x \notin x$)的对象x实际上是all集合。那么，也许我们只需定义X为所有集合的集合，并将短语"$x \in X$"作为我们定义$\mathcal{R}$的一部分。这样就能解决问题，对吧?

$$\mathcal{R} = \{x \in X \mid x \notin x\}$$

嗯，不，一点也不是！**The "set of all sets" is, itself, *not* a set**。如果是这样，这会让我们陷入之前相同的悖论！没有任何不同，只是我们会明确地声明从其中抽取对象x的"更大的集合"，而这个集合之前是未指定的 $implicitly$。

主要问题是，没有指定一个"更大的集合"来从中抽取对象，或者隐含地引用"所有集合的集合"，会导致这种不受欢迎的悖论。因此，我们不允许这样的定义。任何试图定义一个从"所有集合的集合"中抽取对象x的集合，无论是隐含的还是明确的，都不是集合的$proper\ definition$。

Further Discussion

该属性 $P(x)$ 由"$x \notin x$"给出，本身并没有什么固有的错误。问题是出在我们使用的"更大的集合"上。例如，考虑集合

$$\mathcal{S} = \left\{ x \in \left\{ \frac{1}{2}, \frac{3}{4}, \frac{5}{2} \right\} \,\middle|\, x \notin x \right\}$$

它的元素是什么？唯一可能的是从更大的集合 $\left\{\frac{1}{2}, \frac{3}{4}, \frac{5}{2}\right\}$ 中抽取的元素。注意，这些数字都不是包含自身作为元素的集合。因此，这是对集合 $\left\{\frac{1}{2}, \frac{3}{4}, \frac{5}{2}\right\}$ 的正确定义，本身！在 $\mathcal{R}$ 的先前定义中，我们试图定义的对象被允许作为其自身定义中的变量对象 x 之一，这就是问题所在。

我们希望我们没有让您对集合例子的原始讨论产生太大的偏离，但我们认为指出在数学意义上，可以构造出未定义的"集合"，这些"集合"不是集合，是很重要的。在本书中，我们大部分情况下不会遇到这类问题，但忽略这些问题或根本不提它们，对您作为学生来说是不公平的。如果您对这些问题感兴趣，请寻找一本关于集合论入门的书籍。

存在其他方式可以使"集合"的定义不正确，但以下示例基于（英语）语言问题，而不是像罗素悖论那样的数学基础。例如，我们可以

说“让N成为所有20世纪经典小说的集合。”成为“经典小说”是not一个定义良好的属性，不能用来识别此类集合的元素。经典的概念是主观的，并不严格精确。此外，我们还可以说“让B成为明天将要出生的人的集合”但这个定义中的时间依赖性确保了我们永远不知道B的元素是什么。当明天到来时，定义将随后指向下一天，以此类推。你能想出其他不规范的“元素集合”例子吗？你能想出像上面那样的任何悖论吗？

一般来说，以下陈述是从关于罗素悖论的讨论中得出的最重要的观点：

> 在集合论（集合公理）的约定规则下，存在一个包含所有集合的集合 **no**。

3.3.6 Standard Sets and Their Notation

我们已经参考并使用了一些常见的数字集合，因此现在我们将列出一些集合及其标准符号：

- *natural numbers*: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
- 第一个 n 自然数：$[n] := \{1, 2, 3, \dots, n-1, n\}$
- *integers*: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- *rational numbers*: $\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ 和 } n \neq 0\right\}$
- *real numbers*: $\mathbb{R}$
- *complex numbers*: $\mathbb{C}$

我们已经使用 $\mathbb{N}$ 和 $\mathbb{Z}$ 几次了。由于 $\mathbb{R}$ 已经被占用，我们使用有理数 $\mathbb{Q}$ (，因为有理数 *quotients*) 都是 *fractions* 的，或者是有理数的比，包括正数和负数。实数更难描述。为什么我们不能像 $\mathbb{N}$ 和 $\mathbb{Z}$ 那样列出一些元素？为什么是 $\mathbb{R} \neq \mathbb{Q}$ ？目前，我们基本上是理所当然地接受我们对这些数字集合的集体知识，但稍微思考一下。（我们提到复数 $\mathbb{C}$ 是因为你可能熟悉它们，但在这本书中我们不会有机会使用它们。）

我们如何 *know* 存在像 $\mathbb{N}$ 这样的集合？为什么我们会把 $\mathbb{R}$ 视为数轴？与 $\mathbb{N}$ 相比，$\mathbb{Z}$ 中“更多”的元素有多少？与 $\mathbb{Q}$ 相比，$\mathbb{R}$ 中“更多”的元素有多少？我们甚至能回答这些问题吗？在不久的将来，我们将严格推导出集合 $\mathbb{N}$ 并证明它是唯一具有特定性质的集合。当我们回到对数学归纳法的调查时，这将至关重要。（还记得那一章的目标吗？）

3.3.7 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 符号“$\in$”代表什么？(2) 你会如何大声朗读“$x \in S$”？(3) 一个集合能否成为另一个集合的元素？如果是，请给出一个例子。一个集合能否成为它自己的元素？(4) 你会如何大声朗读“$\{x \in \mathbb{N} \mid x \leq 5\}$”？你能列出这个集合的元素吗？(5) 这个集合是什么：$\{z \in \mathbb{Z} \mid z \in \mathbb{N}\}$？(6) 这个集合是什么：$\{x \in [10] \mid x \geq 7\}$？

(7) 对于以下每个集合，说明它们包含的 *how many* 元素：

(a) $\varnothing$b) $\{1, 2, 10\}$c) $\{1, \varnothing\}$d) $\{\varnothing\}$8) 是 $x \in \{1, 2, \{x\}\}$ 吗？是 $\{x\} \in \{1, 2, \{x\}\}$ 吗？(9) 设 $A = \{a, b, c\}$ 和 $B = \{b, c, a\}$ 和 $C = \{a, a, b, c, a, b\}$。这些集合相等吗？

(10) $\mathbb{Z} = \mathbb{Q}$ 吗？为什么或为什么不？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 使用集合表示法定义自然数集合中4的倍数的定义。

(2) 考虑集合 $S = \{3, 4, 5, 6\}$。用集合构造符表示法定义 S 两种不同的方式。

(3) 给出一个满足 $\mathbb{N} \in X$ 的集合 X 的例子 $\mathbb{Z} \notin X$.

(4) 给出一个包含100个元素的集合的例子。

(5) 给出一个集合 A, B, C 的例子，使得 $A \in B$ 和 $B \in C$ 但 $A \notin C$。

(6) W 编写一个使用集合构建的 *odd integers* 集合的定义 r表示法。

(7) 使用集合表示法定义非自然数的整数集合。

(8) 考虑以下集合:

$$A = \left\{x \in \mathbb{R} \mid x^2 - 3x + 2 \geq 0\right\}$$
$$B = \{y \in \mathbb{R} \mid y \leq 1 \text{ or } y \geq 2\}$$

解释为什么 $A = B$。

(9) 考虑以下集合:

$$C = \left\{x \in \mathbb{R} \mid x^2 - 4 \geq 0\right\}$$
$$D = \{y \in \mathbb{R} \mid y \geq 2\}$$

是 $C = D$ 吗? 为什么或为什么不? 用良好的数学符号写出你的解释，使用 $\in$ 和 $\notin$。

(10) 尝试向一个不研究数学的朋友解释罗素悖论，看看他们能理解多少。他们对它有什么看法? 他们反对吗? 他们的想法有道理吗? 进行一次讨论!

3.4 Subsets

3.4.1 Definition and Examples

让我们讨论一个我们已经使用过基本想法的主题。具体来说，让我们研究 **subsets** 的概念。

Definition 3.4.1. *Given two sets A and B, if every element of A is also an element of B, then we say A is a* **subset** *of B.*

The mathematical symbol for subset is $\subseteq$, so we would write $A \subseteq B$.

If we want to indicate that A is a subset of B but is also 不等于 *to B, we would write $A \subset B$ and say that A is a* **proper subset** *of B.*

We can also write these relationships as $B \supseteq A$, or $B \supset A$, respectively. In these cases, we would say B is a **superset** *of A or B is a* **proper superset** *of A, respectively.*

注意这些符号与我们用来比较实数的 *inequality* 符号之间的相似性。我们写出不等式如 $x \leq 2$ 或 $5 > z > 0$，并根据符号的“方向”以及是否在下面加横线来理解这些不等式的含义。符号 $\subseteq, \subset, \supseteq, \supset$ 的工作方式完全相同，只是它们指的是“元素的包含”而不是“数字的大小”。

Standard Sets of Numbers

标准集合的数字，我们在上一节中提到的，通过子集关系相当好地相关联。具体来说，我们可以这样说

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

我们再次理所当然地认为我们对这些数字集合的集体知识使我们能够提出这些主张。然而，在描述为什么例如集合 $\mathbb{R}$ 存在并且是 $\mathbb{Q}$ 的适当超集时，涉及了一些深刻而复杂的数学概念。然而，目前我们使用这些集合来说明 **subset** 关系。

自從我們知道上述子集關係是 **proper**，我們就使用了那個對應的符號，“$\subset$”。在數學寫作中，通常會直接使用“$\subseteq$”符號，即使已知應該使用“$\subset$”。只有在上下文中確實需要指出兩個集合是 *not equal* 時，我們才會求助于使用“$\subset$”符號。如果這些信息對當前的上下文不是必要的，那麼我們可能只是使用“$\subseteq$”符號。

Set-Builder Notation Creates Subsets

一种我们已经“使用”子集概念的方式是在我们使用集合构造符号。这是用来定义一个集合包含所有满足一定性质的“较大”集合的元素。我们定义一个性质 $P(x)$，从一个较大的集合 X 中抽取一个变量对象 x，并包含任何满足性质 $P(x)$ 的元素 x。注意，这个新集合的任何元素都必须是 X 的元素，仅仅基于我们定义它的方式。因此，以下关系成立

$$\{x \in X \mid P(x)\} \subseteq X$$

无论集合 X 和属性 $P(x)$。根据集合 X 和属性 $P(x)$，可能适用适当的真子集符号 $\subset$，但一般来说，我们可以肯定适用 $\subseteq$。

尝试给出一些集合 X 和属性 $P(x)$ 的例子，以便 $\subseteq$ 适用，然后尝试给出一些 $\subset$ 适用的例子。尝试给出一个集合 X 和两个不同的属性 $P_1(x)$ 和 $P_2(x)$，以便 $\subset$ 对 $P_1(x)$ 适用，$\subseteq$ 对 $P_2(x)$ 适用。尝试识别两个 *different* 集合 X_1 和 X_2 以及两个 *different* 属性 $P_1(x)$ 和 $P_2(x)$，以便

$$\{x \in X_1 \mid P_1(x)\} = \{x \in X_2 \mid P_2(x)\}$$

你能做到吗?

Examples

一个集合是另一个集合的子集，当且仅当第一个集合的每个元素都是第二个集合的元素。例如，这意味着以下所有断言都成立：

$$\begin{aligned} \{142, 857\} &\subseteq \mathbb{N} \\ \left\{\sqrt{3}, -\pi, 8.2\right\} &\subseteq \mathbb{R} \\ \left\{x \in \mathbb{R} \mid x^2 = 1\right\} &\subseteq \mathbb{Z} \end{aligned}$$

你看到为什么这些是 True 吗?

为了一个子集关系失败，因此，我们必须能够找到第一个集合中的一个元素是 *not* 第二个集合的元素。例如，这意味着以下所有断言都成立：

$$\begin{aligned} \{142, -857\} &\not\subseteq \mathbb{N} \\ \left\{\sqrt{3}, -\pi, 8.2\right\} &\not\subseteq \mathbb{Q} \\ \left\{x \in \mathbb{R} \mid x^2 = 5\right\} &\not\subseteq \mathbb{Z} \end{aligned}$$

Finding All Subsets of a Set

让我们先针对一个特定的集合进行一些工作。定义 $A = \{1, 2, 3\}$。我们能识别 *all* 的 A 的子集吗? 当然可以，为什么不呢?

$$\begin{aligned} \{1\} &\subseteq A \\ \{2\} &\subseteq A \\ \{3\} &\subseteq A \\ \{1, 2\} &\subseteq A \\ \{1, 3\} &\subseteq A \\ \{2, 3\} &\subseteq A \\ A = \{1, 2, 3\} &\subseteq A \\ \varnothing &\subseteq A \end{aligned}$$

识别前六个子集相当直接，但重要的是要记住A和$\varnothing$也是子集。（注意：一般来说，对于任何集合S，$S \subseteq S$和$\varnothing \subseteq S$都是正确的。想想看！）

考虑集合 B，其元素是我们上面列出的所有集合：

$$B = \left\{ \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A, \varnothing \right\}$$

确实，任何元素 $X \in B$ 都满足 $X \subseteq A$。你明白为什么吗?

3.4.2 The Power Set

这个过程识别给定集合的所有子集是常见且有用的，因此我们用特殊名称来标识结果集合。

Definition 3.4.2. *Given a set A, the* **power set** *of A is defined to be the set whose elements are all of the subsets of A. It is denoted by $\mathcal{P}(A)$.*

我们的括号内观察从上面的段落告诉我们，对于任何集合 S，有 $S \in \mathcal{P}(S)$ 和 $\varnothing \in \mathcal{P}(S)$。

回顾我们上面的示例集 $A = \{1, 2, 3\}$。你注意到 $\mathcal{P}(A)$ 中的元素数量有什么特点吗？它与 A 中的元素数量有何关联？你认为对于任意集合 S，S 和 $\mathcal{P}(S)$ 中的元素数量之间是否存在一般关系？

Example 3.4.3. 让我们找到 $\mathcal{P}(\varnothing)$。空集的子集有哪些？只有一个，就是空集本身！（即 $\varnothing \subseteq \varnothing$，但没有其他集合满足这个条件。）因此，幂集 $\mathcal{P}(\varnothing)$ 只有一个元素，即空集：

$$\mathcal{P}(\varnothing) = \{\, \varnothing \,\}$$

注意，这是从空集本身得到的 *different*：

$$\varnothing \neq \{\, \varnothing \,\}$$

为什么这是真的？比较元素！空集有 *no* 个元素，但右侧的集合恰好有 *one* 个元素。（一般来说，这是一种比较两个集合的有用方法。）为了给你一些练习，我们将指出，上述行可以大声读作：

> 空集和包含空集的集合是两个不同的集合。

Example 3.4.4. 让我们用另一组数据尝试这个过程，比如说 $A = \{\, \varnothing, \{1, \varnothing\} \,\}$。我们可以列出 $\mathcal{P}(A)$ 的元素如下

$$\mathcal{P}(A) = \{\, \{\varnothing\}, \{\{1, \varnothing\}\}, \{\varnothing, \{1, \varnothing\}\}, \varnothing, \,\}$$

这可能看起来很奇怪，因为有所有的空集和大括号，但保持子集关系清晰是很重要的。在这个例子中，确实如此，

$$\varnothing \in A, \quad \{\varnothing\} \subseteq A, \quad \{\varnothing\} \in \mathcal{P}(A), \quad \{\varnothing\} \subseteq \mathcal{P}(A)$$

为什么这些关系是正确的？仔细思考它们，并尝试自己写几个。区分“$\in$”和“$\subseteq$”非常重要！

3.4.3 Set Equality

两个集合何时相等? 主要思想是，如果两个集合包含“相同的元素”，则它们相等，但这并不是等价的精确定义。我们如何更明确、更严格地描述这种属性？说两个集合A和B有“相同的元素”意味着A的任何元素也是B的元素，并且B的每个元素也是A的元素。如果这两个属性都成立，那么我们可以保证这两个集合恰好包含相同的元素，因此它们是相等的。如果你仔细想想，你会发现我们可以用**subsets**来表述这一点。多么方便啊!

Definition 3.4.5. *We say two sets, A and B, are* **equal***, and write $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.*

(如果我们在定义中使用$\subset$符号，而不是$\subseteq$，会发生什么？这是集合相等的同一概念吗？为什么或为什么不呢？)

这个定义在将来当我们学习如何判断两个集合*prove*相等，而我们不能简单地列出每个集合的元素并比较它们时将非常有用。通过构建两个论证并在“两个方向”上证明子集关系，我们可以证明两个集合相等。现在，让我们看看这个定义如何应用于一个简单的例子。

Example 3.4.6. 我们如何使用这个定义来观察以下等式成立?

$$\{x \in \mathbb{Z} \mid x \geq 1\} = \mathbb{N}$$

我们只需确认 $\subseteq$ 和 $\supseteq$ 之间的关系适用于双方。首先，每个至少为 1 的整数是否都是自然数？是的！这解释了为什么

$$\{x \in \mathbb{Z} \mid x \geq 1\} \subseteq \mathbb{N}$$

其次，每个自然数是否都是至少为1的正整数？是的！这解释了为什么

$$\{x \in \mathbb{Z} \mid x \geq 1\} \supseteq \mathbb{N}$$

一起，这表明上述等式是正确的。

3.4.4 The “Bag” Analogy

它们在我们的经验中是相当难以理解的概念，当它们被引入时。特别是，与集合相关的**notation**让学生感到困惑，他们最终写下了一些毫无意义的东西！保持符号$\in$和$\subseteq$之间的区别是至关重要的。

这里是一个有助于记忆的类比：一个集合就像一个里面有些东西的**bag**。袋子本身无关紧要；我们只关心里面有什么东西（即元素是什么）。甚至可以把袋子想象成你在杂货店得到的那些无特色的塑料袋。所有这些袋子都是相同的；要区分任何两个袋子，我们需要知道是什么东西把它们装起来的。

如果我把一个苹果和一个橙子放进购物袋里，显然，它们放在哪里并不重要。你只需要知道我有一些苹果和橙子。袋子里有多少苹果或橙子也不重要，因为我们只关心里面有什么东西。把它想象成回答形式为“袋子里有s吗？是或否？”的问题。我袋子里有两个相同的苹果、七个还是只有一个，这都不重要；如果你问我是否有*any*个苹果，我只会说“是”。这与集合中元素的顺序和重复的概念有关。一个集合完全由其元素来定义。

这也有助于我们将集合视为其他集合的元素，自身。谁能阻止我把整个袋子放进另一个袋子呢？看看我们在上面例子中定义的集合 A：

$$A = \{ \varnothing , \{1, \varnothing\} \}$$

这个集合 A 是一个袋子。袋子里有什么？袋子里有两个物体（即 A 的两个元素）。它们都是袋子！其中一个是一个普通的空袋子，里面什么都没有。（那就是空集。）好吧，这很酷。另一个里面有另外两个物体。其中一个物体是数字1。酷。另一个这样的物体是另一个空袋子。

Distinguishing “$\in$” and “$\subseteq$”

这个类比也有助于理解“$\in$”和“$\subseteq$”之间的区别。再次记住例子A。当我们写$x \in A$时，我们指的是x是包A内的一个物体。如果我们窥视A，我们会看到底部有x坐在一堆东西中间。让我们用这个想法来比较两个例子。

- 我们在这里看到 $\varnothing \in A$ 是正确的。如果我们查看袋子 A，我们会看到其中有一个空袋子（元素）。
- 我们同样看到$\{\varnothing\} \notin A$在这里是正确的。如果我们查看袋子A内部，我们看不到一个包含*only*一个空袋子的袋子。（请注意，这就是$\{\varnothing\}$：另一个袋子内的空袋子。）你看到这样的物体了吗？在哪里？我敢打赌，在袋子A里面的东西中，你找不到一个包含*only*一个空袋子的袋子。我在袋子A里看到了什么？好吧，我看到了两样东西：一个空袋子，和一个里面有*two*个物体（一个空袋子和数字1）的袋子。这两样东西都不是我们正在寻找的东西！

当我们写出 $X \subseteq A$ 时，我们意味着两个袋子，X 和 A，以某种方式是可以比较的。具体来说，我们是在说 X 里面的所有东西也都是 A 里面的东西。我们实际上是在翻遍 X 里面的所有对象，一个一个地拿出来，并确保我们也能看到 A 里面的那个对象。让我们用这个想法来比较两个例子。

- 我们在这里看到 $\{\varnothing\} \subseteq A$ 是正确的。我们正在将左边的袋子与右边的袋子 *comparing*。左边的袋子里装的是什么东西？

那里只有一个对象，它是一个空袋子，本身。现在，我们窥视 A 里面。我们是否也看到一个空袋子？是的，我们看到了！因此，“$\subseteq$” 符号适用于此处。

- 我们同样看到$\{1\} \not\subseteq A$在这里是正确的。为了比较这两个包，我们将从左边的包中取出一个对象，看看它是否也在包A中。这里，我们只有一个对象可以取出：数字1。现在，让我们看看包A里面。我们能看到一个1坐在里面吗？不，我们看不到！

  我们得在包底部的某个地方窥视 $inside$ 才能找到数字 1；这个数字并不是明明白白地放在那里。因此，$\{1\} \not\subseteq A$。

回顾我们已经讨论的一些例子，同时考虑这个新的类比。这有助于你理解定义和例子吗？这有助于你理解“$\in$”、“$\subseteq$”和“$\supseteq$”之间的区别吗？如果不是，你能想到另一个有助于你的类比吗？

3.4.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) $\mathbb{N} \subseteq \mathbb{R}$吗？ $\mathbb{R} \subseteq \mathbb{N}$吗？ $\mathbb{Q} \subseteq \mathbb{Z}$吗？为什么或为什么不？

(2) $\subset$ 和 $\subseteq$ 之间的区别是什么？给出一个满足 $A \subseteq B$ 是 True 但 $A \subset B$ 是 False 的集合 A, B 的例子。

(3) $\in$ 和 $\subseteq$ 之间的区别是什么？给出一个满足 C, D 但不满足 $C \notin D$ 的集合 $C \subseteq D$ 的例子。 (4) 设 S 为任意集合。**power set** 是什么？它是什么类型的数学对象？它是如何定义的？ (5) 假设 $S \subseteq T$。这是否意味着 $S = T$？为什么或为什么不？

(6) 解释为什么对于任意集合 S，有 $\varnothing \subseteq S$ 和 $\varnothing \in \mathcal{P}(S)$。

(7) 假设 $X \in \mathcal{P}(A)$。那么 X 和 A 之间有什么关系呢？

(8) $A = \mathcal{P}(A)$ 是否可能为真？（这个问题相当棘手，但请思考一下！）

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 写出集合 $\mathcal{P}(\mathcal{P}(\varnothing))$ 的元素。 (2) 写出集合 $\mathcal{P}([1])$ 和 $\mathcal{P}([2])$ 和 $\mathcal{P}([3])$ 的元素。你能推测 $\mathcal{P}([n])$ 有多少个元素吗? （你能证明吗? 我们并不期望你 now，但很快就会；想想看！）(3) 让 $A = \{x, \heartsuit, \{4\}, \varnothing\}$。对于以下每个陈述，决定它是 True 还是 False，并简要解释原因。(a) $x \in A$b) $x \subseteq A$c) $\{x, \heartsuit\} \subseteq A$d) $\{x, \varnothing\} \subset A$e) $\{x, \heartsuit, z, 7\} \supseteq A$f) $\{x\} \notin \mathcal{P}(A)$g) $\{x\} \subseteq \mathcal{P}(A)$h) $\{\heartsuit, x\} \in \mathcal{P}(A)$ i) $\{4\} \in \mathcal{P}(A)$j) $\{\varnothing\} \in \mathcal{P}(A)$k) $\{\varnothing\} \subseteq \mathcal{P}(A)$

Hint: 7个是True，4个是False。

(4) 给出一个集合 A, B 的例子，使得 $A \in B$ 和 $A \subseteq B$ 都为真。

(5) 是 $\{1, 2, 12\} \subseteq \mathbb{R}$ 吗? (6) 是 $\{-5, 8, 12\} \subseteq \mathbb{N}$ 吗? (7) 是 $\{1, 3, 7\} \in \mathcal{P}(\mathbb{N})$ 吗? (8) 是 $\mathbb{N} \in \mathcal{P}(\mathbb{Z})$ 吗? (9) 是 $\mathcal{P}(\mathbb{N}) \subseteq \mathcal{P}(\mathbb{Z})$ 吗? 它们是相等的集合吗? 为什么或为什么不? (10) 给出一个无限集合 T 的例子，使得 $T \in \mathcal{P}(\mathbb{Z})$ 但 $T \notin \mathcal{P}(\mathbb{N})$。(11) 假设 G, H 是集合，并且它们满足 $\mathcal{P}(G) = \mathcal{P}(H)$。我们能得出 $G = H$ 吗? 为什么或为什么不? （不要试图正式证明这一点；只需思考并尝试讨论。）

(12) 给出一个集合 W 的例子，使得 $W \subseteq \mathcal{P}(\mathbb{N})$ 但 $W \notin \mathcal{P}(\mathbb{N})$。

3.5 Set Operations

当你第一次了解数字时，下一步自然就是学习如何*combine*它们：乘法、加法等等。因此，我们现在的一个自然下一步就是研究我们如何对两个集合进行*operate*以产生其他集合。我们如何以有趣的方式*combine*集合？有几个这样的操作有标准的符号，我们现在将向您介绍这些操作。

在整个本节中，我们假设我们有两个集合 A 和 B，它们各自是更大集合 **universal set** U 的子集。也就是说，我们假设 $A \subseteq U$ 和 $B \subseteq U$。我们做出这个假设的原因是，每个操作都涉及到通过识别更大集合中具有特定属性的元素来定义另一个集合，因此我们必须有一个集合 U，它保证包含 A 和 B 的所有元素，这样我们甚至可以处理这些元素。（再次强调，确保这一点可能看起来很繁琐，但这是为了避免我们之前研究过的那种讨厌的悖论。）然而，如果那些集合 A, B, U 存在，我们就可以继续进行我们的定义。

3.5.1 Intersection

这个操作收集两个集合的共同元素，并将它们包含在一个新集合中，称为 **intersection**。

Definition 3.5.1. *Let A and B be any sets. The* **intersection** *of A and B is the set of elements that belong to both A 和 B, and is denoted by $A \cap B$. Symbolically, we define*

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

Example 3.5.2. 定义以下集合：

$$\begin{aligned} S_1 &= \{1, 2, 3, 4, 5\} \\ S_2 &= \{1, 3, 7\} \\ S_3 &= \{2, 4, 7\} \\ U &= \mathbb{N} \end{aligned}$$

然后，我们看到例如，

$$\begin{aligned} S_1 \cap S_2 &= \{1, 3\} \\ S_1 \cap S_3 &= \{2, 4\} \\ S_2 \cap S_3 &= \{7\} \end{aligned}$$

此外，由于 $S_1 \cap S_2$ 本身是一个集合，因此考虑 $(S_1 \cap S_2) \cap S_3$ 是有意义的。然而，这两个集合没有共享的元素，所以我们写

$$(S_1 \cap S_2) \cap S_3 = \varnothing$$

两个集合没有公共元素的情况，如上例所示，这种情况很常见，以至于我们有一个特定的术语来描述这样的集合：

Definition 3.5.3. *If $A \cap B = \varnothing$, then we say A and B are* **disjoint**.

Intersections and Subsets

您可能已经注意到，无论 A 和 B 是什么，我们都可以说 $A \cap B \subseteq A$ 和 $A \cap B \subseteq B$。让我们证明这个事实！

Proposition 3.5.4. *Let A and B be any sets. Then,*

$$A \cap B \subseteq A$$

and

$$A \cap B \subseteq B$$

顺便说一句，这样的 **proposition** 只是一个“迷你结果”。它并不困难或重要到足以被称为定理，但它确实需要一点证明。

Proof. 假设我们有两个集合，A 和 B。为了证明一个子集关系，如 $A \cap B \subseteq A$，我们需要证明集合左侧的每个 **element**（$A \cap B$）也是集合右侧的元素（A）。

让我们考虑一个任意元素 $x \in A \cap B$。根据 $A \cap B$ 的定义，我们知道 $x \in A$ 和 $x \in B$。因此，我们知道 $x \in A$。这就是我们的目标，所以我们已经证明了 $A \cap B \subseteq A$。

此外，我们知道 $x \in B$，因此我们也已经证明了 $A \cap B \subseteq B$。 □

这可能看起来像是一个简单的观察和一个容易证明的结论，但我们仍然需要通过这些逻辑步骤来严格解释为什么这些子集关系是正确的。此外，请注意我们在这里使用的 **proof structure** 类型。为了证明一个子集关系是正确的，我们需要考虑一个集合的 **arbitrary element**，并推断它也是另一个集合的元素。这将是我们的证明任何关于子集的断言的方法。

什么如果 $A \subseteq B$? 关于 $A \cap B$，与 A 和 B 的关系，我们能说什么？尝试证明关于这个的陈述！

3.5.2 Union

此操作收集两个集合中的任意一个的元素，并将它们包含在一个新集合中，称为**union**。

Definition 3.5.5. *Let A and B be any sets. The* **union** *of A and B is the set of elements that belong to either A 或 B, and is denoted by $A \cup B$. Symbolically, we define*

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

注意，定义中的“或”是一个 *inclusive* “或”，意味着 $A \cup B$ 包括属于 A 或 B 或可能同时属于这两个集合的任何元素。

Example 3.5.6. 返回到我们在示例3.5.2中定义的集合 S_1, S_2, S_3，我们可以这样说

$$S_1 \cup S_2 = \{1, 2, 3, 4, 5, 7\}$$
$$S_1 \cup S_3 = \{1, 2, 3, 4, 5, 7\}$$
$$S_2 \cup S_3 = \{1, 2, 3, 4, 7\}$$

此外，由于这些并集本身也是集合，我们可以找到它们与另一个集合的并集。例如，

$$(S_1 \cup S_2) \cup S_3 = \{1, 2, 3, 4, 5, 7\} \cup \{2, 4, 7\} = \{1, 2, 3, 4, 5, 7\}$$

Unions and Subsets

注意 $A \subseteq (A \cup B)$ 和 $B \subseteq (A \cup B)$，无论 A 和 B 是什么。让我们来证明这一点！

Proposition 3.5.7. *Let A and B be any sets. Then,*

$$A \subseteq (A \cup B)$$

and

$$B \subseteq (A \cup B)$$

Proof. 假设我们有两个集合，A 和 B。为了证明 $A \subseteq (A \cup B)$，我们需要展示 A 的每个元素也是 $A \cup B$ 的元素。

让 $x \in A$ 为任意且固定的。那么，显然有 $x \in A$ 或 $x \in B$ (因为 $x \in A$)。这表明 $x \in A \cup B$。由于 x 是任意的，我们已经证明了 $A \subseteq A \cup B$。

设 $y \in B$ 为任意且固定的。那么，$y \in A$ 或 $y \in B$ (肯定是正确的，因为我们已经知道 $y \in B$)。这表明 $y \in A \cup B$。由于 y 是任意的，我们已经证明了 $B \subseteq A \cup B$。 □

关于$A \cap B$和$A \cup B$之间的关系，你能说什么？如果$A \subseteq B$，我们能否对B和$A \cup B$之间的关系说些什么？尝试证明你的观察！

我们应该强调，像这样的主张——对于任何集合 A 和 B，$A \subseteq A \cup B$——需要被证明；它们并不成立 **by definition**。两个集合的并集的定义见上文。注意，它并没有说明 A 和 $A \cup B$ 之间的关系；它只是告诉我们对象 $A \cup B$ 实际上是什么。当你引用或引用定义并使用它时，务必这样做；但也要确保解释任何不是定义的主张。由于我们已经证明了这两个小引理，我们可以通过引用它们在未来使用它们；如果我们没有这样做，我们每次尝试引用它们时都必须重新解释这些小事实！

3.5.3 Difference

这个操作取一个集合的元素，并移除也属于另一个集合的元素。

Definition 3.5.8. *The* **difference** *between A and B, denoted by $A - B$, is the set of all elements of A that are* 未 *elements of B. Symbolically, we define*

$$A - B := \{x \in U \mid x \in A \text{ and } x \notin B\}$$

Example 3.5.9. 返回到我们在示例3.5.2中定义的集合 S_1, S_2, S_3，我们可以这样说，例如

$$S_1 - S_2 = \{2, 4, 5\}$$
$$S_2 - S_1 = \{7\}$$
$$S_2 - S_3 = \{1, 3\}$$

Set Difference Is *Not* Symmetric

注意上面示例中的 $S_1 - S_2 \neq S_2 - S_1$。一般来说，在集合的上下文中，操作“$-$”不是 **symmetric**，这个例子就说明了这一点。你能找到两个集合 A, B 使得 $A - B = B - A$ 吗？你能找到两个集合 A, B 使得 $A - B = B - A \neq \varnothing$ 吗？

每个我们迄今为止定义的其他操作实际上都是对称的。也就是说，$A \cap B = B \cap A$和$A \cup B = B \cup A$。回顾一下这些操作的定义，看看为什么这有意义。在操作的性质定义中使用的*language*有什么使得这一点成立?

Notation Notes

关于这个集合差记法的另一个评论。请注意，我们使用标准的减号符号，“$-$”，但这与我们通常所想的“减法”没有关系，就像与数字一样。这可能是有史以来你第一次遇到这种歧义，或者可能不是，但有一个更大的观点与数学符号和术语相关：许多符号根据*context*有不同的含义。

当我们写7 {v*} 5时，我们明显是指减法，即$7 - 5 = 2$。然而，当我们写 $A - A$，其中A已被识别为*set*时，我们指的是集合差操作，即$A - A = \varnothing$。务必检查任何陈述的上下文，以确保其中的符号确实意味着你所认为的意思!

3.5.4 Complement

此操作识别所有位于集合“外部”的元素。此操作依赖于全集 U 的上下文。您会发现这在定义中很明显，我们还将通过示例来说明这一点。

Definition 3.5.10. *The* **complement** *of A is the set of all elements that are* 未 *elements of A, and is denoted by $\bar{A}$. Symbolically, we define*

$$\bar{A} = \{x \in U \mid x \notin A\}$$

记住，我们假设 A, B, U 是满足 $A \subseteq U$ 和 $B \subseteq U$ 的给定集合。在这个背景下，集合$\bar{A}$ 是明确定义的，但这个集合肯定依赖于 A 和 U!

Example 3.5.11. 例如，让我们回到在例3.5.2中定义的集合 S_1, S_2, S_3。在那里，我们使用了上下文 $U = \mathbb{Z}$。在这种情况下，

$$\bar{S_1} = \{6, 7, 8, 9, \dots\}$$

然而，如果我们使用了 $U = \{1, 2, 3, 4, 5, 6, 7\}$ 呢？在这种情况下，

$$\bar{S_1} = \{6, 7\}$$

由于符号表示$\bar{A}$ 没有表明它所依赖的集合 U，因此在我们工作的任何上下文中，明确这个集合都很重要。尝试识别一些集合 A, U_1, U_2，使得$\bar{A}$ 在 U_1 中与$\bar{A}$ 在 U_2 中的不同，并尝试识别一些集合，使得$\bar{A}$ 在两种情况下都相同。

3.5.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆!

(1) 两个集合的并集和交集有什么区别?

(2) 两个集合互斥意味着什么?

(3) 什么是 $\mathbb{Z} \cap \mathbb{N}$? 什么是 $\mathbb{Z} \cup \mathbb{N}$? 什么是 $\mathbb{Z} - \mathbb{N}$?

(4) $A - B = B - A$ 是否可能为真? 如何?

(5) 在$\mathbb{N}$的上下文中[3]是什么? 在$\mathbb{Z}$的上下文中呢? 在$\mathbb{R}$的上下文中呢? 尝试使用良好的数学符号和构建器符号来写出你的答案，也许。

(6) $(A \cap B) \cap C = (A \cap B) \cap C$ 是否总是正确? 为什么或为什么不正确? 用 $\cup$ 代替 $\cap$ 呢?

(7) “7 − 5”和“[7] − [5]”这两个陈述有什么区别?

(8) 假设 $x \in A$。$A - x$ 在符号上是否有意义? 你如何修改它使其有意义? (9) ($\mathbb{Z} - \mathbb{N}) \cup \mathbb{R}$ 是什么?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 列出以下集合的元素：

(a) $[7] \cup [10]$ (b) $[10] \cap [7]$ (c) $[10] - [7]$ (d) $([12] - [3]) \cap [8]$ (e) $(\mathbb{N} - [3]) \cap [7]$ (f) $(\mathbb{Z} - \mathbb{N}) \cap \mathbb{N}$ (g) $\overline{\mathbb{N}} \cap \{0\}$，在$\mathbb{Z}$的上下文中

(2) 找到一组集合 A, B, C，使得 $(A - B) - C = A - (B - C)$。然后，找到一个它们 **not** 相等的例子。

(3) 状态并证明 A 和 $U - A$ 之间的关系。

(4) 设 $A = [12]$，设 E 为偶整数集，设 P 为质自然数集。$A \cap E$ 是什么？$A \cap P$ 是什么？$(A \cap E) \cap P$ 是什么？它与 $A \cap (E \cap P)$ 相同吗？

假设上下文是 $U = \mathbb{N}$。$A \cap E$ 和 $A \cap \overline{E}$ 是什么？

(5) 什么是 $\{1\} \cap \mathcal{P}(\{1\})$？

(6) 考虑集合 $\{1\}$ 和 $\{2, 3\}$。比较集合 $\mathcal{P}(\{1\} \cup \{2, 3\})$ 和 $\mathcal{P}(\{1\}) \cup \mathcal{P}(\{2, 3\})$。你注意到什么？用“$\cap$”代替“$\cup$”重复这个练习。你注意到什么？

(7) 设 A, U 为集合，并假设 $A \subseteq U$。在 U 的上下文中，$B = \overline{A}$。你认为 B 是什么？为什么？

3.6 Indexed Sets

3.6.1 Motivation

让我们讨论一个我们之前简要提及并已经开始使用的概念：**indexing** 集合的集合。当我们希望定义或引用大量集合而不必明确写出所有集合时，这种类型的符号很方便。使用我们已定义的集合运算的类似符号，我们将能够“组合”和“操作”大量

一次所有集合的数量。本节实际上没有新的数学内容，但涉及这些想法的符号可能令人困惑且难以处理，起初，因此我们希望仔细引导您理解这些想法。

Relation to Summation Notation

我们将从之前见过的相关概念开始。还记得我们在第一章中研究自然数之和的时候吗？我们提到了一些特殊的符号，这些符号允许我们将求和中的长串项压缩成一种简洁的形式，使用$\sum$符号。例如，我们可以用$\sum$符号写出一种非正式的求和（“非正式”意味着“不严谨”，因为使用了省略号）如下：

$$1+2+3+4+\cdots+(n-1)+n=\sum_{i=1}^{n} i$$

为什么这个符号有效且合理？**index variable** i 是将求和压缩成这种形式的要害组成部分。在 $\sum$ 符号下方写“$i=1$”意味着变量 i 的值应该从 1 开始，每次增加 1，直到达到终端值 n，该值写在 $\sum$ 符号上方。对于该范围内（从 1 到 n）的每个允许的 i 值，我们在 $\sum$ 符号右侧写出的求和形式中包含一个项；在这种情况下，该项是 i。因此，我们应该有 $1, 2, 3, \ldots, n$ 这样的项，每项之间有一个 $+$ 符号。

我们应该指出，隐含地理解将 $i=1$ 和 n 写作索引变量 i 上的 **limits** 表示 i 假设了所有介于 1 和 n 之间的自然数。

Example

首先，让我们通过一个例子来看一下定义索引集合的过程。我们还将看到如何通过使用索引变量将集合运算应用于几个集合。

Example 3.6.1. 我们可以类似地压缩一些集合运算符号。例如，让我们定义集合 $A_1, A_2, A_3, \ldots, A_{10}$ 为

$$\begin{aligned} A_1 &= \{1,2\} \\ A_2 &= \{2,4\} \\ A_3 &= \{3,6\} \\ &\vdots \\ A_i &= \{i,2i\} \\ &\vdots \\ A_{10} &= \{10,20\} \end{aligned}$$

我们包括了A_i的定义，用于$arbitrary$值i，以给这些集合一个严格的定义。如果不定义那个集合——它定义了A_i对于i的任何相关值——我们将把解释集合A_1, A_2, A_3, A_{10}之间模式的责任留给读者，可能会有多种解释方式。通过这样明确地定义术语A_i，就不会有关于我们想要这十个集合是什么的混淆。

此外，我们可以更轻松地表达这些集合的并集，例如。记住，两个集合的并集是包含两个集合所有元素的集合（即，如果一个元素在第一个集合 or 或第二个集合中，或者可能两个集合都在，那么这个元素就包含在并集中）。多于两个集合的并集是什么？它遵循与仅两个集合定义相同的思路；我们希望在并集中包含一个元素，如果它在通过并集操作组合的构成集合的 any 中。

如何简洁准确地写出这个并集？让我们遵循 $\sum$ 符号的相同动机。这些集合的索引从 1 到 10，因此我们应该在“$\cup$”符号下方写上 $i = 1$，在上方写上 10。并集中的每个项的形式为 $\{i, 2i\}$，因此我们应该将其写在“$\cup$”符号的右侧。对于像这样的 $indexed$ 并集，我们使用一个稍微大一点的“$\bigcup$”符号，如下所示：

$$A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_{10} = \bigcup_{i=1}^{10} A_i = \bigcup_{i=1}^{10} \{i, 2i\}$$

这比写出所有10个集合的元素要简洁得多，因此您可以了解这种符号{v*}是如何的。我们将不断提醒您左边的并集中省略号的模糊性，并告诉您，实际上，右边的表达式是对这个并集的一个真正严格的数学陈述。左边的表达式更多地是一种直观的、启发式的方法来描述应用于这十个集合的并集操作。

When The Index Set Is Not a Range of Numbers

让我们考察一个更难的例子来推动这种符号技术下一步的发展。如果我们要求你用求和符号写出以下和式：所有质数的平方倒数的和。我们如何完成这个任务？（注意：我们只是想表达和式中的所有项，而不包括$evaluating$这个和。这是一个留给另一个时间点的困难任务！）

很遗憾，我们无法使用与上面完全相同的符号，因为我们不想在两个自然数之间的索引值范围内求和；相反，我们只想包括对应于素数的项。为此，我们定义一个 **index set** I，它将描述我们将“插入”到求和右侧任意项的索引的可允许值。

在这种情况下，如果我们有一个素数 i，我们希望将项 $\frac{1}{i^2}$ 包含在我们的和中，因此这个表达式将被写入 $\sum$ 符号的右侧。我们希望在我们的记号中表示值 i 应该是一个素数

数字，并且应包括所有可能的质数。因此，允许值索引集 I 应该是所有质数的集合。也就是说，我们可以将这个和写成

$$\sum_{i \in I} \frac{1}{i^2} \quad \text{, where } I = \{i \in \mathbb{N} \mid i \text{ is prime}\}$$

看看这个符号能做什么！我们不仅将无限多个项压缩成一个表达式，还指出了任意指数 i 的值应限制为素数，这些素数的行为与像 $\sum_{i=1}^{n} i$ 这样的和不同，它们不以“通常”和方便的方式表现。

Example 3.6.2. 这个关于 *index set* 的概念极其有用，并且可以扩展到任意集合甚至非数学对象。例如，在我们上面关于集合的讨论中，我们使用了所有大联盟棒球的集合 B。我们如何使用这个集合来表达所有大联盟棒球的集合 P 呢? 每个球队本身就是一个集合，其元素是该队的球员，因此所有球队的并集（即 B 中所有集合的并集）应该正好产生所有球员的这个集合！在这种情况下，我们的指标集是 B，对于每个元素 $b \in B$，我们希望将其作为 b 包含在我们的并集中。因此，我们会写成

$$P = \bigcup_{b \in B} b$$

该并集中的各个项甚至不依赖于自然数，因此如果没有使用索引集，如这样，就根本无法表达这个并集。此外，这个并集依赖于并集的项是索引集 B 的元素，但它们本身也是集合；因此，对这些项应用并集操作在数学上是合理的。这仍然可能看起来像一个奇怪的想法，所以请务必仔细思考集合具有自身也是集合的元素这一想法。

Reading Indexed Expressions Aloud

为了将这些类型的表达式用语言表达出来，并帮助你在脑海中思考它们，让我们给你举一个例子。我们可能会将上面的表达式读作

> “所有素数 {v*} 的和，为$\frac{1}{i^2}$。” 或 “$\frac{1}{i^2}$ 的和，其中 i 遍历所有素数。”

同样，我们可能将上面的另一个表达式读作

> “2012赛季所有MLB球队的并集b中的那些b。” 或 “所有集合b的并集，其中b遍历2012赛季的所有MLB球队。”

3.6.2 Indexed Unions and Intersections

让我们为多个集合的并集运算给出一个精确的定义，因为我们只严格定义了两个集合的并集。

Definition 3.6.3. *The union of a collection of sets A_i indexed by the set I is*

$$\bigcup_{i\in I} A_i = \{x \in U \mid x \in A_i \text{ for some (i.e. at least one) } i \in I\}$$

where we assume there is a set U such that $A_i \subseteq U$ for every $i \in I$.

在数学语言中，“对于某些 $i \in I$” 这个短语意味着我们希望存在具有指定性质的 *at least one* $i \in I$。如果一个元素 x 满足 $x \notin A_i$ 对于 *every* $i \in I$，那么这意味着 x 不在我们集合中的任何集合中，因此它不应该包含在并集中。

根据这个想法，我们可以为集合交集给出一个类似的定义。

Definition 3.6.4. *The intersection of a collection of sets A_i indexed by the set I is*

$$\bigcap_{i\in I} A_i = \{x \in U \mid x \in A_i \text{ for every } i \in I\}$$

where we assume there is a set U such that $A_i \subseteq U$ for every $i \in I$.

3.6.3 Examples

让我们回到一个先前的例子，使这些想法更清晰。

Example 3.6.5. 之前，在示例3.6.1中，我们定义了

$$A_i = \{i, 2i\}$$

对于每个自然数 i 在 1 和 10 之间。定义这个集合的另一种方法是考虑索引集 $I = [10]$（回忆符号 $[n] = \{i \in \mathbb{N} \mid 1 \le i \le n\}$）并将 A 定义为集合

$$A = \{A_i \mid i \in I\} \text{ , where } A_i = \{i, 2i\} \text{ for every } i \in I$$

这定义了每个由索引集 I 中选择的索引值 i 所决定的集合 A_i，并且“收集”了所有这些集合到一个集合 A 中。然后，另一种写法是我们之前写的那个并集将是

$$\bigcup_{i\in I} A_i$$

在给定的 I 和 A_i 的定义下。

(仔细思考这个并集与集合 A 的区别。那么这个并集究竟是什么？我们如何方便地表示它的元素？我们需要列出每个元素吗？如果我们把指标集 I 改为 $\mathbb{N}$ 会怎样？在这种情况下并集是什么？)

Example 3.6.6. 让 $I = \{1, 2, 3\}$，并且对于每一个 $i \in I$，定义

$$A_i = \{i - 2, i - 1, i, i + 1, i + 2\}$$

让我们识别并写出以下集合的元素:

$$\bigcup_{i \in I} A_i \qquad \text{and} \qquad \bigcap_{i \in I} A_i$$

注意，我们可以写出每个 A_i 集合的元素，如下所示:

$$A_1 = \{-1, 0, 1, 2, 3\}$$
$$A_2 = \{0, 1, 2, 3, 4\}$$
$$A_3 = \{1, 2, 3, 4, 5\}$$

Thus,Thus,

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3 = \{-1, 0, 1, 2, 3, 4, 5\}$$

和

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 = \{1, 2, 3\}$$

现在，考虑 $J = \{-1, 0, 1\}$，其中 A_j 的定义与之前相同。让我们识别集合的元素

$$\bigcup_{j \in J} A_j \qquad \text{and} \qquad \bigcap_{j \in J} A_j$$

每个集合的元素写出来，我们可以确定

$$\bigcup_{j \in J} A_j = A_{-1} \cup A_0 \cup A_1 = \{-3, -2, -1, 0, 1, 2, 3\}$$

和

$$\bigcap_{j \in J} A_j = A_{-1} \cap A_0 \cap A_1 = \{-1, 0, 1\}$$

尝试用不同的索引集回答相同的问题。

例如，考虑 $K = \{1, 2, 3, 4, 5\}$ 或 $L = \{-3, -2, -1, 0, 1, 2, 3\}$。

Example 3.6.7. 定义索引集 $I = \mathbb{N}$。对于每个 $i \in I$，定义集合

$$C_i = \left\{ x \in \mathbb{R} \mid 1 \leq x \leq \frac{i + 1}{i} \right\}$$

然后我们声称

$$\bigcup_{i \in I} C_i = \{y \in \mathbb{R} \mid 1 \leq y \leq 2\} \quad \text{and} \quad \bigcap_{i \in I} C_i = \{1\}$$

你能看出为什么这些是正确的吗？我们将在稍后讨论证明此类等式所需的技术。现在，我们只是要求你思考为什么这些是正确的。你能向同学或朋友解释它们吗？你可能会使用什么技术来证明这些说法?

Example 3.6.8. 设S为选修此课程的学生集合。对于每个$s \in S$，设C_s为学生s在本学期所选修的课程集合。以下表达式代表什么?

$$\bigcup_{s\in S} C_s \qquad \text{and} \qquad \bigcap_{s\in S} C_s$$

我们打赌你至少能识别出右侧集合中的一个元素!

3.6.4 Partitions

现在我们有了写下多个集合的并集的方法，我们可以定义一个有用的概念：即 **partition** 的概念。从语言学的角度来说，划分是将“某物分解成碎片”的一种方式，从数学的角度来说，这个词的意思也差不多。

要言之，一个划分就是一个集合的非重叠子集的集合，其并集是整个集合。让我们在这里写下这个定义，然后看看一些例子和非例子。在未来的许多情况下，我们将使用这个定义，所以让我们在谈论集合和索引并集的时候掌握它。

Definition 3.6.9. *Let A be a set. A* **partition** *of A is a collection of sets that are pairwise disjoint and whose union is A.*

That is, a partition is formed by an index set I and non-empty sets S_i (defined for every $i \in I$) that satisfy the following conditions:

(1) For every $i \in I$, $S_i \subseteq A$.

(2) For every $i, j \in I$ with $i \neq j$, we have $S_i \cap S_j = \varnothing$.

(3) $\bigcup_{i\in I} S_i = A$

The sets S_i are called **parts** *of the partition.*

这里的思想是，集合 S_i “划分” 集合 A 成非重叠、非空的部分。

Example 3.6.10. 让我们看看几个例子。

(1) 考虑集合 $\mathbb{N}$。令 O 为奇自然数集合，令 E 为偶自然数集合。那么 $\{O, E\}$ 是 $\mathbb{N}$ 的一个划分。这是因为

- $E, O \neq \varnothing$，并且
- $E, O \subseteq \mathbb{N}$，并且
- $E \cap O = \varnothing$，并且
- $E \cup O = \mathbb{N}$

(2) 考虑集合 $\mathbb{R}$。对于每一个 $z \in \mathbb{Z}$，定义集合 S_z 通过

$$S_z = \{r \in \mathbb{R} \mid z \leq r < z + 1\}$$

我们断言 $\{\ldots, S_{-2}, S_{-1}, S_0, S_1, S_2, \ldots\}$ 是 $\mathbb{R}$ 的一个划分。你能看出为什么吗？试着写出这个集合划分所需的条件，并看看你是否能理解为什么它们成立。

具体来说，记住我们需要这些集合是 *pairwise* 不相交的。这意味着 *any* 两个集合必须是不相交的。注意，这与要求 *all* 集合的交集为空是相当不同的。

例如，考虑集合的集合{v*}

$$\big\{\, \{1,2\}, \{2,3\}, \{3,4\} \,\big\}$$

这个集合是 *not* 两两不相交的，因为例如，

$$\{1,2\} \cap \{2,3\} = \{2\} \neq \varnothing$$

然而，所有三个集合的交集为空，因为没有任何元素同时属于这三个集合。

Example 3.6.11. 现在，让我们看看几个非示例。

(1) 考虑集合 $\mathbb{R}$。令 P 为正实数集合，令 N 为负实数集合。那么 $\{N, P\}$ 不是一个划分，因为 $0 \notin N \cup P$。

您能否修改我们在这里做出的选择，以识别将 $\mathbb{R}$ 分成两部分的划分?

(2) 考虑集合 $\mathbb{Z}$。令 A_2 为所有2的倍数的整数集合，令 A_3 为所有3的倍数的整数集合，令 A_5 为所有5的倍数的整数集合。集合 $\{A_2, A_3, A_5\}$ 不是划分的原因有两个。

首先，这些集合不是两两互斥的。注意，$6 \in A_2$ 和 $6 \in A_3$，因为 $6 = 2 \cdot 3$。其次，这些集合并没有“覆盖”所有 $\mathbb{Z}$。注意，$7 \in \mathbb{Z}$ 但 $7 \notin A_2 \cup A_3 \cup A_5$。

如我们所述，我们将来会经常使用这个定义，所以请记住。

3.6.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 什么是指标集?

(2) 设 $I = \mathbb{N}$，对于每一个 $i \in I$，设 $A_i = \{i, -i\}$。为什么以下集合都是 *same* 集合?

$$\bigcup_{i \in I} A_i \qquad \bigcup_{x \in \mathbb{N}} A_x \qquad \bigcup_{j \in I} A_j$$

顺便问一下，这个集合的元素是什么?

(3) 列出以下集合的元素:

(a) $\bigcup_{x \in \mathbb{N}} \{x\}$ b) $\bigcap_{x \in \mathbb{N}} \{x\}$ c) $\bigcup_{x \in \mathbb{N}} \{x, 0, -x\}$

((

(4) 你为什么认为我们没有谈论“索引差”或“索引补”，而只谈论了并集和交集?

(5) 什么是划分? 一个集合的集合要满足什么条件才能成为该集合的划分?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) Let $A = \{-2, -1, 0, 1, 2\}$. Let $B = \{1, 3, 5\}$.

For every $i \in \mathbb{Z}$, let $S_i = \{i - 2, i, i + 2, i + 4\}$.

What is $\bigcup_{i \in A} S_i$? What is $\bigcap_{x \in B} S_x$?

(2) 对于每个 $n \in \mathbb{N}$，让 $A_n = [n]$。$\bigcap_{n \in \mathbb{N}} A_n$ 是什么? $\bigcup_{n \in \mathbb{N}} A_n$ 呢?

(3) 找一种方法使用集合构造符号来表示介于-10和10之间（包括两端）的所有整数的集合。然后，使用索引并集定义相同的集合。你能以这种方式做到，使得并集中的集合两两互斥（即它们之间没有任何共同元素）吗? （提示：可以。）

(4) 对于每个 $n \in \mathbb{N}$，令 M_n 为 n 的所有 *multiples* 的集合。（例如，$M_3 = \{3, 6, 9, \dots\}$。）使用集合构造表示法为 M_n 写一个定义。然后，使用这些集合将这些集合表示为并集。

(您能否使用这些集合来定义一个 $\mathbb{N}$ 的 *partition*？)

(5) Let X be any set. What is $\bigcup_{S \in \mathcal{P}(X)} S$? What about $\bigcap_{S \in \mathcal{P}(X)} S$?

(可能先尝试使用特定的集合，例如 $X = \{1, 2\}$，看看会发生什么。)

(6) 确定一个指标集并定义一些集合，以便您可以将 $\mathbb{Q}$ 表示为索引并集。

您能这样做，使得指标集中有无限多个元素吗?

((**Challenge:** 你能把这个收藏做成 *partition* 的 $\mathbb{Q}$ 吗？)

3.7 Cartesian Products

存在一种“组合”集合以产生我们想要研究的其他集合的另一种方法。这种方法基于**order**的想法。当我们通过列举元素来定义集合时，顺序是不相关的；也就是说，集合{1, 2, 3}和{3, 1, 2}以及{2, 1, 3}都是相等的，因为它们包含相同的元素。（更具体地说，它们在两个方向上都是彼此的子集）。然而，当我们观察顺序*is*相关的数学对象时，我们可以以新的方式组合集合并产生新的集合。

您可能已经熟悉实平面的概念，$\mathbb{R}^2$ (也被称为**Cartesian plane**，以法国数学家勒内·笛卡尔的名字命名。平面上每个“点”由两个值描述，一个x-坐标和一个y-坐标，我们书写这些坐标的顺序很重要。我们通常将x-坐标视为第一个，将y-坐标视为第二个，这有助于根据这个顺序区分两个点。例如，点（1, 0）位于x-轴上，但点（0, 1）位于y-轴上。它们不是同一个点。

存在一个更深层次的、数学上的思想是笛卡尔平面的基础。给定任意两个集合，A 和 B，我们可以考虑由 A 和 B 的所有元素组成的集合 **ordered pairs**。当我们说 **pair** 时，我们指的是一个表达式 (a, b)，其中 a 和 b 分别是 A 和 B 的元素。当我们说 **ordered** 时，我们指的是首先写 a，然后写 b 是很重要的。在实平面的情况下，这尤其重要，因为任何实数都可能作为点的 x-坐标 *or* 出现在 y-坐标上，但点 (x, y) 通常与点 (y, x) 不同。（它们何时相等？仔细思考这个问题。）

3.7.1 Definition

在检查一些例子之前，让我们给出这个新集合的显式定义。

Definition 3.7.1. *Given two sets, A and B, the* **Cartesian product** *of A and B is written as $A \times B$ and defined to be*

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

这个定义告诉我们，笛卡尔积 {v*} 将所有有序对 (a, b) 收集到一个新集合中，其中 a 可以是 A 的任何元素，而 b 可以是 B 的任何元素。

Some Technicalities

注意，我们已经放弃了全集 U 的假设。我们已经讨论了在 *not* 指定全集时出现的一些问题，但从此以后，我们处理的集合将不会涉及这些问题。因此，我们只有在这样做会导致歧义的情况下才会指定全集。

在这种情况下，我们可以通过定义有序对(a, b)为*set*来指定一个全集。具体来说，我们可以定义

$$(a, b) = \{\, \{a\}, \{a, b\} \,\}$$

这个定义还包含了这对的 *order*，在以下意义上，

$$(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d$$

检查集合中的单元素告诉我们第一个坐标，检查集合中两个元素的另一个元素告诉我们第二个坐标。如果我们有有序对(a, a)，那么集合就减少到$\{\{a\}\}$，这告诉我们a出现在两个坐标中。

使用此定义，我们可以使用全集 $U = \mathcal{P}(\mathcal{P}(A \cup B))$。我们不会深入探讨这些集合和定义的技术细节，但我们认为指出这些定义的存在是谨慎的。本节中需要记住的重要观点如下：

> 两个有序对相等，当且仅当它们的坐标中有 *both* 相等。

这是为什么我们称之为 **ordered pairs**。

3.7.2 Examples

笛卡尔平面是 $\mathbb{R} \times \mathbb{R}$，这就是为什么我们有时会看到它写成 $\mathbb{R}^2$。确实，如果 $A = B$，那么我们有时会将笛卡尔积写成 $A \times A = A^2$，前提是不混淆 A 是一个集合（而不是一个数字）。让我们看看一些例子，其中笛卡尔积中的两个集合并不相同。

Example 3.7.2. 定义集合 $A = \{a, b, c\}$ 和 $B = \{6, 7\}$ 以及 $C = \{b, c, d\}$。然后我们可以列出以下笛卡尔积的元素:

$$A \times B = \{(a, 6), (a, 7), (b, 6), (b, 7), (c, 6), (c, 7)\}$$
$$B \times C = \{(6, b), (6, c), (6, d), (7, b), (7, c), (7, d)\}$$
$$A \times C = \{(a, b), (a, c), (a, d), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d)\}$$
$$C \times B = \{(b, 6), (b, 7), (c, 6), (c, 7), (d, 6), (d, 7)\}$$

请注意，通常情况下，$B \times C \neq C \times B$，正如这个例子所示。

(您能识别出哪些情况下的 $A \times B = B \times A$? 为了使这个等式成立，我们必须对集合 A 和 B 施加什么条件？)

Ordered Triples and Beyond

这个想法也扩展到三个或更多集合的笛卡尔积。我们简单地用有序的 *triples* 表示三个集合的笛卡尔积，在一般情况下，对于 n 个集合的笛卡尔积，我们写为有序的 n-元组。（再次指出，存在定义这些有序 n-元组的集合论方法，但我们将不会探讨这些细节。）

Example 3.7.3. 卡氏积 $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ (有时写作 $\mathbb{N}^3$) 是所有自然数有序三元组的集合。例如，(1, 2, 3) $\in \mathbb{N}^3$ 和 (7, 7, 100) $\in \mathbb{N}^3$，但 (0, 1, 2) $\notin \mathbb{N}^3$ 和 (1, 2, 3, 4) $\notin \mathbb{N}^3$。

注意 $\mathbb{N}^3$ 和 $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ 之间的细微区别。$\mathbb{N}^3$ 的一个典型元素是一个有序的 *triple*，其坐标每个都是自然数。$(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ 的一个典型元素是一个有序的 *pair*，其第一个坐标也是一个有序对（自然数），第二个坐标是一个自然数。也就是说，((1, 2), 3) $\in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ 但 ((1, 2), 3) $\notin \mathbb{N}^3$。这表明这两个是 *different sets*。

然而，有一种 *natural* 方法可以将这两个集合联系起来，本质上“消除了第一个坐标（有序对）周围的括号”。我们将在讨论函数和 *bijections* 时再讨论这个问题。现在，我们只想让你注意到这两个集合之间的细微差别，并记住两个集合的笛卡尔积是 *ordered pairs* 的 *set*，其中每个坐标来自相应的组成部分集合。

Example 3.7.4. 如果$B = \varnothing$，比如说，会发生什么? 回顾一下$A \times B$的定义。实际上有no个B元素可以写成有序对的第二个“坐标”，所以我们实际上没有$A \times B$的元素可以包含！因此，

$$A \times \varnothing = \varnothing$$

对于任何集合 A。同样地，$\varnothing \times B = \varnothing$，对于任何集合 B。

3.7.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) $\mathbb{R} \times \mathbb{N}$ 和 $\mathbb{N} \times \mathbb{R}$ 之间的区别是什么？给出一个有序对，它是其中一个集合的元素，但不是另一个集合的元素。然后，给出一个实际上属于 *both* 个集合的有序对的例子。

(2) 什么是 $\varnothing \times \mathbb{Z}$?

(3) 将集合 $\{\heartsuit, \diamondsuit\} \times \{\smile, \square, \heartsuit\}$ 的所有元素写出来。

(4) $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ 和 $\mathbb{N} \times (\mathbb{N} \times \mathbb{N})$ 之间的区别是什么？为什么它们在技术上不是同一个集合？你能解释为什么它们“本质上”是同一个集合吗?

(5) 设 A, B, C 为集合。假设 $A \subseteq B$。你认为 $A \times C \subseteq B \times C$ 是真的吗？为什么或为什么不?

(6) 给出一个集合 S 的例子，使得 $\left(\frac{1}{2}, -1\right) \in S$。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 写出[3] × [2]的元素。你能推测出$[m] \times [n]$有多少个元素，对于任何 $m, n \in \mathbb{N}$？(你将如何尝试证明你的推测？)(2) 给出集合$\mathbb{N} \times \mathcal{P}(\mathbb{Z})$的一个元素示例。(3) 给出集合$\big((\mathbb{R} \times \mathbb{N}) \times \mathbb{Q}\big) \cap \big((\mathbb{Q} \times \mathbb{Z}) \times \mathbb{N}\big)$的一个元素示例。(4) 给出满足$C \times D = D \times C$的集合$C, D$的示例。

> 后续挑战：你能像这样描述 *all possible situations* 吗？关于 C 和 D 必须满足什么条件？你能证明它吗?

(5) 写出 $\mathcal{P}\big($ 的元素 [1] × [2] $\big)$。

(6) 对于每个 $n \in \mathbb{N}$，令 $A_n = [n] \times [n]$。考虑集合

$$B = \bigcup_{n \in \mathbb{N}} A_n$$

是 $B = \mathbb{N} \times \mathbb{N}$ 吗？解释，并举例。

(7) 如果你了解一些简单的计算机编程，尝试编写代码（使用你喜欢的语言）输入 $m, n \in \mathbb{N}$ 并打印出 $[m] \times [n]$ 中的所有元素。（如果你对编程不是很舒服，可以使用一些伪代码。）你认为这需要多长时间运行，这取决于 m 和 n?

3.8 [Optional Reading] Defining the Set of Natural Numbers

我们的目标在本节中是将自然数 $\mathbb{N}$ 建立在严谨、数学的基础上。具体来说，我们将通过定义并从集合论公理和原则中推导出自然数来证明自然数的存在。然后，我们将讨论它们的一些性质。在讨论了一些数学逻辑的基本原则和结果之后，我们将使用这些性质在第五章中定义和证明数学归纳法原理。

3.8.1 Definition

我们如何用集合来定义自然数？我们直观地知道它们是什么。我们从1开始，反复加1，得到所有其他自然数。因此，我们必须确定我们所说的“1”和“加1”在集合中的含义。为此，让我们先思考0。我们之前说过，我们不会将0包含在集合$\mathbb{N}$中，但一些作者这样做，这有助于我们推导$\mathbb{N}$，现在，让我们考虑它。我们知道只有一个不包含任何元素的集合，即空集。因此，将0与空集联系起来是有意义的；事实上，我们将0与空集$= \varnothing$联系起来。接下来，我们希望定义1，根据我们对0的定义，选择一个恰好包含一个元素的集合是有意义的。（一个包含一个元素的集合也被称为**singleton**。）存在几个这样的集合：

$$\{\varnothing\}, \{\{\varnothing\}\}, \{\{\varnothing, \{\varnothing\}\}\}$$

我们如何选择一个 *representative* 单例来表示 1？考虑到我们希望继续这个过程，并最终用前一个数来定义 2（以及 3，等等），现在用我们拥有的唯一对象来定义 1 是有意义的：0。因此，让我们 *choose* 来定义

$$1 = \{0\} = \{\varnothing\}$$

这保证了$0 \neq 1$。

接下来定义2，我们考虑包含两个元素的集合 s，如

$$\{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\{\varnothing\}\}\}, \{\{\varnothing\}, \{\{\varnothing\}\}\}$$

等等。我们寻求一个自然代表，我们注意到上面列出的第一个集合包含我们已经定义的两个对象，0 和 1！因此，定义 $2 = \{0, 1\}$ 是一个自然的选择，而且，我们再次知道 $2 \neq 0$ 和 $2 \neq 1$。

Successors

这使我们直观地了解到如何继续这个过程并定义任何自然数：对于任何 $n \in \mathbb{N}$，我们定义

$$n = \{0, 1, 2, \ldots, n-2, n-1\}$$

然而，给定一个集合，使用这个定义来验证该集合是否代表一个自然数是非常困难的。我们希望有一个 *better* 的定义来描述 $\mathbb{N}$ 的元素；我们想知道，对于任何集合，它是否属于 $\mathbb{N}$。回顾上面的元素 n；我们也可以写成

$$n = \{0, 1, 2, \ldots, n-2, n-1\} = \{0, 1, 2, \ldots, n-2\} \cup \{n-1\} = (n-1) \cup \{n-1\}$$

看看那个！我们有一种自然的方法来定义$\mathbb{N}$中的一个元素，既基于前一个元素，也基于集合运算。这促使我们得出以下定义。

Definition 3.8.1. *Given any set X, the* **successor** *of X, denoted by $S(X)$, is defined to be $S(X) = X \cup \{X\}$.*

这个定义适用于所有集合，但在自然数的背景下，它意味着 n 的后继正是我们直觉上认为比它大1的那个自然数，即 $n + 1$。

Inductive Sets

这使我们更接近于我们的定义 $\mathbb{N}$。我们当然希望 $1 \in \mathbb{N}$，并且我们也希望对于任何元素 $n \in \mathbb{N}$ 有 $S(n) \in \mathbb{N}$。为了以符号形式表达这一点，我们做出以下定义：

Definition 3.8.2. *A set I is called* **inductive** *provided*

1. $1 \in I$
2. *If $n \in I$, then $S(n) \in I$, as well.*

当然，$\mathbb{N}$本身（正如我们希望定义的那样）应该是一个归纳集。是否存在*other*归纳集？考虑这个问题。它们会有什么性质？它们会包含哪些是*not*自然数的元素吗？我们不想深入探讨这些问题，但为了我们在这里的讨论，我们将指出，确实存在其他归纳集。我们不希望这些集合中的任何一个是$\mathbb{N}$，因此我们做出这个定义：

Definition 3.8.3. *The set of all* ***natural numbers*** *is the set*

$$\mathbb{N} := \{x \mid \text{ for every inductive set } I,\ x \in I\}$$

Put another way, $\mathbb{N}$ *is the* 最小的 *inductive set, in the sense of set inclusion:*

$$\mathbb{N} = \bigcap_{I \in \{S \mid S \text{ is inductive}\}} I$$

This dictates that $\mathbb{N}$ *is a subset of every inductive set.*

这给了我们所需的“检查属性”。任何集合 x 是自然数（即 $x \in \mathbb{N}$），当且仅当它是 *every* 归纳集（即 $x \in I$ 对于每个归纳集 I）的元素。这也告诉我们 $\mathbb{N} \subseteq I$ 对于每个归纳集 I。

存在一些其他集合论讨论可以在此进行：我们如何知道这样的无限集合存在？（实际上，我们需要将这一点作为集合论的一个 *axiom*！假设这些类型的集合存在，我们如何描述那些不是 $\mathbb{N}$ 的其他归纳集合？解决这些问题超出了本课程的范畴和目标，因此我们不会讨论它们。然而，我们现在将提到 $\mathbb{N}$ 的几个性质，特别是那些有助于在严格的基础上建立数学归纳法的性质。（如果你在好奇，想想整数集 $\mathbb{Z}$。试着解释为什么这个集合确实是归纳的。关于 $\mathbb{R}$ 和 $\mathbb{Z} - \mathbb{N}$ 呢？）

Properties of $\mathbb{N}$

在定义归纳原理之前，让我们思考一下自然数的常见属性和用途：排序和算术。对于任意两个自然数，我们可以 *compare* 它们并决定哪个更大，哪个更小（或者如果它们相等）。我们通常用符号如 $1 < 3$，$1 \leq 5$，$4 \not< 2$，$3 = 3$ 等来表示。

我们可以用 *sets* 来表述这些比较，因为我们已经将 $\mathbb{N}$ 的元素定义为集合，对吗？是的，我们可以！回顾一下 *successor* 的定义。这个定义中包含了一个事实：$X \in S(X)$！这个观察结果给出了以下定义：

Definition 3.8.4. *Given two natural numbers* $m, n \in \mathbb{N}$*, we write* $m < n$ *if and only if* $m \in n$*.*

这定义了集合 $\mathbb{N}$ 上的 *order relation*。我们将在本书后面的章节（第6.3节）中讨论关系和顺序的概念。

关于算术？$m + n$在集合m和n的术语下是什么？我们如何定义这个操作及其输出？我们如何知道$m + n$是另一个自然数？我们能确定$m + n = n + m$吗？这些问题我们可以在讨论函数和关系之后稍后解决。

3.8.2 Principle of Mathematical Induction

现在，让我们呈现一个更严格的归纳版本：

Theorem 3.8.5 (数学归纳法原理)**.** *Let $P(n)$ be some "fact" or "observation" that depends on the natural number n. Assume that*

1. *$P(1)$ is a true statement.*
2. *Given any $k \in \mathbb{N}$, if $P(k)$ is true, then we can conclude* 必须 *that $P(k+1)$ is true.*

Then the statement $P(n)$ must be true for 每个 *natural number $n \in \mathbb{N}$.*

首先证明这个定理，然后再详细讨论其假设和结论。

Proof. 定义集合 S 为使得陈述 P 为真的自然数。也就是说，定义 $S = \{n \in \mathbb{N} \mid P(n) \text{ 为真 }\}$。根据定义，$S \subseteq \mathbb{N}$。

此外，该定理的假设保证了$1 \in S$，并且每当$k \in S$时，我们同样知道$k+1 \in S$。这意味着S是一个*inductive*集合。通过我们在定义$\mathbb{N}$后所做的观察，我们知道$\mathbb{N} \subseteq S$。

因此 $S =$ $\mathbb{N}$, 因此，对于每个自然数，陈述 $P(n)$ 是正确的 n. □

这是相当 *slick*，对吧？似乎所有期望的结论都“从”我们的定义中“掉落”出来了！从这个意义上说，定义和公理是 *natural* 选择，因为它们实现了我们对集合 $\mathbb{N}$ 及其性质的 *intuition* 已经“知道”的事情。

存在一些我们尚未讨论的细微问题。具体来说，我们所说的“事实”或“观察”在自然数 *depends* 上是什么意思？当 $P(k)$ 为真时，*necessarily conclude* $P(k+1)$ 为真意味着什么？*true* 的意思又是什么？这些都是深奥的数学问题，需要深入研究逻辑，我们将在下一章讨论这些问题！继续前进！万岁！

3.8.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 什么是归纳集？给出一个不是 $\mathbb{N}$ 或 $\mathbb{Z}$ 的例子。

(2) 我们在数学归纳法原理的证明中定义 $S = \{n \in \mathbb{N} \mid P(n) \text{ 是真}\}$。这是什么意思？用文字描述这个集合。

(3) 想出一个自己的类比来说明归纳是如何工作的。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 如果我们将 **successor** 的定义改为 $S(X) = \{X\}$，使用 $0 = \varnothing$，1，2，3 和 4 在集合论中分别代表什么？它们是否仍然满足等式 $n = \{0, 1, \ldots, n-1\}$？如果不满足，它们是否满足其他某种关系？探索!

(2) 与朋友辩论关于无限集合是否存在的问题。为什么我们需要$assume$一个归纳集合的存在来定义$\mathbb{N}$？这对你来说似乎合理吗？这在物理上、数学上合理吗?

(3) 考虑一个简单的算术语句，例如 $1 + 2 = 3$。用集合表示数字 1、2 和 3，看看这个等式可能有什么意义。在这个上下文中，“$+$”代表什么意思?

(4) 探讨如何定义 $\mathbb{Z}$，使用 $\mathbb{N}$。在网上或书籍中做一些探索，或者自己想出一个想法。

3.9 Proofs Involving Sets

现在我们已经通过了许多定义和例子，为了介绍集合是什么以及如何操作它们，让我们实际上编写一些关于集合的严谨、数学正确且写得好的 **proofs**。这里包含的所有命题/引理都是有用的事实，我们可以在以后引用，我们希望你能证明这样的主张。（注意：引理只是一个需要一些证明的小结果，以后可以引用来证明更重要的定理。）此外，所有这些证明都是我们未来、非常近的未来所期望的质量和严谨程度。如果你愿意，可以将这些作为指南!

3.9.1 Logic and Rigor: Using Definitions

我们在这里想要强调的主要观点——随着我们从描述性、冗长和直观的证明过渡到更严谨、数学上正确和正式书写的证明——是
formal definitions are very important。从根本上说，它们是必不可少的，因为当我们说，例如，“$A \cup B$”时，我们需要知道你确切地知道这个符号的含义以及它在集合A和B上的操作方式。

作为另一个例子，当我们说“证明 $A = B$”时，我们心中有一个非常具体的目标，你们需要保持一致。对主要概念有一个直观的理解总是有帮助——“哦，陈述 $A = B$ 只是

表示 A 和 B 具有相同的元素”——但这正是我们在严格证明中想要使用的 *not* 语言/思想类型。为了证明像 $A = B$ 这样的陈述，我们需要你在集合的上下文中 **appeal to the definition** “=”： $A = B$ 当且仅当 $A \subseteq B$ 和 $B \subseteq A$。

这是当我们说“满足定义”或“诉诸定义”时的意思：为了证明某个数学对象具有某种属性，你必须证明该对象满足该属性的正式定义。如果你不熟悉这个定义，或者忘记了如何精确地表述它……无论如何，去查查吧！我们明白这需要吸收大量新信息，而且当你对它还不太熟悉时忘记一些东西并没有什么不妥。通过这样做，你将更快、更牢固地内化这些想法。

您将看到我们如何在以下示例中使用“$\subseteq$”、“=”、“$\cap$”等定义，以及等等。对于每个命题/引理，我们将最终写出形式化的证明，但也会简要说明我们如何处理这样的证明。很多时候，这很困难！我们认为您会注意到，许多这样的解释只是回忆一个相关的定义，并思考它的含义以及它在给定情况下的应用。从某种意义上说，这就是许多数学的本质。我们只是允许我们使用的定义变得越来越复杂。

3.9.2 Proving “$\subseteq$”

回忆一下 **subset** 的定义，因为我们在这里会经常使用它：

Definition 3.9.1. *Given two sets A and B, if every element of A is* 也 *an element of B, then we say A is a* **subset** *of B.*

假设我们面临以下问题：

> 设 A 为集合...设 B 为集合...证明 $A \subseteq B$。

如何满足 $A \subseteq B$ 的定义以证明这个论断？是的，直观的想法是“A 的每个元素也是 B 的元素”，但我们不应该只是试图回避问题并试图将这句话作为我们的结论。相反，我们需要验证 *every* 是 A 的元素也是 *necesarily* B 的元素。这正是奇妙短语 **“arbitrary and fixed”** 会派上用场的地方！

The Phrase “Arbitrary and Fixed”

我们如何一次性讨论 *all possible elements* 的 A 呢？当然，如果 A 只有，比如说，3 个元素，我们可能不需要这样做；那时，我们可以逐个处理它们。但如果 A 有 100 个元素呢？或者 100 万个？或者 *infinitely* 那么多？我们如何以合理的方式一次性证明关于它们的所有内容呢？

我们将引入一个 **arbitrary and fixed** 元素，使其成为 A 的一部分，以便我们有所作为。这个元素将是 **arbitrary** 的意思，即

我们不对它是什么或它具有哪些属性做任何额外假设，只假设它是A的一个元素。在这个意义上，这个元素将是**fixed**，即我们将给它指定某个变量名（通常是一个字母，如a或x或t或类似的东西），这个字母将代表我们证明剩余部分中的*same*对象。只要我们能证明这个元素的目标，那么我们就会同时证明关于A中的*all*元素的一些事情。Voilà!

Examples

让我们看看这个过程的实际操作，真正理解其要点。我们将从待证明的陈述开始，然后描述我们构思证明的过程，最后呈现我们的正式书面证明。

Lemma 3.9.2. *Let A, B, X be any sets.*

If $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.

Intuition: 考虑绘制一个维恩图来表示这种情况。为了确保假设 $X \subseteq A$ 和 $X \subseteq B$ 都成立，我们需要使集合 X “位于” A 和 B 之内。相应地，这意味着 X 必须完全“位于”A 和 B 交集的区域内，这正是 $A \cap B$ 所表示的。这有助于我们认识到这个陈述确实是 True。但这并不能证明任何东西!

为了 *prove* 该陈述，我们将引入一个任意且固定的元素 $x \in X$。关于它，我们知道什么？嗯，我们假设了 $X \subseteq A$。"$\subseteq$" 的定义意味着 X 的任何元素都是 *also* A 的一个元素。但我们知道 x 是 X 的一个元素；这意味着它也是 A 的一个元素。多么方便！我们可以对 x 和 X 和 B 作出一些类似的陈述，这将告诉我们 $x \in B$。这究竟意味着什么？哦嘿，"$\cap$" 的定义适用，并告诉我们 $x \in A \cap B$。太棒了！现在，让我们把它写下来。

Proof. 让 $x \in X$ 为任意且固定的。

根据假设 $X \subseteq A$，因此 $x \in A$，同样，根据 $\subseteq$ 的定义。

同样，根据假设 $X \subseteq B$，所以 $x \in B$，也是如此。

自 $x \in A$ *and* $x \in B$ 以来，这意味着 $x \in A \cap B$，根据 $\cap$ 的定义。

总体而言，我们已经表明，每当 $x \in X$ 时，$x \in A \cap B$ 也成立。由于 $x \in X$ 是任意的，我们得出结论 $X \subseteq A \cap B$。 □

还不错，对吧？让我们再试一个，稍微难一点的。

Proposition 3.9.3. *Let A and B be any sets. Then, $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.*

哇，这真的是真的吗？回顾3.5节中的问题6，你就会看到一个例子。这个说法声称这是真的，*in general*，而不仅仅是对那个例子。让我们弄清楚为什么，然后证明它。

Intuition: 这里有几个定义层在工作。特别是，*power set*操作可能让你感到困惑。关键是只需记住

该定义：$\mathcal{P}(A)$ 是所有 *subsets of* A 的集合。现在，这里的主要论断是一种 *subset* 关系：无论集合 $\mathcal{P}(A) \cap \mathcal{P}(B)$ 是什么（我们稍后会分析它，但重要的是你立即识别出它的 *type* 对象：一个 *set*），它应该包含在集合 $\mathcal{P}(A \cap B)$ 中。就是这样，重要的是要注意这一点实际上激发了即将到来的证明的整体形式。

无需思考 $\mathcal{P}(A) \cap \mathcal{P}(B)$ 的含义，我们就可以确信我们的证明将从“设 $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ 为任意且固定的”开始。这是因为我们需要通过取集合左侧的任意元素并推导出它也是右侧集合的元素来满足“$\subseteq$”的定义。这就是我们所说的证明的 **structure**。

元素 $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ “看起来”像什么？它是一个集合，并且它是 $\mathcal{P}(A)$ 和 $\mathcal{P}(B)$ 的元素。这意味着……好吧，我们实际上要跳过前面，直接进入正式证明，因为我们下面还是会重复同样的词语。但在继续阅读 *ours* 之前，我们认为你应该先尝试写出你的 *own* 证明。然后，当你完成时，你可以比较看看你是否正确，是否与我们的步骤相同，是否写得清晰，等等。看看你能做什么！

Proof. 让 $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ 为任意且固定的。

根据 $\cap$ 的定义，这意味着 $X \in \mathcal{P}(A)$ *and* $X \in \mathcal{P}(B)$。

自 $X \in \mathcal{P}(A)$ 以来，根据幂集的定义，我们知道 $X \subseteq A$。

同样，由于 $X \in \mathcal{P}(B)$，我们知道 $X \subseteq B$。

自 $X \subseteq A$ 和 $X \subseteq B$ 以来，我们知道根据我们刚刚证明的引理3.9.2，$X \subseteq A \cap B$。

现在，由于 $X \subseteq A \cap B$，我们根据幂集的定义知道 $X \in \mathcal{P}(A \cap B)$。

由于 X 是任意的，我们得出结论 $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$。 □

你做了我们做的事情吗？你也引用了前面的引理吗？你反而没有意识到，又重新证明了那个结果吗？把这当作一个教训吧！证明结果的一个主要好处是我们可以在以后的证明中使用它们！在这个证明的中间再次证明前面的结果在技术上并没有错误；这也许可以节省一点时间和写作。如果你发现自己正在处理一个问题，并想，“嘿，这感觉好熟悉……”的话，回去寻找相关的定理或引理或例子。也许你可以利用已经获得的知识来占优势。

3.9.3 Proving "="

Double-Containment Proofs

再次，我们需要回忆"="的定义（在集合的上下文中），因为我们在这里会频繁使用它。

Definition 3.9.4. *We say two sets, A and B, are* **equal***, and write $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.*

这是全部！它完全由先前的定义构建而成，即"$\subseteq$"（因为"$\supseteq$"的定义完全等价）。因此，这本身并不是一项新技术，因为它实际上是对先前技术的重复应用。也就是说，为了证明$A = B$，我们只需要使用上一小节中使用的技巧，然后证明$A \subseteq B$，再证明$B \subseteq A$。

这种技术非常常见，事实上，它还被赋予了一个名称：**double-containment**。当我们证明两个集合互为子集，双向证明，并得出它们相等的结论时，我们称之为**double-containment proof**。

Examples

让我们看看这种双重隔离技术在行动中的例子。

Lemma 3.9.5. *Let A and B be any sets. Then, $A - (A \cap B) = A - B$.*

Intuition: 通常，我们可以画一个文氏图来让我们自己相信这个真理，但这并不能证明任何事情。相反，我们将遵循双重包含证明。如果我们取一个元素$x \in A - (A \cap B)$，我们首先可以应用"$-$"的定义，然后是"$\cap$"，以推断关于x的一些内容。希望它能告诉我们$x \in A - B$。然后，如果我们取一个元素$y \in A - B$，我们可以尝试应用一些定义，希望推断出$x \in A - (A \cap B)$。也许我们还不确定如何确切地做到这一点，但通过查看那个文氏图并使用定义，我们肯定能弄清楚。你为什么不先试试，然后再看我们的证明呢！

Proof. 我们将通过双重包含证明展示 $A - (A \cap B) = A - B$。

（"$\subseteq$"）首先，让 $x \in A - (A \cap B)$ 是任意且固定的。根据"$-$"的定义，我们知道 $x \in A$ 和 $x \notin A \cap B$。这意味着 x 是 *both* A 和 B 的元素是 *not* 真实的。我们已知 $x \in A$，因此我们推断出 $x \notin B$。

因此，$x \in A$和$x \notin B$，根据"$-$"的定义，我们推断出$x \in A - B$。这表明 $A - (A \cap B) \subseteq A - B$。

（"$\supseteq$"）其次，令 $y \in A - B$ 为任意且固定的。根据"$-$"的定义，这意味着 $y \in A$ 和 $y \notin B$。现在，由于 y 不是 B 的元素，这意味着当然 y 不是 *both* A 和 B 的元素。也就是说，$y \notin A \cap B$，根据"$\cap$"的定义。

自我们知道 $y \in A$ 和 $y \notin A \cap B$，我们推断 $y \in A - (A \cap B)$。这

显示 $A - B \subseteq A - (A \cap B)$。

总体而言，双重包含证明表明 $A - (A \cap B) = A - B$。 □

查看这个证明的整体结构。我们知道它将分为两部分，因为这是一个双重包含证明，但我们也很体贴地为我们的勇敢读者提供了
point this out ahead of time，并适当地分隔了这两个部分。技术上可以忽略这一点，直接进入证明，但这样可能会让读者感到困惑。证明的全部目的是为了 *convince someone else* 你已经想出的真理，所以你最好尽可能让他们容易理解你在做什么。

让我们看看证明两个集合相等的另一个例子。这个例子会有一点不同，因为双重包含的一部分将使用补集运算。作为预览，现在花一分钟思考为什么陈述 $A \subseteq B$ 和 $B \subseteq \overline{A}$ 在存在某个全集 $A, B \subseteq U$) 的情况下是 *equivalent* (。画一个维恩图并尝试一些例子。甚至尝试证明它！

Proposition 3.9.6.

$$\left\{ x \in \mathbb{N} \mid x + \frac{8}{x} \leq 6 \right\} = \{2, 3, 4\}$$

Proof. 让我们定义 $A = \left\{ x \in \mathbb{N} \mid x + \frac{8}{x} \leq 6 \right\}$，以及 $B = \{2, 3, 4\}$。

为了展示 $A = B$，我们将展示 $A \subseteq B$ 和 $B \subseteq A$。

首先，我们将展示 $B \subseteq A$。我们可以单独考虑这三个元素中的每一个，并验证它们满足 B 的定义不等式：

$$2 + \frac{8}{2} = 6 \leq 6$$
$$3 + \frac{8}{3} = \frac{17}{3} \leq 6$$
$$4 + \frac{8}{4} = 6 \leq 6$$

自$2, 3, 4 \in \mathbb{N}$以来，我们推断出$2 \in A$ 和 $3 \in A$ 以及 $4 \in A$，因此 $B \subseteq A$。

接下来，为了展示 $A \subseteq B$，我们将展示 $B \subseteq \overline{\overline{A}}$，其中补集是在 $\mathbb{N}$ 的上下文中取的。也就是说，我们将展示所有自然数 $1, 5, 6, 7, \ldots$ 都是 *not* 的 A 元素。

为了展示这一点，我们将验证A的定义不等式*not*被这些元素中的任何一个所满足。

第一个和第二个情况可以很容易地考虑：$1 + \frac{8}{1} = 9 \not\leq 6$ 和 $5 + \frac{8}{5} = \frac{33}{5} \not\leq 6$。

为了考虑其他情况，我们可以取一个任意且固定的 $x \in \mathbb{N}$ 与 $x \geq 6$。注意，那么，$x + \frac{8}{x} \geq 6 + \frac{8}{x} > 6$，因为 $\frac{8}{x} > 0$。

这表明 *only* 2,3,4 满足定义不等式 的 A。

总体而言，通过双重包含论证，我们已证明 $A = B$。 □

仔细思考一下，为什么证明的第二部分中使用的方法是有效的。（这实际上是一个使用条件语句的 **contrapositive** 的例子，但我们还没有定义这些术语；我们将在下一章关于逻辑的章节中这样做。）

让我们看看另一个证明集合相等的例子。这个例子只是略有不同，因为我们正在证明某个集合实际上是 *empty set*，为此，我们将证明它具有 *no elements*。

Proposition 3.9.7. *For every $n \in \mathbb{N}$, define $S_n = \mathbb{N} - [n]$. Then*

$$\bigcap_{n\in\mathbb{N}} S_n = \varnothing$$

我们建议您首先对这个陈述进行尝试，如果它没有意义。例如，尝试识别集合 S_1、$S_1 \cap S_2$、$S_1 \cap S_2 \cap S_3$ 等的元素。然后尝试找出左侧大交集的一个候选元素，并弄清楚为什么它实际上是该集合的元素 *not*。之后，尝试找出一个正式的证明并将其写出来；然后，看看下面的我们的证明！

Proof. 让我们定义 $T = \bigcap_{n\in\mathbb{N}} S_n$，以便以后可以引用它。

要证明 $T = \varnothing$，我们将展示 T 不包含任何元素。注意 T 是由许多自然数集合的交集形成的，因此很明显，T 的元素只有自然数。

Con 考虑一个任意且固定的 $x \in \mathbb{N}$。我们想证明那 t $x \notin T$.

Observe that $x \in [x] = \{1, 2, \ldots, x\}$. Thus, $x \notin \mathbb{N} - [x]$, by the definition of "$-$".

根据定义，T 包含属于所有形式为 $\mathbb{N} - [n]$ 的集合的元素。我们已识别（至少）一个交集的集合，$\mathbb{N} - [x]$，使得 x 属于该集合。因此，x 不能是 T 的元素，因为它不属于这些 *all* 集合。因此，$x \notin T$。

由于 $x \in \mathbb{N}$ 是任意的，我们已经证明 T 不包含自然数作为元素，因此它根本不包含 *no* 个元素。 □

Summary: 让我们再陈述一下为什么这种技术有效。我们证明了T中没有元素，即$T \subseteq \varnothing$。这完成了整个过程，因为$\varnothing \subseteq T$也是显而易见真实的。（这个论断适用于任何集合。）因此，双重包含论证的一部分已经实现，我们可以得出$T = \varnothing$。

好的，再举一个例子。我们想包含这个例子，因为它让我们在处理索引集合运算方面有更多的实践。你将发现很多

与此节练习中的类似问题。我们鼓励你们尽可能多地做它们!

Proposition 3.9.8. *For every $n \in \mathbb{N}$, define $A_n = \left\{x \in \mathbb{R} \mid 0 \leq x < 1_n\right\}$. Then,*

$$\bigcap_{n\in\mathbb{N}} A_n = \{0\}$$

考虑这个声明意味着什么。在数轴上绘制 A_n 集合的图像。"$\bigcap$" 交集完成了什么? 为什么 0 是那个交集的元素? 为什么它是 *only* 元素?

$\bigcap$ 的定义在这个证明中至关重要，所以让我们在这里回忆一下定义。关键词是 *for every*:

Definition 3.9.9. *The intersection of a collection of sets A_i indexed by the set I is*

$$\bigcap_{i\in I} A_i = \{x \in U \mid x \in A_i \text{ for every } i \in I\}$$

where we assume there is a set U such that $A_i \subseteq U$ for every $i \in I$.

这是，记住几个集合的索引交集收集属于构成集合的 *all* 的元素。因此，在我们的以下证明中，您将看到我们需要证明（1）0确实是 *all* 的 A_n 集合的一个元素，并且（2）*no other* 数是它们的所有元素，即对于每一个非零实数，我们至少可以确定一个 A_n 集合，该数不是该集合的元素。

Proof. 首先，我们将证明

$$\{0\} \subseteq \bigcap_{n\in\mathbb{N}} A_n$$

这需要我们证明对于 *every* $n \in \mathbb{N}$，有 $0 \in A_n$。

设 $n \in \mathbb{N}$ 为任意且固定的。注意，不等式 $0 \leq 0 < \frac{1}{n}$ 确实成立。

(注意：你可能担心因为“在极限”下0不小于每个分数$\frac{1}{n}$“一次性”，但这不是重点！可以这样想：$0 \in A_1$吗？是的，$0 \leq 0 < 1$。$0 \in A_2$吗？是的，$0 \leq 0 < \frac{1}{2}$。$0 \in A_3$吗？是的，$0 \leq 0 < \frac{1}{3}$。以此类推。不等式对每个$n \in \mathbb{N}$ *individually*都成立，所以0是该集合*every*的一个元素。如果你不担心这个，那就不用担心！继续前进吧！）

因此，对于每个 $n \in \mathbb{N}$，有 $0 \in A_n$，因此 $0 \in \bigcap_{n\in\mathbb{N}} A_n$，根据“$\bigcap$”的定义。这表明 $\{0\} \subseteq \bigcap_{n\in\mathbb{N}} A_n$。

其次，我们将证明

$$\bigcap_{n\in\mathbb{N}} A_n \subseteq \{0\}$$

我们将通过考虑这些集合的 *complements*，在 $\mathbb{R}$ 的背景下完成这项工作。具体来说，我们将证明

$$\overline{\{0\}} \subseteq \overline{\bigcap_{n\in\mathbb{N}} A_n}$$

这意味着我们将证明每个非零实数是 *not every* A_n 的一个元素。

让 $x \in \mathbb{R}$ 为任意且固定的，具有 $x \neq 0$ 的性质。要么 $x > 0$，要么 $x < 0$，因此，让我们分别考虑每种情况。

Case 1: 假设 $x > 0$。考虑数字 $\frac{1}{x} \in \mathbb{R}$。由于自然数在 $\mathbb{R}$ 中是无限且无界的，我们可以选择一个比那个实数 M *bigger* 的自然数 M。也就是说，我们可以选择 $M \in \mathbb{N}$ 使得 $M > \frac{1}{x}$。

（注意：想想为什么这会起作用。我们还没有证明 *proven* $\mathbb{N}$ 是无限的，或者数字“永远延续”在 $\mathbb{R}$ 的数轴上，但我们希望这些想法对你来说直观上是有意义的。）

选择这样的 $M \in \mathbb{N}$，其中 $M > \frac{1}{x}$。由于 $x > 0$，我们可以将不等式两边乘以 x；由于 $M > 0$（因此 $\frac{1}{M} > 0$）我们可以再次乘以 $\frac{1}{M}$。这得到 $x > \frac{1}{M}$。相应地 $x \notin A_M$，因为 $-\frac{1}{M} < x < \frac{1}{M}$ 是 False。

自 $x \notin A_M$ 以来，那么显然 x 不是 *all* 这样的集合的元素。因此，$x \notin \bigcap_{n\in\mathbb{N}} A_n$.

Case 2: 接下来，假设 $x < 0$。我们将像上一个情况一样进行论证；这次，我们只需考虑 $-x$，因为 $-x > 0$。使用上述相同的逻辑，我们肯定可以找到一个满足 $M > \frac{1}{-x} = -\frac{1}{x}$ 的自然数 $M \in \mathbb{N}$。通过操作不等式，我们得知 $x < -\frac{1}{M}$。因此，$x \notin A_M$，所以 $x \notin \bigcap_{n\in\mathbb{N}} A_n$。

因此，我们已经证明，任何具有 $x \neq 0$ 的 $x \in \mathbb{R}$ 都不是至少一个 A_n 集合的元素，因此这样的 x 也不是它们的交集的元素。因此，$\{0\} \subseteq \bigcap_{n\in\mathbb{N}} A_n$，我们通过双重包含论证证明了该命题。

□

这个证明比其他的更难，我们认为，所以请确保阅读几遍，以确保你看到每一步发生了什么。特别是，想想我们是如何想出选择满足 $M > \frac{1}{x}$ 的 $M \in \mathbb{N}$ 这一步的。你认为我们是凭直觉做出这个选择的吗？还是我们认为我们意识到我们希望对于某些 M，$x < \frac{1}{M}$ 是正确的，然后反向操作不等式来找出如何实现这一点？

3.9.4 Disproving Claims

Motivating Example

考虑以下提出的声明:

对于任何集合 F, G, H，如果 $F \subseteq G \cup H$，则要么 $F \subseteq G$，要么 $F \subseteq H$。

这是否是关于 True 的说法？如果是，我们如何证明它？嗯，我们会取一个任意且固定的元素 $x \in F$。由于 $F \subseteq G \cup H$，这也会告诉我们 $x \in G \cup H$，同样。因此，要么 $x \in G$，要么 $x \in H$。就这样了吗？我们完成证明了吗？

我们希望您能认识到这一点，这确实做了*not*工作！特别是，我们在结尾没有满足“$\subseteq$”的定义。如果我们目标是证明“要么$F \subseteq G$要么$F \subseteq H$”，那么我们应该得出结论，以下其中一个命题成立：即*every*是F的元素，同时也是G的元素，或者*every*是F的元素，同时也是H的元素。

我们发现，F的每个元素本身要么是G的元素，要么是H的元素，但我们不能集体决定F中的*all*个元素是其中一个，G或H的元素。再次阅读这两段，以确保你理解这个逻辑观察。实际上写出这个“证明”可能很容易，但可能没有意识到你已经犯了一个错误！

Identifying Errors

这种错误识别是我们正在培养的技能之一，它将在多个方面有所帮助。你会注意到，许多练习（到目前为止有一些，但随着我们继续前进，将会有更多）要求你在某个主张的“证明”中**find the flaw**。通过指出存在缺陷，我们可能正在帮助你找到它（或它们，视情况而定）。阅读一个建议的证明以查找逻辑、事实和清晰度错误是一项基本技能。更重要的是，这种仔细阅读他人的写作将不可避免地使你成为一个更批判性的*your own*阅读者，并帮助你捕捉到像前一段落中那样的潜在错误。如果你没有注意到它，不要担心；现在你已经看到了它，你将在未来留意类似的错误！就像我们说的那样，这种技能是持续发展的，到这本书结束时，你将成为一个伟大的数学证明*reader*者，以及一个伟大的*writer*。

Counterexamples

所以，我们现在该怎么办？我们刚刚意识到我们上面的“证明”并没有奏效。这难道意味着这个主张实际上是 False 吗？实际上，（到目前为止）这仅仅意味着我们的证明尝试失败了。也许其他某种逻辑途径会神奇地带领我们到达那个难以捉摸的结论。

或者，也许这个主张真的是 False。我们如何证明这一点呢？考虑主张的逻辑形式：它说某个陈述对于 *any* 个集合 F, G, H 是正确的。它说假设 $F \subset G \cup H$ 将始终必然地意味着，

那 $F \subseteq G$ 或 $F \subseteq H$。为了证明这 *not* 总是发生，我们需要找到所谓的 **counterexample**。

我们将再次在下一章讨论这些想法，当时我们将正式化 **logic**，但你现在需要知道的是：一个 **counterexample** 是一个具体、详细且描述性的例子，它说明了关于“每一个 . . . ”或“任何 . . . ”或“所有可能的 . . . ”的陈述实际上是如何在每种情况下都成立的。反例相当于 **disproving** 一个关于整个类别的对象具有某种属性的陈述，通过展示该类别中的一个对象 *without* 具有该属性。

Example

让我们看看如何为上面的例子找到并陈述一个反例的过程。

Example 3.9.10. 回忆一下主张：

$$\text{For any sets } F, G, H, \text{ if } F \subseteq G \cup H, \text{ then either } F \subseteq G \text{ or } F \subseteq H.$$

这个主张应该适用于任何集合 F, G, H，因此当我们描述我们的反例时，我们最好描述 *exactly* 那三个集合将会是什么。我们不能只是解释问题，争论可能存在具有某种特性的三个集合。不，我们必须通过明确定义来告诉读者它们的确切内容。这就是我们反驳这个主张的第一行，但我们不能直接跳到那里，因为我们还不知道如何定义它们!

这是有趣/工作的地方：我们需要玩转这些集合的期望属性，以帮助我们想出一个例子。回想一下，我们希望这些集合满足某些属性：我们应该确保假设 $F \subseteq G \cup H$ 成立 True，但我们希望结论——要么 $F \subseteq G$ 要么 $F \subseteq H$——是 False。

这是什么意思? 嗯，我们认为你会同意，从逻辑上讲，那种陈述的“对立面”或“否定”将是“同时 $F \nsubseteq G$ 和 $F \nsubseteq H$”。（这个 **logical negation** 的概念将在下一章中再次出现；现在，我们认为你可以通过应用指导你日常生活的逻辑原则来理解它。很快，我们将使这个想法形式化。）

我们现在有一个具体目标：找到三个集合 F, G, H，它们满足以下三个条件：

$$F \subseteq G \cup H$$
$$F \nsubseteq G$$
$$F \nsubseteq H$$

One thing left to consider is what “{v*}” means. We have a definition of “{v*}”, so what is the “opposite” or “negation” of that? For {v*} to be true, we require that every element of {v*} is also an element of {v*}; so, if this {v*}, then we must have at least one element of {v*} that is {v*} an element of {v*}. The same

观察适用于 $F \not\subseteq H$。现在，我们可以通过应用定义以有助于我们的方式重新陈述我们的目标：

> 每个 F 的元素都是 G 或 H 的元素
> 至少有一个元素属于 F 但不属于 G 至少有一个元素属于 F 但不属于 H

这将极大地有助于最终找到我们的反例！我们已经将主张的所有必要部分提炼出来，并以更直观的方式重新表述了属性。接下来的工作只是在一些草稿纸上随意尝试，看看我们能想出什么。一种方法是绘制一个“空”的文氏图，用于 F 和 G 和 H 以及它们的潜在“重叠”，然后填入足够多的元素，以满足上述三个属性。

第一个条件要求集合 F 完全“位于” G 和 H 内；但是，第二个和第三个条件要求存在 F 的两个元素，其中一个不是 G 的元素，另一个不是 H 的元素。这就足够了！你可能说这是一个简单的例子，但我们称之为 *effective*。现在让我们跳进去，现在就写下我们的反证：

Proof. 以下声明是 False：

> For any sets F, G, H, if $F \subseteq G \cup H$, then either $F \subseteq G$ or $F \subseteq H$.

我们将用反例来证明它是错误的。

定义 $F = \{1, 2\}$ 和 $G = \{1\}$ 以及 $H = \{2\}$。

注意 $G \cup H = \{1, 2\}$。由于 $F = G \cup H$，那么当然 $F \subseteq G \cup H$。因此，该主张的假设成立。

然而，请注意 $2 \in F$ 但 $2 \notin G$。因此，$F \not\subseteq G$。

同样，请注意$1 \in F$但$1 \notin H$。因此，$F \not\subseteq H$。

因此，主张是 False。 □

一个重要的教训是以下内容：

> 旅游反例不必是最有趣或复杂的，你也不必以某种方式描述所有可能的反例。我们只需要看到一个反例，并需要看到它是如何工作的。

这就是了！这正是我们在上面的证明中所做的：我们定义了所有重要的对象（三个集合 F, G, H），然后我们指出了并描述了它们所具有的所有相关性质。我们没有让读者去检查反例是否有效；我们展示了细节。我们没有争论在宇宙的某个地方存在这样的集合；我们明确地定义了它们。

这很重要，我们期望你的反例具有与我们上面类似的证明结构。大部分工作将在幕后进行，在

证明开始，当你尝试提出你的例子时。不过，一旦你有了它，就把它写下来，就像我们做的那样。

3.9.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) $\subseteq$的定义是什么？我们如何用它来证明$A \subseteq B$？(2)两个集合相等意味着什么？(3)*double-containment*证明是什么？(4)*counterexample*是什么？(5)假设A, B, U是集合且$A, B \subseteq U$。为什么我们可以通过证明$B \subseteq \overline{A}$来证明$A \subseteq B$？尝试说服一个朋友这是有效的技术。

—

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 首先，以下主张：**prove**

> 对于任何集合 A, B, C，子集关系 $A - (B - C) \subseteq (A - B) \cup C$ 成立。

其次，找到一个 *counterexample* 来证明这些集合实际上始终是 *equal*。

(2) 假设 A, B, C 是集合且 $A \subseteq B$。证明 $A \times C \subseteq B \times C$。

(3) 假设 $A \subseteq C$ 和 $B \subseteq D$。证明 $A \times B \subseteq C \times D$。

(4) 设 $A = \{x \in \mathbb{R} \mid x^2 > 2x + 8\}$ 和 $B = \{x \in \mathbb{R} \mid x > 4\}$。对于以下每个主张，要么 *prove* 它是正确的，或者提供一个 *counterexample* 来证明它是 False。

(a) $A \subseteq B$b) $B \subseteq A$

(

(5) 设A, B, U为具有$A, B \subseteq U$的集合。证明$A - B = A \cap \overline{B}$通过一个 *double-containment argument*。

(6) 设 $S = \{x \in \mathbb{R} \mid -2 < x < 5\}$ 和 $T = \{x \in \mathbb{R} \mid -4 \leq x \leq 3\}$。在 $\mathbb{R}$ 的背景下，$S \cap \overline{T}$ 是什么？确定一个集合，然后使用双重包含论证来 *prove* 它是正确的。

(7) **Prove**以下主张：如果$A \subseteq B$，则$\mathcal{P}(A) \subseteq \mathcal{P}(B)$。

(8) 对于每个 $n \in \mathbb{N}$，令 $S_n = \left\{x \in \mathbb{R} \mid -\frac{1}{n} < x < \frac{1}{n}\right\}$。证明

$$\bigcap_{n \in \mathbb{N}} S_n = \{0\}$$

(9) 让 $I = \{x \in \mathbb{R} \mid 0 < x < 1\}$。对于每一个 $x \in I$，定义 $S_x = \{y \in \mathbb{R} \mid x < y < x + 1\}$。证明

$$\bigcup_{x \in I} S_x = \{z \in \mathbb{R} \mid 0 < z < 2\}$$

(10) 对于每个 $n \in \mathbb{N}$，通过以下方式定义集合 A_n 和 B_n：

$$A_n = \left\{x \in \mathbb{R} \mid 0 \leq x < \frac{n-1}{n}\right\}$$
$$B_n = \left\{y \in \mathbb{R} \mid -\frac{1}{n} < y < 1\right\}$$

Prove 以下集合等式通过双重包含论证得出：

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcap_{n \in \mathbb{N}} B_n$$

3.10 Summary

这是我们第一次涉足一些抽象概念和结果。我们引入了**set**的概念，通过几个例子来激发其动机。我们讨论了成为**element**和成为**subset**的关键关系，并指出区分这两者是多么重要！（记住“袋类比”可能会在这方面帮助你。）我们还讨论了一些符号，包括*set- builder*符号。随着我们继续进入更抽象的数学领域，使用正确、正式的符号将比以往任何时候都更重要，以确保我们正确地表达我们的想法。一个出现的关键思想是*power set*的概念，它代表了一个*element*和*subset*关系都起作用的地方。

讨论集合 *operations* 展示了如何组合集合并创建新的集合。所有这些操作将在本书剩余部分的工作中使用。我们还展示了这些操作可以被 *indexed*。这使得

我们使用缩写来表示几个集合的并集，只需几个定义和符号。同样，这些想法将在我们的工作中频繁出现，因此我们将展示许多与这些想法相关的练习；我们鼓励你们尝试并尽可能多地完成它们！

我们看到了一种与集合相关的证明技巧：即，**double-containment arguments**。这是数学中的一个基本证明技巧。你们将看到我们经常使用它，你们也会在其他课程和研究中发现它的身影。

一些讨论使我们能够触及抽象集合论中的一些深刻思想，尽管我们无法完全深入其中。首先，*Russell's Paradox*向我们展示了不存在“所有集合的集合”。其次，我们讨论了自然数如何可以用*sets*来形式定义。在实践中，我们不会使用这个定义，而将继续依赖我们对$\mathbb{N}$的直觉。然而，我们希望阅读这样的讨论是有趣的，并且以某种方式是有启发性的。

3.11 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的任何内容，以及可能的一些假设的数学知识。当然，我们并不期望你解决其中的**all**，但工作得越多，你将学到越多！记住，没有*doing*，你无法真正*learn*数学。动手解决一个问题。阅读几个陈述，四处走走，思考它们。尝试写一个证明，并向朋友展示，看看他们是否信服。继续练习将你的想法以清晰、精确和逻辑的方式*write*出来的能力。写完证明后，编辑它，使其更好。最重要的是，继续*doing*数学！

简答题，只需解释或陈述答案，无需严格的*proof*，已用►标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 3.11.1. ► 对于以下关于元素和子集的每个陈述，说明它是 True 还是 False。准备好向一个怀疑的朋友辩护你的选择！

在整个问题中，我们将使用以下定义：

$$
\begin{aligned}
A &= \{x \in \mathbb{Z} \mid -3 \leq x \leq 3\} \\
B &= \{y \in \mathbb{Z} \mid -5 < y < 6\} \\
C &= \left\{x \in \mathbb{R} \mid x^2 \geq 9\right\} \\
D &= \{x \in \mathbb{R} \mid x < -3\} \\
E &= \{n \in \mathbb{N} \mid n \text{ is even } \}
\end{aligned}
$$

(a) $A \subseteq B$b) $C \cap D = \varnothing$c) $4 \in E \cap B$d) $\{4\} \subseteq A \cap E$e) $10 \in C - D$f) $A \cup B \supseteq C$g) $3 \in A \cap C$h) $0 \in (A - B) \cup D$i) E

(((((((((

Problem 3.11.2. ► 设定 $m, n \in \mathbb{N}$。假设 $m \leq n$。解释为什么 $\mathcal{P}([m]) \subseteq \mathcal{P}([n])$。

Problem 3.11.3. 回顾3.9节中的问题7。我们证明了当两个集合满足$A \subseteq B$时，它们也必须满足$\mathcal{P}(A) \subseteq \mathcal{P}(B)$。也要阅读那个证明，以提醒自己细节。

现在，这个说法“反过来也成立”吗？也就是说，假设$\mathcal{P}(A) \subseteq \mathcal{P}(B)$。你能证明$A \subseteq B$也是正确的吗？或者你能找到一个反例，证明这并不成立吗？

Problem 3.11.4. 使用“集合构造表示法”重写以下句子以定义一个集合。然后，如果可能的话，**write out** 使用集合花括号列出集合的所有元素；如果不可能，解释为什么不可能并写出集合的**three**示例元素。

(a) 设 A 为所有平方小于 39 的自然数集合。

(b) 设 B 为所有是方程 $x^2 - 3x - 10 = 0$ 的根的实数集合。

(c) 设 C 为整数对的集合，其和为非负。

(d) 设 D 为实数对集合，其中第一个坐标为正，第二个坐标为负，且它们的和为正。

Problem 3.11.5. 定义以下集合：

$$A = \left\{x \in \mathbb{R} \mid x^2 - x - 12 > 0\right\}$$
$$B = \{y \in \mathbb{R} \mid -3 < y < 4\}$$

证明 $A = B$。

Problem 3.11.6. 让 X 成为你的学校的学生集合 ol.

找到一个属性 $P(x)$，使得 $A := \{x \in X \mid P(x)\}$ 是 X 和 $A \neq \varnothing$ 的真子集。

然后，确定一个属性 $Q(x)$，使得 $B := \{x \in X \mid Q(x)\}$ 是 A (的真子集，即 $B \subset A$) 和 $B \neq \varnothing$。

Problem 3.11.7. 设A、B和C是具有$A \subseteq C$和$B \subseteq C$的集合。

(a) 绘制集合 $A \cap \overline{B}$ 和 $(A \cap B)$ 的文氏图。 (b) 证明 $\overline{A \cap \overline{B}} \subseteq \overline{(A \cap B)}$。 (c) 定义特定的集合 A, B, C，使得包含关系为 *strict*，即 $A \cap \overline{B} \subset (A \cap B)$d) 定义特定的集合 A, B, C，使得 $A \cap \overline{B} = \overline{(A \cap B)}$。 (—

—

Problem 3.11.8. 设 $S = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m = n^2\}$。$S$ 与集合 $T = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2\}$ 的比较如何？如果一个是另一个的子集，请证明它。如果不是，提供例子以示之。

Problem 3.11.9. 设 (a, b) 为笛卡尔平面上的一个点，即 $(a, b) \in \mathbb{R} \times \mathbb{R}$。设 ε (希腊字母 *epsilon*) 为非负实数，即 $\varepsilon \in \mathbb{R}$ 和 $\varepsilon \geq 0$。

设 $C_{(a,b),\varepsilon}$ 为与 (a, b) “接近”的实数集合，定义如下：

$$C_{(a,b),\varepsilon} = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \sqrt{(x-a)^2 + (y-b)^2} < \varepsilon\right\}$$

1. 提出一个集合 $C_{(a}$ 的几何描述 $_{,b)_{,\varepsilon}}$。

当改变 a 和 b 时，集合会发生什么？当改变 ε 时会发生什么？ 2. $C_{(0,0),1} \cap C_{(0,0),2}$ 是什么？ 3. $C_{(0,0),1} \cup C_{(0,0),2}$ 是什么？ 4. $C_{(0,0),1} \cap C_{(2,2),1}$ 是什么？

Problem 3.11.10. 考虑以下（错误！）主张：

$$\bigcup_{n \in \mathbb{N}} \mathcal{P}([n]) = \mathcal{P}(\mathbb{N})$$

(a) 以下“证明”有什么问题？指出任何错误并解释为什么它/它们破坏了“证明”。

首先，我们将证明

$$\bigcup_{n \in \mathbb{N}} \mathcal{P}([n]) \subseteq \mathcal{P}(\mathbb{N})$$

考虑左并集上的任意元素 X .

根据索引并集的定义，我们知道存在某个 $k \in \mathbb{N}$ 使得 $X \subseteq [k]$。

自 $[k] \subseteq \mathbb{N}$ 以及 $X \subseteq [k]$，我们推断出 $X \subseteq \mathbb{N}$。

因此，$X \in \mathcal{P}(\mathbb{N})$。

其次，我们将证明“$\subseteq$”关系在另一个方向上也成立。

考虑一个任意的 $Y \subseteq \mathbb{N}$。

根据子集的定义，以及 Y 是自然数集的事实
数字，我们知道存在某个 $\ell \in \mathbb{N}$ 使得 $Y \subseteq [\ell]$。

根据索引并的定义，我们知道 $Y \in \bigcup_{n\in\mathbb{N}} \mathcal{P}([n])$。

自我们已展示了 $\subseteq$ 和 $\supseteq$，我们知道这两个集合是相等的。

(b) 通过定义一个满足集合 **explicit** 的 S 的例子来反驳这个主张

$$S \in \mathcal{P}(\mathbb{N}) \qquad \text{and} \qquad S \notin \bigcup_{n\in\mathbb{N}} \mathcal{P}([n])$$

Problem 3.11.11. 让 $A = [3] \times [4]$.（记住 $[n] = \{1, 2, 3, \ldots, n\}$。）

让 $B = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq 3x - y + 1 \leq 9\}$。

(a) **Prove**，其中 $A \subseteq B$。

(b) $A = B$ 是否为真？为什么或为什么不？**Prove** 你的主张。

Problem 3.11.12. 设 $n \in \mathbb{N}$ 为一个固定的自然数。设 $S = [n] \times [n]$。设 T 为集合

$$T = \left\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq nx + y - (n + 1) \leq n^2 - 1\right\}$$

证明 $S \subseteq T$ 但 $S \neq T$。

Problem 3.11.13. 假设 A 和 B 是集合。

(a) **Prove** 那个

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$$

(b) 提供 **explicit** 的一个 A 和 B 的例子，其中 (a) 中的包含关系是 **strict**。

Problem 3.11.14. 设 S 和 T 是元素本身也是集合的集合。假设 $S \subseteq T$。

Prove 那

$$\bigcup_{X\in S} X \subseteq \bigcup_{Y\in T} Y$$

Problem 3.11.15. 设 A, B, C, D 为集合。

(a) **Prove** 那个

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$$

(b) 提供一个 **explicit** 的 A, B, C, D 示例，其中 (a) 中的包含关系是 **strict**。

Problem 3.11.16. 设 A, B, C 为集合。证明

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

和

$$A \times (B - C) = (A \times B) - (A \times C)$$

Problem 3.11.17. 设 X, Y, Z 为集合。证明 $(X \cup Y) - Z \subseteq X \cup (Y - Z)$ 但等式 *need not* 成立。

Problem 3.11.18. 找到一个集合 S 的例子，使得 $S \in \mathcal{P}(\mathbb{N})$ 和 S 包含恰好 4 个元素。

然后，找到一个集合 T 的例子，使得 $T \subseteq \mathcal{P}(\mathbb{N})$ 和 T 包含恰好 4 个元素。

Problem 3.11.19. 找到满足以下条件的集合 R, S, T: $R \in S$ 和 $S \in T$ 和 $R \subseteq T$ 但 $R \notin T$。

Problem 3.11.20. 确定以下每个集合是什么，以及 **prove** 你的主张。

$$\bigcap_{n \in \mathbb{N}} [n] \qquad \text{and} \qquad \bigcup_{n \in \mathbb{N}} [n]$$

Problem 3.11.21. 设 $I = \{-1, 0, 1\}$。对于每个 $i \in I$，定义 $A_i = \{i - 2, i - 1, i, i + 1, i + 2\}$ 和 $B_i = \{-2i, -i, i, 2i\}$。

(a) 写出 $\bigcup_{i \in I} A_i$ 的元素。 (b) 写出 $\bigcap_{i \in I} A_i$ 的元素。 (c) 写出 $\bigcup_{i \in I} B_i$ 的元素 (d) 写出 $\bigcap_{i \in I} B_i$ 的元素

(e) 使用您上面的答案来写出 $\left(\bigcup_{i \in I} A_i\right) - \left(\bigcup_{i \in I} B_i\right)$ 的元素。

(f) 使用您上面的答案来写出 $\left(\bigcap_{i \in I} A_i\right) - \left(\bigcap_{i \in I} B_i\right)$ 的元素。

(g) 写出 $\bigcup_{i\in I}(A_i - B_i)$ 的元素。这与你在 (e) 中的答案相比如何?

(h) 写出 $\bigcap_{i\in I}(A_i - B_i)$ 的元素。这与你在 (f) 中的答案相比如何?

Problem 3.11.22. 在这个问题中，我们将“证明”负整数的存在！我们说“证明”，因为我们直到后来才能真正理解我们所做的事情，但请相信我们，这正是我们在做的事情。

由于这个目标，你不能存在任何严格小于0的整数 **assume**，因此你的代数步骤，尤其是在部分（d）中，不应涉及任何可能为负的项。

这是，如果你考虑一个像这样的方程

$$x + y = x + z$$

我们 **can** 推导出 $y = z$，通过从两边减去 x，因为 $x - x = 0$。

然而，如果我们考虑一个如下的方程式

$$x + y = z + w$$

我们 **cannot** 推断 $x - z = w - y$。或许 $y > w$，因此 $w - y$ 在我们的语境中不存在……

设 $P = \mathbb{N} \times \mathbb{N}$。通过以下方式定义集合 R:

$$R = \{((a, b), (c, d)) \in P \times P \mid a + d = b + c\}$$

(a) 找到三组不同的对 (c, d)，使得 $((1, 4), (c, d)) \in R$。

(b) 设$(a, b) \in P$。证明：$((a, b), (a, b)) \in R$。

(c) 设 $((a, b), (c, d)) \in R$。证明 $((c, d), (a, b)) \in R$，a s 也好。

(d) 假设 $((a, b), (c, d)) \in R$ 和 $((c, d), (e, f)) \in R$。同样证明 $((a, b), (e, f)) \in R$。

3.12 Lookahead

现在我们已经介绍了集合，定义了它们，看到了许多例子，并讨论了操作和如何操作集合，是时候转向逻辑了。我们已经在第3.9节中预览了一些重要的逻辑思想，特别是关于如何编写**proofs**关于集合的内容。在下一章中，我们将使所有这些逻辑思想更加正式、明确和严谨。我们将开发一些

符号和语法，帮助我们更精确、更简洁地表达逻辑思想。我们将使用这些来表达我们的数学思想，并用共同的语言与他人交流我们的想法。简而言之，我们将能够自信地谈论和写作数学！

Chapter 4

Logic: The Mathematical Language

4.1 Introduction

我们继续学习数学语言！我们将学习如何正式、精确和简洁地表达我们的想法。这需要学习一些新的术语和符号，同时以更正式的方式进行思考和写作。最终，这将使我们能够解决问题，并写出清晰、正确和优秀的数学 **proofs**。

4.1.1 Objectives

以下本引言中的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作将如何有所帮助，它们将激励我们为什么要关注本章中出现的主题，并且它们将告诉您我们的目标和在阅读过程中您应该牢记什么以实现这些目标。现在，我们将通过一系列声明为您总结本章的主要目标。以下各节将更详细地重申这些观点，但这将为您提供一份供未来参考的简要清单。当您完成本章的学习后，请回到这份清单，看看您是否理解了所有这些目标。您明白为什么我们将它们列为重要吗？您能定义我们使用的所有术语吗？您能应用我们描述的技术吗？

By the end of this chapter, you should be able to ...

- 定义变量命题，使用适当的符号。

- 定义使用量词和其他适当符号的数学陈述，并描述不是适当数学陈述的句子。
- 理解并解释两种量词之间的区别，以及它们的使用方法。
- 定义并理解几个逻辑连接词的含义，以及使用它们来定义更复杂的数学陈述。
- 应用证明技术来创建形式化的论证，以证明数学陈述的真实性。
- 比较和对比不同的证明技术类型，以及根据具体情况了解何时以及如何使用它们。

4.1.2 Segue from previous chapter

我们引入集合是为了有一些标准的、基本的数学对象来工作。你可能已经注意到，尽管如此，我们使用了大量的短语，如“如果……，那么……”和“对于$every$”和“存在$exists$”和“对于$at\ least\ one$”和“和”和“或”和True和False等等。我们依赖你对这些概念的直观理解和先验知识。作为一个活生生的、会与人交谈的人类，你对什么是**logic**有一定的理解。我们的目标现在是在这些直觉的基础上建立，帮助你学会阅读、写作和说数学。

4.1.3 Motivation

在数学中，我们感兴趣的是识别 True 声明，并随后向他人解释 how 和 why 我们知道那些声明是 True。到目前为止，我们已假定对逻辑术语和真理有所了解。例如，回顾 PMI（数学归纳原理，定理 3.8.5）的假设。我们需要知道 $if\ P(k)$ 是真实的 $then\ P(k{+}1)$ 是真实的。这意味着什么？这说明了 $P(k)$ 和 $P(k+1)$ 之间的联系是什么？甚至对某事物是 True 的意义是什么？！？！

我们的本节目标很多，但主要重点在于定义和识别哪些数学陈述是有意义和有趣的。一旦我们做到了这一点，我们就可以弄清楚如何用简洁精确的术语来表达这些陈述。最终，我们将学会如何将这些陈述应用于**prove**，这些陈述是 True (或False，具体情况而定)。

4.1.4 Goals and Warnings for the Reader

在整个章节中请记住这一点:

您正在学习一个 **language**。

一些材料可能看起来很难，一些可能看起来很无聊，一些可能两者兼具！但这都是必要的。

你曾经学过另一种语言吗？或许可以回想一下你在学校上的外语课。你是怎么开始的？我们打赌你并没有直接跳进去尝试写美丽的诗歌。你学习了基本的语法、句法和词汇。你学习了重要的冠词，比如“the”和“an”。你学习了基本动词，如“to be”和“to have”，以及如何变位。你学习了某些常见名词，如“apple”、“dog”和“friend”。从那里开始，你开始拼接短语，随着时间的推移，你学会了利用你开发的所有工具来创造更复杂的句子。一路上，你可能心里有很多关于美好句子的想法，但直到你学会了必要的单词和语法，你才知道如何用你的新语言表达它们。

我们将在本章中做完全相同的事情，但在这里我们的语言是 **mathematics**。你可能已经在脑海中想到了一些关于美妙数学句子的伟大想法，但你只是不确定如何表达它们。有趣的是，我们彼此之间已经“说”了很多数学！我们解决了一些谜题，介绍了一种证明技术（归纳），并使用了一些数学对象的构建块（集合）；一路上，我们确保我们彼此理解，用我们的写作进行冗长的描述，并解释了很多细节。从某种意义上说，我们一直在没有设定共同语言的情况下进行沟通。这就像你在一个你不知道语言的外国国家生存一样：你会用很多手势和哑剧，你会试图听别人说话并记住一些关键词，你会画画并发出声音，等等。如果你只是去度假一周，这都很好，但如果你要去 *live*，你面前还有更多的工作要做。

这正是我们现在面临的情况。我们希望居住在这个数学世界中，因此我们需要定居下来，真正学习其人民的语言。一旦我们通过了这一点，我们就会感到更加自在，就像母语人士一样。然后，我们可能对我们的词汇和语法稍微不那么小心，可以使用一些俚语或缩写或常用习语。（想想一些英语考试中的短语和句子，从技术上讲，它们在语法或词汇方面没有意义，但仍然被你的同乡所理解。）但只有那时我们才能这样做。

在此期间，我们将对我们的语言更加正式和繁琐。

If we don't force ourselves to do this now, we won't truly all speak the same mathematical language。

4.2 Mathematical Statements

我们的第一步是讨论哪些类型的句子甚至可以被认为是需要证明或反驳的数学真理。完成这一步实际上相当困难！许多作者往往对此问题一笔带过

或提供一个简单的定义，忽略数学语言和逻辑中的许多细微差别。我们也有同样的感觉，因为本书/课程提供的时间和空间不足以正确研究抽象逻辑理论领域。我们鼓励您调查一些包含相关信息书籍或网站。就当前语境而言，我们不得不将许多细节扫到地毯下，换句话说。不过，可以说，有一个非常深刻、丰富且富有成效的数学研究领域，正是我们将以更启发式的方式在这里讨论的内容。

记住我们提到我们必须假设实数 $\mathbb{R}$ 的存在及其通常的算术性质。同样，我们将假设许多数学逻辑的结果和概念，有时甚至没有意识到（直到我们指出给你）。这些细节可以在你数学生涯的后期进行更深入的研究。

4.2.1 Definition

目前，让我们讨论一下我们所说的**mathematical statement**是什么意思。我们希望这个术语能够包含我们可以证明或反驳的“事物”种类。

数学在科学中独树一帜，因为该领域的成果是**proven**严格推导出来的，而不是通过实验室实验或现实世界的观察来“证实”的假设。在数学中，我们假设一组公理**axioms**，然后通过严格的逻辑推理从这些公理（以及我们迄今为止已经证明的其他真理）中推导出真理。如果我们遇到一个错误，我们就必须证明或展示它确实是False。

考虑到这些想法，我们现在可以考虑并就几个这样的**mathematical statement**或**proposition**的例子达成一致。（我们甚至已经证明了一些！）例如，这个句子

> For any real numbers $x, y \in \mathbb{R}$, the inequality $2xy \leq x^2 + y^2$ holds.

这是一个有效的数学陈述。事实上，它是 True，我们将在第4.9.2节中证明它。（有时被称为 *AGM Inequality*，即 *Arithmetic-Geometric Mean Inequality* 的简称。）我们应该指出，在数学中，“holds”一词常用来表示“成立”或“是正确的陈述”。

这是另一个数学陈述的例子：

> 对于任何集合 S, T, U，如果 $S \cap T \subseteq U$ 则 $S \subseteq U$ 或 $T \subseteq U$。

此声明，然而，是 False，如下 **counterexample** 所示：

> Let $S = \{1, 2, 3\}$ and $T = \{2, 3, 4\}$ and $U = \{2, 3, 5\}$.
>
> Observe that $S \cap T = \{2, 3\} \subseteq U$ but $S \not\subseteq U$ and $T \not\subseteq U$.

为什么这个例子 *disprove* 这个陈述？你理解吗？你能解释一下吗？我们将在本章后面更详细地讨论这个问题，但我们将

希望现在我们都以某种方式认识到这个例子恰好实现了这一点。

我们也可以同意，一个像这样的句子

为什么我们上午9:00有课？！

这绝对是一个数学陈述。它是一个完全有效的英文句子，但从数学的角度来看，它没有意义：我们无法 *prove* 或 *disprove* 它。

同样，这个句子

$x^2 - 1 = 0$

是 *not* 一个数学陈述，尽管它完全由数学符号组成。问题是，我们不能仅从公理和逻辑推理中验证它是否是 True 或 False。这个关于 x 的陈述 *depends*，无论这个值是什么（即 x 是一个 **variable**），并且不对其施加额外的假设，我们不能宣布这个句子是 True 或 False。这种句子将在以后被称为
variable proposition：其真值取决于句子内部的变量。

所有这些观察和例子/非例子都促使以下定义：

Definition 4.2.1. *A* **mathematical statement** *(or* **proposition** *or* **logical statement***) is a grammatically correct sentence (or string of sentences), composed of English words/symbols and mathematical symbols that has* 精确地 *one truth value, either* True *or* False.

4.2.2 Examples and Non-examples

通过“语法正确”我们指的是句子中的单词和符号被正确使用和组合，并且有意义。这消除了当放在一起时无意义的符号/单词串，例如

$$1+ = 2 \quad , \quad \text{Brendan}^2 = 1 \quad , \quad \{\{\varnothing\}\} - 7 > 5\pi \quad , \quad \text{You am smart}$$

例如，上面第三个不是数学陈述，因为 $\{\{\varnothing\}\}$ 不是一个数字，所以我们不知道如何解释“从这个集合中减去7”。

通过“具有 *exactly* 一个真值”，我们是指该陈述应该是 True 或 False，但肯定不能同时是两者或都不是，或介于两者之间。这排除了上面提到的“$x^2 - 1 = 0$”的例子，因为它没有真值。（如果没有声明 x 是什么，我们也不能决定。）

Not Knowing the Truth Value

一个奇怪/有趣/复杂的方面是我们定义的是，即使我们可以确定存在这样的一个值 *only*，我们可能也不知道给定陈述的真值。为了说明这一点，考虑以下陈述：

任何大于或等于4的偶数自然数都可以写成两个质数的和。

这是陈述 True 还是 False? 如果您有证明或反证，那么数学界将非常乐意看到它！上面的陈述被称为 **Goldbach Conjecture**，它是一个非常著名的未解（目前，我们希望！）数学问题。目前尚无人知道这个主张是 True 还是 False，但可以肯定的是，那些真值中的 *only one* 是适用的。也就是说，这个陈述不能同时是 True 和 False，也不能在两者之间有所折中。要么所有大于或等于4的偶数自然数 *do* 都具有所述性质，要么至少有一个数 *not* 具有该性质。即使我们还不知道两种可能性中哪一个是正确的，我们也可以陈述这种“要么/要么”的性质。因此，这个句子 *does* 实际上满足我们对 *mathematical statement* 的定义。

（术语说明：一般来说，**conjecture** 是某人认为为真但尚未被证明/证伪的陈述。）

Paradoxical Sentences

一种让句子具有 *not* 真值的方法是创建一个 **paradox**。考虑这个句子：

这句话是 False。

非常奇怪，对吧? 这个句子本身正在断言关于其自身真值的内容。让我们尝试分析它具有什么真值：

- 假设句子是 True。然后，句子本身告诉我们它实际上是 False。
- 让我们假设句子是 False。同样地，那么，这个句子告诉我们它实际上是 True。

这不能工作！这句话同时是某种意义上的 True 和 False，或者某种意义上既不是，或者……不管是什么，这都是一个坏主意。我们并不想数学中处理这种奇怪的情况，因此我们的定义禁止这句话作为数学陈述。

(（v27）如果你允许这样的句子成为正确的数学陈述会发生什么? 如果你不坚持每个我们关心的句子必须是 True 或 False 的原则呢? 想想看！这是否以某种方式 *wrong*，或者它只是一个不同的数学宇宙? ……)

一般来说，像上面那样的 **self-referential** 句子（即指代自身的句子）相当奇特，可能会产生我们想要禁止的一些悖论。

一个上述悖论性主张的变体在一张卡通画中给出，其中皮诺曹说：“我的鼻子现在会变长！”那么它变长了吗? 如果他说的是真话，那么它就会变长，但这只在他撒谎的时候才会发生！如果

他在撒谎，然后他的鼻子就会变长（根据定义），但然后他的陈述实际上是真实的！哎呀！

来源：http://www.the-drone.com/magazine/wp-content/uploads/2010/04/BLA6.jpg

一个更奇怪的现象例子是 *Quine's Paradox*:

"当其引号之前时产生虚假"当其引号之前时产生虚假。

我们将让您自己思考这个问题。只需说，像这样的悖论性主张对我们来说太过放肆，不值得我们担心。这就是为什么我们的定义禁止它们。

4.2.3 Variable Propositions

其他不是数学陈述的句子示例包括涉及 **unquantified variables** 的句子。例如，考虑以下句子

"$x^2 - 1 = 0$"

这当然在语法上是正确的，我们可以理解它，但它的真值是什么？我们不知道！如果 $x = 1$，那么这个句子是 True，但如果 $x = 8$，它就是 False，如果 $x = \mathbb{N}$ 或 $x =$ Brendan，那么这个句子甚至没有意义！因此，我们希望禁止这种句子，尽管这些类型的句子是有用且常见的；我们将它们称为 **variable propositions**，因为它们对某个变量提出了一个断言。

在上述句子的情况下，我们可能将 $P(x)$ 定义为变量命题"$x^2 - 1 = 0$"。我们通常会这样写这个声明：

Let $P(x)$ be the statement "$x^2 - 1 = 0$".

通常使用大写字母表示变量命题和数学陈述，而使用小写字母表示其中包含的变量。（这虽然不是 *requirement*，但只是一种常见约定。）

使用这个变量命题现在已定义，我们可以通过将变量 x 表达式中的 *assigning* 特定值来创建适当的数学陈述。我们可以说 $P(1)$ 是 True，而 $P(0)$ 是 False。我们还可以对 $P(x)$ 提出 **quantified** 主张。例如，我们声称以下句子是一个 True 数学陈述：

> 存在一个 $x \in \mathbb{R}$，使得命题 $P(x)$ 是 T rue.

而以下句子是一个 False 数学陈述：

> 对于每个 $x \in \mathbb{R}$，命题 $P(x)$ 是 True。

考虑一下为什么这些陈述具有我们所声称的真值。你能看出为什么它们一开始就是数学陈述吗？你会如何 *prove* 这些主张？

Defining Variable Propositions

注意我们用来定义变量命题的格式，如上面所示：(1) 我们给命题一个字母名称（如 P）；(2) 我们表明它依赖于一些变量，每个变量都有一个字母（如 x 和 y）；(3) 我们将实际命题本身放在引号内；并且(4) 我们不包括任何在命题上下文中没有意义的新的字母。

此格式已被精心选择，因为它精确且无歧义。它为命题中的每个字母赋予意义，并清楚地区分命题的哪些部分属于命题，哪些不属于。

例如，以下是一些 **BAD** “定义” 变量命题。我们将给出一些原因说明它们为什么不好，并提供一些命题的正确修正。

- 设 $Q(y)$ 为命题 “$x < 0$”。

  Reason: 什么是 x？ y 在哪里？在命题的上下文中，我们有了 *no idea*，即 x 是什么，所以这是一个糟糕的定义。

  如果我们说过

  > 设 $Q(x)$ 为语句 “$x < 0$”。

  那本来是完美的。括号内的变量是后来在引号中的陈述中出现的那个。太棒了。

- 设 $P(x)$ 为命题 $x^2 \geq 0$，对于每个 $x \in \mathbb{R}$。

  Reason: 这句话的作者是否想要断言$x^2 \geq 0$，无论$x \in \mathbb{R}$是什么？短语“对于每一个$x \in \mathbb{R}$”是否意味着是命题的*part*，还是不是？

  如果我们解释为 $P(x)$ 被定义为“$x^2 \geq 0$”，并且这个定义适用于每个 $x \in \mathbb{R}$，那么……好吧，这可能是有道理的。

  然而，如果我们解释为 $P(x)$ 被定义为“对于每个 $x \in \mathbb{R}$，$x^2 \geq 0$”的话，那么，这无疑是 *different*。事实上，它甚至不是

一个定义良好的命题！命题 $P(x)$ 应该 *depend* 输入值 x，但不应该允许 *change* 或进一步 *quantify* 该变量 *inside* 命题！

这种方式最初表述的命题有两种可能的解释，它们非常不同。因此，这是一个糟糕的定义。

如果我们说过，

> 让 $P(x)$ 成为“$x^2 \geq 0$”的陈述，对每个 $x \in \mathbb{R}$ 定义。

那本来是可以的。正如我们在下面提到的，我们实际上不必告诉读者我们想要定义命题的 x 的哪些值。尽管如此，这可能只是包含一些有用的信息，所以这并不会造成伤害。

- 让 $T(x, y) =$ “$x^2 - 7 = y$”。

  Reason: 呃！在这个上下文中，“=”是什么意思？这个符号适用于我们想要比较两个 *numbers* 并说它们在数值上 *equal*（或者两个 *sets* 并说它们在元素方面相等）。对象 $T(x, y)$ 的目的是一个 *mathematical statement*，它要么是 True，要么是 False。因此，它没有数值可以与其他任何事物进行比较。

  同样，给定 x 和 y 的值，语句 “$x^2 - 7 = y$” 要么是 True，要么是 False，因此说该等式“等于”其他东西是没有意义的。它有一个真值，而不是数值。

  如果我们说过，

  > Let $T(x, y)$ be “$x^2 - 7 = y$”.

  那将完美无缺。

好的，现在已经有足够的 *non* 个例子了。我们真的不想在你的脑海中灌输任何坏想法！然而，根据以往的经验，我们知道这些是学生写命题的常见方式（要么是无意中，要么是没有意识到 *why* 他们是错的），所以我们觉得有必要分享。

关于变量命题的最后一点。在定义命题时，并不必要说明变量从何而来。这可以在命题被调用或特定变量的值被使用或量化时补充。也就是说，我们可以使定义

> Let $T(x, y)$ be “$x^2 - 7 = y$”.

无需指定x和y是自然数、整数、复数或类似的东西。稍后，我们可以说$T(3, 2)$是True，$T(\pi, -1)$是False，$T(\varnothing, \mathbb{N})$有*no meaning*，但在定义$T(x, y)$时，我们不需要预先猜测任何这些解释。

4.2.4 Word Order Matters!

该概念 **quantifying variables** 我们将在下一节中详细讨论。现在，我们想考虑一个更具代表性的数学陈述的例子，以说明 **word order** 在句子中的重要性。分析如下句子的结构将是下一节的主要目标，同样如此。

存在一个实数 y，使得对于每一个实数 x，都有 $y = x^3$。

这个主张说了什么？它说我们可以找到一个数 $y \in \mathbb{R}$，使得 $y = x^3$ 是 True，*no matter what* $x \in \mathbb{R}$ 是。这太荒谬了！怎么可能有一个数是 *all* 个数的立方呢？这句话确实是一个数学陈述，但它无疑是 False。但是，关于以下主张呢?

无论如何选择一个实数 x，都存在一个实数 y 使得 $y = x3.$

这是一个 True！你看到这两个句子的区别了吗？它们包含的单词和符号完全相同，但顺序不同。前者句子断言存在某个数是每个实数的立方（即 False），而后者断言每个实数都有一个立方根，即 True。这个例子强调了词序的重要性。

4.2.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 数学陈述的重要、定义性属性是什么?

(2) 数学陈述和变量命题之间的区别是什么?

(3) 为什么哥德巴赫猜想是一个数学陈述?

(4) 以下尝试定义一个变量命题有什么问题?

让 $Q(x, y, z)$ 为 $7x - 5y + z$

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 对于以下每个句子，判断它是否是**mathematical statement**。如果是，判断它是True还是False。如果不是，解释原因。

(a) $142857 \cdot 5 = 714285$(b) 对于每个 $n \in \mathbb{N}$，$\sum_{k \in [n]} k = \frac{n(n+1)}{2}$。(c) 对于任何集合 A 和 B，如果 $A \subseteq B$，那么 $B \subseteq A$。(d) 对于任何集合 A 和 B，如果 $A \subseteq B$，那么 $\mathcal{P}(A) \subseteq \mathcal{P}(B)$。(e) 数学很酷。(f) $1 + 2 = 0$(g) 对于任何 $x, y \in \mathbb{Z}$，如果 $x \cdot y$ 是偶数，那么 x 和 y 都是偶数。(h) 对于任何 $x, y \in \mathbb{Z}$，如果 x 和 y 都是偶数，那么 $x \cdot y$ 是偶数。(i) $1+ = 2$(j) $-5 + \mathbb{Z} \geq \pi$k) $x = 7$(l) 这句话不是True。 (

(2) 回顾前三章，并识别一些数学命题的例子和非例子。

您也能找到任何变量命题吗？它们是否按照本节中指定的方式书写？您能修改它们，使它们正确书写吗？

(3) 正确定义一个当两个输入值具有非负和时为真的变量命题。

然后，找到命题为 True 和命题为 False 的两个实例。

(4) 设 S 为集合 $\{1, 2, 3, 6, 8, 10\}$。

(a) 编写一个适当的变量命题定义，该命题输入两个变量并判断它们差的绝对值是否是S的元素。然后，找出命题为True和False的两个实例。 (b) 编写一个适当的变量命题定义，该命题输入两个集合并确定它们的交集是否是S的子集。然后，找出命题为True和False的两个实例。

（注意：对于任意集合 X 和任意对象 x，必须满足 $x \in X$ 或 $x \notin X$。）

(5) 想出一个数学陈述，它是 True，但在我们改变一些词的顺序时变为 False。(参见最后一小节中的示例以获得一些灵感。)

(6) 对于以下定义变量命题的尝试，确定其是否正确。注意：这并不意味着确定它是 True 还是 False；相反，我们想知道该陈述是否写得很好且合乎逻辑。

如果尝试因某些原因不正确，请解释该原因并写出一个新的语句以修复该错误。

(a) 令 $P(x)$ 为 “$x > 1$”。(b) 令 $Q(x)$ 为命题 “$x^2 - 1 > 0$”。(c) 令 $R(a, b)$ 为 “$a^3 = b$”，对于每个 $a, b \in \mathbb{R}$。(d) 令 $P(x)$ 为 $x > 1$。(e) 令 $T(z) =$ 为 “z 是素数”。(f) 令 $Q(x)$ 为命题 “$x^2 - 1 > 0$”，对于每个 $x \in \mathbb{R}$。(g) 对于每个 $x \in \mathbb{R}$，令 $Q(x)$ 为 “$x^2 - 1 > 0$”。(h) 令 $S(a)$ 为 “$b^2 > 4$”。(i) 令 $Q(x)$ 为 $x^2 - 1 > 0$，对于每个 $x \in \mathbb{R}$。

4.3 Quantifiers: Existential and Universal

我们现在将介绍一些方便的符号，这些符号允许我们缩短迄今为止看到的一些陈述，并用数学符号表达冗长、基于语言的表达式。即将到来的符号的另一个好处是我们将能够更容易地表达和分析数学陈述。具体来说，我们现在将介绍符号 “∀” 和 “∃”。

Definition 4.3.1. *The symbol “∀ ” stands for the phrase “**for all**”.*

*The symbol “∃ ” stands for the phrase “**there exists**”.*

We call “∀ ” the 全称量词 *and “∃ ” the* 存在量词*.*

A mathematical statement beginning with “∀ ” is said to be “universally quantified”, and one beginning with “∃ ” is said to be “existentially quantified”.

4.3.1 Usage and notation

其他常见的 “∀” 所替代的短语包括 “对于每一个” 和 “对于任意的” 或 “每当” 和 “给定任何”，甚至 “如果”。

其他常见的 “∃” 所替代的短语包括 “对于某些” 和 “至少有一个” 和 “有” 甚至 “一些”。

Example 4.3.2. 首先让我们考虑一些简单的例子，以便我们熟悉。在每种情况下，我们试图用这些符号表达一个数学思想，或者尝试以更“冗长”的方式解释一个量化陈述。

- 每个实数的平方都是非负的。

  这是一个简单的陈述，实际上就是 True。我们会写成：

  $$\forall x \in \mathbb{R}\,.\; x^2 \geq 0$$

  “大点”将陈述的量化部分与关于变量 x (的断言分开，该变量是在量化) 中引入的。

  另一种写法可以是：

- “定义 $S(x)$ 为 “$x^2 \geq 0$”。然后，主张是：$\forall x \in \mathbb{R}$。 $S(x)$.
- “$\mathbb{N}$ 的一个子集包含元素 7。”

  这是一个 *existence* 主张。它声称我们可以找到一个具有特定属性的对象。我们会将其写成：

  $$\exists S \in \mathcal{P}(\mathbb{N})\,.\; 7 \in S$$

  记住，$\mathcal{P}(\mathbb{N})$ 是 *power set* 的 $\mathbb{N}$，即 $\mathbb{N}$ 的所有子集的集合；因此，说 $S \in \mathcal{P}(\mathbb{N})$ 意味着 $S \subseteq \mathbb{N}$，正如所愿。

- 每个整数都有一个 *additive inverse* (，即一个数，当它加到原始数上时，得到 0)。

  这个“加法逆元”的概念是一个通用概念，适用于一些称为 *rings* 和 *fields* 的数学对象。在这本书中，我们不会讨论这些对象，但在任何抽象代数课程中你都会接触到它们。

  我们将会把这个说法写成

  $$\forall a \in \mathbb{Z}\,.\; \exists b \in \mathbb{Z}\,.\; a + b = 0$$

  并且我们会大声朗读为

  > 对于任何整数 a，存在一个整数 b 使得 $a + b = 0$。

  或者也许

  > 无论给定的整数 a 是什么，我们总能找到一个整数 b，使得 $a + b = 0$。

  再次，我们可以通过定义 $I(a, b)$ 为 “$a + b = 0$” 来稍微缩短符号，然后将声明写为

  $$\forall a \in \mathbb{Z}\,.\; \exists b \in \mathbb{Z}\,.\; I(a, b)$$

Example 4.3.3. 这里是一些正确使用“∀”的例子，以及如何使用此符号的一些等效表达方式。

- $\forall x \in \mathbb{R}\text{.}\ x^{\wedge 2} \geq 0$
- 对于所有实数 x，我们有 $x^2 \geq 0$。
- 每个实数 x 满足 $x^2 \geq 0$。
- 无论 x 是实数，我们知道 $x^2 \geq 0$。

同样，这里有一些符号“∃”的正确使用和等效表达的例子。

- $\exists x \in \mathbb{R}\text{.}\ x^{\wedge 2} - 4x + 4 = 0$
- 存在一个实数 x，使得 $x^2 - 4x + 4 = 0$。
- 存在一个实数 x 满足 $x^2 - 4x + 4 = 0$。
- 某些实数 x 具有性质 taht $x^2 - 4x + 4 = 0$。

Reading Quantified Statements Aloud

Example 4.3.4. 现在，让我们看看一些更难的例子。让我们回顾一下上一节末尾我们写的短语，并使用这种新符号来表示它们。考虑以下陈述:

存在一个实数 y，使得对于每一个实数 x，都有 $y = x^3$。

为了用符号形式表达thi，我们将定义$P(x, y)$为命题“$y = x^3$”，然后写出该陈述为

$$\exists y \in \mathbb{R}\text{.}\ \forall x \in \mathbb{R}\text{.}\ P(x, y)$$

这是正确的，从逻辑上讲，但它相当简洁。目前，我们有时会使用一些“辅助词”来改写这个陈述，以帮助我们阅读这个陈述。特别是，当我们大声朗读句子时，我们会说这些词，所以通过偶尔在这里写下来，我们为您提供了一些额外的练习，以口头解释逻辑符号。我们会大声朗读上述陈述为

存在一个实数 y，使得对于每一个实数 x，命题 $P(x, y)$ 成立。

短语“*such that*”是一个“辅助短语”，它将存在量词与短语的其他部分联系起来。下一个小节包含有关何时以及如何使用此辅助短语的一些重要信息!

“大圆点”在上述陈述的量化部分之间仅用于分隔陈述的各个部分，使其更容易阅读。它对应于说话时的停顿或休息，就像逗号一样，但有时它具有发声的意义（就像“$\exists y \in \mathbb{R}$”部分之后的“such that”）。

我们不希望使用逗号，因为我们已经用它们表示其他含义。例如，我们写

$$x, y \in S$$

表示“x 和 y 都是集合 S 的元素”。“大圆点”只是一个不同的符号。

由于我们的数学生涯相对较年轻，我们鼓励你在可能的情况下，有时写上“使得”和“满足 True”等辅助性短语来引导你的理解。这会让你记住句子的含义，并帮助你练习以这种浓缩形式阅读和书写此类陈述。记住，你在这里学习的是一个 *language*，你需要练习将你已知的一种语言（英语）的句子翻译成另一种语言（数学）的句子。例如，你可能想要将上面的行写成

$$\exists y \in \mathbb{R} \text{ such that } \forall x \in \mathbb{R}\text{.}\ P(x, y) \text{ is True.}$$

至少，这样在心里说。

（顺便说一下，在白板或纸上书写时，通常用“s.t.”代替“such that”，以节省一点书写时间。这正好说明了“such that”这个短语在数学写作中的普遍性；我们已经有了一个为其约定的缩写！）

4.3.2 The phrase “such that”, and the order of quantifiers

注意，帮助短语“such that”始终跟在*existential*全称量化之后，以及*only*这样的量化之后。这是因为带有“∃”的陈述断言关于具有某种属性的对象的存在，而句子的其余部分是对该特殊属性的描述。因此，“such that”是有意义的，并帮助我们正确地阅读句子。考虑这个数学陈述：

$$\exists y \in \mathbb{R}\text{.}\ \forall x \in \mathbb{R}\text{.}\ P(x, y)$$

如果我们大声朗读，但将“such that”短语放错位置，并在“∀”之后而不是“∃”之后使用它，那么就会得到这个句子：

$$\exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \text{ 使得 } P(x, y) \text{ 是 True.}$$

我们声称这可以有两种解释，其中*neither*才是真正的正确意图，这就是为什么我们用红色写出来的原因！

一方面，有人可能会争辩说，这样的句子在语法上根本不成立，也没有意义，因为“such that”不应该跟在*universal*量化词之后。这相当于只是举手投降，说：“我不知道你那里是什么意思！”

另一方面，有人可能会仔细阅读这个句子，并认为作者真正想要表达的是

$$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, \text{以便 } P(x, y) \text{ 是 True。}$$

或者，写出单词，

存在一个 $x \in \mathbb{R}$，对于每个 $y \in \mathbb{R}$，都存在一个 $P(x,y)$ 使得 $P(x,y)$ 是 True。

这里，逗号表示短语顺序的 *inversion*，这在英语语言中很常见。（例如，考虑以下句子：“我笑，对 *30 Rock* 的每一集，都全心全意。” 这与说“我对 *30 Rock* 的每一集都全心全意地笑”是相同的。）因此，这个句子相当于写成

$$\forall x \in \mathbb{R}\text{.}\ \exists y \in \mathbb{R} \text{ such that } P(x,y) \text{ is True.}$$

这是 *not* 与我们考虑的原始数学陈述相同，实际上，这正是我们在上一节中看到的 *other* 陈述（见第4.2.4节），它竟然是 False！回想一下，另一个陈述是相似的，但短语顺序是相反的：

存在一个实数 x，使得对于每一个实数 y，我们有 $y = x^3$。

我们可以表示为

$$\exists x \in \mathbb{R}\text{.}\ \forall y \in \mathbb{R}\ \ \textbf{S}\text{uch that } P(x,y) \text{ is true}$$

看看那个！短语“such that”的位置错误导致了对句子的合理语言解释，其意义与原本意图正好相反。哎呀！这就是为什么我们必须小心使用“such that” *always and only* 在 **existential quantification** 之后。记住，我们并不总是写那个辅助短语，所以当你自己在心里或大声对别人读句子时，你必须记得正确地使用它，以确保你得到正确的、意图上的解释。

这个例子在前一节中的目的是指出*word order*的重要性。现在我们有了符号来替换一些单词和短语，我们还想强调这些符号的顺序也同样重要。上面我们看到的两个数学陈述包含完全相同的单词和符号，但顺序不同，一个是False而另一个是True。显然，顺序非常重要！

4.3.3 “Fixed” Variables and Dependence

当我们在讨论量词顺序时，我们还将提及以下示例，以强调量词的顺序决定了何时将变量视为表达式中的 **fixed**。

考虑以下陈述：“任何大于或等于4的偶数自然数都可以写成两个质数的和。”（回想一下，这是我们之前章节中讨论的著名的**Goldbach Conjecture**。）为了表达这个

逻辑和符号地陈述，我们会写成

设 X 为除了 2. 以外的偶数自然数集合，设 P 为质数集合。定义 $Q(n,a,b)$ 为“ $a+b$ 。那么，断言是：

请注意，这里我们使用了一些缩写。短语“$\exists a, b \in P$”实际上意味着“存在某个$a \in P$并且存在某个$b \in P$”。将上述陈述表达为

$$\forall n \in X \text{ . } \exists a, b \in P \text{ . } Q(n,a,b)$$

$$\forall n \in X \text{ . } \exists a \in P \text{ . } \exists b \in P \text{ . } Q(n,a,b)$$

当两个变量被量化为来自同一集合的元素时，尽管如此，如果量化在句子中紧接着发生，将它们合并成一个量化是非常常见的。我们甚至可能会看到如下数学陈述，

$$\forall x, y \in \mathbb{Z} \text{ . } \exists a, b, c, d \in \mathbb{Z} \text{ . } a+b+c+d = x+y \text{ and } a+b \neq x \text{ and } c+d \neq y$$

(这个陈述到底在断言什么？它是 True 还是 False？它是否取决于 $\mathbb{Z}$ 的上下文？如果我们在这两个地方都使用 $\mathbb{N}$ 或 $\mathbb{R}$ 呢？)

Quantification “Fixes” a Variable

回顾上面的例子，其中我们定义了 $Q(n,a,b)$。我们提出那个例子的原因是为了提到初始量化“$\forall n \in X$”用于指定一个特定的 n 值，该值将用于整个语句的其余部分。之后，断言“$\exists a, b \in P$”及其随后的属性 $Q(n,a,b)$ 依赖于那个 *fixed, but arbitrary,* 值的 n。

整个陈述是说，无论选择什么n，我们都可以找到满足性质Q的值a, b。（当然，那些a, b的值可能会*depend*在n上。）然而，量词的*order*告诉我们，那些值a, b可能会*depend*在所选的n上。这正是我们想要强调的。

作为一个例子，考虑语句中变量 n 的一个特定值。我们知道 $8 \in X$，因为 8 是偶数，$8 \geq 4$。当 $n = 8$ 时会发生什么？你能找到一个 $a, b \in P$ 使得 $a + b = 8$ 吗？当然，我们可以使用 $a = 3$ 和 $b = 5$。好吧，当 $n = 14$ 时呢？你能找到一个满足 $a + b = 14$ 的 $a, b \in P$ 吗？当然，你现在必须选择比之前更多的 *different*。这就是我们说 a 和 b *depend* 在 n 上的意思。（顺便问一下，*can* 你在这个情况下找到了 a 和 b 吗，其中 $n = 14$？我们可以想到几个可行的选择！）

为确保您理解这次讨论，请思考以下问题并回答：上述陈述与以下陈述之间的区别是什么？

$$\exists n \in X \text{ . } \exists a, b \in P \text{ . } Q(n,a,b)$$

这是陈述 True 还是 False？为什么？

4.3.4 Specifying a quantification set

另一个我们想要强调的量词方面是，每次使用量词时都必须指定一个 *set*。这个句子

$$\forall x\,.\; x^2 \geq 0$$

可能看起来是真的，但实际上是 **meaningless**。x 是什么？它从哪里来？“对于每一个 x …” 从哪里来？如果 x 不是一个数字怎么办？

我们 *need* 指定对象 x “来自何处”，以便我们知道 $x^2 \geq 0$ 是否是一个定义良好、语法正确的短语，更不用说它是否是 True。如果我们修改句子为说

$$\forall x \in \mathbb{R}\,.\; x^2 \geq 0$$

然后这是一个定义良好、语法正确的（以及 True！）数学陈述。然而，如果我们修改句子为说

$$\forall x \in \mathbb{C}\,.\; x^2 \geq 0$$

然后这是一个定义良好但 False 的数学陈述！这是因为 $i \in \mathbb{C}$ 但 $i^2 = -1 < 0$。（记住，在这本书中，我们不会显著使用复数集 $\mathbb{C}$，但它提供了有趣且富有启发性的例子，就像这个一样。）

主要教训是 **context** 真的很重要。它可以改变一个陈述的意义，以及其真值。因此，我们必须始终确保指定一个从中抽取变量值的集合。

One Exception

我们羞愧地承认，这个“始终指定一个量化集”规则有一个例外，但这个例外有很好的理由。考虑以下主张：

> For any sets A, B, C, the equality $(A \cup B) \cap C = (A \cap C) \cup (A \cap B)$ holds true.

这是一个 True 数学陈述。（你能证明它吗？尝试使用双重包含论证！）

我们如何尝试用符号形式写出这个陈述？这是一个 *universal* 范畴（“对于任何……”），因此我们需要使用一个“$\forall$”符号。这里的变量（由 A、B 和 C 表示）是 *sets*。它们从哪里来？我们会从哪个对象集合中抽取它们？

我们相当确信你可能会说“所有集合的集合”。对吧？但这确实是个大问题！还记得我们在上一章中关于罗素悖论的讨论吗？（参见3.3.5节以提醒自己。）那个对象——所有可能的集合的集合——是*not*，它本身也是一个集合！因此，我们无法将这个陈述以符号形式写成

$$\forall A, B, C \in \_\_\_\,.\; (A \cup B) \cap C = (A \cap C) \cup (A \cap B)$$

因为我们不知道如何用 se 填空 t.

由于这个问题，我们将继续使用“对于任何集合 A, B, C ...”之类的短语，而不是符号形式。在您自己做笔记或在大白纸上解决问题时，请随意写“$\forall A, B, C$”，并知道它实际上代表集合的量化。然而，在更正式的写作中（比如书面作业），您应该坚持使用上述短语。

4.3.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) $\forall$ 和 $\exists$ 之间的区别是什么?

(2) 你会如何大声朗读以下陈述?

$$\forall x \in \mathbb{R}\text{.}\ \exists y \in \mathbb{R}\text{.}\ x = y^3$$

(3) 为什么以下句子 **not** 是一个正确的数学陈述?

$$\exists y\text{.}\ y + 3 > 10$$

以下两个陈述之间有什么区别，如果有区别的话?

$$\exists x \in \mathbb{N}\text{.}\ \exists y \in \mathbb{N}\text{.}\ x + y = 5$$

$$\exists x, y \in \mathbb{N}\text{.}\ x + y = 5$$

他们是不是 True 或 False?

(4) 如果有任何区别，以下两个陈述之间的区别是什么?

$$\exists a, b \in \mathbb{Z}\text{.}\ a \cdot b = -3$$

$$\exists \heartsuit, \diamondsuit \in \mathbb{Z}\text{.}\ \heartsuit \cdot \diamondsuit = -3$$

他们是不是 True 或 False?

(5) 为什么以下句子 not 是适当的量化陈述?

- $\exists x\text{.}\ x > 7$
- $\forall y \in \mathbb{Z}$
- $\forall z > 2.$
- $\forall w \in \mathbb{Z}\text{.}\ z^{\frac{2}{w}} > 4 = t\text{.}\ \exists t \in \mathbb{N}$

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 回顾第4.3.3节，我们在那里用符号表示了哥德巴赫猜想。我们定义X为所有除了2之外的偶自然数集合。使用符号、量词和集合构造表示法（也许根据你的方法，还需要集合运算）来定义X。

(2) 编写一个以量词开头的数学陈述示例，使得当该量词为“$\exists$”时，该陈述为True，而当该量词为“$\forall$”时，该陈述为False。

(3) 编写一个变量命题 $P(x)$ 的例子，使得

$$\forall x \in \mathbb{Z}\bullet\ P(x)$$

是 True 但

$$\forall x \in \mathbb{N}\bullet\ P(x)$$

是 False。

(4) 对于以下每个数学陈述，使用量词将其写成符号形式。（首先确保正确定义你可能需要的任何变量命题！）然后，确定该陈述是 True 还是 False。

(a) 存在一个实数，它严格大于每一个整数。 (b) 每个整数都具有其平方小于或等于其立方的性质。 (c) 每个自然数的平方根都是一个实数。 (d) $\mathbb{N}$的每一个子集都包含数字3作为元素。

(5) 对于以下每个量化陈述，大声朗读其符号表示。然后，确定该陈述是 True 还是 False。

(a) $\forall x \in \mathbb{N}\ \exists y \in \mathbb{Z}\ x + y < 0$ (b) $\exists x \in \mathbb{N}\ \forall y \in \mathbb{Z}\ x + y < 0$

(c) $\exists A \in \mathcal{P}(\mathbb{Z})\ \mathbb{N} \subset A \subset \mathbb{Z}$

(Recall that $\subset$ means “is a *proper* subset of”.)

(d) Let P be the set of prime numbers. $\exists t \in \mathbb{Z}\ \forall x \in P\ x = 2t + 1$

(e) $\forall a \in \mathbb{N}\ \exists b \in \mathbb{Z}\ \forall c \in \mathbb{N}\ a + b < c$ (f) $\exists b \in \mathbb{Z}\ \forall a, c \in \mathbb{N}\ a + b < c$

4.4 Logical Negation of Quantified Statements

让我们回到我们之前用过的那些示例语句。定义 $P(x, y)$ 为 “$y = x^3$”，然后定义 Q_1 为以下语句

$$\text{“}\exists y \in \mathbb{R}\text{.}\ \forall x \in \mathbb{R}\text{.}\ P(x, y)\text{”}$$

并且 Q_2 为

$$\text{“}\forall x \in \mathbb{R}\text{.}\ \exists y \in \mathbb{R}\text{.}\ P(x, y)\text{”}$$

记住，Q_1 是 False，Q_2 是 True。

我们如何知道 *know* Q_1 是 False? 它说存在某个具有特定性质的实数。为了声明整个陈述为 False，我们可能需要验证该性质是否对 *every* 个实数 y 成立，但这将花费很长时间！集合 $\mathbb{R}$ 是无限大的！一个更有效的方法是证明这个陈述的 **negation** 是 True。

通过“否定”，我们指的是 **logical negation**，即原陈述在逻辑意义上的“对立”陈述。数学陈述的逻辑否定与原陈述具有完全相反的真值，因此如果我们考察 Q_1 的否定并证明它是 True，那么我们就已经证明了 Q_1 本身是 False。

我们如何否定这个陈述呢? 当我们注意到我们必须以某种方式证明关于 *every* 实数 y 的某些内容时，我们已经有了正确的想法，因为原始陈述提出了 *existence* 的主张。在本节中，我们将探讨如何正确地否定这类陈述。

我们应该注意，在我们迄今为止讨论的内容中，有一些微妙而深刻的数学概念。为什么一个数学陈述要么是 True 要么是 False 呢? 嗯，一个俏皮（而且完全正确，请注意）的回答可能是，“因为你把‘**mathematical statement**’定义为那样，傻瓜！”是的，我们确实是这样做的，但 *why* 我们真的这样做了吗? True/False 的对偶性有什么是某种方式对数学或 *helpful* 有所贡献的，或者 *essential*? 这些问题是有意义的且困难的，绝对值得思考。对这些主题的讨论必然要深入到数学和人类思想的哲学中，这无疑是令人感兴趣且值得追求的，但超出了这本书/课程的范畴和目标。我们将依靠我们对真理的普遍、直观的理解。

4.4.1 Negation of a universal quantification

一般来说，全称（即“∀”）命题的否定是存在（即“∃”），反之亦然。在我们解决否定任何量化命题的更大问题之前，让我们先看看一个简单的情况。

假设 S 是一个集合，$R(x)$ 是一个定义在每个 $x \in S$ 上的数学陈述。该陈述

$$\forall x \in S\text{.}\ R(x)$$

断言一个变量命题的真值，对于变量 x 在集合 S 中的 *every* 个可能值。它说集合 S 中的元素 x 是 *no matter what*。

正在引用的，我们可以 {v*} 得出命题 $R(x)$ 是正确的。现在，这个陈述是如何 False 的，我们如何 *prove* 呢?

如果每个元素 $x \in S$ 都满足某个特定属性，那么必须是有 *at least one* 元素满足该属性。为了证明这一点，我们预计会产生这样的值；我们必须定义（即识别）一个元素 x 并解释为什么 $R(x)$ 对该特定元素不成立。（想想我们如何从语言学的角度理解这种否定。我们在日常语言中经常这样做，甚至都不需要思考。）因此，结论是，原始陈述的否定是

$$\exists x \in S \text{ such that } R(x) \text{ is False}$$

我们现在引入符号 $\neg$ 来表示 **"logical negation"** 或 **"not"**。有了这个，我们可以重新写否定陈述

$$\neg\big(\,\forall x \in S\,.\; R(x)\,\big)$$

作为

$$\exists x \in S\,.\; \neg R(x)$$

该陈述的结尾短语 $\neg R(x)$ 可以简化，具体取决于 $R(x)$ 是什么。

例如，如果 $S = \mathbb{R}$ 和 $R(x)$ 是 "$x^2 \geq 0$"，那么否定陈述将读作

$$\text{"}\exists x \in \mathbb{R} \text{ such that } x^2 < 0\text{"}$$

由于"$x^2 < 0$"与"$\neg(x^2 \geq 0)$"在逻辑上是等价的。

通常，尽管如此，我们必须将其留为"$\neg R(x)$"，而不了解关于命题R的任何更多信息。我们还将指出，通常，短语"$R(x)$是False"和"$\neg R(x)$是True"在逻辑上是等价的；它们都断言命题$R(x)$不真实。

我们现在正在发展的这个概念就是指一个 *counterexam- ple*，一个你可能之前听过的术语。要将一个全称量化命题转化为一个存在量化命题，我们必须证明一个存在量化命题；这个证明涉及到明确定义一个满足特定性质的集合元素，因此有了"**counterexample**"这个词。

4.4.2 Negation of an existential quantification

一个类似于 **朗**声

$$\exists x \in S\,.\; R(x)$$

它提出了一个存在主张。它说必须存在某个元素 x 满足属性 $R(x)$。为了反驳这样的主张，我们会试图证明 *any* 的 x 实际上 *fails* 满足属性 R。因此，我们可以这样说，该陈述

$$\neg\big(\,\exists x \in S\,.\; R(x)\,\big)$$

与以下陈述逻辑等价

$$\forall x \in S\,.\,\neg R(x)$$

这有道理，如果我们考虑如何反驳这样的存在性主张。假设你正在和一个告诉你某个kwyjibo具有是zooqa属性的朋友进行辩论。你会如何反驳他/她？你可能会说："不！给我看任何你想要的kwyjibo。我知道它不可能是一个zooqa，因为以下原因……"，然后你会解释为什么这个属性失败，无论是什么。

现在，当你说"给我任何"时，你实际上是在进行全称量化！你是在说，无论你考虑哪个kwyjibo，某件事是真实的；也就是说，对于某个kwyjibo，或者对于某个K是所有kwyjibo的集合)，某件事是True。

考虑这一点，并思考我们发现的/定义的逻辑否定为什么对你有意义。在章节的后面，当我们考虑证明技术时，我们将解释考虑一个 *arbitrary* kwyjibo 的策略，以及为什么这实际上证明了我们刚才写出的逻辑否定。目前，我们希望这很清楚，

$$\forall x \in S\,.\,\neg R(x)$$

和

$$\exists x \in S\,.\,R(x)$$

具有相反的真值。

4.4.3 Negation of general quantified statements

我们迄今为止所观察到的结果激发了一种否定量化陈述的一般程序。我们上面定义的陈述 A 是以下形式

$$\exists y \in \mathbb{R}\,.\,C(y)$$

在 $C(y)$ 是语句的其余部分（其中 *depends* 关于 y 的值，当然）。我们将 $C(y)$ 视为量化变量 y 的某些 *property*；该属性可能包含其他量词和变量，但在根本层面上，它只是断言关于 y 的某些真相。

要否定这个陈述，我们遵循上述讨论的方法并写出

$$\forall y \in \mathbb{R}\,.\,\neg C(y)$$

现在，我们知道 $C(y)$ 是一个全称量化陈述本身：

$$\forall x \in \mathbb{R}\,.\,y = x^3$$

我们也知道如何否定那种陈述！这个否定，$\neg C(y)$，是

$$\exists x \in \mathbb{R}\,.\,y \neq x^3$$

此步骤仅使用我们上面看到的另一个否定过程。然后，将所有这些放在一起，我们可以说 $\neg A$ 是一个陈述

$$\forall y \in \mathbb{R}\,.\,\exists x \in \mathbb{R}\,.\, y \neq x^3$$

这个主张我们可以 *prove* 为真，从而表明原始陈述必须是 False。

(我们将这个证明留作练习。*Hint:* 对于任意的 $y \in \mathbb{R}$，定义一个 x 的值，使得 $y \neq x^3$ 成立。注意，你的选择将取决于 x 的值；它是如何的？)

看看这个否定是如何产生的：我们认识到原始陈述是一个序列 **nested quantifiers** (，即一串连续的量化变量)，最后有一个变量命题，我们注意到我们可以将量化序列的一部分视为其自身的陈述。然后我们将“否定”从外部量化器传递到内部量化器，并将这些否定拼接在一起。

根据这个同样的想法，我们可以找出如何识别一个具有更长量词序列的陈述。例如，看看以下这样的陈述：

$$\forall a \in A\,.\,\exists b \in B\,.\,\exists c \in C\,.\,\forall d, e \in D\,.\, Q(a, b, c, d, e)$$

要开始否定它，我们会断开第一个量化词，并将剩余部分视为它自己的命题，$R(a)$，它只依赖于a：

$$\forall a \in A\,.\,\Big(\underbrace{\exists b \in B\,.\,\exists c \in C\,.\,\forall d, e \in D\,.\, Q(a, b, c, d, e)}_{R(a)}\Big)$$

因此，否定可以写成

$$\exists a \in A\,.\,\neg R(a)$$

但是，我们那时就必须想出另一种方法来写 $\neg R(a)$。但是嘿，我们只是会做同样的事情！我们只是将“$\exists b \in B$”与其他部分分开，... 你知道这会走向何方。试着自己找出步骤，并确保你得到以下作为原始陈述的逻辑否定：

$$\exists a \in A\,.\,\forall b \in B\,.\,\forall c \in C\,.\,\exists d, e \in D\,.\,\neg Q(a, b, c, d, e)$$

一般来说，我们可以这样说：要否定由量词和变量命题组成的陈述 *only*，只需将每个“$\forall$”切换为“$\exists$”，反之亦然，并否定命题。不要改变我们量化的任何集合，只是量词本身以及随之而来的命题；改变论域的宇宙是没有意义的。稍后，我们将探讨如何否定其他类型的陈述，更复杂的陈述是由其他连接词构建的。在我们这样做之前，我们需要继续前进，定义和讨论那些其他连接词。

4.4.4 Method Summary

让我们总结一下本节中我们所发现的内容 .

- **Negating a universal quantification:**
  设 X 为一个集合，设 $P(x)$ 为一个命题。那么，像这样的全称量词的否定，

  $$\neg\big(\forall x \in X\,.\,P(x)\big)$$

  是写成

  $$\exists x \in X\,.\,\neg P(x)$$

  在文字上，我们已表明说

  > It is *not* the case that, for every $x \in X$, $P(x)$ holds.

  等同于说

  > There exists an element $x \in X$ such that $P(x)$ fails.

- **Negating an existential quantification:**
  设 X 为一个集合，设 $Q(x)$ 为一个命题。那么，存在量词的否定，如下所示，

  $$\neg\big(\exists x \in X\,.\,Q(x)\big)$$

  是写成

  $$\forall x \in X\,.\,\neg Q(x)$$

  在文字上，我们已表明说

  > 这是 *not* 的情况，存在一个 $x \in X$ 使得 $Q(x)$ 成立。

  等同于说

  > 对于每个元素 {v*}，{v*} 失败。

Don't Change the Quantification Set!

我们上面提到，在否定一个陈述时改变论域是没有意义的。为了思考为什么这样做是有意义的，可以举一个现实生活中的例子。

假设我们说“这个书架上的每本书都是用英语写的。”你将如何向我们证明我们在撒谎，我们的陈述实际上是 False？你必须出示一本 *on this shelf* 用不同语言写的书。你不能把走廊那边的法国小说带来，说：“看，你错了！”这并不能证明我们提出的任何主张；话语领域是不同的，我们没有做出任何主张

关于其他房间书架上的任何情况。我们只对这个 *particular* 书架有所断言。

由于相同的原因，当否定一个类似如下的陈述时

$$\forall b \in T \,.\, P(b)$$

我们获得

$$\exists b \in T \,.\, \neg P(b)$$

在不变的那个话语领域内，集合 T。原始主张仅断言关于 T 的元素，因此其否定也只是那样，同样。

4.4.5 The Law of the Excluded Middle

你知道什么？让我们实际上讨论 *why* 我们可以讨论一个陈述及其 **logical negation**。在我们的 **mathematical/logical** 定义中内置了 **statement** 的想法，即这样的句子必须恰好有一个真值，要么 True 要么 False。为什么我们可以这样做？嗯，这里我们负责定义！数学家必须设定他们系统的基础规则——**axioms**——我们希望我们的逻辑系统确保我们提出的每一个主张都是明确地 True 或 False，而不是两者都是，也不是两者都不是。

这种二分法确实是我们的系统的一个**axiom**。它在大多数数学中得到了广泛应用，并且因其**The Law of the Excluded Middle**而闻名。这个名字来源于这个非常想法，即每个主张都是True或False，因此在这两个立场之间没有 *middle ground*；那个中间被排除了。

本质上，这使得我们在数学中所做的工作富有成效：每个命题都有一个真值，我们的目标是找到那个真值。有时，尽管如此，我们不得不退回到这个公理，这个我们同意的法律，并且仅仅 *guarantee* 某个命题是 True 或 False，而不了解 *which* 真实值实际上适用。我们在这里提供了一个有趣且引人注目的例子来说明这个想法。

Proposition 4.4.1. *There exist real numbers a and b that are both irrational such that a^b is rational.*

(记住，一个 **rational number** 是可以表示为整数分数的数，而一个 **irrational number** 是一个有理的实数。你能想到一些有理数和无理数的例子吗？)

Proof. 我们知道 $\sqrt{}\wedge 2$ 是无理数。（问题：为什么？你能证明这一点吗？现在试试。我们很快就会证明这一点！）

$\sqrt{}^{2^{\sqrt{2}}}$ 是有理数或无理数。（这里使用了排中律。）让我们分别考虑这两种情况。

- 假设数字 $\sqrt{2}^{\sqrt{2}}$ 确实是有理数。那么 $a = \sqrt{2}$ 和 $b = \sqrt{2}$ 就是我们要找的例子，因为 a 和 b 都是无理数，而 a^b 是有理数。

- 现在，假设数字 $\sqrt{2}^{\sqrt{2}}$ 是无理数。在这种情况下，我们可以使用 $a = \sqrt{2}^{\sqrt{2}}$ 和 $b = \sqrt{2}$ 作为我们寻求的例子，因为 a 和 b 都是无理数并且

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$$

  这是合理的。

在任何情况下，我们都找到了一个实数 $a, b \in \mathbb{R}$ 的例子，使得 a 和 b 都是 irrational，而 a^b 是 rational。这证明了该说法。 □

这是一个 **non-constructive** 证明的例子。它告诉我们某物存在（甚至将其缩小到两种可能性），但实际上并没有告诉我们我们一直寻求的 *exactly* 是哪一种可能性。这正是排中律的直接应用所导致的。

(问题：你能证明 $\sqrt{2}^{\sqrt{2}}$ 是无理数吗？它是，但没有已知的“简单”证明这个事实。也许你能找到一个！)

大多数我们在这里做的证明将是**constructive**类型的（但并非全部）。这些可能对你来说更令人满意，我们也有同样的看法。如果我们声称某物存在，我们应该能够*show*给你看，对吧？如果我们只是谈论了一段时间，说*why*这样的物体存在于别处，而无法指出它，你就得相信我们，但你可能不会对此感到太舒服。正是由于这个原因，构造性证明是*subjectively better*的，而且只要可能，我们总是会努力寻找一个。然而，有时构造性证明并不立即明显，我们就不得不做出非构造性的证明，就像我们在这里所做的那样。

4.4.6 Looking Back: Indexed Set Operations and Quantifiers

回顾第3.6.2节，我们在定义3.6.3和3.6.4中分别定义了集合运算——并集和交集，在索引集上执行——主要思想是我们可以使用缩写符号一次性表达整个类别的集合的并集/交集。

仔细查看那些定义。例如，是什么特征表明一个对象实际上是一个索引联合的元素？该对象需要是联合组成集合的元素。也就是说，需要存在某个集合，该对象是该集合的元素。这听起来像是一个*existential quantification*，不是吗？

同样，什么特征定义了一个对象是否是索引交集的元素？那个对象需要是构成集合 *all* 的元素。也就是说，*for all* 这些集合中，那个对象必须是其中的元素。这是一个 *universal quantification*。

现在做出这些观察后，我们可以使用我们新的量词符号重新编写那些索引集合运算的定义：

Definition 4.4.2. *Suppose I is an index set and $\forall i \in I \bullet A_i \subseteq U$, for some universal set U. Then*

$$\bigcup_{i \in I} A_i = \{x \in U \mid \exists k \in I \bullet x \in A_k\}$$
$$\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I \bullet x \in A_i\}$$

再次尝试与第3.6.2节中的某些示例和练习一起工作。定义现在更有意义了吗?

4.4.7 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆!

(1) 什么是数学命题的 **negation**? 一个命题及其否定之间有何关系?

(2) 为什么一个 $\forall$ 声明的否定是一个 $\exists$ 声明?

为什么一个 $\exists$ 声明的否定是一个 $\forall$ 声明?

(3) 什么是非构造性证明? 这个术语适用于哪种类型的陈述——$\exists$或$\forall$?

(4) 考虑以下主张

$$\forall x \in S \bullet P(x)$$

为什么它是以下内容的否定 *neither*?

$$\forall x \notin S \bullet P(x)$$

$$\exists x \notin S \bullet \neg P(x)$$

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 对于以下每个陈述，写出其否定形式。原始陈述或其否定，哪一个是 True?

(a) $\forall x \in \mathbb{R}$ ○ $\exists n \in \mathbb{N}$ ○ $n > x$ ○ $\forall x \in \mathbb{R}$ ○ $n > x$ ○ $\exists y \in \mathbb{R}$ ○ $y = x^3$ ○ $\forall x \in \mathbb{R}$ ○ $y = x^3$

(b) $\exists n \in \mathbb{N}$ (c) $\forall x \in \mathbb{R}$ (d) $\exists y \in \mathbb{R}$

(2) 对于以下每个陈述，写出其否定形式。原始陈述还是否定陈述是 True?

(a) $\exists S \in \mathcal{P}(\mathbb{N})$ ○ $\forall x \in \mathbb{N}$ ○ $x \in S$ ○ $\exists x \in \mathbb{N}$ ○ $x \in S$ ○ $\exists S \in \mathcal{P}(\mathbb{N})$ ○ $x \in S$ ○ $\forall S \in \mathcal{P}(\mathbb{N})$ ○ $x \in$

(b) $\forall S \in \mathcal{P}(\mathbb{N})$ (c) $\forall x \in \mathbb{N}$ (d) $\exists x \in \mathbb{N}$

(3) 让 $I = \{x \in \mathbb{R} \mid 0 < x < 1\}$。

对于以下定义的每个集合，写出确定一个数 $y \in \mathbb{R}$ 是否属于该集合的定义条件，使用量词。

然后，确定集合是什么，并使用集合表示法写出你的答案。

(也尝试用双重包含论证来{v*}你的主张！)

(a)
$$S = \bigcup_{x \in I} \{y \in \mathbb{R} \mid x < y < 2\}$$

(b)
$$T = \bigcap_{x \in I} \{y \in \mathbb{R} \mid -x < y < x\}$$

(c)
$$V = \bigcup_{x \in I} \{y \in \mathbb{R} \mid -3x < y < 4x\}$$

(4) 让 $P = \{y \in \mathbb{R} \mid y > 0\}$。考虑这个陈述:

$$\forall \varepsilon \in P \,.\, \exists \delta \in P \,.\, \forall x \in \{y \in \mathbb{R} \mid -\delta < y < \delta\} \,.\, |x^3| < \varepsilon$$

写出此陈述的逻辑否定。

这个陈述说了什么? 它的否定说了什么?

哪个是 True? 你能证明它吗?

(5) 设 A, B, C, D 为任意集合。

让 $P(x), Q(x, y), R(x, y, z)$ 为任意变量命题。

写出以下每个陈述的否定形式。

(a) $\forall a \in A \quad \exists b \in B \quad Q(a,b)$

(b) $\forall a \in A \quad \neg P(a)$

(c) $\forall c \in C \quad \forall d \in D \quad \neg Q(c,d)$

(d) $\exists a_1, a_2 \in A \quad \forall d \in D \quad R(a_1, a_2, d)$

(e) $\forall b_1, b_2, b_3 \in B \quad \neg R(b_1, b_2, b_3)$

(f) $\exists b \in B \quad \forall c \in C \quad \forall d \in D \quad R(d, b, c)$

4.5 Logical Connectives

为了从更简单的数学陈述（即仅由量词和命题组成的陈述）构建数学陈述，我们可以用某些词语和短语（如“和”、“或”和“蕴含”）连接几个陈述，以创建更复杂的陈述并断言更多的主张和真理。我们称这些词语和短语为 **logical connectives**，每个都有其对应的数学符号和意义。这些意义将基于我们对英语语言和理性思维的直观理解而对你有意义，但我们强调，引入数学逻辑及其相应符号的主要目标之一是将这些直觉转化为严格和明确的观念。

在整个本节中，让我们假设 P 和 Q 是任意的数学陈述。这些陈述本身可以由量词和其他连接词以及各种数学概念组成的复杂组合。关键在于，我们将 P 和 Q 结合成更大陈述的方式与它们各自的组成无关。在此之前，我们看到了：

我们讨论的是组成陈述，P 和 Q 实际上可能是变量命题。例如，我们将考虑如何连接两个变量命题，$P(x)$ 和 $Q(x)$，它们各自依赖于某个变量 x。本节中我们开发的定义和方法适用于这些变量命题，尽管这些命题本身在没有告知变量 x 的值的情况下没有真值。

当我们想要有意义且数学地讨论那些命题时，我们必须对变量 x 进行 **quantify**。因此，如果我们有变量命题 $P(x)$ 和 $Q(x)$，我们仍然可以有意义地定义 $P(x) \wedge Q(x)$（，其中 $\wedge$ 表示“和”，正如你将在下一节中看到的那样。然后，在一个例子或问题中，我们可以讨论如下形式的断言

$$\exists x \in X \,.\, P(x) \wedge Q(x)$$

这是一个数学 **statement**。

本质上，我们想要表达的观点是，这些连接词仍然适用于变量命题，但相关的变量必须被量化

somewhere 在总体陈述中将变量命题转化为适当的 **mathematical statement** 。

4.5.1 And

要说

$$\text{“}P \text{ and } Q\text{” is True}$$

表示 *both* 陈述的真值是：True。如果陈述 P 或 Q 中的任何一个为 False，那么陈述“P和 Q”也将是 False。这个定义封装了这个想法：

Definition 4.5.1. *We use the symbol “$\wedge$” between two mathematical statements to mean “and”. For instance, we read “$P \wedge Q$” as “P and Q”.*

This is referred to as the ***conjunction*** *of P and Q.*

The truth value of “$P \wedge Q$” is True *when both P and Q are true, and the truth value is* False *otherwise.*

这里有一些示例来展示这个定义：

Example 4.5.2.

$$\begin{array}{ll} (1+3=4) \wedge (\forall x \in \mathbb{R}\text{.}\ x^2 \geq 0) & \text{True} \\ (1+3=5) \wedge (\forall x \in \mathbb{R}\text{.}\ x^2 \geq 0) & \text{False} \\ (1+3=5) \wedge (\exists x \in \mathbb{Q}\text{.}\ x^2 = 2) & \text{False} \end{array}$$

Notation: Parentheses

有时在上述示例中省略括号是常见的。例如，上述示例中的第一行可以等价地写成

$$1+3=4 \ \wedge\ \forall x \in \mathbb{R}\text{.}\ x^2 \geq 0$$

使用括号可以使语句更易读。没有它们，我们不得不多想一会儿才能弄清楚语句的一部分在哪里结束，下一部分在哪里开始，但我们最终还是能理解它的意思。我们将尽量在使语句更容易理解的情况下使用括号。

Notation: Sets and Logic

您可能会注意到逻辑连接词“$\wedge$”和集合运算符“$\cap$”之间的相似性。这绝非巧合！

以下我们将讨论第4.5.4节，我们可以使用连接词“$\wedge$”来写出“$\cap$”的定义，因为该集合运算符的底层逻辑。现在试试，如果你愿意的话，简要地浏览一下那个章节！不过，一般来说，要小心保持这两个符号的区分！如果A和B是集合，短语“$A \wedge B$”没有明确定义；所指的是“$A \cap B$”。

4.5.2 Or

要说

$$\text{“}P \text{ or } Q\text{” is True}$$

表示“P是True，或者Q是True”。我们需要知道陈述的*one*是True，才能声明整个陈述的真值是True。我们不在乎*both* P和Q是否为真，只在乎它们中的*at least one*个为真。

这与所谓的“逻辑异或”相对，也称为XOR，当P和Q都为True时，将其声明为False。在数学中，我们使用**inclusive “or”**。我们只关心是否至少有一个陈述成立。

Definition 4.5.3. *We use the symbol* $\vee$ *between two mathematical statements to mean “or”. For instance, we read “*$P \vee Q$*” as “*P *or* Q*”.*

This is referred to as the **disjunction** *of* P *and* Q*.*

The truth value of “$P \vee Q$*” is* True *when* **at least one** *of* P *and* Q *is* True *(even when both are* True*), and the truth value is* False *otherwise.*

Example 4.5.4.

$$(1+3=4) \vee (\forall x \in \mathbb{R}\text{.}\ x^2 \geq 0) \qquad \text{True}$$
$$(1+3=5) \vee (\forall x \in \mathbb{R}\text{.}\ x^2 \geq 0) \qquad \text{True}$$
$$(1+3=5) \vee (\exists x \in \mathbb{R}\text{.}\ x^2 < 0) \qquad \text{False}$$

Notation

相同的关于符号的说明，我们在前一小节中提到，也适用于此处。首先，括号的使用——如上例所示——是有帮助的，但并非技术要求。尽管如此，我们仍会尽量在需要时使用它们。

其次，你可能注意到逻辑连接词“$\vee$”和集合运算符“$\cup$”之间的相似性。再次强调，这并非巧合！尝试使用“$\vee$”重新表述“$\cup$”的定义，并简要浏览第4.5.4节。不过，一般来说，要小心保持这两个符号的区分！如果A和B是集合，短语“$A \vee B$”没有明确定义；其意是指“$A \cup B$”。

4.5.3 Conditional Statements

这是最难处理的逻辑连接词，并且始终给学生带来一些问题，因此我们想要对此格外小心和明确。我们希望陈述 **“If P, then Q”**（有时写作 “P蕴含Q”）当 Q *necessarily* 的真实性从 P 的真实性中得出时，具有真值 True。也就是说，我们希望以下条件成立时，这个陈述是 True：

无论 P 是 True，Q 就是 *also* True。

Truth Table and Definition

由于这在语义上是最难弄清楚的连接，让我们引入一个 **truth table** 的概念来简化符号：

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$Q \implies P$
T	T	F	T	T	T	T
T	F	F	F	T	F	T
F	T	T	F	T	T	F
F	F	T	F	F	T	T

您可能之前在其他数学课程中见过真值表，但即使没有，也不要担心！这里的主要思想是：每一列对应一个特定的数学陈述及其相应的真值。每一行对应构成陈述 *assigment* 的特定真值，P和 Q。

注意这里有4行，因为P和Q各自可以有两个不同的真值之一，所以有4种可能的组合。阅读特定行，我们可以找到其他陈述的对应真值，这取决于第一列中P和Q的T和F赋值。

注意，$P \wedge Q$ 和 $P \vee Q$ 的列遵循上述定义。$P \wedge Q$ 的列只有一个 T，它对应于 *both* P和 Q 是 True 的情况。所有其他情况都使 $P \wedge Q$ 成为 False 声明。同样，$P \vee Q$ 的列只有一个 F，它对应于 *both* P和 Q 是 False 的情况。所有其他情况都使 $P \vee Q$ 成为 True 声明。

现在，为什么最后两列是这样的呢？假设我提出一个主张：“如果你努力学习，那么你在这门课程中会得到A”。在这里，P是“你努力学习”，Q是“你将得到A”。你什么时候可以称我为*liar*？你什么时候可以宣布我说的是真话？当然，如果你努力学习并得到A，我说的是真话。同样，如果你努力学习但得不到A，那么我对你撒了谎。然而，如果你不努力学习，那么无论发生什么，*you don't get to call me a liar!*我的主张没有涵盖你的情况；我一直以来都在假设你只是会努力学习！因此，我没有说谎，所以根据排中律，我*did*说的是真话。谎言的否定是真理。

这种情况——其中 $P \implies Q$ 列的第三行和第四行是 True——被称为一个 **false hypothesis**。当“$\implies$”左边的陈述不成立时，那么我们就不处于该主张旨在解决的问题的情况，因此我们不能断言该主张是 False。因此，根据排中律)，该主张必须再次是 True (。

让我们给出这个符号的正确定义，然后考虑更多例子来说明这个定义。

Definition 4.5.5. *We use the symbol "$\implies$" between to mathematical statements to mean "If . . . then" or "implies". For instance, we read "$P \implies Q$" as "If P, then Q" or "P implies Q".*

This is referred to as a **conditional statement**.

The truth value of "$P \implies Q$" is True *assuming that Q holds whenver P holds.*

The truth value is False *仅 in the case where P is* True *and yet Q is* False.

We refer to P as the **hypothesis** *of the conditional statement and Q as the* **conclusion**.

那个关键词“whenever”在定义中应该让你明白为什么*false hypothesis*情况是有意义的。当我们知道P是真的，并且可以推断出Q也是真的，那么我们就可以声明$P \implies Q$是True。如果P一开始就不是真的，我们就不能声明$P \implies Q$是False。只有当Q不一定能从P中推导出来时，我们才能说$P \implies Q$是假的，即当存在一个实例，其中假设P是True，但结论Q是False时。

Examples

这里有一些示例，以帮助您理解这个概念：

$$\begin{aligned}
(1+3=4) &\implies (\forall x \in \mathbb{R}.\ x^2 \geq 0) && \text{True}\\
(1+3=5) &\implies (\forall x \in \mathbb{R}.\ x^2 \geq 0) && \text{True}\\
(1+3=5) &\implies (\text{Abraham Lincoln is alive}) && \text{True}\\
(1+1=2) &\implies (0=1) && \text{False}\\
(0=0) &\implies (\exists x \in \mathbb{R}.\ x^2 < 0) && \text{False}\\
(\text{Pythagorean Theorem}) &\implies (1=1) && \text{True}\\
(0=1) &\implies (1=1) && \text{True}
\end{aligned}$$

注意，第二个和第三个例子是True，因为它们有错误的假设“$1+3=5$”。无论结论如何，整个条件语句都必须是True，因为这个原因。

请注意第二个例子是True，但它并不能帮助我们确定勾股定理本身是否是True！这正是我们在第一章中证明的“虚假”伪造中所做的，回顾1.1.1节，特别是“证明2”。我们假设勾股定理是True，然后从这个假设中逻辑地推导出一个True命题。这并不意味着假设有效，仅仅因为我们推导出了一个有效的结论！

Note, the second example is True, but it does not help us determine the statement's truth value.

这个想法非常重要，以至于我们甚至会再次向您展示这个引人注目的例子。请注意，它的逻辑形式与那个其他欺骗性例子完全相同：

“Proof”. 假设$1=0$。然后，根据$=$的对称性质，$0=1$也成立。将这两个方程相加，我们得到$1=1$，即True。因此，$0=1$。

□

这是这里的主要观点：

> 了解一个条件语句，总体上等于True，并不能告诉我们 *anything* 关于组成命题的真值。

注意，第二个和第三个例子是True，因为它们有错误的假设“$1+3=5$”。无论结论如何，整个条件语句都必须是True，因为这个原因。“并不重要”

这在上面第三和第七条陈述中也有惊人的体现；两个条件主张都是 True，但我们当然不能得出亚伯拉罕·林肯还活着，或者 $0 = 1$ 的结论。

"Implies" is not the same as "Can be deduced from"

经常有人混淆使用“意味着”一词来表示“如果……那么……”的陈述，一个条件语句。我们认为这可能是由于“意味着”一词的一些含义；具体来说，它似乎传达了一些某种*causality*。例如，考虑这个陈述：

$$1 + 3 = 4 \implies 2 + 3 = 5$$

这是一个 True 条件语句，我们的大脑可能之所以能识别出来，是因为我们可以直接取假设，即 $1 + 3 = 4$，并将两边都加 1，从而得到结论中的方程。从这个意义上说，假设的真实性似乎对结论的真实性有一定的影响：我们可以从一个中推断出另一个。这并不一定在一般情况下成立！

回顾上面给出的第一个例子：

$$(1 + 3 = 4) \implies (\forall x \in \mathbb{R}.\ x^2 \geq 0)$$

这个事实$1 + 3 = 4$与任何实数平方都是非负的事实有什么关系？它们之间甚至有联系吗？我们实际上并不关心！无论我们是否能找到直接从假设（以及这样的推理是否存在）推导出结论的方法，我们都可以将这个条件语句识别为True。只有构成语句的真值才重要。

当然，当我们致力于证明条件语句时，我们可能会尝试直接从一个语句推导出另一个语句。然而，重要的是要记住，这是我们的证明策略的结果，而不是条件语句定义的内在部分。因此，我们倾向于使用“如果……那么……”的形式来书写条件语句，而不是使用“蕴含”。我们有时可能会用到它，并且我们确信你们会在其他数学写作中看到它。但就目前而言，在我们仍在学习这些逻辑语句和连接词时，我们将尽可能地避免使用它。

Quantifying Variables: Still Important!

在数学中，我们经常想要证明涉及变量的条件语句。例如，我们可能想要证明，在实数 $\mathbb{R}$ 的背景下，以下条件陈述成立：

$$x > 1 \implies x^2 - 1 > 0$$

那句话，写在上面一行，本身就是一个 **variable proposition**，符号“ $\implies$ ”的定义适用于它。

如果我们知道 $x > 1$ 并且也知道 $x^2 - 1 > 0$，那么我们可以声明条件为 True。如果我们知道 $x \leq 1$，那么我们甚至不会在意 $x^2 - 1 > 0$ 是否成立；我们可以声明条件为 True。这就是“ $\implies$ ”的定义在这里的应用方式。

记住，尽管如此，上面所写的条件断言在技术上不是一个数学陈述。我们是在实数的背景下提出这个断言的，因此真正有意义的写法应该是

$$\forall x \in \mathbb{R}. \big(x > 1 \implies x^2 - 1 > 0\big)$$

这是作者最终试图主张的，所以他们应该直接这么说！我们向您提出同样的建议。这些逻辑连接词——$\wedge$、$\vee$和$\implies$——是有意义的，并且可以应用于变量命题。在这个范围之外，在您正在构建的陈述的其他某个地方，必须对这些变量进行某种量化。只有这样，我们才能确保这个句子是一个具有一个真值的数学陈述。

Writing “ $\implies$ ” using “$\vee$”

这是一个值得提到的有用且重要的想法。这部分的理由是因为我们稍后会用到它，但也部分是因为它可能有助于你理解条件语句并学习如何使用它们。

这个想法基于一个 *false hypothesis* 的概念。考虑一个条件语句，$P \implies Q$。如果 P 失败，那么整个语句是 True，无论 Q 的真值如何。然而，如果 P 成立，那么我们肯定需要 Q 也成立，才能宣布整个语句是 True。

这些观察使我们能够识别出条件语句可以成立两种方式，并将这两种方式写成“或”语句。要么 $\neg P$ 成立（即一个错误假设），要么 Q 成立。在这两种情况中，条件语句 $P \implies Q$ 必须成立！让我们直接陈述这个主张，供您考虑：

> 条件语句“$P \implies Q$”和语句“$\neg P \vee Q$”
> 具有相同的真值。

这是一个好的**logical equivalence**例子，这是我们将在下一节讨论的主题。目前，我们将展示上述两个陈述的真值表。请注意，无论构成陈述的真值如何，P和Q，它们的真值都是相同的。这进一步证实了这些陈述是等价的，除了我们上面提供的描述之外。

P	Q	$\neg P$	$\neg P \vee Q$	$P \implies Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Investigating More Examples

让我们考虑一些更多条件性索赔的例子，并决定它们是 True 还是 False。通过这样做，我们正在帮助您更好地理解 $\implies$ 的工作原理。

然后，我们将继续证明 *strategies* 并讨论如何使用逻辑连接词和量词正式且严谨地证明这类主张。

Example 4.5.6. 我们将从这里开始一个“真实世界”的例子，以便熟悉涉及的逻辑。在整个例子中，假设我们在一个只有周一、周三和周五有正式安排的课程中。

您将注意到我们将取两个陈述，P 和 Q，并考虑这些陈述及其否定所有四种可能的组合来制作条件陈述。

- “如果今天有讲座，那么就是工作日。”

  (注意：这个句子中有些*implicit quantification*。我们真正想说的是，“对于每周日历中的所有d天，如果我们有在d天的讲座，那么d是工作日。”我们认为上面的句子更简洁地传达了主要思想，因此我们将使用这个版本。请注意，这是句子的含义，在我们的讨论中，我们必须考虑这种量化所涉及的不同情况。)

  这可以通过定义 P 为“我们今天有讲座”和 Q 为“今天是工作日”来逻辑地表达；那么断言是 $P \implies Q$。

  这是 True 吗？注意，陈述 P 和 Q 没有指定 *what day it is*，所以如果我们断言这个说法是 True，那么这个真相应该是 *independent* 当天的。也就是说，无论今天是 *whatever* 天，我们都需要证明 $P \implies Q$ 成立。让我们通过考虑几个情况来做这件事：

  – 假设今天是星期六或星期日。由于我们在这两天从未有讲座，所以这个条件陈述不是谎言，因此它是 True。– 假设今天是星期一、星期三或星期五。如果我们今天确实有讲座，那么它一定是工作日，所以这个陈述是 True。– 假设今天是星期二或星期四。我们通常今天没有讲座，即使在特殊情况下我们确实有（由于某些重新安排的原因），它仍然会是工作日，所以这个陈述是 True。

  在任何可能的情况下，主张都成立。因此，$P \implies Q$ 是 True。

  您可能会插话来说，“为什么还要考虑这些情况？我们难道不能说无论哪一天，假设我们有讲座，那么我们就可以断定它一定是工作日吗？”嗯，是的，我们可以！这实际上是一个更好的策略，一个更*direct*的方法，你可能会这么说。

  这暗示了我们将如何在将来证明条件陈述。因为我们实际上并不关心我们没有讲座的情况（的

false hypothesis) 我们只需要 *suppose* 我们在 X 和 *deduce* 有讲座，且 X 是工作日。这是我们用来 **directly prove** 一个条件性索赔的方法。

- 如果今天是工作日，那么我们今天有讲座。

  这是逻辑上写成 $Q \implies P$，使用与上一个例子中相同的 P 和 Q 的定义。

  这是否是关于 True 的说法？绝对不是！我们在学期的第一个星期二没有上过课，而那天是工作日。因此，那个说法者在那个例子中撒了谎！在那个星期二，Q 是 True 但 P 是 False。因此，$Q \implies P$ 是 False。

- “如果不是工作日，那么我们今天没有讲座。”

  这是逻辑上写成 $\neg Q \implies \neg P$，使用与上面示例中相同的 P 和 Q 定义。

  这是否是True的说法？是的，我们可以直接证明它。假设今天不是工作日；也就是说，假设今天是周六或周日。显然，大学不会如此残忍地安排在周末举行讲座，因此我们可以必然地声明我们不会有讲座，即$\neg P$成立。这表明$\neg Q \implies \neg P$是一个True陈述。

  （问题：为什么我们不需要考虑今天是工作日的情况？）

- “如果我们今天没有讲座，那么今天不是工作日。”

  这是逻辑上写成 $\neg P \implies \neg Q$，使用与上面示例中相同的 P 和 Q 的定义。

  这是否是True的声明？好吧，让我们来思考一下。如果我们假装今天没有讲座会怎样。我们一定能说什么吗？它肯定不是工作日吗？我不这么认为！也许它是星期二，我们只是没有安排讲座。这表明声明是False；我们有一个假设($\neg P$)成立，但结论($\neg Q$)不成立的情况。

  注意，有 *are* 种情况，其中 $\neg P$ 成立，*and* $\neg Q$ 也成立。例如，如果今天是星期六，那么我们当然没有讲座，因为不是工作日。但这 *specific instance* 并不意味着这个主张是 True！我们需要验证其在 *all instances* 上的真实性。

Example 4.5.7. 让我们用一个更“数学化”的例子来做同样的分析。在整个例子中，设 A 和 B 为任意集合。此外，设 P 为“$A \subseteq B$”，设 Q 为“$A - B = \varnothing$”。

我们将重复上一个例子中的操作，并考虑将 P 和 Q 及其否定以四种可能的方式组合来制作条件语句。

- Is $P \implies Q$ True?

是的！让我们假设 A 和 B 满足关系 $A \subseteq B$。这意味着 *every* 元素属于 A，也是 B 的元素。因此，我们不可能有一个元素 A，它 *not* 属于 B，因为 $A - B$ 是属于 A 而不属于 B 的元素集合，我们得出结论，没有这样的元素，所以 $A - B = \varnothing$。

- 是 $Q \implies P$ True?

  是的！让我们假装 $A - B = \varnothing$。这意味着有 *no* 个 A 的元素也是 B 的非元素。（想想看。）换句话说，任何元素 $x \in A$ *cannot* 都具有这样的性质：$x \notin B$ (否则 $x \in A - B$，因此 $A - B \neq \varnothing$)；因此，$x \in B$ 必然。嘿，这正是 $A \subseteq B$ 的意思！每当 $x \in A$，我们也会得出 $x \in B$。这表明 $Q \implies P$ 是正确的。

- Is $\neg Q \implies \neg P$ True?

  嗯，这更难弄清楚。让我们假设 $\neg Q$ 成立；这意味着 $A - B \neq \varnothing$。也就是说，存在某个元素 x 满足 $x \in A$ 和 $x \notin B$。当然，那么 $A \not\subseteq B$，因为我们已经识别出一个不属于 B (的 A 的元素，而 $\subseteq$ 关系则规定 A 的每个元素也应该是 B) 的元素。因此，$\neg Q \implies \neg P$ 是 True。

- Is $\neg P \implies \neg Q$ True?

  再次，我们需要思考这个问题。让我们先写下 $\neg P$ 的意思。要说明 $A \not\subseteq B$ 意味着存在某个元素 $x \in A$ 也满足 $x \notin B$。（这也是我们在上一个例子中使用的方法。）好的，这告诉我们什么？考虑集合 $A - B$。它有任何元素吗？是的，它至少有 x 作为元素！由于 $x \in A \wedge x \notin B$，我们可以说 $x \in A - B$。因此，$A - B \neq \varnothing$，我们得出结论，$\neg P \implies \neg Q$ 是 True。

Observations and Facts About "$\implies$"

好的，现在我们有一些使用条件语句和确定它们的真值值的练习。你应该注意到我们从讨论的例子中应该注意到的，即知道 $P \implies Q$ 成立是否 **not** 告诉我们关于 $Q \implies P$ 的任何信息。在上面的两个例子中，$P \implies Q$ 是 True；然而，在一个例子中 $Q \implies P$ 是 True，在另一个例子中是 False。即使我们知道 $P \implies Q$ 的真值，我们也不能必然地确定关于 $Q \implies P$ 的任何东西。这个想法非常重要，我们将在下一小节中讨论它。

现在，让我们对"$\implies$"连接词做一些更多说明。

- 记住，给定数学陈述 P 和 Q，句子 "$P \implies Q$" 本身又是另一个数学陈述。它有一个真值。这个真值 *depends* 在 P 和 Q (上，按照我们定义的方式

以上），但它并没有告诉我们 *anything* 关于 P 和 Q 的真值。所以，如果你只是写下这个主张

$$\text{Blah blah} \quad \Longrightarrow \quad \text{Yada yada}$$

在您的论文中，我们不知道您是否试图断言“Blah blah”或“Yada yada”是 True 或 False！对于一个数学家来说，这仅仅意味着：

> 条件语句“‘Blah blah’意味着‘Yada yada’”是 True。

如果您想进行某种推理或演绎，那么请使用一些辅助词语和句子来表明。写点像这样：

> $P \implies Q$ 因为……此外
> ，P成立，因为……
>
> 因此，Q成立。

如果您之前学习过形式逻辑，或者在一门哲学课程中见过这种论证，那么您可能会认出这作为 **Modus Ponens**。

- 一个 **false hypothesis** 产生一个 True 条件的观念有点奇怪；我们意识到这一点。这是排中律的直接后果。在错误假设下，我们无法说整体陈述是 False，所以它必须是 True，因为它必须是其中一个。

- 记住，我们总可以将条件语句转换为“或”语句，而不使用“$\Longrightarrow$”符号。语句“$P \implies Q$”和“$\neg P \vee Q$”始终具有相同的真值。

Converse and Contrapositive

让我们给与给定条件语句相关的不同类型的条件语句起一些名字。我们稍后经常会提到这些。

Definition 4.5.8. *Let P and Q be mathematical statements. Consider the "original" claim, $P \implies Q$.*

We refer to $Q \implies P$ as the **converse** *of the original claim.*

We refer to $\neg Q \implies \neg P$ as the **contrapositive** *of the original claim.*

通过我们在前一小节中的观察，我们知道**converse**并不具有与原始相同的真值。我们将在下一节中看到（并证明），**contrapositive**始终具有与原始主张相同的*same*真值。（这是**logical equivalence**的概念，我们将在下一节中详细讨论。）

您可能会想知道为什么我们需要这种术语。嗯，因为逆否命题可以证明是 *logically equivalent* 原命题，当我们试图证明条件语句时，它产生了一种有效的证明方法。我们很快就会发展这一点。这就是为什么我们使用逆否命题。

相反的情况很有趣，因为它的真值不一定与原始陈述的真值相关联：即使知道原始陈述是 True，其逆命题可能是 True，也可能是 False。因此，每当我们要证明一个陈述 $P \implies Q$ 为真时，数学家（可能）会立即想，“嗯，逆命题也成立吗？”这是一个很自然的问题，每当面对一个条件陈述时都值得思考。（事实上，如果你发现自己在一个数学家的聚会上，听到有人谈论一个“如果……那么……”的陈述，你应该问，“逆命题也成立吗？”你可能会给你的同伴留下深刻印象。）

逆命题也是日常生活中可能遇到的常见逻辑谬误的主题。也许你在和朋友辩论时试图论证$A \implies B$。如果他们反驳说，“嗯，B并不一定意味着A！你的论点是错误的！”你是否曾经因为这种情况感到沮丧？你可能想喊道，“那又怎样？我并没有试图说关于$B \implies A$的任何事情。我在谈论$A \implies B$，你……”（在我们变得粗鲁之前，我们先停下来。）无论你的朋友是否正确，知道逆命题的真值并不能告诉你你原始论断的真值。你应该告诉他们这一点！下次，只需说，“你谈论的是逆命题，这并不一定与我的论断在逻辑上相关。”

好的，现在我们已经定义了所有必要的逻辑符号并看到了一些例子，是时候继续前进并开始证明它们了！但首先，关于集合运算的简要说明，然后是一些练习题。

4.5.4 Looking Back: Set Operations and Logical Connectives

回顾第3.4节和第3.5节，我们在那里定义了子集和集合运算。所有这些定义都使用了某些逻辑思想，但当时我们用英语写了它们，依赖于我们的集体直觉和对逻辑的工作知识。现在我们可以使用量词和连接词来重新编写它们!

首先，回忆一下 **subset** 的定义。我们写 $A \subseteq B$ 如果以下条件成立：每当 $x \in A$，我们也可以说 $x \in B$。请注意关键词“每当”，它既表示一个 *universal quantification* 也表示一个 *conditional statement*。思考一下如何使用这个概念重新编写 $A \subseteq B$ 的定义，然后继续阅读以了解我们的版本……

Definition 4.5.9. *Let A, B, U be sets, where $A, B \subseteq U$ (i.e. U is a universal set). We say A is a* **subset** *of B, and write $A \subseteq B$, if and only if*

$$\forall x \in U \bullet x \in A \implies x \in B$$

这很有道理，因为它断言了我们上面段落中写的“每当”语句：每当 $x \in A$ ，我们也能够得出 $x \in B$；“如果 $x \in A$，那么 $x \in B$”必须成立。

回顾一下我们给出的集合运算的定义。尝试用逻辑符号编写自己的版本，然后在这里阅读我们的版本。思考它们如何有意义，如何表达相同的基本思想。

Definition 4.5.10. *Let A, B, U be sets, where $A, B \subseteq U$ (i.e. U is a universal set). Then,*

$$\begin{aligned} A \cap B &= \{x \in U \mid x \in A \ \wedge \ x \in B\} \\ A \cup B &= \{x \in U \mid x \in A \ \vee \ x \in B\} \\ A - B &= \{x \in U \mid x \in A \ \wedge \ \neg(x \in B)\} = \{x \in U \mid x \in A \ \wedge \ x \notin B\} \\ \overline{A} &= \{x \in U \mid \neg(x \in A)\} = \{x \in U \mid x \notin A\} \end{aligned}$$

当我们在这里时，我们还可以重新定义集合的 **partition**。这将使用逻辑连接词，但这也使人回想起索引集合以及它们如何通过量词来定义。我们在这里所学的一切都汇聚在一起了！

Definition 4.5.11. *Let A be a set. A* **partition** *of A is a collection of sets that are pairwise disjoint and whose union is A.*

That is, a partition is formed by an index set I and non-empty sets S_i (defined for every $i \in I$) that satisfy the following conditions:

(1) $\forall i \in I \bullet S_i \subseteq A$.

(2) $\forall i, j \in I \bullet i \neq j \implies S_i \cap S_j = \varnothing$.

(3) $\bigcup_{i \in I} S_i = A$

回顾定义3.6.9，看看我们最初是如何定义一个划分的。你看到我们在这里说的是同一件事，只是使用了逻辑符号吗?

4.5.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) $\wedge$ 和 $\vee$ 之间的区别是什么?

(2) $\wedge$ 和 $\cap$ 之间的区别是什么? $\vee$ 和 $\cup$ 之间的区别是什么?

(3) 将命题 $P \implies Q$ 的真值表写出来。

(4) 为什么 $P \implies Q$ 和 $\neg P \vee Q$ 是逻辑等价语句?

(5) 条件语句的逆命题是什么?

什么是条件语句的逆否命题?

(6) 条件语句及其逆命题的真值是否相关?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 对于以下每个句子，使用逻辑符号重新编写，并确定它是 True 还是 False。

(a) 每个整数要么是严格正数，要么是严格负数。 (b) 对于任何给定的实数，都存在一个比它严格大的自然数。 (c) 对于每个实数，如果它是负数，那么它的立方也是负数。 (d) $\mathbb{Z}$ 的一个子集具有这样的性质：每当一个数是该集合的元素时，它的平方也是该集合的元素。 (e) 存在一个既是偶数又是奇数的自然数。

(2) 将以下每个 $\forall$ 权利要求重写为条件语句，并确定它是 True 还是 False。

(a) $\forall x \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $\quad y = 2k\}$ ○ $\quad x^2 \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $y = 2k\}$ (b) $\forall x \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $\quad y = 2k + 1\}$ ○ $x^2 \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $y = 2k + 1\}$ (c) $\forall x \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $\quad y = 2k\}$ ○ $x^2 \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z}$ ○ $y = 2k\}$

(3) 将以下每个条件语句重写为 $\forall$ 声明，使用集合构造器符号，并确定它是 True 还是 False。

(a) $\forall x \in \mathbb{R}$ ○ $\quad x > 3 \implies x^2 < 9$ ○ $\quad x < 3 \implies x^2 < 9$ ○ $\quad t^2 - 6t + 9 \geq 0 \implies t \geq 3$

(b) $\forall x \in \mathbb{R}$ (c) $\forall t \in \mathbb{R}$

(4{v*} 让我们定义以下变量命题：

$$P(x) \text{ is “ } \frac{1}{2} < x \text{ ”}$$
$$Q(x) \text{ is “ } x < \frac{3}{2} \text{ ”}$$
$$R(x) \text{ is “ } x^2 = 4 \text{ ”}$$
$$S(x) \text{ is “ } x + 1 \in \mathbb{N} \text{ ”}$$

对于以下每个陈述，确定它是 True 还是 False。

(a) $\forall x \in \mathbb{N}$ ○ $P(x)$ ○ $Q(x) \implies P(x)$ ○ $Q(x) \implies P(x)$ ○ $\neg S(x) \vee R(x)$ ○ $R(x) \wedge \neg S(x$

(b) $\forall x \in \mathbb{N}$ (c) $\forall x \in \mathbb{Z}$ (d) $\exists x \in \mathbb{N}$ (e) $\exists x \in \mathbb{Z}$ (f) $\forall x \in \mathbb{R}$ (g) $\exists x$

(5) 对于以下每个条件语句，用逻辑符号表示它，并据此写出其逆命题和逆否命题；然后，确定这三个命题的真值：原命题、逆命题和逆否命题。

(a) 如果一个实数严格位于0和1之间，那么它的平方也是如此。 (b) 如果一个自然数是偶数，那么它的立方也是如此。 (c) 无论何时一个整数是10的倍数，它也是5的倍数。

4.6 Logical Equivalence

在这一节中，主要目标是介绍 **logical equivalence** 的概念并证明一些基本命题。本质上，我们想要确定某些复杂的逻辑陈述在真值意义上实际上是“相同”的。由于数学陈述可能依赖于某些命题变量，我们可能无法得出关于它们的真值的具体结论。然而，我们有时可以证明，对于包含的变量所有可能的值，两个数学陈述都将具有 *the same truth value*。这是一个非常好的结论！我们可以断言它们具有相同的真值，无论它是什么。从这个意义上说，我们正在从逻辑上证明这两个陈述是 **equivalent**。

4.6.1 Definition and Uses

以下定义引入了一个方便的符号来表示上文段落中描述的逻辑等价概念:

Definition 4.6.1. *Let P and Q be mathematical statements. We use the symbol "$\iff$" to mean "is* **logically equivalent** *to", or "has the same truth value as".*

That is, we write "$P \iff Q$" when P and Q always have the same truth value, regardless of whether it is T *or* F*.*

We read "$P \iff Q$" aloud as "P is logically equivalent to Q" or "P **if and only if** *Q".*

This type of statement is known as a **biconditional** *(or a* **bi-implication***).*

让我们取上节中看到的真值表，并为这个符号添加一列:

P	Q	$\neg P$	$\neg P \vee Q$	$P \implies Q$	$Q \implies P$	$P \iff Q$
T	T	F	T	T	T	T
T	F	F	F	F	T	F
F	T	T	T	T	F	F
F	F	T	T	T	T	T

在 $P \iff Q$ 的列中，当且仅当 P和 Q 具有相同的真值时，一个条目具有真值 T。这发生在第 1 行，其中两者都是 T，以及第 4 行，其中两者都是 F。请注意，$P \iff Q$ 只有在具有真值 T 时才具有真值 T。

$$(P \implies Q) \wedge (Q \implies P)$$

这是一个 True 陈述。这是 **logical equivalence** 的概念：$P \iff Q$ 表示 $P \implies Q$ 和 $Q \implies P$ 都成立。无论 P 具有什么真值，Q 都保证具有相同的真值，反之亦然:

- 假设 P 是 True，那么 $P \implies Q$ 告诉我们 Q 也必须是 True。
- 假设 P 是 False，那么 $Q \implies P$ 告诉我们 Q *cannot* 应该是 True (，因为 $Q \implies P$ 将会是 False，在这种情况下)，所以 Q 也必须是 False。

无论哪种方式，P和 Q 具有相同的真值。

Examples

Example 4.6.2. 再次查看上表中的第三列和第四列。它们证明了以下逻辑等价性:

$$(P \implies Q) \iff (\neg P \vee Q)$$

无论 $P \implies Q$ (的真值如何，这当然取决于 P和 Q)，它必须与 $\neg P \vee Q$ 的真值相同。我们之前已经提到过这种等价性，未来我们将会经常利用它。

Example 4.6.3. 看这个真值表:

P	Q	$\neg P$	$\neg Q$	$P \implies Q$	$\neg Q \implies \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

无论 P和 Q 的真值如何，我们发现 $P \implies Q$ 和 $\neg Q \implies \neg P$具有相同的 *same* 真值。因此，它们是 *logically equivalent*，我们可以写出:

$$(P \implies Q) \iff (\neg Q \implies \neg P)$$

这是我们在上一节中陈述的事实（未证明）：{v*}

逆否命题与原命题在逻辑上是等价的。

一种不同的证明方法利用了将条件语句表示为析取的方法。回忆逻辑等价

$$\big(P \implies Q\big) \iff \big(\neg P \vee Q\big)$$

我们之前例子中提到的。现在，考虑那个原始条件语句的逆否命题:

$$\neg Q \implies \neg P$$

应用相同的析取形式到该陈述中，得到以下等价式:

$$\big(\neg Q \implies \neg P\big) \iff \big(\neg(\neg Q) \vee \neg P\big)$$

现在，注意到 $\neg(\neg Q)$ 等价于仅仅 Q，并且记得析取的顺序无关紧要（即 $P \vee Q$ 和 $Q \vee P$ 具有相同的真值），我们发现

$$\big(\neg Q \implies \neg P\big) \iff \big(\neg P \vee Q\big) \iff \big(P \implies Q\big)$$

这以另一种方式表明，一个条件语句及其逆否命题具有相同的真值!

Example 4.6.4. 本节稍后，我们将证明以下逻辑等价性，无论命题 P和 Q 和 R 是什么，都成立:

$$\begin{aligned}
\neg(P \wedge Q) &\iff \neg P \vee \neg Q \\
(P \wedge Q) \wedge R &\iff P \wedge (Q \wedge R) \\
P \vee (Q \wedge R) &\iff (P \vee Q) \wedge (P \vee R) \\
\neg(P \implies Q) &\iff P \wedge \neg Q
\end{aligned}$$

每个这都是一个断言，$\iff$符号两边的表达式具有相同的真值。你能看出为什么这些主张是True吗？你能想到如何证明它们吗?

If and Only If

逻辑等价与短语“当且仅当”有很好的关系。说“P当且仅当Q”意味着我们断言“P如果Q”和“P仅当Q”都成立。其中之一对应于$P \implies Q$，另一个对应于$Q \implies P$，所以断言两者都为真意味着我们刚才所描述的：

$$P \iff Q \quad \text{is the same as saying} \quad (P \implies Q) \wedge (Q \implies P)$$

现在，哪个是哪个呢？当我们说“P如果Q”，这意味着“如果Q，那么P。”也就是说，

$$\text{“}P \text{ if } Q\text{”} \quad \text{is the same as saying} \quad Q \implies P$$

Sussing out the other direction is a little harder! What does “P *only if* Q” really mean? This sentence is asserting that, in a situation where P holds, it must also be the case that Q holds. That is, knowing P holds means we also immediately know Q holds. Put even another way, whenever P is true, we necessarily know that Q is true. This is the same as saying $P \implies Q$ holds!

另一种思考方式如下。说“P仅当Q”等同于说不能同时满足P成立且Q不成立。从逻辑上讲，我们有

$$\neg\big(P \wedge \neg Q\big)$$

稍后在本节中，我们将陈述并证明 **DeMorgan's Laws for Logic**。其中一条法则告诉我们如何否定括号内的陈述。（实际上，你可能已经知道这些逻辑法则了。如果不是，你可以提前浏览第4.6.5节和第4.6.6节以获取预览。）结论是：

$$\neg P \vee Q$$

嘿，看，这逻辑上等同于$P \implies Q$，正如我们之前观察到的！酷。这只是进一步证实了“P只有当Q”意味着$P \implies Q$。

Using “$\iff$” in Definitions

我们还将经常在**definition**中使用“$\iff$”符号来表示所定义的术语是用于定义中的属性的等价术语。例如：

$$\text{We say } x \in \mathbb{Z} \text{ is } \mathbf{even} \iff \exists k \in \mathbb{Z}\mathbf{.}\ x = 2k$$

这意味着一个整数是偶数的概念等同于知道这个数是某个整数的两倍。同样，我们可以定义 **odd**：

$$\text{We say } x \in \mathbb{Z} \text{ is } \mathbf{odd} \iff \exists k \in \mathbb{Z}\mathbf{.}\ x = 2k + 1$$

这些是正式的定义，请注意，这是保证一个整数是偶数（或奇数）的唯一方法。我们将很快使用这些定义来严格证明一些关于整数和算术的事实。每次我们想要断言一个特定的整数（称之为x）是偶数时，我们需要证明存在一个整数k满足$x = 2k$。也就是说，我们必须通过引用定义中给出的逻辑等价性来 *satisfy the definition*。

Biconditional Statements: A Technical Distinction

我们也可以使用符号“$\iff$”同时表达两个条件语句。从技术上讲，这并不等同于断言逻辑等价，但它传达了类似的概念，因此我们允许以两种方式使用该符号。

逻辑等价涉及一些未定义命题，并断言无论这些命题的真值如何，两个陈述都将具有相同的真值。例如，

$$(P \implies Q) \iff (\neg P \lor Q)$$

这是一个逻辑等价的完美例子。不告诉你 P 和 Q 是什么，我们无法确切知道 $P \implies Q$ 和 $\neg P \lor Q$ 的含义。然而，我们不需要知道 P 和 Q 是什么，就能知道这两个陈述肯定具有相同的真值。

当“$\iff$”两边的两个陈述实际上是正确的数学陈述，没有未定义的命题时，情况略有不同。例如，考虑这个陈述：

$$\forall x \in \mathbb{R}\text{.}\ (x > 0) \iff \left(\frac{1}{x} > 0\right)$$

这是一个逻辑主张，它断言，每当 x 是一个实数时，知道这两个事实之一——$x > 0$ 或 $\frac{1}{x} > 0$——必然保证另一个。也就是说，如果我告诉你我在想一个实数，它是正的，你就会得出结论，它的倒数也是正的。同样，如果我告诉你我在想一个倒数是正的实数，你就会得出结论，这个数本身也是正的。它就是这样 *both ways*。（问题：如果我告诉你我在想一个 *negative* 实数呢？你能得出关于它的倒数的任何结论吗？为什么或为什么不呢？）

你看到这个有什么不同吗？给定一个任意的 $x \in \mathbb{R}$，陈述“$x > 0$”明确是 True 或 False。它的真值不是未确定的。这使它与上面给出的例子不同，在上面的例子中，个别陈述的真值是未知的，但我们仍然可以声明这些真值必须相同。

由于缺乏更好的、更普遍的术语来指称这类陈述，我们将它们称为 **biconditionals**。这是因为它们实际上旨在表示两个“方向相反”的条件语句：

$$\forall x \in \mathbb{R}\text{.}\ \left[\left((x > 0) \implies \left(\frac{1}{x} > 0\right)\right) \land \left(\left(\frac{1}{x} > 0\right) \implies (x > 0)\right)\right]$$

这是上述声明所说的：声明的每一部分都意味着另一部分。

此术语在其他数学写作中不一定标准化，但我们要指出这一技术区别，让您了解。您可能会遇到一位数学逻辑学家或集合理论学家，并使用短语“逻辑的”

等价”，他们可能会感到困惑或对您使用它的方式感到冒犯。不过，这并不是一个大问题！因为我们现在第一次学习这些基本概念，我们不必 necessarily 记住这些概念之下所有技术细节。此外，在这本书的剩余部分，我们可能会将“逻辑等价”和“双条件”互换使用。目前来说，这是可以接受和合理的。

主要使用“$\Longleftrightarrow$”符号的目的是断言两个陈述*have the same truth value*。一个“逻辑等价”与一个“双条件”之间的唯一区别是其中是否包含任何任意、未定义的命题。这在整体上是一个微小的区别，所以我们在这里只简要考虑。

4.6.2 Necessary and Sufficient Conditions

有两个术语在数学中偶尔被使用，它们传达了双条件语句的两个方向：**necessary** 和 **sufficient**。它们与双条件语句的“只有如果”和“如果”部分完全对应。这些术语是由数学家提出的问题的自然类型所激发的。

Sufficient: P, if Q

如果我们识别出一个数学对象的有趣事实或属性——称之为 P——我们可能会想，“我们何时可以 *guarantee* 这样的属性成立？是否存在某种条件我们可以检查，可以立即给出‘是’的答案？”这就是一个 **sufficient** 条件，一个保证 P 也成立的属性。它是“充分的”，因为它是“足够的”来得出 P 的结论；我们不需要任何其他外部信息。

假设我们已将命题 Q 识别为 P 的充分条件。我们如何从逻辑上表达这一点呢？好吧，知道 Q 就足以得出 P，因此我们可以轻松地将这写成条件语句：

$$Q \implies P \qquad \text{means } Q \text{ is a } \textbf{sufficient} \text{ condition for } P$$

赛 另一种方式，这个条件语句表示：“P，　　如果 Q”。

Necessary: P only if Q

我们也可能想知道，“我们如何保证P失败？是否存在某种我们可以检查的条件，可以立即告诉我们这一点？”这就是**necessary**条件，是P属性必要或*essentia*的属性。这个条件并不一定足以得出P成立的结论，但即使P有成立的可能，这个条件也必须成立。

考虑这里的逻辑关系。假设我们已建立了一个属性 Q，它是 **necessary** 条件对于 P 的。我们如何用符号表达 P 和 Q 之间的关系呢？没错，我们可以使用条件语句。知道 P 成立告诉我们 Q 一定成立；它是 P 必要的

要真实。这可以表示为

$$P \implies Q \qquad \text{means } Q \text{ is a } \textbf{necessary} \text{ condition for } P$$

另一种说法是，这个条件语句表达的是：“P仅当 Q”。

我们也可以从逆否命题的角度来考虑这个问题。如果 Q 不成立，那么 P 也不能成立。也就是说，

$$\neg Q \implies \neg P$$

这是上述条件语句的逆否命题，$P \implies Q$。我们知道这些是同一语句的逻辑等价形式。

Examples

Example 4.6.5. 设 $P(x)$ 为命题“x 是一个能被 6 整除的整数”。对于以下每个条件，让我们确定它是否是 **necessary** 或 **sufficient** 条件（或者可能是两者！）以使 $P(x)$ 成立。

(1) 设 $Q(x)$ 为 “x 是一个能被3整除的整数”。

要确定 $Q(x)$ 是否是必要条件，让我们假设 $P(x)$ 成立。我们能否推断 $Q(x)$ 也成立呢？嗯，是的！说一个整数 x 能被 6 整除意味着它能同时被 2 和 3 整除。因此，它当然能被 3 整除，所以 $Q(x)$ 成立。

为了确定 $Q(x)$ 是否是充分条件，让我们假设 $Q(x)$ 成立。我们能否推断 $P(x)$ 也成立呢？嗯……知道 x 是3的整数倍，那么它也是 *definitely* 2的倍数，从而我们可以得出它是6的倍数吗？我们认为不是！考虑 $x = 3$；注意 $Q(3)$ 成立，但 $P(3)$ 不成立。

这表明 $Q(x)$ 只是一个必要条件，而不是充分条件。

(2) 设 $R(x)$ 为 “x 是一个能被12整除的整数。 ”

根据上述例子的类似推理，我们可以得出结论，$R(x)$是$P(x)$的充分条件，但不是必要条件（因为我们可能有$x = 6$，其中$P(6)$成立，但$R(6)$不成立）。

(3) 设 $S(x)$ 为 “x 是一个整数，使得 x^2 能被 6 整除”。

我们将让您自己处理这个。...$S(x)$是$P(x)$的必要条件吗？它是充分条件吗？

小心，并注意我们指定 x 本身是一个整数。

4.6.3 Proving Logical Equivalences: Associative Laws

现在，让我们实际进行一些逻辑等价变换！在这样做的时候，我们将锻炼阅读和理解以及使用量词和连接词书写逻辑语句的能力。我们还将发展一些基本

逻辑结果，我们可以在近期内应用于开发证明技术。这些技术将是我们其余工作的基础，我们做的其他一切都将涉及实施这些证明策略和逻辑概念的某些组合。

让我们从一些简单的符号逻辑定律开始。证明某物是 {v*} 实质上意味着我们可以随意“移动括号”并得到相同的结果。你可能一直在使用加法结合律的事实！要给 x 加上 $y+z$，我们只需将 z 加上 $x+y$ 并知道我们会得到相同的答案。也就是说，我们可以放心地

$$x + (y + z) = (x + y) + z$$

我们可以将括号 $move$ 放在 wherever 我们想要的位置，因此，最终我们可以假装它们甚至不存在，直接写下

$$x + y + z$$

因为我们对两个加法的解释顺序无关紧要。类似的结果适用于逻辑语句的合取和析取，这正是我们现在要证明的。

Theorem 4.6.6. *Let P, Q, R be logical statements. Then*

$$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$$

and

$$P \vee (Q \vee R) \iff (P \vee Q) \vee R$$

我们将实际上以两种不同的方式证明这些主张：（1）通过真值表，和（2）通过语义（即词语）。它们都是完全有效的，但我们想向您展示这两种方式，让您决定您更喜欢哪种风格。

Proof 1. 首先，我们将通过真值表来证明这些主张。观察合取的表格：

P	Q	R	$P \wedge Q$	$Q \wedge R$	$P \wedge (Q \wedge R)$	$(P \wedge Q) \wedge R$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	T	F	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

因此，$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$因为它们对应的列在每个情况下都是相同的。

接下来，观察析取的表格：

P	Q	R	$P \vee Q$	$Q \vee R$	$P \vee (Q \vee R)$	$(P \vee Q) \vee R$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	F	T	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

因此，$P \vee (Q \vee R) \iff (P \vee Q) \vee R$，因为它们对应的列在每个情况下都是相同的。 □

Proof 2. 其次，让我们通过语义分析来证明这些主张，考虑第一个主张，

$$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$$

为了证明两边的 *logically equivalent*，我们需要证明以下两个条件语句都是 True：

$$P \wedge (Q \wedge R) \implies (P \wedge Q) \wedge R$$

和

$$(P \wedge Q) \wedge R \implies P \wedge (Q \wedge R)$$

($\implies$) 让我们证明第一个条件语句。假设 $P \wedge (Q \wedge R)$ 是 True。这意味着 P 是 True，并且 $Q \wedge R$ 是 True。根据定义，这意味着 P 是 True，并且 Q 是 True，并且 R 是 True。当然，那么根据定义，$P \wedge Q$ 是 True，并且 R 是 True。因此，$(P \wedge Q) \wedge R$ 也是 True。

($\impliedby$) 现在，让我们证明第二个条件语句。假设 ($P \wedge Q$) $\wedge R$ 是 True。这意味着 $P \wedge Q$ 是 True 并且 R 是 True。根据定义，这意味着 P 是 True 并且 Q 是 True 并且 R 是 True。当然，那么根据定义，P 是 True 并且 $Q \wedge R$ 是 True。因此，$P \wedge (Q \wedge R)$ 也是 True。

自我们已展示了两个条件语句，我们得出结论，这两边在逻辑上确实是等价的。

接下来，考虑该定理的第二条陈述，

$$P \vee (Q \vee R) \iff (P \vee Q) \vee R$$

为了证明两边的 *logically equivalent*，我们需要证明以下两个条件语句都是 True：

$$P \vee (Q \vee R) \implies (P \vee Q) \vee R$$

和

$$(P \vee Q) \vee R \implies P \vee (Q \vee R)$$

($\implies$) 让我们证明第一个条件语句。假设 $P \vee (Q \vee R)$ 是 True。这意味着要么 P 是 True，要么 $Q \vee R$ 是 True。这给我们提供了两种情况。

1. 假设 P 是 True。这意味着 $P \vee Q$ 是 True，根据定义。因此，$(P \vee Q) \vee R$ 是 True，也根据定义。

2. 假设 $Q \vee R$ 是 True。这意味着要么 Q 是 True，要么 R 是 True。再次，这给我们提供了两种情况。

   (a) 假设 Q 是 True。这意味着 $P \vee Q$ 是 True，根据定义。因此，$(P \vee Q) \vee R$ 是 True，也根据定义。 (b) 假设 R 是 True。这意味着 $(P \vee Q) \vee R$ 是 True，根据定义。

在任何情况下，我们发现 $(P \vee Q) \vee R$ 是 True。因此，这个条件语句是 True。

($\Longleftarrow$) 让我们来证明第二个条件语句。假设 ($P \vee Q$) $\vee R$ 是 True 。这意味着要么 $P \vee Q$ 是 True , 要么 R 是 True 。这给我们提供了两种情况。

1. 假设 $P \vee Q$ 是 True。这意味着要么 P 是 True，要么 Q 是 True。这给我们提供了两种情况。

   (a) 假设 P 是 True。这意味着 $P \vee (Q \vee R)$ 是正确的，根据定义。

   (b) 假设 Q 是 True。这意味着根据定义，$Q \vee R$ 是 True。因此，$P \vee (Q \vee R)$ 也根据定义是正确的。

2. 假设 R 是 True。这意味着根据定义，$Q \vee R$ 是 True。因此，$P \vee (Q \vee R)$ 也是根据定义的 True。

在任何情况下，我们得出结论，$P \vee (Q \vee R)$是True。因此，这个条件语句是 True。

因为我们已经证明了这两个条件语句都成立，所以我们得出结论，这两边在逻辑上确实是等价的。 □

好的，我们通过这些证明完成了什么？我们证明了什么，以及如何证明？为什么它有效?

让我们先提及这些证明的一个后果，然后再继续讨论和比较这些命题本身。我们证明了“$\wedge$”和“$\vee$”连接词是结合的，因此我们评估只涉及这种连接词的括号内语句的顺序并不重要。例如，我们现在知道“$P \wedge (Q \wedge R)$”与“（$P \wedge Q$）$\wedge R$”具有相同的意义。因此，在将来，我们将直接写出这些语句而不使用括号：“$P \wedge Q \wedge R$”。

Reflecting: Truth Tables vs. Semantics

让我们首先谈谈真值表。由于 P、Q 和 R 是逻辑陈述，它们各自单独是 True 或 False。真值表的八行考虑了将这些三个构成陈述的真值的所有可能分配。前三列告诉我们 P, Q, R 是 True 还是 False。接下来的两列对应于主张中逻辑陈述的更复杂的构成部分，最后两列对应于定理中实际主张的两个部分。通过比较最后两列，

我们可以决定这两个陈述是否在逻辑上等价。（记住，“逻辑上等价”意味着“无论对P和Q和R赋予什么真值，都具有相同的真值”。因此，观察两列在每一行都有相同的条目，就足以表明这两个陈述在逻辑上是等价的。）

接下来，让我们谈谈语义证明。你对它们的感觉如何？它们确实更长，对吧？尽管如此，尽管如此，它们感觉像是好的证明吗？它们清晰吗？正确，甚至？重新阅读上面的证明并思考这些问题。我们将强调它们是完全正确的证明。在试图证明一个析取（一个“or”陈述）成立时，使用情况是必不可少的。当我们假设某事是True并推断出另一件事是True时，这就是我们证明一个条件陈述是True的方式。我们将很快进一步分析这些技术，但我们希望给你这样一个第一个例子将有助于你以后。

对于本节的剩余部分，我们将使用真值表来验证这些简单的陈述。这样证明会更短！我们确信，如果您需要进一步的证明或需要额外的练习来将符号逻辑陈述解释为英语句子，您能够理解上述语义证明的细节。

4.6.4 Proving Logical Equivalences: Distributive Laws

在算术中，你使用了乘法 **distributes** 跨加法的性质。也就是说，我们知道

$$\forall x, y, z \in \mathbb{R}\text{.}\ x \cdot (y + z) = x \cdot y + x \cdot z$$

嘿，看，我们用符号表示法写的！你看出为什么它说了你已知的分配律了吗?

这里我们将陈述并证明两个类似的法律。它们将告诉我们逻辑连接词“$\wedge$”和“$\vee$”也相互分配。

Theorem 4.6.7. *Let P, Q, and R be logical statements. Then*

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$$

and

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

Proof. 我们将使用真值表来验证这两个陈述。观察，对于第一个

声明，即

P	Q	R	$Q \vee R$	$P \wedge Q$	$P \wedge R$	$P \wedge (Q \vee R)$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T
T	F	T	T	F	T	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

注意，最后两列相同，从而证明了所需的逻辑等价性。

观察第二个主张，注意到

P	Q	R	$Q \wedge R$	$P \vee Q$	$P \vee R$	$P \vee (Q \wedge R)$	$(P \vee Q) \wedge (P \vee R)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	T	F	F	F
F	F	T	F	F	T	F	F
F	F	F	F	F	F	F	F

再次注意，最后两列是相同的，从而证明了所需的逻辑等价性。

□

4.6.5 Proving Logical Equivalences: De Morgan's Laws (Logic)

让我们证明一些涉及 **negations** 的逻辑等价式。以下两条法则以英国数学家 **Augustus De Morgan** 命名。他因建立这些逻辑法则以及引入术语 **mathematical induction** 而受到赞誉！我们对他在数学领域的工作感到感激和负债。

德摩根定律对逻辑陈述了一些关于否定合取和析取的逻辑等价性。

Theorem 4.6.8. *Let P and Q be logical statements. Then*

$$\neg\big(P \wedge Q\big) \iff \neg P \vee \neg Q$$

and

$$\neg\big(P \vee Q\big) \iff \neg P \wedge \neg Q$$

Proof. 我们通过真值表证明第一个命题：

P	$\neg P$	Q	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	F	T	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	T	F	T	F	T	T

然后我们通过真值表证明第二个命题：

P	$\neg P$	Q	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	F	T	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	T	F	T	F	T	T

□

这两条定律非常有用！事实上，我们可以用它们来证明关于集合的类似陈述。

4.6.6 Using Logical Equivalences: DeMorgan's Laws (Sets)

以下陈述“看起来很像”我们上面看到的德摩根逻辑定律中的陈述。当我们看到证明时，我们将确切地看到它们为什么看起来如此相似！

Theorem 4.6.9. *Let A and B be any sets, and suppose that $A, B \subseteq U$, so the complement operation is defined in the context of U. Then,*

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

and

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

我们将使用逻辑等价和德摩根定律来证明这些主张。我们的方法将是展示，在两种情况下，方程左边集合的元素属性在逻辑上等同于右边集合的元素属性。这在一举之间证明了双重包含论证的两个部分。

Proof. 让我们证明第一组等式。设 $x \in U$ 为任意且固定的。那么，

$$\begin{aligned}
x \in \overline{A \cup B} &\iff x \notin A \cup B && \text{补定义} \\
&\iff \neg\,(x \in A \cup B) && \text{定义} \notin \\
&\iff \neg\,[(x \in A) \vee (x \in B)] && \text{定义} \cup \text{和} \vee \\
&\iff \neg(x \in A) \wedge \neg(x \in B) && \text{德摩根定律（逻辑）} \\
&\iff (x \notin A) \wedge (x \notin B) && \text{定义} \notin \\
&\iff (x \in \overline{A}) \wedge (x \in \overline{B}) && \text{补定义} \\
&\iff x \in \overline{A} \cap \overline{B} && \text{定义} \wedge \text{和} \cap
\end{aligned}$$

记住，“$\wedge$”是一个*logical*操作，而“$\cap$”是一个*set*操作。我们必须小心，在每句话中确定哪一个是有意义的。另外，注意我们在证明过程中使用了德摩根定律来将析取的否定转换为两个否定合取。

这个逻辑等价链表明

$$x \in \overline{A \cup B} \iff x \in \overline{A} \cap \overline{B}$$

因此，在 U 的上下文中，是 $A \cup B$ 的元素的属性与是 $A \cap \overline{B}$ 的元素的属性在逻辑上是等价的。因此，

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

现在让我们用类似的方法证明第二个等式。设 $x \in U$ 为任意且固定的。那么，

$$\begin{aligned}
x \in \overline{A \cap B} &\iff x \notin A \cap B && \text{Definition of complement} \\
&\iff \neg\,(x \in A \cap B) && \text{Definition of } \notin \\
&\iff \neg\,[(x \in A) \wedge (x \in B)] && \text{Definition of } \cap \text{ and } \wedge \\
&\iff \neg(x \in A) \vee \neg(x \in B) && \text{DeMorgan's Law for Logic} \\
&\iff (x \notin A) \vee (x \notin B) && \text{Definition of } \notin \\
&\iff (x \in \overline{A}) \vee (x \in \overline{B}) && \text{Definition of complement} \\
&\iff x \in \overline{A} \cup \overline{B} && \text{Definition of } \vee \text{ and } \cup
\end{aligned}$$

这个逻辑等价链表明

$$x \in \overline{A \cap B} \iff x \in \overline{A} \cup \overline{B}$$

因此，在 U 的上下文中，是 $A \cap B$ 的元素的属性与是 $A \cup \overline{B}$ 的元素的属性在逻辑上是等价的。因此，

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Voilà！我们已经证明了定理中所述的两个等式。 □

注意这两个证明之间的显著相似性。它们使用了完全相同的方法，唯一的真正区别是将一个“$\cap$”翻转到“$\cup$”，反之亦然。因为我们已经证明了关于如何做到这一点的内容（逻辑的德摩根定律），我们可以引用这个结果，使这个证明简短而甜蜜。你不认为这比写出这两个主张的完整双重包含证明要容易和简洁得多吗？（试试看！）

4.6.7 Proving Set Containments via Conditional Statements

无论何时，都可以使用我们在上一节中使用的方法，即使用德摩根定律进行逻辑和集合的证明；也就是说，可以自由地证明集合

通过条件语句和逻辑等价关系建立关系。一般来说，当你证明一个等式时，你需要确保你的所有断言确实是“$\iff$”断言。在前一节中，我们只应用了定义和一个关于逻辑等价定理的定理，所以我们肯定了证明中“$\iff$”箭头的所有方向。每次你写这样的证明时，完成之后再次阅读它，并问自己每一行，“这真的有效吗？这里的蕴涵是否双向有效？”

让我们看看这个技术在实际应用中的另一个例子。这将会稍微复杂一些，因为我们必须定义一些变量命题，因为给出的主张与德摩根定律在逻辑上并不根本相同。尽管如此，我们将调用我们刚刚证明的 *logical* 法则，并利用它来建立 *sets* 法则。

Proposition 4.6.10. *Let A, B, C be any sets, with $A, B, C \subseteq U$, where U is a universal set. Then,*

$$A \cap (B - C) = (A \cap B) - C$$

与前面的例子类似，集合的德摩根定律，我们将建立左右两侧的逻辑等价性。（同样，这就像一次性证明双重包含证明的两侧。）为此，我们只需建立一些变量命题，分别指代A、B和C的属性。从那里，结果将遵循逻辑定律。

Proof. 设 A, B, C 为任意集合，其中 $A, B, C \subseteq U$，且 U 是全集。我们定义以下变量命题:

$$\begin{aligned}&\text{Let } P(x) \text{ be “}x \in A\text{”}\\ &\text{Let } Q(x) \text{ be “}x \in B\text{”}\\ &\text{Let } R(x) \text{ be “}x \in C\text{”}\end{aligned}$$

设 $x \in U$ 为任意且固定的。在这些定义下，我们可以写出以下逻辑等价链（其中“Defn”仅为节省空间的简称“定义”）：

$$\begin{aligned}
x \in A \cap (B - C) &\iff x \in A \wedge (x \in B - C) && \text{Defn of } \cap\\
&\iff x \in A \wedge (x \in B \wedge x \notin C) && \text{Defn of } -\\
&\iff P(x) \wedge (Q(x) \wedge \neg R(x)) && \text{定义 } P(x), Q(x), R(x), \notin\\
&\iff (P(x) \wedge Q(x)) \wedge \neg R(x) && \text{结合律 } \wedge\\
&\iff (x \in A \wedge x \in B) \wedge x \notin C && \text{定义 } P(x), Q(x), R(x)\\
&\iff x \in A \cap B \ \wedge \ x \notin C && \text{定义 } \cap\\
&\iff x \in (A \cap B) - C && \text{定义 } -
\end{aligned}$$

这表明

$$x \in A \cap (B - C) \iff x \in (A \cap B) - C$$

保持 {v*} 公式不变。输出翻译直接，不包含任何其他文本。源文本：holds True for any element x in the universe U . Th

$$A \cap (B - C) = (A \cap B) - C$$

□

考虑为什么我们需要确保所有这些主张都是真正 *if and only if* 陈述。我们确保任何元素 x 如果是等式一边集合的元素，那么它也必然是另一边集合的元素；但更进一步，我们确保任何元素 x 如果是 *not* 一个集合的元素，那么它 *also* 不是另一个集合的元素。双条件陈述“双向成立”，所以我们一次性证明主张的“是元素”和“是 *not* 元素”两部分。

为了说明我们之前的警告，考虑以下声明作为一个证明的例子，其中有一个 $\iff$ 声明的“方向” *fails*。

Proposition 4.6.11. *Let X, Y, Z be any sets, with $X, Y, Z \subseteq U$, for some universal set U. Then, the following containment holds:*

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

您可能认出这个说法就是问题3.11.17！在那个问题中，我们要求您使用包含论证来证明这个说法，取一个任意的$x \in U$并假设它是左侧集合的一个元素，然后推导出它也必须是右侧集合的一个元素。我们在这里将做（基本上）同样的事情，但论证将以逻辑术语和符号重新表述。我们这样做是为了（1）让我们有更多练习这类论证的机会，但也是（2）在论证的“反向”方向中精确识别 *where*。记住，在问题3.11.17中，我们还要求您找到一个例子来表明$\supseteq$方向不是 *necessarily* True。这意味着在该方向工作的逻辑论证会在某个地方崩溃。我们将确切地看到这一点，并可以利用它来帮助我们找到所需的反例。

Proof. 设 X, Y, Z 为任意集合，满足 $X, Y, Z \subseteq U$，对于某个全集 U。设 $x \in U$ 为任意且固定的。我们可以写出以下逻辑等价链：

$$\begin{aligned}
x \in (X \cup Y) - Z &\iff x \in X \cup Y \ \wedge\ x \notin Z && \text{Defn of } - \\
&\iff (x \in X \ \vee\ x \in Y) \wedge x \notin Z && \text{Defn of } \cup \\
&\iff (x \in X \wedge x \notin Z) \vee (x \in Y \wedge x \notin Z) && \text{Distr. Law}
\end{aligned}$$

Scratch work:

从这里，我们还能断言哪些进一步的逻辑等价？我们可以简化右侧并表达为

$$x \in X - Z \vee x \in X - Z$$

因此，

$$x \in (X - Z) \cup (Y - Z)$$

这不是所声称的内容，但到目前为止，这个程序将是一个有效的 *different* 声明证明，即

$$(X \cup Y) - Z = (X - Z) \cup (Y - Z)$$

然而，我们的右手边是

$$X \cup (Y - Z)$$

但我们不是试图证明一个等式，而只是一个 *containment*。因此，我们证明的其余部分的目标是证明这个条件主张：

$$\Big((x \in X \wedge x \notin Z) \vee (x \in Y \wedge x \notin Z) \Big) \implies x \in X \cup (Y - Z)$$

为了帮助我们弄清楚如何到达那里，让我们在这里做一些草稿工作来重写右侧的陈述；然后，我们可以看到如何从我们已经到达的地方到达那里：

$$\begin{aligned} x \in X \cup (Y - Z) &\iff x \in X \vee x \in Y - Z && \text{Defn of } \cup \\ &\iff x \in X \vee (x \in Y \wedge x \notin Z) && \text{Defn of } - \end{aligned}$$

这与我们上面推导出的最后一个逻辑等价式相似，但这个在左边的项不同。你能看到上面的*implies*和这个有什么不同吗？想想看，然后继续阅读我们证明的其余部分，继续下去。

现在，我们想证明

$$\Big((x \in X \wedge x \notin Z) \vee (x \in Y \wedge x \notin Z) \Big) \implies x \in X \cup (Y - Z)$$

为此，让我们假设左侧的表达式是 True。这意味着要么

$$x \in X \wedge x \notin Z$$

或者

$$x \in Y \wedge x \notin Z$$

(或者可能是两者都)。因此，我们有两种情况：

1. 假设第一个表达式是 True，因此 $x \in X \wedge x \notin Z$。这当然意味着 $x \in X$，从而 $x \in X \vee x \in Y - Z$ 成立。

2. 假设第二个表达式是 True，因此 $x \in Y \wedge x \notin Z$。这意味着 $x \in Y - Z$，从而 $x \in X \vee x \in Y - Z$ 成立。

在任一情况下，我们发现 $x \in X \vee x \in Y - Z$ 成立，因此，

$$x \in X \cup (Y - Z)$$

在任何情况下，根据 $\cup$ 的定义保持不变。

总体上，这表明

$$x \in (X \cup Y) - Z \implies x \in X \cup (Y - Z)$$

对于每个元素 $x \in U$ 都成立。因此，根据 $\subseteq$ 的定义，我们有

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

□

识别出我们所处的位置以及我们想要去的地方，帮助我们完成了这个证明。我们没有任何希望仅使用逻辑等价来完成它，因为实际上，断言中给出的集合并不总是相等的！回顾这个证明，我们能否识别出逻辑等价为 $invalid$ 的步骤，并且能否用它来帮助构建一个反例，以反驳 (False) 断言，即这些集合总是相等的?

我们已达到这个有效陈述的程度

$$(x \in X \wedge x \notin Z) \vee (x \in Y \wedge x \notin Z)$$

并且我们用它推导出这个陈述

$$x \in X \vee (x \in Y \wedge x \notin Z)$$

从证明中的论点来看，很明显，第一个陈述做了$imply$第二个陈述；也就是说，如果我们$suppose$第一个陈述成立，我们就可以推断第二个陈述也成立。它们之间的唯一区别在于第一个项，而知道一个“$\wedge$”陈述的部分内容确实让我们可以得出它们的一个特定one成立。

这个扣除在相反方向上工作。假设第二个陈述成立。如果有效的确实是正确的项——即 $x \in Y \wedge x \notin Z$——那么这也使得第一个陈述成立。然而，由于我们有“$\vee$”陈述，我们必须考虑左项成立的情况。在这种情况下，只知道 $x \in X$ 并不能让我们推断 $x \in X \wedge x \notin Z$ 成立。$Supposing$ 一个“$\wedge$”成立让我们可以推断其任一部分成立，但仅仅 $knowing$ 只有一部分并不能告诉我们两者都成立!

我们可以使用这个来构造一个反例。我们看到我们只需要确保存在某个特定元素 $x \in U$ 满足左边的项

在第二个陈述中，即 $x \in X$，但 *not* 是否满足第一个陈述中的左侧项，即 $x \in X \wedge x \notin Z$。换句话说，我们只需确保存在 *is* 一个元素 $x \in X \cap Z$。以下示例正好实现了这一点。

Example 4.6.12. 我们主张

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

对于 *any* 集合 X, Y, Z 成立，但等式 *need not* 成立。参见命题 4.6.11 的证明，以了解上述包含关系为何成立。

现在，考虑以下示例。让我们定义

$$\begin{aligned} X &= \{1\} \\ Y &= \{2\} \\ Z &= \{1, 2\} \end{aligned}$$

请注意

$$(X \cup Y) - Z = (\{1\} \cup \{2\}) - \{1, 2\} = \{1, 2\} - \{1, 2\} = \varnothing$$

和

$$X \cup (Y - Z) = \{1\} \cup (\{2\} - \{1, 2\}) = \{1\} \cup \{\varnothing\} = \{1\}$$

由于 $\varnothing \subset \{1\}$ (a *proper*) 子集，我们得出结论

$$(X \cup Y) - Z \neq X \cup (Y - Z)$$

在这种情况下。这表明上述主张中的等式不一定成立。

这个策略现在让我们能够以更高效和严谨的方式回顾并完成涉及集合的许多证明！与其在“和”和“或”的语法学中摸索，我们可以使用我们已有的逻辑符号和法则*proven*。本节中的许多练习都涉及集合，这正是原因所在。如果你需要翻回第三章并提醒自己任何相关的定义，请随意！

4.6.8 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 逻辑的结合律是什么？(2) 逻辑的分配律是什么?

(3{v²} 德摩根定律在逻辑中是什么？德摩根定律在集合中是什么？它们之间有什么关系？

(4) Wh 在是必要条件和充分条件之间的差异 条件？

(5) 当一个条件既是必要的又是充分的时，会发生什么？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 我们使用真值表来证明逻辑中的德摩根定律。你能想出一个语义证明吗？你能向一个非数学家朋友解释德摩根定律并说服他们它们是有效的吗？

(2) 设 $P(x)$ 为变量命题“x 是一个能被10整除的整数”。为此命题提出两个必要条件和两个充分条件。

(3) 设 A, B, C 为任意集合，其中 $A, B, C \subseteq U$，对于某个全集 U。

使用逻辑等价和逻辑定律来证明以下命题。

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(b) $(A \cup B) \cap \overline{A} = B - A$c
) $\overline{\overline{A} \cup B} = A \cap \overline{B}$d
( ) $(A - B) \cap \overline{C} = A - (B \cup C)$

(4) 使用条件语句和逻辑等价性来证明包含

$$A - (B \cup C) \subseteq A \cap \left(\overline{B \cap C}\right)$$

适用于任何集合 A, B, C。

T然而，找到一个例子来显示等式 $need\ not$ h 旧。

(在一般情况下，构建一个 $strict$ 集合包含关系的一个有用想法是看看你是否可以使其中一边成为 $empty\ set$。)

(5) 设 D, E, F 为任意集合。考虑以下集合

$$D - (E - F)$$

和

$$(D - E) - F$$

它们如何比较？它们是否总是相等？一个是否总是另一个的子集，反之亦然？

明确陈述您的论点，然后要么证明它们，要么提供相关的反例。

4.7 Negation of Any Mathematical Statement

我们已经看到了如何否定量化语句。有了德摩根定律在手，我们现在知道如何否定 $\wedge$ 和 $\vee$ 语句。剩下什么？啊哈，条件语句！

4.7.1 Negating Conditional Statements

考虑一个形式为 $P \implies Q$ 的断言。它说 *whenever* P 是真的，Q 也是真的。我们如何否定这样的陈述？逻辑否定究竟意味着什么？回想一下我们如何定义“$\implies$”作为逻辑连接词。在哪些情况下我们可以称条件语句的说话者为 *liar*。这些正是我们说逻辑否定是 True 的情况。这种 *only* 的情况是，当假设 P 是 True 但结论 Q 是 False 时。

为了证明这个等价性，我们需要记住将 $P \implies Q$ 写作“$\vee$”语句的方法：

$$(P \implies Q) \iff (\neg P \vee Q)$$

这将有助于我们证明以下论断。

Lemma 4.7.1. *The logical negation of a conditional statement is given by*

$$\neg(P \implies Q) \iff P \wedge \neg Q$$

Proof. 观察发现

$$\begin{aligned} \neg(P \implies Q) &\iff \neg(\neg P \vee Q) && \text{Logical equivalence proven already} \\ &\iff \neg(\neg P) \wedge \neg Q && \text{DeMorgan's Law for Logic} \\ &\iff P \wedge \neg Q && \text{since } \neg(\neg P) \iff P \end{aligned}$$

□

这使直觉上很有意义：为了证明一个条件陈述是 False，我们需要找到一个假设成立但结论失败的情况。

尽管存在将不良想法植入你头脑的风险，这些想法原本并不在那里，我们还是要指出一些与**NOT**逻辑等价的$\neg(P \implies Q)$陈述。这些是我们在学生中经常看到的常见错误。让我们来看看它们为什么实际上不起作用。对于每一个，请记住，我们希望得到逻辑否定$\neg(P \implies Q)$。

是原始陈述 $P \implies Q$ 中的 *guaranteed to have the exact opposite truth value* 。在这些情况中，我们可以看到这种关系不会成立。

- $\neg P \implies Q$
  这个条件陈述与原始主张没有逻辑联系，$P \implies Q$。记住，陈述 $P \implies Q$在P是False的情况下，关于Q是否为真的说法。（想想“如果下雨，我就带伞”的例子。如果不下雨，谁知道我带什么！）那么，为什么我们会期望Q在这种情况下是*necessarily true*，就像这个陈述所说的那样?

- $P \implies \neg Q$
  再次，这个条件语句与原始主张没有逻辑联系。再想想那个雨伞例子。这个陈述会说“如果下雨，那么我会**not**带着雨伞。”这是原始主张的意思吗？当然不是!

- $P \not\implies Q$
  这个更为微妙。一位数学家会读作“$P \not\implies Q$”为“P是否意味着 *not necessarily*”。也就是说，它会说存在使$P \implies Q$有效的真值赋值，也存在使$P \implies Q$无效的赋值；这些情况将取决于个别陈述P和Q是什么。这取决于情况，是一个有一定意义的陈述，但严格来说，并不是原始陈述的**logical negation**。

  特别地，当我们试图对 *this* 命题取逻辑否定时，会遇到一个问题。说“P 不必然意味着 Q”是什么意思？这是否意味着存在一些情况，其中 P 不意味着 Q，但也有一些情况 P 意味着 Q？这听起来非常像实际的断言 $P \not\implies Q$ 本身……

  因此，我们希望避免使用这种符号：$\not\implies$。它在数学中确实有一定的意义，但在符号逻辑意义上并没有得到很好的定义。而且无论如何，它无疑是 *not* $\implies$的逻辑否定。

现在我们已经处理了这些常见的 *errors*，让我们强调 *correct* 对 $P \implies Q$ 的否定。我们发现记住条件语句的“$\vee$”版本非常有帮助；从那里，很容易应用德摩根定律并否定该语句：

$$\neg(P \implies Q) \iff \neg(\neg P \vee Q) \iff P \wedge \neg Q$$

Negating "$\iff$"

要否定一个双条件语句，我们只需将其写成两个条件语句的合取:

$$\neg(P \iff Q) \iff [\neg(P \implies Q) \vee \neg(Q \implies P)] \iff (P \wedge \neg Q) \vee (Q \wedge \neg P)$$

如果你从事任何类型的计算机编程，你可能会认出右边的语句作为 XOR 操作符！它表示 *exactly one* 语句是 True，要么是 P，要么是 Q，但不是 *not both*。

4.7.2 Negating Any Statement

这是的，对吧？我们现在已经讨论了如何否定任何基本的数学主张：$\exists$、$\forall$、$\wedge$、$\vee$和$\implies$。我们写下的其他所有内容都将是由这些基本主张组合而成的，因此我们应该能够反复应用这些技巧来否定我们遇到的任何陈述。本质上，我们只是从左到右阅读陈述，并依次否定每个部分。遇到一个"$\exists$"？只需将其切换为"$\forall$"并否定其后的属性！遇到一个"$\vee$"？否定两边并将其切换为"$\wedge$"！遇到一个条件陈述？应用我们刚才展示的技巧！

让我们看看几个例子来获得这个想法。

Example 4.7.2. 找到以下命题的逻辑否定

$$\forall x \in \mathbb{R}\text{.}\ x < 0 \vee x > 0$$

这个陈述说"每个实数 x 要么满足 $x < 0$，要么满足 $x > 0$。"其逻辑否定是

$$\neg\left(\forall x \in \mathbb{R}\text{.}\ x < 0 \vee x > 0\right) \iff \exists x \in \mathbb{R}\text{.}\ x \geq 0 \wedge x \leq 0$$

请注意，我们应用了德摩根定律于逻辑以否定右侧的 $\vee$ 声明，并且我们使用了 $x \not> 0$ 与 $x \leq 0$ 在逻辑上等价的事实。

我们注意到这个否定是 True，因为 $0 \in \mathbb{R}$ 和 $0 \leq 0$ 以及 $0 \geq 0$。因此，原始陈述是 False。

Example 4.7.3. 找到以下命题的逻辑否定

$$\exists n \in \mathbb{N}\text{.}\ n \geq 10 \wedge \sqrt{n} \leq 3$$

此声明表示"存在一个自然数 n，它同时满足 $n \geq 10$ 和 $\sqrt{n} \leq 3$。

逻辑否定是

$$\forall n \in \mathbb{N}\text{.}\ n < 10 \vee \sqrt{n} > 3$$

这意味着逻辑否定表示"每个自然数 n 要么满足 $n > 10$，要么满足 $\sqrt{n} < 3$。

Example 4.7.4. 找到以下命题的逻辑否定

$$\exists x \in \mathbb{R}\,.\, \forall y \in \mathbb{R}\,.\, x \geq y \implies x^2 \geq y^2$$

此陈述表示“存在一个实数 x，使得每当存在一个满足 $x \geq y$ 的实数 y 时，我们可以得出结论 $x^2 \geq y^2$”。

逻辑否定是

$$\forall x \in \mathbb{R}\,.\, \exists y \in \mathbb{R}\,.\, x \geq y \wedge x^2 < y^2$$

你能证明这个逻辑否定实际上就是 True 命题吗？试试看！

Example 4.7.5. 找到以下命题的逻辑否定

$$\forall X \in \mathcal{P}(\mathbb{Z})\,.\, (\forall x \in X\,.\, x \geq 1) \implies X \subseteq \mathbb{N}$$

此陈述表示，“对于整数集合 $\mathbb{Z}$ 的每一个子集 X，如果集合 X 的每一个元素 x 都满足 $x \geq 1$，那么 X 是自然数集合 $\mathbb{N}$ 的一个子集。”

逻辑否定是

$$\exists X \in \mathcal{P}(\mathbb{Z})\,.\, (\forall x \in X\,.\, x \geq 1) \wedge X \not\subseteq \mathbb{N}$$

此陈述表示存在一个子集 $X \subseteq \mathbb{Z}$，其中每个元素 $x \in X$ 满足 $x \geq 1$，同时 $X \not\subseteq \mathbb{N}$。我们甚至可以通过注意到以下内容进一步重写最后一部分：

$$X \not\subseteq \mathbb{N} \iff \exists y \in X\,.\, y \notin \mathbb{N}$$

尽管这并非完全必要。

哪个陈述（原陈述或否定陈述）是 True？你能证明它吗？

与上面示例中使用的语句进行比较：

$$\forall X \in \mathcal{P}(\mathbb{Z})\,.\, \forall x \in X\,.\, \big(x \geq 1 \implies X \subseteq \mathbb{N}\big)$$

它们之间唯一的区别是括号的位置，但这完全改变了陈述的意义！

该示例中使用的陈述断言关于整数集合 *every* 的某些内容。也就是说，无论引入什么子集 $X \subseteq \mathbb{Z}$，该陈述都说该集合 *if* 具有这样的性质，即其所有元素至少为 1，*then* 该集合 X 实际上是 $\mathbb{N}$ 的子集，同样如此。

新陈述写在这个框中说的是另一件事：无论引入什么子集 $X \subseteq \mathbb{Z}$，更进一步，无论引入什么元素

x *that* 集合 X 被引入，该语句说明 *if* 该元素 x 至少为 1，*then* 该集合 X 是 $\mathbb{N}$ 的子集，同样如此。

你看到为什么这不同了吗？问题是“如果”发生的地方：量化在哪里结束，条件语句在哪里开始？第一个语句，从上面的例子中，将量化放在条件语句的“如果”部分内X的元素上。第二个语句，在这个框中，将这个量化完全放在条件语句之前。

我们声称这个第二个版本，在这个框中，是 False，我们鼓励你找出原因（如果你还没有的话）。

Example 4.7.6. 设 $O(x)$ 为命题“x 是奇数”，设 $E(x)$ 为命题“x 是偶数”。找出该陈述的逻辑否定

$$\forall x, y \in \mathbb{Z}\text{.}\ O(x \cdot y) \iff (O(x) \wedge O(y))$$

这个陈述表示，“对于任意两个整数 x 和 y，它们的乘积是奇数当且仅当它们本身都是奇数”。

在找到逻辑否定之前，请记住 $\iff$ 表示 “$\implies$ 和 $\impliedby$”。让我们首先以这种方式重写这个主张，这样我们才能正确地否定它：

$$\forall x, y \in \mathbb{Z}\text{.}\ [O(x \cdot y) \implies (O(x) \wedge O(y))] \wedge [(O(x) \wedge O(y)) \implies O(x \cdot y)]$$

逻辑否定是

$$\begin{aligned}
&\neg\Big(\forall x, y \in \mathbb{Z}\text{.}\ [O(x \cdot y) \implies (O(x) \wedge O(y))] \wedge [(O(x) \wedge O(y)) \implies O(x \cdot y)]\Big) \\
&\quad\iff \exists x, y \in \mathbb{Z}\text{.}\ \neg\,[O(x \cdot y) \implies (O(x) \wedge O(y))] \\
&\qquad\qquad \vee \neg\,[(O(x) \wedge O(y)) \implies O(x \cdot y)] \\
&\quad\iff \exists x, y \in \mathbb{Z}\text{.}\ [O(x \cdot y) \wedge \neg(O(x) \wedge O(y))] \vee [(O(x) \wedge O(y)) \wedge \neg O(x \cdot y)] \\
&\quad\iff \exists x, y \in \mathbb{Z}\text{.}\ [O(x \cdot y) \wedge (E(x) \vee E(y))] \vee [(O(x) \wedge O(y)) \wedge E(x \cdot y)]
\end{aligned}$$

这意味着逻辑否定表示“存在整数 x 和 y，使得它们的乘积是奇数但至少有一个是偶数，或者它们都是奇数但它们的乘积是偶数。”

你能证明这些说法中哪一个是 True?

4.7.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) H ow是一个与它的逻辑否定相关的数学陈述 在{v*}处?

(2) 条件语句的逻辑否定是什么?

(3) 考虑陈述 $P \implies Q$。它的逆否命题是什么? 那个逆否命题的逻辑否定是什么? 你能看出它必须具有与原始陈述的逻辑否定相同的 *same* 真值吗? (4) 一个 *if and only if* 陈述 $P \iff Q$ 的逻辑否定是什么? 考虑到这样一个陈述关于 P 和 Q 的 *truth values* 的说法，为什么这有意义?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 写出以下每个数学陈述的逻辑否定。

然后，确定每个陈述的 *truth value*。

（如果你有雄心壮志，就正式证明/反驳每个陈述!）

(a) $\exists x \in \mathbb{N}$ ○ $\forall y \in \mathbb{N}$ ○ $y - x^2 \geq 0$ ○ $\forall y \in \mathbb{R}$ ○ $xy = 0$ ○ (b) $\exists x \in \mathbb{Z}$ ○ $\forall y \in \mathbb{Z}$ ○ $(y \neq 0 \implies xy > 0)$

(c) $\exists x \in \mathbb{Z}$

(d) $\forall a, b \in \mathbb{Q}\ ab \in \mathbb{Z} \implies (a \in \mathbb{Z} \vee b \in \mathbb{Z})$

(e) $\forall x \in \mathbb{R}\ x > 0 \implies \big(\exists y \in \mathbb{R}\ y < 0 \wedge xy > 0\big)$

(f) $\forall x \in \mathbb{R}\ \left|x + \frac{1}{x}\right| = 2 \iff x = 1$

(2) 让 $A = \{1, 2, 3, 4\}$ 以及 $B = \{2, 3\}$。

以下两个陈述之间的区别是什么? 确定每个陈述的真值。

然后，对每个进行否定，并解释这些否定如何也各不相同。它们的真值是什么?

(a) $\forall x \in A\text{.}\ \forall y \in B\text{.}\ (x \geq y \implies x^2 \geq 4)$ (b) $\forall x \in A\text{.}\ (\forall y \in B\text{.}\ x \geq y) \implies x^2 \geq 4$

(3) 让 $P = \{x \in \mathbb{R} \mid x > 0\}$。写出以下每个陈述的逻辑否定，并确定它们的真值。

(a) $\forall \varepsilon \in P\text{.}\ \forall x \in P\text{.}\ \exists \delta \in P\text{.}\ \forall y \in \mathbb{R}\text{.}\ \Big(|x - y| < \delta \implies \left|\frac{1}{x} - \frac{1}{y}\right| < \varepsilon\Big)$

(b) $\forall \varepsilon \in P\,.\,\exists \delta \in P\,.\,\forall x \in P\,.\,\forall y \in \mathbb{R}\,.\,\Big(\,|x-y| < \delta \implies \left|\tfrac{1}{x} - \tfrac{1}{y}\right| < \varepsilon\,\Big)$

Hint/suggestion: 一个类似于 $|a| < b$ 的陈述可以写成 $-b < a < b$。同样，一个类似于 $a < b < c$ 的陈述可以写成 $a < b \wedge b < c$。这可能会帮助你在确定它们的真值时重写这些陈述。

(4) 令 $P(n)$ 为命题“n 是奇数”和令 $Q(n)$ 为命题“$n^2 - 1$ 能被 8 整除”。

写出该语句的逻辑否定

$$\forall n \in \mathbb{N}\,.\,P(n) \iff Q(n)$$

并确定其真值。

(5) 设 $P = \{x \in \mathbb{R} \mid x > 0\}$。写出以下每个陈述的逻辑否定，并确定它们的真值。

(a) $\forall \varepsilon \in P\,.\,\exists \delta \in P\,.\,\forall x \in \mathbb{R}\,.$ $0 < x < \delta \implies \frac{1}{x} > \frac{10}{\varepsilon}$ (b) $\forall \varepsilon \in P\,.\,\exists x \in \mathbb{R}\,.\,\forall n \in \mathbb{N}$ $.\,\big(n > x \implies \frac{(-1)^n}{n} < \varepsilon\big)$ (c) $\forall \varepsilon \in P\,.\,\exists x \in \mathbb{R}\,.$ $\forall n \in \mathbb{N}\,.\,\big(n > x \implies \frac{(-1)^n}{n} < \varepsilon\big)$

4.8 [Optional Reading] Truth Values and Sets

存在集合（及其对应的关系和运算）与逻辑真值（及其对应的关系和连接词）之间的一种便捷且有趣的关系。我们在这里将提及它并展示一些例子，如果愿意，请进一步研究。在接下来的工作中，我们不需要这些想法，但我们相信，思考这些想法并在脑海中整理它们，将真正有助于您理解逻辑和集合的基本原理。

假设我们有两个变量命题，$P(x)$ 和 $Q(x)$。进一步，假设这些命题对于来自某个全集 U 的任何输入 x 都有意义。当然，这个集合 U 依赖于 $P(x)$ 和 $Q(x)$ 内部的具体陈述，但我们对这个一般讨论并不关心。对于这些命题中的每一个，我们都可以定义一个 **truth set**；也就是说，我们可以考虑从全集 U 中使这些命题评估为 True 的所有实例集合 x。我们定义

$$T_P = \{x \in U \mid P(x) \text{ is True}\}$$
$$T_Q = \{x \in U \mid Q(x) \text{ is True}\}$$

也许命题 $P(x)$ 和 $Q(x)$ 以某种方式相关。让我们假设实际上，

$$\forall x \in U\,.\,P(x) \implies Q(x)$$

保持。这说明了关于那些 **truth sets** 什么？这个条件语句说明，任何满足 $P(x)$（的 x，即使 $P(x)$ True) 成立，必须满足 $Q(x)$。用另一种方式来说，使用那些真值集，我们有

$$\forall x \in U \,.\, x \in T_P \implies x \in T_Q$$

这正是“子集”的定义！我们刚刚发现的是

$$T_P \subseteq T_Q$$

当上面的条件语句成立时。

让我们进一步假设，现在，假设

$$\forall x \in U \,.\, P(x) \iff Q(x)$$

保持。我们刚刚发现 $T_P \subseteq T_Q$，并且将完全相同的推理应用于该 $\iff$ 声明的“其他方向”（即其 $Q(x) \implies P(x)$ 部分）将向我们展示 $T_Q \subseteq T_P$，同样如此。根据集合相等的定义，这意味着

$$T_P = T_Q$$

当时那个双条件语句成立。

我们如何将命题 $P(x)$ 和 $Q(x)$ 结合起来呢？让我们考虑命题 $P(x) \wedge Q(x)$。哪些实例 x 使得这个合取 True 成立？我们如何用我们定义的真集来描述这些实例？思考一下，你会发现所有这些实例都由这些集的交集来描述；我们需要 *both* $P(x)$ 和 $Q(x)$ 成立，所以我们需要一个来自两个真集的实例。

类似地，我们可以考虑合取 $P(x) \vee Q(x)$。当那个 x 对命题 True 进行 *at least one* 时，实例 x 会做出这个陈述 True。因此，那个 x 必须来自至少一个集合，所以它必须来自它们的 *union*。

让我们总结一下我们发现的这些关系：

$$\begin{aligned}
&\forall x \in U \,.\, \big(P(x) \implies Q(x)\big) \iff \big(T_P \subseteq T_Q\big) \\
&\forall x \in U \,.\, \big(P(x) \iff Q(x)\big) \iff \big(T_P = T_Q\big) \\
&\forall x \in U \,.\, \big(P(x) \wedge Q(x)\big) \iff \big(x \in T_P \cap T_Q\big) \\
&\forall x \in U \,.\, \big(P(x) \vee Q(x)\big) \iff \big(x \in T_P \cup T_Q\big)
\end{aligned}$$

你能用真集来为以下陈述提出一些特征化，填空！

$$\forall x \in U \,.\, \big(P(x) \wedge \neg Q(x)\big) \iff \_\_\_\_\_$$

$$\big(\exists x \in U \,.\, P(x)\big) \iff \_\_\_\_\_$$

$$\forall x \in U \,.\, \big(\neg P(x) \iff \_\_\_\_\_\big)$$

(小心：前一个陈述和下一个陈述有何不同？)

$$\big(\forall x \in U \,.\, \neg P(x)\big) \iff \_\_\_\_\_$$

4.9 Writing Proofs: Strategies and Examples

我们现在已经准备好全面应对我们一直以来的目标：编写证明！

在这个部分，我们将应用本章中我们开发的所有基本逻辑原理。具体来说，我们将学习如何使用它们来编写形式化的论证，以证明数学陈述的真实性（或错误性）。一般来说，很难描述如何确定哪些数学陈述是 True 以及哪些是 False。然而，从某种意义上说，我们在这里开发的策略将帮助我们发现真理。更重要的是，它们将为我们提供模板和指南，以实际向他人展示真理，并描述 *why* 它确实是一个真理。

我们已讨论过，仅仅弄清楚一些有趣的事实并希望别人相信它是不够的。我们需要能够*explain*这一事实；我们需要提出一个论证，将使其他人相信其真实性。我们不一定非得解释它从何而来，或者我们最初为什么要调查它（尽管有时你可能想回答这些隐含的问题，如果你认为这会帮助潜在的读者）。总的来说，我们只需要确保其他人——一个同行、一个同学、一个数学家——能够拿起我们的书面证明，阅读它，并在之后完全确信我们所声称的True确实是True。

Outline of this section

大多数情况下，我们希望您能看出后续策略直接源自与命题和量词以及连接词和否定相关的底层逻辑原则。我们将本节分为几个小节，每个小节对应一个特定的量词或连接词。

当你面对一个数学陈述并需要证明它时，只需从左到右阅读陈述。你首先遇到什么？如果是“∃”量词，请参阅第4.9.1节。如果是“∀”量词，请参阅第4.9.2节。之后，你面临的是哪种类型的陈述？接下来的变量命题的形式是什么？它是一个“∨”陈述吗？请参阅第4.9.3节。它是一个条件陈述吗？请参阅第4.9.5节。它是一个假设是“∨”陈述且结论是“∧”陈述的条件陈述吗？请参阅所有三个章节——4.9.3、4.9.4和4.9.5——并适当地将它们结合起来！一般来说，从现在开始我们写的每个证明（除了将在下一章回顾的归纳证明）都将结合这些策略。你使用哪些策略以及如何结合它们取决于你试图证明的陈述以及你决定如何处理它。

在每个小节中，我们提供了一些模板和一些示例。你可能觉得模板过于严格，也许过于正式；我们理解，但我们认为现在尽可能遵循我们的格式将有助于你长期发展。这些模板——以及我们在提供的示例中如何使用它们——旨在强调这些证明策略背后的逻辑原则。与它们紧密合作将为你提供额外的

练习这些逻辑概念，我们坚信，这将有助于您在未来为自己的用途进行适应。

对于每个提供的示例，我们用蓝色框出了证明策略，用绿色框出了示例实现，以及用红色框出了任何必要的草稿工作。关于策略或实现的任何其他讨论都出现在这些框之外。

此外，本节（以及下一节）中我们考虑的几个例子都是有趣且有用的结果，本身就很有价值。您会注意到其中一些有名称或描述性标题，这是为了表明这一点。虽然本节的主要重点是**proof strategies**——发展它们并了解如何使用它们——但我们鼓励您也将这些例子视为有趣的事实本身。当有必要时，我们还会再次提出这个想法，但我们会将这些讨论保持简短，以免分散本节的总体结构。

Direct vs. Indirect methods

您也会注意到，每个小节都包括 **direct** 和 **indirect** 方法的策略。这些术语可能您现在还不熟悉。它们所指的就是我们是否试图通过直接证明它是 True 来证明一个陈述（1），或者通过引用排中律，通过证明其逻辑否定是 False 来间接证明。

两种策略在一般情况下都是同样有效的，但许多读者通常认为 **direct** 证明在主观上更好。（有时，你可能会写出一个实际上是隐藏着直接证明的间接证明！）随着我们通过例子进行学习和讨论，并要求你在练习中自己写证明，这些主观想法将被评估和讨论。

您会注意到我们所有的间接证明都以短语“为了反驳的目的假设”开始，通常缩写为“AFSOC”。这是一个重要且有用的短语。它向我们的证明的读者表明，我们将做出一个假设，但我们不认为这个假设是有效的。相反，我们将利用这个假设推导出某些内容，一个False。这将使我们得出结论，我们的原始假设是无效的，因此它的逻辑否定（即我们希望证明的原始陈述）实际上是True。您会看到我们使用符号“※”来表示矛盾，但我们也会确保指出*why*我们已经找到了矛盾。我们不会让读者去猜测！

好的，前言已经足够了。让我们直接进入主题，写一些证明吧！

4.9.1 Proving ∃ Claims

一个“∃”主张是*existence*之一。它断言某个特定对象作为某个集合的元素存在，并且它具有某种属性。为了证明这样的主张，我们需要展示这样的对象，并验证，对于我们的读者来说，（1）

该对象是正确集合的元素，并且（2）该对象具有正确的属性。

Direct Method

Strategy:

声明： $\exists x \in S$。

$P(x)$

Direct proof strategy:

Prove that $y \in S$.

Define a specific example, $y =$ _____.

Prove that $P(y)$ holds true.

Example 4.9.1. *Solving a system of linear equations:*

Statement: 修复 $a, b, c, d, e, f \in \mathbb{R}$ 具有使 $ad - bc \neq$ 为 0 的属性。

我们声称可以同时解决

$$ax + by = e \tag{4.1}$$
$$cx + dy = f \tag{4.2}$$

对于某些 $x, y \in \mathbb{R}$。

定义 $S(x, y)$ 为“x 和 y 同时满足上述两个方程，即 (4.1) 和 (4.2)”。然后我们声称

$$\exists x, y \in \mathbb{R}\,.\; S(x, y)$$

首先，我们必须做一些草稿工作以 *construct* 解决方案。然后，我们可以写出一个定义对象 x 和 y 并展示它们为何有效的证明。

Scratch work:

我们需要 $ax + by = e$ 和 $cx + dy = f$，并且想知道哪些 x 和 y 能使这起作用。

让我们将第一个和第二个方程分别乘以右系数（即，分别为d和-b）以便通过相加消去y项

以下是两行：{v*}

$$\begin{aligned} adx + bdy &= de \\ +\big(-bcx - bdy &= -bf\big) \\ \hline (ad-bc)x &= de - bf \end{aligned}$$

除法告诉我们 $x = \frac{de-bf}{ad-bc}$，这是可以接受的，因为 $ad - bc \neq 0$。做类似的事情，取消 x 项，告诉我们如何得到 y:

$$\begin{aligned} acx + bcy &= ce \\ +\big(-acx - ady &= -af\big) \\ \hline (bc-ad)y &= ce - af \end{aligned}$$

除法告诉我们 $y = \frac{af-ce}{ad-bc}$。

主要教训是我们不需要在下面的证明中展示这些草稿工作！我们不假设读者会关心我们关于 *how* 的混乱笔记，我们找到了线性方程组的解。相反，我们假设读者只关心 *what* 解是什么以及 *why* 它是一个解。这也使得证明更加简洁，因此可以更容易、更快地阅读。

Implementation:

Proof. 由于 $ad - bc \neq 0$（根据假设），我们可以定义 e

$$x = \frac{de - bf}{ad - bc} \qquad \text{and} \qquad y = \frac{af - ce}{ad - bc}$$

然后，知道 $x, y \in \mathbb{R}$。

$$\begin{aligned} ax + by &= \frac{(ade - abf) + (abf - bce)}{ad - bc} = \frac{ade - bce}{ad - bc} = \frac{e(ad - bc)}{ad - bc} = e \\ cx + dy &= \frac{(cde - bcf) + (adf - cde)}{ad - bc} = \frac{adf - bcd}{ad - bc} = \frac{f(ad - bc)}{ad - bc} = f \end{aligned}$$

因此 $S(x, y)$ 成立。 □

如果你之前学过一些线性代数，你会认出术语 $ad-bc$ 是矩阵 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 的 **determinant**。规定 $ad - bc \neq 0$ 表示我们要求这个系数矩阵 *have an inverse*，要“非-”

单数”。在 该情况下，我们对该系统有解 e $, f \in \mathbb{R}$.

Indirect Method (Proof by Contradiction)

这个策略依赖于一个 $\exists$ 声明的逻辑否定：

$$\neg\big(\exists x \in S \,.\, P(x)\big) \iff \forall x \in S \,.\, \neg P(x)$$

我们将假设这个否定，并从中推导出一些矛盾的结论，这意味着否定是 False，所以原始的是 True。

声明：$\exists x \in S$ ○ $P(x)$
Indirect proof strategy:

对于每个 $y \in S$，$\neg P(y)$ 成立。找到一个矛盾。

Example 4.9.2. *A version of the Pigeonhole Principle:*

Statement: 假设 $n \in \mathbb{N}$，并且我们拥有 n 个实数，$a_1, a_2, \ldots, a_n \in \mathbb{R}$。

我们断言其中一个数至少与它们的平均值一样大。也就是说，

$$\exists B \in [n] \,.\, a_B \geq \frac{1}{n} \sum_{i=1}^{n} a_i$$

Proof. AFSOC 没有任何一个数字至少与平均值一样大，即

$$\forall i \in [n] \,.\, a_i < \frac{1}{n} \sum_{i=1}^{n} a_i$$

定义常数 $S = \sum_{i=1}^{n} a_i$，使得 $a_i < \frac{S}{n}$。

然后我们可以将所有的 a_i 相加，并观察到

$$S = \sum_{i=1}^{n} a_i < \sum_{i=1}^{n} \frac{S}{n} = n \cdot \frac{S}{n} = S$$

这表明实数 S 比它自己少 *strictly*：$S < S$。这是一个矛盾。※

因此，原始假设是错误的，结论成立。 □

As stated, this is a version of the **Pigeonhole Principle**. We will investigate and use this principle again in Section 8.6, when we study **combinatorics**.

4.9.2 Proving ∀ Claims

一个“∀”主张是*universality*之一。它断言集合中的*all*元素具有某种共同属性。为了证明这种主张，我们需要证明集合中的*every*元素具有该属性。为了“一次性”完成此事，我们将考虑集合中的一个**arbitrary and fixed**元素，并证明它具有所需的属性。因为此对象是任意的，我们的论点适用于集合中的每个元素。因为此对象是固定的，我们可以在整个证明过程中通过名称来引用它。

Direct Method

Strategy:

Claim: $\forall x \in S\text{.}\ P(x)$

Direct proof strategy:

Let $y \in S$ be arbitrary and fixed.

Prove that $P(y)$ holds true.

Example 4.9.3. *A version of the AGM Inequality:*

Statement: $\forall x, y \in \mathbb{R}\text{.}\ xy \leq \left(\frac{x+y}{2}\right)^2$

Implementation:

Proof. 让 $x, y \in \mathbb{R}$ 为任意且固定的。

我们知道 $0 \leq (x-y)^2$。

展开并重新排列，我们得到 $2xy \leq x^2 + y^2$。

两边同时加$2xy$，得到$4xy \leq x^2 + 2xy + y^2$。

因式分解，我们得到 $4xy \leq (x+y)^2$。

除以4，然后将其平方，我们得到

$$xy \leq \left(\frac{x+y}{2}\right)^2$$

□

这个结果被称为 **AGM Inequality**，因为它涉及两个实数的算术平均数（AM）和几何平均数（GM）。

算术平均值是 x 和 y 的 $\frac{x+y}{2}$。

几何平均数 x 和 y 是 $\sqrt{xy}$。(注意，这仅适用于

$xy \geq 0$，即当 x 和 y 有 *same sign* 不论是正数还是负数，或者零。）

AGM不等式断言算术平均数总是大于等于几何平均数。一个有用的记忆法是将“**AGM**”读作“**A**算术平均数 **G**大于 **G**几何 **M**平均数”。

我们上面证明的是一个稍微更一般的版本，因为它适用于 *all* 实数 x 和 y，而不仅仅是那些具有相同符号的数。然而，假设 $xy \geq 0$，则可以简单地取等式两边的平方根，从而获得 AGM 不等式的“通常”陈述：$\sqrt{xy} \leq \frac{x+y}{2}$。

Indirect Method (Proof by Contradiction)

Claim: $\forall x \in S \text{ . } P(x)$

Indirect proof strategy:

AFSOC that $\exists y \in S$ such that $\neg P(y)$ holds.

Find a contradiction.

Example 4.9.4. *$\sqrt{2}$ is irrational:*

Statement: $\forall a, b \in \mathbb{Z} \text{ . } \frac{a}{b} \neq \sqrt{2}$

(注意：此说法直接诉诸有理数的定义 $\mathbb{Q}$。它表示 $\sqrt{2} \notin \mathbb{Q}$，因为那个数有 *no* 整数比率的表示。)

Implementation:

Proof.

AFSOC $\exists a, b \in \mathbb{Z} \text{ . } \frac{a}{b} = \sqrt{2}$.

我们可以假设 $\frac{a}{b}$ 已在 *reduced form* 中给出，因此 a 和 b 没有公因数。（如果不是这样，我们只需约简分数并得到这种形式。）

设这样的 $a, b \in \mathbb{Z}$ 已给出。

（**Note:** 我们将在第4.9.8节中讨论这个短语，“给出这样的”，它不仅意味着断言这样的 $a, b \in \mathbb{Z}$ *exist*，而且还意味着我们想要一些 *particular* 实例的这些变量，以便我们可以在剩余的证明中处理它们。）

This means $\frac{a}{b} = \sqrt{2}$, so $\frac{a^2}{b^2} = 2$.

因此，$2b^2 = a^2$，所以 a^2 是偶数，根据定义。

由于 a^2 是偶数，这告诉我们 a 是偶数。

(**Note:** 您应该证明这一点。我们将在第4.9.6节中证明它，但现在您应该尝试自己完成它.) 因此，$\exists k \in \mathbb{Z}$。

$a = 2k$. Let such a k be given, so $a^2 = 4k^2$.

Then $2b^2 = 4k^2$, so $b^2 = 2k^2$.

Thus, b^2 is even, by definition. By the same reasoning as above with a^2 and a, we deduce here that b is even.

This shows both a and b are even so, in fact, they have a common factor of 2. ||

This contradicts our assumption that a and b have no common factors. ※

Therefore, the original assumption must be False, so the claim is True. □

4.9.3 Proving ∨ Claims

一个“∨”主张至少有两个陈述中的一个是True。如果其中一个陈述显然是False，那么就尝试证明另一个是True。这就是直接方法在这里的做法；它很简单，所以我们不会提供实现示例。

Direct Method

Strategy:

声明：$P \vee Q$

Direct proof:

证明 P 是 True，否则证明 Q 是 True。

这取决于你能否提前决定哪个陈述（P 或 Q）是 True，当然。如果你能这样做，那么这甚至根本不是“策略”。只需实施适用于 P (或 Q 的任何策略，视情况而定)。

Indirect Method (Proof by “Otherwise”)

这种方法比直接方法更有趣。一般来说，当陈述 P 和 Q 实际上是变量命题时，它是有帮助的，并且对于某些实例 P 是 True，而对于其他实例 Q 是 True 的那个。在这种情况下，我们与其描述哪些实例满足 P 以及哪些实例满足 Q，不如这样说：“嗯，如果 P 是 True，那么我们的证明就已经完成了。因此，我们只需要担心 P 是 False 的情况；对于这些情况，我们需要证明 Q 仍然是 True。”

Strategy:

声明：$P \vee Q$

Indirect proof strategy 1:

假设 $\neg P$ 成立。证明 Q 成立。

要重申策略：如果 P 成立，那么该主张成立，实际上我们不在乎 Q 是否成立。在 P 失败的情况下，我们需要保证 Q 成立。

注意，$P \vee Q \iff Q \vee P$ (即，在逻辑析取中顺序无关)，因此我们可以将我们的主张重写为$Q \vee P$，并将上述策略重写为：

假设 $\neg Q$ 成立。证明 P 成立。

这是与等效陈述 $Q \vee P$ 完全相同的策略，即交换了 P 和 Q 的角色。

Example 4.9.5. *When a real number is less than its square:*

Statement: 假设 $x \in \mathbb{R}$ 和 $x^2 \geq x$。

我们断言 $x \geq 1$ 或 $x \leq 0$。

Implementation:

Proof. 让 $x \in \mathbb{R}$ 为任意且固定的，并假设 $x^2 \geq x$。如果 $x \leq 0$ 成立，我们就完成了；所以，假设否则。

即，假设 $x > 0$。

根据假设，$x^2 \geq x$。由于 $x > 0$，我们可以将两边都除以 x。

这产生了 $x \geq 1$。 □

这证明了实数小于（或等于）其平方的 *necessary* 条件。这个条件——即 $x \geq 1 \vee x \leq 0$——也是 *sufficient* 条件吗？证明它！这很简单，一旦你做到了，我们就一起证明了这个 *biconditional* 命题：

$$\forall x \in \mathbb{R}\text{.}\ x^2 \geq x \iff (x \geq 1 \vee x \leq 0)$$

Indirect Method (Proof by Contradiction)

这种方法更像是上面考虑的间接方法，因为我们假设逻辑否定是有效的，然后推导出一些荒谬的结论。我们将通过将其应用于直接前一个例子中的相同论断来阐述这种策略。

Strategy:

声明：$P \vee Q$

Indirect proof strategy 2:

AFSOC что $\neg P \wedge \neg Q$ удерживает. Найти противоречие.

Implementation:

Proof. 让 $x \in \mathbb{R}$ 为任意且固定的，并假设 $x^2 \geq x$。

AFSOC $0 < x$ 和 $x < 1$。

自 $x > 0$，我们可以将这两个不等式的两边乘以 x 并保持符号。

乘以 $x < 1$ 和 x，然后，我们发现 $x^2 < x$。

这与我们的假设相矛盾，即 $x^2 \geq x$ ※

因此，我们的假设无效，所以主张是 True。 □

与之前的实现相比如何？我们正在证明完全相同的论断，但证明略有不同。你认为哪个更好？你认为哪个更容易编写？此外，你能回去用量词和“$\Longrightarrow$”重写原始论断吗？做到这一点后，你看到这两个证明完成了什么吗？试试吧！

4.9.4 Proving $\wedge$ Claims

一个“$\wedge$”主张声称两个陈述都是 True。有一种明显直接的方法来做这件事：只需证明一个陈述，然后证明另一个！

我们将向您展示这种方法的一个示例实现，因为我们的示例中的 $\wedge$ 声明提出了 *after* 一个 $\exists$ 主张。因此，实际上需要做一些基础工作来弄清楚如何定义一个确实能满足这两个所需属性的对象。这将是我们的第一个说明性示例，说明这些证明策略如何被 **combined** 用于证明使用量词和连接词的陈述。

Direct Method

Strategy:

声明：$P \wedge Q$

Direct proof strategy:

证明 P 成立。证明 Q 成立。

Example 4.9.6. **A smaller number whose square is bigger:**

Statement: $\forall x \in \mathbb{R}\bullet\ \exists y \in \mathbb{R}\bullet\ \left(x \geq y \wedge x^2 < y^2\right)$

Scratch work:

这是怎么工作的? 让我们取一个特定的 x，比如 $x = 4$。我们需要找到一个比 $x^2 = 16$ 更小的实数，其平方大于 $x^2 = 16$。

关键是我们想要 $y \in \mathbb{R}$，因此我们可以使用 *negative* 个数字。在这种情况下，选择一个具有更大 *magnitude* 的负数，如 $y = -5$，将有效。

让我们取一个不同的 x，比如 $x = -2$。这个数已经是负数了，所以只需选择一个更小的数，比如 $y = -3$，就可以工作。

以下证明分为两种情况，根据 x 是否为正或非正。

现在我们准备好证明我们的主张。

Implementation:

Proof 1. 设 $x \in \mathbb{R}$ 为任意且固定的。我们考虑两 o 个案例。 (1) 假设 $x \leq$ = 0。

定义 $y = x - 1$. 注意 $y \in \mathbb{R}$。

注意 $y \leq x$。此外，请注意

$$y^2 = (x-1)^2 = x^2 - 2x + 1 = x^2 - (2x - 1)$$

自 $x \leq 0$，我们知道 $2x \leq 0$，因此 $2x - 1 \leq -1$。因此，

$$x^2 - (2x - 1) \geq x^2 - 1 > x^2$$

因此，$y^2 > x^2$。

(2) 现在，假设 $x > 0$。定义 $y = -x - 1$。注意 $y \in \mathbb{R}$。注意 $y < 0$ 和 $x > 0$，所以 $y \leq x$。 (事实上，$y < x$，甚至。)另外，注意

$$y^2 = (-x-1)^2 = x^2 + 2x + 1 = x^2 + (2x + 1)$$

自从 $x > 0$，我们知道 $2x + 1 > 0$。因此，

$$x^2 + (2x + 1) > x^2$$

因此，$y^2 > x^2$。

在任何情况下，我们都找到了具有所需性质 y，即 $y \in \mathbb{R}$、$y \leq x$ 和 $x^2 < y^2$。因此，该主张是 True。 □

为什么我们称之为“证明1”？我们根据在草稿中的观察将证明分为两种情况。具体来说，我们认识到我们将根据x的符号，用x) *differently*来定义y (。我们声称可以以这种方式重写这个证明：*avoids*这些情况。这就是“证明2”的内容，我们希望你能写出来！为了重申目标，我们希望你能重写上述证明，使得y以一种通用的方式定义为x，无论x的符号如何都适用。

(*Hint*)什么情况下 $-x$ 为 0? 这是否是我们见过的函数 在之前?)

Indirect Method (Proof by Contradiction)

这种方法就像其他间接方法一样。我们只是对一个命题取逻辑否定，假设它成立，然后得出一些荒谬的结论。这意味着假设是无效的，所以原始陈述是 True 的。

我们将把它留给你去尝试将这种方法应用于前面例子中使用的索赔。（注意：你可能想这样做 *after* 找到我们上面暗示的“第二个证明。”然后，你可以比较两种方法的结果，并决定你更喜欢哪一种，在这种情况下。

Strategy:

声明：$P \wedge Q$

Indirect proof:

AFSOC что $\neg P \vee \neg Q$ удерживает.

考虑第一种情况，其中 $\neg P$ 成立。找到一个矛盾。

考虑第二种情况，其中 $\neg Q$ 成立。找到一个矛盾。

4.9.5 Proving $\Longrightarrow$ Claims

可能有助于您回顾第4.5.3节，在那里我们介绍了连接词“$\Longrightarrow$”。具体来说，我们希望您回忆起$P \implies Q$表示*whenever* P成立，Q也*necessarily*成立。这个条件语句是True

在P本身（即**hypothesis**）是False的情况下。因此，我们的证明策略不需要考虑此类情况。我们只需要确保P成立，然后推导出Q也成立。这样就解决了“每当P成立，Q也成立”的考虑。

Direct Method

Strategy:

声明：$P \implies Q$

Direct proof strategy:

假设 P 成立。证明 Q 成立。

Example 4.9.7. *Monotonicity of squares:*

Statement: $\forall y \in \mathbb{R}.\ y > 1 \implies y^2 - 1 > 0$

Implementation:

Proof. 让 $y \in \mathbb{R}$ 为任意且固定的。

假设 $y > 1$。

两边同时乘以 y (，因为 $y > 0$)，我们得到 $y^2 > y$。

自 $y > 1$ 以来，这告诉我们 $y^2 > y > 1$，因此 $y^2 > 1$。

减法得到所需的结论：$y^2 - 1 > 0$。 □

我们称之为“平方的单调性”，因为它陈述了实数的一个特定性质，即**monotone**。这是一个用来表示在某种运算下保持某个不等式的术语。在这种情况下，某些数大于1的性质被“平方运算”所保持。也就是说，我们证明了如果 $y > 1$，那么 $y^2 > 1^2$ 也成立。

现在，这是一个证明起来相当简单的例子，但我们想包括它以强调条件语句的证明策略。现在让我们来处理一个更复杂的例子。

（您也会注意到练习4.11.22有一个类似的问题陈述。也许您在跟随这个例子之后想先做那个。）

Example 4.9.8. *Working with inequalities:*

Statement: 我们定义以下变量命题 s:

$$P(x) \text{ is } \text{“}\frac{x-3}{x+2} > 1 - \frac{1}{x}\text{”}$$
$$Q(x) \text{ is } \text{“}\frac{x+3}{x+2} < 1 + \frac{1}{x}\text{”}$$

定义 $S = \{x \in \mathbb{R} \mid x > 0\}$。

我们声称

$$\forall x \in S\,.\; P(x) \implies Q(x)$$

Scratch work:

我们猜测在这里直接方法会有效，所以让我们尝试操纵 $P(x)$ 中所述的不等式，使其“看起来”像 $Q(x)$ 中的不等式。

所以我们从那个不等式开始

$$\frac{x-3}{x+2} > 1 - \frac{1}{x}$$

我们将在两边都乘以 $x+2$。我们可以这样做吗？哦，对了，$x > 0$ 以及 $x + 2 > 0$，也同样。呼！这给了我们

$$x - 3 > (x+2) - \frac{x+2}{x} = x + 2 - 1 - \frac{2}{x} = x + 1 - \frac{2}{x}$$

我们想在某个地方看到 $x+3$，所以我们将两边都加上/减去：

$$x - 1 + \frac{2}{x} > x + 3$$

我们可以除以 $x+2$ 并使右边的分数成立吗？嗯……等等！我们已经简化了分数 $\frac{x+2}{x}$ 并将其移到一边。也许我们不应该先简化它，所以让我们尝试撤销这个操作：

$$x + 3 < x - 1 + \frac{2}{x} = (x+2) + \frac{x+2}{x} - 4 = (x+2)\left(1 + \frac{1}{x}\right) - 4$$

啊哈，看起来更好了！我们甚至在形式上有一个“调整空间”，即那里的负4。我们知道右边小于我们想要的，所以结果成立。

让我们取这里我们工作的这些代数步骤，稍作调整顺序，并解释它们，最后将所有内容封装在一个正式的证明中。

Implementation:

Proof. 让 $x \in S$ 为任意且固定的。

假设 $P(x)$ 成立；也就是说，假设

$$\frac{x-3}{x+2} > 1 - \frac{1}{x}$$

我们将证明不等式

$$\frac{x+3}{x+2} < 1 + \frac{1}{x}$$

同样成立，必然。

自 $x \in S$ 以来，我们知道 $x > 0$，因此，当然，$x + 2 > 0$，也是如此。因此，我们可以将已知的非等式两边乘以 $x + 2$，得到

$$x - 3 > (x+2)\left(1 - \frac{1}{x}\right) = x + 2 - \frac{x+2}{x}$$

$3 + \frac{x+2}{x}$ 加到两边，两边减去 2，然后反向重写（便于阅读），我们得到

$$x + 3 < x - 2 + \frac{x+2}{x}$$

由于 $x -$^2 $< x +$^2，我们推断出

$$x + 3 < x + 2 + \frac{x+2}{x}$$

并且因式分解告诉我们

$$x + 3 < (x+2)\left(1 + \frac{1}{x}\right)$$

再次，由于 $x + 2 > 0$，我们可以将两边都除以 $x + 2$，得到

$$\frac{x+3}{x+2} < 1 + \frac{1}{x}$$

这是所期望的不等式。这表明 $P(x) \implies Q(x)$，由于 x 是任意的，我们已证明了这个命题。 □

一个关键教训在于我们如何将我们的草稿工作以不同的方式呈现在我们的证明中。我们省略了不必要的简化和重构步骤，但在执行每一步时，我们也注意到了为什么每一步是有效的。一个更有经验的数学家可能会跳过这些步骤中的几个，并让读者验证代数工作，但由于我们数学生涯刚开始，我们认为尽可能展示更多细节是谨慎的。

Contrapositive Method

回顾第4.6.1节。在那里，我们证明了条件语句与它的逆否命题在逻辑上是等价的。也就是说，条件语句

$$P \implies Q$$

必然具有与该陈述相同的真值

$$\neg Q \implies \neg P$$

因此，当我们试图证明 $P \implies Q$ 是有效的时，我们只需证明 $\neg Q \implies \neg P$ 是有效的即可！根据 P 和 Q 的不同，这种逆否命题可能更容易理解，或者我们可以更快地找到证明。事实上，逆否策略在 P (或 Q，或者可能两者) 中某处有“否定”时特别有用；通过考虑其否定，我们可以用“肯定”陈述而不是否定来工作。

Strategy:

声明：$P \implies Q$

Contrapositive proof strategy:

假设 $\neg Q$ 成立。证明 $\neg P$ 成立。

(注意，这是应用于 $\neg Q \implies \neg P$ 的 *direct proof strategy*。)

Example 4.9.9. *Even products of integers:*

Statement: 设 $E(x)$ 为命题 “x 是偶数”。

我们声称

$$\forall m, n \in \mathbb{Z}\,.\; E(m \cdot n) \implies \big(E(m) \vee E(n)\big)$$

另一种说法是，每当两个整数的乘积是偶数时，这必然意味着至少有一个整数是偶数。

Implementation:

Proof. 我们通过逆否命题来证明这一点
。设$m, n \in \mathbb{Z}$是任意且固定的。假设
$\neg E(m) \wedge \neg E(n)$。

这意味着 m 是奇数且 n 是奇数。

这意味着 $\exists k, \ell \in \mathbb{Z}$。 $m = 2k + 1 \wedge n = 2\ell + 1$.
设这样的 k, ℓ 已知。然后，

$$m \cdot n = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1$$

自$2k\ell + k + \ell \in \mathbb{Z}$以来，同样，这表明$m \cdot n$是奇数。

因此，$\neg E(m \cdot n)$成立，所以我们已经证明

$$\big(\neg E(m) \wedge \neg E(n)\big) \implies \neg E(m \cdot n)$$

逆否命题得出该主张。 □

注意我们在证明的开始向读者指出，我们将使用逆否方法。如果我们不这样做，读者可能会感到困惑！我们的读者可能会想：“我们为什么要假设 $\neg E(m)$ 成立？这有什么好处？！”，通过事先揭示我们的策略，我们确保读者能够跟上，避免不必要的困惑。

Indirect Method (Proof By Contradiction)

此方法依赖于条件语句的逻辑否定。重新阅读第4.7节，以了解我们证明了什么

$$\neg(P \implies Q) \iff (P \wedge \neg Q)$$

这个证明技术利用了这个等价性。

Strategy:

声明：$P \implies Q$

Indirect proof strategy:

AFSOC что Pудерживает и предположим, что Q не в ыполняется. Найти противоречие.

Example 4.9.10. *A surprising form of the AGM Inequality:*

Statement: $\forall x \in \mathbb{R}\text{.}\ x > 0 \implies x + \frac{1}{x} \geq 2$

让我们直接进入这个证明，不做任何草稿工作，因为我们认为这个证明读起来相当直接。之后，我们将讨论一个替代策略。

Implementation:

Proof. 让 $x \in \mathbb{R}$ 为任意且固定的。

假设 $x > 0$。

AFSOC что $x + \frac{1}{x} < 2$.

自 $x > 0$ 以来，我们可以将这个不等式乘以 x，得到

$$x^2 + 1 < 2x$$

减法和因式分解，我们得到

$$(x-1)^2 < 0$$

这是一个矛盾，因为 $(x-1)^2 \geq 0$. ※

因此，我们的原始假设无效，结论成立。 □

现在，你可能想知道这个例子的标题是什么。这与AGM不等式有什么关系？（回想一下，我们在第4.9.2节中证明了这一点。）一个敏锐的读者可能会意识到，这里的事实不仅是一个不等式（就像AGM一样），而且这个证明中的几个步骤与我们证明AGM不等式时所做的是相似的。具体来说，为了证明AGM不等式，我们首先使用了这样一个事实：一个特定的平方表达式是非负的。同样，在这个证明中，我们引用了这样一个事实：一个平方表达式 *should* 是非负的。这种证明之间的相似性表明存在某种潜在的关联。事实上，我们实际上可以直接 *apply* AGM不等式（请注意，这是一种巧妙的方式！）以不同的方式证明上述事实。

考虑几分钟，看看你能否在我们展示它的工作原理之前提出以下证明。将AGM不等式 *apply* 是什么意思？该结果对任何 x 和 y 都成立，但这里我们只有一个 x。我们能否巧妙地选择 y 应该是什么，以便这里的结论立即“出现”？试试看！然后，继续阅读……

Proof. 设 $x \in \mathbb{R}$ 为任意且固定的。假设 $x > \neq 0$。

定义 $y = \frac{1}{x}$，因此 $y \in \mathbb{R}$。

然后，AGM不等式适用于 x 和 y (，因为该事实对 *arbitrary* $x, y \in \mathbb{R}$) 成立。这告诉我们

$$x \cdot \frac{1}{x} \leq \left(\frac{x + \frac{1}{x}}{2} \right)^2$$

简化等式两边得到

$$1 \leq \frac{1}{4}\left(x + \frac{1}{x}\right)^2$$

然后两边乘以4得到

$$4 \leq \left(x + \frac{1}{x}\right)^2$$

由于两边都是非负的，我们可以对两边取平方根并推导出

$$2 \leq x + \frac{1}{x}$$

这证明了该主张。 □

这里有一个教训：

> Alw注意在论证之间寻找相似之处 ts 和
> 证明，而不仅仅是已证明的结果。

您可能可以通过应用已经证明的另一个结果来节省一些工作！（在这种情况下，我们没有节省太多写作；然而，如果我们没有已经注意到矛盾法会很有成效，我们可能已经节省了一些时间。特别是，我们可能没有想到在我们的第一个证明中出现的因式分解技巧。）

4.9.6 Proving $\iff$ Claims

回忆一下，“$\iff$”连接词完全是在“$\implies$”连接词的术语中定义的。也就是说，断言

$$P \iff Q$$

与断言两个条件语句在逻辑上等价：

$$\big(P \implies Q\big) \wedge \big(Q \implies P\big)$$

这导致了一个明显的策略：先证明一个条件语句，然后证明另一个！我们最常见的错误是当有人只证明了一个语句，但没有同时证明两个。始终牢记这一点！

Direct Method

Strategy:

声明：$P \iff Q$

Direct proof strategy:

证明 $P \implies Q$ (使用上述方法之一)。证明 $Q \implies P$ (使用上述方法之一)。

Example 4.9.11. *Even squares of integers:*

Statement: 一个整数是偶数，当且仅当它的平方是偶数。

让我们用逻辑符号表示法重写这个主张。

设 $E(z)$ 为命题 “z 是偶数”。然后我们声称

$$\forall z \in \mathbb{Z}. \left(E(z) \iff E(z^2)\right)$$

Implementation:

Proof. 让 $z \in \mathbb{Z}$ 为任意且固定的。

($\implies$) 首先，假设 z 是偶数，因此 $\exists k \in \mathbb{Z}$

- $z = 2k$. Let such a k be given.

$$z^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Since $z = 2k$, we can square both sides and obtain

定义 $\ell = 2k^2$。注意 $\ell \in \mathbb{Z}$ 和 $z^2 = 2\ell$

这表明 z^2 是偶数。

因此，$E(z) \implies E(z^2)$。

($\impliedby$) 其次，我们将通过逆否命题证明 $E(z^2) \implies E(z)$。

假设 z 是奇数，因此 $\exists m \in \mathbb{Z}$

- $z = 2m + 1$. Let such an m be given.

由于 $z = 2m + 1$，我们可以对两边进行平方并得到

$$z^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$$

定义 $n = 2m^2 + 2m$。注意 $n \in \mathbb{Z}$ 和 $z^2 = 2n + 1$。

这表明 z^2 是奇数。

因此，$\neg E(z) \implies \neg E(z^2)$；由逆否命题，因此，$E(z^2) \implies E(z)$。

因为我们已经展示了两个方向，所以我们得出结论

$$E(z) \iff E(z^2)$$

并且由于 z 是任意的，这个双条件对所有整数 z 都成立。 □

Indirect Method (Proof by Contradiction)

Strategy:

声明：$P \iff Q$

Indirect proof strategy:

AFSOC that $\neg(P \implies Q) \vee \neg(Q \implies P)$.

考虑第一种情况，其中 $P \wedge \neg Q$ 成立。找到一个矛盾。考虑第二种情况，其中 $Q \wedge \neg P$ 成立。找到一个矛盾。

实现此策略——甚至决定何时这样做——取决于实际陈述 P 和 Q。一般来说，直接方法可能更好（不一定），但如果发现自己陷入困境，可以考虑查看否定——$P \wedge \neg Q$ 和 $Q \wedge \neg P$——看看这能否带你去到某个地方。值得一试！

Intermediary Method (TFAE)

由于没有更好的术语，我们将这种策略称为一个 **intermediary method**。正如您将看到的，它既不是一种直接方法，也不是一种间接方法。在实施这种策略时，我们不必考虑任何逻辑否定，但我们也没有直接将陈述 P 和 Q 相关联。

相反，这种方法要求我们找到一些 *intermediary* 陈述 R 并证明两个双条件陈述：即，$P \iff R$ 和 $R \iff Q$。这产生了以下条件语句链

$$P \iff Q \iff R$$

这告诉我们所有三个陈述具有相同的真值。特别是，那么，P和Q必须始终具有相同的真值，因此我们得出结论$P \iff Q$。

缩写 **TFAE** 代表“以下内容等价”。我们选择这个名字是因为它在数学中是一个常用短语；它用于提出一系列条件/性质的定理，这些条件/性质都“相互蕴含”。

是，一些定理列出了几个属性并断言它们都是逻辑等价的，因此有“以下都是等价的”。要证明这样的定理，人们会反复实施上述策略并证明这些陈述确实是等价的。这里唯一的区别是我们必须使用*come up with*中介陈述。（但嘿，whoever presented and proved a TFAE-style theorem probably had to come up with all of those statements to begin with, too！）

Strategy:

声明：$P \iff Q$

Intermediary strategy:

定义一个语句 R。

证明 $P \iff R$ (使用上述方法之一)。证明 $Q \iff R$ (使用上述方法之一)。

4.9.7 Disproving Claims

我们现在已经讨论了（在许多例子中看到了）如何 **prove** 任何类型的数学陈述。太棒了！但你可能会说，“哎呀……如果我想 **disprove** 一个陈述怎么办?”我们对这个问题的回答简短而甜蜜：*there's no difference*。

要 **disprove** 一个陈述意味着你想要展示它的真值是 False。根据逻辑否定的定义，这意味着你想要展示该陈述的否定具有真值 True。因此，你只需找到并写下这个逻辑否定，并证明该陈述是 True，可以使用我们在本节中探讨的任何策略。就这样！

仅为说明起见，让我们看看这一现象的实际例子。具体来说，我们将看到一个例子，其中我们想要反驳一个“$\forall$”主张，这意味着我们想要证明一个“$\exists$”主张。这就是**counterexample**这一概念发挥作用的地方。

Counterexamples

一般来说，一个 **counterexample** 是一个反驳全称量词的语句的实例。它是一个 *example*，因为它旨在证明一个“$\exists$”主张，并且它在意义上表明这个特定例子确实具有所声称的性质。

Example 4.9.12. 回顾示例 4.9.8。在其中，我们定义了集合

$$S = \{x \in \mathbb{R} \mid x > 0\}$$

然后定义了两个变量命题:

$$P(x) \text{ is } \text{“}\ \frac{x-3}{x+2} > 1 - \frac{1}{x}\ \text{”}$$
$$Q(x) \text{ is } \text{“}\ \frac{x+3}{x+2} < 1 + \frac{1}{x}\ \text{”}$$

然后，我们证明了

$$\forall x \in S.\ P(x) \implies Q(x)$$

在这个例子中，我们将考虑以下陈述

$$\forall x \in S.\ Q(x) \implies P(x)$$

具体来说，我们将 **disprove** 它。不过，在我们这样做之前，先自己玩玩这个陈述。尽管我们本质上已经告诉你它是 False，但试着证明它！你发现你的“证明”在哪里崩溃了吗？为什么会这样？你能用你的观察来帮助你找到一个反例吗？看看你能找到什么，然后再继续阅读。

Scratch work:

要开始，我们需要我们反驳的主张的逻辑否定:

$$\exists x \in S.\ Q(x) \wedge \neg P(x)$$

这意味着我们需要找到一个特定的实数 x，它满足三个条件：（1）不等式 $x > > 0$，（2）不等式

$$\frac{x+3}{x+2} < 1 + \frac{1}{x}$$

并且（3）不等式

$$\frac{x-3}{x+2} \leq 1 - \frac{1}{x}$$

有几种策略我们可以使用。就像我们上面提到的，我们可以尝试（当然，是错误地）证明第一个不等式确实意味着第二个不等式，并确定在哪里会失败。或者，我们可以使用“有根据的猜测”方法“尝试一些值”。

知道 $x \in \mathbb{R}$ 和 $x > 0$ 表示，无论如何，我们可能想要尝试 x 的“极端”值。这意味着要么是“小”的 x (，即 x 接近 0)，要么是“大”的 x (，即 x 的值不断增大，直到我们找到一个可行的值)。

看起来先处理一些“小”值更容易，所以让我们尝试 $x = 1$。我们看到（1）成立是因为 $1 > 0$，并且（2）成立是因为 $\frac{4}{3} < 2$，以及（3）成立是因为 $-\frac{2}{3} < 0 \leq 0$。酷，就这样了！

Proof. 这里，我们将反驳 $\forall x \in \mathbb{R}$ 的说法。 $Q(x) \implies P(x)$.
考虑 $x = 1$. 注意到 $x \in \mathbb{R}$ 和 $x > 0$。

此外，请注意 $Q(1)$ 成立，因为

$$\frac{1+3}{1+2} = \frac{4}{3} < 2 = 1 + \frac{1}{1}$$

此外，请注意 $P(1)$ 失败，因为

$$\frac{1-3}{1+2} = -\frac{2}{3} \not> 0 = 1 - \frac{1}{1}$$

因此，我们已经证明

$$\exists x \in S \text{ . } Q(x) \wedge \neg P(x)$$

并且这反驳了该主张。 □

4.9.8 Using assumptions in proofs

另一个重要的方面是创建和编写正式证明，我们有时会被给予 **assumptions** 来使用。当我们陈述一个定理时，它通常有一些 **hypotheses** 和一个 **conclusion**。我们可以暂时将这些假设添加到我们的数学工具箱中；我们可以使用它们来得出所需的结论。同样，在过程中，我们可能会发展一些进一步的事实和观察，我们可以保留这些并使用它们来证明结论，以及。在本节中，我们想指出在您 *using* 证明中的一个假设时可能会出现的三种观察和问题。

"$P \vee Q$" means Use Cases

如果在一个证明的某个点上，你假设或推导出 $P \vee Q$ 成立，你该如何进行？知道这个析取命题成立意味着至少有一个组成命题——P 或 Q——成立。因此，你可以单独考虑这两个 **cases** 中的每一个。例如，你的证明可能包含以下部分：

> 因为 $P \vee Q$，我们有两种情况。
>
> > **Case 1:** 假设 P 成立。那么……
> > **Case 2:** 假设 Q 成立。那么……

只要您在两种情况下都能实现您想要的目标，您就可以进行这项扣除。

注意，没有必要考虑 *both* P 和 Q 同时成立的情况。首先，这甚至可能根本不会发生。而且，如果你最终只使用其中一个陈述来得出你想要的结论，那么就没有必要暂时假设它们两个。

我们一直在某些证明中使用案例。现在，我们确切地看到了它们为什么有效！当存在语句的潜在析取时，我们使用案例。

"There exists ..." vs. "Let ... be given"

这是一个 s微妙但重要的区别。如果你写下一条声明 m 类似

$$\exists x \in S \text{ . } P(x)$$

在证明的中间，你提出了什么？从技术上讲，你实际上只陈述了上面的行是一个 True 声明；你断言存在某些 *does* 具有性质 $P(x)$。但是，如果你移动并开始之后引用 x ... 这是不合法的！在 *existence* 的断言中，你从未引入该声明的 *particular instance*。可能存在多个这样的 x 元素。你想要讨论所有这些元素吗？还是只讨论一个特定的元素？不要让你的证明读者去直观地理解你正在做什么！

如果你知道或假设了一些存在陈述（如上面的行）并且你实际上想要找到一个满足该存在断言的变量 *introduce*，请使用以下神奇的短语：

> "给定这样的 x。"

这向读者表明，你不仅声称存在这样的 x，而且你还在你的证明中使用了它。你希望这封信 x 在你接下来的书面论点中代表具有该属性的一个元素。此后，你可以通过名称来引用那个对象 x。

如果您断言存在多个变量并想引入它们，只需使用略有不同的动词的类似短语即可。例如，您可能会这样写：

> ...因此我们推断出 $\exists x, y, z \in \mathbb{Z}$ 使得 $P(x, y, z)$ 成立。
>
> 设这样的 x, y, z 已知。观察得...

"$P \implies Q$" vs. "P, therefore Q"

这个区别基于一个类似于我们刚才提到的上一个例子中的想法。具体来说，在写一个断言其 *validity* 的陈述和写一个向读者展示你正在从它做出 *con- clusion* 的陈述之间有一个区别。在上一个例子中，这是说某物存在与引入这样一个对象之间的区别。

这里，区别在于断言一个条件语句——如 $P \implies Q$——来说明这种条件关系存在，与使用这个语句来 *deduce* Q 成立。从技术上来说，仅仅在您的论文上写下 "$P \implies Q$" 并不能断言 Q 是有效的。您必须向读者非常清楚地表明您 *also* 知道 P 并且正在使用条件语句来 *deduce* Q。

回顾我们在第4.5.6节中的讨论。在那里，我们描述了这个重要的区别，并提到了“肯定前件法”这种方法。正如我们提到的，如果你实际上要演绎出Q，你应该写类似于以下的内容：

> $P \implies Q$ 因为……此外
> ，P成立，因为……因此
> ，Q成立。

4.9.9 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 什么是 $\exists$ 请求的直接方法？展示一个对象存在的重要步骤有哪些？

(2) 什么是 $\implies$ 请求的直接方法？我们如何通过反证法证明一个 $\implies$ 请求？这些方法有何不同？

(3) 我们如何证明一个 $\iff$ 声明？ (
4) 什么 t 是 AGM 不等式？该缩写词来自何处 从？

(5) 反证法适用于哪种类型的论断？为什么它有效？

(6) 什么是反例？(7) 说“$\exists a \in A$ $P(a)$” and saying “$\exists a \in A$ $P(a)$ so let such an a be given”?”与什么不同？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 证明 $\forall x \in \mathbb{R}$ $x^2 \neq 1 \implies x \neq 1$.
(2) 证明 $\forall n \in \mathbb{N}$ $n > 5 \implies 2n^2 > (n+1)^2$
(3) 用逻辑符号表达以下命题，然后证明它。

存在一个偶数自然数，它可以写成两个质数的和，有 *different* 种方式。

(4) 证明每个自然数要么小于 {v*}10，要么大于3。也就是说，证明

$$\forall n \in \mathbb{N}\,.\; n < \sqrt{10} \vee n > 3$$

(5) 设 A, B, C, D 为集合。证明，如果 $A \cup B \subseteq C \cup D$ 和 $C \subseteq A$ 和 $A \cap B = \varnothing$，那么 $B \subseteq D$。

(6) 定义 $P = \{y \in \mathbb{R} \mid y > 0\}$。证明

$$\forall \varepsilon \in P\,.\; \forall x, y \in \mathbb{R}\,.\; \exists \delta \in P\,.\; |x - y| < \delta \implies |(3x - 4) - (3y - 4)| < \varepsilon$$

你能也证明以下说法吗？它与上面的说法有何不同?

$$\forall \varepsilon \in P\,.\; \exists \delta \in P\,.\; \forall x, y \in \mathbb{R}\,.\; |x - y| < \delta \implies |(3x - 4) - (3y - 4)| < \varepsilon$$

(7) 设 $E(x)$ 为命题“x 是偶数”。证明

$$\forall a, b \in \mathbb{Z}\,.\; E(a) \wedge E(b) \iff E(a + b) \wedge E(a \cdot b)$$

(8) 回顾一下 $\sqrt{}$^2 是无理数的证明。修改它以提供一个证明 $\sqrt{}$^3 也是无理数的证明。

尝试做同样的事情，并证明 $\sqrt{6}$ 是无理数。

Challenge: 你能证明对于素数 *every*，$\sqrt{p}$ 是无理数吗?

(9) 证明存在无限多个有理数。

Hint: 通过反证法来做。（假设有有限多个……）

4.10 Summary

我们现在拥有一个庞大的数学证明策略工具包！我们开发了必要的术语和符号来正确表达数学主张。然后，我们利用这些概念下的概念来开发证明策略，并看到了许多它们如何被使用的例子。

一个更难的部分是 *writing* 证明，首先要弄清楚证明！这不仅仅是要弄清楚一个主张是 True 还是 False，还要最终决定要实施哪种证明策略。我们明白这是具有挑战性的，因为，嗯，它就是。此外，很难确切地 *when* 使用某些策略。我们可以提供指导和建议（我们已经尽可能多地这样做），但从长远来看，掌握实施证明策略和决定使用哪些策略的最好方法是 *just do it*。从一个练习问题开始。尝试玩弄陈述，看看为什么它是 True (或 False，视情况而定)。尝试使用一个

证明策略在它上面。它起作用了吗？怎么做到的？如果没有，为什么，在哪里出了问题？你能用这些观察结果来决定对问题采取不同的方法吗？最终，你能写下一个好的、正式的论点吗？尽可能多地通过这些步骤解决尽可能多的问题确实是最好的实践。简单地 **doing mathematics** 没有替代品。

4.11 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的任何内容，以及可能的一些假设的数学知识。当然，我们不期望你解决其中的 **all**，但工作得越多，你将学到越多！记住，没有 *doing* 数学，你无法真正 *learn* 数学。动手解决一个问题。阅读几个陈述，四处走走，思考它们。尝试写一个证明，并向朋友展示，看看他们是否信服。继续练习将你的想法以清晰、精确和逻辑的方式 *write* 出来的能力。写完证明后，编辑它，使其更好。最重要的是，继续 *doing* 数学！

简答题，只需解释或陈述答案，无需严格的*proof*，已用►标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 4.11.1. ► 考虑通用上下文为 $U = \mathbb{Z}$。

设 $P(x)$ 为命题“$1 \leq x \leq 3$”。

设 $Q(x)$ 为命题“$\exists k \in \mathbb{Z}\text{.}\ x = 2k$”.

设 $R(x)$ 为命题“$x^2 = 4$”。

设 $S(x)$ 为命题“$x = 1$”。

对于以下每个陈述，写出一个英文句子来描述该陈述的含义，然后写出逻辑否定，然后决定哪个陈述是 True 或 False，并解释原因。

(a) $\forall x \in \mathbb{Z}\text{.}\ P(x) \implies Q(x)$. $R(x) \wedge P(x)$. $R(x) \implies P(x)$

(b) $\exists x \in \mathbb{Z}$

(c) $\forall x \in \mathbb{Z}$

(d) $\forall x \in \mathbb{Z}\text{.}\ \exists y \in \mathbb{Z}\text{.}\ x \neq y \wedge P(x) \wedge R(y)$

(e) $\forall x \in \mathbb{Z}\text{.}\ \exists y \in \mathbb{Z}\text{.}\ (S(x) \vee Q(x)) \wedge P(y) \wedge \neg Q(y)$

(f) $\exists x \in \mathbb{Z}\text{.}$

$S(x) \iff P(x) \wedge \neg Q(x)$

(g) $\exists x \in \mathbb{Z}$

. $S(x) \iff \neg P(x) \wedge Q(x)$

Problem 4.11.2. 对于以下每个主张，定义一些集合和变量命题，以简洁的符号、逻辑符号表达该主张。然后，也写出逻辑否定。注意哪个是True或False。

(a) 每个奇数自然数都是素数。

(b) 存在一个实数，它严格大于任何整数的平方。 (c) 在 -1 和 1 之间，存在某个实数，它等于某个 *different* 实数在 -1 和 1 之间的立方。 (d) 质数的倍数集的并集是自然数集本身。

Problem 4.11.3. 考虑以下定义的集合以及关于这些集合的问题。对于每个问题，如果你的答案是 No，请提供一个示例来证明这一点。

(a) 设 $S = \{1, 2, 3, 4\}$ 和 $T = \{3, 4, 5, 6, 7, 8\}$。 $\forall s \in S$ 是否成立? $\exists t \in T$ $s + t = 7$?

(b) Let $S = \{2, 3, 4, 5, 6\}$ and $T = \{3, 4, 5, 6\}$.

Is it true that $\forall s \in S$ $\exists t \in T$ $s + t = 7$? (c) Let $S = \mathbb{N}$ and $T = \mathbb{Z}$.

Is it true that $\forall s \in S$ $\exists t \in T$ $s + t = 7$?

(d) Let $S = \mathbb{Z}$ and $T = \mathbb{Z}$.

Is it true that $\forall s \in S$ $\exists t \in T$ $s + t = 7$?

Problem 4.11.4. 考虑以下定义的集合以及关于这些集合的问题。对于每个问题，如果你的答案是 No，请提供一个示例来证明这一点。

(a) 设 $S = \{1, 2, 3\}$, $T = \{6, 7, 8, 9\}$, 以及 $V = \{7, 8, 9, 10\}$。 $\exists s \in S$ 是否成立? $\forall t \in T$ $\exists v \in V$ $s + t = v$?

(b) Let $S = \{1, 2, 3\}$, $T = \{4, 5, 6, 7\}$, and $V = \{5, 6, 7, 9, 10, 11\}$.

Is it true that $\exists s \in S$ $\forall t \in T$ $\exists v \in V$ $s + t = v$?

(c) Let $S = T = V = \mathbb{N}$.

Is it true that $\exists s \in S$ $\forall t \in T$ $\exists v \in V$ $s + t = v$?

(d) Let $S = \mathbb{N}$, $T = \mathbb{Z}$, and $V = \mathbb{N}$. $\forall t \in T$ $\exists v \in V$

Is it true that $\exists s \in S$ $s + t = v$?

Problem 4.11.5. 证明或反驳以下陈述 rigo rousy:{v*}

$$\exists x \in \mathbb{R}\,.\ \forall y \in \mathbb{R}\,.\ x^2 - y^2 \geq 0$$

Problem 4.11.6. 严格证明或反驳以下命题:

$$\forall x, y \in \mathbb{Z}\,.\ \exists z \in \mathbb{N} \cup \{0\}\,.\ ((x - y) = z) \vee ((y - x) = z)$$

Problem 4.11.7. 证明方程 $x^2 - y^2 = 14$ 没有整数解（即 $x, y \in \mathbb{Z}$）。

Problem 4.11.8.

Problem 4.11.9.

Problem 4.11.10.

Problem 4.11.11.

Problem 4.11.12. 使用 *logical equivalences* 证明

(a) $(A \cup B) \cap \overline{A} = B - A$

(b) $A \cap (B - C) = (A \cap B) - (A \cap C)$

Problem 4.11.13. 定义集合

$$A = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} \mid \frac{x}{y} + \frac{y}{x} \geq 2 \right\}$$

和

$$B = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)\}$$

这是否是情况 $A \subseteq B$? 如果是这样，请证明它。如果不是，请展示一个反例。
这是否是情况 $B \subseteq A$? 如果是这样，请证明它。如果不是，请展示一个反例。

Problem 4.11.14. 设 $P = \{y \in \mathbb{R} \mid y > 0\}$ 为正实数集。证明以下命题:

$$\forall \varepsilon \in P\,.\ \exists \delta \in P\,.\ \forall x \in \mathbb{R}\,.\ |x| < \delta \implies |x^2| < \varepsilon$$

Problem 4.11.15. 以下关于$\mathcal{P}(C \cup D) = \mathcal{P}(C) \cup \mathcal{P}(D)$的“证明”有什么问题?

Let $X \in \mathcal{P}(C \cup D)$ be arbitrary and fixed.

This means $X \subseteq C \cup D$.

So, $X \subseteq C \vee X \subseteq D$.

Then, $X \in \mathcal{P}(C) \vee X \in \mathcal{P}(D)$.

Thus, $X \in \mathcal{P}(C) \cup \mathcal{P}(D)$.

Therefore, $\mathcal{P}(C \cup D) = \mathcal{P}(C) \cup \mathcal{P}(D)$.

Problem 4.11.16. 假设 $x \in \mathbb{Z}$ 和 x^2 是8的倍数。证明 x 是偶数。此命题的逆命题 True 是否成立？如果成立，证明它；如果不成立，给出反例。

Problem 4.11.17. 定义命题 $E(z)$ 为“z 是偶数。证明

$$\forall z \in \mathbb{Z}\text{.}\ E(z) \iff E(z^3)$$

Problem 4.11.18. 使用问题4.11.17的结果来证明$\sqrt[3]{\wedge}2$ 是无理数。

Problem 4.11.19. 让 $P = \{y \in \mathbb{R} \mid y > 0\}$。证明

$$\bigcap_{x \in P} \left\{ y \in \mathbb{R} \mid 1 - \frac{1}{x} < y < 2 \right\} = \{z \in \mathbb{R} \mid 1 < z < 2\}$$

Problem 4.11.20. 设 $A, B, C \subseteq U$ 为集合。定义

$$S = \big((A \cap \overline{B}) \cup C\big) - A$$

和

$$T = C - (A \cup B)$$

是 $S \subseteq T$ 吗？如果是，请证明它；否则，找到一个反例 e.

是 $T \subseteq S$ 吗？如果是，请证明它；否则，找到一个反例 请。Translated Text: {v*}

Problem 4.11.21. 对于每个 $x \in \mathbb{R}$，定义集合

$$S_x = \{y \in \mathbb{R} \mid -x \leq y \leq x\}$$

此外，定义集合

$$P = \{y \in \mathbb{R} \mid y > 0\}$$

证明以下每个命题。

$$\bigcap_{x \in P} S_x = \{0\}$$

$$\bigcap_{x \in \mathbb{N}} S_x = \{y \in \mathbb{R} \mid -1 \leq y \leq 1\}$$

Problem 4.11.22. 设 $P(x)$ 为变量命题

$$\text{“ } \frac{x^2+4}{x^2+1} < 1 + \frac{1}{x} \text{ ”}$$

并且让 $Q(x)$ 成为变量命题

$$\text{“ } \frac{x^2-4}{x^2+1} > 1 - \frac{1}{x} \text{ ”}$$

Also, let $S = \{x \in \mathbb{R} \mid x > 0\}$ be the set of positive real numbers成员。

对于以下每个陈述，确定它是否为True（，如果是，则提供证明)或False（，如果是，则提供反例并展示其有效性)。

(a) $\forall x \in S.\ P(x) \implies Q(x).\ Q(x) \implies P(x)$

(b) $\forall x \in S$

Problem 4.11.23. 设 A 和 B 为任意两个集合。证明 在

$$A \times B = B \times A \iff (A = B \ \vee \ A = \varnothing \ \vee \ B = \varnothing)$$

(别忘了这是一个 *if and only if* 主张！)

Problem 4.11.24. 设 A, B, C, D 为任意集合。证明

$$(A \times B) \cap (C \times D) = \varnothing \iff \big(A \times B = \varnothing \vee C \times D = \varnothing\big)$$

Problem 4.11.25. 设 B 为任意集合。设 I 为一个指标集，并设 A_i 为每个 $i \in I$ 的集合。证明以下集合等式:

(a) $\left(\bigcap_{i\in I} A_i\right) - B = \bigcap_{i\in I}(A_i - B)$

(b) $\left(\bigcup_{i\in I} A_i\right) - B = \bigcup_{i\in I}(A_i - B)$

(c) $\left(\bigcap_{i\in I} A_i\right) \times B = \bigcap_{i\in I}(A_i \times B)$

(d) $\left(\bigcup_{i\in I} A_i\right) \times B = \bigcup_{i\in I}(A_i \times B)$

(e) $B - \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(B - A_i)$

(f) $B - \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I}(B - A_i)$

Problem 4.11.26. 在这个问题中，你将证明有理数 $\mathbb{Q}$ 是 **dense**。也就是说，我们希望考虑以下命题:

Proposition. Strictly between any two distinct rational numbers lies another rational number.

重述此主张使用逻辑符号，然后 **prove** 它。

Problem 4.11.27. 此问题旨在引入**unique- ness**的概念。我们说具有某种属性的对象是**unique**，如果它具有所需的属性，但没有**other**对象具有该属性。

这意味着，我们可以说 x 是具有属性 $P(x)$ 的 S 的唯一元素，当且仅当

$$\exists x \in S \text{ . } P(x) \wedge (\forall y \in S \text{ . } y \neq x \implies \neg P(y))$$

请注意，这与以下逻辑等价{v*}

$$\exists x \in S \text{ . } P(x) \wedge (\forall y \in S - \{x\} \text{ . } \neg P(y))$$

此外，我们还可以写出逆否命题:

$$\exists x \in S \text{ . } P(x) \wedge (\forall y \in S \text{ . } P(y) \implies x = y)$$

使用此方法用逻辑符号重述以下主张。然后，**prove**它。

Claim: 方程 *natural* 有一个唯一的 $n^3 - n - 6 = 0$ 根。

Problem 4.11.28. 此问题提供了一个新集合运算的定义（用其他运算定义）并要求你使用此运算证明几个集合包含和等式。

Definition: 设 A, B 为集合。A 和 B 的 **symmetric difference** 表示为 $A\Delta B$ ，并定义为

$$A\Delta B = (A - B) \cup (B - A)$$

现在，令 A, B, C 为任意集合。证明以下内容:

(a) $A\Delta A = \varnothing$b) $A\Delta B = B\Delta A$

(

(c) $A\Delta\varnothing = \varnothing$

(d) $A \subseteq B \implies A\Delta B = B - A$

(e) $A\Delta(B\Delta C) = (A\Delta B)\Delta C$

(f) $\overline{A}\Delta\overline{B} = A\Delta B$ (假设 $A, B \subseteq U$)

(g) $(A\Delta B) \cap C = (A \cap C)\Delta(B \cap C) = (A\Delta B) - C$

Problem 4.11.29. 在这个问题中，你将证明关于 **primality testing** 的一个有用结果。现代密码学的大部分基于将大合数分解为其质因数的事实。以下命题说明我们只需要检查 *up until* $\sqrt{p}$ 作为 p 的因数。

Proposition. Let p be a natural number that is at least 2. If none of the natural numbers between 2 and $\sqrt{p}$ (inclusive) divide p, then p is prime.

回忆："|"的正式定义是

给定 $a, b \in \mathbb{Z}$，我们写 $a \mid b$ 当且仅当 $\exists k \in \mathbb{Z}$。 $b = ak$.

重述上述命题使用逻辑符号。然后，**prove**它。

（**Hint:** 考虑该命题的逆否命题……）

Problem 4.11.30. 设 A, B 为任意集合。证明以下命题：

$$A \times B = B \times A \iff (A = B \vee A = \varnothing \vee B = \varnothing)$$

Problem 4.11.31. 设S, T为元素也是集合的集合。对于以下每个陈述，要么**prove**该陈述在一般情况下成立，或者提供一个反例：

(a) $\displaystyle\bigcup_{X \in S \cup T} X \subseteq \left(\bigcup_{Y \in S} Y\right) \cup \left(\bigcup_{Z \in T} Z\right)$

(b) $\displaystyle\bigcup_{X \in S \cup T} X \supseteq \left(\bigcup_{Y \in S} Y\right) \cup \left(\bigcup_{Z \in T} Z\right)$

(c) $\displaystyle\bigcap_{X \in S \cup T} X \subseteq \left(\bigcap_{Y \in S} Y\right) \cap \left(\bigcap_{Z \in T} Z\right)$

(d) $\displaystyle\bigcap_{X \in S \cup T} X \supseteq \left(\bigcap_{Y \in S} Y\right) \cap \left(\bigcap_{Z \in T} Z\right)$

4.12 Lookahead

现在我们已经拥有了所有这些数学工具——并且我们已经很好地利用了它们，通过大量的练习来磨练我们的技能——我们更有能力踏入数学的荒野。我们将探索数学的各个分支，学习一些基本的概念和符号，并将我们的证明策略应用于新的奇妙结果。

在这样做之前，我们首先需要处理一个悬而未决的问题：我们想要*formalize*归纳。在此之前，我们对归纳究竟是什么以及它是如何工作的只是“挥了挥手”。我们给出了“多米诺类比”，并在一些例子中使用了它。但现在我们有了必要的术语和知识，可以正确地描述数学归纳法及其各种形式。再次翻阅第二章，提醒自己一些我们使用归纳论证的示例可能是个好主意。你还记得多米诺类比吗？你能预测我们如何形式化数学归纳法原理吗？你能向朋友解释那个定理并说服他们吗？试试吧！然后，继续阅读！

Chapter 5

Rigorous Mathematical Induction: A Formal Restatement

5.1 Introduction

似乎我们在已经讨论了数学归纳法之后又包括这一章显得有些重复。然而，我们的目标很多，你之后会看到为什么我们稍微回顾一下，再次讨论这一材料。

首先，我们对如何处理归纳的初始方法感到有些不舒服。从数学角度来说。其次，我们在第二章留下了一些悬而未决的问题。我们看到的某些后续例子，如Takeaway游戏和汉诺塔，有什么不同？它们在归纳论证中似乎比其他例子，如我们的$\sum_{k\in[n]} k = \frac{n(n+1)}{2}$证明，使用了“更多假设”吗？我们认为是这样，我们将在这里阐述这些差异。第三，还有很多有趣的例子有待观察，它们本身就有价值，通过解决这些问题将有助于我们发展对彼此开始使用的数学语言的了解。第四，本章最后陈述并证明的定理（在您的帮助下！）将是*equivalence*的一个引人注目的例子；具体来说，我们将表明三个定理都通过双条件语句相互联系！（这将是我们指出的“以下都是等价的……”风格定理的第一个伟大例子，就像我们在4.9.6节中提到的双条件语句的证明策略一样。）

5.1.1 Objectives

因为我们之前已经讨论过归纳法，现在只是回到这个话题，所以我们将在本章开头省略通常的介绍内容。

相反，我们将通过一系列陈述在此总结本章的主要目标。

By the end of this chapter, you should be able to ...

- 数学归纳法原理及其证明与自然数集的关系描述如下。
- 强数学归纳法原理，将其与先前的原理进行比较和对比，并描述其证明方法。
- 使用归纳论证来证明主张，尤其是在需要强烈归纳论证的情况下，要识别出来。
- 理解并解释数学归纳法的几种变体，并确定这些变体可能有用的问题。
- 陈述良序原理并解释其与数学归纳法的关系。

5.2 Regular Induction

本节讨论我们之前见过的归纳论证类型。您将在下一节中看到，为什么我们会选择将其称为“常规”归纳。

5.2.1 Theorem Statement and Proof

这里，让我们回顾一下我们在第3章给出的
Principle of Mathematical Induction 的陈述。思考它是如何遵循 **Domino Analogy**，或者哪个类比最适合帮助你理解归纳过程。如果你没有完成关于定义 $\mathbb{N}$ 的可选阅读，可能会错过这个定理陈述，但没关系。我们相信你仍然可以阅读它并以与归纳过程相对应的方式构建它。

Theorem 5.2.1 (数学归纳法原理)**.** *Let $P(n)$ be some "fact" or "observation" that depends on the natural number n. Assume that*

1. *$P(1)$ is a true statement.*
2. *Given any $k \in \mathbb{N}$, if $P(k)$ is true, then we can conclude* 必然 *that $P(k+1)$ is true.*

Then the statement $P(n)$ must be true for 每个 *natural number $n \in \mathbb{N}$.*

看看所有这些冗长的句子、短语和模糊的术语。一些依赖于自然数的“事实”？听起来像是一个 **variable propo- sition**，对吧？“如果……那么我们可以必然得出……”听起来像是一个 **con- ditional statement**，不是吗？所有这些语言都是为了表达某些逻辑基础，现在我们可以用前一章中开发的概念和符号重述整个定理。在查看我们的版本之前，先试试自己来做这个。同时，试着回忆我们是如何 *proved* 那个定理的。（再次提醒，如果你跳过了这个可选阅读，可能错过了这一点，没关系。）回顾第3.8.2节，提醒自己，因为我们在这里将遵循相同的证明，但我们将使用我们现在拥有的逻辑符号和工具。准备好了吗？我们开始了！

Theorem 5.2.2 (数学归纳法原理)**.** *Let $P(n)$ be a variable proposition. Suppose that*

(1) $P(1)$ holds True*, and*

(2) $\forall k \in \mathbb{N}\,.\, P(k) \implies P(k+1)$ holds True

Then $\forall n \in \mathbb{N}\,.\, P(n)$ holds True*.*

这便是全部！这包含了所有相同的思想——某个初始事实成立，并且每个事实都暗示下一个事实，使得所有事实都成立——但它使用逻辑符号和语言来实现。你看到它们说的是同一件事了吗？在继续阅读之前，请确保你明白了！

我们的目标是现在 *prove* 这个定理。是的，我们将证明数学归纳法是一种有效的证明技术！我们为什么不能呢？我们通过真值表证明了条件语句与它的逆否命题在逻辑上是等价的，这给了我们一个证明策略。我们为什么不能证明这个，同样呢？

在展示证明之前，我们希望您先阅读关于定义自然数的章节，即第3.8节。该章节包含以下关键定义，这些定义我们将用于接下来的证明。在该章节中，我们定义了什么是**inductive set**，然后指出$\mathbb{N}$是“最小”的归纳集，即$\mathbb{N}$是宇宙中所有归纳集的*subset*。这正是我们希望$\mathbb{N}$拥有的性质，而这些定义使得这一点成为可能。我们将在这里给出这些重要的定义——稍作修改，使用逻辑符号，并省略一些集合论概念——但我们也建议您阅读该章节，以掌握讨论的全部范围。

Definition 5.2.3. *Let I be a set. If the following conditions hold:*

1. *$1 \in I$,*
2. *For any element k, the implication $k \in I \implies k+1 \in I$ holds;*

then I is called an **inductive set***.*

Definition 5.2.4. *The set of all* ***natural numbers*** *is the set*

$$\mathbb{N} := \{x \mid \text{ for every inductive set } I,\ x \in I\}$$

Put another way, $\mathbb{N}$ *is the* 最小的 *inductive set:*

$$\mathbb{N} = \bigcap_{I \in \{S \mid S \text{ is inductive}\}} I$$

好的，现在我们准备好进行证明了！

Proof. 设 $P(n)$ 为一个变量命题，定义于每一个自然数 n。假设定理中给出的两个条件确实成立，即

(1) $P(1)$ 满足 True，并且

(2) $\forall k \in \mathbb{N}.\ P(k) \implies P(k+1)$ holds True

设 S 为满足 $P(n)$ 是 True 的实例集合。即，定义

$$S = \{n \in \mathbb{N} \mid P(n) \text{ is True}\}$$

根据定义（使用集合构造符号），$S \subseteq \mathbb{N}$。

条件（1）保证了$1 \in S$。

条件（2）保证了 $\forall k \in \mathbb{N}.\ k \in S \implies k+1 \in S$。

这两个条件共同保证 S 是一个 *inductive* 集合。根据上面定义的 $\mathbb{N}$，因此我们知道 $\mathbb{N} \subseteq S$。

因此，通过一个双重包含论证 $S = \mathbb{N}$。这意味着陈述 $\forall n \in \mathbb{N}.\ P(n)$ is True 对一自然数成立，即

理解这些用到的集合论力学并非使用归纳法所必需的。然而，我们认为思考这些逻辑基础只能帮助您理解，或者激发对数学逻辑和集合理论的某些好奇心，或者可能两者兼而有之！

我们在这里通过重申PMI所取得的重大成果是，我们现在有了一个明确的方法来判断一个归纳论证是否成功。整个“归纳证明”的核心在于验证定理陈述中的条件（1）和（2）（即验证命题$P(n)$的“真集”是一个归纳集）。

5.2.2 Using Induction: Proof Template

根据上述观察，我们可以为适当的 **“proof by induction”** 开发一个证明模板。（这也可以添加到上一章的证明策略列表中，从而扩展我们的数学工具箱！）请注意，这个模板中的所有步骤都是为了使我们的证明易于阅读、有序且逻辑正确：

- 我们必须定义一个命题 $P(n)$ 以向读者展示我们旨在证明的内容。

- 我们必须验证 **Base Case (BC)** 以证明 PMI 中的条件（1）得到满足。

- 我们必须验证条件语句 $\forall k \in \mathbb{N}_{\circ}$

  $P(k) \implies P(k+1)$

  to show that condition (2) in the PMI is satisfied. To do this, we will apply the direct proof strategy for proving conditional statements; this has two parts:

  - First, we assume that k is an arbitrary natural number and suppose $P(k)$ holds. This is the **Inductive Hypothesis (IH)**, which introduces an arbitrary variable k and supposes $P(k)$ holds.
  - Second, we go through the **Inductive Step (IS)**, which takes that assumption and deduces that $P(k+1)$, also holds.

  Finally, we make this conclusion to remind our reader of what we have accomplished.

在以下步骤之间——**BC**、**IH** 和 **IS**——我们已验证了PMI的条件，我们可以得出结论：$\forall n \in \mathbb{N}_{\circ}$ $P(n)$.

Template for a "Proof by Induction"

Goal: 证明 $\forall n \in \mathbb{N}_{\circ}$ $P(n)$

Proof.

设 $P(n)$ 为命题 "_____"。我们将证明 $\forall n \in \mathbb{N}_{\circ}$ $P(n)$ by induction on n.

Base Case: Observe that $P(1)$ holds because _____.

Induction Hypothesis: Let $k \in \mathbb{N}$ be arbitrary and fixed. Suppose $P(k)$ holds.

Induction Step: Deduce that $P(k+1)$ also holds.

根据PMI，可以得出 $\forall n \in \mathbb{N}_{\circ}$ $P(n)$. □

Comments and Common Pitfalls

以下是一些推荐和建议。这些基于我们认为构成良好、撰写得当的归纳论证，以及我们在多年中看到学生持续犯的一些错误。

- **Be sure to *define* a proposition.**

  有时，某个主张在问题或练习的陈述中为你定义。然而，它并不总是被明确地定义为 $P(n)$。在这种情况下，稍后引用一个命题 $P(n)$ 没有意义。因此，如果你想引用它，一定要 *define* 一个陈述！

  为了简洁，你可能会说“设 $P(n)$ 为定义的断言”

以上。”（然而，为确保一致性，请确保n确实是上述主张中使用的变量字母！）

- **Explicitly state that you are using mathematical induction and state the variable to which you are applying induction.**

  未来，你可能会遇到一个包含多个变量字母的归纳证明。此外，尽管你的整体证明遵循某种归纳结构，但你是否必然期望读者能理解你正在使用归纳。提前告诉他们这个信息可以节省他们很多麻烦。

- **Be as *explicit* and thorough as possible in the Base Case.**

  仅写出 $P(1)$ 的含义，并期望读者理解为什么它是 True。这个责任在你，证明者身上！

  仅写出陈述 $P(1)$ 本身，并在其旁边放一个 ✓。这并不能证明任何东西！

  如果命题 $P(1)$ 是某种方程（这是常见的），则证明两边的实际相等性，而不仅仅是写出方程并期望读者看到为什么它成立。

- **The IH and IS together apply the** *direct proof strategy* **for $\implies$ statements.**

  IH引入一个任意且固定的自然数，并假设蕴涵的左边为 $P(k) \implies P(k+1)$。这就是我们的*hypothesis*。然后我们使用这个假设来推导$P(k+1)$。这证明了PMI中条件(2)的命题。

  请确保在这里*quantify*变量k！像“假设$P(k)$”这样的陈述没有意义。k是什么？它是一个自然数吗？

  “设 $k \in \mathbb{N}$ 并假设 $P(k)$” 在这里是一种可接受的表述。“设 $k \in \mathbb{N}$”，对于一个数学读者来说，隐含地意味着“设 $k \in \mathbb{N}$ (为任意且固定的)”。

- **It helps to explicitly write out what $P(k)$ means in the IH.**

  首先，这有助于读者理解你的假设并更好地跟随证明的其余部分。

  但这也帮助你 *you* 理解如何证明 $P(k+1)$，这是你在这个步骤中的目标。如果你在脑海中（可能在考试或家庭作业问题中）难以完成这个步骤，只需在纸张顶部写下 $P(k)$ 的含义，并在底部写下 $P(k+1)$ 的含义。现在你看到它们之间可能存在的联系了吗？尝试从 $P(k)$ 向下工作，从 $P(k+1)$ 向上工作，并在中间将它们连接起来。

- **You *must* invoke the IH somewhere in the Induction Step!**

  如果你根本没使用过 **IH**，那你为什么还要使用归纳法？当你使用 **IH**, *say that you are doing so*。不要期望读者能记住/认出你正在这样做。

- **Make a conclusion.**

  告诉读者你取得了什么成就。

好的，既然我们已经讨论了如何写一个好的归纳证明，那么我们就实际来做一下！

5.2.3 Examples

这里有一些好的归纳证明的例子。在撰写自己的证明时，请以它们为指南。我们在这里省略了关于我们如何提出论点的通常讨论，部分原因是我们只想强调证明的 *structure*，但也因为我们已经在第二章中广泛研究了那些问题解决方面。

请注意，我们在这些证明的一些组成部分中使用了缩写，即 **BC** (表示基本情形) 和 **IH** (表示归纳假设) 和 **IS** (表示归纳步骤)。请随意使用这种简写！

Example 5.2.5. *Sum of the odds is a square:*

Claim: 第一个 n 个奇数自然数的和是 n^2。

(注意：我们在第1.4.3节中已经把这个说法作为一个谜题看到了，然后在第2.3.4节中要求你通过归纳细节进行工作。我们将在这里给出这个说法的一个良好证明。)

Proof. 设 $P(n)$ 为命题

$$\text{“}\quad 1+3+5+\cdots+2n-1=\sum_{i=1}^{n}(2i-1)=n^2\quad\text{”}$$

我们将证明 $\forall n\in\mathbb{N}_{\mathsf{O}}\quad P(n)$ by induction on n.

BC: 考虑 $n=1$. 注意到

$$\sum_{i=1}^{1}(2i-1)=1\quad\text{and}\quad 1^2=1$$

然后

$$\sum_{i=1}^{1}(2i-1)=1^2$$

因此，$P(1)$ 是 True，因为 $1=1$。

IH: 让 $k \in \mathbb{N}$ 任意和固定。假设 $P(k)$ 成立。这 意味着

$$\sum_{i=1}^{n}(2k-1) = n^2$$

IS: 考虑 $k+1$. 我们可以写

$$\sum_{i=1}^{k+1}(2i-1) = 2(k+1) - 1 + \sum_{i=1}^{k}(2i-1) = 2k + 1 + \sum_{i=1}^{k}(2i-1)$$

通过分离求和中的 $(k+1)$-th 项。

我们现在使用 **IH** 来替换右侧的求和，并推导出

$$\sum_{i=1}^{k+1}(2i-1) = 2k + 1 + k^2$$

因式分解告诉我们

$$\sum_{i=1}^{k+1}(2i-1) = (k+1)^2$$

因此 $P(k+1)$ 成立。

根据PMI，我们得出结论：$\forall n \in \mathbb{N}_{\bigcirc} \quad P(n)$. □

这是关于几何级数的一个有用事实的另一个好的归纳证明。*Example* 5.2.6 *. Geometric series formula:*

Claim: 对于每个 $q \in \mathbb{R} - \{0, 1\}$ 以及对于每个 $n \in \mathbb{N}$，以下公式成立：

$$\sum_{i=0}^{n-1} q^i = 1 + q + q^2 + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}$$

Proof. 让 $q \in \mathbb{R} - \{0, 1\}$ 为任意且固定的。定义 $P(n)$ 为命题

$$\text{“} \sum_{i=0}^{n-1} q^i = \frac{q^n - 1}{q - 1} \text{”}$$

我们将证明 $\forall n \in \mathbb{N}_{\bigcirc} \quad P(n)$ by induction on n.

BC: 考虑 $n = 1$. 注意到

$$\sum_{i=0}^{n-1} q^i = \sum_{i=0}^{0} q^i = q^0 = 1$$

自 $q \neq 0$。此外，观察一下

$$\frac{q^n - 1}{q - 1} = \frac{q - 1}{q - 1} = 1$$

自 $q \neq 1$。因此，$P(1)$ 成立。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的，并假设 $P(k)$ 成立。这意味着

$$\sum_{i=0}^{k-1} q^i = \frac{q^k - 1}{q - 1}$$

IS: WWTS $P(k+1)$ 保持。 (记住，WWTS 表示“我们想展示”。) 即 WWTS

$$\sum_{i=0}^{k} q^i = \frac{q^{k+1} - 1}{q - 1}$$

注意到 $(k+1) - 1 = k$。

观察我们可以代数化简并利用我们的假设来写出

$$\begin{aligned}
\sum_{i=0}^{k} q^i &= \left(\sum_{i=0}^{k-1} q^i\right) + q^k && \text{summation notation} \\
&= \frac{q^k - 1}{q - 1} + q^k && \text{invoking } \mathbf{IH} \\
&= \frac{q^k - 1 + q^k(q-1)}{q - 1} && \text{common denominator} \\
&= \frac{q^k - 1 + q^{k+1} - q^k}{q - 1} = \frac{q^{k+1} - 1}{q - 1} && \text{algebra}
\end{aligned}$$

这表明 $P(k+1)$ 也成立。

□

根据PMI, $\forall n \in \mathbb{N}_{\mathbf{O}}$ $P(n)$ holds.

Follow-up question: 为什么我们在索赔中需要 $q \notin \{0, 1\}$?

当 $q = 0$ 时会发生什么？这个证明在哪里失效？公式仍然成立吗？如果是这样，请证明它。如果不是，你能修复它吗?

尝试也为 $q = 1$ 提出同样的问题。

5.2.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆!

(1) PMI（数学归纳原理）说明了什么？它是如何被证明的?

(2) 归纳证明的基本情况是什么？它与PMI的陈述有何关系？（3）证明中的归纳假设和归纳步骤是如何相关的？它们与PMI的陈述有何关系？（4）为什么在归纳步骤中某处调用归纳假设很重要？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 证明以下公式：{v*}

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

适用于每个 $n \in \mathbb{N}$。

(2) 证明每个奇数自然数的平方比8的倍数多1。也就是说，证明

$$(2n+1)^2 - 1 \text{ is a multiple of } 8$$

对于每个 $n \in \mathbb{N}$。

(3) 考虑以下主张：$7^n - 4^n$ 是3的倍数，对于每一个 $n \in \mathbb{N}$。

使用逻辑符号表示法重写这个命题。然后，通过归纳法证明它。

(4) 回想一下，斐波那契数列由以下定义：

$$f_0 = 0 \text{ and } f_1 = 1 \text{ and } \forall n \in \mathbb{N} - \{1\}\,.\; f_n = f_{n-1} + f_{n-2}$$

证明以下命题对每个 $n \in \mathbb{N}$ 都成立，通过 n 的归纳法：

(a) $\sum_{i=1}^{n} f_i = f_{n+2} - 1$ (b) $\sum_{i=1}^{n} f_{2i-1} = f_{2n}$ c) f_{4n} 是3的倍数 (d) **Challenge 1:** (n 是3的倍数) $\implies$ (f_n 是偶数) (e) **Challenge 2:** (n 是 *not* 的3倍) $\implies$ (f_n 是奇数)

5.3 Other Variants of Induction

现在我们已经非常熟悉归纳法的工作原理，并且看到了许多例子，我们可以向您展示这种方法的两处修改。想法是使用归纳法证明一个命题对每个 $n \in \mathbb{N}$ 都成立并没有“特别之处”。请别误会；关于 $\mathbb{N}$ 的 *lot* 确实是“特别”的！我们的意思是，可以使用归纳法证明一个命题对每个 $n \in S$ 都成立，其中 S 可能是其他类型的集合。在接下来的讨论和例子中，我们将为您描述这些集合。

5.3.1 Starting with a Base Case other than $n = 1$

我们需要在归纳证明中有一个基本情况，但并没有说它总是必须是 $n = 1$。也许我们有一个命题 $P(n)$，它在 True 对于 $n = 1$ 和 $n = 2$ 时成立，但后来 somehow False 对于 $n = 3$ 和 $n = 4$，然后 True 对于每个至少是 n 5 的 $n =$。我们如何证明这些说法呢？嗯，我们可以分别展示 $n = 1, 2, 3, 4$ 的个别情况，然后使用归纳法证明所有其他情况。这会起作用，因为集合 $\mathbb{N} - \{1, 2, 3, 4\}$ 也是一个 *inductive set*。从多米诺骨牌类比的角度来看，这就好比说，“让我们跳过几个多米诺骨牌，从 $n = 5$ 开始让整行倒下。其余的都会以我们预期的完全相同的方式倒下。”

实际上，我们甚至可以在这里谈论 *negative* 个整数！让我们在数轴上稍微向左滑动，想象我们实际上有一列从，比如说，-3 开始编号的骨牌。也就是说，我们会有一号骨牌 -3 和二号骨牌 -2 和一号骨牌 -1 和骨牌 #0 和骨牌 #1 以及所有其他的骨牌。我们可以从 $n = -3$ 开始让骨牌倒下，并且知道它们会像之前一样全部倒在一起。

整个想法是这样的，我们仍然有一排无穷无尽的骨牌向右移动，它们之间没有空隙。我们给 *first* 骨牌分配什么数字标签都无关紧要。无论我们如何编号第一个骨牌，这样的骨牌排都会相互倒塌。这个想法就是下一个定理所包含的内容。

Theorem 5.3.1 (归纳任何基准情况)**.** *Let $P(n)$ be a variable proposition. Let $M \in \mathbb{Z}$ be arbitrary and fixed.*

Let $S = \{z \in \mathbb{Z} \mid z \geq M\}$.

Suppose that

(1) $P(M)$ holds True*, and*

(2) $\forall k \in S \bullet P(k) \implies P(k+1)$ holds True

Then $\forall n \in S \bullet P(n)$ holds True*.*

这个定理恰好是我们所讨论的内容：如果我们想证明一个命题对于大于或等于某个特定值（定理陈述中的M）的每个值都成立，那么我们只需从那个值开始进行归纳即可。

我们将其作为我们的 **BC** 并将 **IH** 和 **IS** 应用到大于或等于它的每个值上。其他一切完全相同。

Formal Proof

为了说明和完整性起见，我们将正式*prove*这个定理。我们希望上述讨论——参考多米诺类比——能帮助你直观地理解它是如何工作的。通过这个证明的工作不会直接和立即影响你应用归纳作为技术的能力。然而，我们确实认为阅读它并尝试理解*how*它是如何工作的将使你对归纳和证明技术有更好的掌握，也许还会使你对这里工作的数学有更深的欣赏。具体来说，我们将使用PMI来证明这个自我修改版本的定理！

Proof. 设 $P(n)$ 为一个变量命题。设 $M \in \mathbb{Z}$ 为任意且固定的。

Let $S = \{z \in \mathbb{Z} \mid z \geq M\}$.

假设，{v*}

(1) $P(M)$ 保留 True，并且

(2) $\forall k \in S\text{.}\ P(k) \implies P(k+1)$ holds True

我们的目标是证明 $\forall n \in S_{\bigcirc}$ $P(n)$ holds True.

定义命题 $Q(n)$ 通过设置

$$Q(n) \iff P(n+M-1)$$

注意，通过代数操作不等式，我们得到

$$n \geq 1 \iff n+M-1 \geq M$$

这意味着我们的目标现在是要证明 $\forall n \in \mathbb{N}_{\bigcirc}$ $Q(n)$ holds True.

（这样做将证明 $\forall n \in S_{\bigcirc}$ $P(n)$.）

我们将通过在 n 上的归纳法来证明这一点。

BC: 我们知道 $P(M)$ 成立，根据假设。注意 $n+M-1 = M \iff n = 1$。这意味着 $Q(1)$ 成立。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $Q(k)$ 成立。

IS: 由于 $Q(k)$ 成立，我们知道 $P(k+M-1)$ 成立。

此外，自 $k \in \mathbb{N}$ 以来，我们知道 $k \geq 1$。因此，$k+M-1 \geq M$。

因此，根据我们假设的条件（(2)），我们可以推导出 $P((k+M-1)+1)$ 成立，即 $P(k+M)$ 成立。

这告诉我们 $Q(k+1)$ 成立。

通过PMI，我们推断出 $\forall n \in \mathbb{N}_{\bigcirc}$ $Q(n)$ holds.

然后，根据 $Q(n)$ 的定义，这告诉我们 $\forall n \in S_{\bigcirc}$ $P(n)$ holds. □

正如我们所说，尝试理解证明的细节，但总的来说，只需记住我们只是在“滑动”并使用不同的基本情况。归纳过程的机制是相同的。

Example

让我们看看这种修改后的技术在行动中的样子。事实上，我们将向您展示的例子正是我们在介绍这种方法时暗示的那种类型，其中某些命题对一些小的值成立，对其他一些小的值不成立，但自某个点之后对所有值都成立。

Example 5.3.2. *How* 2^n *compares to* n^2*:*

Claim:

$$2^n > n^2 \iff n \in \{0, 1\} \cup \{z \in \mathbb{N} \mid z \geq 5\}$$

这是，满足$2^z > z^2$的*only*整数z是0, 1, 5, 6, 7 . . .。

(我们将把这个任务留给你去探索并弄清楚我们是如何提出这样的说法的。通常，正如你将在本节练习中看到的那样，这样的不等式可能会与问题一起提出，“对于哪些 n 的值，这个不等式成立？”在这种情况下，你需要在开始归纳证明之前做一些基础工作来识别你的说法。)

Proof. 设 $P(n)$ 为命题“$2^n > n^2$”。

首先，观察以下情况:

$$\begin{aligned}
&2^0 > 0^2 \iff 1 > 0 && \text{so } P(0) \text{ is True}\\
&2^1 > 1^2 \iff 2 > 1 && \text{so } P(1) \text{ is True}\\
&2^2 > 2^2 \iff 4 > 4 && \text{so } P(2) \text{ is False}\\
&2^3 > 3^2 \iff 8 > 9 && \text{so } P(3) \text{ is False}\\
&2^4 > 4^2 \iff 16 > 16 && \text{so } P(4) \text{ is False}
\end{aligned}$$

注意，每当 $z \leq -1$ 时，我们有 $2^z < 1$ 和 $z^2 \geq 1$，所以 $2^z \not> z^2$。因此，对于每个满足 $n \leq -1$ 的 n，$P(n)$ 是 False。

接下来，定义 S 为集合 $S = \{z \in \mathbb{N} \mid z \geq 5\}$。

我们将证明 $\forall n \in S$, $P(n)$ holds by induction on n.

BC: 观察 $P(5)$ 成立，因为 $2^5 = 32$ 且 $5^2 = 25$ 且 $32 > 25$。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $P(k)$ 成立。

IS: 自 $k \in S$ 以来，我们知道 $k \geq 5$，因此 $k > 4$。

因此，$k - 1 > 3$ 以及所以 $(k-1)^2 > 9$；当然，那么，$(k-1)^2 > 2$。

观察以下对不等式的以下操作链 ality:

$$\begin{aligned}(k-1)^2 > 2 &\implies (k-1)^2 - 2 > 0\\ &\implies k^2 - 2k - 1 > 0\\ &\implies k^2 > 2k + 1\\ &\implies 2k^2 > k^2 + 2k + 1\\ &\implies 2k^2 > (k+1)^2\end{aligned}$$

自我们观察到第一个不等式成立，我们可以推断出上面的最终不等式也成立。

（注意：如果你没有意识到，这个推理链是第4.9.9节练习2的解决方案！为了解决这个问题，我们做了一些草稿，从底部的所需不等式开始，“逆向工作”直到我们发现显然的True。在这里写下来时，我们是从这个明显的事实开始，一直工作到所需的结论。）

通过 **IH** $P(k)$，我们知道 $k^2 < 2^k$。这告诉我们

$$2k^2 < 2 \cdot 2^k = 2^{k+1}$$

应用不等式的传递性，我们可以推导出

$$(k+1)^2 < 2k^2 < 2^{k+1}$$

因此 $P(k+1)$ 成立。

根据PMI, $\forall n \in S$, $P(n)$ holds.

总体上，我们考虑了每个 $z \in \mathbb{Z}$。我们观察到 $P(z)$ 对于 $z \leq -1$ 失败，对于 $z = 0, 1$ 成立，对于 $z = 2, 3, 4$ 失败，并且对于 $z \geq 5$ 成立。这些观察结果共同证明了该主张。 □

哇！实际上那个证明中有很多内容。你注意到那个主张被表述为 {v*}，所以我们不得不在我们的证明中考虑 *all* 整数吗？这很棘手，但我们做到了！

5.3.2 Inducting Backwards

这种归纳变体在命题 $P(n)$ 对于所有 n *less* 的值都恰好成立时很有用。从多米诺类比的角度来看，这就像想象我们的无限多米诺骨牌向左而不是向右倒下。我们已经知道，根据前一小节讨论的原因，我们如何编号并不重要。现在，我们可以看到，它们要去哪里也不重要！*direction*；它们将遵循相同的原理！以下定理概括了这个观察结果。

Theorem 5.3.3 (反向归纳)**.** *Let $P(n)$ be a variable proposition. Let $M \in \mathbb{Z}$ be arbitrary and fixed.*

Let $S = \{z \in \mathbb{Z} \mid z \leq M\}$.

Suppose that

(1) $P(M)$ *holds* True*, and*

(2) $\forall k \in S \bullet P(k) \implies P(k-1)$ *holds* True

Then $\forall n \in S \bullet P(n)$ *holds* True*.*

请注意本定理与定理5.3.1之间的区别

Formal Proof

在这个开发阶段，我们感到可以放心地给出 you 个重要定理来证明。具体来说，我们希望你们证明上面看到的这个修改后的PMI版本，定理5.3.3！让你们自己处理细节，而不是仅仅看到我们为你们执行它们，从长远来看会更有帮助。此外，我们心中这个证明的细节与我们之前给出的（在第5.3.1节）定理5.3.1的证明非常相似。

在数学中，将证明留给“读者作为练习”实际上相当常见，尤其是在数学书籍中。我们只是在尽我们的一份力，帮助你习惯这种现象！☺

Proof. 作为第5.3.4节中的练习1留给读者。 □

我们将不会展示这个方法在实际中的例子，因为我们认为它与我们已经看到的标准的归纳方法完全一样。实际上，如果你仔细研究上面证明的细节，你甚至可能看到如何“构造”本节的一个例子，只需修改一些我们之前看到的例子即可！（如果我们反转一个不等式……）

5.3.3 Inducting on the Evens/Odds

让我们用一个观察来激发这一节，这将引导我们进入这种方法的第一种应用示例。考虑完全平方数的序列:

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ \ldots$$

看看当我们把它们除以8时会发生什么；具体看看由每个情况中分数的分子所指示的 $re\text{-}\ mainders$ (:

$$0+\frac{1}{8},\ 0+\frac{4}{8},\ 1+\frac{1}{8},\ 2+\frac{0}{8},\ 3+\frac{1}{8},\ 4+\frac{2}{8},\ 6+\frac{1}{8},\ \ldots$$

注意，我们将分数如 $\frac{4}{8}$ 和 $\frac{2}{8}$ 保持未简化，分母为 8，以表示余数。这些余数遵循以下模式:

$$1,\ 4,\ 1,\ 0,\ 1,\ 2,\ 1,\ \ldots$$

看起来每个其他的余数都是1。事实上，当我们把一个*odd*数的平方除以8时，余数看起来是1。有趣！你可能想知道这个模式是否会继续。处理这个想法的一个合理方法就是直接尝试通过归纳法来证明这个说法，看看它是否可行。如果它成功了，那么我们就成功地发现并证明了这一事实。如果它没有成功，那么我们可能能够弄清楚*where*它失败的原因和*why*。这是数学发现的一个很好的、普遍的建议：如果你想看看某件事是否True，就试着证明它，看看会发生什么！

Example

在继续阅读之前，请先独立完成这个问题的细节。这样做时，您需要弄清楚如何对自然数集 *odd* 进行归纳，而不是像之前那样对所有自然数进行归纳。我们实际上将展示这个命题的证明，然后讨论这种方法是如何工作的，但您绝对应该先独立完成这个任务！……

Example 5.3.4. *Remainders of odd squares when divided by 8:*

Claim: 设 O 为奇数自然数集；即，

$$O = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \cup \{0\}\,.\, n = 2m + 1\}$$

设 $P(n)$ 为命题 “n^2 是 8 的倍数加 1”。然后

$$\forall n \in O\,.\, P(n)$$

Proof. 让 $P(n)$ 定义如上所述。我们将证明 $\forall n \in O\,.\, P(n)$ by induction on n.

BC: 观察$1^2 = 1$和$1 = 0 \cdot 8 + 1$（即1是8的倍数加1）。因此，$P(1)$成立。

IH: 设 $k \in O$ 为任意且固定的。假设 $P(k)$ 成立 s.

IS: 我们的目标是推导出 $P(k+2)$ 成立。（这是因为 $k+2$ 是 k 后的下一个奇数自然数。）

由于 $k+$^2 是奇数，根据假设，我们知道 $\exists m \in \mathbb{N} \cup \{0\}$ 到 $k^2 = 8m + 1$. Let such an m be given. 时，我们知道 $\exists \ell \in \mathbb{N}$ $k^2 = 8\ell + 1$. Let such an ℓ be given.

现在，我们利用这些观察结果来了解

$$\begin{aligned}(k+2)^2 &= k^2 + 4k + 4 \\ &= (8\ell + 1) + 4(2m + 1) + 4 \\ &= 8\ell + 8m + 8 + 1 \\ &= 8(\ell + m) + 1\end{aligned}$$

自 $\ell, m \in \mathbb{Z}$ 以来，我们也知道 $\ell + m \in \mathbb{Z}$。因此，$(k+2)^2$ 比一个8的倍数多1。因此，$P(k+2)$ 成立。

通过归纳，对于每个 $n \in O$，$P(n)$ 成立。 □

Follow-up questions: 你能证明当*even*的平方除以8时的余数是*not*1吗？（这将使这个说法成为一个*if and only if*陈述。）你能识别出那些偶数平方的余数中的模式吗？你能证明你的说法吗？

(您可能不需要归纳这些主张！)

Discussion of Method

让我们讨论为什么这行得通。其基本原理与我们所见到的其他归纳形式完全相同。唯一的区别在于归纳步骤。由于奇数自然数“相差两步”，我们的目标是证明

$$\forall k \in O \bullet P(k) \implies P(k+2)$$

这封装了与标准归纳相同的想法：取命题的一个实例，并使用它来推断“下一个”实例成立。这里唯一的区别在于我们所说的“下一个”是什么。为了完整性，我们将陈述一个传达此方法的定理。同样，我们将把它留给你们来填写证明的细节。

Theorem 5.3.5 (归纳概率)**.** *Let O be the set of odd natural num- bers.*

Let $P(n)$ be a variable proposition. Suppose that

(1) $P(1)$ holds, and

(2) $\forall k \in O \bullet P(k) \implies P(k+2)$

Then $\forall n \in O \bullet P(n)$ holds.

Proof. 作为第5.3.4节中的练习2留给读者。 □

以非常相似的方式思考，我们可以看到对 *even* 自然数的归纳也将有效。这里有一个定理说明了这一点。同样，我们将证明留给你们。

Theorem 5.3.6 (归纳偶数)**.** *Let E be the set of even natural numbers.*

Let $P(n)$ be a variable proposition. Suppose that

(1) $P(2)$ holds, and

(2) $\forall k \in E \bullet P(k) \implies P(k+2)$

Then $\forall n \in E \bullet P(n)$ holds.

Proof. 作为第5.3.4节中的练习2留给读者。 □

Combining and Modifying These Methods

让我们假设我们有一个命题 $P(n)$，并且我们想要证明对于每一个 $n \in \mathbb{N}$，$P(n)$ 都成立。也许这个命题以及其背后的想法有些棘手，常规的归纳证明完全让我们束手无策。可能是因为某种代数技巧，可能我们就是看不到如何以最有效的方式去做，或者可能实际上命题背后隐藏着某种深刻的道理，阻止了我们这样做。无论是什么原因，我们可能能够使用这些新的归纳方法组合，并在几个部分中证明命题对所有 $n \in \mathbb{N}$ 都成立。

我们可以将这些新方法视为“跳跃”归纳方法。证明一个命题对每个奇数自然数成立，与之前的精确归纳技术完全相同，但我们只是通过调整归纳步骤中发生的事情“跳过”了偶数。对于对偶数进行归纳也是如此（尽管我们也稍微调整了基本情况，因为2是第一个偶数，而不是1）。如果我们首先执行“奇数”方法，然后执行“偶数”方法 *then*，总体上我们就证明了该命题对所有 *all* 自然数成立。

以下示例做的是类似的事情，但你将注意到它实际上使“跳跃”的大小为3（而不是像“奇数”和“偶数”方法那样为2）。我们不会陈述和证明（甚至要求你这样做）传达这些方法的定理。在这个时候，我们将依靠我们共同的直觉来了解归纳是如何工作的，并指出这些定理/证明将与我们一直在看到的非常相似。如果你想要练习，或者想要将它们作为笔记和记录，那就请随意陈述和证明关于我们即将使用的方法的定理！

Example 5.3.7. *Powers of* 2 *and multiples of* 7*:*

Claim: 对于每个 $n \in \mathbb{N}$，数字 $2^n + 1$ 是 *not* 7 的倍数。

（在这个阶段，我们建议做一些草稿工作，以识别当$2^n + 1$除以7时的余数中的模式。你会发现它们遵循一个长度为3的*cycle*。太酷了！这正是我们在这里要证明的；只是这个主张并没有以那种方式提出，所以我们不得不做一些额外的工作来重新表述它并找到证明。）

Proof. 定义集合 A_1, A_2, A_3 为

$$A_1 = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \cup \{0\}.\ n = 3m + 1\} = \{1, 4, 7, 10, \dots\}$$
$$A_2 = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \cup \{0\}.\ n = 3m + 2\} = \{2, 5, 8, 11, \dots\}$$
$$A_3 = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \cup \{0\}.\ n = 3m\} = \{3, 6, 9, 12, \dots\}$$

(这意味着这三个集合根据除以3的余数将$\mathbb{N}$进行划分.)

设 $P(n)$ 为命题“$2^n + 1$ 不能被 3 整除”。我们将证明 $\forall n \in \mathbb{N}$，$P(n)$ holds, by induction.

定义命题 $Q(n)$ 和 $R(n)$ 以及 $S(n)$ 如下 ws:

$$Q(n) \text{ is “ } \exists \ell \in \mathbb{N} \cup \{0\} \text{ . } 2^n + 1 = 7\ell + 3 \text{ ”}$$
$$R(n) \text{ is “ } \exists \ell \in \mathbb{N} \cup \{0\} \text{ . } 2^n + 1 = 7\ell + 5 \text{ ”}$$
$$S(n) \text{ is “ } \exists \ell \in \mathbb{N} \cup \{0\} \text{ . } 2^n + 1 = 7\ell + 2 \text{ ”}$$

观察发现

$$\forall n \in \mathbb{N} \text{ . } \big(Q(n) \vee R(n) \vee S(n) \big) \implies P(n)$$

这是因为一个7的倍数加3是*not*7的倍数，7的倍数加5或7的倍数加2也不是7的倍数。

F首先，我们将证明 $\forall n \in A_1$○ n 在 n。 $Q(n)$ holds, by inductio

BC: 观察$2^1 + 1 = 3 = 0 \cdot 7 + 3$。因此，$Q(1)$成立。

IH: 设 $k \in A_1$ 为任意且固定的。假设 $Q(k)$ 成立。

IS: 我们的目标是推导出 $Q(k+3)$ 成立。

自 $k \in A_1$ 以来，我们知道 $\exists m \in \mathbb{N}$○ $k = 3m + 1$. Let such an m be given.
到 IH 时，我们知道 $\exists \ell \in \mathbb{N}$○

我们可以推导出 $2^k + 1 = 7\ell + 3$. Let such an ℓ be given. This means $2^k = 7\ell + 2$.

$$2^{k+3} = 2^3 \cdot 2^k = 8 \cdot (7\ell + 2) = 56\ell + 16$$

Thus,Thus,

$$2^{k+3} + 1 = 56\ell + 17 = 7(8\ell) + 14 + 3 = 7(8\ell + 2) + 3$$

并且 $Q(k+3)$ 也成立，同样。因此，$\forall n \in A_1$○ $Q(n)$.

其次，我们将证明 $\forall n \in A_2$○ $R(n)$ holds, by induction on n.

BC: 观察$2^2 + 1 = 5 = 0 \cdot 7 + 5$。因此，$R(2)$成立。

IH: 设 $k \in A_2$ 为任意且固定的。假设 $R(k)$ 成立。

IS: 我们的目标是推导出 $R(k+3)$ 成立。

到 IH 时，我们知道 $\exists \ell \in \mathbb{N}$○

我们可以推导出 $2^k + 1 = 7\ell + 5$. Let such an ℓ be given. This means $2^k = 7\ell + 4$.

$$2^{k+3} = 2^3 \cdot 2^k = 8 \cdot (7\ell + 4) = 56\ell + 32$$

Thus,Thus,

$$2^{k+3} + 1 = 56\ell + 33 = 7(8\ell) + 28 + 5 = 7(8\ell + 4) + 5$$

并且 $R(k+3)$ 成立，同样。因此，$\forall n \in A_2$。 $R(n$

第三，我们将证明 $\forall n \in A_3$。 $S(n)$ holds, by induction on n.

BC: 观察 $2^3 + 1 = 9 = 1 \cdot 7 + 2$。因此，$S(3)$成立。

IH: 设 $k \in A_3$ 为任意且固定的。假设 $S(k)$ 成立。

IS: 我们的目标是推导出 $S(k+3)$ 成立。

到 IH 时，我们知道 $\exists \ell \in \mathbb{N}$。

我们可以推导出 $2^{k+3}+1$ 。

Let such an ℓ be given. This means $2^k = 7\ell + 1$.

$$2^{k+3} = 2^3 \cdot 2^k = 8 \cdot (7\ell + 1) = 56\ell + 8$$

Thus,Thus,

$$2^{k+3} + 1 = 56\ell + 9 = 7(8\ell) + 7 + 2 = 7(8\ell + 1) + 2$$

并且 $S(k+3)$ 也成立，因此，$\forall n \in A_3$。 $S(n$ ）。

总体上，我们已证明对于 *every* 个自然数（取决于一个数除以 3 的余数），要么 $Q(n)$ 要么 $R(n)$ 要么 $S(n)$ 成立。因此，每个自然数都具有 $2^n + 1$ 是 *not* 7 的倍数的性质。 □

实际上，我们在证明中证明了比所声称的 *stronger* 结果更强的结果。也就是说，我们不仅证明了形式为 $2^n + 1$ 的任何数都不是 7 的倍数，而且还精确地证明了 *how* 这些数不是 7 的倍数。

在这个部分的练习中，我们包括了一些练习，通过识别“跳跃”和断言来引导你进行这样的证明。在本章的练习中，第5.7节，我们包括了一些可能需要这种论证的问题（但我们不会像这里那样必然告诉你论证的整体结构）。

值得指出的是，在这个阶段，你可以相当容易地将这些方法适应到你面临的任何情况，只要你想做的“跳跃”遵循一些容易识别的 *pattern*。在前一个例子中，我们进行了大小为3的跳跃，因此我们将所有自然数的集合分成三个集合，并在这些集合内跳跃。本质上，这依赖于我们有一个如何到达命题“下一个”实例的“公式”：我们从 $P(k)$ 开始，并试图推导出 $P(k+3)$。你可以想象进行大小为4或10的跳跃，甚至进行跳跃 *double* 你的值；也就是说，你可以证明某些命题 $P(n)$ 对于每个 n 都成立，例如，通过证明

$$P(1) \text{ holds, and } \forall n \in \mathbb{N}.\ P(n) \implies P(2n)$$

再次，所有这些都依赖于拥有某种“公式”或“规则”，告诉我们正在考虑的 *next* 实例是什么。因此，*we cannot induct on the set of all prime numbers*。如果你试图证明某个事实成立

对于每一个素数，甚至不要尝试使用归纳法！你必须有一些“规则”说，“如果 k 是一个素数，那么 $next$ 素数是……”如果你知道这样的规则，数学界会 $love$ 听到你的消息！这将回答许多未解决的关于素数的问题，并使你成为历史上最著名的数学家。当真！Translated Text: 对于每一个素数，甚至不要尝试使用归纳法！你必须有一些“规则”说，“如果 k 是一个素数，那么 $next$ 素数是……”如果你知道这样的规则，数学界会 $love$ 听到你的消息！这将回答许多未解决的关于素数的问题，并使你成为历史上最著名的数学家。当真！

5.3.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 多米诺类比如何描述一个基例不是1的归纳证明?

(2) 为证明对每个大于或等于7的奇数都成立的命题 $P(n)$ 编写一个证明模板。 (3) 为什么我们不能“对素数进行归纳”？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 证明定理5.3.3。

(2) 证明定理5.3.5和5.3.6。

(3) 提出一个表示对5的所有倍数集合进行归纳的方法的定理。证明你的定理。

(4) 考虑不等式 $n^3 < 3^{n-1}$。

(a) 证明对于满足 $n \geq$ 的每个 n，不等式成立。6. (b) 证明对于 $n \in \{1, 2, 3, 4, 5\}$，不等式不成立。（这很容易。）(c) 证明对于满足 $n \leq 0$ 的每个 n，不等式成立。

(5) 通过以下方式定义一个数列:

$$x_1 = 2 \text{ and } x_2 = 2 \text{ and } \forall n \in \mathbb{N} - \{1, 2\}. \, x_n = x_{n-2} + 1$$

设 $P(n)$ 为命题

$$\text{“ } x_n = \frac{1}{2}(n+1) + \frac{1}{4}\big(1 + (-1)^n\big)$$

(a) 设 O 为奇自然数集。证明 $\forall n \in O$。

(b) 设 E 为偶自然数集。证明 $\forall n \in E$。

$P(n)$ by induction.

(6) 考虑以下主张。

$$\sum_{k=1}^{n}(-1)^{k-1}k^2 = (-1)^{k-1}\sum_{k=1}^{n}k$$

这是，我们声称

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}(1 + 2 + 3 + \cdots + 9)$$

适用于每个 $n \in \mathbb{N}$。

(a) 证明上述公式对 $n = 1$ 和 $n = 2$ 成立。 (b) 证明每当公式对 k 成立时，它也对 $k + 2$ 成立。 (c) 解释为什么 (a) 和 (b) 证明了该命题。

5.4 Strong Induction

现在，我们将看到为什么我们之前与归纳的工作构成了“正规”归纳。接下来是一种称为**Strong Induction**的技术。您将看到为什么这个术语适用。具体来说，它指的是归纳假设，其中我们做出一个*stronger*假设；非正式地说，我们将在证明的这一部分假设“更多内容”，这使得我们更容易得出结论（或者有时是唯一的方法）。本节的重要部分，除了通过几个例子来掌握这种修改后的技术外，还将实际*prove*这种更强的技术甚至有效。为此，我们将实际调用PMI本身！

5.4.1 Motivation

回顾第2.4节中的例子。在那里，我们关于用多米诺骨牌铺满$2 \times n$ 个矩形板的方法数做了一些观察，并玩了Takeaway游戏。在处理这些例子的归纳论证时，我们发现情况略比之前的归纳论证复杂。当我们证明类似以下内容时

$$\sum_{k=1}^{n}\frac{n(n+1)}{2}$$

对于每个 $n \in \mathbb{N}$，在归纳步骤中，我们可以引用紧接的前一个情况并调用归纳假设，如下所示:

$$\sum_{k=1}^{n+1} k = (n+1) + \sum_{k=1}^{n} k = n + 1 + \frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

当然，我们还没有把这些论据部分称为“**IH**”或“**IS**”，但我们确实是在做这样的事情。

当我们考虑多米诺镶嵌的例子时，尽管如此，我们发现我们需要引用 two 个先前的事实实例。具体来说，要找到 $2 \times n$ 董板的镶嵌数量，我们不仅需要知道有多少个 $2 \times (n-1)$ 董板的镶嵌，还需要知道有多少个 $2 \times (n-2)$ 董板的镶嵌。这本质上是不同的！归纳论证的什么特性让我们能够这样做？它是如何遵循我们描述的“多米诺类比”或“Mojo the Monkey”类比的？或者，它根本就是吗？

当我们考虑Takeaway游戏时，我们甚至有“更多”不同的情况，不是吗？在构建玩家2的获胜策略时，我们注意到玩家2应该只是模仿玩家1所做的，但在另一堆上。也就是说，如果玩家1从左边的一堆中移除，比如说，3颗石头，那么玩家2应该从右边的一堆中移除3颗石头，以确保获胜。无论玩家1移除多少颗石头，这一点都成立。从这个意义上说，我们需要玩家2在从$any\ size$到n (（包括)）的堆上有获胜策略的事实，以确保玩家2在大小为$n+1$的堆上有获胜策略。这需要我们做出很多假设才能进入归纳假设。我们怎么知道我们可以这样做呢？

5.4.2 Theorem Statement and Proof

我们的目标是陈述并证明PMI的一个修改版本，该版本反映了这些例子，即多米诺镶嵌和取走游戏。它们代表了归纳论证，我们可能需要（1）引用 $more\ than\ one$ 前一个实例来证明命题的后续实例，或（2）引用 $some\ unknown$ 前一个实例来证明后续实例。这两种论证风格都将被本定理涵盖。让我们首先看看这个陈述，然后讨论它的含义。

Theorem 5.4.1 (强数学归纳原理（强PMI)）**.**
Let $P(n)$ be a variable proposition. Suppose that

(1) $P(1)$ holds True*, and*

(2) $\forall k \in \mathbb{N}\,.\,\big(\forall i \in [k]\,.\,P(i)\big) \implies P(k+1)$ *holds* True

Then $\forall n \in \mathbb{N}\,.\,P(n)$ *holds* True*.*

哇，这是什么意思？我们在讨论之前，先以逻辑符号的形式呈现，给你一些额外的工作，但我们认为你能应付。尝试解析这两个条件，尽管当然条件

(2)是那个棘手的。它说了什么？大声读出来，用英语句子写下来，思考一下。将它与我们之前章节中陈述和证明的常规PMI进行比较。我们为什么称这个为“强”？这些定理有何不同？它们的假设不同吗？结论呢？从阅读中休息几分钟，思考这些问题。然后，继续阅读……

好的，让我们解释这个定理。注意，定理5.4.1与定理5.2.2之间的*only*差异在于条件(2)，它决定了我们在证明的归纳假设部分所做的事情。设置（我们有一个变量命题）和条件(1)（基本情况）以及结论（$P(n)$对每个$n \in \mathbb{N}$都成立）是相同的。现在让我们比较条件(2)。

常规PMI要求$P(k)$足够，以便我们能够推断出$P(k+1)$，对于每个$k \in \mathbb{N}$。如果我们能实现这一点（多米诺骨牌效应），并且我们有基础情况，那么$P(n)$对于每个$n \in \mathbb{N}$都成立。这就是我们在归纳证明的**IH**和**IS**中所做的：假设$P(k)$成立，并利用它来推断$P(k+1)$也必然成立。

让我们重写强PMI的(2)条件，看看它说：

$$\forall k \in \mathbb{N}.\ \big(P(1) \wedge P(2) \wedge P(3) \wedge \cdots \wedge P(k)\big) \implies P(k+1)$$

这是，强PMI要求命题的前一个实例的*all*（$P(1)$和$P(2)$和$P(3)$以及……一直到$P(k)$）都是*together*足够的，以便我们推导出$P(k+1)$。这个定理似乎在说，“嘿，别担心用到达$k+1$，你实际上可以用一的陈述1通过，到达那里！所期望的结论——$\forall n \in \mathbb{N}$ $P(n)$—will still follow!” Isn't that nice?

有三个方面是要讨论这个定理：(1)为什么这种方法实际上是有效的，(2)何时需要使用它，以及(3)如何使用它。我们可以在继续探索一些例子之前，快速解决第三个方面。强归纳证明与常规归纳证明之间的唯一区别将在于**IH**和**IS**。在使用强归纳法证明$\forall n \in \mathbb{N}.\ P(n)$我们将假设$P(k)$为*all*$k \in \mathbb{N}$的值成立，然后使用它来推导$P(k+1)$必然也成立。在**IS**，我们只需注意指出*which*我们使用的**IH**的假设。

为了解决方面（2）——何时使用强归纳法——我们将向您展示几个示例。在解决这些示例的过程中，我们将精确指出为什么常规归纳证明会*fail*。通过观察几个此类实例，我们希望培养对未来识别这些情况的一些直觉。也就是说，我们将学会意识到在证明中哪些类型的陈述*require*是一个强**IH**。

现在让我们解决方面（1），因为它是最紧迫的。在我们继续前进并开始使用证明技术之前，我们想确保它是实际上数学上有效的！如果你像我们一样，你可能会想，“这个定理

甚至 True? 它说我们需要更多地了解 $P(n)$ 的实例是如何相互关联的。我们为什么被允许在 **IH** 中做出这么多假设，并且能够后来使用它们？”

A Modified Domino Analogy and a Heuristic Diagram

我们将从第二章对多米诺类比的一个修改开始，然后向您展示一个 **heuristic diagram**，以说明强归纳法是如何工作的，以满足我们的直觉。之后，我们将正式证明上述定理。

思考一下常规归纳如何遵循多米诺类比。我们只需要知道多米诺 n 将会落入多米诺 $n+1$，以确保整条线都会倒下。在这里，使用强归纳，我们实际上需要知道直到（包括）多米诺 n 的所有多米诺 *all* 都已经倒下并撞击到多米诺 $n+1$，将其推倒，以确保整条线都会倒下。这就像多米诺随着线的延伸变得越来越“沉重”，因此我们需要一大堆多米诺相互撞击，以产生足够的动力来推倒下一个，更沉重的多米诺。

让我们换一种方式来说。想想连接我们所有命题的推论链。我们的 **BC** 将告诉我们 $P(1)$ 是 True。太好了。这将意味着 $P(2)$ 成立。（在SPMI的第（2）个条件中使用 $n=1$。）知道这两点将 *together* 意味着 $P(3)$ 成立。（在SPMI的第（2）个条件中使用 $n=2$。）知道这三点将共同意味着 $P(4)$ 成立。以此类推：

$$\underbrace{\underbrace{\overbrace{\big(P(1)\big)}^{\mathsf{T}\text{ by BC}}\overbrace{\Longrightarrow}^{\text{Use IS}}\overbrace{\big(P(2)\big)}^{\text{Get }\mathsf{T}}}_{\text{Know } P(1)\wedge P(2)}\underbrace{\Longrightarrow}_{\text{Use IS}}\underbrace{\big(P(3)\big)}_{\text{Get }\mathsf{T}}}_{\text{Know } P(1)\wedge P(2)\wedge P(3)} \Longrightarrow \big(P(4)\big) \Longrightarrow \big(P(5)\big) \Longrightarrow$$

在某些意义上，这表明 *why* 该方法总体上是有效的。我们证明 $P(1)$ 成立，就像在常规归纳中一样。但接下来，为了“到达”$P(2)$ 的真相，第一步——$P(1) \implies P(2)$——在强归纳中就像在常规归纳中一样是关键。(在SPMI和PMI的第（2）个条件中使用 $n=1$。这是 **same** 条件。) 从那时起，当我们使用强归纳时，我们只是在利用先前命题实例的 *all* 已经成立的事实 True；我们不妨利用它们继续前进并推导出下一个命题的真相！常规归纳不关心这一点。它说，“好吧，很好，所有之前的实例都成立了。我们实际上不需要它们来证明下一个实例；我们只需要立即前一个实例。”

这里还有一种稍微不同的方式来解释这个“推理链”。这实际上会直接暗示我们很快就会看到的证明，以及！假设我们正在使用强归纳过程进行移动，并且我们已经证明了直到 $P(n)$ 的所有内容；也就是说，$P(1)$ 和 $P(2)$ 以及……和 $P(n)$ 都是

True. 让我们将这些实例全部打包，并标记为一个大的命题，$Q(n)$。 (换个角度想，我们将所有这些多米诺骨牌绑在一起，形成一个巨大的多米诺骨牌。) 下一步是使用这个实例来证明下一个实例，这听起来更像是我们现在更熟悉的常规归纳法。这正是我们将要在证明中做的事情！我们将重新表述强归纳法的整个过程，将其表述为一个 *Regular Induction* 流程。

Formal Proof

如前一段所述，下面的证明将使用PMI。（事实上，我们甚至将使用我们在上一节中看到的归纳证明模板！）从这个意义上说，我们实际上正在证明这个陈述:

$$\textbf{PMI} \implies \textbf{SPMI}$$

让我们做吧!

Proof. 设 $P(n)$ 为一个变量命题。假设

(1) $P(1)$ 满足 True，并且

(2) $\forall k \in \mathbb{N}_{\circ} \quad \big(\forall i \in [k]_{\circ} \quad P(i)\big) \implies P(k+1)$ holds True

我们的目标是证明 $\forall n \in \mathbb{N}_{\circ} \quad P(n)$.

定义命题 $Q(n)$ 通过设置

$$Q(n) \iff \forall i \in [n]\,.\,P(i)$$

(这是，$Q(n)$说“所有命题$P(1)$和$P(2)$以及……和$P(n)$都是True.)”

我们现在将证明 $\forall n \in \mathbb{N}_{\circ} \quad Q(n)$ by induction on n.

BC: 根据命题 $Q(1)$ 的定义，我们有 $Q(1) \iff P(1)$。条件（1）告诉我们 $P(1)$ 成立，因此 $Q(1)$ 也成立。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $Q(k)$ 成立。

IS: 根据 $Q(k)$ 的定义，我们有

$$Q(k) \iff \forall i \in [k]\,.\,P(i)$$

(再次，即 $P(1)$ 以及 ... 以及 $P(k)$ 都成立.)

根据条件（2），我们可以推导出 $P(k+1)$ 成立。

这意味着 $\forall i \in [k+1]_{\circ}$ $P(i)$. (That is, we already knew $P(1)$ and ... and $P(k)$ all hold, and we just found that $P(k+1)$ holds, too.)

根据$Q(k+1)$的定义，这意味着$Q(k+1)$成立。这是**IS**的目标。

相应地，通过PMI，我们推断出 $\forall n \in \mathbb{N}_{\circ} \quad Q(n)$ hold
根据 $Q(n)$ 的定义，我们有

$$\forall n \in \mathbb{N}.\ Q(n) \implies P(n)$$

(这意味着每个实例 $Q(n)$ 都表示实例 $P(1)$ 和 ... 以及 $P(n)$ 成立，因此至少我们知道 $P(n)$ 本身成立。)

自我们刚刚证明对于每个 $n \in \mathbb{N}$，$Q(n)$ 成立，因此我们可以推断出对于每个 $n \in \mathbb{N}$，$P(n)$ 因此 *also* 成立，即

$$\forall n \in \mathbb{N}.\ P(n)$$

这是目标，因此我们的证明是完整的。 □

Proof Summary and a Striking Equivalence

看看我们取得了什么成就：我们使用了正则归纳法来证明强归纳法是一种有效技术。这告诉我们PMI定理*implies*和SPMI定理，正如我们上面提到的：

$$\textbf{PMI} \implies \textbf{SPMI}$$

但当然，这也同样成立！如果我们已经以某种方式证明了（通过其他手段）强归纳法是有效的，那么常规归纳法也必须是有效的。也就是说，我们也知道{v* }

$$\textbf{SPMI} \implies \textbf{PMI}$$

另一种说法是：如果我们已经掌握了强归纳作为一种有效的证明技术，那么每当我们要使用常规归纳来证明某事时，我们就会直接使用强归纳来实现我们的目标。从这个意义上说，强归纳“包含”了常规归纳作为一种技术。

这两个观察结果一起告诉我们关于PMI和SPMI定理在数学真理世界中的某些非凡之处。我们现在已经证明它们是等价的：

$$\textbf{PMI} \iff \textbf{SPMI}$$

每个定理都蕴含另一个定理。

现在，对于*applying*这些技术证明事实的实际目的而言，这种等价性可能看起来并不重要，但它实际上确实告诉我们一些有用的信息。它表明：

> *Whenever we have to prove something by induction, we might as well always use Strong Induction.*

考虑几分钟。阅读定理陈述及其证明，并加以思考。在我们解决接下来的例子时，请记住这一点。

一旦您阅读了下面的证明模板，请回到上一节关于正则归纳的例子，并应用*Strong*归纳于它们。它起作用了吗？看起来不同吗？试试看！在解决下面的例子之后，我们将再次讨论这种正则/强比较，所以让我们继续前进，看看如何使用强归纳。

5.4.3 Using Strong Induction: Proof Template

此模板与常规归纳的模板非常相似，因为这两个定理（以及相应地，应用它们时的各自技术）之间的唯一区别发生在**IH**。

Template for a "Proof by Strong Induction"

Goal: 证明 $\forall n \in \mathbb{N}_{\circ} \quad P(n)$

Proof.

设 $P(n)$ 为命题 "_____"。我们将证明 $\forall n \in \mathbb{N}_{\circ} \quad P(n)$ by induction on n.

Base Case: Observe that $P(1)$ holds because _____.

Induction Hypothesis: Let $k \in \mathbb{N}$ be arbitrary and fixed.
Assume $\forall i \in \mathbb{N}_{\circ} \quad i \leq k \Rightarrow P(i)$ holds.

Induction Step: 假设 $P(k)$ 推导出 $P(k+1)$ 也成立。根据PMI，可以得出 $\forall n \in \mathbb{N}_{\circ} \quad P(n)$. □

所有关于常规归纳的重要观察和建议也适用于此处。我们必须确保*define*一个命题，指出我们正在使用（强）归纳于特定变量，标记我们的步骤，并得出结论。

我们想提出的一个新建议是对旧建议的细化。在使用常规归纳时，我们必须确保每次使用时都要引用 *the* **IH**。在这里，我们将在我们的 **IH** 中有 *many* 个命题实例，因此我们实际上必须小心并引用我们使用的命题的 *which* 个实例！您将在下面的例子中看到这一点。

5.4.4 Examples

我们将看到三种不同的"类型"的例子。尽管它们都使用了我们刚刚介绍过的强归纳法的相同模板，但它们在如何引用 **IH** 中的假设方面有所不同。第一个是该方法的一个直接应用，所以让我们先来处理它，然后再讨论其他例子可能的不同之处。

Example 5.4.2. *A formula for a recursively-defined sequence:*

Claim: 让序列 s_n 定义为

$$s_0 = 1 \text{ and } \forall n \in \mathbb{N}.\ s_n = 1 + \sum_{i=0}^{n-1} s_i$$

找到并证明对于每个 $n \in \mathbb{N} \cup \{0\}$，$s_n$ 的一个封闭公式。

Proof. 设 $P(n)$ 为 “$s_n = 2^n$”。我们证明 $\forall n \in \mathbb{N} \cup \{0\}$，$P(n)$ holds, by induction.

BC: 当 $n = 0$ 时，观察 $s_0 = 1$ 和 $2^0 = 1$，所以 $s_0 = 2^0$。因此，$P(0)$ 成立。

IH: 设 $k \in \mathbb{N} \cup \{0\}$ 为任意且固定的。假设 $P(0) \wedge P(1) \wedge \cdots \wedge P(k)$ 成立。

IS: 观察发现

$$\begin{aligned}
s_{k+1} &= 1 + \sum_{i=0}^{k} s_i && \text{Definition of } s_{k+1} \\
&= 1 + \sum_{i=0}^{k} 2^i && \text{Using } \mathbf{IH}\text{s: } P(0) \wedge \cdots \wedge P(k) \\
&= 1 + \left(2^{k+1} - 1\right) && \text{Standard result (see Exercise 2.7.1)} \\
&= 2^{k+1}
\end{aligned}$$

因此，$P(k+1)$ 成立。因此，$\forall n \in \mathbb{N} \cup \{0\}$，$P(n)$ holds, by induction. □

注意，这个例子要求我们在 **IH** 中使用 *all* 的实例。这难道不令人印象深刻吗？当然，我们在这里使用了强归纳。不知道所有之前的实例都成立，我们就无法有任何希望推断出下一个实例！

此例与下一例的区别在于，我们确切地知道我们使用的 *which* 实例（即所有实例）。在下一例中，我们将调用 **IH**，但无法确切地说出我们使用的是哪个实例。你们会明白我们的意思！

Example 5.4.3. 首先，我们需要向您介绍（或者提醒您）关于素数和自然数的一些概念。

Primes: 一个 **prime number** 是集合的元素

$$P = \{n \in \mathbb{N} \mid n > 1 \wedge (n = ab) \implies (a = 1 \vee a = n)\}$$

这意味着一个质数的唯一因数是1和它本身。

Prime Factorization: 给定 $x \in \mathbb{N}$，**prime factorization** 的 x 是等于 x 的质数乘积，允许重复。

例如，6的素因数分解为$2 \cdot 3$，252的素因数分解为$2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$。

我们现在将陈述并证明以下事实：每个自然数都有一个素数分解。

Claim: 设 $F(n)$ 为命题“n 有素因子分解”，然后我们断言 $\forall n \in \mathbb{N} - \{1\}$。 $F(n)$.

Proof. 我们将证明 $\forall n \in \mathbb{N} - \{1\}$。 $F(n)$ by induction on n.

BC: 注意，$F(2)$成立，因为$2 = 2$是2的素数分解。

IH: 让 $k \in \mathbb{N} - \{1\}$ 为任意且固定的。

假设 $\forall i \in [k] - \{1\}$。 $F(i)$ holds. (That is, suppose $F(2) \wedge F(3) \wedge \cdots \wedge F(k)$.)

IS: 考虑 $k+1$. 我们想要找到 $k+1$ 的素数分解。有两种情况，基于 $k+1$ 本身是否为素数：

Case 1: 如果 $k+1$ 本身是质数，那么 $k+1$ 是 $k+1$ 的质因数分解，从而表明 $F(k+1)$ 成立。

Case 2: 如果 $k+1$ 不是素数，则存在 $a, b \in \mathbb{N} - \{1\}$ 使得 $k+1 = a \cdot b$。由于 $a, b \neq 1$，因此它必须是 $1 < a < k+1$ 和 $1 < b < k+1$。也就是说，$2 \leq a \leq k$ 和 $2 \leq b \leq k$。

因此，$F(a)$ 和 $F(b)$ 由 **IH** 保持。据此，a 和 b 存在一个质因数分解。将这两个因数分解相乘得到 $a \cdot b = k +$ 的一个质因数分解。这表明 $F(k+1)$ 成立。

在任何情况下，我们推断 $F(k+1)$ 成立。

通过归纳，我们得出结论：$\forall n \in \mathbb{N} - \{1\}$。 $F(n)$. □

注意，我们在这次证明中调用了 **IH**，但我们不知道我们调用了哪个“先前实例”的命题。我们只能依据具有某种特性的 *some* a 和 b 进行上诉。这与先前的例子不同，但它也清楚地表明我们在这里使用了强归纳法。关于 k 的素数分解的任何信息都不可能帮助我们找到 $k +$ 的一个。想想看：知道 14 = 2 × 7 帮助我们弄清楚 15 = 3 × 5 吗？知道 16 = 2 × 8 帮助我们弄清楚 17 是素数吗？

这个我们刚刚证明的结果非常重要：它表明每个自然数都有一个素数分解。现在，这些素数分解恰好是 **unique**，从某种意义上说，每个自然数都有一个 *exactly one* 素数分解。当然，这只有在“因子的顺序”上才成立。通过这一点，我们是指 $6 = 2 \cdot 3$ 和 $6 = 3 \cdot 2$ 实际上是 6 的 *same* 分解。同样，$252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$ 是 252 的唯一分解；这与写作 $252 = 7 \cdot 3^2 codt 2^2$ 没有区别。

没有关于上述证明的内容涉及到这个事实！我们只是使用了某些 *existence* 的 a 和 b 来推断某事。谁能说没有一些具有相同性质的 *other* c 和 d 我们可以使用呢？想想

关于这个。你能证明素数分解是唯一的吗？你将使用什么方法?

下一个例子将涉及 **Fibonacci Sequence**，这是我们之前使用过的一串数字。具体来说，我们将陈述并证明该序列的一个 **closed form**，这通常是通过递归定义的。当我们说“闭式”时，我们指的是一个可以通过“直接代入”来评估的简单表达式。例如，要找到 f_{100}，根据序列的递归定义，我们需要计算到那个点为止序列中数字的 *all*：我们需要 f_{99} 和 f_{98}，这意味着我们需要 f_{97}，这意味着……然而，有了闭式，我们只需“代入 n”并直接评估即可找到 f_{100}。

Example 5.4.4. *A closed form for the Fibonacci Sequence:*

Claim: 定义标准斐波那契序列如下

$$f_0 = 0 \text{ and } f_1 = 1 \text{ and } \forall n \in \mathbb{N} - \{1\}\text{.}\ f_n = f_{n-1} + f_{n-2}$$

定义 e $\varphi = \frac{1+\sqrt{5}}{2}$。然后以下等式对每个 $n \in \mathbb{N}$ 都成立 $\cup \{0\}$:

$$f_n = \frac{1}{\sqrt{5}}\left(\varphi^n - (1-\varphi)^n\right)$$

Proof. 让 f_n 和 φ 如上所述定义。

我们将首先证明以下方程:

$$1 + \varphi = \varphi^2 \qquad (\star_1)$$

观察发现

$$\varphi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4}$$
$$= \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \varphi$$

然后，我们可以用这个来证明以下方程:

$$2 - \varphi = (1-\varphi)^2 \qquad (\star_2)$$

观察发现

$$(1-\varphi)^2 = 1 - 2\varphi + \varphi^2 = 1 - 2\varphi + (\varphi + 1) = 2 - \varphi$$

我们在其中使用了事实（$\star_1$）。

我们将利用以下这两个事实。

设 $P(n)$ 为命题

$$\text{“ } f_n = \frac{1}{\sqrt{5}}\left(\varphi^n - (1-\varphi)^n\right) \text{ ”}$$

我们将证明 $\forall n \in \mathbb{N} \cup \{0\}$。 $P(n)$ by induction on n.

BC: 观察 $f_0 = 0$ 和

$$\frac{1}{\sqrt{5}}\big(\varphi^0 - (1-\varphi)^0\big) = \frac{1}{\sqrt{5}}(1-1) = 0$$

因此，$P(0)$成立。

IH: 让 $k \in \mathbb{N} \cup \{0\}$ 为任意且固定的。假设 $\forall i \in [\,]_{k \cup \{0\}}$, $P(i)$ holds.

Case 1: 假设 $k = 0$。然后我们可以直接观察到 $f_1 = 1$ 和

IS: Our goal now is to deduce that $P(k+1)$ holds.

$$\frac{1}{\sqrt{5}}\big(\varphi^1 - (1-\varphi)^1\big) = \frac{1}{\sqrt{5}}\big(2\varphi - 1\big) = \frac{1}{\sqrt{5}}\big(1+\sqrt{5}-1\big) = \frac{1}{\sqrt{5}}\big(\sqrt{5}\big) = 1$$

这表明 $P(1)$ 成立。

Case 2: 假设 $k \geq 1$。然后，观察可知

$$\begin{aligned}
f_{k+1} &= f_k + f_{k-1} && \text{Defn, since } k \geq 1 \\
&= \frac{1}{\sqrt{5}}\big(\varphi^k - (1-\varphi)^k\big) + \frac{1}{\sqrt{5}}\big(\varphi^{k-1} - (1-\varphi)^{k-1}\big) && \textbf{IH}\text{s } P(k), P(k-1) \\
&= \frac{1}{\sqrt{5}}\big(\varphi^k + \varphi^{k-1} - (1-\varphi)^k - (1-\varphi)^{k-1}\big) && \text{Simplify} \\
&= \frac{1}{\sqrt{5}}\big(\varphi^{k-1}(\varphi+1) - (1-\varphi)^{k-1}((1-\varphi)+1)\big) && \text{Factor} \\
&= \frac{1}{\sqrt{5}}\big(\varphi^{k-1}\cdot\varphi^2 - (1-\varphi)^{k-1}(2-\varphi)\big) && \text{By } (\star_1) \\
&= \frac{1}{\sqrt{5}}\big(\varphi^{k+1} - (1-\varphi)^{k-1}(1-\varphi)^2\big) && \text{By } (\star_2) \\
&= \frac{1}{\sqrt{5}}\big(\varphi^{k+1} - (1-\varphi)^{k+1}\big)
\end{aligned}$$

因此，$P(k+1)$ 成立。

通过归纳，我们得出结论：$\forall n \in \mathbb{N} \cup \{0\}$。 $P(n)$. □

A Discussion about Multiple Base Cases

注意，在前一个例子中，我们不得不在 **IS** 中建立两个情况。因为斐波那契数列是递归定义的，所以每个项都依赖于前两个项，我们无法仅凭 $P(0)$ 的真值来推断 $P(1)$。我们必须证明 $P(1)$ 满足 *separately*。(回去试试。你会发现自己在尝试引用 f_{-1}，一个未定义的术语！）之后，我们可以使用 $P(0)$ 和 $P(1)$ 的真值来推断 $P(2)$，然后我们可以使用 $P(1)$ 和 $P(2)$ 来推断 $P(3)$。. . 也就是说，我们确实需要在整个归纳的“等等”开始之前抛入一个 *extra base case*。

有两种合法的方式来处理这个问题，我们刚刚向您展示了一种。另一种方式是提前认识到这种情况会发生，并在 **BC** 步骤中提出两个基本案例。为了说明，让我们看看如果那样做，证明的相关部分会有何不同：

Proof.

. . .

...

BC: 观察 $f_0 = 0$ 和

$$\frac{1}{\sqrt{5}}\big(\varphi^0 - (1-\varphi)^0\big) = \frac{1}{\sqrt{5}}(1-1) = 0$$

因此，$P(0)$成立。

也请注意，$f_1 = 1$ 和

$$\frac{1}{\sqrt{5}}\big(\varphi^1 - (1-\varphi)^1\big) = \frac{1}{\sqrt{5}}\big(2\varphi - 1\big) = \frac{1}{\sqrt{5}}\big(1 + \sqrt{5} - 1\big) = \frac{1}{\sqrt{5}}\big(\sqrt{5}\big) = 1$$

因此，$P(1)$成立。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $\forall i \in [k] \cup \{0\}$。 $P(i)$ holds.

IS: 我们的目标是推导出 $P(k+1)$ 成立。观察发现

...

... □

我们移动了特殊 $P(1)$ 案例到 *into* 部分。因此，我们不得不修改 *quantification* 在 **IH** 和 **IS** 中发生的内容。我们不再想在接下来的论证中使用 $k = 0$，所以在 **IH** 中我们只取一个满足 $k \geq 1$ 的任意 k。然而，我们已看到 $P(0)$ 成立，所以我们仍然可以将其包括在我们的 **IH** 中。

这就可以了！两个证明在本质上完全相同。唯一的区别在于它们的表述，即使如此，这些区别也很小。我们将由你来决定（如果有的话）你更喜欢哪种风格在你的证明中使用。不过，我们想提醒你，这些区别虽小，但它们也是*subtle*，有时也容易忘记！如果你发现自己包含了许多基本情况，确保从寻求证明一个高于这些基本情况值的值开始你的**IS**！你不想无意中声称一些实际上并不成立的逻辑蕴涵。（例如，回顾上面的第二个证明。如果我们允许$k = 0$作为**IS**中的一个情况，我们就会无意中提到f_{-1}，这是不存在的。因此，我们会说些不正确的话，证明就会存在缺陷，尽管不是完全注定失败。）

这种区别通常发生在你需要证明一个递归定义的序列的某些表示公式时，其中序列的每一项都由几个前面的项定义。在练习中，本节和章节末尾都有这种现象的几个例子。在解决这些问题时请记住这一点！

Needing $n = 2$

一个在强归纳证明中相当常见的现象是在跳入 **IS** 之前必须证明 *both* 的 $n = 1$ 和 $n = 2$ 情况的必要性。特别是，这可能发生在你必须证明某些不等式或等式对于 n 变量成立时，其中 $n = 1$ 情况是平凡的，而 $n = 2$ 情况是更有趣的，需要更多的工作，而归纳的其余部分则通过调用 $n = 2$ 情况来完成。请注意，这当然需要将 $k \geq 2$ 取在 **IS** 中。

让我们通过一个例子来展示我们的意思。幸运的是，我们已经为这个论点证明了 $n = 2$ 的情况；这实际上是德摩根定律之一！

Example 5.4.5. *A Generalized DeMorgan's Law for Sets:*

Claim: 设 U 为一个全集。对于每一个 $i \in \mathbb{N}$，设 $A_i \subseteq U$ b e 的一个集合。然后，以下等式对每个 $n \in \mathbb{N}$ 都成立：

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$$

另一种说法是，这个说法表明，对于每个 $n \in \mathbb{N}$，我们有

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$$

Proof. 让 U 和 $A_1, A_2, \ldots$ 定义如所主张。

让 $P(n)$ 成为命题

$$\text{“} \overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i} \text{”}$$

我们将证明 $\forall n \in \mathbb{N}$。 $P(n)$ by induction on n.

BC: 当然，$A_1 = A_1$，因此 $P(1)$ 成立。

此外，根据集合的德摩根定律（定理4.6.9），因此 $A_1 \cup A_2 = \overline{A_1} \cap \overline{A_2}$ 成立，所以 $P(2)$ 成立。

IH: 设 $k \in \mathbb{N} - \{1\}$ 为任意且固定的。假设 $\forall i \in [k]$。 $P(i)$ holds.

IS: 我们的目标是推导出 $P(k+1)$ 成立。首先，观察一下

$$\bigcup_{i=1}^{k+1} A_i = A_{k+1} \cup \bigcup_{i=1}^{k} A_i$$

那么让我们定义

$$B_k = \bigcup_{i=1}^{k} A_i$$

然后，观察可知

$$\begin{aligned}
\overline{\bigcup_{i=1}^{k+1} A_i} &= \overline{A_{k+1} \cup B_k} && \text{Defn of } B_k \\
&= \overline{A_{k+1}} \cap \overline{B_k} && \text{By } \mathbf{BC}, P(2) \text{ (a.k.a. DeMorgan)} \\
&= \overline{A_{k+1}} \cap \overline{\bigcup_{i=1}^{k} A_i} && \text{Defn of } B_k \\
&= \overline{A_{k=1}} \cap \bigcap_{i=1}^{k} \overline{A_i} && \text{By } \mathbf{IH}, P(k) \\
&= \bigcap_{i=1}^{k+1} \overline{A_i} && \text{Simplify}
\end{aligned}$$

因此，$P(k+1)$ 也成立。

通过归纳，$\forall n \in \mathbb{N}_{\bigcirc} \quad P(n)$. □

5.4.5 Comparing "Regular" and Strong Induction

我们想重申我们在介绍强归纳作为一种技术时所说的话。这里再次强调，因为它是一个重要的教训：

> *Whenever we have to prove something by induction, we might as well always use Strong Induction.*

这个原因在于，常规归纳和强归纳是双向关联的；每一个都意味着另一个。在处理归纳证明时，本质上"并不妨碍"提出一个强归纳假设，因为我们知道我们可以。当你处理一个证明时，你可能不会预料到从你需要调用的 **IH** 中 *which* 或 *how many* 的假设。做出一个较弱的假设然后发现自己引用了从未正式证明过的"真理"是件遗憾的事！相反，你不妨提出尽可能强的假设，以防万一你需要它。这可能会过度（在真正只需要 $P(k)$ 来推断 $P(k+1)$ 的意义上），但谁在乎呢，对吧？关键是 *prove* 事实，只要这一点做到了，你就成功了。

随着你在数学领域的进步，你可能会更好地识别出常规/强归纳论证之间的区别。特别是，你可能会注意到当强归纳真正是 *required* 的时候。通常，这发生在我们有一个递归定义的序列时，但这种情况也出现在许多其他地方。当你尝试解决一个问题时，试图找到

提出一个论点，看看你的命题实例之间有哪些类型的 *dependencies*。如果你注意到一个实例依赖于几个之前的实例，你几乎肯定需要一个强归纳论证。

5.4.6 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 强归纳和常规归纳有什么区别？(2) 你如何识别一个强归纳论证是 *required*？(3) 为什么我们不妨总是使用强归纳，而不是决定是否使用常规/强归纳？(4) 我们在质因数分解示例中使用 **IH** 的有趣之处是什么？它与我们在其他示例中证明关于递归定义的数列公式的例子相比如何？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 通过以下方式定义一个数列：

$$x_1 = 2 \text{ and } x_2 = 3 \text{ and } \forall n \in \mathbb{N} - \{1, 2\}\,.\; x_n = 3x_{n-1} - 2x_{n-2}$$

证明以下公式：{v*}

$$\forall n \in \mathbb{N}\,.\; x_n = 2^{n-1} + 1$$

(2) 让序列 a_n 定义为 $a_0 = 0$ 和 $a_1 = 1$ 以及

$$\forall n \in \mathbb{N} - \{1\}\,.\; a_n = 5a_{n-1} - 6a_{n-2}$$

这是，$\langle a_n \rangle = \langle 0, 1, 5, 19, 65, 211, \ldots \rangle$

证明对于每个 $n \in \mathbb{N} \cup \{0\}$，有 $a_n = 3^n - 2^n$。

(3{v段 $a_1 \in \mathbb{Z}$ 为任意且固定的。定义一个序列如下: 设置

$$\forall n \in \mathbb{N} - \{1\}\text{.}\ a_n = \sum_{k=1}^{n-1} k^2 a_k$$

证明以下公式：{v*}

$$a_1 \text{ is even} \implies \forall n \in \mathbb{N}\text{.}\ a_n \text{ is even}$$

(4) 定义一个序列 $\langle t_n \rangle$，通过设置

$$t_1 = t_2 = 2 \text{ and } \forall n \in \mathbb{N} - \{1, 2\}\text{.}\ t_n = \frac{1}{2t_{n-2}}(t_{n-1} - 4)(t_{n-1} - 6)$$

证明 $\forall n \in \mathbb{N}_{\circ}\quad t_n = 2.$

(5) 你可能之前见过 **Triangle Inequality**；它表示

$$\forall x, y \in \mathbb{R}\text{.}\ |x + y| \leq |x| + |y|$$

(在 $|x|$ 是 *absolute value* 的 x)。证明这个不等式对于 n 个变量成立，而不仅仅是 2；也就是说，证明如果我们有一个实数序列 x_i，其中 $\forall i \in \mathbb{N}_{\circ}\quad x_i \in \mathbb{R}$, then

$$\forall n \in \mathbb{N}\text{.}\ \left|\sum_{k=1}^{n} x_i\right| \leq \sum_{k=1}^{n} |x_i|$$

(*Note:* 证明 $n = 2$ 情况，也要！我们不想你只是假设它！)

(6) 回顾第2.4.1节，其中我们考虑了用多米诺骨牌铺满$2 \times n$ 个矩形棋盘。在这里，研究用直线三连棋（即$3 \times n$ 1个矩形块）铺满$3 \times$ 个矩形棋盘的类似问题。确定一个归纳关系，并定义一个序列，以识别铺满$3 \times n$ 个棋盘的方法数。

(不要尝试找到封闭形式并/或证明它！这样做所需的技巧超出了我们当前讨论的范围。如果你好奇，搜索**recurrence relations**。如果你想，尝试将你读到的内容应用到这个问题上，以得出一个封闭形式。你能通过归纳法证明它吗？)

5.5 Variants of Strong Induction

与我们在常规归纳中看到的一些变体——使用不同的基本情况、在不同的集合上、反向等——类似，我们在这里有一个强归纳的变体要讨论。正如您将看到的，“最小犯罪”论证是

本质上使用 *con- trapositive* 条件语句进行的强归纳证明，这类论证在归纳证明中不时出现，理解它们的工作方式将非常有帮助！

此外，我们将陈述并证明自然数集的一个性质。这被称为 **Well-Ordering Principle**。为什么它包含在本节中？嗯，你会看到这个原理与归纳和强归纳都密切相关！

5.5.1 "Minimal Criminal" Arguments

Using a Contrapositive

记住，一个条件语句在逻辑上与其逆否命题等价。此外，记住关于归纳法如何工作的定理陈述都包含条件语句。它们始终处于条件（2）中，并代表**IH**和**IS**的作用。如果我们考虑这样一个条件语句的逆否命题会发生什么？这根本不会改变定理的真实性，但它肯定会影响我们作为证明技术应用归纳法的方式。会发生什么？让我们找出答案吧！

这里是从强PMI中得到的条件语句：

$$\forall k \in \mathbb{N}.\ \big(\forall i \in [k].\ P(i)\big) \implies P(k+1)$$

否定 g 两边并切换箭头，我们找到其逆命题 正的：

$$\forall k \in \mathbb{N}.\ \neg P(k+1) \implies \big(\exists i \in [k].\ \neg P(i)\big)$$

当应用强归纳时，我们试图证明 $P(1)$ 以及 ... 和 $P(k)$ 一起使我们能够推导出 $P(k+1)$。这个陈述的新版本反映了一种不同的方法：假设 $P(k+1)$ 实际上 *fails*，让我们推导出一个也失败的先前实例 *there is*。

How It Works

从技术上讲，这里没有新的东西可说！这种方法之所以有效，是因为条件语句及其逆否命题在逻辑上是等价的。然而，这有点令人不满意。这样"倒退"地争论感觉有点奇怪，假装我们的命题在某处失败，并展示它也失败在某处 *earlier*。难道这不是我们试图做的相反的事情吗？这种方法的核心有两点：(1) 我们已经建立了一个基本情况，(2) 这个"早期失败"的论点是针对一个 *arbitrary* k 的。

这里是我们思考的方式。假设我们有一个命题 $P(n)$，我们想证明 $\forall n \in \mathbb{N}$。

$P(n)$. First, we establish that $P(1)$ holds. Good. Next, we pretend that $P(k+1)$ fails, for some *arbitrary* $k \in \mathbb{N}$. (Notice that $k+1 \geq 2$, so we aren't pretending that $P(1)$ fails, since we already know it holds.) We work through some argument and deduce that an *earlier* instance fails. Let's say $P(\ell)$ fails, for some ℓ that satisfies $1 \leq \ell \leq k$.

现在，我们刚才提出的论点是为了一个 *arbitrary* k，因此相同的论点也适用于我们产生的新值 ℓ。这保证了对于某些满足 $1 \leq m \leq \ell - 1$ 的 m，$P(m)$ 会失败。然后，相同的论点可以被重新包装并应用于 m 的值，然后……你可能已经看到了这个趋势。最终，我们“用尽”了命题可能失败的前置实例；我们 *have* 最终回到 $P(1)$。但我们已经知道 $P(1)$ 成立！

主要思想可以概括如下：如果我们有一个有效的基本情况，并且存在 **no smallest instance that fails**，那么该命题在所有地方都成立。这就是“最小罪犯”这个短语来源的地方。（当然，它被选中是因为其描述性和俏皮的押韵。）“罪犯”指的是命题*fails*的一个实例，以及证明该蕴涵

$$\forall k \in \mathbb{N}.\ \neg P(k+1) \implies \big(\exists i \in [k].\ \neg P(i)\big)$$

相当于表明不可能存在这样的“最小”实例。

另一个包含相同想法的短语是“没有最小反例”。你可能会在其他书中找到这个短语，所以请注意它指的是相同的概念。它传达了这样一个观点：没有反例可以反驳这个主张，使得所有之前的实例都是真实的。此外，这个方法的另一个术语是“无限下降”。这个术语并不立即清楚它指的是相同的概念，因为它暗示了我们给出的关于这种方法如何工作的实际*description*。通过证明我们总能找到一个更小的反例，我们表明存在一个我们的命题失败的“反向”实例序列。然而，这个序列不能是“无限下降”，因为我们最终会遇到$P(1)$，这是我们证明是有效的。请注意，这两个术语也被使用。我们选择“最小罪犯”是因为这样说更有趣。

Proof Template

让我们简要地展示如何编写这种证明的模板，然后我们将直接进入一个有趣事实的例子证明。这里并没有什么特别新的东西。我们正在将直接证明策略应用于一个 $\implies$ 命题；只是这个命题是我们之前已经看到过的命题的逆命题。

Template for a “Proof by a Minimal Criminal Argument”

Goal: 证明 $\forall n \in \mathbb{N}_{\bigcirc}$ $P(n)$

Proof.

设 $P(n)$ 为命题 “ ”。我们将证明 $\forall n \in \mathbb{N}_{\bigcirc}$ $P(n)$ by induction on n (a “minimal criminal”

参数，实际上）。

Base Case: 观察发现 $P(1)$ 成立，因为 。 _____

Induction Hypothesis: 让 $k \in \mathbb{N}$ 为任意且固定的。

假设 $P(k+1)$ 是 False。

Induction Step: 推导出满足$1 \leq \ell \leq k$ 且 $P(\ell)$ 是 False 的 $\exists \ell \in \mathbb{N}$。

因此， $\forall n \in \mathbb{N}$。 $P(n)$. □

如果您担心忘记此模板的技术细节，只需将主要想法保持在您的脑海中：

> 一个“最小犯罪”论点通过应用归纳证明的通常步骤 **contrapositive** 和 **IH、IS** 的 {v*} 来工作。

Example

以下结果是本身很有趣。（事实上，我们将在第7.6.3节中稍后使用它，当我们讨论“大”无限集时。很棒，对吧？）我们鼓励你在跳入证明之前先玩一下这个说法。试着看看为什么它是正确的以及它是如何工作的。检查n的小值。然后，当你阅读证明时，看看你的草稿，看看它如何模仿你可能观察到的模式。

Example 5.5.1. *Expressing naturals uniquely as a product:*

Claim: 每个 $n \in \mathbb{N}$ 都可以表示为 2 的幂次乘以一个奇数。也就是说，

$$\forall n \in \mathbb{N}\text{.}\ \exists m, \ell \in \mathbb{N} \cup \{0\}\text{.}\ n = 2^m \cdot (2\ell + 1)$$

并且存在的 ℓ, m 是满足这个等式的 *only* 值。

Proof. 我们通过在 n 上的归纳法证明这个论断；具体来说，我们使用了一个“最小罪犯”论证。

BC: 观察发现 $n = 1$ 有如下表示：$1 = 2^0 \cdot (2 \cdot 0 + 1)$。此外，这是 *only* 这样的表示，因为任何其他2的幂次都会使乘积至少为2，任何其他奇数都会使乘积至少为3。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $P(k+1)$ 失败，即 $k+1$ 没有这样的表示，或者它有多个这样的表示。根据 $k+1$ 的奇偶性，我们将有两种情况。

Case 1: 假设 $k+1$ 是偶数。这意味着 $\frac{k+1}{2} \in \mathbb{N}$。

首先，假设 $k+1$ 有 *no* 这样的表示。那么，$\frac{k+1}{2}$ 也没有；因为如果

实际上 *did*，然后我们可以简单地将其翻倍（即增加2的幂1）以找到 $k+1$ 的表示。

因此，$P\left(\frac{k+1}{2}\right)$在这种情况下（对于不存在性）失败。

接下来，假设 $k+1$ 至少有 *two* 种这样的表示：

$$k+1 = 2^{m_1}(2\ell_1+1) \text{ and } k+1 = 2^{m_2}(2\ell_2+1)$$

我们假设它们是不同的，即 $(m_1, \ell_1) \neq (m_2, \ell_2)$。由于$k+1$是偶数，我们知道 $m_1, m_2 \geq 1$。通过每次将2的幂次减少1，我们看到

$$\frac{k+1}{2} = 2^{m_1-1}(2\ell_1+1) \text{ and } \frac{k+1}{2} = 2^{m_2-1}(2\ell_2+1)$$

这是 $\frac{k+1}{2}$ 的两种表示。（同时注意，$m_1 - 1, m_2 - 1 \geq 0$。）这是因为 $(m_1 - 1, \ell_1) \neq (m_2 - 1, \ell_2)$，基于我们上面的假设。

因此，$P\left(\frac{k+1}{2}\right)$在这种情况下失败（对于非唯一性）。

在任何情况下，我们都发现 $P\left(\frac{k+1}{2}\right)$ 失败。

Case 2: 假设 $k+1$ 是奇数。这意味着 $\exists \ell \in \mathbb{N} \cup \{0\}$。 $k+1 = 2\ell+1$. Then certainly we can represent $k+1$ as $k+1 = 2^0 \cdot (2\ell+1)$

当然没有 *other* 的方法来做这件事。使用2的不同幂次会使乘积为偶数（但 $k+1$ 是奇数），而使用不同的奇数因子会使乘积不同。因此，这种情况是矛盾的。※

通过归纳，因此，$\forall n \in \mathbb{N}$。 $P(n)$ holds. □

有趣，不是吗？实际上，这个证明的逻辑上比我们一开始所引导的要复杂一些。具体来说，基于奇偶性的情况使得这个问题变得有些棘手。其中一个情况（偶数情况）遵循“最小罪犯”论证。另一个情况（奇数情况）实际上是可以被证明的。在这个证明中，我们假设 $P(k+1)$ *failed*，但后来意识到当 $k+1$ 为奇数时实际上不可能。这就是矛盾所在。回顾起来似乎有些绕弯子，但它允许我们将整个证明作为一个“最小罪犯”论证来呈现，而不是分别对奇数和偶数进行两个独立的证明。

此外，我们不仅要处理这些表示的存在性，还要处理 *uniqueness*。这就是为什么在证明 $k+1$ 为偶数时有两个考虑因素。为了证明这些表示的存在性，我们必须证明 $k+1$ 不可能有 *zero* 个表示；为了证明唯一性，我们必须证明 $k+1$ 不可能有 *two* 个表示。

5.5.2 The Well-Ordering Principle of $\mathbb{N}$

Motivation

我们都很熟悉自然数 $\mathbb{N}$ 上的关系 “$\leq$”。对于任意两个元素 $x, y \in \mathbb{N}$，必须满足以下两个关系之一：要么 $x \leq y$，要么 $y \leq x$ (，或者两者都满足，但仅在 $x = y$) 的情况下。我们还知道，

$$\forall x, y, z \in \mathbb{N} \bullet \big(x \leq y \wedge y \leq z\big) \implies x \leq z$$

并且 $\forall x \in \mathbb{N}$。

此外，这种关系被证明是一个 **well-ordering**。我们不会正式定义这个术语，但成为一个良好排序的关键方面之一是没有任何 *infinitely-descending chains* 想想看这在 $\mathbb{N}$ 中是如何工作的：是否存在一个 *infinite* 元素序列 $a_1, a_2, a_3, \ldots$ 使得 $a_1 > a_2 > a_3 > \cdots$？这是可能的吗？（注意这些不等式是 *strict*）。不，不是！这个想法是，从某个数字 $a_1 \in \mathbb{N}$ 开始，如果我们“下降”，我们最终必须达到 1。我们不能“低于”那个数字。

$x < y$. This makes $\mathbb{N}$ an **ordered** set; we call $<$ an *order relation* on $\mathbb{N}$. (See Section 6.3 for more information)

而不是一般性地讨论良序性——你可以在集合论或形式逻辑的课程中这样做——我们只讨论这个概念在 $\mathbb{N}$ 的上下文中的工作方式。这是一个有用的属性，我们将来也会有机会引用它！在本节中，我们将阐述这个原则，寻求你的帮助来证明它，然后展示它与归纳的关系。

Statement and Proof

Theorem 5.5.2. *Every non-empty subset of* $\mathbb{N}$ *has a* 最小元素. *Stated in logical form,*

$$\forall S \in \mathcal{P}(\mathbb{N}) \bullet [S \neq \varnothing \implies (\exists \ell \in S \bullet (\forall x \in S \bullet \ell \leq x))]$$

考虑这与我们之前的陈述之间的关系，即我们不可能有一个无限下降的自然数链。*If*如果我们确实有这样的链，我们可以定义S为链中所有这些元素的集合。这个集合将会有一个最小元素。给定该集合的一个元素，我们知道它是链中的一个元素；让我们假设它是a_n。那么，a_{n+1}也在集合中，$a_{n+1} < a_n$也在集合中。因此，将没有最小元素。

我们将要求你证明这个定理，因为我们认为通过详细地研究这个过程会有所启发。它被分成了几个步骤概述给你。一个关键的观察是证明是 **by induction**！也就是说，通过这种方式证明良序原理，我们将已经证明了数学归纳原理 *implies* 良序原理。

Proof. 通过归纳。留给读者作为练习5.7.21。 □

任何子集 $S \subseteq \mathbb{N}$ 的最小元素也必须是 *unique*。也就是说，我们不能有两个（或更多）最小元素。假设我们实际上确实有一个集合 S 的两个最小元素；称它们为 ℓ 和 m。

通过最小元素的定义，我们会知道 $\ell \leq m$ 和 $m \leq \ell$。当然，这告诉我们 $\ell = m$ ，所以它们是相同的!

Induction, Strong Induction, and The WOP

如我们之前提到的，因为我们使用了归纳法来证明良序原理，这表明数学归纳法原理 *implies* 与良序原理。下一个定理表明，实际上，这两个定理是 **logically equivalent**：它们蕴含 *each other*。此外，它还说明归纳法原理 *Strong* 也蕴含良序原理，反之亦然。事实上，它说明这三个定理在逻辑上是等价的!

本质上，这是说这三个定理

Theorem 5.5.3. *The following are all logically equivalent:*

- *The Principle of Mathematical Induction*
- *The Principle of Strong Induction*
- *The Well-Ordering Principle*

Proof. 让我们为每个定理使用以下缩写：

- **PMI**数学归纳法原理
- **PSI**强归纳原理
- **WOP**: 好序原理

顺便说一下，我们证明了PSI和WOP，因此我们可以推断出

$$\text{PMI} \implies \text{PSI} \quad \text{and} \quad \text{PMI} \implies \text{WOP}$$

我们还在第5.4.2节中描述了如何

$$\text{PSI} \implies \text{PMI}$$

现在我们知道

$$\text{PMI} \iff \text{PSI} \quad \text{and} \quad \text{PMI} \implies \text{WOP}$$

为了完成证明，我们将展示 WOP $\implies$ PMI。这将会表明 WOP$\iff$PMI，上述等价性将允许我们推断出这三个在逻辑上是等价的。

为了证明这一点，我们假设WOP是有效的。我们将用它来证明PMI。（回顾一下PMI的陈述，在定理5.2.2中，以提醒自己我们即将要做的事情是如何实现我们的目标的。）

假设我们有一个命题 $P(n)$，定义为对每个 $n \in \mathbb{N}_0$ 让我们假设 $P(1)$ 是 True，并且

$\forall k \in \mathbb{N}_0 \quad P(k) \implies P(k+1)$. We need to show that $\forall n \in \mathbb{N}_0 \quad P(n)$ holds.

定义 {v*} 将 F 设置为 $P(n)$ 的“False 实例”集合。即 , 定义

$$F = \{n \in \mathbb{N} \mid P(n) \text{is False}\}$$

为了证明 $\forall n \in \mathbb{N}_{\mathsf{O}}$. $P(n)$, we will AFSOC that $F \neq \varnothing$.
注意 $F \subseteq \mathbb{N}$，因为我们使用了集合构造表示法。根据上面一行中的假设，$\exists f \in F$。设这样的 f 已给出。

由于这两个条件，WOP适用于集合F，告诉我们F有一个最小元素。设ℓ为该最小元素。我们知道$\ell \in F$和，

$$\forall x \in F \,.\, \ell \leq x$$

考虑以下情况 $\ell = 1$。这是不可能的，因为我们的上述假设表明 $P(1)$ 成立，所以 $1 \notin F$。

现在，考虑 $\ell \geq 2$ 的情况。我们上面的假设说

$$\forall k \in \mathbb{N} \,.\, P(k) \implies P(k+1)$$

这与逻辑上等价

$$\forall k \in \mathbb{N} - \{1\} \,.\, \neg P(k) \implies \neg P(k-1)$$

通过取逆否命题。

应用此于元素 $\ell \in \mathbb{N} - \{1\}$，我们得出 $\neg P(\ell - 1)$ 也成立。也就是说，$P(\ell - 1)$ 是 False。

这意味着 $\ell - 1 \in F$。然而，这与 ℓ 是 F 的 **least** 元素的事实相矛盾，因为 $\ell - 1 < \ell$。※

因此，必须满足 $F = \varnothing$，这意味着 $\forall n \in \mathbb{N}_{\mathsf{O}}$. $P(n)$.
这表明定理PMI是有效的。 □

查看这个证明的主要部分。为了证明 $P(n)$ 对 *all* n 成立，我们假设它在某个 *particular* n，即元素 $f \in F$ 上失败。从那里，你可能想这么说，“嗯，$P(f)$ 失败意味着 $P(f-1)$ 失败，这又意味着 $P(f-2)$ 也失败，……**and so on**，一直到最后 $P(1)$，但我们知道 $P(1)$ 是 True。” 但关于“等等”的论点是 PMI 和 WOP 的全部内容！你不能用一个“只是继续”的手势来证明你被允许做出这样的论断！这就是我们为什么调用 WOP 来产生 *least* 元素的原因。我们可能觉得我们引入 $f \in F$ 而从未再次使用它是奇怪的。我们需要它存在来保证 $F \neq \varnothing$，这允许我们 *apply* WOP。

5.5.3 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于你刚刚阅读的部分，所以如果你无法回忆起特定的定义、概念或例子，请返回并重新阅读那部分。确保你

可以自信地回答这些问题后再继续，将有助于你的理解和记忆！

(1) “最小犯罪”论点和强归纳证明之间的区别是什么？(2) 我们证明了每个 $n \in \mathbb{N}$都可以写成2的幂和一个奇数的乘积。关于这种表示，*else*有什么是正确的?

(3) 我们证明了 $\mathbb{N}$ 是良序的。你认为 $\mathbb{Z}$ 也具有这个性质吗？$\mathbb{Q}$ 呢？$\mathbb{R}$ 呢?

(4) PMI、PSI和WOP都等于*logically equivalent*意味着什么?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 证明良序原理。这是练习5.7.21。认真做！

(2) 证明 $\sqrt{3}$ 是无理数。

((**Hint:** AFSOC что $\sqrt{3} = \frac{a}{b}$, где $a, b \in \mathbb{N}$ и дробь находится в *reduced form*. Используйте аргумент спуска, чтобы опровергнуть это *reduced form* предположение.)

(3) 使用良序原理证明，除了1之外，每个自然数都可以写成2和3的非负倍数的和。

例如，$2 = 2$ 和 $8 = 6 + 2$ 以及 $101 = 3 \cdot 33 + 2$。

(4) 考虑以下方程：$4x^4 + 2y^4 = z^4$。在这个问题中，你将通过一个诉诸于良序原理的论点来证明这个方程有 **no** 个解，$(x, y, z) \in \mathbb{N}^3$。

(a) AFSOC $(x, y, z) \in \mathbb{N}^3$ *is* 一个解，并进一步假设这个解在所有解中具有 *smallest* 的 x 值。

这是，我们正在定义

$$T = \{x \in \mathbb{N} \mid \exists y, z \in \mathbb{N}\text{.}\ 4x^4 + 2y^4 = z^4\}$$

并且 *pre-supposing* 这个集合非空（即方程有解），因此 T 有一个最小元素。

(b) 推导出 z 是偶数。

Hint: 在此及下两部分中，您可以使用以下事实：某些自然数 m 的倍数的和/差是 *also* m 的倍数。）

(c) 推导出 y 是偶数。 (d) 推导出 x 是偶数。 (e) 利用这一点推导出存在另一个解 (a, b, c)，其第一个变量的 *smaller* 值为 $a < x$。 (f) 解释为什么这证明了没有解。

5.6 Summary

现在，我们终于将 **induction** 放在了坚实、数学的基础上！我们为此已经努力了一段时间，所以当我们最终到达这里时，我们想要完整地展示这一点。我们正式陈述了 *and* 并证明了数学归纳法原理，并看到了它在实际应用中的几个例子。然后，我们使用PMI证明了更一般的 **Strong** 归纳法原理。在这个过程中，我们指出，任何归纳证明 *might as well* 都可以是一个强归纳证明，因为一种技术“包含”了另一种。此外，我们后来在关于 $\mathbb{N}$ 良序原理的章节中证明了——我们引入的两个归纳原理是 *logically equivalent* 相互关联的（以及与良序原理也是）。

我们看到了几个归纳的变体以及每个变体的一个或两个例子。我们将要使用的一个更有帮助的技术是“最小犯罪”论证。这相当于一个归纳证明，其中归纳步骤证明了所需条件语句的 *contrapositive*。

对于所有这些归纳的变体，我们为您提供了某些证明模板。将来请参考它们，并使用它们使您的证明井然有序、清晰易懂。这不仅会让读者更容易理解您的书面工作，还会重申这些证明技术背后的重要概念。请注意，这些并非我们出于迂腐而创造的：它们牢牢基于基本原理！

以下练习将使你在处理各种归纳论证方面获得大量实践。我们提出了一些比我们在第二章中看到的问题更具挑战性的问题。这是因为我们现在已经彻底研究了归纳原理，并对其应用于解决问题充满信心。此外，你在这些问题中证明的一些结果是很有趣且对我们有帮助的事实。我们将在本书后面的工作中有机会参考其中的一些，甚至！

5.7 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的所有内容，以及可能的一些假设的数学知识。当然，我们并不期望你解决其中的**all**，但你所做的越多，你将学到的就越多！记住，没有*doing*数学，你无法真正*learn*数学。动手解决一个问题。读几条陈述，四处走走，思考它们。

尝试写一个证明并展示给你的朋友看，看看他们是否信服。继续练习将你的想法和*write*以清晰、精确和逻辑的方式表达出来的能力。写出一个证明，然后编辑它，使其更好。最重要的是，持续*doing*数学！

简答题，只需解释或陈述答案，无需严格的*proof*，已用▶标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 5.7.1. 证明

$$\forall n \in \mathbb{N}. \sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$$

Problem 5.7.2. 对于以下每个不等式，确定使它成立的 *natural numbers* 集合。做一个 **claim** 并然后 **prove** 它（如果需要，通过归纳）。

(a) $3^n > n^4$b) $(n-3$
$)^2 > (n-2)^3$c) $3^n < n!$
(d) $4^n > n^4$

Problem 5.7.3. 以下主张的“证明”有什么问题?

Claim: 每个偶数自然数都是2的幂。

> 我们通过在 n 上的归纳法证明这一点。注意，$2 = 2^1$ 是 2 的幂。
>
> 接下来，假设 $k \in \mathbb{N}$ 和 $k \geq$ 是4，且 k 是偶数。假设从（但不包括）k 到的所有偶数自然数都是2的幂。
>
> 由于 k 是偶数，我们可以考虑 $\frac{k}{2}$。根据假设，$\frac{k}{2}$ 是 2 的幂，因此 $\frac{k}{2} = 2^j$ 对于某个 j。
>
> 这表明 $k = 2^{j+1}$，因此 k 是2的幂。

Problem 5.7.4. 假设一个数 $n \in \mathbb{N}$ 在 (x, y) 的土地上是“特殊的”，如果 n 可以写成 x 和 y 的非负倍数之和。

例如，在 $(3, 5)$ 的领域中，11是特殊的，因为$11 = 5 + 2 \cdot 3$。同样，在那个领域中，15也是特殊的，因为$15 = 3 \cdot 5 + 0 \cdot 3$。然而，在那里7不是特殊的。

对于以下每一对(x, y)，陈述并证明一个断言，以识别在各自领域中的所有特殊数字的集合$S_{x,y}$。

1. (2, 3)
2. (3, 5)
3. (4, 9)
4. (7, 6)

Problem 5.7.5. 证明对于任何 $n \in \mathbb{N}$，对于满足 $\forall i \in$ 的任何实数 $x_1, x_2, \ldots, x_n$，有 n。

$$\prod_{i=1}^{n}(1 - x_i) \geq 1 - \sum_{i=1}^{n} x_i$$

$0 \leq x_i \leq 1$, the following inequality holds:

这是已知为 **Bernoulli's Inequality**。

Problem 5.7.6. 设 $P(n)$ 为一个依赖于变量 n 的命题，该变量可以取任何 **integer** 值。

对于以下每种情况，你都会得到一些“基础情况”和一些“归纳假设”。识别并解释你能从这些假设中推导出哪些命题实例。

例如，如果你被给出 $P(3)$ 作为基准情况，以及 $\forall n \in \mathbb{N}$。 $P(n) \implies$

$P(n+1)$ as an inductive implication, a correct answer would be "We would know $P(3)$ holds for every $n \in \mathbb{N}$ with $n \geq 3$."

2. 已

1. 基本情况：3。蕴含：$\forall n \in \mathbb{Z}$。 $P(n) \implies P(n+1)$

se 案例：1, 2。含义：$\forall n \in \mathbb{N}$。$P(n) \implies P($

基本情况：$P(0)$。蕴含：$\forall n \in \mathbb{Z}$。

4. 基本情况：1, 0。蕴涵：$\forall n \in \mathbb{N}$。 $P(n) \implies P(n+2)$.

Problem 5.7.7. 证明对于任何整数 $x, y \in \mathbb{Z}$（满足 $x \neq y$），数 $x^n - y^n$ 是 $x - y$ 的倍数，对于每个 $n \in \mathbb{N} \cup \{0\}$。

Problem 5.7.8. (a) 确定满足不等式 $n! > 2^n$ 的自然数集 n。

(Recall: $n! = n \cdot (n-1) \cdots 1$.)

(b) 确定满足不等式 $n! > 3^n$ 的自然数集合 n。

(c) 确定满足不等式 $n! > 5^n$ 成立的自然数集合 n。

Problem 5.7.9. ⋆ 证明以下问题的推广：

$$\forall m \in \mathbb{N} - \{1\}\,.\,\exists B_m \in \mathbb{N}\,.\,\forall n \in \mathbb{N}\,.\; n \geq B_m \implies n! > m^n$$

Problem 5.7.10. 回想一下，**Fibonacci Numbers** 是通过将 $f_0 =$ 设为 0 和 $f_1 =$ 设为 1 定义的，然后对于每个 $n \geq 2$，设置 $f_n = f_{n-1} + f_{n-2}$。

证明以下对于此序列成立：

(a) $\forall n \in \mathbb{N} \cup \{0\}.\ f_n < 2^n$

(b) $\forall n \in \mathbb{N}.\ f_{n-1} f_{n+1} = f_n^2 + (-1)^n$

(c) $\forall n \in \mathbb{N}.\ 1 \leq \frac{f_{n+1}}{f_n} \leq 2$

(d) $\forall n \in \mathbb{N}.\ \sum_{k=1}^{n} f_{2k} = f_{2k+1} - 1$

(e) $\forall n \in \mathbb{N}.\ \sum_{k=1}^{n} f_k^2 = f_n f_{n+1}$

Problem 5.7.11. 在问题 5.7.1 中，你证明了前 n 个完全立方数之和的公式。具体来说，你证明了它是那些基数之和的 *square*。

在这个问题中，我们希望您证明这个断言的 *converse*，即具有这个性质的数字序列 *only* 是 $\langle 1, 2, \ldots, n \rangle$。我们将在下面为您重述这个主张，然后进行证明。

Claim: 假设 $\langle a_i \rangle$ 是一个实数序列，即 $\forall i \in \mathbb{N}$ ○ $a_i \in \mathbb{R}$. Suppose this sequence has the property that

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

证明，必然地，$\forall n \in \mathbb{N}$○ $a_n = n$, by induction on n.

Problem 5.7.12. (a) 证明 $\forall n \in \mathbb{N}$○ $7^n + 7 < 7^{n+1}$.

(b) 证明 $\forall n \in \mathbb{N}$○ $3^n + 3 < 3^{n+1}$.

(c) 确定满足 $\forall n \in \mathbb{N}$ 的实数集 S○ $r^n + r < r^{n+1}$.

Prove your claim by induction.

Problem 5.7.13. 证明对于每个 $n \in \mathbb{N}$，$2^{3^n} + 1$ 是 3^{n+1} 的倍数。

Problem 5.7.14. ⋆ 假设 $x + \frac{1}{x}$ 是一个整数。证明对于所有 $n \in \mathbb{Z}$，$x^n + \frac{1}{x^n}$ 是一个整数

(**Note:** 为每个 $n \in \mathbb{Z}$ 都这样做，而不仅仅是 $n \in \mathbb{N}$！)。

Problem 5.7.15. 通过对n进行归纳证明，对于每个$n \in \mathbb{N}$，$n^3 + 5n$ 是6的倍数。

Problem 5.7.16. 证明以下求和等式对每个 $n \in \mathbb{N}$ 都成立：

$$\sum_{k=n}^{2n-1} 2k + 1 = 3n^2$$

Problem 5.7.17. 对于每个 $n \in \mathbb{N} \cup \{0\}$，定义

$$s_n = \left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$$

证明每个这样的 s_n 实际上是一个整数。此外，实际上 s_n 是 2^n 的倍数。（！）

Problem 5.7.18. ► 在这个问题中，我们将证明熟悉的 **Harmonic Series**，由以下给出

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

是 **divergent**；也就是说，我们将证明所有项之和不会趋近于一个有限极限。

我们断言以下不等式对每个自然数 n 都成立：

$$\sum_{k\,=\,1}^{2^n} \frac{1}{k} > \frac{n+1}{2}$$

调用此不等式 ⋆。

(a) 证明当 $n = 1$ 时，⋆ 成立。

(b) 假设 $m \in \mathbb{N}$ 是任意且固定的，并且假设 ⋆ 对于值 $n = m$ 成立。

推导出 ⋆ 也适用于值 $n = m + 1$。务必引用上述关于 $n = m$ 的情况的假设。

(c) 想想你已经取得的成就。解释谐波级数不能收敛到任何有限极限的原因。

Problem 5.7.19. 证明以下不等式对每个 $n \in \mathbb{N}$ 都成立：

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots \frac{1}{\sqrt{n}} \geq \sqrt{n}$$

使用此方法推导出无穷级数 $\sum_{k=1}^{\infty} \frac{1}{\sqrt{k}}$ 是否收敛于一个有限的极限。

Problem 5.7.20. 证明以下不等式对每个 $n \in \mathbb{N}$ 都成立：

$$\prod_{i=1}^{n} \left(i + \frac{1}{i^2}\right) = \left(1+\frac{1}{1^2}\right)\left(1+\frac{1}{2^2}\right)\cdots\left(1+\frac{1}{n^2}\right) < 4 - \frac{1}{n}$$

Problem 5.7.21. 在这个问题中，你将证明自然数的 **Well-Ordering Principle**。这在定理 5.5.2 中有说明，但我们将在此重新陈述：

$$\forall S \in \mathcal{P}(\mathbb{N})\,.\,[S \neq \varnothing \implies (\exists \ell \in S\,.\,(\forall x \in S\,.\,\ell \leq x))]$$

这是 每个非空自然数集都有一个 **least ele ment.**
您将通过归纳法证明这一主张，即给定集合 S 是否包含 n 作为其元素。

我们将为您开始证明，然后引导您完成剩余部分：

设 $S \subseteq \mathbb{N}$ 为任意且固定的。对于每一个 $n \in \mathbb{N}$，定义 $P(n)$ 为命题

$$\text{“ } n \in S \implies [\exists \ell \in S \text{ . } (\forall x \in S \text{ . } \ell \leq x)] \text{ ”}$$

(a{v*} 证明 $P(1)$ 成立。（提示：最小的自然数是什么？）（b）设 $k \in \mathbb{N}$ 为任意且固定的。用逻辑符号写下，一个断言对于 1 和 k 之间的每个 i (包含在内的 $P(i)$ 都成立的假设。（提示：这应该很容易；只需写一个“和”语句。想想这代表什么。）接下来，假设 $k+1 \in S$。定义 $T = S - \{k+1\}$。有三种情况：（c）考虑 $T = \varnothing$ 的情况。证明 S 有最小元素。 (d) 考虑 $T \neq \varnothing$ 和 $\forall x \in S$ 的情况。(提示：*Here* 是您需要从 (b) 的 least element 归纳假设。）并应用假设的地方！

$x \geq k+1$. Prove that S has (e) Consider the case that $T \neq \varnothing$ and $\exists x \in S$.

$x < k+1$. Prove that S has a least element.

由于 S 在每种情况下都有一个最小元素，我们推断 $P(k+1)$ 成立。通过归纳，

(f) 让我们展示这个证明在实际（有效）考虑一些任意的 k，使得 $S \neq \varnothing$。我们如何知道 S 有一个最小元素？也就是说，哪个 **instance** 的断言 $P(n)$ 有保证成立的？

(提示：如果 $S = \varnothing$ ... 则会失败) (g) [加分] 为什么我们不直接对集合 S 的大小进行归纳？为什么那不能证明 **WOP**？

Problem 5.7.22. 设 W 为 **well-formed strings of parentheses** 的集合。集合 W 的任意元素 w 满足以下条件之一：

(i) w 是字符串 “( )”

(ii) $\exists x \in W$ 使得 w 是字符串 “(x)” （即 w 是围绕字符串 x 的括号字符串）

(iii) $\exists x, y \in W$ 使得 w 是字符串 “$x\,y$” （即 w 是在字符串 y 后附加的字符串 x）

例如，“( ) ( )”是W中的良好格式字符串，因为它由有效的字符串“( )”自身附加而成。然而，“(( )”不是W中的良好格式字符串，因为它不满足上述任何条件。

(作为一个更复杂的例子，我们将让您弄清楚为什么“((()))”是一个合法字符串。)

证明关于该系统的以下陈述。

(a) 证明每个元素 $w \in W$ 都有一个 **even** 个括号的数目，总共。

（**Hint:** 使用最小犯罪论点。假设 w 是一个 *smallest* 长度的奇数字符串⋯⋯）

(b) 对于 $w \in W$，令 $L(w)$ 为出现在 w 中的左括号数量，令 $R(w)$ 为右括号的数量。

证明 $\forall w \in W$，$L(w) = R(w)$.
(**Hint:** 对字符串的 *length* 进行归纳.)

Problem 5.7.23. 以下“欺骗”有什么问题，所有的笔都有相同的颜色?

“Spoof”: 我们声称所有钢笔颜色相同。我们将通过展示任何一组**size**钢笔中只有一种颜色在那些钢笔中代表来证明这一点。我们将通过按大小进行归纳来为这一主张提供归纳论证。

考虑一组尺寸为1的钢笔。由于只有1支钢笔，它当然与自己颜色相同。

现在，假设任何一组 n 钢笔在组内只代表一种颜色。

任取一组 $n+$ 支笔。将它们在桌子上排成一行，从左到右编号为 1 到 $n+1$。

查看它们中的第一个 n，即查看钢笔 $1, 2, 3, \ldots, n$。这是一组 n 钢笔，所以根据假设，这个组中只代表一种颜色。（我们还不清楚那是什么颜色。）

然后，查看笔的最后 n；即查看笔 $2, 3, \ldots, n+1$。这也是一套 n 笔，所以，根据假设，这个组中也只有一种颜色。

现在，笔#2恰好属于这两个集合。因此，无论笔#2是什么颜色，这也是*both*组中每支笔的颜色。因此，所有$n+1$支笔都有相同的颜色。

通过归纳，这表明任何尺寸的笔组，都只有一种颜色被代表。因此，观察世界上有限的笔的集合，我们只应找到一种颜色。“□”

Problem 5.7.24. 一个 n**-gon** 是一个有 n 边的凸多边形。例如，3-边形是三角形，4-边形是任何矩形，依此类推。（“凸”意味着形状中没有“凹口”，或者说，如果你在形状内部取任意两点并画出它们之间的线段，该线段不会超出形状。）

证明，通过在 n 上的归纳，存在 $\frac{n(n-3)}{2}$ 条可以在 n-边形顶点之间绘制的对角线。（不要将形状的实际边界 *sides* 计算为对角线，只计算 *interior* 对角线。）

5.8 Lookahead

我们现在拥有整个证明技术和逻辑知识的宝库，可以尝试探索数学宇宙的任何地方。我们将选择探索一些特定领域，目标是讨论**functions**。我们之前提到过这个想法，但尚未在数学环境中进行讨论。在接下来的两章中，我们将对这个概念进行形式化。

Part II

Learning Mathematical Topics

Chapter 6

Relations and Modular Arithmetic: Structuring Sets and Proving Facts About The Integers

6.1 Introduction

现在我们已经建立了数学术语、概念和材料的基础，你可能想知道我们接下来要讨论什么！嗯，就像我们想要*rigorize*数学归纳法的概念——这是我们直觉上“理解”但尚未以精确的数学方式发展的东西——在接下来的两章中，我们将建立在已经使用过的、你可能在直觉上熟悉的更稳固的基础上：一个**function**。

为了完成这个，我们将首先谈论 **relations**。这将引导我们进入 **equivalence relations** 的特定领域，使我们能够讨论集合的一些定性属性。特别是，我们将使用集合 $\mathbb{Z}$ 上的某些等价关系来陈述和证明关于整数的许多有趣属性。这将为我们提供机会简要探索 **Number Theory** 的数学分支。这是一个丰富、深入和广泛的领域，我们实际上只能通过陈述和证明一些有用的定理以及使用它们来解决一些有趣的谜题和问题来触及表面。然后，我们将直接进入下一章，并回到讨论 **functions** 的目标。

6.1.1 Objectives

以下本介绍中的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作

将有助于您，它们将激励我们为什么要调查本章中出现的话题，并且它们将告诉您我们的目标以及您在阅读时应该注意什么以实现这些目标。现在，我们将通过一系列声明为您总结本章的主要目标。这些描述了您在本章结束时应该掌握的技能和知识。以下各节将更详细地重申这些观点，但这将为您提供一份简短的参考清单。当您完成本章的学习后，请回到这份清单，看看您是否理解了所有这些目标。您明白为什么我们将它们列为重要吗？您能定义我们使用的所有术语吗？您能应用我们描述的技术吗？

By the end of this chapter, you should be able to ...

- 定义一个关系并提供许多示例。
- 定义并理解关系可能具有的各种属性，提供具有和不具有这些属性的关系的例子。
- 考虑一个已定义的关系，并发现和证明它具有哪些性质。
- 定义等价关系和等价类，并解释为什么这些是关系中的特别有趣和重要例子。
- 考虑一个定义的等价关系并对其等价类进行分类。
- 使用整数集上的特定等价关系来陈述和证明数论中的有趣结果。
- 定义乘法逆元的概念，理解这在模算术特定情境中的含义，并将这一想法应用于证明/反驳特定方程的解的存在性。
- 状态和了解数论中的各种定理，并将它们应用于解决给定问题。

6.1.2 Segue from previous chapter

这一章并不完全直接遵循前一章，就像其他章节那样。相反，我们实际上正在进入这本书的全新 *part*。从现在开始，我们将把迄今为止所发展的所有数学知识应用于学习其他有趣领域。我们需要先处理所有其他材料，才能达到这个阶段。从现在开始，我们将陈述复杂的命题并应用证明技术来证明它们。我们将为您提供定义和定理，并期望您使用它们来证明其他命题。从这个意义上说，这一章是从前几章的 *all* 发展而来的。我们将把所获得的所有知识、术语和经验都用于良好的用途！

6.1.3 Motivation

你可能在微积分（求导和积分）或高中代数课程（绘制函数图像或寻找其根）中接触过函数，甚至在计算机科学（编写算法或使用递归编程）中接触过。但试试这个：{v*}什么是函数。你将如何向从未学过数学的叔叔解释它？你将如何向一个超级智能的外星人解释它？你将如何尝试用我们通过数学归纳法提供的严谨程度来解释它？这并不容易，对吧？

为了发展一个关于 *functions* 的严谨概念，我们首先将讨论 *relations*，一种比较集合元素的方法。我们将研究许多例子及其性质。然后，在下一章中，我们将看到函数只是关系的一种特定类型！当我们讨论关系时，我们将探索它们的性质，并发现某些性质的组合会产生一个特殊性质。具体来说，我们将看到 *equivalence relations* 产生集合的自然 *partitions*，反之亦然。这个结果将使我们能够陈述并证明关于整数的一些结果。

6.1.4 Goals and Warnings for the Reader

这一章将继续我们探索抽象思想和严谨数学的旅程，因此，如果你觉得这种不断增长的抽象水平和其中所需的语言让你感到不适，那么你绝对不能被卷入其中，认为这些信息都不是“重要”或“适用”的。所有这些概念将继续出现在这本书的整个过程中——当然，还包括所有数学！——所以如果你发现自己失去了焦点，请记住这一点。我们建议你记下自己正在学习的笔记，以提醒自己你在做什么。当你看到定理并多次阅读它，最终理解它时，请在页边空白处写下定理的摘要或类似内容，这样你以后就能找到它。画一张小图来帮助你概念化例子或定理的重要部分。当你阅读定义时，写下典型例子和非例子。在阅读完证明后，简要记录论证步骤的概要，这样你就可以“块化”概念，更有效地记住（和回忆）它们。如果你理解了一个定义、定理或证明，也请记下你的困惑！在办公时间将问题带到同学、聪明的数学朋友、助教或教授那里，看看他们是否能解决你的困惑。最重要的是，请记住，消化和吸收这些类型的抽象概念和论证需要*time*，而且这和以前一样重要，始终通过例子来确保你以有意义的方式跟随*you*。如果你能足够理解某件事，以至于可以向别人解释它，那么你做得很好。

6.2 Abstract (Binary) Relations

6.2.1 Definition

让我们直接进入主题，开始讨论关系。我们将给出一个定义，然后提供一些例子。

Definition 6.2.1. *Let A, B be sets. A* **relation** *between A and B is a set of* **ordered pairs***, $R \subseteq A \times B$. Given elements $a \in A$ and $b \in B$, we say a and b are* **related** *if and only if $(a, b) \in R$.*

The set A is called the **domain** *and the set B is called the* **codomain***. The set R is called the* **relation set***.*

If $A = B$, we say R is a relation **on** *A.*

它也很常见将 $x\,R\,y$ 写作 $(x, y) \in R$。当我们以这种方式定义一个关系时，我们将坚持使用 $(x, y) \in R$ 的符号来表示其背后的 **set** 结构。稍后，我们有时会使用一些符号，如 $x < y$ 或 $x \star y$ 等来定义关系。

Remark 6.2.2. 一个关系，正如我们在这里定义的，有时也被称为一个 *binary relation*。这是因为关系有两个“输入”；集合 R 由有序的 *pairs* 组成。

我们可以将这个想法推广到 *ternary relations*。也就是说，给定集合 A, B, C，我们可以定义一个集合 $R \subseteq A \times B \times C$ 为一个三元关系，并说 a, b, c 如果且仅如果 $(a, b, c) \in R$ 则相关。我们还可以进一步推广到具有 n “输入” 的关系。然而，在这种情况下，我们只考虑 *binary* 关系，因此我们将使用术语 *relation* 来表示 *binary relation*。

Remark 6.2.3. 一个关系 R 通常通过识别 A 和 B (的元素的一个 *property*，并以变量命题 $P(a, b)$) 的形式表述来定义

$$(a, b) \in R \iff P(a, b)$$

Examples

Example 6.2.4. 设$W = \{$英语单词$\}$和$L = \{$英语字母$\}$。通过设定定义关系R

$$(w, \ell) \in R \iff w \text{ begins with } \ell$$

然后，（数学，m）$\in R$和（高尔夫，g）$\in R$，因为这些是有效的单词，并且我们已经确定了它们的起始字母。对于一些非示例，请注意（知识，n）$\notin R$和（你，u）$\notin R$。此外，请注意（zyzyxyqy，z）$\notin R$，因为zyzyxyqy$\notin W$。

通常情况下是 $A = B$，因此 R 定义了一个来自一个集合的元素对的二元关系。下一个例子考虑了这种情况。

Example 6.2.5. 设 $A = B = \mathbb{Z}$ 和定义在 $\mathbb{Z}$ 上的关系 R 由 设置

$$(x, y) \in R \iff x \text{ and } y \text{ have the same parity}$$

然后 $(2, 8) \in R$ 和 $(-3, 7) \in R$ 以及 $(-99, -99) \in R$，但 $(1, 2) \notin R$ 和 $(0, -3) \notin R$ 以及 $(\pi, 0) \notin R$ (由于 $\pi \notin \mathbb{Z}$)。

Example 6.2.6. 在 $\mathbb{R}$ 上定义一个关系 L，通过设置

$$(x, y) \in L \iff x < y$$

然后 $(-1, \pi) \in L$ 和 $(0, 100) \in L$ 但 $(2, 2) \notin L$ 和 $(\pi, -1) \notin L$。

注意，这些是 *ordered* 对（由于 $A = B = \mathbb{R}$ 我们可能忘记它们，所以元素的顺序很重要。实际上，知道 $(x, y) \in L$ 并不 *necessarily* 意味着 $(y, x) \in L$，通常情况下。在这个例子中，这个蕴涵总是 False，事实上！

回忆一下，我们有时写作 $x\, L\, y$ 来表示 $(x, y) \in L$，因此让我们注意，我们可以说 -1 $R\, \pi$ 但 $\pi \not R$ -1 这里，以及 2 $\not R$ 2。

The Empty Relation

Remark 6.2.7. 我们迄今为止看到的例子在某种意义上是 *interesting* 关系。对于任何 $x, y \in \mathbb{R}$，我们只需比较它们并决定该属性是否成立，就可以确定 $x < y$ 或不。也就是说，我们迄今为止看到的每个例子都是通过说 $(a, b) \in R \iff P(a, b)$ 对于某些属性 $P(a, b)$ 是真的来定义的。

一个关系不需要以这种方式定义，尽管如此。例如，我们知道对于集合 *any* set S。因此，给定两个集合，我们总是可以通过使用事实 $\varnothing \subseteq A \times B$ 来定义 *trivial relation*；也就是说，平凡关系是没有任何元素相关联的关系！这确实相对“无趣”，但它仍然满足关系的定义，所以我们允许它。

Any Set of Ordered Pairs is a Relation

Remark 6.2.8. 给定集合 A, B，**any** 是 $R \subseteq A \times B$ 的子集，定义了一个关系。可能很难（或者可能不可能）找到一个能表征该关系的属性。

例如，如果 $A = \{1, 3, 5\}$ 和 $B = \{\star, \heartsuit\}$，那么我们可以通过设置来定义 A 和 B 之间的关系

$$R = \{\, (1, \star), (5, \heartsuit) \,\}$$

为什么1与$\star$相关？为什么3与任何事物都不相关？谁知道呢？这仅仅是一组有序对！从数学上来说，这完全没问题。

The Equality Relation

Example 6.2.9. 任何集合 X 上定义关系的另一种方法是定义等价关系。也就是说，让 $(x, y) \in R \iff x = y$。注意，这并不取决于 X 是什么，或者它包含哪些对象作为元素，只是它是一个 *set*。

Similarities Between Relations

Example 6.2.10. 设S为你的班级中的学生集合。定义一个关系R_1，通过说如果一个人$s \in S$是n岁，则称其为$\in R_1$。写出这个关系集合的一些元素。

现在，通过说如果人员 s 和 t 的年龄（以年为单位）相同，定义一个在 S 本身上的关系 R_2。写出这个关系集的一些元素。

如何比较关系 R_1 和 R_2？它们是否以某种方式“编码”了集合 S 中元素的信息？为什么或为什么不呢？我们能否使用 R_1 来确定 R_2？反过来又如何？仔细思考这个问题，并尝试写几句话总结你的想法。我们将在下一小节立即讨论这些问题，但现在请花些时间自己调查！

Relations “Encode” Information

前一个例子旨在说明抽象关系的实际应用，并激发我们为什么要谈论它们（除了我们使*function*概念严格化的总体目标之外）。在某种意义上，关系是一种“存储”关于两个集合或一个集合的元素信息的方式；它是一种*comparing*两个元素并声明它们是否满足某些*property*的方式。然而，在更广泛的意义上，关系可以提供有关集合（或集合）的元素在特定属性方面“表现如何”的信息。

例如，注意在先前的例子中，关系 R_1 让我们关于 S 的元素了解得“更多”。当然，R_1 告诉我们谁和任何人一样大：我们可以寻找两个像 (s, n) 和 (t, n) 这样的对，它们的第二个坐标相同。但 R_1 也告诉我们 *what* 的年龄：只需看看这些对共享的第二个坐标。这 *not* 与 R_2 一样有效。知道 $(s, t) \in R_2$ 只告诉我们学生 s 和 t 一样大；它 *not* 并没有告诉我们那个年龄是多少！从这个意义上说，R_1 是一个“更好”的关系，提供了“更多”的信息。

也存在一些原因，使得 R_2 也“更好”，尽管如此！例如，看看它的一项良好属性：如果 $(x, y) \in R_2$，那么 $(y, x) \in R_2$ 也是 *necessarily* 真实的，同样如此。这当然 *not* 真实于 R_1，因为当 $(s, n) \in R_1$ 时，甚至没有意义去说 $(n, s) \in R_1$ 是否成立，因为这对的顺序与定义域和值域不匹配！这个属性现在使 R_2 成为一个“更好”的关系吗？嗯，是的，也不是。这取决于上下文以及我们想要编码和检索的信息类型。在某些情况下，可能你想使用 R_1，而在其他时候，你可能想使用 R_2。

但我们在这里有点超前了！我们还没有办法向您描述这些属性的含义以及为什么它们可能或可能不是所希望的。总的来说，我们对这些类型的属性以及它们在给定集合中对于*all*对元素（是否）成立感到好奇。在下一个小节中，我们将定义和探讨抽象关系的一些常见属性。并不是任何关系都保证（或要求）具有一个或多个这些属性，但这些属性已经在数学和现实世界中关系出现的环境中证明是有趣和有用的。之后，我们将看到许多关系示例并讨论如何*prove*这些属性成立。在这样做的同时，我们将培养一些关于如何处理关系以及甚至弄清楚我们最初试图证明的断言类型的直觉！

6.2.2 Properties of Relations

让我们立即定义一些属性。对于这些属性中的每一个，每个关系要么满足它，要么不满足它。我们鼓励您逐个阅读这些属性，并尝试构造一个满足该属性的关系，然后构造一个不满足该属性的关系。这将帮助您真正理解属性的内在原理以及关系是如何工作的。（然后，尝试定义一些具有属性组合的关系！）在这些定义之后，我们将提供一些您可能自己也能想到的典型例子！但说真的，请尽量自己想出一些，并分享您遇到的任何有趣的例子！

Definitions: Properties of a Relation on a Set

这些属性依赖于能够 *reverse* 一对顺序的能力。也就是说，给定 $(x, y) \in R$，我们可能会对 (y, x) 这对产生疑问；然而，定义域和值域之间的关系要求 $(y, x) \in A \times B$ 也必须如此。因此，我们将需要 $A \times B = B \times A$，这仅在 $A = \varnothing$ 或 $B = \varnothing$ 或 $A = B$ 时发生。（记住我们在第三章讨论集合时已经证明了这一点！）由于 $A = \varnothing$ 和 $B = \varnothing$ 是无趣的情况，因此在这些属性中，我们将假设 $A = B$（和 $A \neq \varnothing$），因此我们正在定义一个在 *one non-empty set* 上的关系，并比较其元素。

Definition 6.2.11. *Let A be a set and let R be a relation on A, i.e. $R \subseteq A \times A$.*

- *We say R is* **reflexive** *if*

  $$\forall x \in A \bullet (x, x) \in R$$

  That is, 每个元素都与自身相关.

- *We say R is* **symmetric** *if*

  $$\forall x, y \in A \bullet (x, y) \in R \implies (y, x) \in R$$

  That is, 比较的顺序无关紧要.

- *We say R is* **transitive** *if*

$$\forall x, y, z \in A \bullet [(x, y) \in R \land (y, z) \in R] \implies (x, z) \in R$$

That is, 关系可以通过中间人.转换

- *We say R is* **anti-symmetric** *if*

$$\forall x, y \in A \bullet [(x, y) \in R \land (y, x) \in R] \implies x = y$$

That is, two different elements can be related in at most one way, or not at all. To see why this is the same statement, let's look at the contrapositive of the conditional statement in the line above:

$$\forall x, y \in A \bullet x \neq y \implies [(x, y) \notin R \lor (y, x) \notin R]$$

注意：重要的是指出，*anti-symmetric* 与 *not symmetric* 并不相同。仔细观察属性的逻辑顺序和量词，以便理解这一点。例如，$\leq$ 在 $\mathbb{R}$ 上的关系是反对称的，但不是对称的。想想这是为什么。

实际上，试着找到一个既是 *anti-symmetric* 又是 *sym- metric* 的关系。这实际上并不难！我们已经提到了一个具有这种性质的基本关系。

6.2.3 Examples

再次，尝试找出一些满足和不满足我们刚才定义的四个性质的关系。以下我们将给出一些定义在$\mathbb{N}$上的关系的好例子，以给你一些具体想法。当你想到简单例子时，可以自由地添加到这个列表中，也许是在其他集合如$\mathbb{Z}$和$\mathbb{R}$上定义的。

Example 6.2.12. 在本例中，关系定义在集合 $\mathbb{N}$ 上。

- 定义 R_1 在 $\mathbb{N}$ 上为

$$(x, y) \in R_1 \iff x \text{ divides } y$$

(即 y 可被 x 整除，或 $\exists k \in \mathbb{N}$ 满足 $y = kx$。此定义在下面正式重述；参见定义6.2.15)

然后 R_1 是自反的，因为 $x|x$ 由于 $x = 1 \cdot x$。

The divisibility relation is reflexive.

- 定义 R_2 在 $\mathbb{N}$ 上通过

$$(x, y) \in R_2 \iff x \text{ and } y \text{ have the same parity}$$

然后 R_2 是对称的，因为如果 x 和 y 有相同的奇偶性，那么当然 y 和 x 也有相同的奇偶性。

The "has the same parity" relation is symmetric.

- 定义 R_3 在 $\mathbb{N}$ 上通过
$$(x, y) \in R_3 \iff x < y$$
然后 R_3 是传递的，因为如果 $x < y$ 和 $y < z$，那么 $x < y < z$，所以 $x < z$。
The "$<$" relation is transitive.

- 定义 R_4 在 $\mathbb{N}$ 上通过
$$(x, y) \in R_4 \iff x \leq y$$
然后 R_4 是反对称的，因为如果 $x \leq y$ 和 $y \leq x$ 则 $x \leq y \leq x$ 所以 $x = y$。

The "$\leq$" relation is anti-symmetric.

Example 6.2.13. 记住，一个关系只是一组有序对。我们不需要 *have* 用一个 *property* 来定义它。让我们用一个这样的例子来探讨，并研究其性质：

定义集合 $S = \{a, b, c\}$ 上的关系 R 为

$$R = \{(a, a), (a, c), (b, c), (c, b)\}$$

请注意，这个关系是：

- *Not Reflexive*(c, c) $\notin R$
- *Not Symmetric*(a, c) $\in R$ 但 $(c, a) \notin R$
- *Not Transitive*(: $(a, c) \in R$ 和 $(c, b) \in R$ 但 $(a, b) \notin R$
- *Not Anti-Symmetric*(: $(b, c) \in R$ 和 $(c, b) \in R$ 但 $b \neq c$)

Example 6.2.14. 让我们稍微练习一下使用稍微不同的关系符号。记住，我们也可以写像$x\, R\, y$这样的东西，表示$(x, y) \in R$。

定义你班级中人的集合 S 上的关系 $\star$，通过以下方式说明，对于任何 $x, y \in S$,

$$x \star y \iff x\ y \text{ 和 \{v*\} 同月出生}$$

我们断言这个关系是自反的、对称的和传递的。你明白为什么吗?

- 关系是 *reflexive*，因为每个人肯定是在和他们自己相同的月份出生的（即，$x \star x$）。
- 关系是 *symmetric*，因为如果人物 x 和人物 y 在同一个月（即 $x \star y$）出生，那么当然人物 y 和人物 x (只是顺序不同！) 也在同一个月（即 $y \star x$）出生。
- 关系是 *transitive* 因为……嗯，你明白的，对吧? 我们只是在反复诉诸"相同"这个概念!

关于这里的 *anti-symmetry* 呢？这取决于！你们班上有两个人 *different* 是在同一个月出生的吗？如果是这样，这种关系是 *not* 反对称的。然而，你们班上每个人都是在不同的月份出生的吗？如果是这样，这种关系 *is* 反对称，因为没有人会与除他们自己以外的人相关！想想这个……

6.2.4 Proving/Disproving Properties of Relations

当我们面对一个集合及其上的关系时，我们马上会想知道这些性质是否成立。通过玩弄所讨论集合的一些特定元素，我们可以尝试推测关系是否满足某个性质，然后尝试证明/反驳它。这有时相当于一点“猜测和检查”，但最终，为了证明一个性质成立，我们必须证明形式为“对于所有 . . . ，. . . 都成立”的陈述。（回顾第4.9节中的证明技巧！）因此，证明一个关系性质相当于取一个任意元素（或多个元素）并论证它们之间的关系。为了 *disprove* 这样的陈述，我们会证明其逻辑否定，形式为“存在 . . . 使得 . . . 。”（再次，回顾我们的证明技巧！）因此，反驳一个性质相当于找到一个 *counterexample*。让我们看看几个证明/反驳关系性质的例子。在练习中还有更多这类证明风格的例子。

The “Divides” Relation on $\mathbb{Z}$

我们将首先介绍（或许，提醒您）一个定义，因为它将成为我们例子中的一个基础。这是对整数对另一个整数进行*divide*的正式定义。

Definition 6.2.15. *Let $a, b \in \mathbb{Z}$. We say* **x divides y**, *and write* $\mathbf{x} \mid \mathbf{y}$, *if and only if*

$$\exists k \in \mathbb{Z} \bullet y = kx$$

Example 6.2.16{v*} 在 {v*} 上定义关系 {v*} 如下

$$(x, y) \in R \iff x \mid y$$

让我们确定 R 是否满足关系的四个性质之一，然后证明/反驳我们所有的主张！

一般来说，根据所讨论的集合和关系，你可能立即就能察觉到某个性质是否成立，通过某种直觉或者立刻就能“看到”它。如果是这样，太好了！如果不是（这更可能发生），我们建议开始一个“证明”，就像一个性质实际上成立一样，看看你是否能完成。如果你做到了，那么，你就证明了该性质！如果在某个地方遇到困难，可能是因为该性质不成立，你在证明中遇到的问题将为你提供一些寻找反例的启示。这种策略不*always*奏效（也许你正处

努力通过一个证明，因为实际上很有挑战性（比如说）但它可能非常有帮助，所以请记住。我们也会在这个例子中看到它的作用。

另一种策略——实际上更简单的一种策略——就是大声说出一个声明，或者用文字写下所讨论的关系和属性。有时，仅仅用普通语言让自己明白*say*某事，而不是在页面上阅读抽象符号，就会迫使你的大脑意识到一些有用的东西！我们在这里也会看到这种策略的实际应用。

- 让我们看看 R 是否等于 **reflexive**。这实际上意味着什么？让我们大声说出这句话。我们会期待这样的说法：“任何整数都能被自身整除。”当然！现在，让我们尝试用证明所需的符号术语将其写下来。

  Proof. 我们断言 R 是自反的。设 $x \in \mathbb{Z}$ 为任意且固定的。那么 $x \mid x$ 因为 $x = 1 \cdot x$ 和 $1 \in \mathbb{Z}$。因此，$(x, x) \in R$。因此，R 是自反的。 □

  Voilà！只是大声思考就帮助我们意识到一个事实，这使得我们更容易用数学语言写下这个陈述。

- 让我们看看 R 是否等于 **symmetric**。这个性质是用一个 *implication*，一个 *conditional statement* 来定义的。所以，让我们假设我们有一个任意的相关对，$(x, y) \in R$。我们是否一定会相信 $(y, x) \in R$，也是这样吗？换句话说：

  > 假设 x 能整除 y，我们是否也可以说 y 能整除 x?

  这实际上似乎相当不可能！知道 $x \mid y$ 告诉我们对于某些 $k \in \mathbb{Z}$，$y = kx$，但为什么这会让我们相信 $x = \frac{1}{k}y$ 意味着 $y \mid x$? 如果 $\frac{1}{k} \notin \mathbb{Z}$ 呢?

  您可能会在这个时候想说些像“嗯，$\frac{1}{k}$只有在k =1或$k = -1$时才是一个整数，所以就是这样。”但这并不是一个完整的解释！记住，为了反驳一个“对所有...”的断言，我们尽可能需要提供一个 *explicit counterexample*。我们不需要描述*all*在属性成立和不成立的情况下的特征，并试图一般性地解释事情。我们只需要*an*个例子来让某人相信该属性不成立。这比挥舞手臂并指出某个反例存在要直观得多。让我们只向读者展示一个，然后继续！

  Proof. 考虑$2, 6 \in \mathbb{Z}$。由于$6 = 3 \cdot 2$，我们有$(2, 6) \in R$。
  然而，编写 $2 = \ell \cdot 6$ 需要 $\ell = \frac{1}{3}$，以及 $\frac{1}{3} \notin \mathbb{Z}$。因此，$(6, 2) \notin R$。
  这表明 R 是 *not symmetric*。 □

- 让我们看看 R 是否等于 **transitive**。一般来说，传递性通常是思考起来最困难的一个属性。这部分的困难是由于它由一个带有 *two* 假设的条件语句定义，并且使用了 *three* 个变量。

  在这个特定例子中，我们将假设 $x \mid y$ 和 $y \mid z$，然后思考 $x \mid z$ 是否必然。试着大声说出来，看看你是否相信它。

  这似乎是真的，对吧？现在，试着用数学语言写下假设和结论。你能看到如何将这些拼凑在一起吗？在继续阅读之前，试着写出你自己的这个证明版本。

  Proof. 设 $x, y, z \in \mathbb{Z}$ 为任意且固定的。假设 $(x, y) \in R$ 和 $(y, z) \in R$。

  这意味着 $x \mid y$ 和 $y \mid z$，因此 $\exists k, \ell \in \mathbb{Z}$ 使得 $y = kx$ 和 $z = \ell y$。设这样的 k, ℓ 已给出。

  将第一个方程代入第二个方程，我们得到 th 在

  $$z = \ell y = \ell(kx) = (k\ell)x$$

  自 $k\ell \in \mathbb{Z}$ 以来，我们也已表明 $x \mid z$。因此，$(x, z) \in R$ 必然。

  因此，R 是传递的。 □

- 让我们看看 R 是否是 **anti-symmetric**。这个性质也由一个包含两个假设的条件语句定义，因此我们将假设我们有一个 x 和一个 y，以及 $x \mid y$ 和 $y \mid x$。我们能否得出 $x = y$ 的结论？这个问题让人回想起证明 R 不是对称的。记住，我们证明了 $x \mid y$ 并不必然意味着 $y \mid x$，实际上，如果你稍微思考一下，$x \mid y$ *and* $y \mid x$ 两者都为真的可能性实际上非常低。这怎么可能呢？仔细思考一下，在你阅读我们的证明之前，试着提出你自己的证明。

  Proof. 设 $x, y \in \mathbb{Z}$ 为任意且固定的。假设 $(x, y) \in R$ 和 $(y, x) \in R$。

  这意味着 $x \mid y$ 和 $y \mid x$，因此 $\exists k, \ell \in \mathbb{Z}$ 使得 $y = kx$ 和 $x = \ell y$。给定这样的 k, ℓ。

  将第一个方程代入第二个方程，我们得到 $y = kx = k(\ell y) = (k\ell)y$。现在有两种情况。

  Case 1: 假设 $y = 0$。那么我们不能同时除以 y。相反，我们观察到 $x = \ell y = \ell \cdot 0 = 0$，因此 $x =$ 也为 0。因此，在这种情况下，$x = y$。

  Case 2: 假设 $y \neq 0$。然后我们可以将两边都除以 y。这得到 $k\ell = 1$。由于 $k, \ell \in \mathbb{Z}$ 这意味着要么 $k = \ell = 1$ 要么 $k = \ell = -1$。

If $k = \ell = 1$, then $x = \ell y = y$. In the other case ... ⍁

哦，糟糕！这不起作用！你看到了发生了什么吗？在“大多数”情况下，我们确实得出结论 $x = y$，但实际上有 $y = -x$ 的可能性。例如，当 $y = 3$ 和 $x = -3$ 时，请注意 $x \mid y$ 和 $y \mid x$ 但 $x \neq y$。这正是我们需要的反例，而试图完成我们的“证明”帮助我们找到了它。也许你从一开始就看到了这个情况；如果是这样，做得好！让我们通过展示这个反例来结束这个话题：

Proof. 考虑 $x = 3$ 和 $y = -3$，因此 $x, y \in \mathbb{Z}$。注意 $x \mid y$ 和 $y \mid x$ 因为 $3 = (-1)(-3)$ 和 $-3 = (-1) \cdot 3$，并且由于 $-1 \in \mathbb{Z}$。

然而，当然 $x \neq y$。这表明 R 是 *not* 反对称的。 □

作为一个后续问题，考虑当我们在这个集合 $\mathbb{N}$ 上而不是 $\mathbb{Z}$ 上定义这个关系时会发生什么。有什么变化？现在哪些性质成立？与 $\mathbb{Z}$ 相比，是否有任何答案不同？请思考一下。这些问题的答案将激发我们下一个子节的讨论。

Constructing a Relation with Specific Properties

在继续之前，再举一个例子。一个有趣的“游戏”是取一个集合并构造一个满足四个特定属性之一的关联 R。（注意：四个属性可以或不可以成立的16种不同方式。）我们将在练习中提出类似的问题，所以让我们在这里通过一个例子来解决这个问题。

Example 6.2.17. **Goal:** 设S为这个班级的学生集合。定义一个关系R，它满足以下条件：(1) 不是自反的，(2) 不是对称的，(3) 是传递的，(4) 是反对称的。

为确保 R 不是自反的，我们必须确保没有任何元素与自身相关。为确保 R 不是对称的，我们必须确保每当有一对 $(x, y) \in R$，那么 $(y, x) \notin R$。为确保 R 是传递的，我们必须确保每当 $(x, y) \in R$ 和 $(y, z) \in R$，那么 $(x, z) \in R$。而要确保 R 是反对称的，我们将考虑该属性定义的逆否形式，这要求任何一对元素在 *at most* 中以某种方式相关。这个最后的属性可能是最难思考的；它表明对于每个 $x, y \in S$，要么 x 与 y 相关但不是另一种方式，要么 y 与 x 相关但不是另一种方式，要么 x 和 y 两种方式都不相关。也就是说，我们不允许任何一对满足 *both* $(x, y) \in R$ 和 $(y, x) \in R$。（再次，重新阅读反对称的定义，写下条件语句的逆否，并思考为什么这有效。）

现在让我们尝试构造 R 以满足这些属性。属性（1）意味着我们的定义不能允许任何形式为“或等于”的东西，而（2）意味着定义必须以“唯一一种方式”关联“任何 x 和 y”。因此，我们可能会猜测一个 *comparison* 属性，类似于 $\mathbb{Z}$ 上的“小于”关系，可能有效。让我们试试，并尝试证明/反驳所需的属性。

让我们在 S 上定义 R 为

$$x\,R\,y \iff x \text{ 严格小于 } y \text{ (岁)}$$

现在，让我们探索它的属性并确保它们是我们想要的。在阅读我们的解决方案之前，尝试自己证明/反驳它们！此外，在 S (上玩一个 *different* 关系，自己想一个！)，看看它的属性有何不同。你能想出一个具有与这个完全相同属性的关系吗?

- R 是 **not reflexive**。这是因为任何一个人 $x \in S$ 都和他/她有相同的年龄，所以 $x \not R\ x$。
- R 是 **not symmetric**。这是因为如果 x 严格小于 y，那么 y 严格 *older* 于 x，所以 $y \not R\ x$
- R 是 **transitive**。这是因为如果 x 比 y（严格）年轻，并且 y 比 z（严格）年轻，那么当然 x 比 z（严格）年轻。
- R 是 **anti-symmetric**。这是因为对于任何两个人 $x, y \in S$，其中一个人必须比另一个人年轻，否则他们年龄相同；他们不能 *both* 严格地互相年轻。（本质上，我们通过确保该属性定义中的条件语句的 *hypothesis* 永远不成立，从而确保反对称性成立，因此条件语句始终是 True。）

因此，此关系 R 满足所有所需性质。

您会注意到我们在这些论点中并不 *completely* 严谨，但这是有原因的。具体来说，我们没有为失败的属性提供 *explicit* 反例。最好能找到你们班上的两名学生，展示一个比另一个年轻，但反过来不行。但我们不知道你们班上有谁！这就是为什么我们把论点留在了“解释某物的存在而不明确指出它”的状态。

我们将指出，一般来说，这种形式的关系——定义为（x, y）$\in R \iff x$比 y (“小”，然而在这种语境中“小”是有意义的)——将是非自反的、非对称的、传递的和反对称的。事实上，我们甚至可以用“大于”来替换“小于”，这仍然成立。要了解为什么这是真的，考虑在$\mathbb{N}$、$\mathbb{Z}$或$\mathbb{R}$上的“$<$”关系，或者考虑那些集合上的“$>$”关系。考虑在人群集合上的“比某人年轻”关系，或者“比某人高”关系，或者“孩子比某人多”关系。关于$\mathbb{Z}$上的“$\leq$”关系又是怎样的呢？这与“$<$”关系有何不同？哪些属性发生了变化?

(这些类型的问题将在下一小节中进一步探讨，我们将研究一种类似于这些“$\leq$”和“$\geq$”关系的特定类型的关系。它们自然被称为**order relations**。)

6.2.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 如何根据集合定义 *(binary) relation*?

(2) 假设我们有一个在 A 和 B 之间定义的关系 R。为了能够讨论 R 是否是 **reflexive**，关于 A 和 B 必须满足什么条件？(3) 何时一个关系 **reflexive**？给出一个集合和该集合上的一个自反关系的例子。(4) 何时一个关系 **symmetric**？给出一个集合和该集合上的一个对称关系的例子。(5) 何时一个关系 **transitive**？给出一个集合和该集合上的一个传递关系的例子。(6) 何时一个关系 **anti-symmetric**？给出一个集合和该集合上的一个反对称关系的例子。

(7) *not symmetric* 和 *anti-symmetric* 之间的区别是什么?

给出一个集合及其上既对称又反对称的关系的例子。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 考虑集合 $A = \{1, 2, 3\}$。对于以下在 A 或 $\mathcal{P}(A)$ 上定义的每个关系，决定它是否是 (i) 自反的，(ii) 对称的，(iii) 传递的，(iv) 反对称的。不需要太多论证，只需一个 Yes 或 No 以及一两句话。 (a) R_a 在 A 上定义为 $R_a = \{ (1, 1), (1, 2), (2, 1), (2, 2), (3, 3) \}$ (b) R_b 在 A 上定义为 $R_b = \{ (1, 1), (1, 2), (2, 2), (2, 3), (3, 3) \}$ (c) R_c 在 $\mathcal{P}(A)$ 上定义为 $\forall S, T \in \mathcal{P}(A)$。

$(S, T) \in R_c \iff S \cap T = \varnothing$ (d) R_d on $\mathcal{P}(A)$ defined by $\forall S, T \in \mathcal{P}(A)$。

$(S, T) \in R_d \iff S \cap T \neq \varnothing$

(e) R_e 在 $\mathcal{P}(A)$ 中定义的 $\forall S, T \in \mathcal{P}(A)$ $S \subseteq T$ $(S, T) \in R_e \iff$

(2) 定义在 $\mathbb{Z}$ 上的关系 $\star$，通过以下方式说明

$$\forall x, y \in \mathbb{Z}\text{.}\ x \star y \iff 3 \mid x - y$$

(a) 证明 $\star$ 是自反的。

(b) 证明 $\star$ 是对称的。

(证明 $\star$ 是传递的。)

（请记住，“$\mid$”表示“除以”。务必使用正式定义；参见定义6.2.15。）

(3) 通过以下方式在 $\mathbb{Z}$ 上定义关系 $\sim$:

$$\forall x, y \in \mathbb{Z}\text{.}\ x \sim y \iff 3 \mid x + 2y$$

(a) 证明 $\sim$ 是自反的。 (b) 证明 $\sim$ 是对称的。 (c) 证明 $\sim$ 是传递的。

(4) 定义在 $\mathbb{R}$ 上的关系 T，说法是，对于任何 $x, y \in \mathbb{R}$,

$$(x, y) \in T \iff \left(\frac{y}{x} \in \mathbb{R} \ \wedge \ \frac{y}{x} \geq 0 \right)$$

(a) 找到 $x \in \mathbb{R}$ 使得 $(x, x) \notin T$。这是否意味着 T 不是自反的? 为什么或为什么不? (b) 找到 $x, y \in \mathbb{R}$ 使得 $(x, y) \in T$ 和 $(y, x) \in T$。这是否意味着 T 是对称的? 为什么或为什么不? (c) 找到 $x, y \in \mathbb{R}$ 使得 $(x, y) \in T$ 但 $(y, x) \notin T$。这是否意味着 T 不是对称的? 为什么或为什么不? (d) 确定是否 T 是传递的，并证明你的主张。

(5) 定义在 $\mathcal{P}(\mathbb{N})$ 上的关系 $\leftrightarrow$，说法是，对于任何 $X, Y \subseteq \mathbb{N}$,

$$X \leftrightarrow Y \iff \left(X \subseteq Y \quad \vee \quad X \cap Y = \varnothing \right)$$

证明/反驳该关系的四个标准性质（即自反性、对称性、传递性、反对称性）。

(6) 以下“证明”中，对称性和传递性属性如何导致自反性属性出现问题?

设 A 为一个非空集合。设 R 是 A 上的一个关系。

假设 R 是对称和传递的。我们将证明 R 是自反的。

设 $x \in A$ 为任意且固定的。定义集合 T 为

$$\{y \in A \mid (x, y) \in R\}$$

设 $y \in T$ 已知。因此，$(x, y) \in R$。

由于 R 是对称的，我们可以推断 $(y, x) \in R$。

由于 R 是传递的，并且 $(x, y) \in R$ 和 $(y, x) \in R$，我们推断 $(x, x) \in R$。

由于 x 是任意的，我们已经证明了自反性质成立。

6.3 [Optional Reading] Order Relations

让我们讨论一些像“$\leq$”这样的关系，并具有类似固有属性的关系。这源于这些关系可以轻易地定义在我们拥有的标准数字集合上——$\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$——并且它们也适用于一些其他，可能令人惊讶的情况。我们首先给出定义，然后考虑一些例子。然后我们将使用这些例子来激发一些有序关系有趣性质的动机，然后陈述并证明这些事实。

Definition 6.3.1. *Let R be a relation defined on the set A.*

- *If R is reflexive, transitive, and anti-symmetric, then we say R is a* **partial order** *on A.*
- *If R is reflexive, transitive, and anti-symmetric and, in addition, it satisfies*

  $$\forall x, y \in A \bullet (x, y) \in R \vee (y, x) \in R$$

  then we say R is a **total order** *on A. (That is, a total order is a partial order such that every two elements of the set are comparable one way or the other.)*

这个定义告诉我们什么是偏序和全序。下一个定义只是为我们提供了一些有用的缩写，用于指代集合上的偏序和全序。

Definition 6.3.2. *When R is a partial order on A, we say that the pair (A, R) is a* **partially ordered set**, *or sometimes just a* **poset**, *for short.*

When R is a total order on A, we say that the pair (A, R) is a **totally ordered set**, *or sometimes just a* **toset**, *for short.*

我们将通过给出几个相关例子来解释这些术语的原因。

Example 6.3.3. 在 $\mathbb{R}$ 上定义以下四个关系 :

$$(x, y) \in R_1 \iff x \leq y$$
$$(x, y) \in R_2 \iff x < y$$
$$(x, y) \in R_3 \iff x = y$$
$$(x, y) \in R_4 \iff \lfloor x \rfloor = \lfloor y \rfloor$$

(回忆一下，$\lfloor x \rfloor = \max\{a \in \mathbb{Z} \mid a \leq x\}$ 是一个实数的“地板”；它是向下取整后得到的整数.)

这些中哪些是偏序？全序？都不是？思考几分钟，尝试绘制一些证明你主张的草图，或者向朋友/同学大声解释。

现在，这里是我们的想法。关系 R_1 和 R_3 都是偏序，但只有 R_1 是全序。关系 R_2 和 R_4 既不是偏序也不是全序（因为 R_2 不是自反的，R_4 不是反对称的）。任何类型（偏序或全序）的顺序关系的背后思想是，我们可以以某种方式 *compare* 集合 A 的元素并将它们 . . . 良好地分配，一个 *ordering* 给它们。从启发式角度讲，偏序在 A 中诱导“元素链”，这样我们就可以沿着任何链排列元素，有点像数轴以及我们通常如何想象 $\mathbb{R}$；对于 *total* 序，只有一个“链”，它就是所有的 A。

您可能会反对这样的观点，即 R_2 并非某种“顺序”关系，您确实有合理的观点。R_2 和 R_1 之间的唯一基本区别是我们不允许相等；字面上讲，“或等于”这一短语被纳入了“$\leq$”的定义中，然而这一短语却未出现在“$<$”的定义中。这导致 R_2 是非自反的，但仅此而已。您可能还会注意到，关系 R_4 并不具有与 R_1 相同类型的这种关系；它似乎是一种不同的事物（我们很快就会讨论这一点）。这促使以下几个定义的产生，其中部分或全序可以被“放宽”为相关的排序。

Definition 6.3.4. *Let A be a set and let R be a relation on A. We say R is* **irreflexive** *if and only if*

$$\forall x \in A \bullet (x, x) \notin R$$

请注意，这与仅仅是 *not reflexive* 相同。考虑量词：自反性意味着 *every* 元素与其自身相关，因此该命题的否定意味着至少有一个元素与其自身不相关。非自反性意味着 *every* 元素不与其自身相关。

Definition 6.3.5. *Let A be a set and let R be a relation on A. We say R is a* **strict partial order** *if it is irreflexive, transitive, and anti-symmetric.*

We say R is a **strict total order** *if it is irreflexive, transitive, anti-symmetric, and satisfies the following property:*

$$\forall x, y \in A \bullet x \neq y \implies [(x, y) \in R \vee (y, x) \in R]$$

您可能会想知道这里与非严格顺序关系有什么联系。嗯，有一种自然的方法可以将任何顺序关系转换为严格顺序，反之亦然。我们总是可以通过在元素之间建立或删除关系来定义一个从另一个，这样做可以总结以下引理如何进行，并且在这个过程中表明严格顺序和非严格顺序的数量是相同的。

Lemma 6.3.6. *Let (A, R_1) be a partially ordered set. Then the relation S_1 defined by*

$$(x, y) \in S_1 \iff [(x, y) \in R_1 \wedge x \neq y]$$

is a strict partial order on A.

Let (A, R_2) be a totally ordered set. Then the relation S_2 defined by

$$(x, y) \in S_2 \iff [(x, y) \in R_2 \wedge x \neq y]$$

is a strict total order on A.

Let (A, S_3) be a strictly partially ordered set. Then the relation R_3 defined by

$$(x, y) \in R_3 \iff [(x, y) \in S_3 \vee x = y]$$

is a (non-strict) partial order.

Let (A, S_4) be a strictly totally ordered set. Then the relation R_4 defined by

$$(x, y) \in R_4 \iff [(x, y) \in S_4 \vee x = y]$$

is a (non-strict) total order.

回顾上面在 $\mathbb{R}$ 上定义的 R_1 和 R_2 关系，用“小于等于且不等于”来定义“小于”可能有点奇怪。这当然更啰嗦！然而，这只是我们语言描述“$\leq$”的一个结果。从数学的角度讲，更自然的是谈论自反关系和偏序与全序，然后修改这些关系以成为严格序。我们很快就会看到——当我们谈到 *minimal* 元素时——为什么自反性是一个很好的属性，这也是我们为什么从偏序开始，然后修改定义以允许严格序，而不是反过来，一个合理的解释。现在，只需注意 R_2 是对应于全序 R_1 的严格全序。

问题：是否存在与偏序 R_3 对应的严格偏序？如果存在，它是什么？如果不存在，为什么？

R_4 不是任何类型的序关系，无论是严格的还是其他类型的。然而，请注意 R_4 很好地将 $\mathbb{R}$ 的元素“打包”在一起。本质上，每个满足 $1 \leq y < 2$ 的实数 y 在这个关系下“相同”。同样，对于每个满足 $2 \leq y < 3$ 的 y，以及每个满足，比如说 $-5 \leq y < 4$ 的 y，以此类推。一旦完成这种“打包”，我们就“知道”可以给这些“打包”分配一个顺序，但关于这个顺序的信息并没有编码在关系 R_4 本身中。我们必须做一些额外的工作来强加这种顺序。这就是为什么 R_4 不是一个序关系

任何类型的，它的定义方式。然而，我们称之为“*equivalence relation*”，因为这种“包装”属性将集合的元素划分为不同的类别。这是我们将在下一节中探讨的概念。一旦我们建立了这些“包裹”，我们就可以比较它们并对其进行排序。

让我们在其他上下文中探索一些示例，而不是 $\mathbb{R}$。以下这些关系中的一个实际上是偏序的标准示例。

Example 6.3.7. 让 $S = [3]$ 并考虑幂集，$\mathcal{P}(S)$。(记住，S 的幂集是 S 的所有子集的集合。) 在 $\mathcal{P}(S)$ 上定义以下关系，其中 $X, Y \subseteq S$:

$$(X,Y) \in R_1 \iff X \subseteq Y$$
$$(X,Y) \in R_2 \iff X \subset Y$$
$$(X,Y) \in R_3 \iff X \cap Y = \varnothing$$
$$(X,Y) \in R_4 \iff X \Delta Y = S$$

回忆一下，$X\Delta Y$ 是 *symmetric difference* 的 X 和 Y，定义为 $X\Delta Y = (X - Y) \cup (Y - X) = (X \cup Y) - (X \cap Y)$。

我们声称 R_1 是一个偏序但不是全序。在我们继续证明这个论断之前，考虑以下挑战问题：你能否在 $\mathcal{P}(S)$ 上定义一个全序？你能否以一种可以推广到 $S = [n]$ 的情况下的方式来做这件事，其中 $n \in \mathbb{N}$ 是任意的。

现在，为了证明 R_1 是一个偏序，我们必须证明它是自反的、传递的和反对称的。为了证明它不是全序，我们必须证明它未能满足任何两个元素都是可比较的附加性质。我们将完成其中一些步骤，其余的作为练习。

- 让我们证明 R_1 是反对称的：设 $X, Y \in \mathcal{P}(S)$ 并假设 $(X, Y) \in R_1$ 和 $(Y, X) \in R_1$。这意味着 $X \subseteq Y$ 和 $Y \subseteq X$，因此根据集合的标准性质，有 $X = Y$。
- 让我们证明 R_1 不是一个 *total* 次的。考虑 $X = \{1\} \subseteq S$ 和 $Y = \{2, 3\} \subseteq S$。注意 $X \not\subseteq Y$ 和 $Y \not\subseteq X$，所以 $(X, Y) \notin R_1$ 和 $(Y, X) \notin R_1$。也就是说，X 和 Y 在这个关系下是 *incomparable*。

这个关系将整个集合 $\mathcal{P}(S)$ 分成 *chains*，这些集合内部是有序的，但不同的链可能包含不可比较的元素。例如，考虑以下 $\mathcal{P}(S)$ 的子集:

$$A_1 = \{\varnothing, \{1\}, \{1,2\}, \{1,2,3\}\}$$
$$A_2 = \{\varnothing, \{1\}, \{1,3\}, \{1,2,3\}\}$$
$$A_3 = \{\varnothing, \{2\}, \{1,2\}, \{1,2,3\}\}$$
$$A_4 = \{\{3\}, \{2,3\}\}$$

这些集合不是互斥的，因此它们不形成 *partition* 的 $\mathcal{P}(S)$。注意，尽管如此，R_1 在每个子集中都按照 *induce* 的 *total* 顺序排列。当我们说“诱导”时，我们的意思是我们使用 R_1 的相同的定义属性，但将我们的域限制为集合 A_1，例如，而不是 $\mathcal{P}(S)$ 的全部。当然，我们还可以定义更多的集合，这些集合在这个关系下是链。

让我们将这个概念形式化，然后继续我们的例子

Definition 6.3.8. *Let (A, R) be a partially ordered set, and let $B \subseteq A$. Let $\hat{R}$ denote the relation induced by R on B; that is, we set*

$$\forall x, y \in A \bullet (x, y) \in \hat{R} \iff [x, y \in B \wedge (x, y) \in R]$$

If $(B, \hat{R})$ is a totally ordered set, then we say B is a **chain** *of A (under R).*

有了这个定义，我们看到A_1, A_2, A_3, A_4是在R_1下的$\mathcal{P}(S)$的链。现在，尝试证明R_2是一个（严格）偏序，然后尝试写出一些在关系R_2下的$\mathcal{P}(S)$的链。它们与在R_1下的$\mathcal{P}(S)$的链相比如何?

在下一个小节中，我们将了解为什么链很重要；具体来说，我们将研究偏序、链和全序的特殊性质，这些性质使我们能够找到子集的“最小”和“最大”元素。

在继续之前，让我们看看两个更多相关的偏序关系示例。

Example 6.3.9. 考虑集合 $\mathbb{R} \times \mathbb{R}$。我们通过确定一个实数 *pair* 与另一个实数 *pair* 之间的关系来在 $\mathbb{R} \times \mathbb{R}$ 上定义一个关系 R。具体来说，让我们假设

$$\big((u, v), (x, y)\big) \in R \iff [u \leq x \wedge v \leq y]$$

可以证明 R 是 $\mathbb{R} \times \mathbb{R}$ 上的偏序。我们将证明传递性性质，其余的留作练习:

Proof. 设$(u, v), (x, y), (z, w) \in \mathbb{R} \times \mathbb{R}$。假设$((u, v), (x, y)) \in R$且$((x, y), (z, w)) \in R$。这意味着$u \leq x$和$x \leq z$，因此$u \leq z$；这也意味着$v \leq y$和$y \leq w$，因此$v \leq w$。因此，$((u, v), (z, w)) \in R$。这表明$R$是传递的。 □

提示：为了证明 R 不是 *total* 阶，我们必须找到一个反例。也就是说，我们需要一个对 $(x, y), (u, v)$，使得既不是 $((x, y), (u, v)) \in R$ 也不是 $((u, v), (x, y)) \in R$。从直观上，即从几何上考虑 R 的关系，来想出这样的例子。

考虑在这个关系下链是什么。尝试从几何角度描述它们并绘制几个代表。

Example 6.3.10. 设 A 为26个字母的标准英文字母表，设 W 为所有由 A 中的字母组成的 *finite* 字符串的集合。也就是说，W 是所有可能的“单词”的集合，其中我们允许任何字母组合包含在我们的“字典”中。让我们尝试定义 L，即标准 *lexicographic* 排序在

W. 它有助于将 A 表示为集合 [26]，其中 a = 1 和 b = 2，依此类推，直到 z = 26。然后，我们说一个单词 $w \in W$ 是由

$$w = (w_1, w_2, \ldots, w_n) \quad \text{where } n \in \mathbb{N} \text{ and } \forall i \in [n]\,.\; w_i \in A$$

注意，对于任何两个单词 $v, w \in W$，我们可以“逐字母”地比较它们，从左到右阅读，直到我们找到它们之间的差异。差异发生的地方，我们根据这两个字母的比较来对这两个单词进行排序。如果一个单词比另一个单词长，并且它们的字母相同，那么我们希望将较长的单词 *after* 排在较短的单词之前，就像在字典中“there”排在“therefore”之前一样。

$$(v, w) \in L \iff \text{at the smallest index } i \text{ where } v_i \neq w_i, \text{ we have } v_i < w_i$$
$$\text{(and where a blank space is treated as 27)}$$

考虑为什么这与字典中单词的通常顺序相对应。（你能用更严谨的数学符号来定义这个吗？试试看！）

现在我们已经看了几个有序关系的例子，我们建议你尝试几个练习来练习识别这些关系并证明它们的性质。之后，我们可以继续讨论有序关系的许多其他有趣和有用的性质！

6.3.1 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 部分序和全序之间的区别是什么？

(2) 给出一个不是全序的偏序的例子。给出一个全序的例子。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 设 $S = [2]$，并在 $\mathcal{P}(S)$ 上通过 (x, y) 定义 R，使得 $\in R \iff x$ 在 *least* 中有与 y 相同的元素个数。证明 S 不是一个偏序。

(2) 令 S = [3]，T = [2]，并定义 $R \subseteq S \times T$ 为 $(x, y) \in R \iff x \supseteq y$。证明/反驳 R (的四个标准关系属性，即自反性、对称性、传递性、反对称性。) 使用你的结果来确定 R 是否是任何类型的序关系。

6.4 Equivalence Relations

6.4.1 Definition and Examples

让我们稍微换一下话题，讨论另一种满足关系四个标准属性不同子集的关系。事实上，让我们回到之前例子中提到的一个特定关系：在集合 $\mathbb{R}$ 上，定义 R 为满足以下关系：

$$(x, y) \in R \iff \lfloor x \rfloor = \lfloor y \rfloor$$

(在您错过可选阅读内容的情况下，这在示例6.3.3中可以看到。) 注意到这个关系是

- *reflexive* 因为 $\forall x \in \mathbb{R}$ $\lfloor x \rfloor = \lfloor x \rfloor$
- *symmetric* 因为 $\forall x, y \in \mathbb{R}$ $\lfloor x \rfloor = \lfloor y \rfloor \implies \lfloor y \rfloor = \lfloor x \rfloor$
- *transitive* 因为 $\forall x, y, z \in \mathbb{R}$ $\left(\lfloor x \rfloor = \lfloor y \rfloor \wedge \lfloor y \rfloor = \lfloor z \rfloor\right) \implies \lfloor x \rfloor = \lfloor z \rfloor$

这个特定的属性集有一些有趣和有用的后果，因此我们为具有这三个属性的任何关系赋予一个名称。

Definition 6.4.1. *Let A be a set and R a relation on A. If R is reflexive, symmetric, and transitive, then we say R is an* **equivalence relation**.

这就可以了！对于集合 S 上的任何关系 R，我们只需要逐一证明/反驳这三个性质，以确定 R 是否实际上是一个等价关系。让我们回顾一下我们已经看到的一些关系的例子，并根据我们对它们的证明来确定它们是否是 *equivalence* 关系。

Example 6.4.2. (1) 回顾我们在例6.2.9中定义的任意集合X上的等价关系。这是一个等价关系。当然，$(x, x) \in R$，因为$x = x$。然而，对于任何$x \neq y$，假设$x \, R \, y$是错误的，这使得条件语句为真。因此，对称性质中的唯一“相关情况”是$x = y$，在这种情况下，是的，$y = x$也是。同样，对于传递性质，如果$x \neq y$或$y \neq z$，定义条件语句的假设是错误的，因此该语句本身为真；当$x = y$和$y = z$时，是的，当然$x = z$。这可能看起来不是一个特别有启发性的发展，但知道我们总可以在any集合上定义至少一个等价关系，is感觉很好。

(2) 在 $\mathbb{Z}$ 上的“除以”关系是 **not** 一个等价关系，因为它不是对称的。

(参见示例6.2.16。)

(3) 在一个（非空）人群集合上的“严格小于关系”是**not**一个等价关系，因为它不是自反的。

(参见示例6.2.17。)

(4) 在 $\mathbb{Z}$ 上通过以下方式定义的 R 关系

$$\forall x, y \in \mathbb{Z}\textbf{.}\ x \star y \iff 3 \mid x - y$$

is 一个等价关系，因为它具有自反性、对称性和传递性。

(参见第6.2.5节中的练习2。)

这个特定等价关系的例子将在本章后面详细讨论并推广。你甚至可能已经认出它就是“模3等价”关系！

许多本章的练习将采取以下形式：“判断这个定义是否产生一个等价关系。”这些类似于我们之前见过的形式为“证明/反驳以下命题”的问题。我们需要（以某种方式）弄清楚我们认为给定的关系实际上是否是等价关系；如果是，我们需要证明这一点；如果不是，我们需要确定哪个性质失败，并给出一个反例来证明这一点。让我们看一个例子来说明这个想法。

Example 6.4.3. 设 $S = \mathbb{N} - \{1\}$ 并定义 $(x, y) \in R \iff x$ 和 y 有一个公因数（即 *not* 1，即严格大于 1）。让我们通过 *trying* 来证明它是一个等价关系，并看看论点是否在任何地方失效。如果没有失效，那么我们就成功了，如果失效了，那么我们可以利用这个知识来构造一个反例。

首先，我们注意到 $(x, x) \in R$，因为x和x有一个公因数，x。此外，根据S的定义，我们有$x > 1$，因此R是自反的。其次，我们注意到如果 $(x, y) \in R$，那么x和y有一个公因数，某个$k > 1$。然后，当然，交换这对字母不会改变这个事实：y和x有一个公因数$k > 1$，因此 $(y, x) \in R$，同样，R是对称的。

第三，假设$(x, y) \in R$和$(y, z) \in R$。这意味着x和y有一个公因数，称为$k > 1$，而y和z有一个公因数$\ell > 1$。我们能用这个来找到x和z的公因数吗？不一定，似乎...我们无法确定k和ℓ有公因数，例如。如果$k = 2$和$\ell = 3$呢？我们能识别出一些x, y, z的值，以实现这些公因数，然后验证x和z没有公因数吗？当然，让我们考虑$x = 2$和$y = 6$以及$z = 9$。那么$(2, 6) \in R$和$(6, 9) \in R$，但$(2, 9) \notin R$。这是一个反例，表明这个关系的传递性是False，因此它不是一个等价关系。

我们推荐这种方法来识别给定的关系是否是等价关系或有序关系。只需逐一检查相关的属性——自反性、对称性、传递性，以及其他你可能考虑的任何属性——以及 **try to prove them**。如果你成功了，那就行了！如果你在证明其中之一时遇到困难，请利用你的努力来识别问题，并看看为什么该属性失败。用这个来构造该属性的逆例。

Motivation

再次考虑我们在本节中提到的第一个例子，其中 $x\,R\,y \iff \lfloor x \rfloor = \lfloor y \rfloor$。注意，每个实数都与一个整数相关联，具体来说，是与通过 *rounding down* 得到的整数相关联。例如，$1.5\,R\,1$ 和 $\pi\,R\,3$ 和 $-1.5\,R\,{-2}$。此外，任何与同一整数相关联的两个实数都与 *each other* 相关。例如，$3.5\,R\,3$ 和 $\pi\,R\,3$，和 $3.5\,R\,\pi$。由于这些观察结果，我们声称我们可以将满足 $0 \leq x < 1$ 的所有实数“打包”成一个“簇”，并用该簇的单个元素来表示它们，比如说 0。同样，我们可以将满足 $1 \leq x < 2$ 的所有实数打包成一个由 1 表示的“簇”。依此类推。我们没有 *have* 选择 0 和 1 作为代表元素。我们完全可以选择 $\frac{1}{2}$ 和 $\frac{3}{2}$，例如。但关键是那些实数“簇”都在同一个簇内，我们可以用其中一个 **representative** 元素来表示每个这样的簇。

这个观察将直接带我们进入下一节，我们将讨论如何正式描述这些“簇”。这些被称为 **equivalence classes**。然后我们将研究许多例子并确定一些一般性质。

在这样做之前，我们强烈建议您尝试一些我们已经看到的示例，寻找这些类型的“簇”和“代表”。例如，考虑由以下公式定义在 $\mathbb{Z}$ 上的关系 R:

$$\forall x, y \in \mathbb{Z}\mathbf{.}\ x \star y \iff 3 \mid x - y$$

这是一个等价关系。在这种情况下，“簇”是什么？你能识别出所有这些簇吗？每个簇中有多少个元素？你能选择代表吗?

尝试用另一个等价关系做同样的工作，比如在你班级学生集合上的“在同月出生”关系。（这确实是一个等价关系，你稍加思考就会意识到。）

一个同样有教育意义的任务是考虑一个 **non**-等价关系，并试图弄清楚 *why/how* 它不具有这种“簇”属性。例如，考虑 $\mathbb{Z}$ 上的“整除”关系。它在何处不具有这种属性？它是否“接近”具有这种属性?

本质上，做一些探索！这真的有助于巩固你对关系属性的掌握，并使下一节更容易理解。

6.4.2 Equivalence Classes

Definition

设我们在集合 A 上有一个等价关系 R。我们做出以下定义的原因在上一段中有所暗示。这三个性质——自反性、对称性和传递性——共同构成了集合 A 的典范 *partition*。任何相互关联的元素形成一种“封闭俱乐部”或“簇”，这使得我们可以将“俱乐部”中的任何一个元素作为代表，而不是所有元素。这些“俱乐部”被称为 *equivalence classes*，这一思想在以下定义中得到了探讨。

Definition 6.4.4. *Let R be an equivalence relation on the set A, and let $x \in A$. The* **equivalence class of** *x (under the relation R) is the set of all elements related to x and is denoted by $[x]_R$. That is,*

$$[x]_R = \{y \in A \mid (x, y) \in R\}$$

Motivation and Examples

这个定义背后的思想是，等价类允许我们将集合 A **partition** 到一些基于关系 R 的规范集合中。回顾第3章中的定义3.6.9，以了解我们是如何定义集合的 **partition** 的。（实际上，还可以看看定义4.5.11，以了解我们是如何使用逻辑符号重述该定义的。）现在，只需记住，一个划分是非空集合的集合，这些集合两两不相交，并且它们的并集是所讨论的整个集合。

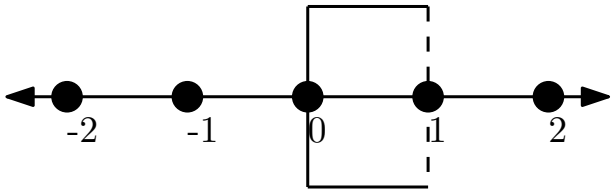
Example 6.4.5. 让我们回到本节最初的激励示例。我们通过以下方式在 $\mathbb{R}$ 上定义关系 R:

$$\forall x, y \in \mathbb{R}\text{.}\ (x, y) \in R \iff \lfloor x \rfloor = \lfloor y \rfloor$$

让我们考虑一个特定的等价类，使用我们刚才定义的。具体来说，让我们考虑

$$\begin{aligned}[0]_R &= \{y \in \mathbb{R} \mid (0, y) \in R\} = \{y \in \mathbb{R} \mid \lfloor 0 \rfloor = \lfloor y \rfloor\} = \{y \in \mathbb{R} \mid \lfloor y \rfloor = 0\} \\ &= \{y \in \mathbb{R} \mid 0 \le y < 1\}\end{aligned}$$

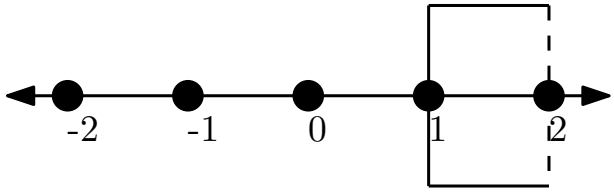
通过使用上面定义的$[0]_R$，R的定义以及一些关于$\lfloor y \rfloor$含义的知识，我们已确定 *equivalence class of 0 under the relation R*是这个特定区间，介于0（包含）和1（不包含）。我们可以这样想象这个区间:



同样，我们可能会发现

$$[1]_R = \{y \in \mathbb{R} \mid (1, y) \in R\} = \{y \in \mathbb{R} \mid 1 \leq y < 2\}$$

并且图片设置为这样：



注意这两个集合是互斥的（它们不重叠），因为第一个集合不包含1作为元素，但第二个集合包含。此外，注意实数 *every* 属于 *exactly one* 区间，如下所示。例如，我们可以这样说

$$\pi \in [3]_R,\ \mathrm{e} \in [2]_R,\ -1.5 \in [-2]_R,\ \frac{1}{2} \in [0]_R$$

然而，请注意，*equivalence class*的定义并没有说明我们必须恰好使用一个元素来*represent*那个类别。例如，我们可以说

$$[0]_R = \left[\frac{1}{2}\right]_R$$

因为这两个集合相等；它们包含相同的元素，因为任何“地板”为0的实数与0相关（在R下），因此也在R (下与$\frac{1}{2}$相关，因为*its*的“地板”也是0)。

再玩玩这个例子，并试图说服自己这个划分性质在这里真的有效。在下一部分，我们将正式以完全的普遍性 *prove* 这个事实，在你的帮助下！因为这将是一个相当抽象的讨论，我们鼓励你亲自处理像这样的实际例子。尝试在另一个集合上定义一个等价关系。它的等价类是什么？你看到为什么它们形成一个划分了吗?

Equivalence Classes Partition the Set

现在我们已经探讨了等价类 *partition* 是一个集合的想法，让我们将这个想法形式化。我们需要定义一个概念，然后我们可以证明一个定理！这个定理本质上是一个“当且仅当”风格的定理，我们将证明一个方向，将另一个方向留给你们作为练习。

Definition 6.4.6. *Let R be an equivalence relation on the set A. The set of equivalence classes (under R), denoted by A/R, is A* **modulo** *R. That is,*

$$A/R = \{[x]_R \mid x \in A\}$$

Equivalently,

$$A/R = \{X \subseteq A \mid \exists x \in A.\ X = [x]_R\}$$

让我们看看几个例子，在证明一个重要结果之前，先掌握这些概念。在每个例子中，让我们说服自己我们有一个等价关系，检查等价类，并思考*modulo*操作的作用。

Example 6.4.7. 再次考虑由 $(x, y) \in R \iff \lfloor x \rfloor = \lfloor y \rfloor$ 在 $\mathbb{R}$ 上定义的关系 R。我们之前讨论了为什么这是一个等价关系，所以让我们来考察等价类。

任何两个相关元素具有相同的等价类，这是定义。例如，$[0]_R = [0.5]_R = [0.999]_R$。同样，$[3.5]_R = [3.75]_R$，以及 $[-\pi]_R = [-4]_R$，但 $[\pi]_R \neq [4]_R$。每个实数 $x \in \mathbb{R}$ 都有一个相关的等价类，$[x]_R$，但操作的想法是通过只考虑必要的等价类来减少集合 $\mathbb{R}$。由于 $[0]_R = [0.5]_R = [0.333]_R$ 等等，我们可以用一组表示所有这些相同的集合，即 $[0]_R$。因此，我们可以说

$$\mathbb{R}/R = \{\dots, [-2]_R, [-1]_R, [0]_R, [1]_R, [2]_R, \dots\}$$

本质上，因此，$\mathbb{R}/R$“是”整数集$\mathbb{Z}$。然而，我们实际上只感到舒适地写出 $\mathbb{R}/R$“=”$\mathbb{Z}$，因为这个等式并不是*exact*。特别是，我们还没有严格推导出实数或整数，只有$\mathbb{N}$。在这里，我们只是观察到在这种关系下的等价类集合与整数集合之间的一种“对应”关系。我们可以将它们相互识别，反之亦然，但这并不意味着它们是*equal*，从技术上来说。

无论！这个例子的全部目的只是指出 $\mathbb{R}/R$ 是等价类的 *set*。记住，当我们写下一个集合时，*order* 和 *repetition* 是无关的。也就是说，$\{1, 3, 5, 3, 1\} = \{1, 3, 5\}$ 在集合的意义上。它们有 *same elements*，所以它们是 *same object*。在当前上下文中，我们不需要在我们的集合 $\mathbb{R}/R$ 中包含 *both* $[0]_R$ 和 $[0.5]_R$，因为它们是同一件事；我们会在我们的元素列表中包含那个 *repeating* 对象，但这不会起任何作用。

一般来说，我们将关注的是识别等价类“看起来”如何，并对它们进行一些定性描述。特别是，我们经常会想知道在A/R中有多少个*many*等价类。我们也会想知道这些类是如何分布的。它们是否都是相同的大小？有些类是否只有几个元素，而其他类是无限大的？为什么或为什么不呢？这些类是否都有大致相同的元素“描述”？

在这个特定例子中，我们发现$\mathbb{R}/R$中的所有等价类在形式上都非常相似。有无限多个类——每个类对应$\mathbb{Z}$中的一个元素——并且它们都是无限大的——包含一个实数区间。此外，所有类都具有形式 $[z]_R = \{y \in \mathbb{R} \mid z \leq y < z + 1\}$，其中包含某个$z \in \mathbb{Z}$。从这个意义上说，这些等价类都是*qualitatively similar*。

Example 6.4.8. 在所有人的集合 S 上定义关系 B，通过说 $(x, y) \in B \iff x$ 和 y 出生在同一个月。然后，例如 (Leonhard Euler,Henri Poincaré) $\in B$ 和 (Paul Erdös ,Emmy Noether) $\in B$。为什么这是

一个等价关系？嗯，任何人与自己有相同的出生月份（自反性），如果任何两个人有相同的出生月份，那么他们 . . . (duh) 有相同的出生月份（对称性），并且如果 x 和 y 有相同的出生月份，而 y 与 z 有相同的月份，那么 x 和 z 也有相同的出生月份（传递性）。

（注意：一般来说，由“具有相同的 . . .”或“是相同的 . . .”定义的关系将是一个等价关系。）

等价类对应于月份！由于我们是通过出生月份来描述人们的，等价类是一组所有同月出生的人。例如，保罗·埃尔德什和艾米·诺特∈都出生在三月，因此我们可以说艾米·诺特·[保罗·埃尔德什$_B$]。这个等价类*corresponds*对应于三月，但请注意，它是在所有人群集合S (的特定元素)的基础上定义的。

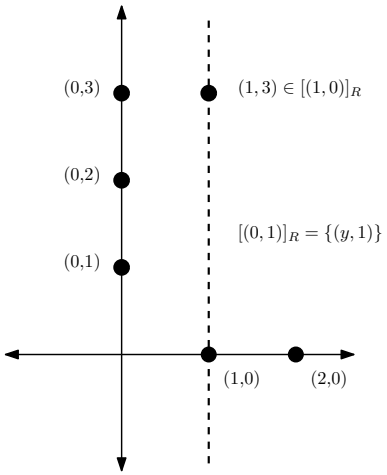
如果我们定义 M 为所有在三月出生的人的集合，那么我们可以说 $M =$ [保罗·埃尔德什]$_B$。将这些观察结果综合起来，我们可以这样说：按出生月份取模的人的集合，记为 S/B，由12个集合组成，每个集合对应一个不同的月份，并包含该月出生的所有人。

Example 6.4.9. 考虑所有实数有序对的集合 $\mathbb{R} \times \mathbb{R}$。我们通过声明 *two pairs* 何时相关来在 $\mathbb{R}\times\mathbb{R}$ 上定义一个关系 R。具体来说，让我们说

$$((x, y), (u, v)) \in R \iff x = u$$

这意味着，在平面上，当两对点的第一个坐标相同时，它们在 R 下是相关的。想想为什么这是一个等价关系：从几何学的角度来看，这个关系只关心一个点所在的与 y-轴平行的垂直线。有了这个想法，你可以很容易地“看到”并解释为什么 R 是一个等价关系，而严格证明只需要稍微多写一些文字和符号。（试试看！）

这也使我们能够轻松描述和可视化这个关系下的等价类。所有位于同一条垂直线上的点都被打包成一个等价类，我们只需观察这条线与水平轴的交点即可索引（即跟踪）这些类。也就是说，例如，$(1, 3) \in [(1, 0)]_R$，因为点 $(1, 3)$ 和 $(1, 0)$ 位于同一条垂直线上。我们可以这样写 *every* 等价类，$[(x, 0)]_R$，对于某个 $x \in \mathbb{R}$。

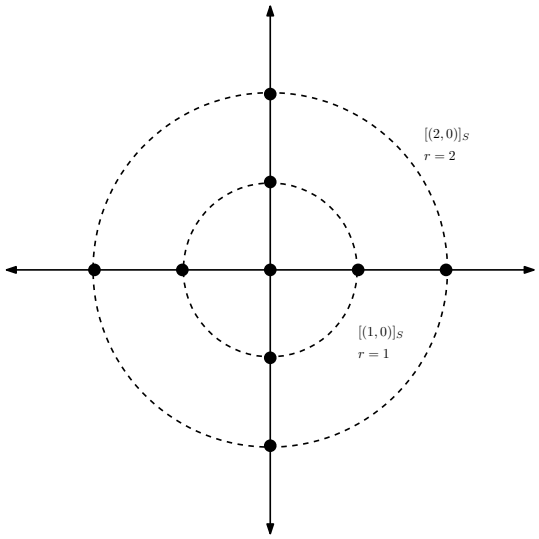


因此，等价类集合（$\mathbb{R}\times\mathbb{R}$）$/R$在某种意义上与实数线$\mathbb{R}$“相同”！我们只需忽略它们的第二个坐标，就可以将平面的所有点压缩到水平轴上。从数学的角度来说，有一种方法可以使这个想法更加精确，但在这个背景下我们无法真正正式地讨论它。只需说，这里确实有一些有趣的事情发生，即这个在$\mathbb{R}\times\mathbb{R}$上的关系产生了由$\mathbb{R}$表示的等价类。

这里是在 $\mathbb{R}\times\mathbb{R}$ 上的另一个关系。通过设置定义 S:

$$((x,y),(u,v)) \in S \iff \sqrt{x^2+y^2} = \sqrt{u^2+v^2}$$

记住一些基本的几何和代数知识，你可能认出表达式 $\sqrt{x^2+y^2}$ 描述了从点 (x, y) 到原点（$0, 0$）的 $distance$。（在数学中，我们称这样的表达式为 $metric$。）因此，这个关系表明，当两个点与原点的距离相同时，它们是相关的。直观上，这解释了为什么 S 是一个等价关系，and 它向我们展示了等价类是以原点为中心的圆！因此，我们可以通过仅表示这些圆的一个显著特征来描述集合 ($\mathbb{R}\times\mathbb{R}$)$/S$ 的元素：它们的 $radius$，某个实数 $r \geq 0$。相应地，在 S 下，等价类的集合“相同”于非负实数集合！



这是一个相当奇怪的想法，对吧？我们从二维集合和相关点对开始，整理了等价类，最终得到了一维集合。（注意：我们在这里没有正式定义*dimension*的方法，但我们认为你对我们所说的有直观理解。）回顾上面定义在$\mathbb{R}^2$上的关系R。如果我们只在那“右半部分”定义这个关系，即所有第一坐标非负的点，那么等价类集合*also*将与非负实数集合“相同”。这个集合在什么意义上会与$(\mathbb{R} \times \mathbb{R})/S$“相同”？这甚至是一个合理的问题吗？我们如何*prove*这样的陈述？这些都是非常有趣的问题，我们鼓励你思考！

不要被这些概念和广泛的问题分散注意力，尽管如此。更大的观点是：等价类集合构成了底层集合的 **partition**。

现在我们已经看到了几个例子，让我们陈述（并证明！）一些关于等价关系的重要结果。主要，这些定理提出了我们一直在用言语暗示的想法，即一个等价关系 *partitions* 将一个集合划分为其对应的等价类。然而，也许有些令人惊讶的是，我们还有一个很好的结果，它说我们可以反过来做这个过程：给定任何划分，我们可以为它定义一个等价关系！

Theorem 6.4.10. *Let R be an equivalence relation on the set A. Then the sets belonging to A/R form a partition of A. That is, they are nonempty, they are pairwise disjoint, and their union is A.*

Proof. 查看练习6.7.13！ □

我们将引导您通过本章末尾的练习6.7.13中的这个结果证明。我们已检查的示例应该已经给了您

直观理解这个定理为什么成立，但通过证明细节的工作将使你对背后的数学严谨性有更深入的理解。

A Partition Yields an Equivalence Relation

现在，让我们继续前进，看看一个类似且重要的结果，它是前一个定理的逆命题。为了熟悉它，我们首先将研究一个例子，这也会给我们提供一个定理证明的草图。

Example 6.4.11. 考虑集合 $S = [6]$。定义集合的集合

$$\mathcal{F} = \{\, \{1,4\}\, \{2,3,5\}\, , \{6\}\, \}$$

注意，$\mathcal{F}$ 是 S 的一个划分，因为集合是互斥的，没有一个为空，它们的并集是 S。如果存在某种等价关系 R，当我们考虑 S/R 时能产生这些集合，那岂不是很好？结果证明确实存在！当然，我们可能无法以我们迄今为止所见到的那些方式，比如通常定义为“$(x, y) \in R \iff x$ 和 y 具有某些共同属性”的关系，来优雅地 *define* 它。然而，手头已经有了划分，这使我们能够定义关系 *in terms of the partition*。具体来说，划分集合 *are* 等价类。划分本身构建了等价类结构，我们只需通过说 $(x, y) \in R \iff x$ 和 y 属于同一个划分集合来定义一个等价关系 R。

在这个例子中，我们将定义 $S_1 = \{1, 4\}$ 和 $S_2 = \{2, 3, 5\}$ 以及 $S_3 = \{6\}$。然后，我们通过以下方式定义关系 R:

$$(x, y) \in R \iff \exists i \in [3]\,\boldsymbol{.}\; (x \in S_i \wedge y \in S_i)$$

考虑为什么这行得通。你看到为什么这是一个等价关系吗？你看到等价类是什么吗？

现在我们准备好陈述定理并证明它。

Theorem 6.4.12. *Let S be a set and let $\mathcal{F}$ be a partition of S. Then there exists an equivalence relation R such that $S/R = \mathcal{F}$.*

我们上面暗示过，这个结果完全取决于这样一个事实：一个划分是一组集合，这些集合是我们要定义的等价类 *precisely*。我们只需要证明关系“x 和 y 如果且仅如果它们属于同一个划分集合则它们是相关的”是一个等价关系。这并不太难！在阅读我们的版本之前，试着勾勒出证明的细节！

Proof. 设 $\mathcal{F}$ 是 S 的一个划分。这意味着我们有一个指标集 I，并且

$$\mathcal{F} = \{S_i \mid i \in I\}$$

在集合 S_i 满足 $S_i \subseteq S$ 和 $S_i \neq \varnothing$ 的条件下

$$\bigcup_{i \in I} S_i = S \qquad \text{and} \qquad \forall i, j \in I\,\boldsymbol{.}\; i \neq j \implies S_i \cap S_j = \varnothing$$

让我们通过以下方式定义 R 与 S 上的关系 {v*}：

$$(x, y) \in R \iff \exists i \in I \,.\, \big(x \in S_i \wedge y \in S_i\big)$$

我们现在将证明 R 是一个等价关系。

- 设 $x \in S$ 为任意且固定的。由于集合 S_i 覆盖 S，我们知道 $\exists i \in I$。
- 设 $x, y \in S$ 为任意且固定的。假设 $(x, y) \in R$。这意味着 $\exists i \in I$ $\big(x \in S_i \wedge y \in S_i\big)$。让这样的 i 给定。
- 设 $x, y, z \in S$ 为任意且固定的。假设 (x, y) 和 $(y, z) \in R$。这意味着 $\exists i \in I$ $\big(x \in S_i \wedge y \in S_i\big)$ 和 $\exists j \in I$ $\big(y \in S_j \wedge z \in S_j\big)$。让这样的 i, j 给定。

  注意 $y \in S_i \wedge y \in S_j$。由于 $S_i \cap S_j = \varnothing$ 对于任何 *distinct* i, j，必须 $i = j$。（否则，$y \in \varnothing$，这是不可能的！）

  因此 $x \in S_i$ 和 $y \in S_i$ 和 $z \in S_i$。因此，$(x, z) \in R$。

  Therefore, R is transitive.

Certainly, then, we have $x \in S_i \wedge x \in S_i$, thus $(x, x) \in R$ as well. Therefore, R is reflexive.

Certainly, then, we have $y \in S_i \wedge x \in S_i$, thus $(y, x) \in R$ as well. Therefore, R is symmetric.

Notice that $y \in S_i \wedge y \in S_j$. Since $S_i \cap S_j = \varnothing$ for any *distinct* i, j, it must be that $i = j$. (Otherwise, $y \in \varnothing$, which is impossible!)

Accordingly $x \in S_i$ and $y \in S_i$ and $z \in S_i$. Thus, $(x, z) \in R$.

Therefore, R is transitive.

由于所有三个性质都成立，R 是一个等价关系！

S 模 R、S/R 的等价类形式为 $[x]_R$，其中 $x \in S$。由于 $\mathcal{F}$ 是 S 的一个划分，$x \in S_i$ 对于某些 i。因此，对于某些 i，有 $[x]_R = S_i$。因此，所有等价类都等于某个集合 S_i。

同样，任何集合 $S_i \neq \varnothing$，因此 $\exists x \in S_i$，从而存在一个相应的等价类 $S_i = [x]_R$。因此，每个等价类都是形式为 S_i 的集合，反之亦然。

□

这表明任何划分都很好地对应于一个等价关系，以及它的类！

6.4.3 More Examples

现在我们手头有了这两个定理，让我们来处理一些关系的例子。对于每一个，我们将尝试确定它是否是等价关系。如果是，我们可以描述它的等价类。如果不是，我们可以尝试调用其中一个定理，看看*why*它不是。

Example 6.4.13. 让我们从简单的开始。回顾一下我们在例6.2.9中定义的等价关系。我们已经解释过，“=”是任何集合上的等价关系。具体来说，它将集合划分为等价类，这些等价类就是...，集合本身的元素！也就是说，在

集合 $\mathbb{N}$，例如，$[1]_= = \{1\}$ 和 $[2]_= = \{2\}$，以此类推。等价类都是每个元素为 *singletons* (的) 集合。

Example 6.4.14. 让我们再做一个相当简单的例子。回顾一下我们在例6.2.5中定义的$\mathbb{Z}$上的奇偶关系。它是一个等价关系，所以现在我们来证明这一点。

Proof. 让 $a, b, c \in \mathbb{Z}$ 为任意值。

首先，注意因为 a 与自身具有相同的奇偶性，所以 $(a, a) \in R$。因此，R 是自反的。

其次，假设$(a, b) \in R$，因此 a 和 b 具有相同的奇偶性；当然，那么，b 和 a 也具有相同的奇偶性，所以 $(b, a) \in R$。因此，R 是对称的。

第三，假设$(a, b) \in R$和$(b, c) \in R$。如果a是奇数，我们可以推断b是奇数，然后c是奇数；同样地，如果a是偶数，我们可以推断b是偶数，然后c是偶数。在任何情况下，a和c具有相同的奇偶性，所以$(a, c) \in R$必然成立。因此，R是传递的。

由于 R 是自反的、对称的和传递的，R 是一个等价关系。 □

这意味着等价类集 $\mathbb{Z}/R$ 形成了 $\mathbb{Z}$ 的一个划分。让我们确定那个划分。

考虑$[0]_R$。这是与0相关的所有整数的集合，即与0具有相同奇偶性的整数的集合，即所有*even*整数。因此，在这种情况下

$$\mathbb{Z}/R = \{O_{\mathbb{Z}}, E_{\mathbb{Z}}\}$$

$O_{\mathbb{Z}}$ 是奇数集，$E_{\mathbb{Z}}$ 是偶数集。存在两个等价类，每个都是无限大的。

Example 6.4.15. 回顾我们在例6.2.6中定义在 $\mathbb{R}$ 上的顺序关系。这是一个等价关系吗？为了弄清楚这一点，我们可以检查定义中的每个属性。注意，无论 $x \in \mathbb{R}$ 是什么，我们都有 $(x, x) \notin R$ 因为 $x \not< x$。因此，R 不是自反的，因此不是等价关系。（同时，R 也不是对称的，但它 *is* 是传递的。）

为什么这个严格的顺序关系不会是一个等价关系是有意义的？为什么我们希望等价关系是自反的？考虑一下*equivalence class*的概念；等价关系应该将整个集合的元素放入一个划分中，我们可以通过属于它的任何一个元素来识别任何划分集合。对于一个非自反的关系，我们就会有某些不属于“等价类”*their own*的元素，这肯定是一个不希望出现的情况！

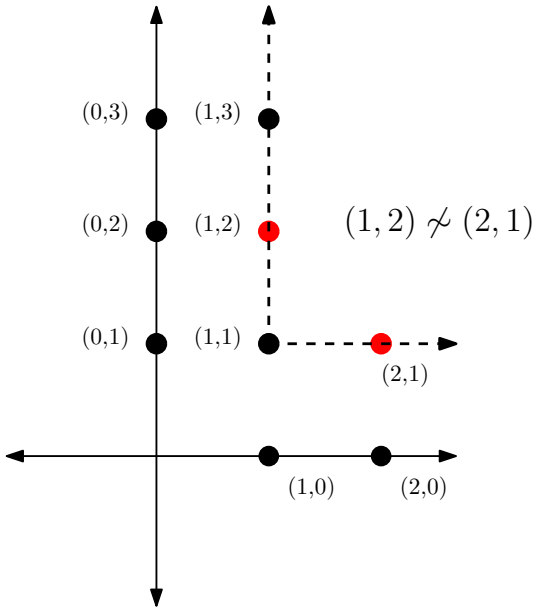
(后续问题：关于顺序关系 $\leq$，它是自反的；这是一个等价关系吗？为什么或为什么不？)

另一种说法是，我们可以看到在 $\mathbb{R}$ 上的关系 “$<$” 并没有将实数分成一个划分。正因为如此，考虑到定理 6.4.10 的 *contrapositive*，我们得出结论，“$<$” *cannot* 是一个等价关系。

Example 6.4.16. 在 $\mathbb{R} \times \mathbb{R}$ 上定义关系 $\sim$ 如下

$$(x, y) \sim (u, v) \iff x \leq u \wedge y \leq v$$

未检查其属性，让我们看看我们能否确定它是否是一个等价关系。为此，让我们取集合的一个特定元素，并查看与该特定元素相关的所有元素。对于下面的图，我们将使用（1, 1）作为特定元素。



注意，∼的定义条件要求一个点位于另一个点的“上方和右侧”，这两个点才相关。另外，不等式是“≤”，所以第二个点不必在*strictly*的上方或右侧。

因此，（1, 2）∼ (1, 1)，如图所示（同时观察到$1 \leq 1 \wedge 1 \leq 2$）。此外，（1, 1）∼ (2, 1)，原因类似。相应地，点（1, 2）和（2, 1）都与（1, 1）相关，因此，为了使这种关系∼成为一个*equivalence*关系，我们需要*would*要求（2, 1）和（1, 2）*to each other*相关。这是因为它们都必须属于（1, 1）的“等价类”。然而，请注意（1, 2）$\not\sim$ (2, 1)，遗憾的是！第二个点严格位于第一个点的“下方和左侧”，因此它不满足∼的定义条件。

这意味着与（1, 1）相关的所有元素构成一个“封闭俱乐部”。从数学的角度讲，这个元素集不是一个等价类。因此，∼不是一个等价关系。

现在，尝试确定 ∼ 具有哪些属性以及不具有哪些属性。它是自反的？对称的？传递的？为什么是或不是？通过这样做，你将再次证明 ∼ 不是一个等价关系。不是已经很有帮助了吗？

提前想出它 *isn't* 吗？通常情况下，当你面对一个定义好的关系时，我们建议做一些类似的事情。你能想出“等价类”可能是什么吗？如果是这样，那么你已经对关系为何是等价关系以及为什么是等价关系有了某种直觉，这将有助于你描述等价类。如果不是这样，那么你已经对如何反驳这种说法有了某种直觉。

[Optional Reading] How $\mathbb{Z}$ comes from an Equivalence Relation on $\mathbb{N} \times \mathbb{N}$

记住第三章中那个让你证明关于自然数对对集的某个性质的那个疯狂练习，我们声称这是在证明关于整数存在性的某个性质？那究竟是怎么回事？现在回顾一下练习，练习3.11.22。你会发现问题的最后三部分要求你证明我们定义的集合R是集合P上的一个**equivalence relation**。（基础集合是$P = \mathbb{N} \times \mathbb{N}$。）看吧！你证明了$R$是自反的、对称的和传递的。

那项练习表明的是（本质上，我们在这里省略了一些细节）任何负整数都可以表示为差为该负整数的整数对的 **equivalence class**。也就是说，

$$-1 \text{ “}=\text{”} [(1,2)]_R = \{(1,2),(2,3),(3,4),\dots\}$$

并且，另一个例子，

$$-3 \text{ “}=\text{”} [(1,4)]_R = \{(1,4),(2,5),(3,6),\dots\}$$

这是一个直观的解释，而不是严格的，从数学的角度来说，但这才是主要思想！

6.4.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 一个 *equivalence relation* 需要满足哪些性质?

(2) 等价类是什么？一个等价类中的所有元素必须满足什么条件?

(3) 给定一个集合 S 和在 S 上的一个等价关系 R，等价类的集合中必须满足什么条件?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 回顾第6.2.5节中练习2中定义的关系。在那里，我们通过设置 $\star$ 在 $\mathbb{Z}$ 上定义关系

$$\forall x, y \in \mathbb{Z}\text{.}\ x \star y \iff 3 \mid x - y$$

你已经在那里证明了它确实是一个等价关系。

现在，描述 $\mathbb{Z}/\star$ 中的等价类。有多少个？它们“多大”？你能列出它们的元素或以某种方式描述它们吗？

(2) 回顾第6.2.5节中练习3中定义的关系。在那里，我们通过以下方式在$\mathbb{Z}$上定义了关系$\sim$：

$$\forall x, y \in \mathbb{Z}\text{.}\ x \sim y \iff 3 \mid x + 2y$$

你已经在那里证明了它确实是一个等价关系。

现在，识别并描述 $\mathbb{Z}/\sim$ 中的等价类。有多少个？它们有多大？你能列出它们的元素或以某种方式描述它们吗？

与之前的练习相比。你注意到什么了？

(3) 考虑集合 $[5] = \{1, 2, 3, 4, 5\}$。定义关系 $\approx$ 在 $[5]$ 上，对于任意的 $x, y \in [5]$

$$x \approx y \iff |x^2 - y^2| \leq 5$$

对于每个 $x \in [5]$，令 $S(x)$ 为所有满足 $x \approx y$ 的元素 $y \in [5]$ 的集合。

(a) 将集合 $S(1), S(2), S(3), S(4), S(5)$ 的所有元素写出来。 (b) 你能否通过观察这些集合来确定 $\approx$ 是否是等价关系？如何？ (c) 通过证明/反证反身性、对称性和/或传递性来证明 $\approx$ 是否是等价关系。

(4) 考虑集合 $\mathbb{N} \times \mathbb{N}$。通过设定关系 $\sim$ 在此集合上定义为

$$(a, b) \sim (c, d) \iff a + b = c + d$$

确定这是否是一个等价关系。如果是，请用图形方式描述其等价类。

6.5 Modular Arithmetic

一个自然且常见的等价关系，你可能已经见过并使用过，就是 *congruence*，在整数的情况下。这是“偶数/奇数奇偶性”等价关系的直接推广，它根据一个特定的属性对整数进行分类。在这里，我们通过定义一些整数的属性，然后定义一系列关系来扩展这个想法。我们还将通过一些有趣的结果，这些结果通过使用这些关系变得容易证明（或者根本可证明！）

6.5.1 Definition and Examples

Divisibility

我们将从一个我们已经见过几次的定义开始。

Definition 6.5.1. *Let $a, b \in \mathbb{Z}$. We say that a* **divides** *b if b is evenly divisible by a, i.e. $\exists k \in \mathbb{Z}$ such that $b = ak$, or equivalently, $\frac{b}{a} \in \mathbb{Z}$ (except for the case where $a = b = 0$). We denote this by $a \mid b$.*

注意，这个定义说明每个整数都能整除0（例如，$5 \mid 0$），但0除了自身外不能整除任何数（例如，$0 \nmid 5$但$0 \mid 0$）。思考一下这与你对“整除”的直观理解如何相符，以及它如何满足给定的定义。此外，注意这里也考虑了负数，因为存在量词接受一个 *integer* $k \in \mathbb{Z}$。因此，$-2 \mid 4$和$8 \mid -24$也是如此。

现在，一个像$2 \nmid 5$这样的陈述告诉我们一些关于整数2和5之间关系的信息，但它并没有说出所有内容。我们知道存在一个可能的整数 *no* 满足$2k = 5$，但它没有说明我们如何 *close* 得到。当然 $k = -100$是一个糟糕的估计，但$2 \cdot 2 = 4$和$2 \cdot 3 = 6$相当接近5 . . . 对于这样的小数，我们可以手动检查，这似乎很明显，但关于大数呢？我们知道$7 \nmid 100000$（为什么？想想素数 . . . ），但我们如何解决这个问题“找到一个 k 使得$7k$ 尽可能接近100000”？我们如何知道甚至有一个特定的答案？可能存在两个同样“合理”的答案，就像$2 \nmid 5$一样？

关于第二个问题，关于复数，我们希望限制自己，只保留一个合理的答案。这源于对简单的渴望，不需要在找到一个答案后还担心找到另一个答案。因此，我们将遵循*The Price Is Right*标准：我们希望得到*closest*答案，而不需要 *going over*。以示例$2 \nmid 5$为例，我们认为$k = 2$是最好的估计，因为$4 < 5$。同样，以示例$7 \nmid 100000$为例，我们认为$k = 14285$是最好的估计，因为$7 \cdot 14285 = 99995$。（注意，在这种情况下，有一个“更接近”的估计超过了，但我们不考虑它。）

这现在激励了如何得出这样的估计。给定 $a, b \in \mathbb{Z}$，我们只需查看 a 的越来越大倍数，直到我们走得太远，超过 b；在那之前的倍数将是最好的。估计的“准确性”

必须介于0和a −1之间的某个数量，其中0表示$a \mid b$实际上为真。（注意：“走得太远”的概念是>的顺序关系，因此请仔细思考这如何应用于负整数。例如，$2 \nmid -3$和$2 \cdot -2 = -4$被认为是最佳估计，因为$-4 \leq -3$。）以下引理封装了这些迭代查看a的倍数以找到b的最佳估计的想法，并声明在所同意的约束下，始终存在唯一解。

Lemma 6.5.2 (除法算法)**.** *Let $a, b \in \mathbb{Z}$. Then $\exists!\ k, r \in \mathbb{Z}$ such that $ak + r = b$ and such that $0 \leq r \leq a - 1$. Said another way, given any two integers, there is always a unique multiple of a that is closest to b without being greater, and there is a corresponding unique remainder. We call this r the "remainder of b upon division by a" or "the remainder when b is divided by a".*

这是从该结果中我们将最频繁使用的 *remainder* 的概念。具体来说，我们将比较两个除法的余数，并基于这些余数定义一个关系。我们很快就会看到这些细节。首先，我们希望您证明这个重要的引理！

Proof. 作为练习6.7.14留给读者。 □

这个被称为除法 *Algorithm* 的原因是因为存在一个隐含的 *process*，通过它可以实际上 *find* 这些倍数和余数。这种方法虽然简单但足够有效，*repeated subtraction*。也就是说，给定 a 和 b，我们只需不断从 b 中减去 a——找到 $b - a$ 然后是 $2a$，然后是 $b - 3a$，然后是……——直到我们剩下介于 0 和 a 之间的余数。

Example 6.5.3. 让我们看看这个过程是如何进行的，只是为了展示这个想法。让我们使用 $a = 8$ 和 $b = 62$。我们不断地从 62 中减去 8，找到

$$62,\ 54,\ 46,\ 38,\ 30,\ 22,\ 14,\ 6$$

我们在6处停止，因为它满足$0 \leq 6 < a = 8$。这告诉我们 $r = 6$。我们还注意到，我们从 b 中减去了 a 七次，因为我们的列表中有八个项，第一个项只是 $b - 0 \cdot a$。因此，我们可以写出

$$\underbrace{62}_{b} = \underbrace{7}_{k} \cdot \underbrace{8}_{a} + \underbrace{6}_{r}$$

这里的主要观点是存在一种方法 *exists* 找到这个余数，并且它是唯一的。有了这个结果在手，让我们用它来定义 $\mathbb{Z}$ 上的某些关系。我们将继续证明这些关系都是等价关系，并且更具体地，看看它们的等价 *classes* 有多有用！

Congruence modulo n

Definition 6.5.4. *Let $n \in \mathbb{N}$. We define a relation R_n on $\mathbb{Z}$ by saying $(a, b) \in R_n$ if and only if a and b have the same 余数 upon division by n.*

Equivalently, we say $(a, b) \in R_n \iff n \mid a - b$.

Notationally, we also write this as

$$a \equiv b \mod n$$

and read this as "a and b are **congruent modulo** *n. (Verbally, we usually shorten "modulo" to "mod".)*

Remark 6.5.5. 我们在我们的定义中指出，说"a和b除以n的余数相同"是等同于说"*equivalent*"。为什么是这样呢？这并不是*by definition*；它需要一点证明。我们将在练习6.7.15中要求你这样做。

Remark 6.5.6. 在实践中（即在解决问题和证明其他结果时），我们将如下使用此定义：知道 $a \equiv b \bmod n$ 保证我们可以将 a 表示为 n 的倍数加上 b。

让我们看看这是为什么。假设它们的公共余数是 r。这意味着存在 $k, \ell \in \mathbb{Z}$ 使得

$$a = kn + r \quad \text{and} \quad b = \ell n + r$$

(它们有相同的余数，但它们可能不具有相同的 *multiple* 的 n。) 从中减去以求解 r，然后使它们相等，我们发现

$$a - kn = b - \ell n$$

然后加法和因式分解告诉我们

$$a = (k - \ell)n + b$$

看看那个！项 $(k - \ell)n$ 是 n 的倍数，第二个项就是 b 本身。这告诉我们 a 是 n 的倍数加上 b。

通常，b在除以n时可能不是a的余数；特别是当b不满足我们要求余数的$0 \leq r \leq a - 1$条件时，这种情况会发生。

让我们总结这个评论，写下我们将来会调用的这个定义的形式。当我们使用*congruence modulo* n的定义进行证明或举例时，我们将引用以下陈述:

$$a \equiv b \mod n \iff \exists m \in \mathbb{Z}.\ a = mn + b$$

Example 6.5.7. 让我们通过考虑n的一些小值来弄清楚这些关系"看起来"是什么样子。

- 让 $n = 1$. 关系 R_1 看起来是什么样子？这实际上是一个有点愚蠢的问题，因为任何整数除以1的余数都是0，所以每个整数都与每个其他整数相关。也就是说，$\forall x, y \in \mathbb{Z}$，$(x, y) \in R_1$. Because this is relatively uninteresting, mathematicians would hardly ever speak of "mod 1".

- 让我们 $n = 2$。关系 R_2 正是我们之前定义的“奇偶性关系”。想想为什么这是真的。当我们把任何整数 a 除以 2 时，唯一可能的余数是 0 和 1。如果 a 和 b 在除以 2 时有相同的余数 0，那么它们都是偶数；如果它们有相同的余数 1，那么它们都是奇数。（想想这与我们在第三章的定义如何对应，当时 *odd* 和 *even* 是根据 *existence* 声明定义的：例如，x 是偶数当且仅当存在一个整数 $\exists k \in \mathbb{Z}$ 使得 $x = 2k$。这正是这里除法算法的结果所说的：x 是偶数当且仅当它除以 2 的余数是 0，因为我们可以找到一个整数使得 $x = 2k$。）

  现在，考虑等价公理的等效公式。如果两个整数都是偶数，我们可以说它们的差是什么吗？没错，它也是偶数！这里，这意味着 $a \equiv b$ 模 2 $\iff a - b \mid 2$；即 a 和 b 都是偶数（或都是奇数），当且仅当它们的差也是偶数。（注意：我们还没有 *proven* 这另一种公式真正等同于关于余数的定义。我们将在这个例子之后立即做到这一点。）

- 让 $n = 3$。然后，例如，$0 \equiv 9 \bmod 3$ 和 $-1 \equiv 2 \bmod 3$ 以及 $4 \equiv 28 \bmod 3$。一般来说，我们也可以将几个同余语句连在一起，只要我们在行尾加上“mod 3”（或类似的表达式）。当我们这样做时，整个前面的行被认为是模3的。例如，以下行在符号上有效，在数学上也是正确的：

$$-100 \equiv -1 \equiv 8 \equiv 311 \equiv -289 \equiv 41 \mod 3$$

  (我们不确定你为什么必须写这样的声明，但我们只是指出这样做是完全没问题的！)

- 让 $n = 10$。一个自然数除以10的余数就是它的最后一位，它的 *ones* 位！这有助于我们轻松地比较两个数对10取模。例如，$12 \equiv 32 \equiv 448237402 \bmod 10$ 但 $37457 \not\equiv 38201 \bmod 10$。

  这是不同的，当我们考虑 *negative* 数字时。原因是，我们通过取最大的倍数 *without going over* 来定义余数。例如，$-1 \equiv 9 \bmod 10$；这是因为 $-1 = (-1) \cdot 10 + 9$ 和 $9 = (0) \cdot 10 + 9$。它们共享一个余数 9，需要加到某个 10 的倍数上。思考以下 True 声明背后的细节：

$$-3 \equiv 17 \equiv -33 \equiv 107 \mod 10$$

Notation

一个关于 *notation* 的重要评论：在数学中，**mod** 是一个关系，而不是运算符或函数。在计算机科学和编程中，你可能会看到类似于“$5 \bmod 3 = 2$”的表达，以表示“当我们除以 3 时 5 的余数是 2”。

5乘以3等于2”。（在许多语言中，这可能会表达为`5 % 3 = 2`。）在这里，您不会看到我们写任何类似的东西。相反，我们使用mod来表示某种**equivalence**，在过程中使用$\equiv$，因为我们谈论的数字不一定是*equal*。如果我们表达一个在某个自然数n模下有意义的等价链，我们将在行尾写上“$\mod n$”来表示。从这个意义上讲，mod更像是我们在说“这一行中做出的所有陈述都只意味着在除以n时的余数意义上考虑”时写的*modifier*。因此，我们可以写如下

$$100 \equiv 97 \equiv 16 \equiv 4 \equiv z \cdot w \equiv 1 \equiv x - y \equiv -2 \equiv -8 \mod 3$$

这表示所有这些数字和表达式在模3的情况下是等价的。我们并没有断言它们是相等的，也没有断言它们在模其他任何数的情况下必然等价。最后的“模3”表示，“我们是在模3的整数宇宙中工作，而不在其他任何地方。”

(问题：你能找到使上面的线 True 成立的 $x, y, z, w \in \mathbb{Z}$ 吗？)

Three Important Lemmas

这里，我们将要求你证明两个重要结果；也就是说，你将证明模 n 的同余可以等价地用 *divisibility* 来表示，并且这些关系是 *equivalence relations*。在阅读本节的同时，完成这些相应的练习 *now*。在讨论这些关系下的等价性 *classes* 的下一节中，如果你已经处理过这些细节，将会更容易理解。在这两个证明之后，我们将再提出一个结果，并为你证明它。在讨论等价类之前，我们看到的最后一个例子将是一个有趣的算术问题，使用同余很容易解决，但如果你想要“手动”解决，则并不完全容易。

Lemma 6.5.8. *The two formulations of congruence modulo n given in Definition 6.5.4 are indeed equivalent. That is, for every $a, b \in \mathbb{Z}$ and for every $n \in \mathbb{N}$,*

$$a \text{ and } b \text{ have the same remainder upon division by } n \iff n \mid a - b.$$

Proof. 查看练习6.7.15。 □

Lemma 6.5.9. *For any $n \in \mathbb{N}$, R_n is an equivalence relation on $\mathbb{Z}$.*

Proof. 查看练习6.7.16 □

感谢您证明了那些引理！☺我们现在知道模n的等价关系（因此我们*can*谈论等价类），并且我们可以总是通过确定$a - b$是否是n的*multiple*来判断两个整数（比如说a和b）是否在模n下同余。这将是一种方便的方法来读取所提出的同余关系并评估它们是否成立。

下一个引理告诉我们，我们可以在“模 n”的上下文中执行 **arithmetic**—加法和乘法—并且可以放心，结果仍然正确。如果我们有两个 *equations*，关于整数的两个等式陈述，我们将它们相加呢？我们知道结果等式仍然成立，对吧？也就是说，如果我们知道 $a+b=c$ 和 $d+e=f$，那么我们可以将它们相加并知道 $a+b+d+e=c+f$。这个引理说的是，用模 n 的同余代替等式，同样的情况也成立。同样，我们可以 *multiply* 同余，并且可以放心它们会保持同余。

这个引理的证明并不太难，但我们还是为你证明它，因为我们最近让你做了很多工作。

Lemma 6.5.10 (模运算引理，或MAL)**.** *Let $n \in \mathbb{N}$ be given.*
Let $a, b, r, s \in \mathbb{Z}$ be arbitrary and fixed. Suppose that $a \equiv r \bmod n$ and $b \equiv s \bmod n$. Then

$$a + b \equiv r + s \mod n$$
$$a \cdot b \equiv r \cdot s \mod n$$

(如果您仔细思考，这个引理告诉我们我们只需处理余数。无论我们给出的 a, b 是什么，我们都可以将它们简化为它们的余数，r 和 s，然后使用这些数进行计算。这个想法是，$0 \leq r, s \leq n-1$，因此它们保证是 *small*，与 a 和 b 相比。这使得我们在实际中进行算术运算更快。以下证明保证了这在所有情况下都有效.)

Proof. 假设 $a \equiv r \bmod n$ 和 $b \equiv s \bmod n$。这意味着 $\exists k, \ell \in \mathbb{Z}$ 使得

$$a = kn + r$$
$$b = \ell n + s$$

这些方程相加得到

$$a + b = (kn + r) + (\ell n + s) = (k + \ell)n + (r + s)$$

因此，$a + b \equiv r + s \bmod n$，因为我们可以将 $a + b$ 表示为 n 的倍数加上余数 $r + s$。

两个方程相乘得到

$$a \cdot b = (kn + r) \cdot (\ell n + s) = k\ell n^2 + (ks + \ell r)n + r \cdot s = n \cdot \big(k\ell n + ks + \ell r\big) + r \cdot s$$

因此，$a \cdot b \equiv r \cdot s \bmod n$，因为我们可以将 $a \cdot b$ 表示为 n 的倍数加上余数 $r \cdot s$。 □

Remark 6.5.11. 注意，这里我们没有提到 **subtraction** 或 **division**，只有加法和乘法。这有两个不同的原因。第一个原因是减法只是“加一个负数”。因此，引理实际上说的是我们可以通过应用两个步骤来 *subtract* 两个同余：(1) 将其中一个同余乘以 -1（调用 *multiplication* 的引理），

并且（2）将结果相加（调用*addition*的词元）。注意它如何使用词元的结果中的*both*。很棒，对吧?

第二个原因稍微复杂一些。实际上并不存在“模除”n这样的概念。主要原因是我们在这里将讨论限制在*integers*上，除法可能会导致非整数 *rational numbers*。例如，我们知道4除以7模3，但这能告诉我们$\frac{4}{2} \equiv \frac{7}{2}$模3吗? 这又是什么意思呢? 一个整数（即，2）怎么可能和一个小数（即，7/2）同余呢? 因此，主要是出于这个原因，我们不在$\mathbb{Z}$模n的上下文中讨论**division**的操作。

存在这个“除法”问题的一些更微妙细节，我们将在第6.5.3节中讨论它们，当我们谈到*multiplicative inverses*时。为了避免现在产生混淆，我们不会尝试讨论这些细节。尽管如此，我们将开发出一种感觉“非常像”模n除法的东西，但这只可能在特定情况下实现。

在此期间，为确保我们只讨论 *integers*，我们将坚持加法和乘法 *only*。

Two Examples of Usefulness

我们还没有确定是否已经说服您，这些模块化算术中的任何一个是有效的*useful*或有用的。为了确保我们已经确立了这些关于同余作为等价关系的概念在数学上既有趣*and*又适用，我们将在此考虑两个有趣且有用的例子。第一个是一个简单陈述的问题，使用模算术比“标准”算术容易得多。第二个是一个您可能以前使用过但从未考虑过*how*或*why*它如何工作的实用技巧。我们将证明它!

Example 6.5.12. 考虑以下问题:

> **Questions:**
>
> 存在一个自然数 *exist*，使得 5^k 比 7 的倍数多 1 吗?
>
> 如果这样，那么什么是这样的自然数 *smallest*?
>
> 您能否用这个性质来描述自然数中的 *all*?

我们可能尝试通过仅将值插入 k 并观察结果来回答这些问题。然而，你很快就会注意到计算大的指数数可能会很繁琐，而且确定一个大的数是否正好比某个7的倍数多1甚至更难! 如果你愿意，就试试吧。如果你想，甚至可以使用计算器。看看你是否能解决它!

这里是我们更愿意做的事情：让我们一次又一次地利用模运算引理（MAL）。指数运算只是重复的乘法，所以让我们一次又一次地调用引理的乘法结果。想法是我们可以一直乘以5和*reduce everything mod- ulo 7 along the way*。也就是说，我们只需要找到一个比1大1的数

一个7的倍数——即模7同余于1——我们不需要立即知道这个数是什么*exactly*, 只需要知道它是否*has that property*。让我们展示我们的意思。

我们从$5^1 \equiv 5 \bmod 7$开始。我们将其乘以5，得到 ing

$$5^2 \equiv 5 \cdot 5 \equiv 25 \equiv 4 \mod 7$$

我们通过仅仅注意到$25 = 21 + 4$，并且知道21是7的倍数来找到这个。（当数字“小”像这样时，我们经常可以做算术 **by inspection**。也就是说，我们只需要花一分钟看看，做一些心算。当然，如果我们不确定，我们总是可以应用除法算法，只是从25中减去7，直到我们剩下余数。）

我们可以找到

$$5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6 \mod 7$$

再次，我们只是通过检查发现“$20 = 14+6$”。请注意，我们现在知道5^3与7同余，但我们*didn't have to actually compute* $5^3 = 125$ *and then reduce it*。因为我们一直在将所有数字模7进行化简，所以我们节省了很多计算。具体来说，我们总是将数字化简为小于7的数，所以无论如何，我们可能需要查看的最大数字都在20和30之间。多么方便！让我们继续看看我们会得到什么：

$$5^4 \equiv 5^3 \cdot 5 \equiv 6 \cdot 5 \equiv 30 \equiv 2 \mod 7$$

$$5^5 \equiv 5^4 \cdot 5 \equiv 2 \cdot 5 \equiv 10 \equiv 3 \mod 7$$

$$5^6 \equiv 5^5 \cdot 5 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \mod 7$$

这就是我们要找的！我们已经确定5^6比7的倍数多1。而且这比计算5^6 =乘以15625和弄清楚15625除以7余2232，再减去1要简单，不是吗？

这已经回答了前两个问题：我们发现存在一个具有所需性质的5的幂，*exists*，并且因为我们是通过迭代找到的（从$k = 1$开始），我们知道这是*smallest*这样的数。我们将把它留给你去研究第三个问题，即描述*all*这样的数。尝试继续我们的过程，乘以5的幂并化简。你注意到一个模式吗？那是什么？做出一个猜想。试着证明它！（我们稍后会回到这个例子……）

Example 6.5.13. 考虑数字474。它是3的倍数吗？也许你只是把它的数字加起来—$15 = 4 + 7 + 4$—然后注意到15是3的倍数，然后得出结论474必须 *also* 是3的倍数。（当然，你也可以直接进行长除法来找到$474 = 3 \cdot 158$。）你为什么能这样做？是因为你的老师在三年级时告诉你这件事，你相信了他们的话吗？这对我们来说还不够好！ ☺

这里，我们将正式证明一个自然数 **prove** 可被3整除当且仅当其各位数字之和也可被3整除。（在证明中，我们

已包含括号内的说明，用于解决特定 *example* 的细节。我们包括它们是为了帮助您理解我们在写什么，但我们把它们放在括号中是为了提醒您，仅仅展示一个例子是 *not* 一个正式的证明。它可以帮助读者更容易地理解 *actual* 证明，但仅仅一个例子不足以证明这个 *universally-quantified* 命题。）

Proof. 设 $x \in \mathbb{N}$ 为任意且固定的。我们可以通过写出它的十进制展开来表示这个数

$$x = \sum_{k=0}^{n-1} x_k \cdot 10^k$$

在 n 是数字 x 的位数，而 x_k 是对应于 10^k-位的数字，所以 $0 \leq x_k \leq 9$。（即 x_k 是从右向左读取的 $k+1$-位数字 x。）

例如，我们可以将47205写成$47205 = 4{\cdot}10^4 + 7{\cdot}10^3 + 2{\cdot}10^2 + 0{\cdot}10^1 + 5{\cdot}10^0$。在这种情况下，$x_0 = 5$和$x_1 = 0$和$x_3 = 2$等等。

The Divisiblity Trick 声称

$$x \equiv 0 \mod 3 \iff \sum_{k=0}^{n-1} x_k \equiv 0 \mod 3$$

为了证明这一点，我们将考虑10的模3的展开。注意，$10 \equiv 1 \bmod 3$，因为$10 = 9 + 1$。因此，

$$\forall k \in \mathbb{N} \cup \{0\}\,.\; 10^k \equiv 1^k \equiv 1 \mod 3$$

(这来自于模算术引理以及对于任何 k，$1^k = 1$ 的事实。想想这个！)

这允许我们将十进制展开中的10的幂替换为1！因此，

$$\begin{aligned}
x \equiv 0 \mod 3 &\iff \sum_{k=0}^{n-1} x_k \cdot 10^k \equiv 0 \mod 3 && \text{Rewrite } x \text{ in decimal form} \\
&\iff \sum_{k=0}^{n-1} x_k \cdot 1^k \equiv 0 \mod 3 && \text{Since } 10 \equiv 1 \mod 3 \\
&\iff \sum_{k=0}^{n-1} x_k \equiv 0 \mod 3
\end{aligned}$$

这证明了该主张。

□

(注意3 | 47205，因为3 | (4 + 7 + 2 + 0 + 5)，也就是说3 | 18。实际上，15735 · 3 = 47205)。

有趣的是，我们在这里实际上已经证明了一个 **stronger** 结果。因为上面的陈述是 *if and only if* 陈述，我们实际上知道更多：如果 x 的数字之和是 not 3 的倍数，那么 x 是 not 3 的倍数并且有 $same\ remainder$。例如，3 ∤ 122，因为 3 ∤ 5；此外，5 ≡ 2 mod 3，所以我们知道 122 ≡ 2 mod 3。（实际上，122 = 3 · 40 + 2。）

可以找到并证明类似的可除性技巧用于9和11（尽管11的那个稍微有点复杂）。甚至还有一个用于7的，但很难写下来。这些想法将在本章的练习中探讨。

记住这个结果及其证明。在聚会上拿出来是个不错的选择。挑战你的朋友：他们真的知道 **why** 这个技巧是有效的吗？你做到了！

6.5.2 Equivalence Classes modulo n

您证明了（参见引理6.5.9）模 n 的同余关系确实是底集 $\mathbb{Z}$ 上的一个等价关系。您还证明了（参见定理6.4.10）等价关系的等价类构成了底集。结合这两个结果，我们知道模 n 的同余关系产生了 $\mathbb{Z}$ 的一个划分。多么方便！然而，我们如何表示这些等价类呢？选择每个类的代表元素，哪个会是 $natural$ 的一个合适选择呢？

让我们从两个更简单的问题开始：(1) $many$模n下有多少个等价类？(2) 等价类有多少个“big”？

How many equivalence classes?

要回答问题（1），我们只需记住我们在除以n时如何定义$remainders$。除法算法（参见引理6.5.2）要求一个余数r满足$0 \le r \le n-1$，当我们用其他数除以n时。这表明余数可能的情况最多有n种：要么是0，要么是1，要么是2，……要么是$n-1$。（也就是说，$r \in [n-1] \cup \{0\}$。）我们是否确定存在这样的数，它们的余数是这些可能性？当然，我们可以直接使用这些数本身！显然$n-1$除以n (的余数是$n-1$，因为$n-1 < n$)。这些观察结果告诉我们，在模n下，存在**exactly** n **equivalence classes**个$\mathbb{Z}$。

我们也可以通过这些相同的观察结果识别出这些等价类中的一些自然选择$representatives$！由于$a \equiv b \bmod n$表示a和b除以n的余数相同，为什么我们不直接宣布这两个数属于由$that\ re\text{-}\ mainder$表示的等价类，无论它是什么。这个余数$r$必须满足$0 \le r \le n-1$，我们将用$a, b \in [r]_{\bmod n}$来表示$a$和$b$属于由余数$r$（表示的等价类，同时，用下标“mod n”来表示余数来自除以n)。

How big are the classes?

让我们通过一个特定的值来思考这个问题，比如说 $n = 4$。一个整数 $z \in \mathbb{Z}$ 属于对应于 0 的等价类意味着什么？也就是说，如果我们知道 $z \in [0]_{\mathrm{mod}\ 4}$，我们可以说些什么关于 z 的?

通过模的定义，我们知道这意味着当我们将 z 除以 4 时，余数为 0。啊！这意味着 z 是 4 的一个 *multiple*。$\mathbb{Z}$ 中有多少个 4 的倍数？无限多个！我们有 4, 8, 12, 16, . . . ，以及 $0, -4, -8, -12, \ldots$。集合 $[0]_{\mathrm{mod}\ 4}$ 是一个 *infinite* 集合。

关于知道 $z \in [1]_{\mathrm{mod}\ 4}$ 是什么？这说明了关于 z 的什么？余数为 1 意味着 z 可以表示为 $4k + 1$；也就是说，存在这样的 k，使得我们可以用这种方式写出 z。那这可能是什么？嗯，*any* 的 $k \in \mathbb{Z}$ 选择创建了一个这样的数 z，因此我们可以考虑让 $k = 0$ 和 $k = 1$ 和 $k = 2$……以及 $k = -1$ 和 $k = -2$……等等，看看会发生什么。我们发现这生成了集合

$$\begin{aligned}[1]_{\mathrm{mod}\ 4} &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\ &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 4k + 1\} = \{4k + 1 \mid k \in \mathbb{Z}\}\end{aligned}$$

注意我们最初使用了“. . .”符号来向您展示我们注意到的模式，然后我们用集合构造符号（两种不同的方式）重新编写了这个集合。

这是一个无限集合。我们将让您尝试其他余数（除以4以及对于一般的n），让您发现这些集合都是*infinite*。（此外，我们尚未提供一个适当的、*formal*定义集合为何为*infinite*，但我们正依靠我们共同的直觉来理解这个含义。如果您想找到一个好的思考方式，试试这个：这个集合是无限的，因为我们开始列出所有元素，并识别出一个我们确信*will*生成所有元素的规律，但这个过程不会*end*在有限的时间内。）

The Partition of $\mathbb{Z}$ modulo n

让我们利用我们对等价类的观察来对这些等价类进行总结，即关于 *canonical* (的标准/自然/方便) 表示，即 $\mathbb{Z}$ 模 n 的等价类。我们知道有 n 个等价类，每个都是无限大的。我们知道每个类对应于 *exactly* 当你将一个整数除以 n 时可能得到的余数之一。由于那个余数必须满足 $0 \leq r \leq n - 1$，我们将使用集合 $\{0, 1, 2, \ldots, n - 1\} = [n - 1] \cup \{0\}$ 作为规范代表元的集合。

等价类对应于余数 r 将收集所有在除以 n 时得到该余数的整数。换句话说，所有元素 $z \in [r]_{\mathrm{mod}\ n}$ 必须正好比某个 n 的倍数多 r。这意味着我们可以通过从 r 开始并反复加减 n 来 *generate* 等价类中的所有元素。（想想看，你会发现这意味着同一等价类中的任何两个元素之间的差都是 n 的倍数。）

The equivalence classes of $\mathbb{Z}$ modulo n:

给定 $n \in \mathbb{N}$，恰好有 n 个等价类：

$$[0]_{\text{mod } n},\ [1]_{\text{mod } n},\ [2]_{\text{mod } n},\ \ldots,\ [n-1]_{\text{mod } n}$$

它们的特点是：

$$\begin{aligned}
[0]_{\text{mod } n} &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\
&= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = kn\} \\
[1]_{\text{mod } n} &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\} \\
&= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = kn+1\} \\
[2]_{\text{mod } n} &= \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\} \\
&= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = kn+2\} \\
&\vdots \\
[n-1]_{\text{mod } n} &= \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\} \\
&= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = kn+(n-1)\} \\
&= \{z \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z}.\ z = \ell n-1\}
\end{aligned}$$

这总结了我们的所有观察结果 *generality*。以下是一些具有 *specific* 值的 n 的例子。

- 考虑 $n = 2$. 等价类是

$$\begin{aligned}
[0]_{\text{mod } 2} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 2k\} = \{\text{even integers}\} \\
&= \{\ldots, -6, -4, -2, 0, 2, 4, 6\ldots\} \\
[1]_{\text{mod } 2} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 2k+1\} = \{\text{odd integers}\} \\
&= \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}
\end{aligned}$$

- 考虑 $n = 3$。等价类是

$$\begin{aligned}
[0]_{\text{mod } 3} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 3k\} = \{\text{multiples of 3}\} \\
&= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\
[1]_{\text{mod } 3} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 3k+1\} = \{\text{multiples of 3, plus 1}\} \\
&= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\
[2]_{\text{mod } 3} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 3k+2\} = \{\text{multiples of 3, plus 2}\} \\
&= \{\ldots, -7, -4, -1, 2, 5, 8, 11\ldots\}
\end{aligned}$$

- 考虑 $n = 4$。等价类是

$$\begin{aligned}
[0]_{\text{mod } 4} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 4k\} = \{\text{multiples of } 4\} \\
&= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} \\
[1]_{\text{mod } 4} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 4k + 1\} = \{\text{multiples of } 4, \text{ plus } 1\} \\
&= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\} \\
[2]_{\text{mod } 4} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 4k + 2\} = \{\text{multiples of } 4, \text{ plus } 2\} \\
&= \{\ldots, -10, -6, -2, 2, 4, 6, 10, 14, \ldots\} \\
[3]_{\text{mod } 4} &= \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}.\ z = 4k + 3\} = \{\text{multiples of } 4, \text{ plus } 3\} \\
&= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}
\end{aligned}$$

Using the Equivalence Classes

为什么这有帮助? 我们为什么要费心带你了解整数集在特定等价关系下的这种发展?

该事实表明 $\mathbb{Z}$ 通过这些等价类是 **partitioned** 的，这一点非常重要。因此，每当我们在 $\mathbb{Z}$ 模 n 的上下文中进行算术运算时，我们只需要考虑等价类，即 **remainders**。我们可以将所有东西简化为沿路仅涉及数字 $\{0, 1, 2, \ldots, n-1\}$，因为它们代表 *all* 整数。我们不需要进行大量的大数算术和 *then* 求余数；我们只需处理余数 *alone*。让我们看看几个例子，以展示这种划分确实是有用的。

Example 6.5.14. 考虑以下声明:

$$\forall n \in \mathbb{N}.\ 6 \mid n^3 + 5n$$

我们之前要求你通过在 n 上的归纳法来证明这一点！（参见第5.7节中的问题5.7.15。）在这里，我们将利用等价类来证明这一点！

考虑 $\mathbb{Z}$ 模 6。由于 $\mathbb{N} \subseteq \mathbb{Z}$，我们知道每个 $n \in \mathbb{N}$ 必须落入 **exactly one** 的等价类中——$[0]_{\text{mod } 6}$，$[1]_{\text{mod } 6}$，$[2]_{\text{mod } 6}$，$[3]_{\text{mod } 6}$，$[4]_{\text{mod } 6}$，$[5]_{\text{mod } 6}$——根据其除以 6 的余数。

我们可以单独检查每个情况。假设 n 属于一个特定的等价类，这使我们能够计算 n^3+5n 必须属于哪个等价类。在每种情况下，为了乘法（以及指数，即重复乘法）和加法，我们正在应用模算术引理 6.5.10。

(1) $n \equiv 0$ 模 6 $\implies$ $n^3 + 5n \equiv 0^3 + 5 \cdot 0 \equiv 0$ 模 6 **(1)** $n \equiv 1$ 模 6 $\implies$ $n^3 + 5n \equiv 1^3 + 5 \cdot 1 \equiv 6 \equiv 0$ 模 6 **(1)** $n \equiv 2$ 模 6 $\implies$ $n^3 + 5n \equiv 2^3 + 5 \cdot 2 \equiv 18 \equiv 0$ 模 6 **(1)** $n \equiv 3$ 模 6 $\implies$ $n^3 + 5n \equiv 3^3 + 5 \cdot 3 \equiv 42 \equiv 0$ 模 6

(1) $n \equiv 4 \bmod 6 \implies n^3 + 5n \equiv 4^3 + 5 \cdot 4 \equiv 84 \equiv 0 \bmod 6$

(1) $n \equiv 5 \bmod 6 \implies n^3 + 5n \equiv 5^3 + 5 \cdot 5 \equiv 150 \equiv 0 \bmod 6$

在每种情况下，我们发现 $n^3 + 5n$ 是6的倍数（因为它除以6的余数为0）。这告诉我们，无论 n 是什么，都有 $6 \mid n^3 + 5n$。这证明了对于所有 $n \in \mathbb{N}$，该命题成立，而不需要使用任何归纳论证！

Example 6.5.15. **Quadratic Residues**:

在这个例子中，我们将研究完全平方数。具体来说，我们将观察完全平方数被各种数除后得到的余数。这个例子将很有趣，因为你会发现根据我们除以的数不同，会出现一些不同的模式，你可能会想自己去探索这些模式。（如果是这样，太棒了！）但这个例子也会很有帮助，因为我们的某些研究将引导我们得到其他结果，这些结果在本文本和练习中已经得到证明。特别是，这些关于完全平方数的研究在探索**Pythagorean Triples**时可能很有帮助；这些是满足 $a^2 + b^2 = c^2$的整数三元组$(a, b, c) \in \mathbb{N}^3$。了解关于完全平方数的信息可以帮助我们证明一些关于这些三元组的有趣事实！

对于以下每个情况，我们将固定一个特定的 $n \in \mathbb{N}$，然后研究 x^2 在模 n 下的简化形式，对于每个 $x \in \mathbb{Z}$。知道 $\mathbb{Z}$ 在模 n 下的划分后，我们可以简单地查看所有 n 可能的余数模 n 并将其平方，然后进行简化。这些可能的余数被称为 **quadratic residues** (*quadratic*，因为我们使用了完全平方数，并且 *residues*，因为我们找到了余数)。在每个情况之后，我们将用这些可能的二次剩余的列表进行总结。

n = 2: 我们知道，一个完全平方数是偶数当且仅当其底数是偶数，而一个完全平方数是奇数当且仅当其底数是奇数。我们早在第四章讨论了双条件语句、量词和证明技术时对这些说法进行了研究。现在没有必要回头重新正式证明这些说法；我们可以通过模运算轻松地看到这些结果！

让 $x \in \mathbb{Z}$ 为任意且固定的。

- 首先，假设 $x \equiv 0$ 模 2（即 x 是偶数）。然后应用 MAL 告诉我们 $x^2 \equiv 0^2 \equiv 0$ 模 2（即 x^2 是偶数）。
- 其次，假设 $x \equiv 1$ 模 2（即 x 是奇数）。然后应用 MAL 告诉我们 $x^2 \equiv 1^2 \equiv 1$ 模 2（即 x^2 是奇数）。

这就是了！$\mathbb{Z}$模2的分割告诉我们，这些是需要考虑的唯一情况。

二次剩余模2：$\{0, 1\}$

n = 3: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $3 \implies x^2 \equiv 0^2 \equiv 0$ 模 3
- $x \equiv 1$ 模 $2 \implies x^2 \equiv 1^2 \equiv 1$ 模 3
- $x \equiv 2$ 模 $3 \implies x^2 \equiv 2^2 \equiv 4 \equiv 1$ 模 3 二次剩余模 3：$\{0, 1\}$

n = 4: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $4 \implies x^2 \equiv 0^2 \equiv 0$ 模 4
- $x \equiv 1$ 模 $4 \implies x^2 \equiv 1^2 \equiv 1$ 模 4
- $x \equiv 2$ 模 $4 \implies x^2 \equiv 2^2 \equiv 4 \equiv 0$ 模 4
- $x \equiv 3$ 模 $4 \implies x^2 \equiv 3^2 \equiv 9 \equiv 1$ 模 4

四次方剩余模4：$\{0, 1\}$

n = 5: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $5 \implies x^2 \equiv 0^2 \equiv 0$ 模 3
- $x \equiv 1$ 模 $5 \implies x^2 \equiv 1^2 \equiv 1$ 模 3
- $x \equiv 2$ 模 $5 \implies x^2 \equiv 2^2 \equiv 4$ 模 5
- $x \equiv 3$ 模 $5 \implies x^2 \equiv 3^2 \equiv 9 \equiv 4$ 模 5
- $x \equiv 4 \bmod 5 \implies x^2 \equiv 4^2 \equiv 16 \equiv 1 \bmod 5$ 二次剩余模5：$\{0, 1, 4\}$

n = 6: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $6 \implies x^2 \equiv 0^2 \equiv 0$ 模 6
- $x \equiv 1$ 模 $6 \implies x^2 \equiv 1^2 \equiv 1$ 模 6
- $x \equiv 2$ 模 $6 \implies x^2 \equiv 2^2 \equiv 4$ 模 6
- $x \equiv 3$ 模 $6 \implies x^2 \equiv 3^2 \equiv 9 \equiv 3$ 模 6
- $x \equiv 4$ 模 $6 \implies x^2 \equiv 4^2 \equiv 16 \equiv 4$ 模 6
- $x \equiv 5$ 模 $6 \implies x^2 \equiv 5^2 \equiv 25 \equiv 1$ 模 6

二次同余模6：{v*}0{v*} 1{v*} 3{v*} 4{v*}

n = 7: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $7 \implies x^2 \equiv 0^2 \equiv 0$ 模 7
- $x \equiv 1$ 模 $7 \implies x^2 \equiv 1^2 \equiv 1$ 模 7
- $x \equiv 2$ 模 $7 \implies x^2 \equiv 2^2 \equiv 4$ 模 7
- $x \equiv 3$ 模 $7 \implies x^2 \equiv 3^2 \equiv 9 \equiv 2$ 模 7
- $x \equiv 4$ 模 $7 \implies x^2 \equiv 4^2 \equiv 16 \equiv 2$ 模 7

- $x \equiv 5$ 模 $7 \implies x^2 \equiv 5^2 \equiv 25 \equiv 4$ 模 7
- $x \equiv 6$ 模 $7 \implies x^2 \equiv 6^2 \equiv 36 \equiv 1$ 模 7

二次剩余模7：$\{0, 1, 2, 4\}$

n = 8: 设 $x \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $x \equiv 0$ 模 $8 \implies x^2 \equiv 0^2 \equiv 0$ 模 8
- $x \equiv 1$ 模 $8 \implies x^2 \equiv 1^2 \equiv 1$ 模 8
- $x \equiv 2$ 模 $8 \implies x^2 \equiv 2^2 \equiv 4$ 模 8
- $x \equiv 3$ 模 $8 \implies x^2 \equiv 3^2 \equiv 9 \equiv 1$ 模 8
- $x \equiv 4$ 模 $8 \implies x^2 \equiv 4^2 \equiv 16 \equiv 0$ 模 8
- $x \equiv 5$ 模 $8 \implies x^2 \equiv 5^2 \equiv 25 \equiv 1$ 模 8
- $x \equiv 6$ 模 $8 \implies x^2 \equiv 6^2 \equiv 36 \equiv 4$ 模 8
- $x \equiv 7$ 模 $8 \implies x^2 \equiv 7^2 \equiv 49 \equiv 1$ 模 8

二次剩余模8：$\{0, 1, 4\}$

我们将让您继续研究其他二次剩余。您甚至可以尝试编写一个计算机程序来为您生成这些列表。您注意到任何模式吗？给定 $n \in \mathbb{N}$，模 n 下有多少个二次剩余？它们是什么？您能否 *guarantee* 一些数字，这些数字 *do* 和 *do not* 出现在任何给定的列表中？尝试并探索！

Example 6.5.16. 让我们推广前一个例子中的想法，并考察一些*cubic residues*，看看它们在特定情况下的应用。

> 假设 $x, y, z \in \mathbb{Z}$ 满足 $x^3 + y^3 = z^3$。证明至少有一个值 $\{x, y, z\}$ 是 7 的倍数。

重申我们的目标，我们想要证明

$$x \equiv 0 \mod 7 \ \vee \ y \equiv 0 \mod 7 \ \vee \ z \equiv 0 \mod 7$$

为了做到这一点，让我们来考察一下模7的立方剩余是什么。

设 $z \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们:

- $z \equiv 0$ 模 $7 \implies z^3 \equiv 0^3 \equiv 0$ 模 7
- $z \equiv 1$ 模 $7 \implies z^3 \equiv 1^3 \equiv 1$ 模 7
- $z \equiv 2$ 模 $7 \implies z^3 \equiv 2^3 \equiv 8 \equiv 1$ 模 7
- $z \equiv 3$ 模 $7 \implies z^3 \equiv 3^3 \equiv 9 \cdot 3 \equiv 2 \cdot 3 \equiv 6$ 模 7
- $z \equiv 4$ 模 $7 \implies z^3 \equiv 4^3 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1$ 模 7

- $z \equiv 5 \bmod 7 \implies z^3 \equiv 5^3 \equiv 25 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6 \bmod 7$
- $z \equiv 6 \bmod 7 \implies z^3 \equiv 6^3 \equiv (-1)^3 \equiv -1 \equiv 6 \bmod 7$

(请注意，我们方便地选择将6写成–1模7，以使计算更简单.)

我们注意到唯一可能的情况是 {0, 1, 6}。

现在，假设我们有一个方程的解，即我们有一个满足 $x^3 + y^3 = z^3$ 的 $x, y, z \in \mathbb{Z}$。每个项——x^3, y^3, z^3——模 7 同余于 0 或 1 或 6。让我们看看一些情况。

- 假设 $x^3 \equiv 0$ 模 7。那么 y^3 可以满足其他任何可能性——即 y^3 可以与 0 或 1 或 6 同余模 7——我们只需要求 z^3 落在相同的等价类中。无论如何，在这种情况下，我们有 $x^3 \equiv 0$ 模 7。

- 假设 $y^3 \equiv 0$ 模 7。我们刚才使用的相同论点适用于 x^3 和 z^3，但无论如何，我们都有 $y^3 \equiv 0$ 模 7。

- 假设 $x^3 \equiv 1 \bmod 7$。AFSOC $y^3 \equiv 1 \bmod 7$。然后 $x^3 + y^3 \equiv 1 + 1 \equiv 2 \bmod 7$，但这不可能，因为 2 不是 7 模下的立方剩余。然而，我们注意到 $y^3 \equiv 0 \bmod 7$ 是一种可能性，因为我们可能有 $x^3 + y^3 \equiv 1 + 0 \equiv 1 \bmod 7$。此外，我们注意到 $y^3 \equiv 6 \bmod 7$ 是一种可能性，因为我们可能有 $x^3 + y^3 \equiv 1 + 6 \equiv 7 \equiv 0 \bmod 7$。

  无论什么情况下，在这个例子中，我们有一个立方体 *at least*——要么是 y^3，要么是 z^3——与7同余0。

- 假设 $y^3 \equiv 1$ 模 7。我们刚才使用的相同论点适用于 x^3 和 z^3，因此我们发现，无论如何，至少有一个立方数模 7 同余于 0。

- 假设 $x^{\equiv}6 \bmod 7$。

  AFSOC $y^3 \equiv 6$ 模 7。然后 $x^3 + y^3 \equiv 6 + 6 \equiv 12 \equiv 5$ 模 7，但这不可能，因为 5 不是模 7 的立方剩余。

  然而，我们发现 $y^3 \equiv 0$ 模 7 是一种可能性，因为我们可能有 $x^3 + y^3 \equiv 6 + 0 \equiv 6$ 模 7。

  此外，我们看到 $y^3 \equiv 1 \bmod 7$ 是一种可能性，因为我们可能有 $x^3 + y^3 \equiv 6 + 1 \equiv 7 \equiv 0 \bmod 7$。

  无论什么情况下，在这个例子中，我们有一个立方体 *at least*——要么是 y^3，要么是 z^3——与7同余0。

- 再次，假设 $y^3 \equiv 6 \bmod 7$，相同的论点适用于 x^3 和 z^3。

我们已经看到，无论什么情况适用，总有一个与0模7同余的立方体 *at least one* 。具有这种性质的立方体取决于情况（在某些情况下，可能有多个立方体具有这种性质），但总是至少有一个。

这对我们来说很有成效，因为我们可以回顾我们的立方剩余数列表，并注意到一些东西：立方同余于7的0的底数*only*本身就是0！换句话说，

$$\forall z \in \mathbb{Z}\text{.}\ z^3 \equiv 0 \mod 7 \implies z \equiv 0 \mod 7$$

这意味着，在上述每一种情况下，我们至少有一个立方体与7同余，这意味着进一步地说，我们至少有一个*base*变量与7同余。通过列出可能性并分析几个案例，我们现在已经证明了关于*all possible solutions*此方程的一个性质，而无需找到任何解！

现在，所有这些工作都已经完成，我们有一些不幸的消息：原始方程的 *only* 解是 *trivial* 的一个，其中 $x = y = z = 0$。这就是全部！你可以尝试找到其他解，但你的努力将是徒劳的。这个事实是 **Fermat's Last Theorem** 结论的一个特例，该结论说，非平凡积分解（即 $x, y, z \in \mathbb{Z}$）存在于方程 $x^k + y^k = z^k$（中，其中 $k \in \mathbb{N}$）当且仅当 $k = 1$ 或 $k = 2$；也就是说，当 $k \in \mathbb{N} - \{1, 2\}$ 时，唯一的解是 $x = y = z = 0$。

这个事实是费马在世时自己说的，但他从未发表过证明。他在一本笔记本的边角处声称有一个简短的证明，但无法放入这些边角中，但我们现在已经意识到这可能并不真实。尽管费马在17世纪工作，但这个定理直到20世纪90年代才得到证明！此外，这个证明涉及到了费马提出和最终证明之间这段时间内发展起来的许多强大的数学。

如果我们知道这个定理，那么我们可以很容易地证明这个例子中的陈述！如果唯一的解是 $x = y = z = 0$，那么显然至少有一个值是7的倍数；它们全都是！但这没有意思，而且不给我们提供任何使用模运算和等价类的练习。

Example 6.5.17. 这里是另一个处理三次方程的问题 sidues:

Suppose $x, y, z \in \mathbb{Z}$ satisfy $x^3 + y^3 + z^3 = 3$.

Prove that $x^3 \equiv y^3 \equiv z^3 \mod 9$.

这个问题涉及特定的 *Diophantine Equation*。这是一个泛称，用于涉及多个变量和系数为整数的多项式方程的类型。此类丢番图方程的一个 *solution* 是对变量的选择，这些选择是 *integers* 且满足方程。在这里，我们说的是，这个方程的 *any* 解必须使所有项——x^3、y^3 和 z^3——在模 9 下同余。

首先，尝试找到这个方程的几个解，只是为了看看一些例子。我们将给你一些简单的例子让你开始：我们可能会

有 (x, y, z) 等于 (1, 1, 1) 或 (4, 4, −5)。你看到这些解具有指定的属性吗？你能找到其他解吗？（这是一个难题，所以不要太努力 *too*。）

有趣的是，我们甚至不需要尝试确定所有解“看起来”如何或尝试找到它们，就可以证明这个说法。我们只需要找到模9的立方剩余数：

设 $z \in \mathbb{Z}$ 为任意且固定的。应用 MAL 告诉我们：

- $z \equiv 0$ 模 $9 \implies z^3 \equiv 0^3 \equiv 0$ 模 9
- $z \equiv 1$ 模 $9 \implies z^3 \equiv 1^3 \equiv 1$ 模 9
- $z \equiv 2$ 模 $9 \implies z^3 \equiv 2^3 \equiv 8$ 模 9
- $z \equiv 3$ 模 $9 \implies z^3 \equiv 3^3 \equiv 9 \cdot 3 \equiv 0$ 模 9
- $z \equiv 4$ 模 $9 \implies z^3 \equiv 4^3 \equiv 16 \cdot 4 \equiv (-2) \cdot 4 \equiv -8 \equiv 1$ 模 9
- $z \equiv 5$ 模 $9 \implies z^3 \equiv 5^3 \equiv 25 \cdot 5 \equiv (-2) \cdot 5 \equiv -10 \equiv 8$ 模 9
- $z \equiv 6$ 模 $9 \implies z^3 \equiv 6^3 \equiv 36 \cdot 6 \equiv 0 \cdot 6 \equiv 0$ 模 9
- $z \equiv 7$ 模 $9 \implies z^3 \equiv 7^3 \equiv 49 \cdot 7 \equiv 4 \cdot (-2) \equiv -8 \equiv 1$ 模 9
- $z \equiv 8$ 模 $9 \implies z^3 \equiv 8^3 \equiv (-1)^3 \cdot -1 \equiv 8$ 模 9

注意，在某些情况下，我们使用了 *negative* 数字来使计算更容易。这完全没问题，对你可能也有帮助！例如，我们不是先计算 $4^3 = 64$，然后尝试对 9 取模，而是可以将 16 替换为 -2 以保持数字较小。我们可以总是从任何项中加上或减去 9 的倍数，所以我们不妨在过程中尝试这样做，而不是找到一个很大的数然后再对 9 取模。（当然，这个点可能看起来完全无关紧要，因为 64 并不是一个很大的数；然而，当你必须处理更大的数时，这一点就更加相关。此外，尽可能将这个减法做到个位数，可以减少心算错误的发生率！）注意，我们只在最右边看到了三种可能性；9 模下的立方剩余是 $\{0, 1, 8\}$。就是这样！

当然，为了使 $x^3 + y^3 + z^3 = 3$ 成为 *equality*，我们肯定需要 $x^3 + y^3 + z^3 \equiv 3 \bmod 9$，因为 $3 \equiv 3 \bmod 9$。但是，当我们看可能的立方剩余之和——0、1 和 8 时，我们发现 $1 + 1 + 1$ 是产生 3 的 *only* 之和。尝试其他的：$0 + 1 + 8 \equiv 9 \equiv 0 \bmod 9$ 和 $8 + 8 + 8 \equiv 24 \equiv 6 \bmod 3$ 等等。这意味着我们 *require* $x^3 \equiv y^3 \equiv z^3 \equiv 1 \bmod 9$，以便 (x, y, z) 成为解。

在解决这个问题时，我们证明了一个稍微更强的结果。我们不仅现在知道 x^3, y^3, z^3 必须模 9 同余，它们还必须模 9 同余于 1。这比我们所需的信息要多一点。

现在，事实证明关于这个问题甚至 *stronger* 也是正确的。恰好 $x \equiv y \equiv z \bmod 9$。也就是说，不仅 *cubes* 在模9下同余，*bases* 也是如此。（注意这并没有说基数）

与9同余1；事实上，我们的另一个例子（4, 4, –5）表明这并不一定成立。）不幸的是，证明这个事实需要深入很多高等数学，远远超出了本书的范围。尽管如此，这应该让你对这样一个“简单”问题（表述简单、数字小、整数）需要极其复杂和深入的数学来解决的想法有所认识。然而，与其把这看作是一种打击，不如把它看作是一种鼓舞：只需一点数学知识，我们就能触及这个问题的表面，这进一步暗示了非常深刻和复杂的底层结构。

（如果你好奇，这里有一篇解决完整结果的论文，证明 $x \equiv y \equiv z \bmod 9$，必然：

http://www.ams.org/journals/mcom/1985-44-169/
S0025-5718-1985-0771049-4/S0025-5718-1985-0771049-4.pdf

您需要查阅一些定义才能读懂前两段。这也将要求您学习相应的数学知识，这可能需要，哦……几个月或几年，也许，取决于您的兴趣。请记住这一点，并在您的数学生涯中稍后回到它！

6.5.3 Multiplicative Inverses

我们之前提到——当我们证明了MAL，引理6.5.10时——我们不会在$\mathbb{Z}$模n的上下文中讨论“除法”。在本节中，我们将重新审视这个想法，并解释为什么（以及如何）在某些“良好”的情况下“除法”是有意义的。然而，我们想强调，我们实际上是在呼吁一个更一般的**multiplicative inverses**概念，并且我们应该**not**实际上从这个“除法”的角度来思考这个问题。我们将首先通过几个激励性例子来解释这一点，然后我们将陈述并证明关于这些“良好”情况的确切结果。

The General Concept

给定一个特定的数学对象，其 **multiplicative inverse** 是另一个对象，当我们“相乘”这两个对象时，我们得到“1”。我们在这里使用引号，因为“相乘”和“1”的概念在很大程度上取决于上下文！

Example 6.5.18. 首先考虑一个熟悉的例子。假设我们的上下文是实数集 $\mathbb{R}$，具有通常的乘法。让我们取数字 2。它的乘法逆元是什么？也就是说，是否存在另一个实数 x，使得 $2 \cdot x = 1$，如果是这样，它是什么？当然，$x = \frac{1}{2}$ 是有效的！注意 $2 \cdot \frac{1}{2} = 1$。因此，我们写

$$2^{-1} = \frac{1}{2} \quad \text{in the context of } \mathbb{R}$$

当我们“将方程的两边都除以2”时，我们实际上是用2的*multiplicative inverse*除以方程的两边。

Example 6.5.19. 现在让我们考虑一个可能不太熟悉的例子。考虑一个带有围绕边缘均匀分布的12小时凹槽的挂钟。我们将考虑围绕挂钟旋转，因此我们宣布标准放置——顶部为12——是我们的“1”。也就是说，这是没有额外旋转的*usual*表示，因此我们将其称为我们的*identity*，我们的*unit element*。本质上，我们的“1”是经过“0°旋转”后的时钟。

现在，让我们假设“相乘”两个旋转只是简单地一个旋转后跟另一个旋转。例如，假设我们以顺时针方向（当然，是顺时针）将时钟旋转45°，然后我们再将时钟进一步旋转（顺时针）另一个90°。在我们的上下文中，我们只有*multiplied*了“45°旋转”和“90°旋转”。这产生了另一个对象，“135°旋转”。

建立这些约定的目的是——我们的上下文是什么，对象是什么，“乘以”意味着什么，以及“1”意味着什么——我们可以识别任何旋转的 {v*}。如果你稍微思考一下，你会发现，如果我们取对象“θ (以度为单位)旋转”并将其通过“$360-\theta$ (以度为单位)旋转”进行 *multiply*，那么我们就完全旋转了时钟360°并到达了标准位置，我们在这个上下文中的“1”。这意味着

$$\big(\theta \text{ (in degrees) rotation}\big)^{-1} = 360-\theta \text{ (in degrees) rotation}$$

在我们的当前语境中。

这两个例子旨在向您展示*inverse*这一概念是普遍的，并不局限于任何*dividing*数字的标准上下文。事实上，我们稍后还会看到这一概念的另一个例子，当我们谈到*inverse of a function*时。（在那个上下文中，“乘法”是函数的组合，“1”是恒等函数。您将在下一章中看到我们的意思，但我们现在想指出这一点，以防您已经熟悉这些概念。）

Relatively Prime Integers

您可能熟悉以下定义。我们将在后续结果中使用它，该结果声明了乘法逆元存在的时间（在 $\mathbb{Z}$ 模 n 的上下文中），因此我们现在想为您重申它并展示一些示例。

Definition 6.5.20. *Given $x, y \in \mathbb{Z}$, we say x and y are* **relatively prime** *if and only if they have no common factors (divisors), other than 1.*

(**Note:** 相对质数这个短语意味着 x 和 y 是相对质数 *to each other*。它并没有说 x 是“有点像质数”或者类似的东西。)

Example 6.5.21. 例如，12和35是互质的，因为$12 = 2^2 \cdot 3$和$35 = 5 \cdot 7$，所以我们可以看出它们没有公共因子。

它通常有助于将这些 *prime factorizations* 写出来，因为我们真的想知道两个数是否有任何 *prime* 公因数（这

将意味着它们有 a 个共同因素。）

对于一个非例子，12和33不是互质的，因为3 | 12和3 | 33。

Example 6.5.22. 此示例将在稍后，在以下所述结果之后，有所帮助。

Claim: 如果 p 是一个素数且 a 是一个不是 *multiple* 的 p 的整数，那么 p 和 a 是互质的。

（即，如果 p 是素数且 $p \nmid a$，那么 p 和 a 是互质的。）

让我们看看这是为什么！

Proof. 设 p 为一个素数，设 $a \in \mathbb{Z}$。假设 $p \nmid a$。

自 $p \nmid a$ 以来，a 的素因数中有 p 个是 *none*。由于 p 本身是素数，因此 a 的那些素因数中没有任何一个能整除 p。这意味着 a 和 p 不共享 *any* 个素因数，因此它们是互质的。 □

这是方便的！特别是，我们现在知道每当 p 是一个素数时，$1, 2, 3, \ldots, p-1$ 这几个数与 p 互质。

Definition and Examples

让我们讨论在 $\mathbb{Z}$ 模 n 的上下文中 *multiplicative inverse* 的含义。在这里，“乘法”意味着通常的乘法，但所有操作都在模 n 下进行。此外，“1”实际上是指与 1 对应的 *equivalence class*。在这种情况下，我们将说对于任何 $x \in \mathbb{Z}$，它的乘法逆元——表示为 x^{-1}——等于 y 当且仅当 $xy \equiv 1 \mod n$。即

$$\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.\ y \equiv x^{-1} \mod n \iff xy \equiv 1 \mod n$$

请注意，所有这些断言都是在 $\mathbb{Z}$ 模 n 的上下文中提出的，所以我们不写 “$y = x^{-1}$”。数字 x 代表一个整个等价类，x^{-1} 也是如此。

让我们练习 *finding* 这些乘法逆元，或者确定它们不存在的情况。这里的关键观察是以下内容：

如果 $x \cdot y \equiv 1 \bmod n$，则对于每个 $k \in \mathbb{Z}$，有 $x \cdot (y + kn) \equiv 1 \bmod n$。

为了了解原因，我们只需将 x 分配到右侧的表达式中：

$$x \cdot (y + kn) \equiv xy + xkn \equiv xy + n(xk) \equiv xy + 0 \equiv xy \equiv 1 \mod n$$

这意味着将 n 的一个倍数加到 y 上，在展开式中只会得到 n 的一个倍数，当我们对一切进行模 n 的约简时，我们可以“扔掉”它。

这个事实的后果是：**If** x 在模 n 下有乘法逆元，**then** (a) 存在 *infinitely* 个这样的逆元，并且它们都属于模 n 的同一个等价类，但（b）我们可以在集合 $\{1, 2, 3, \ldots, n-1\}$ 中恰好找到 *one* 个这样的逆元。

这些事实是有帮助和有趣的。特别是，这告诉我们，我们不必提出一些疯狂或复杂的存在论据来尝试找到乘法逆元：我们只需逐个检查，直到找到为止。如果我们找不到，那么就不存在。换句话说，我们不必“直觉”答案或随机猜测和检查；我们有一个更系统的猜测和检查算法。

让我们通过以下示例来实际看看。

Example 6.5.23. 在本例中，我们将提供一个 $n \in \mathbb{N}$ 和一个 $x \in \mathbb{Z}$，并寻求一个满足 $y \equiv x^{-1} \bmod n$ 的 y。如果不存在这样的逆元，我们将说明原因。

- **$\mathbf{n = 3}$ and $\mathbf{x = 2}$**:

  我们知道我们只需要检查 $y = 1$ 和 $y = 2$。注意 $2 \cdot 2 \equiv 4 \equiv 1 \bmod 3$，所以

  $$2^{-1} \equiv 2 \mod 3$$

- **$\mathbf{n = 4}$ and $\mathbf{x = 3}$**:

  我们知道只需检查 $y = 1$ 和 $y = 2$ 和 $y = 3$。注意 $3 \cdot 3 \equiv 4 \equiv 1$ 模 3，所以

  $$3^{-1} \equiv 3 \mod 4$$

- **$\mathbf{n = 4}$ and $\mathbf{x = 2}$**:

  我们知道我们只需要检查 $y = 1$ 和 $y = 2$ 和 $y = 3$。然而，请注意 x 是偶数，所以 x 的任何倍数也是偶数，但任何 $y \equiv 1$ 模 4 的数必须是奇数。因此，2 在模 4 下的乘法逆元是 no。

- **$\mathbf{n = 10}$ and $\mathbf{x = 3}$**:

  我们只需在此检查情况：

  $$\begin{aligned} 3 \cdot 1 &\equiv 3 \mod 10 \\ 3 \cdot 2 &\equiv 6 \mod 10 \\ 3 \cdot 3 &\equiv 9 \mod 10 \\ 3 \cdot 4 \equiv 12 &\equiv 2 \mod 10 \\ 3 \cdot 5 \equiv 15 &\equiv 5 \mod 10 \\ 3 \cdot 6 \equiv 18 &\equiv 8 \mod 10 \\ 3 \cdot 7 \equiv 21 &\equiv 1 \mod 10 \end{aligned}$$

  啊哈！这意味着

  $$3^{-1} \equiv 7 \mod 10$$

  请注意，这也显示

  $$7^{-1} \equiv 3 \mod 10$$

因为乘法是交换律的（即顺序不重要）。这个观察导致我们得出以下事实:

$$(a^{-1})^{-1} \equiv a \bmod n, \text{ 假设首先存在 } a^{-1} \quad .$$

- **n = 15 and x = 7**:

  如果我们开始检查7的所有倍数，我们会发现当我们到达13时，我们已经成功了:

  $$7 \cdot 13 \equiv 91 \equiv 6 \cdot 15 + 1 \equiv 1 \mod 15$$

  所以

  $$7^{-1} \equiv 13 \mod 15$$

  我们将也将验证工作留给你，例如，6 在模 15 下的乘法逆元为 no。

When Do Multiplicative Inverses Exist?

现在我们已经玩了几种示例，我们应该坐下来并描述存在乘法逆元的情况 all。以下引理正是如此。

Lemma 6.5.24 (乘法逆元当相对质数时，或MIRP引理
)**.** *Suppose $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, and that a and n are* **relatively prime**. *Consider the congruence $a \cdot x \equiv 1 \bmod n$. Then there exists a solution $x \in \mathbb{Z}$ to this congruence.*

In fact, there are infinitely-many solutions to this congruence, and they are all congruent modulo n. This implies there is exactly one solution in the set $[n-1] = \{1, 2, \ldots, n-1\}$.

We use a^{-1} to denote the equivalence class corresponding to the solutions of this congruence, and we call this the **multiplicative inverse** *of a modulo n.*

Furthermore, this is an 仅当 *statement; that is, if a and n are* 不等于 *relatively prime, then there is* **no** *solution $x \in \mathbb{Z}$ to the congruence $a \cdot x \equiv$* 且 *1 模 n.*

这个引理完全描述了乘法逆元存在和不存在的情况。我们可以用它来处理如下同余

$$15x \equiv 1 \mod 33$$

立即声明存在 **no** 解 $x \in \mathbb{Z}$ 因为 3 | 15 且 3 | 33 因此它们不是互质的。同样，我们可以取一个同余，如

$$40x \equiv 1 \mod 51$$

并且知道存在一个解 **must**，因为 $40 = 2^3 \cdot 5$ 和 $51 = 3 \cdot 17$ 是互质的。（注意，引理只能帮我们到这里）

find 解决方案；它只是保证我们可以在 $\{1, 2, \ldots, n-1\}$ 的元素中找到它。）

为了 **prove** 这个引理，我们将将其分为两部分，因为它是一个双条件。我们将为您证明其中一个方向；即，我们将表明每当 a 和 n 互质时，a^{-1} 在模 n 下存在。我们将引导您通过证明另一个方向（如果 a 和 n 有一个公共因子，那么 a^{-1} 在模 n 下不存在）的证明（现在尝试证明它！）在问题 6.7.21 中。

我们需要在证明中使用以下有用的引理。

Lemma 6.5.25 (欧几里得引理)**.** *Let $a, b, c \in \mathbb{Z}$ be given. Suppose $a \mid bc$, and suppose a and b are relatively prime. Then $a \mid c$.*

我们将推迟证明这个特定的引理，直到我们看到MIRP引理的证明。我们认为，处理这个证明的所有细节将暂时使我们分心，偏离本节的主要目标。此外，我们认为这个结果，欧几里得引理，本身就足够可信，我们可以暂时假设它的有效性，并在MIRP引理的证明中使用它。只需看看一些例子：

- 我们知道$3 \mid 30$，和$30 = 5 \cdot 6$。由于3和5互质，我们推断$3 \mid 6$，这确实如此。
- 假设 $3 \mid 5x$，对于某个整数 x。关于 x 我们能说什么？再次，3 和 5 是互质的，所以对于乘积 $5x$ 是 3 的倍数，它必须“包含”一个 3 的因子。也就是说，$3 \mid x$ 是必要的。

现在，我们意识到这还不够好！我们并不是说我们应该在没有证据的情况下就 *accept* 这个陈述；我们只是想在深入探讨之前等待几分钟。在此期间，你可能想尝试自己证明它！看看你能想出什么。

相反，让我们大步前进，现在证明MIRP引理（假设欧几里得引理的结果，将在中间某处恰好使用一次）。

Proof. 设 $n \in \mathbb{N}$ 和 $a \in \mathbb{Z}$。假设 a 和 n 是 **relatively prime**。

WWTS $\exists x \in \mathbb{Z}\,.\, ax \equiv 1 \mod n$.

考虑集合 n 的前 a 个倍数；即，定义集合 N 为

$$\begin{aligned} N &= \{0, a, 2a, 3a, \ldots, (n-1)a\} \\ &= \{z \in \mathbb{Z} \mid \exists k \in [n-1] \cup \{0\}\,.\, z = ka\} \end{aligned}$$

注意该集合 N 中有 n 个元素。

Claim: N 的所有元素在模 n 下的余数都是 *distinct*；也就是说，

$$\forall i, j \in [n-1] \cup \{0\}\,.\, i \neq j \implies ai \not\equiv aj \mod n$$

Let us prove this claim. To this end, we AFSOC the claim is false.

Translated Text: 让我们证明这个说法。为此，我们 AFSOC 该说法是 False.

这意味着 $\exists i, j \in [n-1] \cup \{0\}$。$ai \equiv aj \mod n$. Let such i, j be given.
子—牵引和因式分解告诉我们 $ai - aj = a(i-j) \equiv 0$ 模 n.

这意味着 $n \mid a(i-j)$。我们知道 n 和 a 是互质的。根据上述引理6.5.25，我们可以推断出 $n \mid i-j$。

现在，我们声称这暗示了 $i = j$。记住 $i, j \in [n-1] \cup \{0\}$，因此我们知道 0 $\leq i, j \leq n-1$，从而也 $-(n-1) \leq -j, ij \leq 0$。

这些不等式对于 i 和 $-j$ 的加和，我们发现

$$-(n-1) + 0 = n - 1 \leq i + (-j) = i - j \leq n - 1 = (n-1) + 0$$

这是，$-(n-1) \leq i - j \leq n-1$。我们还知道，$n \mid i-j$，即 $i-j$ 是 *multiple* 的 n。注意，然而，位于 $-(n-1)$ 和 $+(n-1)$ 之间的 *only* 倍数 n 是 0。

因此，$i - j = 0$，所以 $i = j$。这证明了当前 cl 目标。

我们现在知道 N 的元素对 n 取模得到 *distinct* 个余数。我们也已经知道那些可能的余数是 $\{0, 1, 2, \ldots, n-1\} = [n-1] \cup \{0\}$。注意，有 n 个不同的 N 元素，并且有 n 个不同的余数（即等价类）模 n。这意味着 *ev- ery* 模 n 的余数在集合 N 中表示 *exactly once*。

这告诉我们存在一个元素 *exactly* 属于 N (，即恰好有一个 a) 的倍数对应于模 n 的余数为 1。这个 N 的元素形式为 ax，对于某个 $x \in [n-1] \cup \{0\}$。给定这样的 x。这是引理断言中的同余式的解。

□

哇！花了一些功夫，但我们现在到了。既然你已经证明了问题6.7.21中的断言（你证明了，对吧？☺），我们现在知道在$\mathbb{Z}$模n的上下文中，乘法逆元存在时的情况*exactly*。我们还知道一种合理的寻找方法：我们只需要检查a的前$n-$个1的倍数，寻找一个在模n下得到1的倍数。

现在我们已经完成了这个，让我们退一步证明欧几里得引理。这需要完成，因为重要的MIRP引理的证明依赖于这个结果。注意，这个证明中有一个棘手的 *induction* 论证。具体来说，我们有 *two variables*—a 和 b—，并且我们想要证明对于每一个这样的 a 和 b，某个陈述都成立。为了做到这一点，

Proof. 设 $a, b, c \in \mathbb{Z}$。假设 $a \mid bc$，并且 a 和 b 互素。

WWTS，即 $a \mid c$，必然。我们将通过首先证明来完成这一点：

Claim: 如果 $a, b \in \mathbb{N}$ 和 a 和 b 互质，那么 $\exists x, y \in \mathbb{Z}$。$ax + by = 1$.
从这个主张中，结果将很容易得出。我们为了便于阅读，在一个框中概述了这个主张的证明。在框之后，您将找到我们如何

use 此结果以证明lemm原始陈述 a.

在解决这个证明之前，先尝试用例子来“说服”自己这个命题是 True。取两个互质的数——比如 5 和 11，或者 15 和 22，或者 10 和 23——并尝试构造这些 *linear combinations*，使得它们等于 1。然后，取一些有公因数的数——比如 5 和 10，或者 6 和 15，或者 21 和 27——并尝试理解为什么你会 *cannot* 找到这样的组合。

Proof of claim: 我们将通过在求和 $a+b$ 上的归纳法来证明这一点。在开始之前，让我们观察一些事实：

- 如果 $a = 1$ 或 $a = -1$，那么 b 必须是 0 或 1，它们才能互质。

  在任何情况下，我们都可以使用 $x = a$ 和 $y = 0$ 来编写

  $$ax + by = a^2 + 0 = 1$$

  相同的论点适用于当 $b = 1$ 或 $b = -1$ 的情况（即 a 必须为 0 或 1）。

- 如果 $b =$ 为 0，且 $|a| \geq$ 为 2（即 $a \neq$ 为 1 和 $a \neq -$ 为 1），那么 a 和 b 与 a 具有公因数，因此它们不是互质的。相同的论点适用于 $a =$ 为 0 的情况。

一起，这些观察表明我们不需要考虑任一值为0的情况。也就是说，我们只考虑满足 $|a| \geq 1$ 和 $|b| \geq 1$ 的值。

- 由于 a 和 b 互质，因此 $-a$ 和 $-b$ 也互质（同样 $-a$ 和 b，以及 a 和 $-b$ 也互质）。这是因为取整数的相反数不会影响它的因数，只会影响它的符号。

- 如果我们已经知道 $\exists x, y \in \mathbb{Z}$ $ax + by = 1$, then certainly $(-a)(-x) + (-b)(-y) = ax + by = 1$

  自 $-x, -y \in \mathbb{Z}$ 以来，这也表明 $-a$ 和 $-b$ 有这样的表示。

一起，这些观察表明我们只需要考虑满足条件的 a 和 b 的值。（也就是说，如果其中任何一个或两个都是负数，我们只需取它们的相反数。）

结合之前的推导，我们得出我们只需要考虑 $a, b \in \mathbb{N}$。对这些值进行结果证明将 *imply* 当与我们所做的观察相结合时，得出完整结果。

现在，我们可以通过（强）归纳法对和 {v*} 进行证明。由于 $a, b \in \mathbb{N}$，我们有 $a + b \geq 2$。我们上面已经考虑了基本情形 $a + b = 2$，但为了完整性，我们在此再次陈述。

给定 $a, b \in \mathbb{N}$，定义 $P(a, b)$ 为以下陈述

$$\text{“ } a \text{ and } b \text{ are relatively prime } \implies \exists x, y \in \mathbb{Z}\text{.}\ ax + by = 1 \text{ ”}$$

BC: 考虑 $P(\text{^}2)$，即假设 $a, b \in \mathbb{N}$、a 和 b 互素，且 $a + b = \text{^}2$。这意味着 $a = b = \text{^}1$，因此我们可以选择 $x = \text{^}1$ 和 $y = \text{^}0$，得到

$$ax + by = 1 + 0 = 1$$

因此，$P(2)$成立。

IH: 设 $k \in \mathbb{N}$ 为任意且固定的。假设 $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ 成立。（即，假设每当两个互质数相加等于 2 或 3 或 ... 或 k 时，我们知道我们可以找到一个 *linear combination* 使得它们等于 1。）

IS: WWTS，$P(k+1)$ 成立。也就是说，令 $a, b \in \mathbb{N}$ 给定，且 $a + b = k + 1$，假设 a 和 b 互素. WWTS: $\exists x, y \in \mathbb{Z}$. $ax + by = 1$

首先，我们可以假设$a \geq b$具有对称性。（也就是说，我们正在*given*这些值a和b。无论它们是什么，我们都可以“重新命名”它们，因为其中之一必须至少与另一个一样大；较大的那个我们将标记为a。）事实上，由于a和a不是互质的（当$a \geq 2$时），我们甚至可以假设$a > b$。

现在，我们想要根据 b 和 $a - b$ 是 *also* 相对互质的这一事实进行论证。为了说明这一点，我们需要证明 b 和 $a - b$ 除了 1 以外没有公因数。

设 d 是 b 和 $a - b$ 的一个公因数，即 $d \mid b$ 和 $d \mid a - b$。我们知道这暗示了 $d \mid b + (a - b)$，即 $d \mid a$。同样，我们已知 $d \mid b$，因此 d 实际上是 a 和 b 的公因数，所以它必须是 1。因此，b 和 $a - b$ 是互质的。

(我们刚刚证明的是:

$$\big(d \mid b \wedge d \mid a - b\big) \implies \big(d \mid a \wedge d \mid b\big)$$

这个说法也是一个 $\iff$ 声明，我们鼓励你花一分钟思考一下，看看为什么 $\impliedby$ 方向也成立。）

我们现在有的是 $b, a - b \in \mathbb{N}$ (，因为 $b < a$) 是互质的。注意，同样地，$b + (a - b) = a < a + b = k + 1$，因为 $b \in \mathbb{N}$ (所以 $b \geq 1$)。这意味着 $a + b \leq k$，因此归纳假设 $P(a + b)$ 适用！

(请注意，$P(a+b)$不一定等于$P(k)$，因此我们在这里使用强归纳法！)

该陈述 $P(a+b)$——即 $P(b+(a-b))$，正如我们将使用的那样——告诉我们 b 和 $a-b$ 的线性组合可以得到 1；也就是说，

$$\exists u, v \in \mathbb{Z}\text{.}\ ub + v(a-b) = 1$$

我们现在想要将这个表达式改写为 a 和 b 的线性组合，使其结果为 1。为此，我们只需重写上述方程并重新标记系数：

$$ub + v(a-b) = 1 \iff \underbrace{v}_{x} a + b\underbrace{(u-v)}_{y} = 1$$

这意味着我们现在可以 *define* $x = v$ 和 $y = u - v$，以便 $x, y \in \mathbb{Z}$ 和 $ax + by = 1$。

我们现在已经证明 $P(a+b)$ (，即 $P(k+1)$) 成立。通过强归纳法，我们推断对于每个满足 $n \geq 2$ 的 $n \in \mathbb{N}$，$P(n)$ 成立。

这个命题的证明所取得的成果，提醒我们的是，我们现在知道任何互质的数都可以被放入1的线性组合中。

让我们回到引理的原始陈述。我们给定 $a, b, c \in \mathbb{N}$，我们假设 a 和 b 是互质的，并且 $a \mid bc$。

第一个假设告诉我们 $\exists x, y \in \mathbb{Z}$○ $ax + by = 1$. Let such x, y be given.

第二个假设告诉我们 $\exists k \in \mathbb{Z}$○ $bc = ak$. Let such a k be given.

我们将通过第一个假设的方程乘以 c，然后应用第二个假设：

$$ax + by = 1 \implies acx + (bc)y = 1 \implies acx + (ak)y = c \implies c = a\underbrace{\big(cx + ky\big)}_{\ell}$$

这意味着知道 $ax + by = 1$ 让我们推断出 $c = a\ell$，其中 $\ell \in \mathbb{Z}$ 是用其他整数定义的。

根据定义，这意味着 $a \mid c$。这证明了原始陈述。 □

哇！那个证明中发生了很多事情。确保你仔细阅读几遍，逐行跟随并做笔记。你看到为什么每个断言都源于我们已知的内容吗？你看到归纳是如何工作的吗？我们有两个变量可以操作，但我们是在对 *one* 变量进行归纳，它定义为其他两个变量的和。我们意识到这是一个棘手的证明，这就是为什么我们把它放在这里，在更重要的结果之后，即本节的 MIRP 引理。

让我们拿我们现在拥有的这个结果——知道当存在乘法逆元时*precisely*——并用来解决一些问题！

Using Multiplicative Inverses

这个有什么用？你可能认为这个答案有点厚颜无耻，但它确实是有效的：乘法逆元在用模运算解决同余问题时很有用。现在，这可能会让人觉得我们开发了一些数学工具来解决它们产生的问题，但这并不完全正确。事实上，正如你将从下面的例子中看到的那样，在尝试*solve*这些问题时，你可能会不得不创新我们将要应用的技巧。也就是说，你可以尝试在没有学习乘法逆元的情况下解决这些问题，但在这样做并考虑更一般的问题时，你最终会重新发现我们与你一起工作的结果！

好的，前言到此为止。让我们提出并解决几个问题。这些问题都具有以下形式：“这里有一个提议的共形；找出所有的整数解，或者证明不存在解。”

Example 6.5.26. 找出所有满足条件的整数 $x, y \in \mathbb{Z}$

$$3x - 7y = 11$$

我们断言存在无限多对$(x, y) \in \mathbb{Z} \times \mathbb{Z}$满足此方程。此外，我们可以陈述所有解的形式；我们将通过定义所有此类解的*set*来实现这一点。

通过重写给定的方程，我们看到我们想要找到一个 $all\ x, y \in \mathbb{Z}$，使得

$$3x = 7y + 11$$

另一种说法是，我们想要找到 $all\ x \in \mathbb{Z}$ 使得

$$3x \equiv 11 \mod 7$$

假设我们可以找到所有这些整数 $x \in \mathbb{Z}$，我们可以通过重新排列上面的方程轻松找到相应的 $y \in \mathbb{Z}$：$y = \frac{3x-11}{7}$。

注意$3^{-1} \equiv 5 \bmod 7$，因为$3 \cdot 5 \equiv 15 \equiv 2 \cdot 7 + 1 \equiv 1 \bmod 7$。因此，根据MAL，我们可以将同余式的两边乘以$3^{-1}$，得到

$$\begin{aligned} \forall x \in \mathbb{Z}\text{.}\ 3x \equiv 11 \mod 7 &\iff 3^{-1} \cdot 3 \cdot x \equiv 3^{-1} \cdot 11 \mod 7 \\ &\iff 1 \cdot x \equiv 5 \cdot 4 \mod 7 \\ &\iff x \equiv 20 \equiv 6 \mod 7 \end{aligned}$$

由于我们知道3^{-1}表征了这个同余方程的解的*all*（即它代表了3模7的乘法逆元的等价类），因此我们可以推断出

$$\forall x \in \mathbb{Z}\text{.}\ 3x \equiv 11 \mod 7 \iff x \equiv 6 \mod 7 \iff \exists k \in \mathbb{Z}\text{.}\ x = 7k + 6$$

这描述了给定方程解中所有可能的 $x \in \mathbb{Z}$ 值。

现在，我们用这个来识别解中 $y \in \mathbb{Z}$ 的对应值。假设我们已给出 $k \in \mathbb{Z}$，其中 $x = 7k + 6$。然后我们代入并发现

$$y = \frac{3x - 11}{7} = \frac{3\big(7k + 6\big) - 11}{7} = \frac{21k + 7}{7} = 3k + 1$$

现在，我们有一个表示 *all possible solutions* 到给定方程的表单。我们知道 *any* $k \in \mathbb{Z}$ 产生相应的 x，这又产生相应的 y。此外，由于我们的推导使用了 $\iff$ 个语句，我们知道这描述了 *all* 个解。

我们可以通过设定来表示给定方程的解集 S。

$$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \exists k \in \mathbb{Z}\text{.}\ (x, y) = (7k + 6, 3k + 1)\}$$

Interesting Fact:

在这个例子中，我们解决了 **Linear Diophantine Equation** 并建立了其所有解。通过 *linear*，我们指的是变量 x 和 y 都只被提升到第一幂。没有平方或立方或其他类似情况。

使用本例中我们应用的技术，您可以解决 *any* 这样的线性丢番图方程，或者轻松地确定它是否有解。事实上，我们将 *prove* 一个关于此类方程何时有 *no* 个解的结果（参见贝祖恒等式，定理6.5.31），这里使用的方法在存在 *are* 个解的情况下适用。

在下一个例子中，我们将研究一个 **Quadratic Diophantine Equation**，其中变量被平方（我们将有一个 x^2 和 y^2 项）。在示例之后，我们将讨论解决这类方程的可能性。

Example 6.5.27. 现在让我们看一个例子，它使用与上一个例子类似的程序（使用乘法逆元进行简化），但同时也使用了二次剩余。

Claim: 存在 **no** 个整数解 $x, y \in \mathbb{Z}$ 到

$$3x^2 - 5y^2 = 1$$

设 $x, y \in \mathbb{Z}$ 已知。WWTS $3x^2 - 5y^2 = 1$ 是 *impo ssible.*

我们首先将给定的方程重写为

$$3x^2 = 5y^2 + 1$$

这意味着，特别是，这意味着

$$3x^2 \equiv 1 \mod 5$$

自 $5y^2 \equiv 0$ 模 5。注意 $3^{-1} \equiv 2$ 模 5，因为 $3 \cdot 2 = 6 = 5 + 1$。因此，我们可以将两边乘以 3^{-1} 并简化：

$$3x^2 \equiv 1 \mod 5 \iff 3^{-1} \cdot 3x^2 \equiv 3^{-1} \cdot 1 \mod 5 \iff x^2 \equiv 2 \mod 5$$

然而，回顾一下示例6.5.15，我们考察了*quadratic residues*。我们看到了模5的二次剩余集合是$\{0, 1, 4\}$。也就是说，存在一个整数x满足$x^2 \equiv 2 \bmod 5$。这意味着给定的方程没有整数解。

Interesting Fact:

我们上面提到，我们确切地知道何时线性丢番图方程是可解的，以及如何求解它们。不幸的是，关于这些 **Quadratic Diophantine Equations** 我们并不那么幸运。看一眼就确定它是否可解是非常困难的。即使知道了它是可解的，实际上求解它也是非常困难的！

实际上，我们对这些二次丢番图方程感到非常不幸。众所周知，存在
no possible computer algorithm that
can input any Diophantine Equation with variables raised to the 1st and 2nd powers and output whether or not that equation has any solutions。这个事实甚至没有触及到**how**解这样一个方程的想法，只是是否有一个解。哇！这个事实是希尔伯特第十问题的形式。

放心，我们在这里给出的例子和练习中的丢番图方程都是可以用我们提供的技术进行分析的。这里提到的这个事实是对所有这类方程的类的一个更广泛的陈述，具有普遍性。

A Little Bit of Group Theory

在这个小节中，我们只想指出，当前主题背后有一些强大而深刻的数学原理。遗憾的是，我们没有足够的时间和空间来全面开发这些主题。为此，我们将在此陈述一些观点和事实，并用例子来说明。

我们想要传达的主要思想是，当我们考虑 $\mathbb{Z}$ 模 p 时，会发生一些特殊的事情，其中 p 是一个 **prime**。在这种情况下，小于 p 的 *every* 个数是 *relatively prime* 到 p，因为 p 除了 1 没有其他除数。这意味着在 $\{1, 2, \ldots, p-1\}$ *must* 中的所有数在模 p 下都有乘法逆元。多么方便！这意味着每个等价类（除了 $[0]_{\mod p}$）

具有相应的乘法逆元类。

例如，考虑 $p = 5$。注意

$$\begin{aligned} 1^{-1} &\equiv 1 \mod 5 \\ 2^{-1} &\equiv 3 \mod 5 \\ 3^{-1} &\equiv 2 \mod 5 \\ 4^{-1} &\equiv 4 \mod 5 \end{aligned}$$

作为另一个例子，考虑 $p = 7$。注意

$$\begin{aligned} 1^{-1} &\equiv 1 \mod 7 \\ 2^{-1} &\equiv 4 \mod 7 \\ 3^{-1} &\equiv 5 \mod 7 \\ 4^{-1} &\equiv 2 \mod 7 \\ 5^{-1} &\equiv 3 \mod 7 \\ 6^{-1} &\equiv 6 \mod 7 \end{aligned}$$

注意，所有元素都有一个乘法逆元。

(此外，请注意，这些逆元只是从1到$p-1$的*permutation*。这不是巧合！试着证明这种情况会发生！试着证明存在两个自逆元素—$1^{-1} \equiv 1 \bmod p$和$((p-1)^{-1} \equiv p-1) \bmod p$—但每个元素 *cannot* 都是它的自逆元。)

这当然是在我们考虑 *not* 模 n 时的情况，其中 n 是 **composite**。在这种情况下，我们知道 n 有某种分解；比如说我们可以写成 $n = ab$，对于某个 $a, b \in \mathbb{N} - \{1\}$。然后 $1 < a < n$ 但 a 与 n (互质，它们共享公共因子 a)，所以 a 在模 n 下有 *no* 乘法逆元。实际上，n (的所有除数及其倍数) 在模 n 下都没有乘法逆元。

例如，考虑 $n = 6$。然后，

$$\begin{aligned} 1^{-1} &\equiv 1 \mod 6 \\ 2^{-1} &\text{ Does Not Exist } \mod 6 \\ 3^{-1} &\text{ Does Not Exist } \mod 6 \\ 4^{-1} &\text{ Does Not Exist } \mod 6 \\ 5^{-1} &\equiv 5 \mod 6 \end{aligned}$$

因为这种区别，$\mathbb{Z}$ 模 p 的数学“结构”脱颖而出。它具有一些“良好”的性质，并且在某种意义上“表现良好”。当然，这些是我们使用的模糊术语，但主要思想是这样的：其元素对 *all* 的逆存在使 $\mathbb{Z}$ 模 p 变得特殊。事实上，$\mathbb{Z}$ 模 p 形成了一种称为 **group** 的数学结构。

一般来说，从启发式角度讲，一个群是一组可以“相乘”的对象，使得乘法满足（a）交换律和（b）结合律，并且所有元素都有乘法逆元。我们已经知道，整数的标准乘法（即使在 $\mathbb{Z}$ 模 n 下，对于任何 n）是交换的和结合的，而对于素数 p) 的工作 $\mathbb{Z}$ 模 p (告诉我们每个元素都有一个逆元。

如果您想进一步探索这些想法，我们在本章末尾包含了一些练习，这些练习涉及了这些属性的一些方面。您还可以查阅关于 **Abstract Algebra** 或 **Modern Algebra** 或 **Group Theory** 或类似内容的入门教科书。那里有许多强大而深刻的数学思想，**groups** 在许多领域都是相关和适用的!

6.5.4 Some Helpful Theorems

在这个部分，我们将探讨一些数论中的定理，这些定理依赖于模运算，并且本身具有实用性和趣味性。我们将陈述并证明这些定理（有时，通过一些练习在你的帮助下！）然后通过例子展示它们的有用性。

Chinese Remainder Theorem

为了激励这个定理，我们首先将描述其有用性通过 故事:

> 总司令孙武在他的部队中有许多士兵，经过一场战斗后，他想计算还剩下多少士兵。逐个计数会花费太多时间，所以他希望更有效率。幸运的是，士兵们训练有素，可以很容易地组成大小相等的队伍。
>
> 将军孙武将士兵排列成两行长度相等的纵队，发现多出一个士兵。
>
> 他随后命令他们制作三个大小相等的戒指，但又发现又多出一个士兵。
>
> 最后，他命令他们制作五个大小相等的侧翼，但发现还剩下两名士兵。
>
> 在这个时候，他认为他有了足够的信息。在最近的战斗之后，他可以宣称这个团总共有250到300名士兵。利用这条信息，他知道 *exactly*有多少名士兵。
>
> 你能确定这个数字吗? 有多少士兵?

我们将让您尝试操作这个，看看您是否能弄懂。继续阅读我们的解决方案、定理陈述以及解决这类问题的技术描述。

再次阅读这个故事。设x为孙子将军部队中的士兵数量，那么故事告诉我们x必须满足以下三个同余和以下不等式：

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ 250 &\leq x \leq 300 \end{aligned}$$

(你看到这些是从故事中来的吗？)

现在有两个问题需要考虑：(1) *Must* 是否存在一个 x 满足所有三个同余条件？(2) 是否存在这样的 $several\, x$ 值？我们是否可以保证这样的一个 x 也满足不等式？

Chinese Remainder Theorem，如下所述，将保证（1）同余方程有无限多个解，以及（2）存在（至少）一个满足给定不等式的解。然而，在我们陈述和证明定理之前，让我们先尝试解决这个初始问题。我们将将其分解为几个观察和步骤：

- 第一个同余要求解 x 是 **odd**。这消除了所有偶数作为潜在解。潜在解列表：

  $$1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, 23, \ldots$$

- 第二个同余要求解必须是3的倍数加1。这消除了所有与3同余为0或2的数。潜在解的列表：

  $$1, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, \cancel{11}, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, \cancel{17}, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, \cancel{23}, \ldots$$

- 第三种同余要求解必须是5的倍数加2。这消除了任何与5同余为0、1、3或4的数。潜在解的列表：

  $$\cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, \textcircled{7}, \cancel{8}, \cancel{9}, \cancel{10}, \cancel{11}, \cancel{12}, \cancel{13}, \cancel{14}, \cancel{15}, \cancel{16}, \cancel{17}, \cancel{18}, \cancel{19}, \cancel{20}, \cancel{21}, \cancel{22}, \cancel{23}, \ldots$$

看起来7是唯一可见的解，但我们怎么知道没有其他的呢？我们只看了前23个潜在的解……我们能确定没有其他的吗？我们现在把这个问题的调查留给你。尝试一些更大的数字。你能找到其他的解吗？你能猜到一个模式吗？7是唯一的解吗？

现在，让我们在解决这些同余问题时变得更加聪明一些。具体来说，让我们假装我们有一个满足所有三个同余的解 x（。

并且看看我们是否能从中推断出更多关于它的信息。到这个推导的末尾，我们将已经确立了一个关于这些同余方程的所有 *possible* 解的事实。

通过 模的定义，我们知道存在 $k, \ell, m \in \mathbb{Z}$ 这样的 那

$$x = 2k + 1$$
$$x = 3\ell + 1$$
$$x = 5m + 2$$

设这样的 k, ℓ, m 已知。

考虑前两个方程。让我们尝试将它们合并成一个关于 x 的方程。具体来说，让我们将第一个方程乘以 3，第二个方程乘以 2；这分别创建了一个 $6k$ 和 6ℓ 项，因此如果我们从方程中减去，我们可以适当地分解。也就是说，我们首先找到

$$3x = 6k + 3$$
$$2x = 6\ell + 2$$

然后

$$(3x - 2x) = (6k + 3) - (6\ell + 2) \implies x = 6(k - \ell) + 1$$

自從給我們 $k, \ell \in \mathbb{Z}$ 之後，我們就定義 $u = k - \ell$，這樣 $u \in \mathbb{Z}$。注意，這告訴我們 $x = 6u + 1$，或者換句話說，

$$x \equiv 1 \mod 6$$

现在，我们通过组合前两个同余得到了这个新的同余，而且这个同余写成模6的形式，以及6除以2余3，这真是一个巧合。你将在我们引导你证明即将到来的定理时看到这是如何发生的！

继续进行，让我们尝试将这个新的同余与上面给出的第三个同余结合起来。我们将采用类似的方法：我们将刚刚推导出的乘以5，上面的乘以6，这样当我们相减时，我们可以提取出一个30。（这也说明了为什么我们将要推导出的新同余将写成模30的形式。）我们得到

$$5x = 30u + 5$$
$$6x = 30m + 12$$

然后

$$(6x - 5x) = (30m + 12) - (30u + 5) \implies x = 30(m - u) + 7$$

再次，由于 m, u 已被提供给我们，让我们只需定义 $v = m - u$，因此 $v \in \mathbb{Z}$。这现在告诉我们 $x = 30v + 7$，或者说，

$$x \equiv 7 \mod 30$$

这个最终同构是通过将每个给定的同构组合到另一个中得到的，因此它代表了这三个同构提供的信息的 *all*。我们声称这现在告诉我们 **all** 的解！

首先，这个新导出的同余告诉我们，*any*解模30必须与7同余。换句话说，任何除以30后余数大于7的数，都不可能是解。本质上，这把我们在上面三个观察中——我们划掉了潜在解——所做的工作综合成一个陈述。

其次，我们可以解释，实际上，与30同余7的*any*数确实可以是解。让我们看看为什么。设$n \in \mathbb{Z}$，并定义$y =$为$30n + 7$（即我们选择一个任意满足$y \in \mathbb{Z}$的$y \equiv 7 \bmod 30$）。注意，y满足：

- 第一个同余，因为 $y = 30n + 7 = 2(15n + 3) + 1$，所以 $y \equiv 1 \bmod 2$；
- 第二个同余，因为 $y = 30n + 7 = 3(10n + 2) + 1$，所以 $y \equiv 1 \bmod 3$；
- 第三种同余，因为 $y = 30n + 7 = 5(6n + 1) + 2$，所以 $y \equiv 2 \bmod 5$。

这就完了！我们现在知道（1）*any*解x必须满足$x \equiv 7 \bmod 30$，并且（2）任何这样的x实际上*is*是一个解。这两个陈述共同构成一个$\Longleftrightarrow$陈述，即

$$x \text{ is a solution to all three congruences} \Longleftrightarrow x \equiv 7 \mod 30$$

因此，集合 S 的 **all solutions** 由以下公式给出

$$S = \{x \in \mathbb{Z} \mid x \equiv 7 \mod 30\} = \{30n + 7 \mid n \in \mathbb{Z}\}$$

返回到原始问题陈述，我们只需要考虑给定的不等式。是否存在一个数 x 满足 $x \equiv 7 \bmod 30$ 和 $250 \leq x \leq 300$？哎呀，当然有！我们可以从7开始，加上30的倍数，或者猜测接近300并调整，或者类似的方法。无论你如何做，你会发现 $\mathbf{x = 277}$ 就是我们要找的解。这就是孙武将军在他的部队中的士兵数量。

现在，为了比较，考虑以下可能来自类似问题陈述的同余方程组：

$$x \equiv 3 \mod 4$$
$$x \equiv 2 \mod 6$$

这个同余方程组有解吗？我们上面使用的方法在这里适用吗？如果你尝试一下——尝试“划掉不良候选”方法，或者“合并同余”方法——你会发现

nothing works. 回顾这个系统，你会发现这很有道理。第一个同余要求 x 是4的倍数加3；由于4的倍数是偶数，我们要求 x 是 *odd*。然而，第二个同余要求 x 是6的倍数加2；由于6的倍数也是偶数，我们要求 x 是 *even*。一个解怎么可能同时是奇数和偶数呢？！这显然是不可能的。

Chinese Remainder Theorem告诉我们何时有*guaranteed*解的方程组。它适用于我们上面解决的第一个问题，实际上它告诉我们我们找到的最终结果：有无限多个解，并且它们在模30下都相同。然而，它并没有*not*告诉我们第二个问题有*no*个解。这个定理是*guarantee*，适用于某些情况。当我们面对那些情况时，我们可以对解做出有效的陈述。当我们面临一个*different*情况时，尽管如此，定理对解的存在性做出了*no claim*。现在让我们看看这个陈述，然后进一步讨论它，然后请你的帮助来证明它（两种不同的方式！）

Theorem 6.5.28. *Suppose we are given a system of r-many different congruences. That is, suppose $r \in \mathbb{N}$ and we have r natural numbers, $n_1, n_2, \ldots, n_r \in \mathbb{N}$, and we also have r integers, $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, and the system of congruences is given by*

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_r \mod n_r \end{aligned}$$

(Put another way, the system asks for $x \in \mathbb{Z}$ such that $\forall i \in$ [v24]$\bullet$ $x \equiv a_i \mod n_i$.) **If** *the moduli n_i are* 两两互质*—that is, no two of the numbers n_i share any common factors, besides 1—*__then__ *the system of congruences has a solution.*

Furthermore, in this case, there are in fact 无限多个 *solutions, and they are all congruent modulo N, where N is defined as the product of the moduli:*

$$N = \prod_{i \in [r]} n_i$$

注意，主要结论是“**If**……**then**……”这一陈述。还记得我们关于这种条件语句所说的吗？这个定理提供了*no statement*关于当两个模数互质时会发生什么。在这种情况下可能会发生任何事情！我们上面看到的例子有*non*互质模数：一个同余是在模4下给出的，另一个是在模6下，而4和6有公共因子2。然而，定理并没有说有**no**个解；我们必须自己找出这一点。如果

我们有了changed the numbers slightly and posed the following congru{v*}ences:

$$x \equiv 3 \mod 4$$
$$x \equiv 5 \mod 6$$

T这里 *are* 个该系统的解。你能找到它们吗?

一个中国剩余定理的证明遵循我们解决上述问题的方法。给定一个系统中任意数量的同余，我们可以迭代地将一个结合到另一个中，最终得到一个同余，其模数是所有其他模数的乘积。你认为如何证明这种方法是有效的？一个迭代过程……啊哈，归纳法！是的，你可以通过在给定系统中同余的数量 r 上进行归纳来证明中国剩余定理。这个证明在练习6.7.26中概述。我们喜欢这个证明，因为它还为你提供了解决这类问题的 *technique*，在实践中。

另一个证明是 **constructive**。也就是说，它将定理陈述中的信息结合起来，得到一个数 *define*，这个数是一个解（当然，这也证明了这一点）。这个证明在练习6.7.27中有概述。我们喜欢这个证明，因为它确实是构造性的；它不是通过论证 *why* 某个对象存在来证明存在结果，而是实际上 *produces* 给你。然而，它构造的解与通过执行“排除不良候选者”或“组合同余”方法找到的解 *not* 是相同的。实际上，这是一个有些“不自然”的方法来使用，但它确实 *work* 而不必进行任何归纳过程。为了比较，我们鼓励你完成这个定理的 *both* 证明。然而，如果我们 *had* 推荐一个，我们会建议归纳证明。

Bezout's Identity

这个定理回到了我们关于线性丢番图方程的讨论。在例6.5.26中，我们通过谨慎地应用乘法逆元解决了这样一个特定的方程。除了向您展示这种方法外，我们还指出了一种简单的方法来验证这样的方程是否有解。这个定理精确地描述了当两个变量的线性丢番图方程有解时的情况。它被称为**Bézout's Identity**，以18世纪法国数学家Étienne Bézout的名字命名。

在陈述定理之前，我们需要提供一个定义。你可能已经熟悉它了，但它在定理中扮演着重要角色，因此我们想在这里分享它并提供一些示例。

Definition 6.5.29. *Let $a, b \in \mathbb{Z}$ be given. The* **greatest common divisor** *of a and b is denoted by* 最大公约数(a, b) *and is defined to be the* 最大 *integer that divides both a and b. That is,*

$$\gcd(a, b) \mid a \ \wedge \ \gcd(a, b) \mid b$$

and

$$\forall d \in \mathbb{Z} \bullet \big(d \mid a \wedge d \mid b\big) \implies d \leq \gcd(a, b)$$

我们将假设大家对这一概念有一定了解，或者至少对其有一些直觉。接下来的定理及其证明将不会过多地依赖于对这个概念的彻底理解。此外，任何涉及这个定义或定理的练习都不会要求你们拥有强大的计算能力，或者假设你们对这一概念有任何了解。相反，把这视为你们继续练习吸收新的数学概念 *definitions*、运用这些抽象概念并证明更多事实、发展例子和非例子的一个组成部分。这是一个重要的技能！在陈述并证明定理之前，让我们快速看看这个概念在实际中的应用的一些例子。

Example 6.5.30. 在这些情况中，我们将取两个数并说明它们的最大公约数。通常，实际上找到这样一个最大公约数*find*的合理方法是通过找到这两个数的 **prime factorization**，并适当地将它们结合起来。也就是说，gcd(a, b)是a和b共有的质因数的乘积，因此考虑这些因数可以很容易地告诉我们最大公约数。

在某些情况下，我们将对一般情况下的gcd做出一些陈述，并证明它（或者也许要求你证明它！）这些陈述将仅依赖于我们上面提供的定义。

- 让 $a = 15$ 和 $b = 6$。由于 $a = 3 \cdot 5$ 和 $b = 2 \cdot 3$，我们发现它们只共享因子 3。因此，
$$\gcd(6, 15) = 3$$
- 让 $a = = 30$ 和 $b = = 40$。由于 $a = = 2 \cdot = 3 \cdot = 5$ 和 $b = = 2^3 \cdot = 5$，我们发现它们共享一个2的因子和一个5的因子。因此，
$$\gcd(30, 40) = 10$$
- 一般来说，
$$\gcd(a, b) = \gcd(b, a)$$
这显然是 True，因为 a 和 b 的任何公约数都是 *also*，也是 b 和 a 的公约数。
- $a = 77$ 和 $b = 72$。由于 $a = 7 \cdot 11$ 和 $b = 2^3 \cdot 3^2$，我们发现它们没有公共的质数因子。因此，
$$\gcd(72, 77) = 1$$
- 让 $a = 13$，并让 $b \in \mathbb{N}$ 使得 $a \nmid b$。由于 a 是质数，且 b 不是 13 的倍数，那么 b 不能有 13 作为质数因子，因此，
$$\gcd(13, b) = 1$$
这意味着 a 和 b 是 **relatively prime**。这是一个普遍的事实：
$$a \text{ and } b \text{ are relatively prime} \iff \gcd(a, b) = 1$$

此外，

$$\forall a, b \in \mathbb{N}\text{.}\ a \text{ prime} \implies \big(\gcd(a,b) = 1 \iff a \nmid b\big)$$

现在，我们感觉准备好陈述和证明 **Bézout's Identity**！

Theorem 6.5.31 (贝祖恒等式{v*} 线性组合*of a and b; that is, define*

$$L = \{z \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z}\text{.}\ ax + by = z\} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

Also, define M to be the set of all 乘以$\gcd(a,b)$*; that is, define*

$$M = \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}\text{.}\ z = k \cdot \gcd(a,b)\} = \{k \cdot \gcd(a,b) \mid k \in \mathbb{Z}\}$$

Then,

$$L = M$$

That is, the Linear Diophantine Equation $ax + by = c$ has a solution 仅当 c *is a* 是 *of* 和 $\gcd(a,b)$. 的最大公约数时

多么方便啊！注意，这个定理告诉我们，当线性丢番图方程——$ax + by = c$，给定 $a, b, c \in \mathbb{Z}$——有解时，*precisely*。我们只需要找到 $\gcd(a,b)$ 并确保 $\gcd(a,b) \mid c$。

为了证明这个定理，我们需要证明一个 *set equality*，因此我们将使用一个 *double-containment argument*，这是我们之前多次见过的策略。在这里我们将为您证明其中一个包含关系，另一个留给您作为练习。

Proof. 设 $a, b \in \mathbb{Z}$ 已知。定义 L 和 M 如定理所述。

首先，我们将证明 $L \subseteq M$。设 $z \in L$ 为任意且固定的。

根据 L 的定义，我们知道 $\exists x, y \in \mathbb{Z}$。$ax + by = z$. Let such x, y be given.

由于$\gcd(a,b)$同时整除a和b，我们知道存在$\exists k, \ell \in \mathbb{Z}$，使得$a = k \cdot \gcd(a,b)$和$b = \ell \cdot \gcd(a,b)$。设这样的$k, \ell$为已知。

我们取这些表达式 a 和 b 并将其替换在上面的方程中：

$$z = ax + by = k \cdot \gcd(a,b) \cdot x + \ell \cdot \gcd(a,b) \cdot y = \gcd(a,b) \cdot \underbrace{(kx + \ell y)}_{m}$$

定义 $m = kx + \ell y$。由于 $m \in \mathbb{Z}$，这表明 z 是 $\gcd(a,b)$ 的倍数。

因此，$z \in M$。这表明$L \subseteq M$。

其次，我们必须证明 $M \subseteq L$。……

这是留给读者作为练习6.7.12的内容。 □

现在这个结果已经完成并得到证明，我们知道一个二元线性丢番图方程是否有解。几个练习将要求你确定这样的方程是否有解。为此，只需引用

此结果。如果您被进一步要求对所有解进行 {v*}，请应用我们在示例6.5.26中向您展示的技术。

Challenge Question: 您认为关于*more*的线性丢番图方程比两个变量的情况能说些什么？例如，考虑

$$6x + 8y + 15z = 10$$

这个方程有解吗？有多少个？作为另一个例子，考虑

$$3x + 6y + 9z = 2$$

这个方程有解吗？为什么有或为什么没有？

尝试陈述并证明关于这个的结果。你能将其推广到任意数量的变量吗？

6.5.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 为什么在考虑 n 模 $\mathbb{Z}$ 时，$\mathbb{Z}$ 被划分为几个集合？(2) n 模 $\mathbb{Z}$ 的等价类是什么？

(3) 如何确定两个整数 $x, y \in \mathbb{Z}$ 是否属于 $\mathbb{Z}$ 模 n 的同一个等价类？

(4) 模数算术引理说了什么？为什么它有帮助？我们如何用它来代数地处理同余？

(5) *multiplicative inverse*的一般概念是什么？给定$a \in \mathbb{Z}$和$n \in \mathbb{N}$，如何在$\mathbb{Z}$模n的上下文中确定a的乘法逆元是否存在？

(6) 当 p 是 *prime* 时，$\mathbb{Z}$ 模 p 的等价类集合有什么特殊之处？

(7) 以下同余系统 *guaranteed* 是否可以通过中国剩余定理求解？为什么或为什么不可以？

$$x \equiv 2 \mod 6$$
$$x \equiv 5 \mod 9$$

您能识别这个系统的解吗？(**Hint:** 当然可以！)

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 状态并证明一个用于确定自然数 $x \in \mathbb{N}$ 是否为9的倍数的 *divisibility trick*。

（**Hint:** 参见例6.5.13，了解类似问题。）

(2) 设 $n \in \mathbb{N}$ 和设 $a \in \mathbb{Z}$。证明 $(n-a)^2 \equiv a^2 \bmod n$。

(3) 设 $n \in \mathbb{N} - \{1\}$。证明 $(n-1)^{-1} \equiv n-1 \bmod n$。

(4) 给定每一对值(a, n)，求a模n的乘法逆元，或者说明它不存在。

(a) $a = 5$ 和 $n = 12$ (b) $a = 7$ 和 $n = 11$ (c) $a = 6$ 和 $n = 27$ (d) $a = 11$ 和 $n = 18$ (e) $a = 70$ 和 $n = 84$ (f) $a = 8$ 和 $n = 17$

(5) 描述方程的所有整数解 $x, y \in \mathbb{Z}$

$$4x - 7y = 18$$

(6) 确定 *all* 以下同余方程组的解 影响:

$$x \equiv 3 \mod 5$$
$$x \equiv 4 \mod 7$$

6.6 Summary

作为我们持续构建正式化 **functions** 的部分，我们详细讨论了二元关系。我们定义关系为有序对的集合，并讨论了关系可能具有的几个性质。特别是，*reflexivity*、*symmetry* 和 *transitivity* 的组合产生了一种特别强大的关系，称为 *equivalence relation*。我们看到了关于此类关系的一个有用的定理，它说等价关系与 *partition* 精确对应。在 $\mathbb{Z}$ 上定义的特定等价关系“模 n”下，我们能够利用这些划分并陈述和证明关于整数的一些有趣结果！以下许多练习涉及我们对抽象关系的处理，而其中许多也涉及我们在数论和整数领域的处理工作。

6.7 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的任何内容，以及可能的一些假设的数学知识。当然，我们不期望你解决其中的 **all**，但工作得越多，你将学到越多！记住，没有 *doing* 数学，你无法真正 *learn* 数学。动手解决一个问题。阅读几个陈述，四处走走，思考它们。尝试写一个证明，并向朋友展示，看看他们是否信服。继续练习将你的想法以清晰、精确和逻辑的方式 *write* 出来的能力。写完证明后，编辑它，使其更好。最重要的是，继续 *doing* 数学！

简答题，只需解释或陈述答案，无需严格的*proof*，已用►标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 6.7.1. ► 考虑集合 $A = \{1, 2, 3, 4\}$。对于以下在 A 或 $\mathcal{P}(A)$ 上定义的每个关系，决定它是否是（i）自反的，（ii）对称的，（iii）传递的，（iv）反对称的。

(a) R_a 在 A 中由 $R_a = \{\ (1,2), (2,2), (3,1), (4,2), (3,3)\ \}$ 定义

(b) R_b 在 A 中由 $R_b = \{\ (1,1), (2,2), (3,3), (3,4), (4,3), (4,4)\ \}$ 定义

(c) R_c 在 $\mathcal{P}(A)$ 中由 $\forall S, T \in \mathcal{P}(A)$ 定义。 $(S,T) \in R_c \iff S - T \subseteq \{1\}$

(d) R_d 在 $\mathcal{P}(A)$ 中由 $\forall S, T \in \mathcal{P}(A)$ 定义。 $(S,T) \in R_d \iff S \cap T \subseteq \{1\}$

Problem 6.7.2. 通过设置定义$\sim$上的关系$\mathbb{R}$

$$\forall a, b \in \mathbb{R}\,.\ a \sim b \iff \forall x \in \mathbb{R}\,.\ x > 0 \implies ax^2 + bx > 0$$

对于关系的四个性质——(i) 反身性，(ii) 对称性，(iii) 传递性，(iv) 反对称性——要么证明 $\sim$ 具有该性质，要么通过找到一个反例来反驳它。

Problem 6.7.3. 通过设置定义$\approx$在$\mathcal{P}(\mathbb{R})$上的关系

$$\forall X, Y \in \mathcal{P}(\mathbb{R})\,.\ X \approx Y \iff X - Y \subseteq \mathbb{N}$$

对于关系的四个性质——(i) 反身性，(ii) 对称性，(iii) 传递性，(iv) 反对称性——要么证明 $\sim$ 具有该性质，要么通过找到一个反例来反驳它。

Problem 6.7.4. 在 $\mathbb{Z} \times \mathbb{N} - \{0\}$ 上定义关系 #，通过设定 ing

$$\forall (a,b), (c,d) \in \mathbb{Z} \times \mathbb{N} - \{0\}\,.\ (a,b)\,\#\,(c,d) \iff ad = bc$$

(a) 证明 # 是一个等价关系。

(b) 确定等价类 [(0, 3)] 中的元素。证明你的主张。

(c) 确定等价类 [(2, 3)] 中的元素。证明你的主张。

(d) 确定等价类 [(−2, 2)] 中的元素。证明你的主张。

(e) $(\mathbb{Z} \times \mathbb{N} - \{0\})/\#$ 中有多少个 *many* 等价类?

Problem 6.7.5. 设 $p \in \mathbb{N}$ 为一个奇素数（即 $p \neq 2$）。证明 $p^2 \equiv 1 \bmod 24$。

Problem 6.7.6. 使用欧几里得引理（见引理6.5.25）来证明自然数的素数分解是**unique**。

(注意：我们之前在例5.4.3中证明了素数分解 *exist*，但我们没有证明它们的唯一性。)

Problem 6.7.7. 定义在 $\mathbb{R}$ 上的关系 T，通过设置

$$\forall x, y \in \mathbb{R}\text{.}\ (x, y) \in T \iff \left(\frac{y}{x} \in \mathbb{R} \wedge \frac{y}{x} \geq 0\right)$$

(a) 对于每个 $x \in \mathbb{R}$，令集合 $S(x)$ 为

$$S(x) = \{y \in \mathbb{R} \mid (x, y) \in T\}$$

写下集合 $S(-1)$、$S(0)$ 和 $S(1)$ 是什么。

(b) 使用(a)部分中的三个集合，推导出T是**not**一个等价关系。

(版权) 通过证明 T 既不是自反的也不是对称的来验证此结果。

(d) T 是传递的吗？证明你的说法。

Problem 6.7.8. 考虑以下 *spoof*。确定 *argu- ment* 中的哪个论断是不正确的。然后，提供一个解释（包括一个 **example**），说明为什么该论点的 *conclusion* 也是不正确的。

> 让 $n \in \mathbb{N}$ 和让 $a, b, x \in \mathbb{Z}$。假设 $ax \equiv bx \bmod n$。我们声称我们可以“约去”并推断出 $a \equiv b \bmod n$。
>
> 自从 $ax \equiv bx \bmod n$，根据定义，$n \mid ax - bx$。因此，$n \mid x(a - b)$，所以 $n \mid a - b$。根据定义，那么，$a \equiv b \bmod n$。

Problem 6.7.9. 考虑以下同余方程组 by:

$$x \equiv 1 \mod 2$$
$$x \equiv 2 \mod 6$$

是否**Chinese Remainder Theorem**保证了解的存在X? 你能找到一个解吗?

Problem 6.7.10. 在定义6.5.29中，我们定义了两个整数的
greatest common divisor 是一个 *largest* 整数，它能同时整除这两个整数。

这里，我们希望您证明以下gcd的定义与我们所提供的定义相同**equivalent**。首先，阅读定义：

Definition: 设 $a, b \in \mathbb{Z}$ 为已知。定义 $G(a, b)$ 为 a 和 b 的一个公约数，使得 *all* 的公约数 a 和 b 的公约数能整除它。即，

$$G(a, b) \mid a \ \wedge \ G(a, b)$$

和

$$\forall d \in \mathbb{Z}\textbf{.} \ \big(d \mid a \ \wedge \ d \mid b\big) \implies d \mid G(a, b)$$

现在，证明这个定义是等价的。也就是说，证明

$$\forall a, b \in \mathbb{Z}\textbf{.} \ \gcd(a, b) = G(a, b)$$

Problem 6.7.11. 考虑以下 False（显然！）声明：

Claim: 1 是 3 的倍数。

以下“伪造”的声明有什么问题：

WWTS $1 \equiv 0 \bmod 3$. 注意到

$$\begin{aligned} 1 \equiv 4 &\implies 2^1 \equiv 2^4 \equiv 2 \equiv 16 \implies 2 \equiv 1 \\ &\implies 2 - 1 \equiv 1 - 1 \implies 1 \equiv 0 \end{aligned}$$

Problem 6.7.12. 通过证明 $M \subseteq L$ 完成 Bézout 的恒等式（定理 6.5.31）的证明。（这些集合在定理陈述中定义。）

Problem 6.7.13. 在这个问题中，你将证明定理6.4.12的逆命题。也就是说，你将证明以下内容：**Theorem:** 设$S \neq \varnothing$为一个集合，设R为S上的一个等价关系。等价类集合S/R构成了**partition**的S。

记住，我们使用符号 $[x]_R$ 来表示 **equivalence class cor- responding to** x，它是与 x 相关的 S 的所有元素的集合；即，

$$[x]_R = \{y \in S \mid (x, y) \in R\}$$

在整个问题的各个部分中，我们假设 S 是一个集合，R 是 S 上的一个等价关系，因此 R 是自反的、对称的和传递的。

(a) 设 $x \in S$。证明 $x \in [x]_R$。

(b) 设 $x, y \in S$。假设 $x \neq y$，并假设 $(x, y) \in R$。证明 $[x]_R = [y]_R$。

（**Hint:** 使用传递性。你需要它 *twice*。）

(c) 设 $x, y \in S$。假设 $x \neq y$，并假设 $(x, y) \notin R$。证明 $[x]_R \cap [y]_R = \varnothing$。

（**Hint:** 使用矛盾论证。）

(d) 解释为什么这已经证明了所声称的 **Theorem**。

Problem 6.7.14. 在这个问题中，你将证明6.5.2引理中陈述的除法算法。也就是说，你将证明

$$\forall a, b \in \mathbb{Z}\text{.}\ \exists!\, k, r \in \mathbb{Z}\text{.}\ ak + r = b \wedge 0 \leq r \leq a - 1$$

1. 设 $M = \{\ell \in \mathbb{Z} \mid \ell a \leq b\}$。证明 M 有一个 **maximum** 元素。

2. 令 $k \in M$ 为该最大元素。定义 $r = b - ka$。证明 $0 \leq r \leq a - 1$。

3. 假设 $K, R \in \mathbb{Z}$ 也满足 $aK + R = b$ 且 $0 \leq R \leq a - 1$。证明 $K = k$ 和 $R = r$，从而表明 k, r 是 *unique*。

Problem 6.7.15. 证明引理6.5.8，即$n \mid a - b \iff a$和b在除以n时具有相同的余数

Problem 6.7.16. 证明引理6.5.9。也就是说，证明模n的同余关系在$\mathbb{Z}$上确实是一个等价关系。

（**Hint:**只需证明它是（1）自反的，（2）对称的，和（3）传递的。）

Problem 6.7.17. 此问题要求你证明/反驳关于 **Pythagorean Triples** 的某些陈述，这些陈述是满足 $x^2 + y^2 = z^2$ 的三元组 $(x, y, z) \in \mathbb{N}^3$。

在每个情况下，确定该属性是否必须满足 *necessarily*。如果是这样，证明它。否则，找到一个反例。

(a) 是否必然成立至少有一个 $\{x, y, z\}$ 是偶数?

(b) 是否必然成立，至少有一个 $\{x, y, z\}$ 是3的倍数?

(c) 是否必然成立，至少有一个 $\{x, y, z\}$ 是4的倍数?

(d) 是否必然成立，至少有一个 $\{x, y, z\}$ 是5的倍数?

Problem 6.7.18. 状态并证明一个 *divisibility trick*，用于确定一个自然数 $x \in \mathbb{N}$ 是否是11的倍数。

（**Hint:** 参见例6.5.13，了解类似问题。）

Problem 6.7.19. 注意到有几个“小”素数与4同余3；例如$3, 7, 11, 19, 23, 31 \equiv 3 \bmod 4$。在这个问题中，你将证明实际上存在*infinitely many*个这种形式的素数！

（您可能会注意到这个证明的步骤与我们证明存在无限多个素数的证明非常相似！）

(a) 假设 $n \in \mathbb{N}$ 和 $n \equiv 3$ 模 4。证明必须存在一个素数 p 满足 $p \equiv 3$ 模 4 和 $p \mid n$ 。

((**Hint:** $3 \equiv -1$ 模 4.)

(b) 现在，在AFSOC中，只有*finitely*个素数满足$p \equiv 3$ mod 4。让我们定义这些特定素数的集合为$P = \{p_1, p_2, \ldots, p_k\}$，其中$p_k$是最大的这样的素数。

定义新数字 $N = p_1 \cdot p_2 \cdot p_3 \cdots p_k$。

解释为什么 N 必须是奇数，以及为什么 N 严格大于特定集合 P 中的所有素数。

(c) 定义 M 为在 N 之后，与 3 同余于 4 的下一个最大数。解释为什么 $M - N$ 要么是 2，要么是 4。

(d) 解释为什么，在两种情况下（$M - N$ =^2 或 $M - N$ =^4），可以得出结论：*none* 是 N 的质因数中的一个，也可以是 M 的质因数。

(**Hint:** 回想一下 $a \mid b \wedge a \mid c \implies a \mid (b \pm c)$ 。)

(e) 使用你至今已证明的内容来解释为什么 M 必须是质数。

(f) 我们达到了什么矛盾？得出结论。

Problem 6.7.20. 模仿前一个问题6.7.19的细节，证明也存在无限多个与6同余5的质数。

Problem 6.7.21. 在这个问题中，你将证明MIRP引理6.5.24的第二结论。具体来说，你将证明以下命题：

设 $a \in \mathbb{Z}$ 和 $n \in \mathbb{N}$ 已知，并假设 a 和 n 是 *not* 互质的。那么，方程 $ax \equiv 1 \bmod n$ 没有解 $x \in \mathbb{Z}$。

(a) 我们假设 a 和 n 不是互质的。这又意味着什么?

(b) AFSOC ЧТО $\exists x \in \mathbb{Z}$, $ax \equiv 1 \bmod n$ and let such an x be given.

使用此功能来编写一个 *equation* (而不是一个 *congruence*)，其中包含 a, x, n。

(c) 从(a)部分调用你的知识并重新写下方程。

(d) 你发现了什么矛盾?

Problem 6.7.22. 对于以下每个主张，确定它是 True 还是 False。如果是 True，则证明它；如果是 False，则找到一个反例。

(a) $\forall x, y \in \mathbb{Z}$。

$(x + y)^2 \equiv x^2 + y^2 \bmod 2$ (b) $\forall x, y \in \mathbb{Z}$

- $(x + y)^3 \equiv x^3 + y^3 \bmod 3$

(c) $\forall x, y \in \mathbb{Z}\text{.}\ (x+y)^4 \equiv x^4 + y^4 \mod 4$

(d) $\forall x, y \in \mathbb{Z}\text{.}\ (x+y)^5 \equiv x^5 + y^5 \mod 5$

(e) $\forall x, y \in \mathbb{Z}\text{.}\ (x+y)^6 \equiv x^6 + y^6 \mod 6$

Challenge: 你能对哪些 n 的值使得以下陈述 True 成立做出猜想吗?

$$\forall x, y \in \mathbb{Z}\text{.}\ (x+y)^n \equiv x^n + y^n \mod n$$

你能 **prove** 吗? 你还能描述一下哪些 n 的值会使陈述 False 成立吗?

Problem 6.7.23. 判断方程是否有任何整数解 $x, y \in \mathbb{Z}$

$$3x^2 - 5y^2 = 2$$

(**Hint:** 使用乘法逆元和二次剩余.)

Problem 6.7.24. 证明方程没有整数解 $x, y \in \mathbb{Z}$

$$3x^2 - 5y^2 = 15$$

Problem 6.7.25. 对于以下每个方程，识别所有整数解集 $x, y \in \mathbb{Z}$，或者解释为什么不存在这样的解。

(a) $2x + 4y = 9$ (b)
$18x - 15y = 21$ (c)
$6x - 15y = 17$ (d) 6
$x - 15y = 33$

Problem 6.7.26. 在这个问题中，你将通过 *induction* 证明中国剩余定理（定理6.5.28）。然后，你将应用在证明中开发的迭代方法来解决一个特定的同余方程组。

(a) 假设我们有两个同余式需要同时求解

$$x \equiv a_1 \mod n_1$$
$$x \equiv a_2 \mod n_2$$

n_1, n_2 是互质的。

使用“模”的定义，从这些同余式中写出两个 **equations**。将这些方程代数组合起来，推导出 **one** 同余式，即写成模 $n_1 n_2$。

(b) 假设 n_1, n_2 互质，推导出 $n_2 - n_1, n_1 n_2$ 也互质。

（**Hint:** 您需要欧几里得引理6.5.25。）

(c) 推导出你可以写出单个同余 $X \equiv \underline{\text{mod}}\ n_1 n_2$。

这已经证明了基本案例：我们可以将两个同余合并为一个。

(d) 现在，证明归纳步骤：

假设 $r \in \mathbb{N} - \{1\}$，并且我们有 r 个自然数，$n_1, n_2, \ldots, n_r \in \mathbb{N}$，它们两两互质。（也就是说，除了 1 之外，这些数没有其他公共因子。）假设我们还有 r 个整数，$a_1, a_2, \ldots, a_r \in \mathbb{Z}$。

我们将让你证明

$$\exists X \in \mathbb{Z}\,.\ \forall i \in [r]\,.\ X \equiv a_i \mod n_i$$

通过 r 的归纳，给出了公理的数量。

使用你在这个问题中已经证明的，将这个表达式重写为包含 $r-$ 个 1 同余的方程组。

(e) 解释为什么这已经通过归纳证明了同余定理。

(f) 现在，考虑以下同余方程组：

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$

应用上述证明生成的迭代方法来解决该系统。

Problem 6.7.27. 在这个问题中，你将通过一种 *constructive* 方法证明中国剩余定理（定理6.5.28）。然后，你将应用这种方法来解决一个特定的同余方程组。

假设 $r \in \mathbb{N}$，并且我们有一些自然数 r，$n_1, n_2, \ldots, n_r \in \mathbb{N}$，它们是两两互质的。（也就是说，除了1之外，这些数没有其他公共因子。）假设我们还有一些整数 r，$a_1, a_2, \ldots, a_r \in \mathbb{Z}$。

我们将让你证明

$$\exists X \in \mathbb{Z}\,.\ \forall i \in [r]\,.\ X \equiv a_i \mod n_i$$

通过帮助您定义这样的 X 并证明它确实满足所有同余关系。

在整个问题中，我们使用定理陈述中定义的 N:

$$N = \prod_{i \in [r]} n_i$$

(a) 对于每一个 $i \in [r]$，定义 $N_i = \frac{N}{n_i}$。解释为什么 n_i 和 N_i 是互质的。

(b) 引用一项结果，该结果保证（对于每个 $i \in [r]$）存在一个整数 y_i 满足 $y_i N_i \equiv 1 \bmod n_i$。

(c) 定义

$$X = \sum_{j=1}^{r} a_j N_j y_j$$

我们的目标是证明对于每个 $i \in [r]$，有 $X \equiv a_i \bmod n_i$。

设 $i \in [r]$ 为任意且固定的。证明对于每一个 $j \neq i$，上述求和中的对应项与 n_i 同余于 0；即证明

$$\forall j \in [r] \,.\, j \neq i \implies a_j N_j y_j \equiv 0 \mod n_i$$

(d) 取 i 为与上一部分相同的固定值。现在，证明当 $j = i$ 时，上述定义 X 的和中的对应项与 a_i 在模 n_i 下同余；即证明

$$a_i N_i y_i \equiv a_i \mod n_i$$

(e) 使用你刚刚证明的内容来解释为什么 X 满足 *all* 的 r-多个同余。

奖金 证明 **CRT** 的第二个结论，即所有解在模 N 下同余。

(f) 现在，考虑以下同余方程组:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$

这是，$n_1 = 3, n_2 = 5, n_3 = 7$，和 $a_1 = 2, a_2 = 2, a_3 = 4$.

根据上述步骤中的定义，找到 N、N_i 和 y_i (对于每个 $i \in [3]$)，并使用这些来找到一个解 X。

(g) 使用 **CRT** 的另一个结论，用集合表示法写下前一部分给定系统的 *all* 解集，并利用此找到 **smallest** 个自然数解。

Problem 6.7.28. 以下谜题由印度数学家**Brahmagupta**在7世纪提出。（这正好说明人们已经思考过这类问题数千年了！）

阅读它并使用故事来表述一个同余方程组。

然后，解决问题！

（**Hint:** 我们建议一种迭代方法，因为中国剩余定理在这里不适用，正如问题所陈述的。[为什么不行？] 你能否在方法的第一步变得聪明一些，以便中国剩余定理 *does* 然后适用？）

> 一位妇女从市场上回来，手里提着一篮鸡蛋。突然，一个路过的人撞到了她，把鸡蛋篮子撞到了地上。所有的鸡蛋都碎了！
>
> “非常抱歉！”男人说。“请允许我走到市场给你买更多的鸡蛋来替换这些。你有多少个？”
>
> 这位女士看着地面，只发现一堆混乱的贝壳、蛋黄和泥土。在这里简单地数它们毫无希望。
>
> “我不太记得了，”她对那个男人说，“但我确实记得这些事实：
>
> 我首先尝试将鸡蛋成对计数，但剩下了一个。然后我用三来计数，剩下两个。接着我用四来计数，剩下三个。然后用五来计数，剩下四个。再用六来计数，剩下五个。最后，当我用七来计数时，它们可以整除，所以我那样把它们堆在篮子里。唉，我不记得有多少组是七的。”
>
> “没关系，”那人笑着回答。“你已经告诉我足够多了。我知道你有多少鸡蛋，我将在几分钟内回来，带同等数量的鸡蛋，再加上一块甜面包作为对你的补偿。”他朝女人笑了笑，转身走向市场。
>
> 这位女士在那里站了几分钟等待，在这段时间里，她也算出了自己买了多少个鸡蛋。
>
> 有多少鸡蛋?

Problem 6.7.29. **Challenge:** 等价关系研究

(a) 假设 R 和 S 是集合 A 上的等价关系。假设 $A/R = A/S$ (，即每个等价关系下的等价类集合是相同的)。证明实际上$R = S$。

(b) 假设 R 和 S 是集合 A 上的等价关系。$R \cap S$ 必须是等价关系吗?

(c) 假设 R 和 S 是集合 A 上的等价关系。$R \cup S$ 必须是等价关系吗?

(d) 假设 R 和 S 是集合 A 上的等价关系。定义关系的 *compo- sition* 为

$$S \circ R = \{(x, z) \in A \times A \mid \exists y \in A \mathbf{.}\ (x, y) \in R \wedge (y, z) \in S\}$$

必须 $S \circ R$ 是一个等价关系吗?

(e) 假设 R 和 S 是集合 A 上的等价关系。回忆 A/R 和 A/S 是 A 的 *partitions*。

我们称一个划分 $\mathcal{F}$ **refines** 与一个划分 $\mathcal{G}$ 相等，当且仅当

$$\forall X \in \mathcal{F} \mathbf{.}\ \exists Y \in \mathcal{G} \mathbf{.}\ X \subseteq Y$$

证明以下公式：{v*}

$$R \subseteq S \iff A/R \text{ refines } A/S$$

6.8 Lookahead

我们现在准备正式讨论**functions**。我们已经发展了必要的背景知识、术语和符号，不仅能够从数学上定义函数，还能讨论它们的各种性质并证明一些强大的定理。尽管我们的等价关系和数论探索可能看起来是出于好奇心而非实用性，但这远非事实！我们讨论的一些数论结果将在下一章讨论整数和其他集合的进一步性质时有用。此外，我们还将能够讨论等价类集合上的函数，例如。本质上，不要觉得我们做的事情是独立的结果。正如我们所意识到的，所有数学都是某种程度上的联系！首先，我们将看到**function**只是**relation**的一种特殊类型……

Chapter 7

Functions and Cardinality: Inputs, Outputs, and The Sizes of Sets

7.1 Introduction

我们正在继续我们的两章函数开发。在本章中，我们将正式定义一个函数 *define*。具体来说，我们将看到函数实际上是一种具有特定性质的 **relation**。这就是我们一开始花时间探索关系的原因——当然，除了它们本身有趣且有用之外。在定义函数之后，我们将通过许多例子和证明来探索函数可能具有的性质。在这个探索中，我们将使用我们迄今为止开发的所有概念，特别是第4.9节中的证明技术。

稍后在本章中，我们将使用 *bijective* 函数的概念——本质上，是两个集合元素的“配对”——来讨论集合的“大小”以及如何比较它们。这个主题，*cardinality*，将向我们展示一些相当引人注目且反直觉的关于无限集合的事实。它还将为我们提供进入下一章的途径，在那里我们将我们的关注点限制在有限集合以及如何计数它们。

7.1.1 Objectives

以下本引言的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作将如何有所帮助，它们将激励我们为什么要关注本章中出现的话题，并且它们将告诉您我们的目标以及您在阅读时应该注意什么以实现这些目标。现在，我们将通过一系列来为您总结本章的主要目标。

语句。这些描述了你在本章结束时应该掌握的技能和知识。以下各节将更详细地重申这些观点，但这将为你提供一个供未来参考的简要列表。当你完成本章的学习后，回到这个列表，看看你是否理解了所有这些目标。你明白为什么我们把它们列为重要吗？你能定义我们使用的所有术语吗？你能应用我们描述的技术吗?

By the end of this chapter, you should be able to ...

- 定义一个函数，并提供许多示例。
- 非正式描述和函数的视觉图示，并利用它们构建关于函数及其性质的例子（和非例子）的正式论证。
- 定义函数中集合的像和原像，并证明这些运算的各种性质。
- 函数的几个性质，以及应用相关技术来确定和证明给定的函数是否具有这些性质。
- 找到两个函数的复合，认识如何利用这种方法创建新的函数，并识别和证明这种复合对相关函数性质的影响。
- 描述双射函数与逆函数之间的关系，并利用此解决问题和证明命题。
- 使用双射来定义集合的基数并证明关于这些基数的主张。
- 说明有限集、可数无限集和不可数无限集之间的区别，并分别提供每种类型的几个例子。

7.1.2 Segue from previous chapter

上一章中的重要思想，在本章中也将有所帮助，就是 **relation** 的概念。正如我们之前提到的，我们将看到 **function** 只是一种特定的关系。这将在我们关于函数的正式定义中出现。

上一章探讨的其他想法——等价关系和数论结果——在本章中不会如此明确地出现。也就是说，我们在这里探讨的函数的例子及其性质，并不依赖于上一章探讨的其他想法。相反，我们将使用这些想法在这里创建有趣的例子和练习。

7.1.3 Motivation

如我们在上一章中提到的，你很可能对函数是什么以及如何与之打交道有一个直观的理解。这可能是来自其他数学课程中的先前工作，或者可能是某些计算机编程。正如我们一直强调的，我们想要正确、正式地定义我们工作中使用的概念。函数也不例外！通过完成这项工作，我们将能够更好地讨论一些你可能之前见过但无法表达的功能的定性属性。正如上面提到的，函数的特定属性将使我们能够讨论集合的*cardinalities*。请放心，如果我们首先不探索函数，我们就无法对这个主题进行适当的讨论！

7.1.4 Goals and Warnings for the Reader

我们希望重复上一章中提到的相同警告和建议。我们正在继续探索数学的一些抽象领域。特别是，本章将把您可能熟悉的概念 *visually* 和 *intuitively* 放在一个更加严谨的地位。只要可能，我们将诉诸于我们的集体直觉，但无法避免我们一直在发展的那种抽象思维和问题解决方法。特别是，我们并不总是能够将一个函数与其 **graph** 相关联，这是我们在数学生涯早期了解图的标准（并且很有帮助）方式。此外，在我们对 *cardinality* 的讨论中，一些结果将完全无视您的直觉。真的！我们将看到一些奇怪、反直觉的事实，保持对这些事实的开放心态将有所帮助。

7.2 Definition and Examples

你通常是如何思考函数的？你对它的直观感觉是什么？你实际上会如何用数学对象来{v*}它？你之前尝试过这样做吗？试试吧！思考一下我们已经看到的观点和工具。你能否只用这些概念来传达你通常对*function*的看法？认真试试！首先阅读下几段，因为我们正在为定义做准备，然后尝试自己提出一个。

我们通常认为函数是一种*rule*或*map*，它告诉我们如何将输出值分配给任何给定的输入值。例如，让我们考虑$\mathbb{R}$上的函数，它说$f(x) = x^2$。这个函数“接收”一个实数，并“输出”输入的平方。从某种意义上说，函数f是一种“机器”，它将一个数字转换为其平方；说函数“在$\mathbb{R}$上”意味着我们只能将实数放入机器。然而，我们如何知道什么可以*out*从机器中出来呢？我们的函数的常规解释已经存在缺陷。理想情况下，我们希望在传达函数的所有必要信息时

我们定义它：输入可以是什么，输出可以是什么（不是所有输入*are*必然，而是它们*could*可以是什么类型的对象），以及“规则”是什么。如果你把函数看作一个*map*，那么它就像是如何从一个数字集合（在这种情况下，$\mathbb{R}$）导航到另一个数字集合（在这种情况下，也$\mathbb{R}$）的描述，通过遵循集合之间的某种“道路”（在这种情况下，取第一个数的平方）。在这种解释中，我们仍然想要传达我们刚才提到的一切信息，但我们只是指出，还有其他思考它的方式。

让我们在定义之前先扔进一个“搅局者”。想想这个“规则”，它输入这个班级中的人，输出他们的眼睛颜色。你将如何用$f(x) = \ldots$的形式写下它？这很难！你基本上只能将上一句话完整地重写为“规则”的定义。允许的输入和输出是什么？它们不是实数或整数或任何类似的东西。它们是其他完全不同的东西。然而，这个函数是一个完全合理的函数，我们希望它被我们的定义所涵盖。想想这种情况（实际上并不是）与$f(x) = x^2$在$\mathbb{R}$上的情况有何不同。（你甚至可能会在这里提出异议，这根本不是*function*！那么，有两个人眼睛颜色不同的人怎么办？这个“映射”的输出是什么？哦，天哪！）

好的，现在轮到你了。尝试使用我们在这些前几章中讨论的概念、术语和数学对象来定义一个 *function*。

7.2.1 Definition

这里是我们将要使用的。可能它接近你的定义，也许它们是相同的，也许我们的措辞略有不同。然而，最终，这个定义完美地概括了我们之前对函数的直观概念（将其视为一个*rule*的赋值），但它用我们一直在发展的集合和逻辑语言来表达。这有几个目的：(a)它使函数建立在严谨的基础上，并允许我们自信地在数学意义上使用它们；(b)它允许我们使用数学术语和概念来讨论函数和*prove*等属性；以及(c)它允许我们将函数的概念进行推广，并将其应用于比我们熟悉的数字标准集更抽象的设置。好了，解释到此为止，让我们进入定义。

Definition 7.2.1. *Let A, B be sets. Let f be a* 关系 *between A and B, so $f \subseteq A \times B$. Also, assume that f has the property that*

$$\forall a \in A \bullet \exists ! b \in B \bullet (a, b) \in f$$

(Recall that "$\exists !$" means "there exists a **unique** *...", i.e. "there is one and only one ...")*

Such a relation is called a **function** *from A to B.*

We call A the **domain** *of the function and B the* **codomain** *of the function.*

We write

$$f : A \to B$$

to mean f *is a function* **from** A **to** B.

If $(a, b) \in f$, *then we write*

$$f(a) = b$$

knowing that b *is the* 独特的 *element that satisfies that property for the given* a.

那就可以了！现在把一个 *function* 当作一个 *relation* 来思考可能很奇怪，但实际上它是一种特定的 *set*，就是这样。用这些术语来表述函数，我们可以用集合和关系的语言来谈论它们，但请注意，我们仍然可以使用一些熟悉的符号。知道对于每一个“输入” a (，即 *domain*) 的每一个元素，都有一个 *unique* “输出” b (，即 *codomain*) 的一个元素，我们可以写出 $f(a) = b$ 并知道“=”实际上是一个等式。没有其他 B 的元素可以满足这种关系，因为那个 b 是唯一的。

这部分定义包含了我们上面提到的想法：我们想知道一个函数将“输出”什么 {v*}。这就是指定值域所实现的。例如，用 $f : \mathbb{R} \to \mathbb{R}$ 定义函数 $f(x) = \sqrt{x}$ 没有意义；在定义域中存在一些元素（即负数）的“输出”将是未定义的。（技术上，输出将是一个复数，它不是值域 $\mathbb{R}$ 的元素；但在 $\mathbb{R}$ 的上下文中，我们会认为复数是“未定义”的。）当一个函数被正确定义，并且定义域和值域被指定，并且相关对属于集合的笛卡尔积时，我们说这个函数是 **well-defined**。有时，我们将向您展示两个集合上的一个关系，并要求您判断它是否是一个 *well-defined function*。在这种情况下，我们实际上只是在询问这个关系是否对应于一个正确的函数。

The word “Range”

codomain 这个词可能对你来说很陌生。事实上，你可能更习惯于使用 **range** 这个词来指代函数的潜在“输出”集合。我们想在这个语境中完全避免使用“范围”这个词，因为它可能存在歧义。一些作者和教师使用“范围”这个词来表示我们在这里所说的“值域”：函数的 *potential* “输出”集合。然而，一些作者和教师使用这个词来表示我们在这里所说的“像”。正如你将在第7.3节中看到的那样，这是函数的 *actually-achieved* “输出”集合。一般来说，像是一个值域的子集，但它可能是一个 *proper* 子集。当有人使用“范围”这个词时，他们可能是在考虑这些解释中的一个，但你可能是在考虑另一个！为了避免这种混淆，我们只会使用 *codomain* 和 *image* 这两个词。

7.2.2 Examples

让我们看看一些函数（以及非示例）的例子，使用我们新的定义。在处理这些例子时，我们将描述定义函数和操作它们的适当方法，并描述如何“可视化”一些函数并诉诸我们的直觉。

Notation

有几种正确定义函数的方法。以下都是定义“实数上的平方函数”的可接受方式：

Let $f \subseteq \mathbb{R} \times \mathbb{R}$ be the function defined by $(x, y) \in f \iff y = x^2$.
Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f = \left\{(x, x^2) \mid x \in \mathbb{R}\right\}$.
Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $\forall x \in \mathbb{R}\text{.}\ f(x) = x^2$.

考虑每个这些如何符合我们上面看到的 *function* 的定义。第一个直接符合函数是一种从 $\mathbb{R}$ 到 $\mathbb{R}$ 的 *relation* 的观点。第二个使用相同的概念，但用集合构造器符号而不是 *if and only if* 表达 f。第三个符合每个 f 的“输入”都有一个 *unique* “输出”的观点，因此我们可以简单地声明那个“输出”是 *for all* $x \in \mathbb{R}$。

我们将 *usually* 坚持第三种表示法，因为它更容易理解，并且更直接地符合我们对函数的直觉。有时，我们会使用其他表示法；我们可能试图强调函数的底层结构，或者根据上下文，这可能更容易书写。不过，在定义函数时，我们需要向读者指定所有重要的组成部分：*domain*、*codomain*、*letter name*，以及一个将有序对分配的 *rule* 或 *set*。

如果你想知道为什么在定义函数时指定*codomain*如此重要，那么从编写计算机代码的角度来考虑。如果你定义一个函数，你通常需要*declare*输出变量的对象类型。（当然，这取决于语言。）例如，在Java中，你可能写成

```
public int PlusOne (int x) {
    return x+1;
}
```

这定义了一个函数，它输入一个整数，加一，然后输出另一个整数。注意，你必须告诉程序 *going in* 是什么类型的对象，以及 *coming out* 将是什么类型。

Example 7.2.2. 考虑一个函数，它接受一个自然数并输出其二进制表示。让我们用 B 来表示这个函数。进行一些计算，我们发现我们想要 $B(1) = 1$ 和 $B(2) = 10$ 和 $B(10) = 1010$，例如。这个函数的定义域是什么？值域是什么？能否

你把它定义得严密的“规则”写下来了吗？难道不是更好直接按照我们所说的那样，用文字表述吗？

我们将会以下方式定义此函数。设S为所有有限二进制字符串的集合，即由0和1组成的序列。然后我们定义函数$B : \mathbb{N} \to S$如下：

$$B = \{(n, s) \mid n \in \mathbb{N} \text{ 并且 } s \text{ 是的二进制表示 } n\}$$

Example 7.2.3. 再次考虑“平方函数”：令$f : \mathbb{R} \to \mathbb{R}$由$\forall x \in \mathbb{R}$定义。

- 让$g : \mathbb{R} \to \mathbb{C}$是由以下函数定义的

$f(x) = x^2$. Is this function any different from the following functions?

$$\forall x \in \mathbb{R}.\ g(x) = x^2$$

- 让$h : \mathbb{Z} \to \mathbb{R}$是由以下函数定义的

$$\forall x \in \mathbb{Z}.\ h(x) = x^2$$

函数g的值域不同，但实际上是$\mathbb{R} \subseteq \mathbb{C}$。所有的有序对$(x, x^2) \in g$仍然满足$x \in \mathbb{R}$和$x^2 \in \mathbb{R}$。在这种情况下，$f$和$g$是*same*函数，我们可以写成$f = g$。我们将在后面精确地看到两个函数相等意味着什么。现在，只需说，对应于f和g的基本关系具有相同的实数有序对作为元素。函数g理论上对第二坐标中的复数*allows*，但根据域和“规则”的建立方式，这实际上并没有发生。

函数h的定义域不同，且$\mathbb{Z} \subset \mathbb{R}$ (a *proper* 子集)。因此，对应函数f的关系中存在许多有序对，其中*don't*属于对应函数h的关系。例如，$(1/2, 1/4) \in f$但$(1/2, 1/4) \notin h$。换句话说，$f(1/2) = 1/4$，但$h(1/2)$的概念不是*well-defined*；$1/2$不属于h的定义域。

Example 7.2.4. 我们还可以定义一个函数**piece-wise**。例如，考虑在$\mathbb{R}$上定义的*absolute value function*：

让$a : \mathbb{R} \to \mathbb{R}$是由以下函数定义的

$$\forall x \in \mathbb{R}. \quad a(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

每个域元素都落入*exactly*中的一个情况，因此没有歧义。

“Well-defined” Functions

它并不总是清楚一个定义的关系*is*实际上是一个函数。给定一个提议的定义域、值域和“规则”或集合，我们如何检查这些是否代表一个函数？这正是下一个定义（完全基于我们上面看到的函数定义）所解决的：

Definition 7.2.5. *Given a domain A, a codomain B, and a proposed "rule" for f, then we say f is a* **well-defined function** *if and only if (1) the rule is defined on* 所有 *elements of A, and (2) for every $a \in A$, the rule outputs a* 唯一 *element of the set B.*

让我们在这里用一个例子来说明。在本节的后面，我们将看到一些函数的 *non-examples*，我们还将再次引用 **well- defined** 的这个定义。

Example 7.2.6. 设 $f : \mathbb{Z} \to \mathbb{N}$ 为由以下函数定义

$$\forall z \in \mathbb{Z}\text{.}\ f(z) = |2z + 1|$$

等等，我们怎么能这么肯定 $|2z + 1|$ 将是一个 *natural* 数，对于 *any* 整数 z? 这并不立即明显，但我们能想出办法。

假设 $z \in \mathbb{Z}$ 满足 $z \geq 1$。那么当然 $2z+1 \in \mathbb{Z}$ 和 $|2z+1| = 2z+1 \geq 3$。因此，$f(z) \in \mathbb{N}$。

假设 $z \in \mathbb{Z}$ 满足 $z \leq -1$。那么 $2z + 1 \in \mathbb{Z}$ 和 $2z + 1 \leq -1$。因此，$f(z) = |2z + 1| \geq 1$，所以 $f(z) \in \mathbb{N}$。

假设 $z = 0$。那么 $f(z) = |\text{^}2 \cdot 0 + 1| = 1$，所以 $f(z) \in \mathbb{N}$。

在任何情况下，我们看到定义 f 的"规则"确实产生了一个自然数，它是 *codomain* 的一个元素。此外，它还产生了 *exactly* 这样一个数。因此，这是一个定义良好的函数。

Example 7.2.7. 设 P 为世界上所有人的集合。设 $b : P \to \mathbb{N} \cup \{0\}$ 为定义如下函数

$$b = \{(p, n) \mid p \in P \wedge \text{ person } p \text{ has } n \text{ sisters}\}$$

(请注意，我们在这里使用了一种集合强调的符号风格，以供练习。此外，将数学符号和文字结合起来，如"$b(p)$ =有p个姐妹的人数"，可能看起来有些滑稽.)

这是一个定义良好的函数吗? 我们会说是的。走到某个人（即元素 $p \in P$）面前，问他们有多少个姐妹（即 $b(p)$ 是什么）。他们会告诉你一个非负整数作为回应。而且，他们也不可能告诉你两个 *different* 数。

现在，你可以指出，在当今离婚和再婚的社会中，很多人有 *half-sisters*，并且 $\frac{1}{2} \notin \mathbb{N} \cup \{0\}$。好吧。这是一个合理的观点。但是，在"简化假设"下，每个人都有些 *whole number* 的姐妹，这个函数是有明确定义的。

The Identity Function

Example 7.2.8. 设 S 为任意集合。*Must* 是否存在一个从 S 到 S 的函数? 当然，我们可以想到从 $\mathbb{R}$ 到 $\mathbb{R}$ 的无数函数，但如果 S 只是一些任意集合呢? 我们能保证存在一个从 S 到 S 的函数吗? 这会转

出那个 . . . 是的，我们可以！回想一下我们在讨论关系时考虑的类似问题。（参见示例6.2.9。）我们知道我们总可以在集合 S 上定义 *equality relation*；也就是说，我们可以通过 $(x, y) \in R \iff x = y$ 在 S 上定义 R。这个关系由所有形式为 (x, x) 的有序对组成，对于每个 $x \in S$。这个关系代表一个函数吗？我们只需要检查定义属性：每个输入是否有 *exactly one* 输出？看起来确实如此！集合的任何元素只等于它自己，不等于其他任何东西。因此，R 确实代表一个函数。这是一个足够特殊的函数，我们给它取了一个自己的名字。

Definition 7.2.9. *Let S be a set. The* **identity function** *on S is defined to be the function* ID：$S \to S$ *given by*

$$\forall x \in S \bullet \mathrm{Id}(x) = x$$

这意味着恒等函数“输出与输入完全相同”。（将函数视为一台机器，这是一个懒惰的机器，它什么都不做，只是吐出进入的任何东西。）

有时，我们希望将恒等函数定义为在 *different* 集合上。为了避免这种情况下的混淆，我们将写作 Id_S 来表示“恒等函数 **on the set** S”。

Non-Examples

有时，在解决问题的背景下，我们可能会写下两个集合之间的一组“规则”，并想知道它是否是一个函数。也许我们需要它是一个函数来帮助我们解决问题。那么这个 *fail* 呢？也就是说，我们想要寻找什么来证明一个提议的规则是 *not* 一个函数？回顾 **well-defined function**（的定义，见定义7.2.5)。可能出现三种不同的问题：

- 可能存在定义 **no “output”** 的域元素。
- 可能存在定义 **more than one “output”** 的域元素。
- 可能存在域中的一个元素，对于该元素恰好定义了一个“输出”，但它是 **not** 的一个元素，即 **codomain**。

以下示例说明了这些可能性。

Example 7.2.10. 设 $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 由以下定义

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N} \bullet G(a, b) = a - b$$

这是一个定义良好的函数，因为存在许多定义域元素，其“输出”是陪域的元素。例如，$(5, 10) \in \mathbb{N} \times \mathbb{N}$ 和 $G(5, 10) = -5$，但 $-5 \notin \mathbb{N}$。

Example 7.2.11{v*} 设 W 为英语语言中的单词集合。定义 $A : W \to W$ 为接收一个单词并输出该单词的排列（不是原单词）的过程。这是 **not well-defined** 的几个原因。例如，A(HI) 不存在；同样，A(FUNCTION) 也不存在。此外，注意，例如，A(INTEGRAL) 有多个（即非唯一的）输出：TRIANGLE，ALERTING，ALTERING，...

7.2.3 Equality of Functions

有时，两个函数由不同的“规则”或公式定义，但它们对应于相同的底层关系！从这个意义上说，这两个函数是 **equal**。我们首先想用函数符号来描述这意味着什么，然后我们将使用底层关系和集合符号来证明我们提出的这个想法。

如何两个函数可能是 *equal* 呢？当然，它们的定义域必须相同。如果不是，那么其中一个定义域集合包含一个不属于另一个定义域集合的元素，这是一个问题。（想想看：其中一个函数将在另一个函数为 *undefined* 的元素上定义，所以它们不可能相等）。所以，假设我们有两个集合，A 和 B，以及两个函数，$f : A \to B$ 和 $g : A \to B$。为了使 f 和 g 相等，我们有什么要求？函数的定义特征是对于任何输入，比如说 $x \in A$，都有一个输出 $f(x)$ 和一个输出 $g(x)$。如果 f 和 g 要成为同一个函数，我们最好有 $f(x) = g(x)$！这使得我们可以陈述以下定理。

Theorem 7.2.12. *Let A, B be sets, and let $f : A \to B$ and $g : A \to B$ be functions. Suppose that*

$$\forall x \in A \bullet f(x) = g(x)$$

Then we say f and g are **equal** *as functions, and we write $f = g$.*

这确实是一个 *theorem*。这个想法非常直观，但它并不是函数的 *definition* 的明确部分。因此，我们必须 *prove* 这个想法。为了完成这个证明，我们将考虑属于关系 f 和 g 的有序对。通过证明这些有序对是 *same*，我们可以在 *sets* 的意义上得出 $f = g$。注意，我们正在提出一个 *double-containment* 论证！

Proof. 设 A, B 为集合，设 $f : A \to B$ 和 $g : A \to B$ 为函数。假设

$$\forall x \in A \bullet f(x) = g(x)$$

首先，我们证明 $f \subseteq g$。设 $(a, b) \in f$ 已知。由于 f 是一个函数，这意味着 $f(a) = b$。根据主要假设，$f(a) = g(a)$，因此 $g(a) = b$ 也同样如此。因此，$(a, b) \in g$。这表明

$$(a, b) \in f \implies (a, b) \in g$$

因此，$f \subseteq g$。

其次，我们以类似的方式证明 $g \subseteq f$。设 $(c, d) \in g$ 已知。由于 g 是一个函数，这意味着 $g(c) = d$。根据主要假设 $f(c) = g(c)$，因此，$f(c) = d$ 也同样如此。因此，$(c, d) \in f$。这表明

$$(c, d) \in g \implies (c, d) \in f$$

因此，$g \subseteq f$。

自我们已证明 $f \subseteq g$ 和 $g \subseteq f$，我们可以得出 $f = g$。 □

这为我们提供了一种方便的方法来展示两个函数相等，而无需深入研究其底层关系/集合结构。相反，我们只需展示域中的每个元素在两个函数下都产生相同的输出。让我们看看在几个例子中它是如何工作的。

Example 7.2.13. 设 $A = \{-1, 0, 1\}$。定义函数 $f_1 : A \to \mathbb{Z}$ 和 $f_2 : A \to \mathbb{Z}$ 如下：

$$\forall x \in A \text{.}\ f_1(x) = x \ \wedge\ f_2(x) = x^3$$

让我们证明 $f_1 = f_2$。由于域只包含三个元素，我们可以逐个验证这些输出。注意

$$f_1(-1) = -1 = (-1)^3 = f_2(-1)$$
$$f_1(0) = 0 = 0^3 = f_2(0)$$
$$f_1(1) = 1 = 1^3 = f_2(1)$$

因此，对于每个允许的输入（即 $\forall x \in A$），函数 f_1 和 f_2 有相同的输出（即 $f_1(x) = f_2(x)$）。因此，$f_1 = f_2$。

Example 7.2.14. 设 $B = \{1, 2, 3\}$。定义函数 $g_1 : B \to \mathbb{Z}$ 和 $g_2 : B \to \mathbb{Z}$ 如下：

$$\forall n \in B \text{.}\ g_1(n) = n^3 - n^2 - 6 \ \wedge\ g_2(n) = 5n^2 - 11n$$

让我们证明 $g_1 = g_2$。再次，我们只需考虑三个元素，因此我们可以手动验证所有等式：

$$g_1(1) = 1^3 - 1^2 - 6 = 1 - 1 - 6 = -6$$
$$g_2(1) = 5 \cdot 1^2 - 11 \cdot 1 = 5 - 11 = -6$$

$$g_1(2) = 2^3 - 2^2 - 6 = 8 - 4 - 6 = -2$$
$$g_2(2) = 5 \cdot 2^2 - 11 \cdot 2 = 20 - 22 = -2$$

$$g_1(3) = 3^3 - 3^2 - 6 = 27 - 9 - 6 = 12$$
$$g_2(3) = 5 \cdot 3^2 - 11 \cdot 3 = 45 - 33 = 12$$

因此，$\forall n \in B$。 $g_1(n) = g_2(n)$, and so $g_1 = g_2$.

由于这两个例子中的域“较小”，我们能够逐个检查每个元素。但这并不总是如此。有时，我们必须考虑域中的 *arbitrary* 元素（因为我们要证明的所需性质以“∀”量词开始）并与之合作。实际上，在这个例子中有一个有趣的方法来做这件事，所以现在让我们向您展示它是如何工作的，以了解它是如何运作的。

设 $n \in B$ 已知。由于 $g_1(n), g_2(n) \in \mathbb{Z}$，我们可以考虑它们的差。具体来说，我们看到

$$\begin{aligned} g_1(n) - g_2(n) &= (n^3 - n^2 - 6) - (5n^2 - 11n) \\ &= n^3 - 6n^2 - 11n - 6 \\ &= (n-1)(n-2)(n-3) \end{aligned}$$

(注意：读者可以通过简单地展开三个项的乘积来验证最后一个等式.)

自 $n \in B$ 以来，我们知道 $n = 1$ 或 $n = 2$ 或 $n = 3$。在每种情况下，必须有一个项——要么 $n - 1$，要么 $n - 2$，要么 $n - 3$——为零。因此，

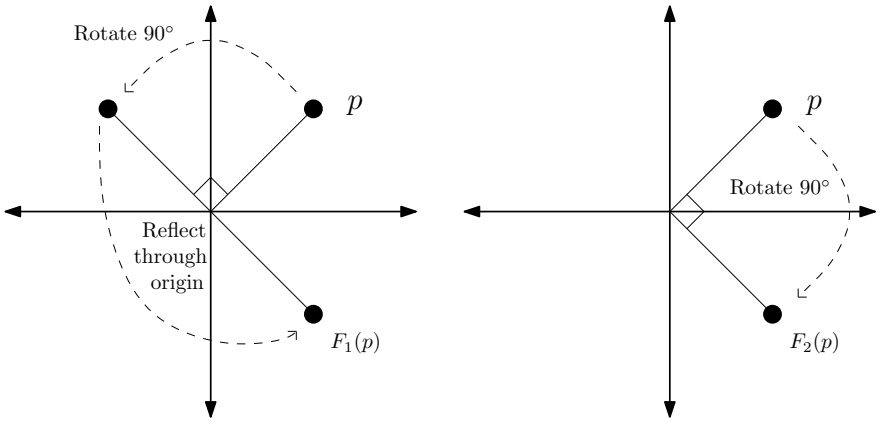
$$g_1(n) - g_2(n) = (n-1)(n-2)(n-3) = 0$$

相应地，通过在两边添加，我们得到 $g_1(n) = g_2(n)$。由于这对于任意的 $n \in B$ 都成立，我们得出结论 $g_1 = g_2$。

我们将会指出，这在这个特定例子中肯定比“检查所有情况”的方法要复杂。我们是如何知道要查看差异的呢？我们是如何知道它会以那种方式分解的呢？！这正是数学如此有趣的原因！我们可能通过思考如何处理一个更一般的问题来检查类似的东西，其中领域太大，无法逐个考虑每个情况。我们可能识别出分解，或者从$B = \{1, 2, 3\}$这一事实中猜测它。如果你仔细思考，你可能会意识到我们是如何想出这个例子的！☺

让我们来看一个更复杂的函数相等性的最终例子。它涉及一些我们没有假设熟悉的概念，我们不会再讨论它们，但我们认为它很有趣且足够说明问题，所以在这里包括它。

Example 7.2.15. 我们在这里将定义两个函数并论证它们是相等的。让每个函数的定义域和值域为 $\mathbb{R}^2$，实平面。现在，让我们通过描述它们的几何作用（即视觉上）来定义两个函数，F_1 和 F_2。我们希望 F_1 输入平面上的一点——让我们称它为 p——然后输出通过以原点逆时针旋转 p 90° 并通过原点反射得到的点。我们希望 F_2 输入 p 并输出通过顺时针旋转 p 90° 得到的点。为了更好地理解这意味着什么，请看以下 F_1 和 F_2 应用到特定点的图示。



我们声称，在函数的意义上，$F_1 = F_2$。通过几个例子进行尝试，我们可以看到这一点*might*是正确的；也就是说，我们无法提出反例，甚至可能开始“看到”为什么它是正确的。但这都不是严格的证明。这只是理解某事的一种直观方式。为了严格证明这一事实，我们需要使用一些超出本课程范围的数学工具。因此，我们实际上只会“概述”这个证明，并将一些技术细节留给感兴趣的读者去探索。

主要思想是这样的：我们可以用 *vectors* 来表示平面上的点，用 *matrices* 来表示函数，用矩阵乘法来表示函数对一个点的操作。如果你对矩阵或向量没有了解，不用担心；你可以直接跳过这个例子，你不会错过任何关键内容！不过，如果你想跟上来，我们可以这样说：矩阵只是实数数组的集合，向量是只有一列的矩阵。例如，实平面上的点 (1, 1) 可以用向量 $\begin{bmatrix}1\\1\end{bmatrix}$ 来表示。向量的 *rotation* 操作可以用一个 *rotation matrix* 来表示。（你可能在电磁学或力学等中级物理课程中看到这个。）例如，逆时针旋转 90° 的操作可以用以下矩阵来表示

$$\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}$$

旋转点 (a, b) 逆时针90° 等于将相应的向量乘以这个矩阵，遵循常规的矩阵乘法规则（其中我们将左边的行乘以右边的列，逐项相乘并相加）。例如，让我们旋转点 (1, 1)：

$$\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix} = \begin{bmatrix}0+(-1)\\1+0\end{bmatrix} = \begin{bmatrix}-1\\1\end{bmatrix}$$

看看这个，它符合我们的预期！查看上面的图片以查看这个旋转的效果。

Simi向右旋转90°可以通过这个m表示 atrix:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

(注意条目中的相似之处，甚至。这有原因，我们将留给你通过一些谷歌搜索来发现。或者，我们猜是必应搜索。)

反射通过原点也可以用矩阵乘法表示，但有一个更简单的方法来考虑它：只需对两个坐标取反。例如，向量$(-1, 1)$通过原点的反射是$(1, -1)$。

这使我们能够完全表示 F_1 和 F_2 的动作。由于 F_1 表示“逆时针旋转 90° 并取反两个条目”，我们可以写成

$$F_1\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = -\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ -a \end{bmatrix}$$

(在前面 $-$ 符号完成否定)，并且由于 F_2 表示“顺时针旋转 90°”，我们可以写出

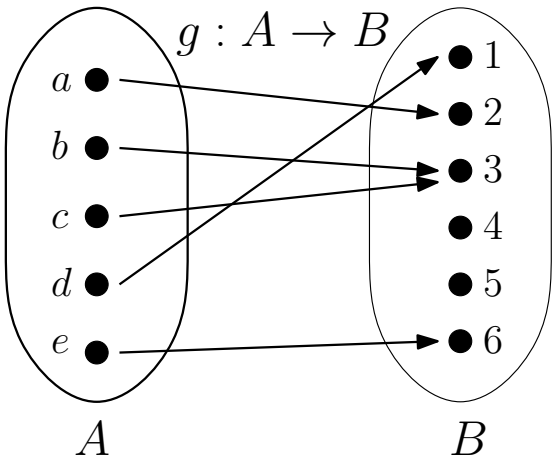
$$F_2\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ -a \end{bmatrix}$$

通过遵循矩阵和向量乘法的规则，我们可以轻松看出这两个表达式对于任何 a 和 b 都是相等的。因此，假设对旋转矩阵有一些了解，这就证明了 $F_1 = F_2$!

7.2.4 Schematics

在继续讨论函数的一些更抽象的性质以及如何证明它们之前，我们将描述一种表示函数的有用方法。我们想强调，这种方法在数学意义上并不是 *rigorous*，并且在这些表示中使用 *proof* 可能不是最好的主意。（例如，在评分作业问题中，即使“有正确的想法”，你可能也得不到满分。）然而，这种方法确实提供了一些关于函数如何工作的直观见解，并可以帮助你发现某些东西，并指导你更严谨地证明它。特别是，这种方法在构建关于函数性质的特定断言的 *counterexamples* 时将非常有帮助。

一个 **schematic diagram** 的概念类似于我们如何使用 *venn diagrams* 来表示集合。集合是一组元素，而不是一张纸上的阴影圆圈，但这些阴影圆圈及其重叠可以帮助我们弄清楚并描述有关集合的某些内容。同样，函数是两个集合上的具有特定性质的关系，而不是像这样：



然而，这以某种方式 *represent* 函数的概念。在这张图中，我们用椭圆形表示了定义域 A，同样也用椭圆形表示了值域 B。A 和 B 的元素用椭圆形内的点表示（并标记了），我们根据函数 $g : A \to B$ 的作用在这些点之间画了箭头。

大多数情况下，这种方法用于探索函数的某个性质，也许可以构造一个反例来反驳某个说法。通过绘制一些点和箭头，并尝试它们如何连接，我们可能可以发展出一个示例的潜在 *structure*；然后，我们可以回头给图中的各个部分命名和公式化，使画面更加严谨。

我们将使用一些示意图来阐述一些性质和概念，但我们始终会伴随一个更严谨的陈述或描述。我们鼓励您采用类似的方法。

7.2.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 写下 **function**、*without* 的定义，查阅它。然后，与我们的定义进行比较。你的定义传达了相同的信息吗？如果不是，你遗漏了什么？

(2) 函数的 **domain** 和 **codomain** 之间的区别是什么？(3) 函数 **well-defined** 的含义是什么？

(4) 什么是 **identity function** 以及它是如何定义的？（5
）我们如何证明两个函数是 **equal**?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 使用适当的符号定义一个函数，该函数输入一个整数并输出其绝对值的平方根。

函数的定义域是什么？它的值域是什么?

(2) 使用适当的符号定义一个函数，该函数输入一对自然数并输出它们的平均值（算术平均值）。

函数的定义域是什么？它的值域是什么?

(3) 设 $A = \{-2, -1, 0, 1, 2\}$。设 $g : A \to A$ 由 $\forall x \in A$ 定义。 $g(x) =$ $x^2 - 3$。判断 g is well-defined or not? Justify your answer.

(4) 设 X 为任意集合。使用适当的符号定义一个函数，该函数输入 X 的一个 *subset* 并输出该集合的补集（在 X 的上下文中）。

函数的定义域是什么？它的值域是什么?

(5) 设 $B = \{-1, 0, 1\}$。设 $h : B \to B$ 由 $\forall b \in B$ 定义。令 $h(b) = b^3$. What special function is this equal to?

(6) 令 $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ 由 $\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}$ 定义。 $f(x, y) = \frac{1}{2}|x + 1| \cdot |y|$. Is this a well-defined function? Why or why not?

7.3 Images and Pre-images

7.3.1 Image: Definition and Examples

回顾函数的定义。我们要求每个输入都有一个唯一的输出。这确保了函数在其定义域上被定义 *everywhere*。那么，关于值域呢？我们只要求所有的 *outputs* 都属于值域。我们从未说过关于“覆盖”值域“多少”的事情。函数的 **image** 的概念正是为了捕捉这个概念。正如我们将从一些例子中看到的那样，即使我们知道值域是什么，确定函数的像也并不总是容易的。正因为如此，我们才首先定义了 *function* 和它的 *codomain*，然后再引入 *image*；所以不要以为我们试图欺骗你或任何东西!

Definition

Definition 7.3.1. *Let A, B be sets and let f $A \to B$ be a function. Let $X \subseteq A$.*

The **image of X under the function f** *is written and defined as*

$$\mathrm{Im}_f(X) = \{b \in B \mid \exists a \in X \bullet f(a) = b\}$$

That is, the image of X under f is the set of all "outputs" that come from "inputs" in the set X.

An equivalent way of writing this is

$$\mathrm{Im}_f(X) = \{f(a) \mid a \in X\}$$

(We will sometimes abbreviate the notation as just $\mathrm{Im}(X)$*, when the function is clearly identified and unambiguous, and consequently refer to the set as just "the image of X", instead of "the image of X under f".)*

When we say **the image of f***, we mean the image of the entire domain, i.e.* $\mathrm{Im}_f(A)$.

注意，这是在定义域的 *any* 子集 $X \subseteq A$ 上定义的，因此我们可以讨论定义域的任何“部分”的像，或者全部的像。现在我们将看到一些例子——稍后会有一些练习——这些例子将考虑严格的子集 $X \subset A$，以及 A 本身。

One Observation

请注意

$$\mathrm{Im}_f(A) \subseteq B$$

no matter what f 并且 A 和 B 是。这遵循 *by definition*，因为我们使用集合构造表示法通过 B 的元素来定义像。在下一节中，我们将探讨当 $\mathrm{Im}_f(A) = B$ 时会发生什么。

现在，让我们练习识别某些函数的图像。在某些情况下，我们将被提供函数及其图像，并要求验证这一说法，但在其他情况下，我们需要开发一些技巧来首先弄清楚图像是什么！

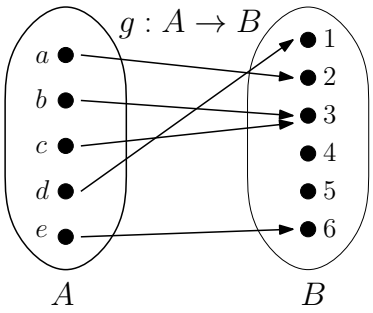
Examples

Example 7.3.2. 定义一个函数 $g : A \to B$ 通过设置 $A = \{a, b, c, d, e\}$ 和 $B = \{1, 2, 3, 4, 5, 6\}$ 和

$$g = \{(a, 2), (b, 3)(c, 3), (d, 1), (e, 6)\}$$

定义 $X_1 = \{a, b, c\}$ 和 $X_2 = \{a, c, e\}$ 和 $X_3 = \{c, d, e \qquad\}$.

您可能会注意到，这正是我们在上一节中定义的与电路图中的相同函数！让我们再次看看这个图，因为它可以帮助我们识别以下列表中的图像。



(1) $\text{Im}_g(\{a\}) = \{2\}$

这是因为 $g(a) = 2$。

注意使用 *set brackets*。我们总是找到 *set* 的像，所以写作 $\text{Im}_g(a)$ 就会是 *incorrect*。

(2) $\text{Im}_g(\{b, c\}) = \{3\}$

这是因为 $g(b) = g(c) = 3$。

(3) $\text{Im}_g(X_1) = \{2, 3\}$

这是因为 $g(b) = g(c) =$^3 和 $g(a) =$^2。

(4) $\text{Im}_g(X_2) = \{2, 3, 6\}$

This is because $g(a) = 2$ and $g(c) = 3$ and $g(e) = 6$.

(5) $\text{Im}_g(X_3) = \{1, 3, 6\}$

这是因为 $g(c) = 3$ 和 $g(d) = 1$ 和 $g(e) = 6$。

(6) $\text{Im}_g(A) = \{1, 2, 3, 6\}$

查看原理图中的集合 B，我们发现这些是唯一被函数“击中”的值。注意 4 , $5 \in B$ 但 $4, 5 \notin \text{Im}_g(A)$，所以 $\text{Im}_g(A) \subset B$ (a *proper* 子集)。

Example 7.3.3. 考虑水在其液态时的温度（以摄氏度为单位）。具体地，定义集合

$$C = \{x \in \mathbb{R} \mid 0 < x < 100\}$$

并且定义函数 $F\colon C \to \mathbb{R}$ 为

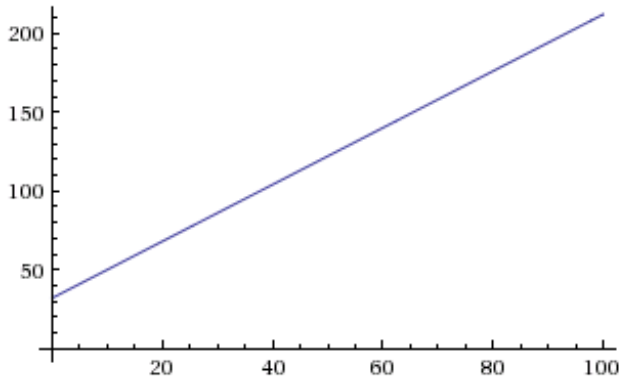
$$\forall c \in C\,.\; F(c) = \frac{9}{5}c + 32$$

什么是 $\text{Im}_F(C)$? 它代表什么?

为了解决这类问题，我们必须（a）通过定义一个集合来识别一个 *claim*，使得 $\text{Im}_F(C)$ 成立，然后（b）证明我们定义的集合实际上是 *equal*

到 $\text{Im}_F(C)$，在集合的意义上。这意味着我们将使用 *double-containment argument*!

Solution: 定义 $S = \{y \in \mathbb{R} \mid 32 < y < 212\}$。 (注意，这代表水在其液态状态下的温度集合（华氏度）。我们声称 $S = \text{Im}_F(C)$。



很难就如何 *come up with* 这样的声明提供建议，通常情况下。通常，这需要一些对函数的尝试和测试一些值，也许还有一些关于函数其他属性的洞察。在这个特定情况下，我们注意到这个函数是 *increasing*；也就是说，如果我们有两个具有 $c_1 < c_2$ 的输入值，那么我们知道 $F(c_1) < F(c_2)$。我们可以从函数的图像（见上面）和/或认识到它是一个 *linear* 多项式中获取这些信息。因此，为了识别图像，我们只需考虑最小和最大的输入值并确定它们的输出。（同样，我们可以从图像中获取这些信息。）我们发现

$$F(0) = 0 + 32 = 32 \quad \text{and} \quad F(100) = \frac{900}{5} + 32 = 212$$

从这一点，我们定义了集合 S。（注意，我们之所以在不等式中使用“$<$”，是因为实际上 $0 \notin C$，即定义域！）我们还给这个集合起了一个名字，这样我们就可以在以后提到它时，而无需隐含地声称它 *is* 映射。这是一个相当微妙的区别，但非常重要！现在，让我们证明我们的主张。

Proof. 首先，我们将证明 $\text{Im}_F(C) \subseteq S$。换句话说，我们将证明函数 F 的每个输出实际上满足 S 定义中的不等式。

（为此，我们将从$\text{Im}_F(C)$的任意元素开始，并利用图像的 *defintion* 将 *domain* 的一个元素引入作用。）

让 $y \in \text{Im}_F(C)$ 为任意且固定的。根据像的定义，这意味着 $\exists x \in C$ 使得 $F(x) = y$。给定这样的 x。

根据C的定义，我们知道$0 < x < 100$。根据F的定义，我们知道

$F(x) = 95\,x + 32$. 由于将一个 *positive* 数乘以并加到两个不等式 *preserves* 的两边，我们可以得出结论

$$\frac{9}{5} \cdot 0 + 32 < F(x) < \frac{9}{5} \cdot 100 + 32$$

并且，简化后，这告诉您

$$32 < F(x) < 212$$

因此，$F(x) \in S$，即 $y \in S$。因此，$\text{Im}_F(C) \subseteq S$。

其次，我们将证明 $S \subseteq \text{Im}_F(C)$。换句话说，我们将证明 S 的每个元素实际上是通过函数 F 以某种方式“实现”的。这相当于证明一个存在性命题，即域 *exists* 中存在某个元素。

设 $s \in S$ 为任意且固定的。根据 S 的定义，我们知道 s 和 $32 < s < 212$。我们需要证明 $\exists c \in C$ 使得 $F(c) = s$.

(通过在旁边做一些复杂的工作，我可以看到 $s \in \mathbb{R}$，并且 $32 < s < 212$，我们提出了以下想法。需要一个证明，设为 s 并解出 c ...)

定义 $c = \frac{5}{9}(s - 32)$。

让我们展示 $c \in C$。通过使用我们关于 s 的信息并操纵不等式，我们观察到

$$\begin{aligned} 32 < s < 212 &\implies 0 < s - 32 < 180 \\ &\implies 0 < \frac{5}{9}(s - 32) < \frac{5}{9} \cdot 180 = 100 \\ &\implies 0 < c < 100 \end{aligned}$$

自 $c \in \mathbb{R}$ 以来，当然，这表明 $c \in C$。

接下来，让我们证明 $F(c) = s$。我们观察到

$$\begin{aligned} F(c) = \frac{9}{5}c + 32 &= \frac{9}{5}\left(\frac{5}{9}(s - 32)\right) + 32 \\ &= (s - 32) + 32 = s \end{aligned}$$

一起，这表明 $s \in \text{Im}_F(C)$，也是如此。因此，$S \subseteq \text{Im}_F(C)$。

总体而言，通过双重包含论证，我们得出结论：$S = \text{Im}_F(C)$。 □

我们证明的第二部分无疑是更难的部分，这种情况对于这类证明通常也是成立的。在提出候选 c 时，我们实际上必须“撤销”函数 F 所执行的过程，并找到对应于我们给定输出 s 的输入 c。在这种情况下，如果函数是对实数进行的数值/算术运算，最佳途径是设置所需的等式，例如

$$\frac{9}{5}c + 32 = s$$

解这个等式以得到 c。这个函数是线性的，所以这个过程只会产生一个这样的 s，但在一般情况下，我们可能期望有多个 s 的值可以工作。最终，我们只需要 *one* 的一个有效值来完成这个证明部分，所以我们只需选择一个有效的 *any* 并将其用作我们的主张。有时，这会使找到这样的值变得更难。这完全取决于具体情况。有时，我们可能正在处理不在数字集合上定义的函数，我们必须使用一些更抽象的洞察力来提出一个候选元素。同样，这完全取决于给定的情况，并且通过实践，你会变得越来越好！

哦对了，我们问这幅图像代表什么！由于该域表示水为液体的温度（摄氏度），因此该图像表示水为液体的温度（华氏度）。

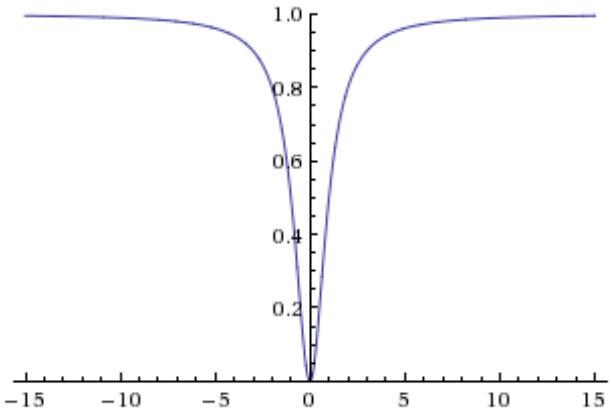
让我们看看另一个证明函数的像是一个特定集合的例子。

Example 7.3.4. 定义 $f\colon \mathbb{R} \to \mathbb{R}$ 通过

$$\forall x \in \mathbb{R}\text{.}\ f(x) = \frac{x^2}{1+x^2}$$

让我们确定图像，$\mathrm{Im}_f(\mathbb{R})$，并证明我们的主张！

这里，我们再次必须使用一些外部策略和直觉来首先识别图像。使用微积分或代数的一些技术，我们可以绘制这个函数的图像并尝试猜测图像。如果您愿意，可以试试。您最终会得到这个图像：



我们也可以认识到分母大于分子，因此随着 x 越来越大，这两个量相对越来越接近。（也就是说，它们的比率趋近于 1。）此外，由于它们涉及平方，两个项都是非负的，所以它们的比率至少为 0。无论如何，我们可以将我们的观察结果拼接起来，并得出以下结论：

定义集合

$$T = \{y \in \mathbb{R} \mid 0 \leq y < 1\}$$

我们断言 $T = \text{Im}_f(\mathbb{R})$。

我们现在遵循与上一个例子中相同的策略。在这样做之前，让我们记住，那个证明的第二部分——证明所声称的集合是像的子集——是更难的部分，并尝试预测那里会发生什么。

在该部分，我们将与一个任意元素 $y \in T$ 进行工作，并希望找到一个满足 $f(x) = y$ 的元素 $x \in \mathbb{R}$。为了找到这样的 x，让我们设置等式并尝试求解 x：

$$\begin{aligned} y = \frac{x^2}{1+x^2} &\iff (1+x^2)y = x^2 \\ &\iff y + yx^2 - x^2 = 0 \\ &\iff (y-1)x^2 = -y \\ &\iff x^2 = \frac{y}{1-y} \end{aligned}$$

现在怎么办？我们能否确保 $\frac{y}{1-y} \in \mathbb{R}$，甚至？我们能否确保它是非负的，因此存在这样的$x$？关于可能存在*two*个根的事实怎么办？在阅读我们的证明之前，考虑这些潜在问题并尝试自己编写这个证明的版本！

Proof. 首先，让我们证明 $\text{Im}_f(\mathbb{R}) \subseteq T$。

让 $y \in \text{Im}_f(\mathbb{R})$ 为任意且固定的。根据像的定义，我们知道 $\exists x \in \mathbb{R}$ 使得 $f(x) = y$。给定这样的 x。

自 $x \in \mathbb{R}$ 以来，我们知道 $x^2 \geq 0$ 和 $0 < x^2 + 1$。然后我们可以推断出 $0 < \frac{1}{x^2+1}$。

通过将前两个不等式相乘——由于所有项都是非负的，我们可以这样做——我们可以得出 $0 \leq \frac{x^2}{1+x^2}$。

接下来，我们知道 $0 \leq x^2 < x^2 + 1$，因此 $\frac{x^2}{1+x^2} <$ 也为 1。（注意：指出 $x^2 \geq$ 为 0 为什么很重要？那里可能会出什么问题？）

这表明 $0 \leq \frac{x^2}{1+x^2} < 1$。由于 $y = f(x) = \frac{x^2}{1+x^2}$，这相当于说 $0 \leq y < 1$。

因此，$y \in T$，因此所以 $\text{Im}_f(\mathbb{R}) \subseteq T$。

其次，让我们证明 $T \subseteq \text{Im}_f(\mathbb{R})$。

让 $y \in T$ 为任意且固定的。这意味着 $y \in \mathbb{R}$ 和 $0 \leq y < 1$。

为了展示 $y \in \text{Im}_f(\mathbb{R})$，同样，我们必须产生一个 x 使得 $f(x) = y$。

我们声称 $x = \sqrt{\frac{y}{1-y}}$ 是有效的。

注意 $y \geq 0$，且 $y < 1$ 意味着 $-y > -1$ 所以 $1 - y > 0$。因此，$\frac{y}{1-y} \geq 0$，并且因此 $x \in \mathbb{R}$ 作为平方根是良好定义的，并且 x 属于定义域 $\mathbb{R}$。

接下来，注意 $x^2 = \frac{y}{1-y}$，以及如此

$$f(x) = \frac{x^2}{1+x^2} = \frac{\frac{y}{1-y}}{1+\frac{y}{1-y}} = \frac{\frac{y}{1-y}}{\frac{(1-y)+y}{1-y}} = \frac{\frac{y}{1-y}}{\frac{1}{1-y}} = \frac{y}{1-y} \cdot \frac{1-y}{1} = \frac{y}{1} = y$$

这表明 $y \in \text{Im}_f(\mathbb{R})$，因此 $T \subseteq \text{Im}_f(\mathbb{R})$。

总体而言，通过双重包含证明，我们得出结论 $T = \text{Im}_f(\mathbb{R})$。 □

注意我们是如何在证明之前解决之前讨论的问题的。是的，存在两个潜在的 x 值可以工作（即，$+$ 和 $-$ 的平方根），但我们只 *needed* 一个，所以我们只选择了一个（正数）并继续使用它。

（问题：如果这个函数仅在非负实数上定义，会怎样？仅对负实数呢？这种限制可能会如何影响我们的选择？）

Example 7.3.5. 考虑由以下公式定义的函数 $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}\text{.}\ p(a, b) = ab + a$$

什么是 $\text{Im}_p(\mathbb{N} \times \mathbb{N})$?

这个例子可能感觉有点棘手，因为域是集合的笛卡尔积；也就是说，p 输入一个自然数的有序对并输出一个自然数。在这种情况下，一个好的方法就是开始输入一些值并观察会发生什么。以下表格可以作为开始的方法，其中左侧列表示 a 的值，顶部行表示 b 的值，表格中的条目是 $p(a, b)$ 的值。

	1	2	3	4	5
1	2	3	4	5	6
2	4	6	8	10	12
3	6	9	12	15	18
4	8	12	16	20	24
5	10	15	20	25	30

它看起来每个自然数都“实现”了函数 p，除了1。具体来说，看看值数组的顶部行：除了1之外，所有自然数都在那里。让我们在下面的证明中使用这个见解。

Proof. Let $V = \mathbb{N} - \{1\}$. We claim $V = \text{Im}_p(\mathbb{N} \times \mathbb{N})$.

首先，我们证明 $\text{Im}_p(\mathbb{N} \times \mathbb{N}) \subseteq V$。设 $n \in \text{Im}_p(\mathbb{N} \times \mathbb{N})$ 为任意且固定的。

这意味着 $n \in \mathbb{N}$ 和 $\exists (a, b) \in \mathbb{N} \times \mathbb{N}$ 使得 $p(a, b) = n$。让这样的 (a, b) 为

给定。

这表示 $n = ab + a$。由于 $a, b \geq 1$，因此 $ab \geq 1$，从而 $n = ab + a \geq 2$。根据 V 的定义，这表明 $n \in V$。

因此，$\text{Im}_p(\mathbb{N} \times \mathbb{N}) \subseteq V$。

(在继续阅读并看到我们的之前，试着写下证明的后半部分！)

其次，我们证明 $V \subseteq \text{Im}_p(\mathbb{N} \times \mathbb{N})$。设 $v \in V$ 为任意且固定的。

这意味着 $v \in \mathbb{N}$ 和 $v \geq 2$. 定义 $(a, b) = (v - 1, 1)$。

注意 $v - 1 \geq 1$，因此 $v - 1 \in \mathbb{N}$，从而 $(a, b) \in \mathbb{N} \times \mathbb{N}$。

此外，请注意

$$p(a, b) = p(v - 1, 1) = (v - 1) \cdot 1 + 1 = v - 1 + 1 = v$$

因此，$p(a, b) = v$，因此 $(a, b) \in \text{Im}_p(N \times \mathbb{N})$。因此，$V \subseteq \text{Im}_p(\mathbb{N} \times \mathbb{N})$。

通过双重包含证明，我们已证明 $V = \text{Im}_p(\mathbb{N} \times \mathbb{N})$。 □

7.3.2 Proofs about Images

您可能通过尝试我们看到的某些示例而观察到以下事实。无论如何，我们可以通过处理图像的定义来证明这个命题。注意，这是一个关于 *arbitrary* 函数的命题；无论 f 是什么，它都成立！

Proposition 7.3.6. *Let A, B be sets. Let f $A \to B$ be a function. Let $S, T \subseteq A$. Then,*

$$\text{Im}_f(S \cap T) \subseteq \text{Im}_f(S) \cap \text{Im}_f(T)$$

Proof. 让 $z \in \text{Im}_f(S \cap T)$ 为任意且固定的。这意味着 $\exists a \in S \cap T$ 使得 $f(a) = z$。给定这样的 a。

自 $a \in S \cap T$ 以来，我们知道 $a \in S$ 和 $a \in T$。

因此，$z \in \text{Im}_f(S)$ 和 $z \in \text{Im}_f(T)$，根据像的定义。

我们根据交集的定义推导出 $z \in \text{Im}_f(S) \cap \text{Im}_f(T)$。

这显示了所需的集合包含。 □

为什么我们没有在这里声称一个 *equality*? 结果证明，等式 *need not hold*，事实上！也就是说，存在至少一个函数，使得逆包含——即，$\text{Im}_f(S) \cap \text{Im}_f(T) \subseteq \text{Im}_f(S \cap T)$——是 False。我们将在下面提供一个这样的函数的例子。

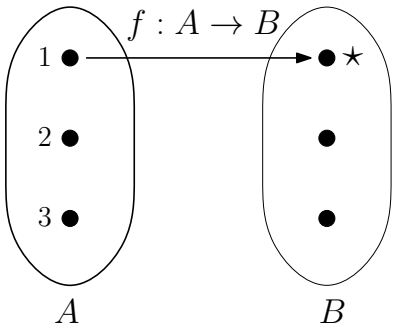
（你应该尝试提出一个函数的例子，其中这个反向包含 *does* 成立。这样，我们就将证明不能得出关于这个包含 *necessarily* 成立的结论！）

我们将使用示意图来用示例 *come up* 具有所需特性的情况。然后我们将使用这个来正式 *define* 一个函数并陈述其特性，指出它们如何与我们的主张相匹配。

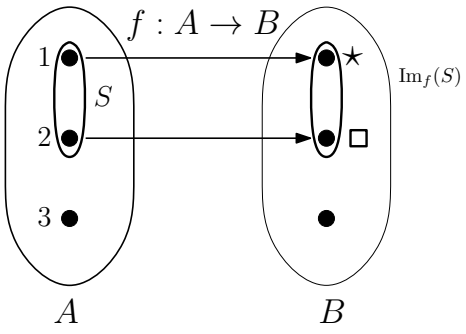
我们想指出，只要你在之后回过头来写下正式的定义，采用这种技术是完全有效的。仅仅提交一个示意图作为“证明”并不够严谨，但这确实可以帮助你的直觉产生富有成效的*ideas*证明！

此外，请记住在这种情况下没有必要构造最 *com- plicated* 或 *interesting* 反例。如果你试图 *disprove* 一个全称量化命题，你只需要 *one* 个有效的例子即可！特别是，不要觉得你需要定义一个与 *numbers* 一起工作的函数，使用某些 *formula*。有时，这实际上会使你的工作更加困难！通常情况下，可以使用只有几个元素（即两个或三个）的集合来构造反例。

Example 7.3.7. 我们声称存在集合 A, B, S, T 和一个函数 $f : A \to B$，使得 $\text{Im}_f(S) \cap \text{Im}_f(T) \not\subseteq \text{Im}_f(S \cap T)$。让我们来找出如何构造这样的例子。根据我们上面的评论，我们将尝试构造一个包含三个或更多元素的集合的例子。让我们从将 A 设为 $\{1, 2, 3\}$ 并定义 $f(1)$ 开始：



现在，为了有一个定义在手，让我们选择 $S = \{1, 2\}$。看起来在 S 中工作两个元素会更合理，所以我们将做出那个选择。此外，看起来我们应该做出 $f(1) \neq f(2)$。否则，$\text{Im}_f(S)$ 将只包含一个元素，那么让 S 有两个元素就没有意义了。所以让我们定义 $f(2)$，以及：

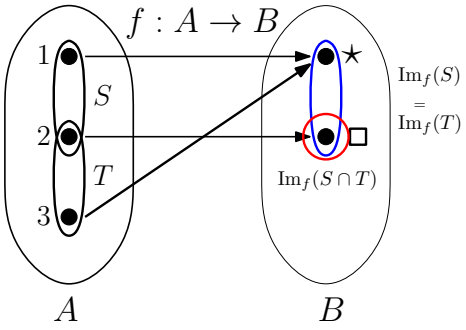


现在，我们需要选择 T。拥有 $S \cap T \neq \varnothing$ 将很有趣，但如果 $T \supseteq S$ 那么处理起来可能很困难。所以，让我们假设 $T = \{2, 3\}$。然后，我们只需选择 $f(3)$。在考虑这些情况时，查看上面的示意图，并想象画一条箭头来表示 $f(3)$。

- 什么如果 $f(3) = f(2) = \square$? 在这种情况下，$\mathrm{Im}_f(T) = \{\square\}$，所以 $\mathrm{Im}_f(S) \cap \mathrm{Im}_f(T) = \{\square\}$。但是 $\mathrm{Im}_f(S \cap T) = \{\square\}$，同样！这不行。

- 如果 $f(3)$ 是其他东西，比如 $f(3) = \smiley$ 呢? 这也不行！我们将有 $\mathrm{Im}_f(S) \cap \mathrm{Im}_f(T) = \{\square\} = \mathrm{Im}_f(S \cap T)$。

- 如果 $f(3) = f(1) = \star$ 会怎样? 看起来这个方法可行!



我们已将其设置为 $\mathrm{Im}_f(S) \cap \mathrm{Im}_f(T)$ 是 $\mathrm{Im}_f(S \cap T)$ 的 *strict* 超集。

回顾我们的构建，看看你是否理解我们的思考过程。我们必须遵守的限制是什么? 我们在哪里有选择自由? 我们决定做什么?

我们想指出，这绝对不是这样的*only*例子，尽管如此！试着想出其他的例子吧!

现在我们只剩下最后一步，就是用我们构建的最终图来 *define* 一个例子，然后证明它有效。开始了!

Proof. 定义 $A = \{1, 2, 3\}$ 和 $B = \{\star, \square\}$。

定义 $f : A \to B$ 通过设置 $f(1) = \star$，以及 $f(2) = \square$，和 $f(3) = \star$。

定义 $S = \{1, 2\}$ 和 $T = \{2, 3\}$。

观察 $S \cap T = \{2\}$，因此 $\text{Im}_f(S \cap T) = \{f(2)\} = \{\square\}$。

然而，观察得知 $\text{Im}_f(S) = \text{Im}_f(T) = B$，因此 $\text{Im}_f(S) \cap \text{Im}_f(T) \neq \{\square\}$。

自 $\star \in \text{Im}_f(S) \cap \text{Im}_f(T)$ 但 $\star \notin \text{Im}_f(S \cap T)$，这证明了我们的主张。 □

我们现在已经看到了一个如何 **prove** 关于任意函数和图像的断言的例子，以及如何 **construct** 一个针对 **disprove** 断言的具体反例。在练习中，你将被要求解决类似的问题。有时，你需要 *figure out* 一个断言是否 True。（在这里，我们 *told* 你哪个断言是有效的。）我们建议尝试以下两种方法之一：（1）尝试证明断言，看看它是否在某个地方崩溃，或者（2）尝试构造一个反例，看看你是否会遇到困难。如果你完成任何一项任务……嘿，你解决了！但如果你感到困难，这可能有助于你弄清楚真正发生的事情。

具体来说，你将被要求检查我们上面讨论的断言，但用“∪”代替“∩”。你认为会发生什么？试试看吧！

7.3.3 Pre-Image: Definition and Examples

一个你可能会问的自然问题是：反过来怎么样？我们能否从*codomain*中取一个子集，并识别出其输出“落在”该集合中的元素？当然可以！接下来的定义为我们提供了这个概念的一个术语，你也会注意到它与*image*的定义有很多相似之处。

Definition

Definition 7.3.8. *Let A, B be sets and let $f : A \to B$ be a function. Let $Y \subseteq B$.*

The **pre-image of Y under the function f** *is written and defined as*

$$\text{PreIm}_f(Y) = \{a \in A \mid f(a) \in Y\}$$

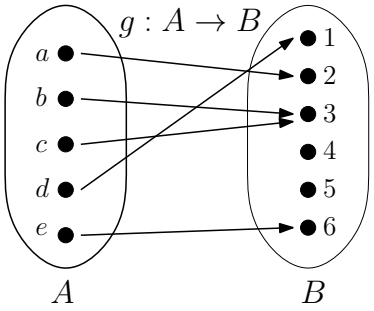
That is, the pre-image of Y under f is the set of all “inputs” that produce an “output” in Y.

(We will sometimes abbreviate the notation as just PreIm(Y) *, when the function is clearly identified and unambiguous, and consequently refer to the set as just “the pre-image of Y”, instead of “the pre-image of Y under f”.)*

首先考虑这个问题：$\text{PreIm}_f(B)$是什么，其中B是整个值域？回顾定义：这是所有输入（在A中）的输出“落在”B中的集合。当然，A中的所有元素都是这样，因为f是一个定义良好的函数！因此，我们实际上只将与集合$Y \subset B$一起工作，因为那些情况更有趣。

Examples

Example 7.3.9. 这个第一个例子使用我们在上一节讨论图像时定义的相同函数。我们将再次向您展示示意图，但不会让您重新定义函数的所有细节。（有关详细信息，请参阅示例7.3.2。）



定义 $Z_1 = \{1, 2, 3\}$ 和 $Z_2 = \{2, 3, 4\}$ 以及 $Z_3 = \{4, 5, 6\}$。

让我们识别以下前像并解释它们。

(1) $\text{PreIm}_g(\{1\}) = d$ 这是因为 $g(d) = 1$ 并且没有 *other* $x \in A$ 满足 $g(x) = 1$。 (注意：这里我们需要使用 *set brackets*。“$\text{PreIm}_g(1)$” 将没有意义。)

(2) 预$\text{Im}_g(\{4\}) = \varnothing$

这是因为 *no* $x \in A$ 满足 $g(x) = 4$

(3) $\text{PreIm}_g(Z_1) = \{a, b, c, d\}$ 这是因为 $g(a) = 2$, $g(b) = g(c) = 3$, 和 $g(d) = 1$, 但没有其他 $x \in A$ 满足 $g(x) \in Z_1$。 (4) $\text{PreIm}_g(Z_2) = \{a, b, c\}$ 这是因为 $g(a) = 2$ 和 $g(b) = g(c) = 3$, 但没有其他 $x \in A$ 满足 $g(x) \in Z_2$。 (5) $\text{PreIm}_g(Z_3) = \{e\}$ 这是因为 $g(e) = 6$, 但没有其他 $x \in A$ 满足 $g(x) \in Z_3$。 (6) $\text{PreIm}_g(\{5\}) = \varnothing$ 这是因为 $\forall x \in A$。 $g(x) \neq 5$.

Example 7.3.10. 设 $f : \mathbb{R} \to \mathbb{R}$ 为由 $\forall x \in \mathbb{R}$ 定义的函数。 $f(x) = x^2$.

让我们用这个函数识别几个前像。我们将让 *you* 了解我们的主张为什么是有效的，以及这次如何解释和证明它们!

(1) 预$\text{Im}_f(\{1\}) = \{-1, 1\}$

(2) 预$\text{Im}_f(\{y \in \mathbb{R} \mid y < 0\}) = \varnothing$

(3) PreIm$(\{y \in \mathbb{R} | y \geq 0\}) = \mathbb{R}$

(4) PreIm$(\{y \in \mathbb{R} | 0 < y < 1\}) = \{x \in \mathbb{R} \mid -1 < x < 1\}$

7.3.4 Proofs about Pre-Images

请注意，以下陈述是 **equality** 之一。将其与命题 7.3.6 进行比较，该命题有关于 *images* 的类似陈述，但它只是一个集合 *containment*。有趣，对吧?

Proposition 7.3.11. *Let A, B be sets. Let f $A \to B$ be a function. Let $X, Y \subseteq B$. Then,*

$$\text{PreIm}_f(X \cap Y) = \text{PreIm}_f(X) \cap \text{PreIm}_f(Y)$$

注意以下证明如何直接引用预像的正式 *definition*。我们将直接进入并证明两部分。练习将要求您用“∪”而不是“∩”来调查这个主张。

Proof. 让 $x \in$ PreIm$_f(X \cap Y)$ 是任意且固定的。

根据前像的定义，这意味着 $f(x) \in X \cap Y$。因此，$f(x) \in X$ 和 $f(x) \in Y$。

自 $f(x) \in X$以来，这意味着根据前像的定义，$x \in$ PreIm$_f(X)$ (。同样，由于 $f(x) \in Y$，这意味着 $x \in$ PreIm$_f(Y)$。

因此，根据交集的定义，我们可以推导出 $x \in$ PreIm$(X) \cap$ PreIm(Y)。

这显示了 PreIm$(X \cap Y) \subseteq$ PreIm$(X) \cap$ PreIm(Y)。

接下来，令 $y \in$ PreIm$(X) \cap$ PreIm(Y) 为任意且固定的。

根据前像的定义，这意味着 $y \in$ PreIm$_f(X)$ 和 $y \in$ PreIm$_f(Y)$。

自 $y \in$ PreIm$_f(X)$ 以来，我们可以根据前像的定义推断出 $f(y) \in X$。同样地，由于 $y \in$ PreIm$_f(Y)$，我们可以推断出 $f(y) \in Y$。

通过交集的定义，这告诉我们 $f(y) \in X \cap Y$。然后，根据前像的定义，这告诉我们 $y \in$ PreIm$(X \cap Y)$。

这显示了 PreIm$(X \cap Y) \supseteq$ PreIm$(X) \cap$ PreIm(Y)。

通过双重包含证明，我们已证明该命题。 □

您可能会阅读这段内容后想，“一个人是如何想出这样的证明的？”嗯，这样的结果并没有太多独创性。我们只是直接引用了定义。从那里一切就位了。

如果你在解决问题时发现自己处于 *stuck* 状态，或者你不确定从哪里开始……就写下相关的定义。尝试将它们应用到你要证明的陈述中。看看会发生什么！

A Proof with Pre-Images and Images

让我们研究一个涉及本节中引入的概念 *both* 的结果。我们将证明一个包含关系，并要求你在练习中 *disprove* 另一个。

Proposition 7.3.12. *Let A, B be sets. Let f $A \to B$ be a function. Let $Y \subseteq B$. Then,*

$$\mathrm{Im}_f\big(\mathrm{PreIm}_f(Y)\big) \subseteq Y$$

Proof. 让 $b \in \mathrm{Im}_f\big(\mathrm{PreIm}_f(Y)\big)$ 为任意且固定的。

根据图像的定义，这意味着 $\exists a \in$ PreIm$_f(Y)$ 使得 $f(a) = b$。Let such an a be given.

自 $a \in$ 预像$_f(Y)$，这意味着 $f(a) \in Y$；根据预像的定义。

自 $b = f(a)$ 和 $f(a) \in Y$ 以来，这意味着 $b \in Y$。

这证明了该主张。 □

7.3.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) **image** 和 **pre-image** 之间的区别是什么?

(2) 假设 $f : A \to B$ 是一个函数。$\mathrm{PreIm}_f(B)$ 是什么?

(3) 假设 $g : \mathbb{R} \to \mathbb{R}$ 是一个函数。为什么表达式 $\mathrm{Im}_g(0)$ 不是一个正确的陈述？你认为这样的表达式的作者想表达什么?

(4) 说 $f : A \to B$ 是一个函数并且 $Y \subseteq B$。如果 $\mathrm{PreIm}_f(B) = \varnothing$，这意味着什么？这是可能的吗?

(5) 说 $f : A \to B$ 是一个函数并且 $X \subseteq A$。如果 $\mathrm{Im}_f(A) = \varnothing$ 是什么意思？这是可能的吗?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 令 $h : \mathbb{R} - \{-1\} \to \mathbb{R}$ 由 $\forall x \in \mathbb{R} - \{-1\}$ 定义

- $h(x) = \frac{x}{1+x}$. Prove that $\text{Im}_h(\mathbb{R} - \{-1\}) = \mathbb{R} - \{1\}$.

Then, define $P = \{y \in \mathbb{R} \mid y > 1\}$ and $U = \{y \in \mathbb{R} \mid y > -1\}$.

Prove that $\text{PreIm}_h(P) = U$.

(2) 设 $f : A \to B$ 为一个函数。设 $S, T \subseteq A$。对于以下每个命题，**prove** 它必须成立，或者通过找到一个 **counterexample** 来反驳它。

(a) $\text{Im}_f(S \cup T) \subseteq \text{Im}_f(S) \cup \text{Im}_f(T)$b) $\text{Im}_f(S \cup T) \supseteq \text{Im}_f(S) \cup \text{Im}_f(T)$

(

(3) 设 $f : A \to B$ 为一个函数。设 $Y, Z \subseteq B$。对于以下每个命题，**prove** 它必须成立，或者通过找到一个 **counterexample** 来反驳它。

(a) $\text{PreIm}_f(Y \cup Z) \subseteq \text{PreIm}_f(Y) \cup \text{PreIm}_f(Z)$ (b) $\text{PreIm}_f(Y \cup Z) \supseteq \text{PreIm}_f(Y) \cup \text{PreIm}_f(Z)$

(4) 回顾命题7.3.12。考虑*reverse*包含：

$$\text{Im}_f\big(\text{PreIm}_f(Y)\big) \supseteq Y$$

Disprove 这个说法是，通过构造一个特定的反例并证明它有效，对于任何函数 $f : A \to B$ 和任何 $Y \subseteq B$ 都成立。

7.4 Properties of Functions

7.4.1 Surjective (Onto) Functions

您现在可能想知道一些事情 . . . 如果我们可以识别给定函数下域的像，为什么还要麻烦一个“比”那个集合“更大”的陪域呢？当然 $f : \mathbb{R} \to \mathbb{R}$ 由 $f(x) = x^2$ 定义是一个很好的函数，但将陪域仅改为非负实数实际上并没有影响什么。这甚至可能使其变得更好，因为陪域中没有任何东西被函数“遗漏”！ 如果您这样想，那么您已经预见了我们接下来的定义，它精确地封装了函数的这一性质：当陪域和域的像相同的时候。

Definition

Definition 7.4.1. *Let A, B be sets and let f $A \to B$ be a function. We say f is a* **surjective** *function if and only if* $\text{Im}_f(A) = B$.

Equivalently, we just say "f is surjective" (adjectival form), or that "f is a surjection" (nounal form).

(The word "onto" is a fairly commonly used synonym for this term, so we will mention it here but won't use it again. This is just in case you've seen this word somewhere else.)

Referring back to the definition of image, we can state this property equivalently in the form of a quantified statement:

$$f \text{ is surjective} \iff \forall b \in B \bullet \exists a \in A \bullet f(a) = b$$

That is, f is surjective if and only if every output has 至少一个 *corresponding input.*

一分钟想想为什么这个定义的第二种形式实际上和第一种是一样的。Im$_f(A) = B$是关于*sets*的一个陈述。我们已经知道，根据定义，$\text{Im}_f(A) \subseteq B$ (图像中的任何东西都不能“超出”陪域)，所以这个额外的属性意味着$B \subseteq$ Im$_f(A)$，也是如此。这正是定义的第二种形式所说的：陪域中的每个元素都满足作为图像元素的界定属性。

此外，请注意定义中没有任何内容说明我们找到的 a 与 b 对应必须是唯一的！这个属性所要求的只是，对于每一个 $b \in B$，我们都可以找到一个满足 $f(a) = b$ 的 *at least one* $a \in A$。可能有多个，也可能恰好有一个。这无关紧要，只要没有 *none*。

什么是*surjection*属性在示意图中的含义？由于函数的值域中的每个元素都被“击中”，这意味着示意图右侧的每个点都有一个进入的箭头。（记住：这种启发式语言可以记住——我们毕竟是在用它来帮助描述这些概念——但这并不构成证明。你在证明中使用的任何此类句子都应该伴随着一个更严谨的陈述，使用数学语言和/或逻辑符号。）我们为什么关心这样的属性呢？一般来说，很难声明函数的像是什么，我们可能（最初）只能声明值域是什么。证明实际上值域的*all*元素是函数的输出，可以提供额外的有用信息！

Negating the Definition

通常，我们定义一个函数然后问：这是一个满射吗？如果我们认为函数 *is* 是一个满射，我们应该通过展示

陪域和像相同。如果我们认为它是 not 一个满射，我们应该通过找到一个 $counterexample$ 来证明它。让我们看看定义满射函数的命题的逻辑否定：

$$\neg(\forall b \in B\text{.}\ \exists a \in A\text{.}\ f(a) = b) \iff \exists b \in B\text{.}\ \forall a \in A\text{.}\ f(a) \neq b$$

这是，为了证明一个函数 f 是 not 满射，我们必须找到一个属于陪域且属于像的元素。这需要一些草稿工作和直觉来识别这样的 b。从那里，我们必须以某种方式证明没有任何可能的 a 满足 $f(a) = b$。我们可能通过取一个任意的 $a \in A$ 并解释为什么 $f(a) \neq b$ 来直接论证这一点。或者，我们可能通过反证法来论证：假设存在一个 $a \in A$ 使得 $f(a) = b$，我们寻求矛盾。这两种方法都是合理的，并且它们在逻辑上是等价的。

Examples

让我们通过一些例子来看看这些技术的实际应用。对于其中一些，我们可能能够利用一些图形直觉或尝试几个测试案例来找出一个 $guess$，但最终我们需要坐下来并 $prove$ 一些逻辑语句来验证我们的主张。

Example 7.4.2. 考虑 p：由 $p(a, b) = ab$ 定义 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$。$p$ 是满射吗？是的，它是！看起来我们只需允许 a 为 1，这样函数就会输出 whatever b 是。让我们用证明使这个观察更加正式：

Proof. 设 $n \in \mathbb{N}$ 为任意且固定的。定义 $(a, b) = (1, n)$。

请注意（$1, n$）$\in \mathbb{N} \times \mathbb{N}$和$p(1, n) = 1 \cdot n = n$。

由于 n 是任意的，这表明 p 是满射的。 □

Example 7.4.3. 设 C 为美国所有汽车组成的集合。设 S 为所有长度最多为7的字母和数字字符串的集合（即这些是您可能在汽车牌照上看到的 $potential$ 字符串）。

让 $f : C \to S$ 通过输入一辆车并输出其车牌字符串来定义。函数 f 是否是满射？

不，绝对不是！如果你不知道的话，$curse\ words$在车牌上是不允许的！所以当然，存在许多你将在美国车牌上看到的字母字符串。（我们将让你自己提供一些例子……）

因为我们已经展示了一个元素 S，它是 $\text{Im}_f(C)$ 的一个元素 not——或者至少，you 考虑了一个例子——我们已经表明 f 是 not 一个满射。

Example 7.4.4. 设 $d : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ 为由以下函数定义

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}\text{.}\ d(a, b) = a - b$$

让我们确定 d 是否是满射并证明我们的主张。我们可能从尝试输入变量 a 和 b 的“小值”开始。在下面的表中，左侧列是 a，顶部行是 b，条目是 $d(a,b) = a - b$：

	1	2	3	4	5
1	0	-1	-2	-3	-4
2	1	0	-1	-2	-3
3	2	1	0	-1	-2
4	3	2	1	0	-1
5	4	3	2	1	0

它 *looks* 像所有的整数 $z \in \mathbb{Z}$ 都会出现在这个表中。然而，它们并不都出现在某一特定的行或列中。相反，看起来所有的 *non-negative* 整数都出现在第一列，而所有的 *non-positive* 整数都出现在第一行。让我们利用这些观察结果来写一个证明。我们将取一个任意的整数 $z \in \mathbb{Z}$ 并考虑两个 **cases**；如果 $z \geq 0$，我们将做一件事，如果 $z < 0$，我们将做另一件事。只要我们在两种情况下都成功，我们就能证明 d 是一个满射。

Proof. 我们断言 d 是一个满射。令 $z \in \mathbb{Z}$ 为任意且固定的。WWTS

(1) 假设 $z \geq 0$。然后定义 $(a,b) = (z+1, 1)$。我们知道 $z+1 \geq 1$，因此 $z+1 \in \mathbb{N}$。这保证 $(z+1, 1) \in \mathbb{N} \times \mathbb{N}$。

esTranslated Text: es

$d(a,b) = z$. To do this, we consider two cases:

Also, notice that $d(z+1, 1) = (z+1) - 1 = z$.

(2) 假设 $z < 0$。然后定义 $(a,b) = (1, -z+1)$。

自 $z < 0$，我们知道 $-z > 0$，因此 $-z+1 \geq 2$，意味着 $-z+1 \in \mathbb{N}$。这保证了 $(1, -z+1) \in \mathbb{N} \times \mathbb{N}$。

Also, notice that $d(1, -z+1) = 1 - (-z+1) = z$.

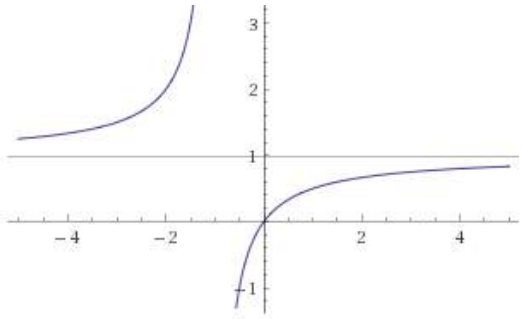
在任一情况下，我们都能定义 $(a,b) \in \mathbb{N} \times \mathbb{N}$ 且 $d(a,b) = z$。由于 $z \in \mathbb{Z}$ was arbitrary, this proves that d is surjective.

Example 7.4.5. 设 $g : \mathbb{R} \setminus \{-1\} \to \mathbb{R}$ 为由以下定义的函数

$$\forall x \in \mathbb{R}\setminus\{-1\}.\ g(x) = \frac{x}{1+x}$$

(注意为什么我们从域中移除了 -1。这确保 g 是一个 *well- defined* 函数！)

让我们确定 g 是否是满射并证明我们的主张。如前所述，我们可以做一些基础工作来弄清楚我们的主张：我们可以尝试插入一些 x 的值，通过让 x 非常接近 -1 或让 x 越来越大来测试“极端情况”……所有这些都可以帮助我们绘制函数的图像，或者我们可以直接使用一些绘图软件：



无论怎样，这一切 **proves** 都没有任何意义！它所做的是帮助我们观察这个函数 g 是 **not** 满射的。似乎在 *horizontal asymptote* $y = 1$ 处有一个 g。也就是说，这个函数 *surjectivity* 永远“达不到”1，而是无限接近。根据我们新的定义 NO，这显然是一个 – 答案！

尝试现在证明这一点。你如何证明元素 $-1 \in \mathbb{R}$ 是 **not** $\mathrm{Im}_g(\mathbb{R})$ 的一个元素？试试看！然后继续阅读我们的证明。

我们将实际上在这里展示 *two* 个证明，供您比较和对比。它们都实现了相同的目标——证明 g 不是满射的——但一个是通过 **contradiction** 方法，另一个是通过 **direct** 方法（使用情况）来做到的。你认为哪个更好？你想到其中之一了吗？哪个更容易阅读？我们对这些问题没有明确的观点；它们都是同样有效的证明！

Proof 1 (Direct). 设 $x \in \mathbb{R} - \{-1\}$ 为任意且固定的。考虑以下两个情况：

- 假设 $x > -1$。这意味着 $x + 1 > 0$，因此 $\frac{1}{x+1} > 0$。我们还知道 $x + 1 > x$ (，这对于每个 $x \in \mathbb{R}$ 都成立.) 通过将这个不等式乘以正项 $\frac{1}{x+1}$，我们得出 $1 > \frac{x}{x+1}$。当然，那么 $g(x) = \frac{x}{x+1} \neq 1$。

- 假设 {v*}1。这意味着 {v*} 1 {v*} 0，因此 {v*} 0。我们还知道 {v*} 1 {v*}。通过将这个不等式乘以负项 {v*} 并改变符号，我们得出 1 {v*} 。当然，那么 {v*} 1。

在任何情况下 $g(x) \neq 1$. 这些情况涵盖了所有可能性，因为 $x \in \mathbb{R} - \{-1\}$ 是任意的（我们也不必考虑 $x = -1$）。这表明

$$1 \notin \mathrm{Im}_g(\mathbb{R} - \{-1\})$$

所以 {v*} 不是一个满射。 □

请注意，这个第一个证明证明了关于图的一个有趣的 *qualitative* 观察：该函数在 $x = -1$ 的左侧位于水平渐近线之上，在 $x = -1$ 的右侧位于渐近线之上。

Proof 2 (Contradiction). AFSOC g 是满射的。这意味着

$$\forall y \in \mathbb{R}\text{.}\ y \in \mathrm{Im}_g(\mathbb{R} - \{-1\})$$

特别地，因此，我们知道 $1 \in \mathrm{Im}_g(\mathbb{R} - \{-1\})$，所以，$\exists x \in \mathbb{R} - \{-1\}$ s.t. $g(x) = 1$. Let such an x be given.

这意味着 $\frac{x}{x+1} = 1$。乘以两边，$g(x) = 1$。Let such an x be given. 我们得到 $x = x + 1$。相减，我们得到 $0 = 1$，显然是一个矛盾 ※

因此，$1 \notin \mathrm{Im}_g(\mathbb{R} - \{-1\})$，所以 g 不是一个满射。 □

注意，这个第二个证明确实证明了 g 不是一个满射，但它并没有提供关于函数如何表现的其他信息（就像前面的证明所做的那样）。

让我们从满射继续前进，讨论函数的一个密切相关性质。

7.4.2 Injective (1-to-1) Functions

当试图证明一个函数是满射时，我们取了陪域的一个任意元素，并必须找到与原始元素相对应的定义域中的 *at least one* 元素。有时存在这样的元素，有时存在多个，有时则不存在。我们现在要考虑那些属于“*exactly one*”情况的函数。在这里，我们不会假设函数已经是满射的。相反，我们施加这个条件：我们希望对于任何给定的输出都有一个 *no more than one* 输入。可能恰好有一个，也可能没有，但肯定不是两个或更多。这类函数足够特殊，以至于我们给它们一个名字。

Definition

Definition 7.4.6. *Let A, B be sets and let f $A \to B$ be a function. We say f is an* **injective** *function if and only if it has the property that*

$$\forall a_1, a_2 \in A\text{.}\ a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Equivalently, we just say “f is injective” (adjectival form), or that “f is an injection” (nounal form).

(The term “1-to-1”—sometimes written “1-1”—is a fairly commonly used synonym for this word, so we will mention it here but won't use it again. This is just in case you've seen this term somewhere else.)

In other words, this defining property requires that “distinct inputs yield distinct

outputs". Also, remembering that the 逆否命题 *of a statement is logically equivalent, we can express this property as*

$$\forall a_1, a_2 \in A \,.\, f(a_1) = f(a_2) \implies a_1 = a_2$$

This expresses the equivalent notion that "if two outputs are equal, they must come from the same input".

考虑这个定义如何传达我们上面描述的概念。假设我们有一个单射函数 {v*} : {v*}，并且我们给出一个元素 {v*}。这个定义是否说明存在一个元素 {v*} 使得 {v*}? 这个定义允许哪些可能性?

Motivation

让我们通过一个特定函数的应用来激发这个概念。将函数想象成你与朋友发送和接收秘密消息的 *code-word machine*。你的朋友写下一条秘密消息，将其放入编码器，然后输出一段混乱的代码，并发送给你。稍后，你收到这段混乱的代码。你可能会想知道，这个代码只来自 *at most one* 输入短语。如果你尝试解码它，它同时出现了 `I HATE YOU` **and** `I LOVE YOU` 两种结果? 那时你该想什么呢? 你的朋友是不是故意要给你发送两条消息? 如果你设计的代码系统将这两条冲突的消息都编码成相同的混乱代码，那可真是个糟糕的系统! 在这种情况下，有一个编码函数，其中两个 *distinct* 输入不可能产生 *same* 输出，那就更好了。这正是注入的定义属性。

Negating the Definition

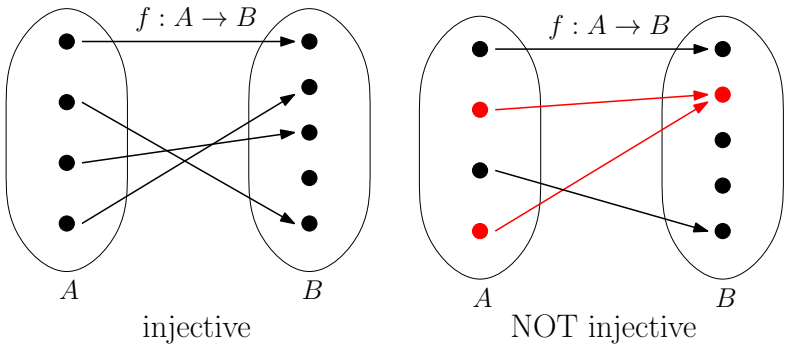
可能有助于从示意图和定义的**negation**方面来考虑*injection*的性质。让我们首先找到那个否定:

$$\begin{aligned}\neg\big(\forall a_1, a_2 \in A \,.\, a_1 \neq a_2 \implies f(a_1) \neq f(a_2)\big) \\ \iff \big(\exists a_1, a_2 \in A \,.\, a_1 \neq a_2 \wedge f(a_1) = f(a_2)\big)\end{aligned}$$

(记住，$P \implies Q$的否定是$P \wedge \neg Q$!)

这表示一个函数是 *not* 单射的，当且仅当我们能找到两个 *distinct* 定义域元素，它们输出 *same* 的陪域元素。

考虑到这一点，以下是一个单射和非单射函数的规范示例:



非单射函数有两个不同的定义域元素输出相同的值域元素，而单射函数避免了这种情况。用这种 *negative* 的方式来表述一个性质可能有点奇怪——一个函数只有在它 *doesn't* 有 . . . 时才是单射——但实际上这在数学中相当常见。（当我们谈到 *infinite* 集合时，我们甚至会看到这个想法，这些集合只是 . . . 集合，它们是 *not* 有限的！）这种负表述很容易记住，我们总是可以将其与另一个正表述联系起来：一个单射函数只有 0 或 1 个输入对应于 *any* 给定的输出。

Examples

让我们思考 *how* 来证明/反证函数的单射性。正如你可能猜到的，上面给出的定义的前两个版本在尝试证明函数 *is* 单射时很有用：取定义域中的两个不同元素并展示它们的输出不同，或者取两个相同的输出并展示它们来自相同的输入。否定也可以用来通过反证法证明函数是单射。此外，第三个版本在证明函数是 *not* 单射时很有用：反例相当于找到两个具有相同输出的不同输入。

让我们通过一些例子来看看这些技术的实际应用。实际上，我们将使用我们在上一节关于满射中看到的一些相同例子！

Example 7.4.7. 考虑 p：由 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 定义。p 是单射吗?

通过尝试一些特定的(a, b)值，我们可以看到p绝对不是一个注入。选择任何有两个不同分解的数，比如$12 = 3 \cdot 4 = 2 \cdot 6$。通过让$(a, b) = (3, 4)$和$(c, d) = (2, 6)$，我们可以轻松证明这个说法。但我们可以通过注意到一个像(a, b) *matters*!这样的元素的坐标的*order*来做这件事，甚至更简单。

Proof. 此函数不是单射的。令$(a, b) = (1, 2)$ 和 $(c, d) = (2, 1)$。注意$(a, b) \neq (c, d)$，因为$1 \neq 2$。另外，注意$p(a, b) = 1 \cdot 2 = 2$ 和 $p(c, d) = 2 \cdot 1 = 2$。因此，$p(a, b) = p(c, d)$。这表明p不是单射的。 □

Example 7.4.8. 设 C 为美国所有汽车组成的集合。设 S 为所有长度最多为7的字母和数字字符串的集合（即这些是您可能在汽车牌照上看到的 *potential* 字符串）。

让 $f : C \to S$ 通过输入一辆车并输出其车牌字符串来定义。函数 f 是否是注入函数?

不，我们不这么认为！相同的车牌字符串可能出现在注册在不同*states*的*different*辆车上。现在，我们手头没有这样的例子，所以这并不是一个完全正式的证明，但希望你能理解这个想法。

我们可以修改函数定义，使其成为*make*一个注入吗？当然可以，我们可以试试！还可以考虑定义S为美国各州的集合。让函数g：$C \to L \times S$定义为输入一辆车，输出该车的车牌字符串和家乡州的有序对。这*will*是一个注入，因为同一州内没有两辆车可以有相同的车牌。（再次强调，这并不是一个真正的形式证明；我们只是在用非数值示例来说明注入性的概念。）

Example 7.4.9. 设 $d : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ 为由 $d(a, b) = a - b$ 定义的函数。确定 d 是否为单射并证明你的结论。

结果发现 d 不是一个单射！注意 $a - b = (a + 1) - (b + 1)$。我们可以利用这一点来找到一个反例：

考虑对$(2, 1) \in \mathbb{N} \times \mathbb{N}$和$(3, 2) \in \mathbb{N} \times \mathbb{N}$。注意$d(2, 1) = 1$和$d(3, 2) = 1$。由于$(2, 1) \neq (3, 2)$并且$d(2, 1) = d(3, 2)$，我们得出结论$d$不是单射。

Example 7.4.10. 令 $F : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{Z})$ 定义为

$$\forall X \in \mathcal{P}(\mathbb{N}) \text{ . } F(X) = \bigcup_{a \in X} \{a, -a\}$$

你看到这个函数做了什么吗？（你能解释为什么它甚至是一个 *well- defined* 函数吗？）

让我们给你展示几个例子，让你有个概念：

$$\begin{aligned} F(\{1\}) &= \bigcup_{a \in \{1\}} \{a, -a\} = \{-1, 1\} \\ F(\{1, 3, 5\}) &= \bigcup_{a \in \{1,3,5\}} \{a, -a\} = \{-1, 1\} \cup \{-3, 3\} \cup \{-5, 5\} \\ &= \{-5, -3, -1, 1, 3, 5\} \\ F(\varnothing) &= \bigcup_{a \in \varnothing} \{-a, a\} = \varnothing \\ F(\mathbb{N}) &= \mathbb{Z} - \{0\} \end{aligned}$$

我们断言 F 是一个单射。在阅读我们的证明之前，先思考一下如何证明这一点。特别是，思考我们可能在这里采用的不同策略，基于单射的正式 *definition* 定义。是否有一种策略可能比另一种策略更有成效?

Proof. WWTS F是一个注射。设 $X, Y \in \mathcal{P}(\mathbb{N})$。

假设 $X \neq Y$. WWTS $F(X) \neq F(Y)$。

辛 e $X \neq Y$，我们有两种情况：要么 $X \not\subseteq Y$，要么 $Y \not\subseteq X$（或时）。

假设 $X \not\subseteq Y$。这意味着 $\exists n \in X$。 $n \notin Y$. Let such an n be given.
自 $n \in \{-n, n\}$ 和 $n \in X$ 以来，我们发现 $n \in F(X)$，根据 F的定义。

然而，自 $n \notin Y$ 以来，我们发现 $\forall a \in Y$。

相应地，$n \neq F(Y)$。这表明$F(X) \neq F(Y)$.
$n \neq -a, a$. This follows because

在其他情况下，当 $Y \not\subseteq X$时，我们可以按照完全相同的论点进行，角色相反（
$n \notin Y$, as well as the fact that $n \in \mathbb{N}$ and $Y \subseteq \mathbb{N}$, so $\forall a \in Y$。 $n \neq a \in \mathbb{Z}$.
即在每一步中交换 X 和 Y）。这表明 $F(Y) \neq F(X)$。

一起，我们已经证明了 $\forall X, Y \in \mathcal{P}(\mathbb{N})$。 | |

$X \neq Y \to F(X) \neq F(Y)$. This shows F is an injection.

考虑如果我们使用不同的技术，这个证明可能会怎样进行。比如说，我们首先假设 $X, Y \in \mathcal{P}(\mathbb{N})$，并且 $F(X) = F(Y)$。我们能否推断出 $X = Y$?

7.4.3 Proof Techniques for Jections

让我们通过展示一些 **proof templates** 来总结到目前为止本节的概念。这些可以在你试图证明/反驳一个函数是单射/满射时使用。我们喜欢使用简称“Jections”来指代这两个函数属性。

Prove that f is surjective

1. 令 $b \in B$ 为任意且固定的。

2. 定义 $a =$. 3. 证明 $a \in A$。4. 证明 $f(a) = b$。5. 这表明 $b \in \text{Im}_f(A)$。
因此，$\text{Im}_f(A) = B$，所以 f 是满射的。

Prove that f is not surjective

1. 定义 $b =$。 2. 证明 $b \in B$
。

3. 令 $a \in A$ 为任意且固定的。

4. 证明 $f(a) \neq b$。 (或者，假设 $f(a) = b$ 并找出矛盾。) 5. 这表明 $\exists b \in B$。 $b \notin \mathrm{Im}_f(A)$, so f is not surjective.

Prove that f is injective

1. 令 $x, y \in A$ 为任意且固定的。2. 假设 $f(x) = f(y)$。3. 推导出 $x = y$。

或者:

1. 令 $x, y \in A$ 为任意且固定的。2. 假设 $x \neq y$。3. 推导出 $f(x) \neq f(y)$。

Prove that f is not injective

1. 定义 $x =$ 并定义 $y =$。2. 证明 $x \in A$ 和 $y \in A$。3. 证明 $x \neq y$。4. 证明 $f(x) = f(y)$。

Prove that f is bijective

1. 证明 f 是单射的。2. 证明 f 是满射的。

7.4.4 Bijections

你可能已经猜到了我们一直在努力构建的内容。想想我们刚才研究函数的两个主要属性：*surjectivity* 和 *injectivity*。当一个函数具有 *both* 这些属性时会发生什么？如果一个函数具有这样的属性，即对于值域中的每个元素，在定义域中都有一个 *at least one* 对应的元素（满射性）*and*，那么也存在这样的元素 *at most one*（单射性）？没错：对于每个输出，都有一个 *exactly* 输入！这是一个非常不错的属性，将成为我们接下来讨论 *cardinality*（即集合的 *size* 的基础。让我们先定义一下，然后讨论一些例子。

Definition

Definition 7.4.11. *Let A, B be sets and let f $A \to B$ be a function. We say f is a* **bijective** *function if and only if f is* 都 *injective and surjective.*

Equivalently, we just say "f is bijective" (adjectival form), or that "f is a bijection" (nounal form).

We will sometimes say that f is a bijection 在 *the sets A and B, instead of saying "from A to B". (The reason for this will become clear in the next section!)* 之间

注意，从逻辑上讲，这个定义是一个 AND 声明。目前，我们唯一用来证明一个函数是双射的方法就是证明它是满射 *and* 或证明它是单射。同样，要证明一个函数不是双射，我们需要证明它不是满射 *either* 或不是单射。（可能这两个性质都失败了，但一个这样的证明就足以表明一个函数不是双射。）我们不会重复这些相同的技术（这些技术在前面的部分有很好的总结），我们只会指出到目前为止我们看到的某些例子是否是双射。

Example 7.4.12.

(a{v*} 设 {v*} : {v*} 为由 {v*} 定义的功能。

我们证明了 p 是满射但 *not* 是单射，因此它是 **not** 双射。

(b) 设 $d : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ 为由 $d(a, b) = a - b$ 定义的函数。我们证明了 d 是满射但 *not* 不是单射，因此它是一个 **not** 双射。

(c) 设 $g : \mathbb{R} - \{-1\} \to \mathbb{R}$ 为由以下函数定义的

$$\forall x \in \mathbb{R}\text{.}\ g(x) = \frac{x}{1+x}$$

我们证明了 g 不是满射的。（具体来说，我们展示了 $1 \notin \text{Im}_g(\mathbb{R} - \{-1\})$。）在本节的练习中，我们将要求你证明 g *is* 是一个注入。这意味着 g 不是一个双射。

然而，请考虑用与 g 相同的“规则”定义 $h : \mathbb{R} - \{-1\} \to \mathbb{R} - \{1\}$，即 $h(x) = \frac{x}{1+x}$。

我们要求你在第7.3.5节的练习中证明这个函数满足 $\text{Im}_h(\mathbb{R} - \{-1\}) = \mathbb{R} - \{1\}$。这表明$h$是一个满射。

此外，我们将在本节练习中要求你证明以这种方式定义的函数——通过取一个注入，使用相同的“规则”，并将值域重新定义为像——产生一个双射。

所有这些加在一起证明 h 是从 $\mathbb{R} - \{-1\}$ 到 $\mathbb{R} - \{1\}$ 的 **bijection**。

Example 7.4.13. 让我们来看一个新例子，这个例子特意选择来预览一些即将出现的主要思想。定义$E \subseteq \mathbb{N}$为所有*even*的集合

自然数；也就是说，

$$E = \{e \in \mathbb{N} \mid \exists k \in \mathbb{N}\text{.}\ e = 2k\}$$

定义函数 $d : \mathbb{N} \to E$ 为 $d(n) = 2n$。我们声称 d 是一个双射。

Proof. 首先，让我们证明 d 是一个满射。设 $e \in E$ 为已知。

根据E的定义，存在$\exists k \in \mathbb{N}$使得$e =$属于k。给定这样的k。

这告诉我们 $d(k) = 2k = e$。由于 e 是任意的，我们得出结论 d 是一个满射。

其次，让 的证明 {v*} 是一个注入。设 $m, n \in \mathbb{N}$ 和假设 $d(m) \qquad = d(n)$.

这意味着 $2m = 2n$。从两边消去2，我们得到 $m = n$。因此，d 是一个注入。

一起，这证明了 d 是一个双射。 □

我们通过提出一些问题来激发一些未来的考虑：您觉得在 $\mathbb{N}$ 和 E 之间存在一个 *bijection*，这个集合是 $\mathbb{N}$ 的一个 *proper* 子集，这有点奇怪吗？是否总是可以在一个集合与其自身的子集之间找到一个双射？我们之前是否见过这种情况的其他例子？

Motivation

双射 $f : A \to B$ 的主要思想是我们可以将 A 和 B 的元素 **pair up** 并逐个将它们相互识别。这个想法源于全射性和单射性的定义：每个输出都有一个 *exactly one* 对应的输入。此外，更仔细地思考我们在 *proofs* 中展示的这些属性。在证明 f 是全射时，我们表明我们可以至少以一种方式“移动”从陪域回到定义域，然后在证明 f 是单射时，我们表明这是 *only* 做这件事的唯一方法。在某种意义上，我们正在展示如何“撤销”函数 f 并反转其作用。事实上，我们正在隐式地定义一个从 B 到 A 的新函数。你之前讨论过函数的 *inverse* 吗？这正是我们现在正在重新发现的东西！为了使“从陪域移动到定义域”的概念足够严谨，我们需要简要讨论如何“适当”组合函数。在那之后，我们将能够给出我们所说的函数 *inverse* 的精确定义，并将其与双射联系起来。所有这些都在下一节发生。

7.4.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于你刚刚阅读的部分，所以如果你无法回忆起特定的定义、概念或例子，请返回并重新阅读那部分。确保你

可以自信地回答这些问题后再继续，将有助于你的理解和记忆！

(1) 用一个 **image** 来表示 **surjective** 的定义。然后，用量词来表示满射的定义。

(2) 描述证明函数是 **injective** 的两种不同方法。

(3) 一个函数能否既是单射又是满射？如果是，请给出一个例子。

(4) 一个函数既不是单射也不是满射吗？如果是，请给出一个例子。

(5) 考虑以下示意图。对于每一个，声明它是否是一个函数；如果是，声明它是否是（a）一个注入和（b）一个满射。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 假设 $f : \mathbb{R} \to \mathbb{R}$ 是一个 *increasing* 函数；即，假设

$$\forall x, y \in \mathbb{R}.\ x < y \implies f(x) < f(y)$$

证明 f 必须是 *injective*。

然后，通过定义一个非满射的递增函数来证明 f *need not* 是满射的。

(2) 设 $g : \mathbb{R} - \{-1\} \to \mathbb{R}$ 为由以下函数定义的

$$\forall x \in \mathbb{R}.\ g(x) = \frac{x}{1+x}$$

是 g 单射吗？*Prove* 你的说法。

(3) 给出一个函数 $f : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ 的例子，它是满射的。*Prove* 它是。

(请注意 $\varnothing \in \mathcal{P}(\mathbb{N})$ 的实际情况。此外，考虑查看第5.5.2节以获取一些灵感……)

(4) 给出一个函数 $F : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ 的例子，它是单射的。*Prove* 它是。

然后，*prove* 您的函数 F 是 *not* 单射的。

(注意：是的，我们要你证明你的函数不是满射 *without knowing what function you defined*。我们知道我们是正确的！你将在本章后面了解我们的技巧……)

(5) 假设 $f : A \to B$ 和 $g : B \to C$ 是满射函数。证明 $g \circ f : A \to C$ 也是满射的。（6）设 $f : A \to B$ 是一个单射函数。定义 $g : A \to \mathrm{Im}_f(A)$，通过设置 $\forall x \in A$，$g(x) = f(x)$. Prove that g is a bijection.

(7) Define $F : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by $F(x, y) = (x + y, 2x - y)$. Prove F is bijective.

(**Hint:** In your scratch work, you should try to solve a system of two equations. See Section 1.3.2 for some suggestions about how to do that.)

(8) Let A, B be sets. Let $g : A \to B$ be an *injection*.

设 $X \subseteq A$。设 $h : X \to B$ 为由 $\forall x \in X$ 定义的函数。证明 h 也是一个注入。

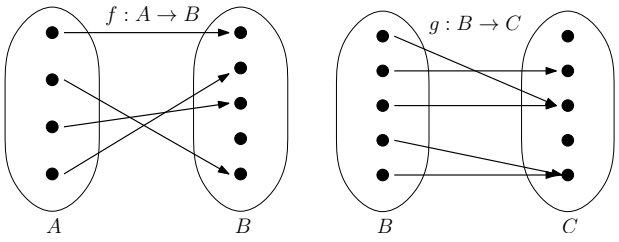
(That is, h is defined by the same "rule" as g, but on a "restricted domain".)

7.5 Compositions and Inverses

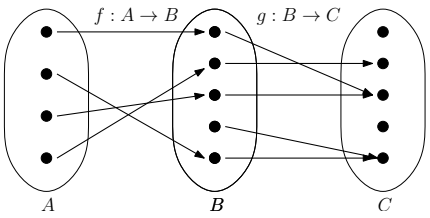
7.5.1 Composition of Functions

Motivation

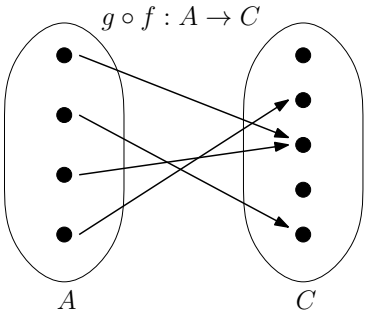
让我们暂时思考一下函数的示意图解释。想象一下，我们有一个函数 $f : A \to B$，同时我们还有一个函数 $g : B \to C$，定义如下：



在启发式意义上，f就像一张“地图”，为我们从A的元素到B的元素提供了一条特定的路线，而g则像一张从B的元素到C的元素的“地图”。如果我们简单地依次跟随这些“地图”会发生什么？也就是说，让我们通过叠加它们来组合这两个，



然后简单地从 A 一直旅行到 C，省去中间人：



这似乎是件合情合理的事情，对吧？是的，当然！每当我们有数学对象可供使用时，我们总是好奇如何合理地组合、操作和推广它们。在函数的情况下，我们称这种组合为函数的**composition**。你可能注意到，这种组合只有在“第一个”函数的值域和“第二个”函数的定义域相同时才有意义。这一点包含在以下定义中。

Definition

Definition 7.5.1. *Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Consider the function $h : A \to C$ defined by*

$$\forall a \in A \bullet h(a) = g(f(a))$$

We say that h is the **composition** *of g with f and we write $h = g \circ f$.*

We also shorten this terminology and say h is “g composed with f”.

这包含了我们上面提到的所有想法。它要求应用“第一个”函数的f (的值域是应用“第二个”函数的g (的定义域。

另一个直观的想法是将一个函数视为一个 *machine* 或一个 *black box*。定义域的元素进入，值域的元素出来。我们不一定知道机器做了什么；我们只看到结果。现在，

考虑连接两台机器，一台用于 f，另一台用于 g；将 f 机器的输出插入到 g 机器中。输出的是 C 的一个元素。我们可以将这两台机器的工作视为一台更大机器的工作。这正是 *composition* $g \circ f$ 所做的；它是一台更大的机器，它按照指定的顺序执行两台机器的操作。

Notation

注意符号 $g \circ f$ 的顺序以及它与我们将函数 *apply* 的顺序的比较：f 先于 g，即 $g(f(a))$。用文字来说，我们会把 “$g(f(a))$” 读作 “g 的 f 的 a”。实际上，如果你发现自己难以记住这个顺序，这里有一个建议：大声读出 “$\circ$” 为 “之后”。因此，$h = g \circ f$ 就意味着 “g *after* f”，因为我们先取 a 的一个元素，然后先应用 f，再应用 g。

也很重要的是要记住组合函数的 *notation*，并将函数 $g \circ f$ 本身与函数 $g \circ f$ 对某些元素 $x \in A$ 的 *application* 区分开来。例如，要使用“$\circ$”符号来写“g of f of x”，我们会写成

$$(g \circ f)(x)$$

因为我们用函数 $g \circ f$ “击中” 元素 x。然而，以下符号 **make no sense** 因为它混淆了函数和元素的概念：

$$g \circ f(x)$$

你看到区别了吗？对象 $f(x)$ 是 B 的一个元素，f 的值域。但 g 是一个函数。将一个函数与集合的元素组合意味着什么？这行不通。一般要小心这个，这个区别在我们需要组合几个函数时尤其重要，比如 $(h \circ (g \circ k) \circ f)(z)$，其中 z 是 f 的定义域中的一个元素，f, g, h, k 是函数。

Examples

Example 7.5.2. 令 $C : \mathbb{R} \to \mathbb{R}$ 定义为

$$\forall x \in \mathbb{R}.\ C(x) = x - 273.15$$

让 $F : \mathbb{R} \to \mathbb{R}$ 定义为

$$\forall x \in \mathbb{R}.\ F(x) = \frac{9}{5}x + 32$$

函数 C 将开尔文温度转换为摄氏度。函数 F 将摄氏度转换为华氏度。

然后函数 $F \circ C$ 将开尔文度转换为华氏度

直接。我们可以为函数编写“规则”，并找到一个直接转换的公式:

$$\begin{aligned}\forall x \in \mathbb{R}.\ (F \circ C)(x) &= F(C(x)) = F(x - 273.15) \\ &= \frac{9}{5} \cdot \big(x - 273.15\big) + 32 = \frac{9}{5}x - 459.67\end{aligned}$$

Example 7.5.3. 设 $f : \mathbb{R} \to \mathbb{Z}$ 为由以下函数定义

$$\forall x \in \mathbb{R}.\ f(x) = \lfloor x \rfloor$$

(回忆起 $\lfloor x \rfloor$ 是 *floor* 的 x: 它是满足 $z \leq x$ 的 *largest* 整数 $z \in \mathbb{Z}$。令 $g : \mathbb{Z} \to \mathbb{N}$ 为定义如下函数

$$\forall z \in \mathbb{Z}.\ g(z) = \begin{cases} -z & \text{if } z < 0 \\ z + 1 & \text{if } z \geq 0 \end{cases}$$

让我们找到 $g \circ f$。注意，每当 $x \in \mathbb{R}$ 满足 $x < 0$ 时，我们也将有 $\lfloor x \rfloor x < 0$。同样，每当 $x \in \mathbb{R}$ 满足 $x \geq 0$ 时，我们也将有 $\lfloor x \rfloor \geq 0$。这告诉我们，组合 $g \circ f$ 也将是一个 **piece-wise** 函数:

$$\forall x \in \mathbb{R}.\ (g \circ f)(x) = \begin{cases} -\lfloor x \rfloor & \text{if } x < 0 \\ \lfloor x \rfloor + 1 & \text{if } x \geq 0 \end{cases}$$

问题: 这个函数是单射吗? 满射吗? 尝试证明你的说法! *Example* 7.5.4. 定义 $f : \mathbb{N} \to \mathbb{N}$ 和 $g : \mathbb{N} \to \mathbb{N}$ 以及 $h : \mathbb{N} \to \mathbb{N}$ 为

$$\begin{aligned}&\forall n \in \mathbb{N}.\ f(n) = n + 3 \\ &\forall n \in \mathbb{N}.\ g(n) = n^2 \\ &\forall n \in \mathbb{N}.\ h(n) = 2n - 1\end{aligned}$$

(问题: 你确定这些是定义良好的函数吗? 为什么?)

我们可以找到 $g \circ f$ 和 $h \circ f$ 的“规则”:

$$\begin{aligned}&\forall n \in \mathbb{N}.\ (g \circ f)(n) = g(f(n)) = g(n + 3) = (n + 3)^2 = n^2 + 6n + 9 \\ &\forall n \in \mathbb{N}.\ (h \circ g)(n) = h(g(n)) = h(n^2) = 2n^2 - 1\end{aligned}$$

然后我们可以使用这些来找到一个进一步组合的规则，例如 $h \circ (g \circ f)$:

$$\begin{aligned}\forall n \in \mathbb{N}.\ \big(h \circ (g \circ f)\big)(n) &= h\big((g \circ f)(n)\big) = h\big(n^2 + 6n + 9\big) \\ &= 2(n^2 + 6n + 9) - 1 = 2n^2 + 12n + 17\end{aligned}$$

同样，我们可以使用这些来找到一个关于 $(h \circ g) \circ f$ 的规则:

$$\begin{aligned}\forall n \in \mathbb{N}.\ \big((h \circ g) \circ f\big)(n) &= \big(h \circ g\big)(f(n)) = (h \circ g)(n + 3) \\ &= 2(n + 3)^2 - 1 = 2(n^2 + 6n + 9) - 1 \\ &= 2n^2 + 12n + 17\end{aligned}$$

Let's look at that one, too. Translated, it is the same rule! That is to say, we only *proved* that

$$(h \circ g) \circ f = h \circ (g \circ f)$$

in the sense of *functions*, by showing that they produce the same outputs for *every* allowable input.

Composition is Associative

The functions f, g, h used in the previous example have no special properties. The result we got is actually correct *in general*. The following theorem and its proof will demonstrate this. We are proving that function composition is **associative**. This means that whenever we have a series of compositions, we can move the parentheses around however we like; we know the order in which to apply the parentheses doesn't matter.

Theorem 7.5.5. *Let A, B, C, D be any sets. Let $f : A \to B$ and $g : B \to C$ and $h : C \to D$ be functions. Then,*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof. WWTS, that the two functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ have the same outputs for every possible input.

Let $x \in A$ be known. Applying the definition of *composition*, we see

$$[h \circ (g \circ f)](x) = h\big(g \circ f)(x)\big) = h\big(g(f(x))\big)$$

and

$$[(h \circ g) \circ f](x) = \big(h \circ g\big)(f(x)) = h\big(g(f(x))\big)$$

□

Compositions and Jections

There are interesting things to think about here: what if we take two functions with shared properties and compose them? Does the property "survive"? For example, if we compose two injections, do we get another injection? In order for a composition of functions to be injective, do *both* functions in the composition *need* to be injections?

Similarly, suppose we have a composition of two functions. If we know that the composition is surjective, can we *necessarily* deduce that one of the functions in the composition is surjective? Do they both need to be?

We will state and prove some claims about questions like these. We will leave you to prove some claims and find counterexamples in the exercises, both for this section and for the end of the chapter.

Proposition 7.5.6. *Let A, B, C be sets and let $f : A \to B$ and $g : B \to C$ be functions. If $g \circ f$ is injective, then f is necessarily injective.*

(请注意，这并不假设 *any* 的 g 属性；它甚至不必是必然单射的！作为一个练习，尝试找到一个函数 $f: A \to B$ 和 $g: B \to C$ 的例子，使得 $g \circ f$ 是单射的，g 也是单射的，以及一个例子，其中 $g \circ f$ 是单射的但 g 不是单射的。)

Proof. 设 $x, y \in A$ 已知。假设 $f(x) = f(y)$。WWTS $x = y$。

由于 g 是一个定义良好的函数，$g(f(x)) = g(f(y))$。

这表示 $(g \circ f)(x) = (g \circ f)(y)$。

由于 $g \circ f$ 是单射的，$x = y$。这就是我们的目标，因此该命题已证明。 □

结果证明，我们刚刚证明的断言的 *converse* 是 False。由于这个断言是关于 *all* 函数的，反驳它需要我们提供一个反例。

Proposition 7.5.7. *Let A, B, C be sets and let $f : A \to B$ and $g : B \to C$ be functions. Suppose f is injective. Then it is not necessarily the case that $g \circ f$ is injective.*

尝试自己做一些草稿工作，在阅读我们的例子之前提出一个反例。记住，你不需要找到最有趣或最复杂的例子，也不一定需要一个由 *rule* 定义的反例；你只需要能够定义一个！

Proof. 我们将展示一个反例。

Define $A = \{1, 2\}$ and $B = \{\heartsuit, \diamondsuit\}$ and $C = \{\star\}$.

定义 f 通过设置 $f(1) = \heartsuit$ 和 $f(2) = \diamondsuit$。

注意 f 是单射的，因为 $f(1) \neq f(2)$。

定义 g 通过设置 $g(1) = g(2) = \star$。

注意 $g \circ f$ 由 $(g \circ f)(1) = \star$ 和 $(g \circ f)(2) = \star$ 定义。

这表明 $g \circ f$ 不是单射的，因为 $(g \circ f)(1) = (g \circ f)(2)$ 但 $1 \neq 2$。 □

7.5.2 Inverses

Motivation

如我们之前所说，一个 **bijection** $f: A \to B$ 具有一个非常好的性质，即在 f “配对”了两个集合 A 和 B 的元素。给定一个元素 $a \in A$，存在一个 *exactly one* 元素 $b \in B$ 满足 $f(a) = b$。这是因为 f 是一个定义良好的函数。但我们还知道 a 是以这种方式与 b 关联的 *only* 定义域元素。这是因为 f 是一个双射。由于这种双向的独特关联，我们可以考虑“反转” f 的作用。给定一个元素 $b \in B$，确定会产生那个 b 的 a。这就是一个 **inverse** 函数所做的事情。在这里，我们将用函数 **composition** 和 **identity** 来定义它。这也是我们说双射的原因。

是 *between* 两个集合相对，而不是仅仅从一个集合到另一个集合；一旦我们有一种方式，我们就知道我们也可以有另一种方式！

在我们看到定义之前，让我们快速回顾一下之前看到的 **identity** 函数的定义。它在后续逆函数的定义中起着重要作用。

Definition: 给定一个集合 X，**identity function** $\mathrm{Id}_X : X \to X$ 由 $\forall z \in X$ 定义。 $\mathrm{Id}_X(z) = z$.

Definition

注意，这个定义并没有说 *anything* 关于函数是双射的。这纯粹是关于逆函数含义的正式定义。之后，我们将不得不证明关于逆函数和双射之间关系的任何断言。

Definition 7.5.8. *Let $f : A \to B$ be a function. Suppose there is a function $g : B \to A$ such that $f \circ g : A \to A$ satisfies $f \circ g = \mathrm{Id}_A$ and $g \circ f : B \to B$ satisfies $g \circ f = \mathrm{Id}_B$.*

Then we say g is the **inverse** *of f and write $g = f^{-1}$.*

(注意，上述定义中的假设和结论隐含了一些条件。具体来说，必须满足 $B = \mathrm{Im}_f(A)$，以确保 g 是一个函数。同样，$A = \mathrm{Im}_g(B)$.)

Example

让我们回顾一下我们在讨论双射时看到的一个函数。在练习中，在你的帮助下，我们了解到这个函数是一个双射。在这里，我们将找到它的逆函数。

Example 7.5.9. 令 $h : \mathbb{R} - \{-1\} \to \mathbb{R} - \{1\}$ 定义为

$$\forall x \in \mathbb{R} - \{-1\}.\ h(x) = \frac{x}{1+x}$$

为了得到一个将是 h 的逆函数的候选函数 *find*，通常有助于将“规则” h 设置为某个新变量，然后求解 x。

这里，让我们假设 $h(x) = y$。我们如何“逆向”这个过程，并确定 x 在 y 中的含义？观察一下，我们可以进行一些代数步骤，如下：

$$\begin{aligned} h(x) = y &\iff \frac{x}{1+x} = y \\ &\iff (1+x)y = x \\ &\iff xy + y = x \\ &\iff y = x(1-y) \\ &\iff x = \frac{y}{1-y} \end{aligned}$$

这个 *scratch work* 给我们提供了 h 的逆的候选者。我们没有 *proven* 这些观察结果！我们现在必须提出一个主张，然后向读者展示所有必要的事实。注意，我们仔细定义了一个 *new* 函数 H，并使用它来 **prove** 实际上 $H = h^{-1}$。在 **define** h^{-1} 并然后使用它是自以为是和错误的。我们试图证明 h 有一个逆，所以我们不能在证明的开始就宣布它有一个逆！

Proof. 定义 $S = \mathbb{R} - \{-1\}$ 和 $T = \mathbb{R} - \{1\}$ 以便方便的缩写，因此 $h : S \to T$。

让 $H : T \to S$ 是由 $\forall y \in T$ 定义的函数。$H(y) = \frac{y}{1-y}$.

首先，让我们证明 H 是一个定义良好的函数。对于每一个 $y \in T$，我们知道 $y \neq 1$，因此 $1 - y \neq 0$。因此，分数 $\frac{y}{1-y}$ 是一个定义良好的实数。

此外，我们可以论证 $\frac{y}{1-y} \neq -1$. AFSOC中 $\frac{y}{1-y} = -1$. 然后将整个表达式乘以 $1 - y$ 告诉我们 $y = y - 1$，这是一个明显的矛盾。

第二 d，让我们证明 $H \circ h = \mathrm{Id}_S$。设 $x \in S$ 为已知。Obser 请提供需要翻译的英文文本，以便我进行

$$\begin{aligned}(H \circ h)(x) = H(h(x)) &= H\left(\frac{x}{1+x}\right) \\ &= \frac{\frac{x}{1+x}}{1 - \frac{x}{1+x}} \cdot \frac{1+x}{1+x} = \frac{x}{(1+x)-x} \\ &= \frac{x}{1} = x\end{aligned}$$

第三，让我们证明 $h \circ H = \mathrm{Id}_T$。设 $y \in T$ 为已知。观察得知

$$\begin{aligned}(h \circ H)(y) = h(H(y)) &= h\left(\frac{y}{1-y}\right) \\ &= \frac{\frac{y}{1-y}}{1 + \frac{y}{1-y}} \cdot \frac{1-y}{1-y} = \frac{y}{(1+y)-y} \\ &= \frac{y}{1} = y\end{aligned}$$

因此，根据逆的定义，$H = h^{-1}$。 □

Checking Both Directions

假设 $f : A \to B$ 是一个函数，并且你通过定义一个函数 $g : B \to A$ 对 f 有逆函数进行了断言。重要的是你要证明 **both** 的复合产生恒等函数；也就是说，你必须证明以下两点

$$f \circ g = \mathrm{Id}_B \quad \text{and} \quad g \circ f = \mathrm{Id}_A$$

您可能会偶尔忘记这样做，或者您可能看不到为什么这是必要的。为了帮助您理解这一点的重要性，我们包括了练习

2 在下面的7.5.4节中。它要求你找到一个例子，其中“一种方式”产生恒等函数，但“另一种方式”产生 *not*，因此所提出的函数实际上不是 *inverse*。如果能找到几个例子，就试试吧。你越能突出这一点，就越好！

7.5.3 Bijective $\iff$ Invertible

正如我们一直暗示的那样，一个双射函数有一个逆函数。这个命题的逆命题同样成立，因此我们可以陈述并证明这个 *if and only if* 命题。这里章节标题中的词—**invertible**—通常用来表示“有一个逆函数”。

Theorem 7.5.10. *Let A, B be any sets. Let $f : A \to B$ be a function. Then,*

$$f \text{ is bijective} \iff f \text{ has an inverse } f^{-1} : B \to A$$

Proof. ($\implies$) 假设 f 是双射。这意味着 f 是满射和单射。

我们需要为 f 定义一个逆函数。让我们定义 $g : B \to A$ 如下：

设 $b \in B$ 已知。由于 f 是满射的，我们知道 $\exists a \in A$。 $f(a) = b$. Let such $\forall x \in A.\ x \neq a \implies f(x) \neq f(a) = b$ an a be given. Since f is injective, we know that
这是，我们知道这个 a 是满足 $f(a) = b$ 的 *unique* 的 A 元素。让我们定义 $g(b) = a$。因为这个观察，这是一个定义良好的函数。

Next, observe that $(f \circ g)(b) = f(g(b)) = f(a) = b$, so $f \circ g = \mathrm{Id}_B$.

此外，观察 $(g \circ f)(a) = g(f(a)) = g(b) = a$，因此 $g \circ f = \mathrm{Id}_A$。

因此，$g = f^{-1}$，所以 f 有一个逆元。

($\impliedby$) 假设 f 有一个逆函数，$f^{-1} : B \to A$。

首先，让我们证明 f 是单射的。设 $a_1, a_2 \in A$ 为已知。观察如下

$$\begin{aligned}
f(a_1) = f(a_2) &\implies f^{-1}(f(a_1)) = f^{-1}(f(a_2)) && f^{-1} : B \to A \text{ is a } \textit{function} \\
&\implies (f^{-1} \circ f)(a_1) = (f^{-1} \circ f)(a_2) && \text{definition of composition} \\
&\implies \mathrm{Id}_A(a_1) = \mathrm{Id}_A(a_2) && \text{definition of identity} \\
&\implies a_1 = a_2 && \text{definition of identity}
\end{aligned}$$

因此，f 是单射的。

其次，让我们展示 f 是满射的。设 $b \in B$ 为已知。由于 f^{-1} 是一个函数，我们知道 $\exists a \in A$。

$f^{-1}(b) = a$. Let such an a be given. Then observe that$f^{-1}(b) =$

a.

$$\begin{aligned} f^{-1}(b) = a &\implies f(f^{-1}(b)) = f(a) && f : A \to B \text{ is a function} \\ &\implies (f \circ f^{-1})(b) = f(a) && \text{definition of composition} \\ &\implies \mathrm{Id}_B(b) = f(a) && \text{definition of identity} \\ &\implies b = f(a) && \text{definition of identity} \end{aligned}$$

□

Proving a Function is Bijective

这个有用的定理现在为我们提供了一种证明给定函数 $f : A \to B$ 是双射的另一种方法。我们不必证明 f 是一个注入 *and* 或一个满射，我们只需定义一个新的函数 $g : B \to A$ 并证明它是 f 的 **inverse**，即 $g = f^{-1}$。然后，这个定理适用，并告诉我们 f 是一个双射！根据上下文，这些策略中的一个可能更容易应用，或者你可能更习惯于其中一个。记住，这两种策略都是可行的！

Inverse of an Inverse

以下推论直接由上面的定理得出。我们称之为 *corollary*，而不是它自己的定理，因为它并没有真正断言任何令人惊讶的新东西；相反，其结论来自应用上述定理，正如你在证明中将会看到的那样。

Corollary 7.5.11. *Let A, B be any sets. Let f $A \to B$ be a function.*

If f is a bijection, then $f^{-}1$ exists and it is 也 *a bijection.*

Furthermore, $\left(f^{-1}\right)^{-1} = f$.

Proof. 假设 f 有一个逆元，$f^{-1} : B \to A$。这意味着 $f \circ f^{-1} = \mathrm{Id}_B$ 和 $f^{-1} \circ f = \mathrm{Id}_A$，根据逆元的定义。

这些正是显示 $\left(f^{-1}\right) = f$ 的条件，再次根据逆的定义！这表明 f^{-1} 有一个逆（即，f 本身），因此上述定理告诉我们 f^{-1} 必须是一个双射。

□

Inverse of a Composition

在继续进行一些练习和下一节之前，让我们寻求您的帮助，将到目前为止本章的主要思想整理出来。具体来说，我们在这里将陈述两个结果。证明留给您在章节练习中完成。通过解决这些证明，您将（a）巩固对迄今为止介绍的大多数概念的理解——函数、单射、复合、逆元——以及（b）获得有关如何定义函数复合的逆的有用结果！

Proposition 7.5.12. *Let $f : A \to B$ and $g : B \to C$ be bijective functions. Define $h : A \to C$ to be $h = g \circ f$. Then h is also bijective.*

Proof. 将留给读者作为问题7.8.9。 □

Proposition 7.5.13. *Let $f : A \to B$ and $g : B \to C$ be bijective functions. Define $h : A \to C$ to be $h = g \circ f$. Then h is invertible and $h^{-1} = f^{-1} \circ g^{-1}$.*

Proof. 问题 7.8.10 留给读者 □

7.5.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 函数**associative**的组成是什么？(也就是说，括号的顺序重要吗？)为什么或为什么不重要？(2) 函数**commutative**的组成是什么？(也就是说，我们可以颠倒顺序吗？)为什么或为什么不可以？(3) 假设$f : A \to B$和$g : B \to A$是函数。我们如何**prove** $g = f^{-1}$？(4) 假设$f : A \to B$是一个双射。它的逆也是双射吗？

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 设 O 为奇自然数集，设 E 为偶自然数集。定义一个函数 $f : O \to E$，它是一个 **bijection**，并通过找到其逆函数来证明它是这样的。

(2) 在这个问题中，我们希望您构建一个示例，以展示当我们试图找到一个函数的逆函数时，验证 **both** 组合产生恒等函数的重要性。

定义集合 A, B 和函数 $f : A \to B$ 和 $g : B \to A$ 使得

$$\forall x \in A \text{.}\ g(f(x)) = x$$

但是

$$\exists y \in B\,.\; f(g(y)) \neq y$$

(**Suggestion:** 您可能会找到一个例子，其中 A 和 B 都只有一个或两个元素……或者，您可能会找到一个例子，其中 $A = B = \mathbb{N}$.)

(3) 让 $U = \{y \in \mathbb{R} \mid -1 < y < 1\}$ 和 $I = \{y \in \mathbb{R} \mid -6 < y < 12\}$。

让 $g : U \to I$ 是由 $\forall x \in U$ 定义的函数。 $g(x) = 9x + 3.$

证明 g 是双射，通过找到 g^{-1}。

(4) 定义函数 $f : \mathbb{Z} \to \mathbb{N}$ 为

$$\forall z \in \mathbb{Z}\,.\; f(z) = \begin{cases} -2z + 2 & \text{if } z \leq 0 \\ 2z - 1 & \text{if } z > 0 \end{cases}$$

证明 f 是双射，通过找到 f^{-1}。

(您的建议的逆函数也将是分段定义的。在证明中注意随后出现的各种情况。)

(5) **Challenge:** 定义 $I = \{y \in \mathbb{R} \mid -1 < y < 1\}$。找到一个函数 $f : I \to \mathbb{R}$，它是双射，并证明它是。

(**Hint:** 您不需要使用任何三角函数。考虑在您的表达式中使用 $|x|$ ...)

7.6 Cardinality

7.6.1 Motivation and Definition

一个关心双射的重要原因是，它们允许我们比较集合的 **sizes**！这是一个你有所直觉的概念。例如，很明显，集合

$$\{1, 2, 3, 4, 5\}$$

具有5个元素。它是**finite**。然而，该集合

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

是 **infinite**。我们还理解 $\mathbb{Z}$ 是一个无限集。$\mathbb{Q}$ 和 $\mathbb{R}$ 也是如此。它们的大小是多少？我们甚至能比较它们吗？我们如何才能 *mathemat- ically* 呢？成为 *infinite* 集究竟意味着什么？是否存在“不同的无限”呢？

Bijections "Pair" Elements

假设我们面前桌子上有一支笔和一本书。但是，让我们假装我们不知道如何**count**它们。我们如何验证笔的数量和书的数量一样多？除了说"有5支笔和5本书，5=5"，我们能否以某种方式展示书的*set*和笔的*set*有相同的*size*，而不必知道这个大小是多少?

这是*bijection*发挥作用的地方。我们可以逐个*pair off*钢笔和书籍。我们可以将它们排列在桌子上，并在它们之间画一条线，显示它们之间的对应关系。在集合的语言中，我们正在识别钢笔集合和书籍集合之间的一个*bijection*。这个想法非常重要，因此我们想用一句引语来给你留下深刻印象:

In the land of Cardinality, the Bijection is King.

想象我们的基数研究是一次穿越基数王国的旅程。在这个王国里，我们向bijection国王鞠躬，因为他统治一切。只有他才能告诉我们两个集合何时具有*same cardinality*，无论它们是有限的还是无限的。

此外，我们确实 *need* 使用这个术语集，因为我们将会看到一些令人惊讶且反直觉的结果。使用这些正式的定义和概念将使我们能够做到严谨和精确。我们所看到的例子和结果可能会让我们有点（或很多！）惊讶，但它们根植于我们已经看到的概念和我们已经证明的定理，这使得我们实际上 *belive* 这些结果，从数学的角度来说!

Definitions and Notation

首先，让我们定义什么是**finite**。

Definition 7.6.1. *Let S be any set. We say S is* **finite** *if and only if*

$$\exists n \in \mathbb{N} \cup \{0\} \text{ such that there exists a bijection } f : S \to [n]$$

In this case, we write $|S| = n$ to indicate that the **size** *of S is n.*

注意：空集 $S = \varnothing$ 是有限的，因为 $[0] = \varnothing$。这就是为什么我们在定义中说 $n \in \mathbb{N} \cup \{0\}$，而不是仅仅 $n \in \mathbb{N}$。那个是双射的函数 $f : \varnothing \to \varnothing$ 简单地就是 *empty relation*。（记住，函数是一种关系！）

根据定义，形式为$[n]$的集合是有限的。它们是我们有限集合的标准例子，大小为$|[n]| = n$。因此，要证明一个集合S的大小为n，我们需要在S和$[n]$之间找到一个双射。例如，考虑集合$\{1, 3, 5\}$。这显然看起来大小为3。我们可以通过展示双射f: $\{1, 3, 5\} \to [3]$，定义为$f(1) = 1$和$f(3) = 2$以及$f(5) = 3$来证明这一点。

有趣的是思考一个有限集是否可以有两个 *different* 大小。定义技术上并不排除这种情况，但我们可以说有限集的大小是唯一的。想想如何做到这一点……在给出几个更基本的定义之后，我们将这样做。

Definition 7.6.2. *Let S be any set. We say S is* **infinite** *if and only if S is* 非有限{v*}

That is, S is infinite if $\forall n \in \mathbb{N} \cup \{0\}$, every possible function $f : S \to [n]$ fails to be a bijection.

When S is infinite, we use $|S|$ to indicate the **cardinality** *of the set.*

它可能看起来很愚蠢，用这种方式定义无限——*not*有限——但它确实反映了这两个概念之间的直观二分。一个集合不能既是*both*有限的又是无限的，所以我们不如将其中一个分类，并将另一个定义为“其他任何东西”。

此外，我们用 **not** 写 $|S| = \infty$ 来表示一个集合是无限的。正如我们很快就会看到的，实际上有 **many different "levels" of infinite sets**。现在这可能会让你觉得非常奇怪，但你会明白我们的意思。是的，无限集合有不同的“大小”，我们将用 $|S|$ 来表示 **cardinality** 的 S，以便我们可以将其与其他集合的大小进行比较。写 $|S| = \infty$ 会表示只有一个“无限”，这是非常错误的。

现在，话虽如此，我们将主要区分无限集合中的两种 *types*，以适应我们的目的。我们这样做是为了向您展示一些关于我们已熟悉的集合的显著结果，即 $\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$ 和 $\mathbb{R}$。以下定义告诉我们这两种类型是什么。

Definition 7.6.3. *Let S be any set.*

We say S is **countably infinite** *if and only if there exists a bijection f $S \to \mathbb{N}$.*

We say S is **uncountably infinite** *(or just* **uncountable***) if and only if S is infinite and every function f $S \to \mathbb{N}$ fails to be a bijection.*

给定一个无限集合 S，此定义基于其基数 $|S|$ 与 $\mathbb{N}$ 的比较，为 S 建立了两种可能性。我们使用术语 **countably infinite**，因为它代表了为什么我们直观地认为 $\mathbb{N}$ 是无限的。集合 $\mathbb{N}$ 有“很多”元素，如此之多，以至于如果我们试图计数，我们将永远无法完成；然而，我们甚至可以尝试以这种方式计数的事实表明了某种特殊性。集合 $\mathbb{N}$ 有第一个元素，第二个元素，第三个，……。我们无法在我们的有生之年命名它们所有，但我们可以编写一个神奇的不朽机器人，一个接一个地打印它们。如果我们事先想到了一个自然数，无论这个数字有多大，我们知道机器人将 *eventually* 打印出那个数字。

也许我们无法用 *all* 无穷集合来做这件事。这就是无穷集合的概念所要传达的意思。这样的集合是无穷的，所以它与形式为 $[n]$ 的集合没有对应关系，但它也是 *"so large"* 我们无法识别“第一个元素”、“第二个元素”、“第三个元素”等等。这就是一个 **bijection** $f : S \to \mathbb{N}$ 要传达的，一种以显示它们与自然数配对的方式展示 S 所有元素的方法。如果我们 *cannot* 这样做，那么这个集合就是不可数的无穷集合。现在，你可能不相信这样的集合存在！别担心，我们会向你展示一些。现在，只需

请注意 **countably** 和 **uncountably** 无穷之间的区别：区别在于是否存在一个具有 $\mathbb{N}$ 的 **bijection**。

Comparing Cardinalities

如我们所述，当 S 为无穷大时，我们使用 $|S|$ 来 **compare** S 的基数与其他集合的基数。我们不会写像 $|S| = \infty$ 这样的东西。相反，我们将写像 $|S| = |T|$ 这样的东西来表示 S 和 T 具有相同的 *same* 基数，无论这可能是怎样的。我们还可以写像 $|S| < |P|$ 这样的东西来表示 P 的基数比 S 的基数 *strictly larger*。以下定义告诉我们基数比较是基于函数的，特别是不同类型的映射。

Definition 7.6.4. *Let S, T be any sets.*

- *We write $|S| = |T|$ if and only if there exists a* **bijection** *$f\ S \to T$. In this case, we say S has the* **same cardinality** *as T.*
- *We write $|S| \leq |T|$ if and only if there exists an* **injection** *$f\ S \to T$. In this case, we say S has cardinality* **at most** *$|T|$.*
- *We write $|S| < |T|$ if and only if $|S| \leq |T|$ and $|S| \neq |T|$.*

  In this case, we say S has a **strictly smaller** *cardinality than T.*
- *We write $|S| \geq |T|$ if and only if there exists a* **surjection** *$f\ S \to T$. In this case, we say S has cardinality* **at least** *$|T|$.*
- *We write $|S| > |T|$ if and only if $|S| \geq |T|$ and $|S| \neq |T|$.*

  In this case, we say S has a **strictly larger** *cardinality than T.*

让我们以两种不同的方式解释这些定义背后的动机：

一般来说，$f : A \to B$ 是一个 *injection* 告诉我们 $|A| \leq |B|$ 和 $g : A \to B$ 是一个 *surjection* 告诉我们 $|A| \geq |B|$。考虑 f 和 g 的示意图，看看为什么这个定义是有意义的。从 $A \to B$ 有一个注入意味着我们可以肯定地将 A 的元素与 B 的元素“配对”而不重叠，但可能还有“更多”的 B 元素剩下。同样，从 $A \to B$ 有一个超射意味着我们可以肯定地将 B 的所有元素用 A 的元素“覆盖”，但也许为了做到这一点，有时需要重叠，所以 A 可能比 B 有“更多”的元素。这两种情况同时存在（即从 A 到 B 的 *bijection*）意味着 A 和 B 实际上具有相同的基数：我们可以配对它们的元素。请注意，这是一个直观的解释，以激发这些定义。这类解释不是严格的证明。但现在我们有了 *made* 这些定义，我们可以用它们来证明和反驳陈述！要比较集合的基数——甚至是无限的——我们只需要找到一个具有适当性质的功能。本章其余部分的所有工作都将对我们穿越基数王国之旅大有裨益。

另一种思考这些定义的方法是，“具有相同的基数”是“所有集合的集合”上的“等价关系”。我们必须在这些短语周围加上引号，因为我们已经在3.3.5节中详细解释了罗素悖论，其中有一个*no such thing*作为“所有集合的集合”。因此，在我们的语境中谈论那个“集合”上的等价关系在数学上是没有意义的。然而，在某种模糊的意义上，这正是所发生的事情：

- 给定任何集合 S，肯定存在与其自身的双射：恒等函数，$\mathrm{Id}_S : S \to S$。这表明 $|S| = |S|$，即“具有相同的基数”关系是“自反的”。

- 假设 $|S| = |T|$，因此存在一个双射 $f : S \to T$。是否存在一个双射 $g : T \to S$，也是吗？为什么是，当然可以使用 $g = f^{-1}$！我们知道它也是一个双射。这同样通过一个双射展示了 $|T| = |S|$，即“具有相同的基数”关系是“对称”的。

- 假设 {v*}，因此存在双射 $f : S \to T$ 和 $g : T \to U$。是否存在一个双射 $h : S \to U$，同样存在吗？是的！复合 $g \circ f$ 也是一个双射（这是你在练习中将要证明/已经证明的）。这也通过一个双射展示了 $|S| = |U|$，即“具有相同的基数”关系是“传递的”。

再次，这并不是 *exactly* 正在发生的事情，但它确实可以帮助你整理这些困难、抽象的概念。我们正在建立一个方法，通过函数比较任意两个集合的基数。宇宙中的所有集合将根据它们的基数“划分为”不同的“类别”。真正令人惊讶的是我们即将为您证明的事情：那就是有 *infinitely-many cardinalities*。

Cantor's Theorem

以下结果和证明归功于19世纪中后期德国数学家乔治·康托尔。到目前为止，数学家们已经完全接受了这个结果及其后果。然而，在当时，这个想法如此具有争议性，以至于一些数学家拒绝相信他。然而，随着时间的推移，他的工作和思想帮助导致了形式集合论的发展。

这个特定结果的证明被称为 **Cantor's Diagonalization Argument**。我们稍后将会使用类似的论据，指出为什么它像“对角线”一样。目前，我们更感兴趣的是这个定理的结论。

Theorem 7.6.5. *Let S be any set. Then $|S| < |\mathcal{P}(S)|$.*

这表示 **the power set of a set always has *strictly larger* cardinality than the set itself**。这对于有限集合是有意义的。你已经发现，$[n]$ 的幂集有 2^n 个元素，即 $|\mathcal{P}([n])| = 2^n$。（你将在问题 7.8.30 中通过归纳法，使用关于基数的结果来证明这一点。）实际上，我们看到对于每个 $n \in \mathbb{N}$，都有 $n < 2^n$。然而，这个定理还断言

这个关系适用于 **infinite** 个集合。哇！这立即告诉我们存在一个无限的集合链，每个集合都比前一个大。我们只需继续取之前集合的幂集：

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < \left|\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)\right| < \left|\mathcal{P}\Big(\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)\Big)\right| < \cdots$$

让我们证明这个定理。证明非常简短且巧妙，所以不用担心如何用这样的论据来*come up*。专注于理解逻辑流程。

Proof. 设 S 为任意集合。AFSOC $|S| \geq |\mathcal{P}(S)|$。

未指定的翻译函数 $g : S \to \mathcal{P}(S)$ 是满射 无效的。

定义 $T = \{X \in S \mid X \notin g(X)\}$。(这是有意义的，因为对于任何 $X \in S$，$g(X) \in \mathcal{P}(S)$，即 $g(X) \subseteq S$。因此，$X \in g(X)$ 或 $X \notin g(X)$ 必须成立。)

注意 $T \subseteq S$，通过集合构造表示法定义。这意味着 $T \in \mathcal{P}(S)$。

由于 g 是满射的，存在 $\exists Y \in S$ 使得 $g(Y) = T$。给定这样的 Y。

现在，是 $Y \in T$ 吗？我们考虑两种情况：

- 如果 $Y \in T$，那么 T 的定义表明 $Y \notin g(Y)$。然而，$g(Y) = T$，这意味着 $Y \notin T$。这是一个矛盾 ※。
- 如果 $Y \notin T$，那么 T 的定义表明 $Y \in g(Y)$。然而，$g(Y) = T$，这意味着 $Y \in T$。这是一个矛盾 ※。

在任一 r情况，$Y \in T$和$Y \notin T$都成立。这是一个矛盾 离子 ※

因此，不存在从 S 到 $\mathcal{P}(S)$ 的这种满射，即 $|S| < |\mathcal{P}(S)|$。 □

回顾第7.4.5节中的练习4。注意，我们要求你定义一个从$\mathbb{N}$到$\mathcal{P}(\mathbb{N})$的函数，然后我们要求你证明它是**not surjective**。我们不必知道你的函数是什么！因为我们知道这个定理，所以我们知道你不可能*possibly*定义一个满射！

Discussion: Axioms and Definitions

我们想要进行一个陈述。我们忽略了一些关于构成 *definition* 而不是 *theorem* 的细节，这是一个需要从基本假设中证明的结果。至少在 *definition* (，在我们的上下文中)，从 A 到 B (的一个注入和满射，请注意)，构成了等势性的充分证明，这保证了双射。同样，从 A 到 B 的一个注入和一个从 B 到 A 的注入足以保证 $|A| = |B|$，因此 A 和 B 之间必须存在一个双射。

尽管不是 *totally obvious*，但这些主张为什么应该是真实的呢？假设我们有一个从 A 到 B 的注入和一个从 B 到 A 的注入。这 *guarantee* 两个集合之间的双射吗？嗯，人们希望如此！但这不是证明。这个结果实际上被称为 **Cantor-Schroeder-Bernstein Theorem**：

Theorem 7.6.6 (康托尔-施罗德-伯恩斯坦)**.** *Suppose A, B are any sets, and $f : A \to B$ and $g : B \to A$ are injections. Then there exists a* 双射 *$h : A \to B$.*

是的，那是一个 *theorem*；它不是平凡的！其中一个证明实际上就是 *constructive*：它提供了一种构造那个双射 $h : A \to B$ 的算法方法，使用两个注入，$f : A \to B$ 和 $g : B \to A$。就我们的目的——以及时间和空间限制而言——没有必要将其作为一个定理单独提出来，更不用说是一个具有构造性证明的定理了。考虑注入和满射及其相对于基数的结果作为 *definitions* 就足够了；这些结果“感觉”上是直观的，我们可以接受它们。不过，请记住，我们是在基于严格的数学知识。如果你对了解这些细微差别及其后果感兴趣，考虑参加关于 **set theory** 的课程或阅读相关书籍。

本质上，真正的问题是，我们预先假设了两个集合 *any*，A 和 B，它们可以在某种有意义的数学方式下具有它们的基数 *compared*。也就是说，对于任何 A 和 B，我们预先假设我们可以以某种方式声明 $|A| \leq |B|$ 或 $|B| \leq |A|$ 有意义（或者如果集合“大小相等”，也许两者都有意义）。但是，我们如何 *guarantee* 这样的比较，或者两者都适用，对于任何两个给定的集合？这不是一个简单的问题！在本书的背景下，我们的一个公理是，我们考虑的任何两个集合的基数都可以进行比较。然而，在数学宇宙的背景下，这需要从更基本的假设中证明。

7.6.2 Finite Sets

在进入这个有些奇特（但非常迷人！）的无限集合世界之前，让我们先关注一些关于 **finite** 集合的结果。这些结果将更容易理解，直观，并将使我们通过函数及其性质来证明关于基数的事实获得一些良好的实践。

Theorems

对于这些结果中的每一个，我们将陈述一个定理/命题/引理，并对其进行证明或通过一些练习让您帮助我们进行证明。

Theorem 7.6.7. *Suppose A, B are* 不交集 *finite sets. Then $|A \cup B| = |A| + |B|$.*

在示例中尝试一下，看看为什么这个说法是 True。你明白为什么我们需要集合是 *disjoint* 才能使这起作用吗？你能证明这个说法吗？记住，我们想要在这两个集合之间找到一个 *bijection*……

Proof. Let A, B be finite sets that are disjoint.

We know $\exists a, b \in \mathbb{N} \cup \{0\}$ and there exist bijections $f : A \to [a]$ and $g : B \to [b]$.

(Tha t 是，我们假设 $|A| = a$ 和 $|B| = b$)。设这样的 a, b, f, g b e 给定。

WWTS $|A \cup B| = |A| + |B| = a + b$；即，在WWTS中存在一个双射 $h : A \cup B \to [a + b]$。

定义函数 $h : A \cup B \to [a + b]$ 为

$$\forall x \in A \cup B. \quad h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) + a & \text{if } x \in B \end{cases}$$

注意，h 被良好定义，因为 $A \cap B = \varnothing$，所以每个 $x \in A \cup B$ 都满足 $x \in A$ 或 $x \in B$，当然不是两者都满足。此外，对于每个 $x \in A$，有 $1 \le h(x) \le a$，对于每个 $x \in B$，有 $a + 1 \le h(x) \le a + b$，因此对于 h 的定义域中的每个 x，有 $h(x) \in [a + b]$。

我们断言函数 $H : [a + b] \to A \cup B$，定义为

$$\forall y \in [a + b]. \quad H(y) = \begin{cases} f^{-1}(y) & \text{if } 1 \le y \le a \\ g^{-1}(y - a) & \text{if } a + 1 \le y \le a + b \end{cases}$$

是 h 的逆。如果这成立，那么我们就证明了 h 是一个双射。

让我们证明 H 是良好定义的。每个 $y \in [a + b]$ 满足定义 H 中给出的两个不等式之一。此外，f 和 g 被给出是双射，因此 f^{-1} 和 g^{-1} 是良好定义的函数（它们本身也是双射）。进一步地，如果 $a + 1 \le y \le a + b$ 则 $1 \le y - a \le b$ 所以 $y - a \in [b]$（g^{-1} 的定义域）。

让我们证明 $h \circ H = \mathrm{Id}_{[a+b]}$。设 $y \in [a + b]$ 为已知。我们有两种情况。

(1) 假设 $1 \le y \le a$；即，假设 $y \in [a]$。然后，

$$(h \circ H)(y) = h(H(y)) = h\big(f^{-1}(y)\big) = f\big(f^{-1}(y)\big) = \mathrm{Id}_{[a]}(y) = y$$

我们在其中使用了事实 $f^{-1}(y) \in A$。

(2) 假设 $a + 1 \le y \le b$；即，假设 $y - a \in [b]$。那么，

$$\begin{aligned}(h \circ H)(y) = h(H(y)) &= h\big(g^{-1}(y - a)\big) = g\big(g^{-1}(y - a)\big) + a \\ &= \mathrm{Id}_{[b]}(y - a) + a = (y - a) + a = y\end{aligned}$$

我们在其中使用了 $g^{-1}(y - a) \in B$ 的性质。

在任何情况下，我们都找到$(h \circ H)(y) = y$，并且这两种情况是互斥的，覆盖了所有可能性。

接下来，让我们证明 $H \circ h = \mathrm{Id}_{A \cup B}$。设 $x \in A \cup B$ 为已知。我们有两种情况。

(1) 假设 $x \in A$。那么，

$$(H \circ h)(x) = H(h(x)) = H\big(f(x)\big) = f^{-1}\big(f(x)\big) = \mathrm{Id}_A(x) = A$$

我们在其中使用了事实，即 $f(x) \in [a]$。

(2) 假设 $x \in B$。然后，

$$(H \circ h)(x) = H(h(x)) = H\big(g(x) + a\big) = g^{-1}\Big(\big(g(x) + a\big) - a\Big)$$
$$= g^{-1}\big(g(x)\big) = \mathrm{Id}_B(x) = x$$

我们在其中使用了事实 $g(x) \in [b]$ 因此 $a + 1 \leq g(x) + a \leq a + b$。

在任何情况下，我们都找到$(H \circ h)(x) = x$，并且这两种情况是互斥的，覆盖了所有可能性。

因此，$H = h^{-1}$，所以 h 有逆元。因此，h 是一个双射。

Therefore, $|A \cup B| = \big|\,[a+b]\,\big| = a + b = |A| + |B|$. □

Corollary 7.6.8. *Suppose S, T are finite sets and $S \subseteq T$. Then, $|T - S| = |T| - |S|$.*

Proof. 定义 $U = T - S$。注意 $U \cap S = \varnothing$。将上述定理应用于 U 和 S，得到

$$|U| + |S| = |U \cup S| = |T|$$

从两边减去以得到 $|T - S| = |U| = |T| - |S|$。 □

您可以使用上述两个结果来证明以下推广：{v*}

Proposition 7.6.9. *Suppose A, B are finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof. 作为第7.6.5节中的练习1留给读者。 □

这是上述定理的另一个推论。

Corollary 7.6.10. *Suppose $A_1, A_2, \ldots, A_n$ are finite and pairwise-disjoint (remember this means any two of the sets are disjoint).*

Then $|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$.

Proof. 作为第7.6.5节中的练习2留给读者。 □

您还应该查看本章练习中的问题7.8.32。在那里，我们通过两个变量的归纳法引导您证明两个有限集合的 *Cartesian product* 的大小。

7.6.3 Countably Infinite Sets

让我们继续研究可数无限集合的领域。我们将从一个著名的思想实验开始，这个实验以数学家大卫·希尔伯特的名字命名。

The Hilbert Hotel

让我们玩假装游戏。这有助于我们掌握无穷的奇怪之处。

假设我们拥有一家酒店。在我们的神奇建筑中，房间数量是可数无穷的。它们被编号为1号房间、2号房间、3号房间、……也就是说，我们的房间由自然数集*indexed*、$\mathbb{N}$组成。

我们想容纳尽可能多的人（为了赚很多钱！）而且由于我们的酒店非常时尚且宽敞，我们的客人完全愿意在我们要求时搬到新房间。他们只需要几分钟时间收拾好他们的东西，然后沿着走廊走到新房间。

我们还有一个扬声器系统，可以让我们一次性向所有客人传达信息。

- 假设所有房间都已满员。这是一个非常繁忙的周末。有一个人走进大堂，想找一间房间。我们能挤进去吗？如果不能，为什么？如果能，怎么挤？

  结果显示我们可以！我们只需将所有客人向下移动一个房间，并将这位新来的客人安排在1号房间。

  捕捉的关键是利用我们的扬声器系统。如果我们不得不去敲*everyone's*的门告诉他们搬到下一个房间，我们就会*never actually finish*；我们会花费永恒的时间敲门和传递信息。

  相反，我们做出以下公告：

  > 注意客人：如果您发现自己身处n房间，请移至$n+$房间 1. 感谢！

  五分钟后，客人都已离开，1号房间为新客人空出。

  从道德上讲，我们刚刚验证了对于任何特定的对象$\star$，集合$\mathbb{N}$和集合$\mathbb{N} \cup \{\star\}$具有相同的基数。特别是，比如说$|\mathbb{N}| = |\mathbb{N} \cup \{0\}|$。我们的酒店只有可数多个房间，并且我们已经为每个自然数安排了一个人，以及一个*more*人。

- 第二天。我们的房间仍然满员。假设有一个有可数无限多人的Scrabble会议出现。人们都戴着带有自然数的名牌，所以有第1个人，第2个人，第3个人，……。

  我们能容纳这些人吗？我们如何分配房间给他们？我们如何处理目前在酒店里的客人？

  结果是我们可以！想法是释放一个无限集的房间。

再次，关键是要通过一次性向*all*客人发出一项全面公告来实现，而不是逐一敲门。

我们认识到偶数房间集合和奇数房间集合都是无限的，因此让我们让当前酒店客人占据偶数房间，并将会议的新客人分配到奇数房间。我们通过扬声器向酒店客人做出以下宣布：

> 注意客人：如果您发现自己身处n房间，请移至2n房间。谢谢！

然后，我们向在大厅等待的会议人员做出以下公告：

> 请注意：如果您佩戴的姓名牌编号为 n，请前往2n −号房间。1 . 感谢！

五分钟后，每位酒店客人已经移动，再过五分钟，每位会议参与者都找到了他们的房间。Voilá！

从道德上讲，我们刚刚验证了两个不相交的可数无穷集合的并集也是可数无穷的。也就是说，我们取了当前酒店客人的集合A（注意A是可数无穷的）和等待房间的会议客人的集合B（注意B是可数无穷的，并且注意$A \cap B = \varnothing$），并找到了$A \cup B$和$\mathbb{N}$之间的双射，其中$\mathbb{N}$代表房间集合。

- 现在，假设出现了一种新的惯例。他们用不同的语言玩Scrabble，所以不想与其他惯例联系在一起。我们如何调动人们，让每个人都有一间房间？

  我们可以做完全一样的事情！这就像我们之前面临同样的情况一样，只是酒店满了，还有可数无限多的人等着房间。

- 现在，假设有可数无穷多个惯例出现，每个都不想与其他相关联。哦我的！

  幸运的是，酒店会议组织者已经为每个会议分配了一个自然数，并且每个会议内的成员都会得到一个印有该数字的帽子。此外，在每次会议中，每个人都会被分配一个自然数，他们佩戴一个带有该数字的徽章。因此，每个人都有两种身份识别方式：一顶帽子和一个徽章。所以我们有来自第1次会议的第1个人，来自第7次会议的第3个人，来自第8次会议的第12个人，等等。

  我们如何在酒店重新安排所有人？我们甚至能做吗？我们如何做它*efficiently*？

这里的问题是，我们反复应用与前面两个案例相同的方法 **cannot**。是的，我们可以用那种方法挤进公约1。完成之后，我们会挤进公约2。以此类推。但 **never** 我们会到达 all 的公约。这是之前我们遇到的问题，即敲每个个体的门需要花费很长时间才能完成；我们需要向 $everyone\ at\ once$ 发送消息。同样，在这里，我们需要向所有酒店客人发送消息，然后向所有在门外等待的会议参与者发送消息。需要的是一个关于哪个房间要去的“通用公式”。

如果有助于理解，请从情况另一面思考。假设你身处大会 x，并且你是那个大会中的个人 y。你正急切地期待着一张舒适的床过夜。你想要知道 $exactly$ 去哪个房间。尽快。你不想四处闲逛，一个接一个地查看你前面的所有大会分配的房间。你想要 all 一次性进入并找到你对应的房间。

这里有一种方法可以做到。让我们利用 $prime\ numbers$ 的结构。我们知道存在可数无穷多个质数，并且对于任意两个质数 $different\, p$ 和 q（，即 $p \neq q$），对于任何自然数 k，都成立 $p^k \neq q^k$。考虑到这一点，我们发现，将单个惯例分配给对应质数的幂的房间，我们可以确保没有两个（潜在的）客人被分配到同一个房间。我们向当前的酒店客人做出以下宣布：

> 注意客人：如果您发现自己身处n房间，请移至2^n房间。谢谢！

我们随后向门外等待的会议做出以下宣布：

> 请注意，大会参与者：
>
> 如果您是第 k 号参会者，请前往第 1 号会议的第 3^k 号房间。
>
> 如果您是第 k 号参会者，来自第 2 号会议，请前往第 5^k 号房间。
>
> 如果您是第 k 号参会者，来自第 3 号会议，请前往第 7^k 号房间。
>
> 通常，如果您是大会编号 n 的第 k 号人员，请前往由 $(n+1)$-次质数幂的第 k 次方确定的房间编号。
>
> 谢谢！

(注意：我们假设所有我们的客人和潜在客人都是数学天才，他们可以迅速计算出 $(n+1)$-th 质数)

数字是，并将其提高到k次幂。否则，我们最初就不希望他们在我们豪华的数学酒店里停留！）

请注意，这保证了*everyone*有一个房间完全属于他们。没有人需要共享房间。然而，它*does*会留下许多房间*empty*。谁在1号房间？6号房间？18号房间？一般来说，你能描述将空置的房间集合吗？

我们怎么能在这方面更“高效”呢？我们能否发布某个公告，以便*all*房间被填满？

从道德上讲，我们刚刚验证了$\mathbb{N}$和$\mathbb{N} \times \mathbb{N}$具有相同的基数。我们与可数无限多的人有可数无限多的习俗，所以每个我们想要容纳的人都对应一个*ordered pair of natural numbers*，其中第一个坐标是他们的个人编号，第二个坐标是他们的习俗编号。由于我们能够将这些人匹配到房间集合（对应于$\mathbb{N}$），因此我们证明了$\mathbb{N} \times \mathbb{N}$是可数的。（注意：我们实际上“做得过头了”，并找到了一种将集合$\mathbb{N} \times \mathbb{N}$嵌入到$\mathbb{N}$的*strict subset*中的方法！）

这或许能让你对可数无穷的概念有所体会。一个需要记住的重要点是，在这里，**infinity**是一个**cardinality**，而不是一个**number**。并不是自然数“一直持续”下去，并且存在某个神奇数字∞在它们之后。在这里，我们将可数*infinite*称为一个**cardinality**；它代表某物“有多大”。它更像一个*magnitude*，而不是一个*position*。

Examples

让我们从 **Hilbert Hotel** 例子传达的一些想法中汲取灵感，并以更正式的方式表达它们。我们将利用注入、满射和双射。 (哦我的天哪！）以下结果在接下来的过程中将非常有用，所以现在让我们来证明它。

Lemma 7.6.11. *Let S, T be any sets. Suppose $S \subseteq T$. Then $|S| \leq |T|$.*

Proof. 定义“恒等函数” $f\colon S \to T$，由$\forall x \in S$给出。 $f(x) = x$.
自 $S \subseteq T$ 以来，这是一个定义良好的函数。

（注意：我们无法从技术上将其定义为通常的恒等函数 Id_S，因为定义域和值域可能不是相等的集合；本质上，f 执行与 Id_A 相同的操作，但具有不同的值域）。

注意 f 是单射的！

（注意：它不一定是一一对应的，因为可能存在 $S \neq T$ 的情况。）

由于 f 是单射的，这告诉我们 $|A| \leq |B|$。 □

您可能想知道为什么我们在这里不能得出 $|A| < |B|$。为什么是“$\leq$”而不是其他呢？当然，$\{1, 2\} \subseteq \{1, 2, 3\}$ 以及 $|\{1, 2\}| = 2 < 3 = |\{1, 2, 3\}$。这对于 **finite** 集是正确的，但正如我们将在本节中看到的，还有 **infinite** 集具有相等基数 *strict* 的子集！

Example 7.6.12. $\mathbb{Z}$ **is countably infinite:**

我们知道 $\mathbb{N}$ 通过 *definition* 是可数无限的。恒等函数 $\mathrm{Id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ 显然是一个双射，因此 $\mathbb{N}$ 是可数的。

在这个例子中，我们将证明$\mathbb{Z}$是可数无限的！为了完成这个证明，我们需要找到一个双射$f\colon\ \mathbb{Z} \to \mathbb{N}$。我们在这里陈述一个，然后通过找到它的*inverse*来证明它是一个双射。在继续阅读之前，试着自己找一个双射！也许你会想出一个不同于我们的函数！如果你需要一些提示来想出一个，想想这个：为了证明一个无限集是*countably*无限的，我们想要找到一种方法来逐个*listing*元素。试着找到一个模式来识别“第一个”整数，然后是“第二个”，然后是“第三个”，……

让我们定义一个函数 $f : \mathbb{Z} \to \mathbb{N}$，然后通过识别 f^{-1} 来证明它是一个双射。

Explicit bijection: 我们选择通过设置来定义 $f : \mathbb{Z} \to \mathbb{N}$

$$\forall z \in \mathbb{Z}.\ f(z) = \begin{cases} -2z + 2 & \text{if } z \leq 0 \\ 2z - 1 & \text{if } z > 0 \end{cases}$$

我们选择这个函数，因为它“配对”整数与自然数，如下所示：

$$\begin{array}{cccccccccc} \ldots, & -3, & -2, & -1, & 0, & 1, & 2, & 3, & \ldots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \ldots, & 8, & 6, & 4, & 2, & 1, & 3, & 5, & \ldots \end{array}$$

(这是，我们将偶数自然数与非正整数配对，将奇数自然数与正整数配对。观察这种对应关系，我们可以看到如何“反转”它。这就是我们将找到 f 的逆元的方法.)

接下来，定义 $F : \mathbb{N} \to \mathbb{Z}$ 为

$$F(n) = \begin{cases} -\frac{n}{2} + 1 & \text{if } n \text{ is even} \\ \frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

让我们展示 $F = f^{-1}$。设 $z \in \mathbb{Z}$ 为已知。我们有两种情况。

- 假设 $z \geq 1$。那么 $f(z) = 2z - 1$。注意 $2z - 1 \in \mathbb{N}$ 和 $2z - 1$ 是奇数。这意味着

$$(F \circ f)(z) = F(f(z)) = F(2z - 1) = \frac{(2z - 1) + 1}{2} = \frac{2z}{2} = z$$

- 假设 $z \leq 0$。那么 $f(z) = -2z + 2$。注意 $-2z \geq 0$ 所以 $-2z + 2 \geq 2$ 因此 $-2z + 2 \in \mathbb{N}$。此外，$-2z + 2$ 是偶数。这意味着

$$\begin{aligned}(F \circ f)(z) = F(f(z)) = F(-2z + 2) &= -\frac{-2z + 2}{2} + 1 \\ &= -(-z + 1) + 1 = (z - 1) + 1 = z\end{aligned}$$

在任何情况下，$(F \circ f)(z) = z$。这表明 $F \circ f = \mathrm{Id}_{\mathbb{Z}}$。

接下来，设 $n \in \mathbb{N}$。我们有两种情况。

- 假设 n 是偶数。那么 $F(n) = -\frac{n}{2} + 1$. 注意到 $\frac{n}{2} \geq 1$，因此 $-\frac{n}{2} \leq -1 + 1 = 0$。这意味着

$$\begin{aligned}(f \circ F)(n) = f(F(n)) = f\left(-\frac{n}{2} + 1\right) &= -2\left(-\frac{n}{2} + 1\right) + 2 \\ &= \left(\frac{2n}{2} - 2\right) + 2 = n\end{aligned}$$

- 假设 n 是奇数。那么 $F(n) = \frac{n+1}{2}$。注意 $n + 1 \geq 2$ 因此 $\frac{n+1}{2} \geq 1$。这意味着

$$\begin{aligned}(f \circ F)(n) = f(F(n)) = f\left(\frac{n+1}{2}\right) &= 2\left(\frac{n+1}{2}\right) - 1 = \frac{2n+2}{2} - 1 \\ &= (n + 1) - 1 = n\end{aligned}$$

在任何情况下，$(f \circ F)(n) = n$。这表明 $f \circ F = \mathrm{Id}_{\mathbb{N}}$。因此，$F = f^{-1}$。 □

这表明 $\mathbb{Z}$ 和 $\mathbb{N}$ 具有相同的基数，即 $|\mathbb{Z}| = |\mathbb{N}|$。你可能觉得整数比自然数多一倍，但这是你的直觉出错的地方。我们可以逐个 *pair up* 这两个集合的元素，因此它们必须具有相同的大小！这是一个例子，说明了为什么引理7.6.11的结论是最好的。在这里，$\mathbb{N} \subset \mathbb{Z}$ (a *strict* 是) 的一个子集，但 $|\mathbb{N}| = |\mathbb{Z}|$。这只有在有无限（而不是有限）集合的情况下才会发生，这里是一个这样的例子。

(本节稍后，我们实际上将 *prove* 这是一种描述集合无限性的等价方式：我们是否能够找到一个集合与其自身的 *strict* 子集之间的双射。)

Example 7.6.13. $\mathbb{N} \times \mathbb{N}$ **is countably infinite:**

与上一节中的 **Hilbert Hotel** 讨论一样，我们本质上论证了 $\mathbb{N} \times \mathbb{N}$ 与 $\mathbb{N}$ 具有相同的基数。当我们有无限可数多个公约，每个公约中都有无限可数多个人时，我们能够用无限可数多个房间将它们全部放入我们的酒店！但这更多是一种直观讨论，因此让我们在这里正式证明这一事实。我们将在这两个集合之间找到一个明确的 *bijection*。

与其求其逆，我们将会证明它是满射的，并请求您的帮助来证明它是单射的。

Explicit bijection: 定义 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 通过设置

$$\forall (x, y) \in \mathbb{N} \times \mathbb{N}. \quad f(x, y) = 2^{x-1}(2y - 1)$$

在证明 f 是双射时，我们将证明这个 f act:

> 每个自然数都可以写成*uniquely*的形式，即2的幂乘以一个奇数自然数。

查看我们定义的函数。它接受一对自然数，并输出2的幂次乘以一个奇数自然数。证明这是一个双射表明它永远不会输出相同的自然数两次（注入性）并且每个自然数都是某个对的输出（满射性）。你可能尝试玩弄这个函数，输入一些值并看看会发生什么。你也可以尝试“反向”工作，试图弄清楚f^{-1}可能做什么。例如，取你最喜欢的$n \in \mathbb{N}$。你能将它表示为2的幂次乘以一个奇数吗？如果n是奇数，这相当简单，因为$2^0 = 1$。例如，

$$11 = 1 \cdot 11 = 2^0 \cdot (2 \cdot 6 - 1) = f(1, 6)$$

(注意我们在 f 的定义中必须使用 $x - 1$ 和 $2y - 1$，因为我们正在处理 $\mathbb{N}$，以及 $0 \notin \mathbb{N}$。)

如果 n 是偶数，我们可以简单地迭代除以 2，直到不能再除为止；剩下的必须是奇数。例如：

$$40 = 2 \cdot 20 = 4 \cdot 10 = 8 \cdot 5 = 2^3 \cdot (2 \cdot 3 - 1) = f(4, 3)$$

和

$$32 = 2 \cdot 16 = 2^2 \cdot 8 = 2^3 \cdot 4 = 2^4 \cdot 2 = 2^5 = 2^5 \cdot (2 \cdot 1 - 1) = f(6, 1)$$

这个观察对于证明 f 是满射至关重要：

f is surjective: 我们主张 $\forall n \in \mathbb{N}$。

BC: 注意 $f(1, 1) = 2^0 \cdot 1 = 1$。因此 $1 \in \text{Im}_f(\mathbb{N} \times \mathbb{N})$。

We prove this by a minimal criminal argument.

IH: 假设我们有一个 $n \in \mathbb{N} - \{1\}$，它没有作为2的幂乘以奇数的表示，即假设 $n \notin \text{Im}_f(\mathbb{N} \times \mathbb{N})$。

IS: 我们有两种情况：

- 如果 n 是奇数，那么……嗯，$n \cdot 2^0 = n \cdot 1 = n$ 是这样的表示。也就是说，我们知道 $\frac{n+1}{2} \in \mathbb{N}$ 并且我们看到

  $$f\left(1, \frac{n+1}{2}\right) = 2^0 \cdot \left(2 \cdot \frac{n+1}{2} - 1\right) = 1 \cdot (n + 1 - 1) = n$$

  所以 $n \in \text{Im}_f(\mathbb{N} \times \mathbb{N})$。这与我们的假设 $n \notin \text{Im}_f(\mathbb{N} \times \mathbb{N})$ 相矛盾，因此这种情况不成立。

- 如果 n 是偶数，那么，考虑 $\frac{n}{2}$。在 AFSOC 中，我们有 $\frac{n}{2}$ 的表示为 2 的幂次乘以一个奇数，即假设 $\frac{n}{2} \in \text{Im}_f(\mathbb{N} \times \mathbb{N})$。这意味着 $\exists (x, y) \in \mathbb{N} \times \mathbb{N}$。

  $f(x, y) = \frac{n}{2}$. Let such (x, y) be given. Consider then $f(x, y) = 2 \cdot \frac{n}{2} = n$

  $f(x + 1, y)$ (which is valid since $x + 1 \in \mathbb{N}$, as well). We see that

  这表明我们会有这样的表示形式 n；即实际上，$n \in \text{Im}_f(\mathbb{N} \times \mathbb{N})$。再次，这与我们假设的 $n \notin \text{Im}_f(\mathbb{N} \times \mathbb{N})$ 相矛盾。

  因此，$\frac{n}{2}$ *also*没有这样的表示，即$\frac{n}{2} \notin \text{Im}_f(\mathbb{N} \times \mathbb{N})$。

我们已经表明，假设 n 是该命题的反例，$\frac{n}{2}$ 是该命题的 *smaller* 反例。通过“最小犯罪”论证（因为我们已经证明了我们的基本情况），我们得出结论，该命题对每个 $n \in \mathbb{N}$ 都成立。这表明 f 是满射的。

□

(注意：您可能需要回顾第5.5.1节，以刷新您对“最小犯罪”论点如何工作的记忆。)

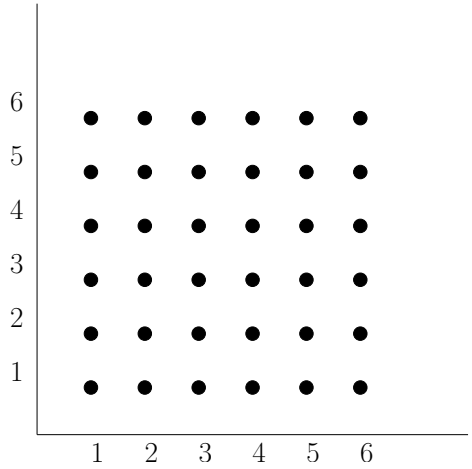
f is injective: 你证明这个！见练习7.8.21。

一起，我们已经证明 f 是一个双射，因此 $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$。也就是说，$\mathbb{N} \times \mathbb{N}$，所有自然数的有序 *pairs* 的集合，是可数无穷的。这让你感到惊讶吗？这看起来反直觉吗？你认为关于所有自然数的有序 *triplets* 的集合 $\mathbb{N}^3$ 可能是什么？如果你取 $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \cdots$，你认为会发生什么？思考这些想法。与你的同学讨论，并尝试证明一些东西！

Example 7.6.14. $\mathbb{N} \times \mathbb{N}$ **as a lattice:**

在继续到另一个例子之前，让我们再展示一种思考为什么 $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ 的方法。这将会是一个直观的解释，更像是描述如何定义集合之间的双射，而不实际给出定义。然而，这是一个常见的论点，非常值得一看。

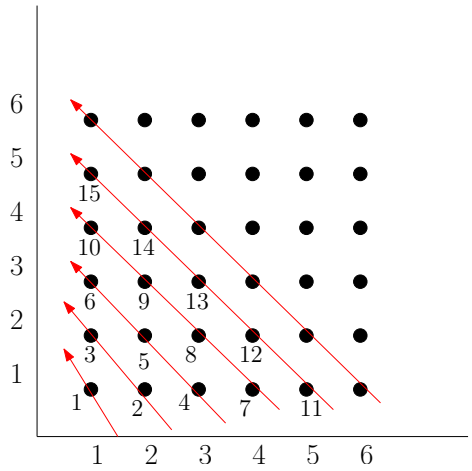
想法是将 $\mathbb{N} \times \mathbb{N}$ 视为一个点集的 *lattice*，如下所示：



为了表明这个点阵是 **countably** 无穷的，我们可以描述一条路径，它穿越 *all* 的点（满射性！）一次（单射性！）并且由自然数索引（可数无穷！）来表示。也就是说，我们可以仅仅描述一种通过一系列步骤遍历整个网格的方法；将会有“第一个点”和“第二个点”等等。

关键观察点是，这个网格的“西北”对角线都是 **finite**。例如，从点 (5, 1) 开始，向上和向左移动，斜着走。你会经过 (4, 2)、(3, 3)、(2, 4) 和 (1, 5)，然后到达网格的边界。无论 *where* 你从网格底部的行开始，这都是正确的。

让我们使用这个事实来根据（a）它位于哪个对角线上，以及（b）它在对角线上的位置，用自然数对每个晶格点进行标记。我们将从（1, 1）开始的对角线视为第1对角线，从（2, 1）开始的视为第2对角线，依此类推。这给我们以下标签：



我们可以看到晶格中的每个点都将位于恰好一条这样的对角线上。此外，存在可数无穷多条这样的对角线（它们由$\mathbb{N}$索引）并且每条对角线上只有*finitely*个点。这意味着（正如我们将在下面证明的那样）对角线上的点集合*all*是可数无穷的。

你应该尝试通过写下实现我们所展示标签的函数来验证 *formalizing* 这个论点。或者，至少你可以使用一个类似且有效的方法，即你可以向东南方向移动，或者反转交替对角线的方向……

Example 7.6.15. $\mathbb{Q}$ **is countably infinite:**

这个结果是关于我们的直觉*failing*与无限集合及其基数的一个更引人注目的例子。想象一下$\mathbb{Q}$的元素在实数线上的排列。它们无处不在！实际上，看看练习4.11.26；在那里，你证明了有理数是**dense**，而且它们也是稠密的*in* $\mathbb{R}$ (，即在任意两个不同的实数之间都存在一个有理数)。此外，有理数集*seems*比$\mathbb{Z}$大得多：仅在0和1之间，就存在无限多个有理数！因此，你可能会认为$\mathbb{Q}$是不可数的无限大，但这是False。

在这个例子中，我们将提出几个支持这一事实的论点，尤其是因为我们意识到它是如此奇怪和引人注目。{v*}

(1) **Intuitive argument:**

考虑以下将 $\mathbb{Q}$ 表示为集合并的“表示”：

$$\mathbb{Q} \text{ “=” “}\mathbb{N}\times\mathbb{N}\text{” } \cup \text{ “}-\text{”}(\mathbb{N}\times\mathbb{N}) \cup \{0\}$$

在某些意义上，$\mathbb{N}\times\mathbb{N}$ 对应于所有正有理数。为了了解原因，只需考虑由 $f(x,y) = \frac{x}{y}$ 定义的功能 $f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{Q}_+$。我们确实输出所有正有理数（因此 f 是满射），但 $\frac{4}{2} = \frac{2}{1}$ 因此这不是一个单射。至少，这表明 $|\mathbb{N}\times\mathbb{N}| \geq |\mathbb{Q}|$ 因为 f 是一个满射。由于 $\mathbb{N}\times\mathbb{N}$ 是可数无穷的，并且我们确实期望 $\mathbb{Q}$ 是无限的，这表明正有理数是可数无穷的。

负有理数集——让我们称其为$\mathbb{Q}_-$——必须与正有理数集——让我们称其为$\mathbb{Q}_+$——具有相同的基数，它们之间存在一个明显的双射：通过设定g：

所有这些省略的都是0！$\mathbb{Q}$ 两个可数无限集的并集也是可数无限（我们将在下面证明），添加一个额外的元素也不会改变这一点，因此，$\mathbb{Q}$ 是可数无限。

请注意，这相当“随意”。上面“方程”中的所有“引号”都意味着你应该将其视为只是一个启发式论证，而不是一个证明。然而，有方法可以使所有这些论证形式化。试着自己试试！

(2) **Listing** $\mathbb{Q}$**:**

考虑编写一个计算机程序来打印出列表中所有正有理数。你会使用什么算法？只要你能保证你的程序“最终”会成功并打印出它们，那么你就证明了$\mathbb{Q}$可以逐个枚举，因此它必须是可数的无限。（记住，这就是我们为什么使用$\mathbb{N}$作为*canonical*可数无限集的原因：我们可以逐个枚举其元素，我们可以*count*它们。）

这里是我们可能编写此类程序的一种方法：遵循与之前示例中用于 $\mathbb{N} \times \mathbb{N}$ 的相同的“通过晶格的路径”论点。不过，这次只需“跳过”您已经打印出的任何有理数。

这意味着我们将打印对（1, 1）$\leftrightarrow$ 1，然后（2, 1）$\leftrightarrow$ 2，然后（1, 2）$\leftrightarrow \frac{1}{2}$，然后（3, 1）$\leftrightarrow$ 3，然后……

Aha！我们必须省略写（2, 2）$\leftrightarrow$ 1。我们是怎么知道的？我们*see*我们已经打印了1。我们是怎么知道的？我们只是浏览了我们已经打印的有理数列表，并检查我们即将打印的内容是否已经出现。如果是这样，我们就继续；如果不是，我们就打印它，然后继续。

在枚举过程中，这仅仅意味着对于通过晶格的每一个点，我们必须检查 *finitely-many* 件事情；也就是说，我们必须查看我们已经打印过的 *finitely-large* 个有理数集合。这意味着在任何单个步骤中的打印过程将“稍微长一点”，但不是 *infinitely-longer*。因此，我们的程序最终将打印出每一个有理数；无论你心里想的是哪一个，我们都会在有限的时间内到达那里。

(3) $\mathbb{Q}$ **is *at most* countably infinite:**

这里还有一个关于 $\mathbb{Q}$ 是可数的论点。（如果这感觉像是过度，那也行，继续就好。我们只知道这是一个令人惊讶的结果，有几种思考方式可能有助于理解！）

考虑这一点：我们可以事先肯定地同意 $|\mathbb{Q}| \geq |\mathbb{N}|$。这从 $\mathbb{Q} \supseteq \mathbb{N}$ 的事实中得出。现在，唯一的问题是这些基数是否是 *equal*。为了得出这个结论，我们需要找到（a）从 $\mathbb{Q}$ 到可数集的注入，或者（b）从可数集到 $\mathbb{Q}$ 的满射。

我们将证明以下内容：$\mathbb{Z} \times \mathbb{N}$ 是可数的。（也就是说，我们将普遍证明任意两个可数无穷集合的笛卡尔积也是可数无穷的。）然后我们可以通过以下方式定义函数 $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$：

$$\forall (z, n) \in \mathbb{Z} \times \mathbb{N}. \quad f(z, n) = \frac{z}{n}$$

这是一个到 $\mathbb{Q}$ 的满射。它显然不是单射（为什么不是？）但我们不在乎。它表明 $|\mathbb{Z} \times \mathbb{N}| = |\mathbb{Q}|$。一旦我们证明了 $|\mathbb{Z} \times \mathbb{N}| = |\mathbb{N}|$，这将表明 $|\mathbb{N}| = |\mathbb{Q}|$。

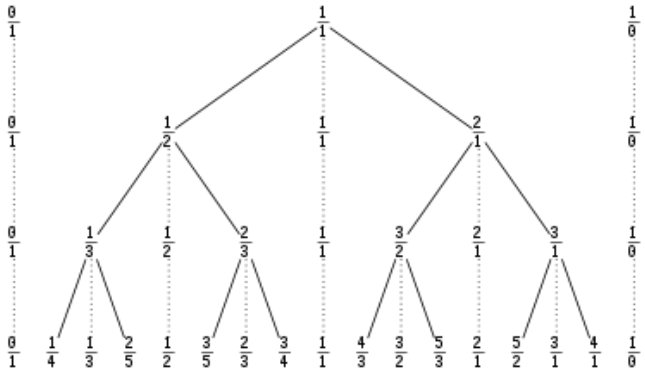
(4{v²}

存在其他 $\mathbb{Q}$ 的视觉表示！**Stern-Brocot Tree** 尤其是启发人心。实际上，这个想法最初是由一位名叫 Achille Brocot 的法国钟表匠引入并发展的，他正在寻找在制作手表时所需齿轮的近似测量方法。在差不多同一时间（19世纪50年代和60年代），德国数学家 Moritz Stern 也发展了这个想法。想到一个非数学家会 *indpendently* 发展这个迷人的想法来解决他面临的现实世界问题，真是令人惊讶！

(不要过分担心这里 *graphs* 和 *trees* 的术语。我们不会过多地讨论这些，只是介绍这种表示 $\mathbb{Q}$ 的方法，并证明它是可数无限的。)

这棵树的 **root** 是 1。（这是图中最顶部的数字。）生成位于树中的点 *below* 的) 的方法是用连分数来定义的。（我们在这里不会描述这意味着什么；相反，我们将在下面描述如何 *construct* 树。）

这种情况发生的是，从根节点到另一个节点的任何路径都会得到一个有理数序列 *sequence*，这些有理数是越来越接近最终节点的更好近似；此外，序列中的每个后续有理数的分母都比前一个大。这就是激发布罗科先生兴趣的性质。他需要确定在手表内部制作两个齿轮的大小，使得它们的 *ratio* 非常接近一个特定的数字。通过从这棵树向下工作，他可以找到更好的近似比例来满足他所需的数字！很酷，对吧?



为了实际上 *construct* 树，我们找到 *mediants*。给定两个有理数 $\frac{a}{b}$ 和 $\frac{c}{d}$，这两个数的调和平均定义为 $\frac{a+b}{c+d}$。（注意，这是一个特殊的

obj 等等，中项；它是 *not* 添加两个分数的正确方式　　动作！

每个树的层级由从上一层级连续有理数对中生成的所有中项组成；我们不“计数”直接垂直的元素；它们只是为了阅读和构建的方便而保留。此外，请注意，分数 $\frac{0}{1}$ 和 $\frac{1}{0}$（（这是未定义的，甚至！）以及) 都包含在外侧列中，以帮助生成每个层级外侧的元素。

(在这个树的属性上玩玩，并了解更多。它是一个有趣的数学对象！)

我们在这里不会证明这棵树包含 *all* 有理数，但我们认为你可以看到为什么这是可信的。此外，我们认为你可以看到为什么这棵树中所有节点的集合是 **countably** 无穷的。每一层只有有限个节点，而且有可数无穷多个层次。

Theorems

现在我们知道，我们标准数集的三组——$\mathbb{N}$、$\mathbb{Z}$和$\mathbb{Q}$——都是可数无穷的，以及集合$\mathbb{N}\times\mathbb{N}$。通过以下定理，我们将向您展示一些从现有集合生成更多可数无穷集合的方法。

让我们用一个有用的结果让你热身。它说我们可以取一个可数无限集，并“附加”有限多个额外元素，这样结果仍然是可数无限。

Lemma 7.6.16. *If A is countably infinite and B is finite and $A\cap B=\varnothing$, then $A\cup B$ is countably infinite.*

Proof. 作为练习7.8.19留给读者。

Hint: 尝试使用与我们的定理7.6.7证明类似的想法。 □

Remark 7.6.17. 注：在本引理中，假设 $A\cap B=\varnothing$ 不等于 *essential*，但这使得证明更容易。

当 $A\cap B\neq\varnothing$ 时，我们可以将刚刚证明的结果应用于可数无限集 $A-B$ (和有限集 $B-A$ (以得到可数无限集 $(A-B)\cup(B-A)$ (，因为它们是互斥的)。然后我们可以再次将上述结果应用于该集——$(A-B)\cup(B-A)$——以及 $A\cap B$ 以得到可数无限集

$$A\cup B=(A-B)\cup(B-A)\cup(A\cap B)$$

下一个结果表示这同样适用于 A,B 的可数无限情况。

Lemma 7.6.18. *If A and B are countably infinite and $A\cap B=\varnothing$, then $A\cup B$ is countably infinite.*

Proof. 由于 A 和 B 是可数无穷的，存在双射 $f : A \to \mathbb{N}$ 和 $g : B \to \mathbb{N}$。设这些函数已给出。我们将使用它们来找到一个双射 $h : A \cup B \to \mathbb{N}$。

首先，通过设置 $\forall n \in \mathbb{N}$ 定义函数 $p : \mathbb{N} \to \mathbb{Z} - \mathbb{N}$。 $p(n) = -n + 1$.
这是一个双射，因为 $p^{-1} : \mathbb{Z} - \mathbb{N} \to \mathbb{N}$ 由 $p^{-1}(z) = -z + 1$ 给出。（自己检查一下！）

由于 p 和 g 是双射，我们知道 $p \circ g : B \to \mathbb{Z} - \mathbb{N}$ 也是一个双射。

接下来，我们通过设定来定义分段函数 $q : A \cup B \to \mathbb{Z}$

$$\forall x \in A \cup B. \qquad q(x) = \begin{cases} f(x) & \text{if } x \in A \\ p(g(x)) & \text{if } x \in B \end{cases}$$

这是定义良好的，因为 $A \cap B = \varnothing$。此外，这是一个双射，因为它是每个部分的同构双射。（再次，你自己检查一下，确保它有意义。另见练习7.8.31，它证明了这一点，具有普遍性。）

从前的工作中，我们知道如何找到一个双射 $r : \mathbb{Z} \to \mathbb{N}$。（还记得我们是怎么做的吗？回顾一下示例7.6.12！）

最后，定义 $h : A \cup B \to \mathbb{N}$ 为 $h = r \circ q$。这是一个双射的复合，因此它是一个双射。这证明了 $|A \cup B| = |\mathbb{N}|$，即 $A \cup B$ 是可数无限的。 □

下一个推论表明，实际上我们没有 *need* 假设 $A \cap B = \varnothing$。这使得证明更容易。我们将要求你证明这个推论。

Corollary 7.6.19. *If A and B are countably infinite, then $A \cup B$ is countably infinite.*

Proof. 作为练习7.8.20留给读者。

（**Hint:** 将引理7.6.18应用于适当选择的集合。 ...） □

这证明了关于寻找集合的 *union* 的几个案例。让我们证明一个关于取 *Cartesian product* 的结果。

Theorem 7.6.20. *If A and B are countably infinite, then $A \times B$ is countably infinite.*

这实际上很容易证明，但仅仅是因为我们已经在关于一个可以表示为笛卡尔积且本身是可数无穷的规范集的结果上进行了证明。看看我们在证明中是如何使用 $\mathbb{N} \times \mathbb{N}$ 的:

Proof. 假设 A, B 是可数无穷的。那么存在双射 $f : A \to \mathbb{N}$ 和 $g : B \to \mathbb{N}$。设这些函数已给出。

定义函数 $h : A \times B \to \mathbb{N} \times \mathbb{N}$ 为

$$\forall (x, y) \in A \times B. \quad h(x, y) = \big(f(x), g(y)\big)$$

我们断言这是一个双射。由于 f, g 是可逆的，我们断言 $H : \mathbb{N} \times \mathbb{N} \to A \times B$ 给出

$$\forall (k, \ell) \in \mathbb{N} \times \mathbb{N}. \quad H(k, \ell) = \big(f^{-1}(k), g^{-1}(\ell)\big)$$

满足 $H = h^{-1}$。

为了看到原因，请注意

$$\begin{aligned} \forall (x, y) \in A \times B. \quad (H \circ h)(x, y) &= H(h(x, y)) = H\big(f(x), g(y)\big) \\ &= \big(f^{-1}(f(x)), g^{-1}(g(y))\big) = (x, y) \end{aligned}$$

和

$$\begin{aligned} \forall (k, \ell) \in \mathbb{N} \times \mathbb{N}. \quad (h \circ H)(k, \ell) &= h(H(k, \ell)) = h\big(f^{-1}(k), g^{-1}(\ell)\big) \\ &= \big(f(f^{-1}(k)), g(g^{-1}(\ell))\big) = (k, \ell) \end{aligned}$$

所以 $H \circ h = \mathrm{Id}_{A \times B}$ 和 $h \circ H = \mathrm{Id}_{\mathbb{N} \times \mathbb{N}}$。这表明 $H = h^{-1}$。

因此，h 是一个双射，因此 $|A \times B| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$。 □

通过将归纳应用于前两个结果，我们可以证明以下内容:

Corollary 7.6.21. *Suppose $A_1, \ldots, A_n$ are countable (where $n \in \mathbb{N}$, so we only have finitely many sets).*

Then $A_1 \cup \cdots \cup A_n$ and $A_1 \times \cdots \times A_n$ are countably infinite.

Proof. 作为练习7.8.22留给读者 □

A Countable Union of Countable Sets is Countable

您现在可能会想知道，当我们取一个由 *countably-infinite* 个集合组成的并集或积时，其中 *each* 个集合是可数无限的……让我们在这里解决并集的情况。这个结果如此基本且重要，以至于我们在本节标题中甚至再次提到了它!

Theorem 7.6.22. *Suppose we have, for each $n \in \mathbb{N}$, a countably infinite set A_n. Then the set*

$$A = \bigcup_{n \in \mathbb{N}} A_n = A_1 \cup A_2 \cup A_3 \cup \cdots$$

is also 可数地 *infinite.*

我们将证明在集合为 **pairwise-disjoint** 的情况下，其余的细节留给你们。

Proof. 假设对于每个 $n \in \mathbb{N}$，我们有一个可数无限集 A_n。此外，假设 $\forall i, j \in \mathbb{N}$。 $A = \bigcup_{n \in \mathbb{N}} A_n$

$i \neq j \implies A_i \cap A_j = \varnothing$. Define

我们断言 A 是可数无穷的。

由于每个 A_n 都是可数无穷的，我们知道对于每个 $n \in \mathbb{N}$，存在一个双射 $f_n : A_n \to \mathbb{N}$。这使得我们可以根据双射 f_n 的行为“编号”每个集合 A_n 的元素。此外，我们在 A_n 个集合上有一个数（它们由 $\mathbb{N}$ 索引）。本质上，我们有一个与 $\mathbb{N} \times \mathbb{N}$ 对应的 A 元素的“编号”。让我们正式定义这个对应关系。

让我们定义一个函数 $F : A \to \mathbb{N} \times \mathbb{N}$。对于任意的 $x \in A$，我们知道 $\exists n \in \mathbb{N}$。

我们断言 F 是一个双射。为了了解原因，考虑由以下函数 $G : \mathbb{N} \times \mathbb{N} \to A$ 定义

$x \in A_n$ and that this n is *unique*. (This follows because the given sets were

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}, G(a, b) = f_a^{-1}(b)$$

pairwise-disjoint). Set $F(x) = (n, f_n(x))$.

这是，G使用第一个坐标a来识别集合A_a，然后使用函数f_a来识别产生$b \in \mathbb{N}$作为输出的A_a中的元素。

（我将留给读者验证，确实，$G = F^{-1}$.)

这表明 $|A| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$，因此 A 是可数无限的。

在 A_n 集合是 *not* 必然两两互斥的情况下……我们将此作为练习7.8.37。

□

Corollary 7.6.23. *Suppose we have, for every $n \in \mathbb{N}$, a* **finite** *set A_n. Furthermore, suppose that these sets are pairwise-disjoint. Define*

$$A = \bigcup_{n \in \mathbb{N}} A_n$$

Then A is countably infinite.

Proof. 作为练习7.8.36留给读者 □

这个结果非常强大。让我们看看它应用于两个例子。

Example 7.6.24. **The set of all powers of primes:**

回忆希尔伯特酒店讨论，我们在无限多个无限大的人群中安排住宿。我们将人们送到对应质数幂的房间。对于每个 $n \in \mathbb{N}$，定义 p_n 为第 n 个质数。然后，对于每个 $n \in \mathbb{N}$，定义

$$A_n = \{p_n^k \mid k \in \mathbb{N}\}$$

这是 所有 n-次质数的幂的集合。上述定理 s ays that

$$\bigcup_{n\in\mathbb{N}} A_n = \{\text{all powers of primes}\}$$

是可数无限的，也是。事实上，我们本应该预料到这一点，因为那个并集只是自然数的一个子集，而自然数本身也是可数无限的!

Example 7.6.25. **The set of all finite binary strings:**

二进制字符串被定义为0和1的有序列表。一个**finite binary string**是有限长度的。

例如，以下都是有限二进制字符串:

$$0, \quad 1, \quad 101010, \quad 10000000000000000001$$

对于每个 $n \in \mathbb{N}$，让我们定义 F_n 为所有长度为 n 的二进制字符串的集合。例如，

$$\begin{aligned} F_1 &= \{\,0\,,\,1\,\} \\ F_2 &= \{\,00\,,\,01\,,\,10\,,\,11\,\} \\ F_3 &= \{\,000\,,\,001\,,\,010\,,\,100\,,\,011\,,\,101\,,\,110\,,\,111\,\} \end{aligned}$$

等等。（注意 $|F_n| = 2^n$。试着证明它！）然后，定义所有有限二进制字符串的集合为

$$F = \bigcup_{n\in\mathbb{N}} F_n$$

一个F的元素必须来自大并集中的某个集合；这意味着任意元素$x \in F$是某个有限长度的二进制字符串。这个长度可能是一个非常大的数字，但它是有穷的。（这指出了允许某物“任意大（但有限）”和允许某物“无限”之间的区别。）

这个例子的目的是，根据上面的定理，{v*} 是可数无限的！（实际上，它实际上是从紧接着陈述的推论中得出的。）将这一点与所有 *infinite* 二进制字符串的集合 S 进行对比，这个集合——正如我们很快将要证明的——是不可数无限的。我们将相当频繁地使用这些二进制字符串集合作为例子!

Passing Off To A “Limit”

我们已经在上面证明了，如果 A 和 B 是可数无穷的，那么 $A \cup B$ 和 $A \times B$ 也是可数无穷的。我们还鼓励你通过在并集/积的集合数量上进行归纳来证明这一点。

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i\in[n]} A_i \qquad \text{and} \qquad \prod_{i\in[n]} A_i = A_1 \times A_2 \times \cdots \times A_n$$

同样都是可数无穷，对于任何 $n \in \mathbb{N}$。

这些结果如果有什么话，告诉我们关于

$$A_1 \cup A_2 \cup A_3 \cup \cdots \quad = \quad \bigcup_{k \in \mathbb{N}} A_k$$

和

$$A_1 \times A_2 \times A_3 \cdots \quad = \quad \prod_{k \in \mathbb{N}} A_k$$

这意味着，当我们从拥有一个*finite*并/积（任意大的大小，但仍然是有限的）尝试“跳到极限”到拥有一个*infinite*并/积时，会发生什么？我们能得出必要的结论吗？我们能找到反例吗？

主要思想是，“取极限”确实创建了一个 *some* 数学对象，但我们不能必然预设这个对象具有 *exact same properties*，就像定义该对象的序列中的所有对象一样。

考虑有限集合 $[n]$，对于每个 n。它们每一个都是有限的，但在“极限”情况下我们得到 $\mathbb{N}$，它是 *not* 有限的。所以，是的，我们确实得到了某个对象（另一个集合），但它不必具有相同的属性。

上述重要定理表明，在 *union* 中取极限确实保留了可数性。正如我们将在下一节中看到的那样，*product* 确实 **not** 保留了可数性。（事实上，即使是有限集的无限乘积也是不可数的。哎呀！）

在微积分中也有类似的概念。我们承诺不会使用微积分，但这两个想法之间存在着如此自然的关系，所以我们觉得有必要提及一个简单的例子。如果你从这个例子中一无所获，请不要担心；如果你有所收获，尽管如此，也请记住这个联系，并思考它可能从根本上改变你对微积分中学到的一切的看法。）

考虑一个 *limit*，类似于

$$\lim_{x \to \infty} \frac{1}{x} = 0$$

在什么意义上这个极限 **equal** 是趋近于 0 的？为什么作为数学家，我们多年来会选择以这种方式选择极限？从形式上讲，这个极限是有意义的，因为它是基于极限的量化定义。设 P 为正实数集。那么极限的定义（应用于这个例子）是说

$$\forall \varepsilon \in P \,.\, \exists M \in \mathbb{N} \,.\, \forall n \in \mathbb{N} \,.\, \big(n > M \implies \left|\frac{1}{x}\right| < \varepsilon\big)$$

这意味着，对于任何小的正阈值($\varepsilon > 0$)，我们可以找到一个特定的截止点（一个依赖于ε的大自然数 M），使得对于每一个点 *after* M，函数 $\frac{1}{x}$ 都落在该 ε-阈值内，即零点。

请注意，这比说一些像 “$\frac{1}{\infty} = 0$”这样的废话要好。这就是**not**正在发生的事情。我们从未真正到达“插入”极限的末端并对其进行评估。极限是用量化定义的，对于*arbitrarily large*值发生的一些事情，但对于一个*infinite*值则不发生。

7.6.4 Uncountable Sets

为了开始我们对不可数集的讨论，让我们证明我们已经提到的一个结果。具体来说，我们将证明一个可数无限 *Cartesian product* 的集合是不可数无限。请注意，我们甚至不需要集合是无限的：我们可以将它们都做成有限集合，大小为2！我们将在下一部分使用这个结果来展示一些不可数集的例子，包括我们已知的熟悉集合……

An Uncountable Cartesian Product

Theorem 7.6.26. *A countably infinite Cartesian product of sets with just two elements is uncountably infinite. That is,*

$$\{0,1\}^{\mathbb{N}} = \{0,1\} \times \{0,1\} \times \{0,1\} \times \cdots$$

is uncountably infinite.

Proof. AFSOC这个集合$\{0,1\}^{\mathbb{N}}$实际上是可数无限的。这意味着我们可以在该集合和$\mathbb{N}$之间找到一个双射；也就是说，我们可以在该集合的所有元素和所有自然数之间建立一种对应关系。因此，该集合有一个*1st*元素，对应于1的元素；有一个*2nd*元素，对应于2的元素；以此类推。

我们不知道这些元素具体是什么，但我们保证这种对应关系存在。尽管如此，我们仍然可以列出 y_i 的所有元素 $\{0,1\}^{\mathbb{N}}$。每个 y_i 是一个有序的、无限的 0 和 1 的列表，因此我们可以这样写：

$$\begin{aligned}
1 &\leftrightarrow (a_{1,1}\ ,\ a_{1,2}\ ,\ a_{1,3}\ ,\ a_{1,4}\ ,\ a_{1,5}\ ,\ \ldots) = y_1 \\
2 &\leftrightarrow (a_{2,1}\ ,\ a_{2,2}\ ,\ a_{2,3}\ ,\ a_{2,4}\ ,\ a_{2,5}\ ,\ \ldots) = y_2 \\
3 &\leftrightarrow (a_{3,1}\ ,\ a_{3,2}\ ,\ a_{3,3}\ ,\ a_{3,4}\ ,\ a_{3,5}\ ,\ \ldots) = y_3 \\
4 &\leftrightarrow (a_{4,1}\ ,\ a_{4,2}\ ,\ a_{4,3}\ ,\ a_{4,4}\ ,\ a_{4,5}\ ,\ \ldots) = y_4 \\
5 &\leftrightarrow (a_{5,1}\ ,\ a_{5,2}\ ,\ a_{5,3}\ ,\ a_{5,4}\ ,\ a_{5,5}\ ,\ \ldots) = y_5 \\
&\ \ \vdots
\end{aligned}$$

每个值 $a_{i,j}$ 要么是 0，要么是 1。i 告诉我们对应哪个自然数（即列表中的 *vertical* 位置）以及 j 告诉我们处于哪个坐标（即列表中的 *horizontal* 位置）。

因为我们假设对应是一个双射，所以我们知道这个列表包含 *all* 个 $\{0,1\}^{\mathbb{N}}$ 的元素。为了完成矛盾论证，我们将构造一个保证在 $\{0,1\}^{\mathbb{N}}$ 中 **not** 出现的元素！（这是康托尔对角线论证的一个版本。）

让我们通过以下方式定义对象 $x = (x_1, x_2, x_3, \ldots)$：

$$x_i = \begin{cases} 0 & \text{if } a_{i,i} = 1 \\ 1 & \text{if } a_{i,i} = 0 \end{cases}$$

这是，我们通过向下遍历元素网格的 *main diagonal*（因此我们看到所有元素 $a_{i,i}$）和从 1 到 0，或反之，来构建 x。

以下图示是 *specific example* 的一个示例，说明如何进行此操作，但它并不属于这个更普遍的证明的一部分。然而，我们包括它是为了说明的目的：

$$\begin{aligned}
1 &\leftrightarrow \big(\textcircled{1}, 1, 0, 0, 1, \ldots\big) = y_1 \\
2 &\leftrightarrow \big(1, \textcircled{0}, 0, 0, 1, \ldots\big) = y_2 \\
3 &\leftrightarrow \big(0, 0, \textcircled{1}, 1, 0, \ldots\big) = y_3 \\
4 &\leftrightarrow \big(1, 1, 0, \textcircled{1}, 1, \ldots\big) = y_4 \\
5 &\leftrightarrow \big(0, 1, 1, 1, \textcircled{0}, \ldots\big) = y_5 \\
&\vdots \\
x &= \Big(\textcircled{0}, \textcircled{1}, \textcircled{0}, \textcircled{0}, \textcircled{1}, \ldots\Big)
\end{aligned}$$

为什么我们会选择这样做呢？嗯，想想看对象 x 是否可能属于上面元素的列表。

- 是 $x = y_1$ 吗？不是，因为 x 和 y_1 在它们的第一个坐标上不同。（在我们的例子中 $x_1 =$ 为 0，因为 $y_{1,1} =$ 为 1。）
- 是 $x = y_2$ 吗？不是，因为 x 和 y_2 在它们的第二个坐标上不同。（在我们的例子中，$x_2 =$ 为 1 因为 $y_{2,2} =$ 为 0。）
- 是 $x = y_3$ 吗？不是，因为 x 和 y_3 在它们的第三个坐标上不同。（在我们的例子中，$x_3 =$ 为 0，因为 $y_{3,3} =$ 为 1。）

通常，对于任意的 $i \in \mathbb{N}$，我们可以保证 x 和 y_i 在 i-th 坐标上不同。因此，y_i 个对象中的 **none** 可以等于这个新对象 x。也就是说，

$$\big(\forall i \in \mathbb{N}\,.\; x_i \neq y_{i,i}\big) \implies \big(\forall i \in \mathbb{N}\,.\; x \neq y_i\big)$$

但是，我们定义的 {v*} 只是一个有序的、无限的 0 和 1 的列表，因此它肯定是 $\{0,1\}^{\mathbb{N}}$ 的一个元素，本身。

这是一个矛盾。我们假设我们可以列出我们集合的所有元素，但随后我们使用这个顺序来构造我们集合中的一个元素，这个元素肯定不在列表中。※

因此，$\{0,1\}^{\mathbb{N}}$ 是不可数无穷的。 □

注意：这是一个非常漂亮的论点。这是我最喜欢的数学证明之一。康托尔提出这个论点是个天才，而且更有趣的是，它实际上相当简单且容易记住。我们相信你们不会忘记这个“沿着主对角线切换值”的论点。我们甚至能用九个字概括整个证明

这是其卓越的进一步证明。

Corollary: 一个至少包含两个元素的集合的可数无限积是不可数无限。

（注意：我们实际上只需要说明产品中的集合都不是空的，并且只允许有限多个集合恰好有一个元素。）

Examples

你现在可能想知道：哪些类型的集合是不可数无限的？我们是否知道一些？当然，我们知道！以下是一些例子。

Example 7.6.27. **The set of all infinite binary strings:**

您可能已经注意到，我们在上述证明中使用的集合——即 $\{0,1\}^{\mathbb{N}}$——“本质上”就是无限二进制字符串的集合 S！$\{0,1\}^{\mathbb{N}}$ 的一个元素是一个无限长的有序坐标列表，每个坐标都是 0 或 1。S 的一个元素是一个无限长的有序 0 和 1 的列表，但只是没有括号和逗号。因此，这两个集合之间存在一个非常自然的双射（只需去掉括号和逗号，或者把它们放回去），因此我们将这两个集合视为相同的。

我们在上面的例子7.6.25中看到，所有有限二进制字符串的集合是可数无穷的。这个最新的结果表明，所有无限二进制字符串的集合是不可数无穷的。这个事实的一个替代证明涉及在S和$\mathcal{P}(\mathbb{N})$之间找到一个双射，然后应用说$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$的康托定理。（有关这些细节，请参阅练习7.8.33。）

Example 7.6.28. $\mathbb{R}$ **is uncountably infinite:**

这是我们的第一个例子，是一个不可数无限的标准数集。我们可以使用上述结果来证明这个事实。

这个说法在直觉上有些道理，因为它“看起来”实数线比仅仅 $\mathbb{N}$ 或 $\mathbb{Z}$ “大得多”。但我们还看到 $\mathbb{Q}$ 是可数无穷的，并且有无数有理数散布在实数线上；事实上，在 *any two real numbers* 之间就有无穷多个有理数！

我们现在将看到，是的，确实$\mathbb{R}$是不可数无限的。此外，我们甚至将证明$\mathbb{R}$和$\mathcal{P}(\mathbb{N})$具有相同的“无限大小”；也就是说，我们将展示$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$。（记住，这比仅仅说这两个集合都是不可数的有更多信息；存在许多不可数无限集合的级别，我们只是选择不过多地谈论它们，以免伤到我们的脑筋。）

从道德上讲，展示 $\mathbb{R}$ 的想法背后是不可数无穷的，首先是要将 $\mathbb{R}$ 与集合 $\{0,1,2,3,4,5,6,7,8,9\}^{\mathbb{N}}$ 相关联。每个实数都可以用十进制表示，这仅仅是一些可数无穷多个数字的有序列表。其中有一个小数点，并且有

问题如$0.999999\cdots = 1$，但这并不是什么大问题。因为我们已经看到，即使像$\{0, 1\}$这样的“小”集合，当我们无限次地取其乘积时，也会得到一个不可数集合，那么一个“更大”的集合，如$\{0, 1, \ldots, 9\}$，当然也会给出一个不可数集合，即使考虑到这些问题。这就是你可以带在脑子里，用来向朋友解释结果的直观论证。（事实上，这也是你会在大多数教科书中找到的论证。）

更正式地说，我们只需证明$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$。这个更强的结果意味着$\mathbb{R}$是不可数的无穷大（因为康托尔定理告诉我们$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$。）为了做到这一点，我们将考虑集合

$$I = \{y \in \mathbb{R} \mid 0 \leq y \leq 1\}$$

这是区间$[0, 1] \subseteq \mathbb{R}$。我们将证明

$$|\{0, 1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| = |I|$$

然后应用一些关于区间与$\mathbb{R}$之间双射的结果。

考虑函数$f_1 : \{0, 1\}^{\mathbb{N}} \to I$，它接受一个无限二进制字符串，在所有0和1前面加上小数点，并说：“将这个数作为**decimal**展开式来评估”。

作为一个例子，考虑元素$(1, 1, 0, 0, 1, 0, \ldots)$，其余都是0。然后

$$f_1(1, 1, 0, 0, 1, 0, \ldots) = 0.110010\ldots_{\text{DEC}} = \frac{1}{10^1} + \frac{1}{10^2} + \frac{1}{10^5} = \frac{11001}{100000}$$

注意，这是一个函数，因为任何输出肯定是一个实数（因为它有一个小数展开；我们刚刚提供了它）并且它在0和1之间，因为我们把小数点放在前面。此外，请注意f_1是一个**injection**；两个不同的无限二进制字符串必须在某个坐标上不同，因此它们产生两个在某处不同的十进制展开，因此不能是同一个实数。这表明$|\{0, 1\}^{\mathbb{N}}| \leq |I|$。

考虑函数$f_2 : \{0, 1\}^{\mathbb{N}} \to I$，它接受一个无限二进制字符串，在所有0和1前面加上小数点，并说，“将这个数作为**binary**展开式来评估”。

作为一个例子，考虑与上面相同的元素。然后

$$f_2(1, 1, 0, 0, 1, 0, \ldots) = 0.110010\ldots_{\text{BIN}} = \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^5} = \frac{25}{32}$$

注意，这是一个函数，因为任何输出肯定是一个实数；只需评估结果的分数之和，它就会得到一个介于0和1之间的实数（即使该级数是无限的，也保证会收敛）。例如，所有输入为0的结果为0，所有输入为1的结果为1，因为

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = \sum_{k \in \mathbb{N}} \frac{1}{2^k} = 1$$

此外，请注意 f_2 是一个 **surjection**。这个事实依赖于关于有理数/无理数的一些外部知识；具体来说，任何无理数都可以被一系列 *dyadic* 有理数（分母是2的幂的有理数）近似。我们不会陈述或证明这些结果，但我们认为通过玩一些例子，你会开始看到为什么这行得通。事实上，你可以搜索一下无理数的二进制展开，你会发现一些有趣的结果。

由于 f_2 是满射，这表明 $|\{0,1\}^{\mathbb{N}}| \geq |I|$。因此，我们得出结论 $|\{0,1\}^{\mathbb{N}}| = I$。我们还知道 $|\mathcal{P}(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}|$ (参见练习7.8.33)，因此我们现在知道 $|I| = |\mathcal{P}(\mathbb{N})|$。

最后一步是证明 $|I| = |\mathbb{R}|$。查看第7.5.4节中的练习5。在那里，你发现集合 $J = \{y \in \mathbb{R} \mid -1 < y < 1\}$ 和 $\mathbb{R}$ 之间存在双射。很容易找到 J 和集合 $K = \{y \in \mathbb{R} \mid 0 < y < 1\}$ (try it now!) 之间的双射。这表明 $|\mathbb{R}| = |J| = |K|$。此外，$K \subseteq I$ 并且它们只相差两个元素，0 和 1，所以 $|K| = |I|$。最后，这表明 $|I| = |\mathbb{R}|$，因此我们得出结论：

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$$

查看我们提到的两个参数：

- 考虑到集合 $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^{\mathbb{N}}$，并且
- 考虑到集合 $\{0, 1\}^{\mathbb{N}}$

Both 涉及一些关于十进制展开（以及二进制展开）的知识。似乎没有简单的解决办法，所以我们希望上述结果仍然具有说服力。特别是，你可能想尝试上述讨论中的 f_2 是一个 **surjection** 但不是一个 **injection** 的想法。你能说服自己这些主张吗？你能说服别人吗？

Theorems

让我们看看关于不可数集的一个结果。然后，在继续前进之前，我们将陈述一个关于无限集的最终定理！

Lemma 7.6.29. *Suppose A is uncountably infinite and B is countably infinite, and $B \subseteq A$. Then $A - B$ is uncountably infinite.*

(注意：我们不需要 *need* 假设这里 $B \subseteq A$。如果不是这样，我们只需将 A 和 $B \cap A$ 视为集合即可.)

Proof. 作为第7.6.5节中的练习5留给读者。

（**Hint:** 使用一个 *contradiction* 参数 ...） □

Characterizing a Set as Infinite

为了定义 **infinite** 集合，我们首先定义了 **finite** 集合，然后声明任何集合如果它是 *not* 有限的，则它是无限的。以下定理表明我们可以以不同的方式定义 **infinite**。也就是说，我们可以这样说，一个集合是无限的，当且仅当我们能找到一个与其自身的真子集的双射。首先，让我们陈述并证明这个有用的引理；我们将在下面定理的证明中需要它。

Lemma 7.6.30. *Let A be any set. Then, A is infinite $\iff$ there exists $B \subset A$ such that B is countably infinite.*

Proof. $\impliedby$ 方向很明显。如果 A 大于某个无限集合，它也是无限的。

$\implies$ 方向更有趣。假设 A 是无限的。设 $\star \in A$ 为某个特殊元素。我们将将其排除在外，并构造一个不包含 $\star$ 作为元素的、可数无限的集合 B。这将保证 $B \subset A$，具有 $B \neq A$。

考虑 $A_1 = A - \{\star\}$。这个集合也是无限的，因此我们可以选择某个元素 $b_1 \in A_1$。

考虑 $A_2 = A_1 - \{b_1\} = A - \{\star, b_1\}$。这个集合也是无限的，因此我们可以选择某个元素 $b_2 \in A_2$。

考虑 $A_3 = A_2 - \{b_2\} = A - \{\star, b_1, b_2\}$。此集合也是无限的，因此我们可以选择某个元素 $b_3 \in A_3$。

我们可以永远继续这个过程。定义 $B = \{b_1, b_2, b_3, \dots\}$。（注意：我们在这里使用“趋向极限”，但这是可以接受的，因为我们不是用它来“保留”B的任何属性。我们只是*constructing*这个对象B。）

注意，B 是可数无限的，因为它与 $\mathbb{N}$ 存在一个明显的双射。

□

使用这个引理，我们可以陈述并证明下一个结果：

Theorem 7.6.31. *Let A be any set. Then, A is infinite $\iff$ there exists $B \subset A$ such that there exists $f : A \to B$ that is bijective.*

Proof. ($\implies$) 假设 A 是无限的。我们必须确定一个适当的子集 $B \subset A$ 和一个双射 $f : A \to B$。

自 $A \neq \varnothing$ 以来，取任意 $x \in A$。考虑 $B = A - \{x\}$。注意 $B \subset A$。

我们想证明存在一个双射 $f : A \to B$。

通过上述引理7.6.30，我们知道我们可以找到一个可数无限严格子集$C \subset B$。（注意：A是无限的，因此$B = A - \{x\}$也是无限的，因为我们只移除了一个元素。如果您需要更多的说服力，AFSOC B是有限的，因此它有一定的规模；那么A的规模是多少呢？）

由于 C 是可数无穷的，我们可以列出 C 的元素为 $\{y_1, y_2, y_3, \dots\}$。

(注意：这个想法是存在某种双射 $g : \mathbb{N} \to C$，因此我们可以让 $y_1 = g(1)$ 和 $y_2 = g(2)$ 等等。)

定义 $f : A \to B$ 为

$$\forall y \in A. \quad f(y) = \begin{cases} y & \text{if } y \neq y_i \text{ for all } i \in \mathbb{N} \text{ and } y \neq x \\ y_1 & \text{if } y = x \\ y_{i+1} & \text{if } y = y_i \text{ for some } i \in \mathbb{N} \end{cases}$$

这是一个双射，因为我们能识别其逆函数 $F : B \to A$，它是

$$\forall z \in B. \quad F(z) = \begin{cases} z & \text{if } z \neq y_i \text{ for every } i \in \mathbb{N} \\ x & \text{if } z = y_1 \\ y_{i-1} & \text{if } z = y_i \text{ for some } i \in \mathbb{N} - \{1\} \end{cases}$$

我们将把它留给读者作为练习来验证 $F = f^{-1}$。（至少画一张图来直观地说服自己。）

($\Longleftarrow$) 这个方向声称无限集合是具有这个性质的 *only* 集合。我们将通过逆否命题来证明这个命题。也就是说，我们将表明任何有限集合 *cannot* 都有一个与一个真子集的双射。

假设 A 是有限的。这意味着它有一个（唯一的）大小，比如说 $n \in \mathbb{N}$。考虑一个任意的真子集 $B \subset A$。在 WWTS 中，不存在从 A 到 B 的双射。

AFSOC存在这样一个双射 $f : A \to B$。由于 B 是有限的，且 $B \subset A$，B 有一些大小 $m < n$。因此，存在一个双射 $g : B \to [m]$。将这些双射组合起来，我们得到一个双射 $h : A \to [m]$。因此，$|A| = n$ 和 $|A| = m$，所以 $m = n$。然而，我们也知道 $m < n$。这是一个矛盾。※

(注意：我们也可以通过 *Pigeonhole Principle* 来论证这一点，我们尚未讨论但很快就会讨论。本质上，当 $n > m$ 时，我们不能有一个双射 $p : [n] \to [m]$，因为“箱子”太少，无法装下“鸽子” n)。

在解决问题的背景下，你可能想论证某个集合是无限的。与其证明你不可能找到一个到*any*有限集合的双射，不如考虑使用这个定理！如果你能识别出一个真子集和一个双射，那么你就已经达成了目标，借助这个结果。

7.6.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 当一个集合 **finite** 是什么时？(2) 有哪两种方式来描述一个集合是 **infinite** ？(3) **countably** 和 **uncountably** 无穷之间的区别是什么？给出每种类型的两个例子。(4) 给定两个可数无穷集合，A 和 B，我们可以对它们执行哪些操作以得到一个可数无穷集合？对这些集合执行任何操作会产生一个 *finite* 集合吗？(5) $\mathbb{R} \times \mathbb{N}$ 是可数无穷还是不可数无穷？$\mathbb{R} - \mathbb{N}$ 呢?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 证明命题7.6.9。也就是说，证明：如果A和B是有限集，那么

$$|A \cup B| = |A| + |B| - |A \cap B|$$

(2) 证明推论7.6.10。也就是说，证明：

如果 $A_1, \ldots, A_n$ 是有限的且两两互斥，那么

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$$

(3) 找出以下“欺骗”中的缺陷，其中 $\mathbb{R}$ 是可数无穷的：

设 $S \subseteq \mathbb{R}$ 为由 $S = \{y \in \mathbb{R} \mid 0 \leq y < 1\}$ 定义的集合。

对于每个 $x \in S$，定义集合 $A_x = \{x + z \mid z \in \mathbb{Z}\}$。

(For example, $A_{1/2} = \{\ldots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \ldots\}$.)

由于 $\mathbb{Z}$ 是可数无穷的，每个集合 A_x 也是可数无穷的。

此外，请注意

$$\mathbb{R} = \bigcup_{x \in S} A_x$$

这是可数无限集的并集，因此 $\mathbb{R}$ 也是可数无限。

请务必指出任何不正确的特定步骤，以及*why*该步骤不正确。理想情况下，您应该指出为什么该欺骗的最终结论是不正确的，但不要仅仅明确地说“$\mathbb{R}$ 是不可数的，因为我们已经证明了”。*Why*是不正确的步骤，是对结果的误用，*and*为什么该特定步骤的结论无效?

(4) 对于以下每种期望情况，提供示例或说明其不可能。

例如，如果情况是“有限集合 A 和 B，使得 $A \cup B$ 的大小为 4”，一个答案可能是“考虑 $A = \{1, 2\}$ 和 $B = \{3, 4\}$。”如果情况是，“对于每一个 $x \in \mathbb{N}$，一个无限集合 S_x，使得 $\bigcup_{x \in \mathbb{N}} S_x$ 是“有限”，答案将是“不可能”。

这里无需*prove*你的答案；一个很好的例子就足够了。

(a) 一个不可数无限集 A 和一个可数无限集 B，使得 $A \cap B$ 是有限的。 (b) 不可数无限集 C 和 D，使得 $C - D$ 是可数无限。 (c) 不可数无限集 E 和 F，使得 $E - F$ 是不可数无限。 (d) 对于每一个 $x \in \mathbb{N}$，一个可数无限集 S_x，使得 $\bigcup_{x \in \mathbb{N}} S_x$ 是不可数无限。 (e) 对于每一个 $y \in \mathbb{R}$，一个可数无限集 T_y，使得 $\bigcup_{y \in \mathbb{R}} T_y$ 是可数无限。

(5) 证明引理7.6.29。也就是说，假设A是不可数无穷大，$B \subseteq A$是可数无穷大；证明$A - B$是不可数无穷大。

使用此结果解释为什么实数集 *irrational* 是不可数无穷的。

7.7 Summary

现在，我们已经完全探索了**functions**及其相关属性！我们看到了一个函数只是一个具有特定属性的关联。这个期望的属性对应于我们通常认为函数对每个可能的“输入”都有一个“输出”。我们通过定义术语如定义域、值域和像等数学概念来形式化这些概念。函数的进一步属性包括单射性和满射性。我们看到了具有这些属性函数的许多例子和非例子，并讨论了如何证明/反驳这些属性，将其与我们逻辑证明技术联系起来。

这个 *bijection* 的概念特别有帮助和强大。我们将它与 *inverse* 函数的概念联系起来。具体来说，我们看到了并证明了如果一个函数有逆函数，那么它就是双射 *if and only if*！这在后来我们讨论 **cardinality** 时是一个重要的结果，在那里“双射是王”。“配对元素”的概念帮助我们理解了一些关于“集合大小”的更奇特和反直觉的结果。

我们定义无限集合为可数无限或不可数无限。然而，我们还证明了具有历史意义的结果，即康托尔的结果。

定理，它表明实际上存在无限多个 *cardinalities*！就我们在这里的目的而言，区分这两种无限集合是足够的。我们看到了每种类型的几个例子，并证明了关于如何从其他集合中创建特定基数集合的一些定理。最终，我们发现这些结果引人入胜且具有数学上的指导意义。然而，从现在起，我们将只关注 **finite** 集合。

7.8 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的任何内容，以及可能的一些假设的数学知识。当然，我们不期望你解决其中的**all**，但工作得越多，你将学到越多！记住，没有*doing*数学，你无法真正*learn*数学。动手解决一个问题。阅读几个陈述，四处走走，思考它们。尝试写一个证明，并向朋友展示，看看他们是否信服。继续练习将你的想法以清晰、精确和逻辑的方式*write*出来的能力。写完证明后，编辑它，使其更好。最重要的是，继续*doing*数学！

简答题，只需解释或陈述答案，无需严格的*proof*，已用►标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 7.8.1. 对于以下每个“规则”以及提出的定义域和值域，确定该“规则”是否定义了一个 **well-defined function**。如有必要，请用例子解释你的答案。

(a) 令 $a : \mathbb{Z} - \{1\} \to \mathbb{R}$ 由 $a(x) = \dfrac{x^2}{x-1}$ 定义。

(b) 令 $b : \mathbb{Q} \to \mathbb{Q}$ 由 $b(x) = \sqrt{|x|}$ 定义。

(c) 在每个输入 $x \in \mathbb{Z}$ 上定义 $c : \mathbb{Z} \to \mathbb{Z}$，通过输出一个 $s \in \mathbb{Z}$ 使得 $x \equiv s \bmod 3$。

(d) 令 $d : \mathbb{N} \to \mathbb{N}$ 由 $d(x) = \left\lfloor \dfrac{x}{10} \right\rfloor$ 定义。

(e) 令 $e : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{Z})$ 通过取一组自然数并输出该集合中最小元素的整数倍集合来定义。

Problem 7.8.2. 考虑集合 $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ 和 $\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$。

考虑函数 f：由 $f(x, y, z) = (xz, yz)$ 定义。f 是单射吗？满射吗？证明你的论断。

Problem 7.8.3. 定义 $f\colon \mathbb{R} \to \mathbb{R}$ 和 $g\colon \mathbb{R} \to \mathbb{R}$ 通过 $f(x) = x + 1$ 和 $g(x) = x^2 + x$。

找到组成 $f \circ g$ 和 $g \circ f$ 的公式。（注意，它们是 *different*。）

证明这些组合中的 {v*} 是单射的。

Problem 7.8.4. 设 $f : \mathbb{Z} \to \mathbb{Z}$ 由 $f(x) = 2x - 3$ 给出。设 $g : \mathbb{Z} \to \mathbb{N}$ 由 $g(z) = |z| + 4$ 给出。

什么是 $g \circ f$ 的定义域？什么是值域？

写下定义 $g \circ f$ 的规则。这个函数是单射的吗？满射的吗？

什么是 $\text{Im}_{g\circ f}(\mathbb{Z})$？

证明你的主张。

Problem 7.8.5. 每条以下规则定义了从 $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ 到的函数。对于每条规则，确定所得函数是否是单射或满射，或者两者都是，或者都不是。证明你的论断。

(a) $f_1(a, b) = a - b$b) $f_2(a, b) = 2a + 3b$c) $f_3(a, b) = a$d) $f_4(a, b) = a^2 - b^2$e) $f_5(a, b) = 2^a \cdot 3^b$

((((

Problem 7.8.6. 定义具有以下属性的定义域为 $\mathbb{N}$ 和值域为 $\mathcal{P}(\mathbb{N})$ 的函数 f_1, f_2, f_3, f_4，否则解释为什么期望的属性 **not** 可行。

- f_1 是单射但不是满射
- f_2既不是单射也不是满射
- f_3 是满射但不是单射
- f_4 是双射

Problem 7.8.7. 考虑函数 $f\colon$ 由 $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ 定义

$$\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}\textbf{.} \quad f(x, y) = (y + 1, 3 - x)$$

找到一个函数 F，它是 f 的逆函数，并证明它是。这告诉我们关于函数 f 的什么？

Problem 7.8.8. 定义集合 $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$。定义函数 $g : S \to \mathbb{R}$ 为

$$g(x) = \frac{2x - 1}{2x(1 - x)}$$

证明 $\text{Im}_g(S) = \mathbb{R}$。

（**Hint:** 您需要使用二次公式。）

Problem 7.8.9. 假设 $f : A \to B$ 和 $g : B \to C$ 是函数。

(a) 假设 f, g 是满射。证明 $g \circ f : A \to C$ 也是满射。

(b) 假设 f, g 是单射。证明 $g \circ f : A \to C$ 也是单射。

(c) 假设 f, g 是双射。证明 $g \circ f : A \to C$ 也是一个双射。

Problem 7.8.10. 假设 $f : A \to B$ 和 $g : B \to C$ 是双射。定义 $h : A \to C$ 为 $h = g \circ f$。

证明 h 是可逆的，并且 $h^{-1} = f^{-1} \circ g^{-1}$。

（**Hint:** 使用函数复合的结合律。）

Problem 7.8.11. 设 $f : A \to B$ 和 $g : B \to C$ 为函数。设 $X \subseteq A$。证明 $_{g\circ f}(X) =$ 的像 $_g(\ _f(X))$。

Problem 7.8.12. 设 $f : A \to B$ 为双射，因此 $f^{-1} : B \to A$ 是一个函数。设 $X \subseteq A$。证明 $\text{Im}_f(X) = \text{PreIm}_{f^{-1}}(X)$。

Problem 7.8.13. 设 A, B 为集合，设 $f : A \to B$ 为一个函数。假设 $X, Y \subseteq A$。

(a) 以下等式是否必然成立 ?

$$\text{Im}_f(X \cup Y) = \text{Im}_f(X) \cup \text{Im}_f(Y)$$

声明你的主张并证明它。

(b) 以下等式是否必然成立 ?

$$\text{Im}_f(X \cap Y) = \text{Im}_f(X) \cap \text{Im}_f(Y)$$

声明你的主张并证明它。

Problem 7.8.14. 设 $f : A \to B$ 为一个函数。通过以下方式在 B 上定义关系 $\sim$：对于任何 $x, y \in B$,

$$x \sim y \iff \text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{y\})$$

解释为什么 $\sim$ 是一个等价关系。

什么是等价类?

假设 f 是满射，等价类是什么?

Problem 7.8.15. 设 $f : A \to B$ 为一个函数。通过以下方式在 A 上定义关系 $\approx$：对于任何 $x, y \in A$,

$$x \approx y \iff f(x) = f(y)$$

≈是一个等价关系吗？如果是，证明它，并描述等价类。如果不是，提供反例。

现在，假设 f 是一个单射。≈ 是一个等价关系吗？如果是，证明它并描述等价类。如果不是，提供一个反例。

Problem 7.8.16. 设 $f : A \to B$ 为一个函数，并设 $X, Y \subseteq A$。考虑以下关于 $\text{Im}_f(X) \cap \text{Im}_f(Y) \subseteq \text{Im}_f(X \cap Y)$ 的声明，这个“恶作剧”有什么问题?

> 让 $z \in \text{Im}_f(X) \cap \text{Im}_f(Y)$。由于 $z \in \text{Im}_f(X)$，这意味着 $\exists a \in X$ 使得 $f(a) = z$。由于 $z \in \text{Im}_f(Y)$，这意味着 $\exists a \in Y$ 使得 $f(a) = z$。由于 $a \in X$ 和 $a \in Y$，这意味着 $a \in X \cap Y$。由于 $f(a) = z$，这意味着 $z \in \text{Im}_f(X \cap Y)$。

提供一个反例以表明该陈述实际上为 False。

Problem 7.8.17. 证明/反驳 $\mathcal{P}(\mathbb{N})$ 和 $\mathcal{P}(\mathbb{Z})$ 是否具有相同的基数。

Problem 7.8.18.修复任意$n \in \mathbb{N}$。考虑集合$[n] = \{1, 2, 3, \ldots, n\}$。

设E为包含n的子集的集合，这些子集具有**even**个元素（如$\varnothing$或$\{1, 4\}$），设O为包含n的子集的集合，这些子集具有**odd**个元素（如$\{5\}$或$\{1, 2, 3\}$）。

定义一个函数 $p : E \to O$，它是一个 **bijection**，并证明它是一个双射。

(**Hint:** 写出一些小案例，其中 $n = 1$ 和 $n = 2$ 和 $n = 3$。然后尝试进行推广。)

Problem 7.8.19. 证明引理7.6.16。

Hint: 尝试使用类似于我们定理7.6.7证明中的想法：使用B的大小“提升”A和$\mathbb{N}$之间的双射关系一定量。

Problem 7.8.20. 证明推论7.6.19。也就是说，假设A和B是可数无穷集合；通过将引理7.6.18应用于适当选择的集合来证明$A \cup B$是可数无穷。

Problem 7.8.21. 回顾示例7.6.13。在那里，我们通过设置定义了 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\forall (x, y) \in \mathbb{N} \times \mathbb{N}. \quad f(x, y) = 2^{x-1}(2y - 1)$$

证明 f 是 **injective**。

Problem 7.8.22. 证明推论7.6.21。也就是说，假设我们有一些有限个集合—$A_1, A_2, \ldots, A_n$—其中每个集合都是可数无限的；证明

$$A_1 \cup A_2 \cup \cdots \cup A_n$$

和

$$A_1 \times A_2 \times \cdots \times A_n$$

两者也都是可数无穷的。

Problem 7.8.23. 考虑由以下定义的集合 A:

$$A = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \leq b\}$$

证明 A 以两种方式是可数无限的:

(1) 通过将 A 写作集合的并集并引用一个结果。

(2) 通过找到一个显式的双射 A 和你选择的可数集之间的映射。

Problem 7.8.24. 定义 g: 通过设置 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \forall (x, y) \in \mathbb{N} \times \mathbb{N}. \quad g(x, y) = (x + y)^2 + x$$

证明 g 是（a）单射的并且（b）非满射的。

Problem 7.8.25. 设 A, B, C 为集合。设 $f : A \to B$ 和 $g : B \to C$ 和 $h : B \to C$ 为函数。

(a) 假设 $g = h$。这是否必然导致 True，即 $g \circ f = h \circ f$? 证明或反驳这一说法。(b) 假设 $g \circ f = h \circ f$。这是否必然导致 True，即 $g = h$? 证明或反驳这一说法。

Problem 7.8.26. 设A, B为有限集合，满足$|A| = |B| = n$。假设f: $A \to B$是一个函数。证明

$$f \text{ is injective} \iff f \text{ is surjective}$$

Problem 7.8.27. 考虑以下声明:

> 假设 $f : A \to B$ 和 $g : B \to C$ 是函数。假设 $g \circ f : A \to C$ 是单射。
>
> 然后 g 也是单射的。

以下这个声明的“恶搞”有什么问题?

> 假设 $g \circ f$ 是一个单射。我们想要证明 g 是一个单射。
>
> 设 $x, y \in B$ 已知。假设 $g(x) = g(y)$。
>
> 我们知道 $\exists a, b \in A$ 使得 $f(a) = x$ 和 $f(b) = y$。
>
> 由于 g 是一个定义良好的函数，这意味着 $g(f(a)) = g(x)$ 和 $g(f(b)) = g(y)$。
>
> 由于 $g \circ f$ 是单射且 $g(f(a)) = g(f(b))$，这意味着 $a = b$。
>
> 由于 f 是一个定义良好的函数，因此 $f(a) = f(b)$。
>
> 这意味着 $x = y$。因此，g 是单射的。

同样，找到一个反例来证明该命题的结论是错误的。*Problem* 7.8.28. 设 $a, b \in \mathbb{R}$ 为任意且固定的。假设 $a^2 + b^2 \neq 0$。

考虑函数 $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ 定义为

$$\forall (x, y) \in \mathbb{R} \times \mathbb{R}\text{.} \qquad f(x, y) = (ax - by, bx + ay)$$

证明 f 是一个双射，通过找到其逆函数并证明该逆函数是正确的。

Problem 7.8.29. 设 A 和 B 是有限集，并且假设 $|A| = |B|$。

假设 $f : A \to B$ 是一个单射函数。

证明f也必然是满射的，通过展示$\text{im}_f(A) = B$。

Problem 7.8.30. 设 $k \in \mathbb{N} - \{1\}$ 已知。定义

$$S_1 = \{X \in \mathcal{P}(\,[k]\,) \mid k \notin X\}$$

和

$$S_2 = \{X \in \mathcal{P}(\,[k]\,) \mid k \in X\}$$

(a) 证明集合 S_1 和 S_2 构成 $\mathcal{P}($ 的一个划分 $[k \qquad\qquad\qquad\qquad]\,)$.

(b) 定义一个函数 $f_1 : S_1 \to \mathcal{P}(\,[k-1]\,)$，它是一个双射，并证明它是。

(c) 定义一个函数 $f_2 : S_2 \to \mathcal{P}(\,[k-1]\,)$，它是一个双射，并证明它是。

(d) 使用你在(a)、(b)和(c)中证明的内容，写出一个 **induction** 证明，证明 $\mathcal{P}(\,[n]\,)$ 有 2^n 个元素，对于每一个 $n \in \mathbb{N}$。

> 注意：由于上述 $k \geq$^2 的限制，将 $n =$^1 作为你的基准情况，在归纳假设中使用 $n = k \geq$^1，并在归纳步骤中证明 $n = k +$^1 的命题。

Problem 7.8.31. 设 A, B, C, D 为集合，并假设 $A \cap B = C \cap D = \varnothing$。假设 $f : A \to B$ 和 $g : C \to D$ 是双射。

定义分段函数 $h : A \cup B \to C \cup D$ 通过设置

$$\forall x \in A \cup B\text{.}\ h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B) \end{cases}$$

解释为什么 h 是一个定义良好的函数。然后，证明它是一个 **bijection**。

Problem 7.8.32. 在这个问题中，你将证明每当 A 和 B 与 $|A| = a$ 和 $|B| = b$ 都是有限的时，就必然有 $|A \times B| = ab$。这将被结构化为关于两个变量 $a, b \in \mathbb{N}$ 的“双重归纳”证明。

(a) 证明 $\big|\,[1] \times [1]\,\big| = 1$.（这非常、非常简单，但有必要。）

(b) 假设 $n \in \mathbb{N}$ 和 $\left|\, [1] \times [n] \,\right| = n$。证明 $\left|\, [1] \times [n+1] \,\right| = n+1$。

(c) 解释为什么 (a) 和 (b) 已经表明 $\forall n \in \mathbb{N}_{\mathbf{O}} \quad \left|\, [1] \times [n] \,\right| = n.$

(d) 假设 $k \in \mathbb{N}$ 和假设 $\forall n \in \mathbb{N}_{\mathbf{O}}$

$\left|\, [k] \times [n] \,\right| = kn$. Show that $\forall n \in \mathbb{N}_{\mathbf{O}} \quad \left|\, [k+1] \times [n] \,\right| = (k+1)n$.

(e) 解释为什么 (c) 和 (d) 已经表明 $\forall k, n \in \mathbb{N}_{\mathbf{O}} \quad \left|\, [k] \times [n] \,\right|$

(f) 解释为什么（e）证明了上述问题描述中的结果。

Problem 7.8.33. 设 S 为所有无限二进制字符串的集合。（即，S 的元素是无限长的 0 和 1 的字符串。）

找到一个从 S 到 $\mathcal{P}(\mathbb{N})$ 的双射。利用这一点来证明 S 是不可数无穷的。

Problem 7.8.34. 对于以下每个集合，你都会得到其基数。通过找到一个与相关集合的双射或引用一个结果来证明所给的基数是正确的。

(**Hint:** 如果你不用某种归纳论证，你的证明可能不够严谨……)

(a) A 是从 $\mathbb{N}$ 到 $\mathbb{N}$ 的所有函数的集合。证明 A 是不可数无穷的。

（**Hint:** 将 A 与从 $\mathbb{N}$ 到 $\{1, 2\}$ 的所有函数集合 S 进行比较。你能解释为什么 S 是不可数无穷的吗？这说明了关于 A 的什么？……）

(b) B 是从 $\mathbb{N}$ 到 $\mathbb{N}$ 的所有函数的集合，具有附加性质

$$\forall x \in \mathbb{N}.\ f(x+1) = f(x) + 1$$

证明 B 是可数无限的。

(c) C 是从 $\mathbb{N}$ 到 $\mathbb{N}$ 的所有函数的集合，具有以下附加属性:

$$\forall x \in \mathbb{N}.\ f(x+1) = f(x) + 1$$
$$f(1) = 42$$

证明 C 是有限的，并且只有一个元素。

Problem 7.8.35. 回顾第7.6.14例，我们在其中（非正式地）通过将集合描绘为点格并描述一个覆盖所有点的可数无限路径来论证 $\mathbb{N} \times \mathbb{N}$ 是可数无限的。

通过定义一个函数 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (或反之亦然) 来形式化这个论证，该函数实现了我们描述的路径（或类似的路径）并证明它是一个双射。

Problem 7.8.36. 证明推论7.6.23。也就是说，证明有限集合的可数无穷并集是可数无穷的。

Problem 7.8.37. 考虑定理7.6.22，该定理表明可数无限个可数无限集的并集也是可数无限集。在我们的证明中，我们只考虑了给定的集合是*pairwise-disjoint*的情况。在这个问题中，你应该证明一般情况，即集合不一定两两互斥。

（**Hint:** 考虑我们在证明中使用的函数。你能将它们改编来找到从 $\mathbb{N} \times \mathbb{N}$ 到集合的并集的 *surjection* 吗？）

Problem 7.8.38. 考虑所有无限二进制字符串的集合 S。我们之前已经证明了 S 是不可数无限的。

考虑集合 $T \subseteq S$，它是所有仅包含 *finitely* 个 1 的无限二进制字符串的集合。

在这个问题中，你将证明实际上 T 是 *countably* 无穷大！

(a) 考虑所有自然数的有序 k-元组集合 $\mathbb{N}^k$。(注意：$\mathbb{N}^1 = \mathbb{N}$ 和 $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$。) 提供一个归纳论证，以表明对于每个 $k \in \mathbb{N}$，$\mathbb{N}^k$ 是可数无穷的。(提示：这应该是一个相当简短的证明。你应该引用在讲座中证明的关于可数无穷集合笛卡尔积的结果。)

(b) 对于每个 $k \in \mathbb{N}$，令 $T_k \subseteq T$ 为所有包含 *exactly* k 1s 的无限二进制字符串的集合。

找到一个从 T_k 到 $\mathbb{N}^k$ 的双射（或至少是单射）函数。解释为什么你的函数是良定义的，并且是一个双射（或注入）。

(©) 使用(b)推导出T_k是可数无限的。（注意：如果您只找到一个注入，您还应该解释为什么T_k不是有限的。）

(d) 将 T 表示为集合的并集，并推导出 T 是可数无穷的。

(提示：您需要应用讲座中的一个重要定理。)

（旁白：考虑这个结果的可能后果。通过一个简单的双射，你可以推断出所有只有有限个0的无限二进制字符串集合 *also* 是可数无限的。这意味着集合 S，即无限二进制字符串集合，是无限的完全与包含无限个1和0的字符串集合 *uncountably* 相关联。仅这个集合就足够大，足以使 S 不可数！

Problem 7.8.39. (a) 让 $n \in \mathbb{N}$。考虑集合

$$S = \{f : [n] \to [n] \mid f \text{ is a bijection } \}$$

证明 S 是 *closed under composition*；也就是说，证明

$$\forall f, g \in S \,.\, f \circ g \in S$$

(**Hint:** 引用本章练习部分的一个问题.)

(b{v²} 考虑集合

$$T = \Big\{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a bijection and } \{i \in \mathbb{N} \mid f(i) \neq i\} \text{ is finite} \Big\}$$

证明 T 也是 *closed under composition*。

(©) 证明 T 是 *closed under inverses*；也就是说，证明

$$\forall f \in T \,.\; f^{-1} \text{ exists } \wedge\; f^{-1} \in T$$

(d) 考虑集合

$$U = \big\{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a bijection} \big\}$$

证明 U 在逆元下是闭合的。

(e) 证明以下公式：{v*}

$$\forall f \in T \,.\; \forall g \in U - T \,.\; \big(f \circ g \notin T \;\wedge\; g \circ f \notin T \big)$$

(f) 找到一个反例以表明 $U - T$ 在复合运算下是 **not** 闭的。

(r) 此外，给定 $A \subseteq \mathbb{N}$ 和 A **finite**，找到函数 $f, g \in U - T$ 使得

$$\{i \in \mathbb{N} \mid (f \circ g)(i) \neq i\} = A$$

(h) 什么是 S, T, U 的基数? 如果你的答案是“有限”，也请说明其大小。如果你的答案是“无限”，也请说明是 *countable* 还是 *uncountable*，并通过找到一个适当的集合的双射或引用相关结果来证明你的说法。

7.9 Lookahead

在下一章中，我们将研究**combinatorics**，“计数事物”的数学分支。我们在关于基数的那一节中看到，关于有限集的许多结果似乎相当直观。当我们研究组合数学时，我们将通过描述它们具有哪些属性来*describing*集合的元素，而不是简单地陈述所有属性或列出它们。这实际上会使确定我们描述了多少元素变得相当有趣（有时也非常困难！）。组合数学是研究确定具有某些属性的集合元素数量的技术。我们将陈述并证明一些计数的基本原理（实际上会引用本章的结果），并使用它们来构建更高级的技术并解决一些有趣的问题。

Chapter 8

Combinatorics: Counting Stuff

8.1 Introduction

现代数学中最活跃和令人兴奋的兴趣领域之一是**combinatorics**的领域。有时它也被称为“离散数学”，以区别于**analysis**，后者研究更“连续”的概念，如实数线和定义在该集合上的函数。在本章中，我们将探讨组合数学的一些基本思想，并将它们应用于解决有趣的问题。本质上，我们将学习有关如何*count*有限集合中元素数量的有趣和有用的原则，其中这些元素以某种方式描述但未为我们列举。

8.1.1 Objectives

以下本引言中的简短部分将向您展示本章如何融入本书的体系结构。它们将描述我们之前的工作将如何有所帮助，它们将激励我们为什么要关注本章中出现的主题，并且它们将告诉您我们的目标和在阅读过程中您应该牢记什么以实现这些目标。现在，我们将通过一系列声明为您总结本章的主要目标。以下各节将更详细地重申这些观点，但这将为您提供一份供未来参考的简要清单。当您完成本章的学习后，请回到这份清单，看看您是否理解了所有这些目标。您明白为什么我们将它们列为重要吗？您能定义我们使用的所有术语吗？您能应用我们描述的技术吗？

By the end of this chapter, you should be able to ...

- 列出加法和乘法规则，并使用和组合它们来构建简单的计数论证。
- 将几个标准计数对象进行分类，以及列出相应的计数公式，并理解如何证明它们。
- 说明二项式系数的含义，评估它们的数值公式，了解如何在计数论证中使用它们，并理解如何推导这些数值公式。
- 对所提出的计数论点进行批判，通过适当展示它是否是低估或高估。
- 证明组合恒等式，通过构建“两种方式计数”的证明。
- 理解具有重复的选代的多种表述，并使用它们解决问题。
- 陈述抽屉原理并使用它在计数论证中。
- 陈述包含-排除原理，并在计数论证中使用它。

8.1.2 Segue from previous chapter

第7章，我们中断了对集合的基数（有限和无限）的讨论。虽然关于无限集合的许多结果都很有趣且数学上丰富，但那个特定领域可能会引导我们进入一些令人困惑和难以理解的地方，遗憾的是，这些内容超出了我们当前研究的范围。现在，我们将专注于有限集合。特别是，我们将探讨有限集合的某些结果如何用于解决关于“计数”数学对象的问题。也就是说，我们将探讨如何回答形式为“有多少对象具有属性X？”的问题。这一数学分支被称为*combinatorics*。你可以将其视为“对象组合的研究”。在研究这一数学分支时，我们将开发一些新的符号和定义，证明并使用一些关于有限集合的结果，并描述和研究一些存在于组合数学和计算机科学领域的特定对象。重要的是，我们将学习一种基于计数对象的新证明技术！

8.1.3 Motivation

考虑玩扑克。如果你不熟悉这个游戏，只需将其视为一个简单的系统，其中两名玩家各自收到一副5张随机牌，然后他们比较以确定谁赢。牌面按照以下列表从高到低排序：

- 同花顺（一色五张），例如 $T\clubsuit$ $J\clubsuit$ $Q\clubsuit$ $K\clubsuit$ $A\clubsuit$
- 四种同花，例如 3♣ 3♠ 3♡ 3♢ 7♡
- 全堂（三张同点和一对），例如 4♣ 4♠ 4♢ 6♣ 6♡
- 洗牌（同花五张），例如 2♡ 5♡ 8♡ $Q\heartsuit$ $K\heartsuit$
- 直排（一行五张，不要求花色相同），例如 8♢ 9♣ $T\diamondsuit$ $J\heartsuit$ $Q\heartsuit$
- 三种同花，例如 $K\spadesuit$ $K\heartsuit$ $K\diamondsuit$ $Q\heartsuit$ 9♣
- 两对，例如 $A\spadesuit$ $A\heartsuit$ $J\spadesuit$ $J\diamondsuit$ 2♣
- 一对，例如 8♡ 8♢ 2♠ 5♣ $K\heartsuit$
- 高牌，例如 $Q\spadesuit$ $J\clubsuit$ 9♢ 7♢ 2♢

这是公平的游戏吗？如果你以前玩过扑克，尤其是如果你玩得很多，你不仅学会了接受这个排名系统，而且也学会了如何利用它并做出决策。在五张牌单抽中，如果你被发到22345，你应该保留对子还是追求顺子？哪一种情况更有可能发生？哪一种会带来更大的回报？

通过我们的问题，“这是一场公平的游戏吗？”，我们真正想知道的是 *why* 排名是否就是这样！抽到同花是否实际上比顺子更罕见？满贯是否应该输给四条？为什么？我们如何 *prove* 这些结果？为了回答这些问题，我们将用 *counting* 而不是概率来重新表述问题。我们将询问有多少 *many* 个不同的五张牌手牌是同花，有多少 *many* 个是顺子，等等。这将使我们能够直接比较它们。你看到这与我们上一章的工作有什么关系了吗？我们将真正识别所有同花扑克手牌集合的 *cardinality*，例如，并将其与其他手牌集合的基数进行比较。

8.1.4 Goals and Warnings for the Reader

我们需要开发一些符号和定义来开始制定一种计算特定有限集合元素数量的方法，但我们想强调，这确实是整个过程的核心：*combinatorics*是关于使用特定方法（我们将在本章中开发）来计算有限集合中元素的数量。更具体地说，我们希望从抽象的角度研究这些计数技术，以便我们可以以*efficient*的方式应用它们。也许我们可以通过查看所有可能的五张牌的手牌，并在看到同花顺时做一个记号来回答我们上面提出的扑克问题，但显然这会花费太多时间！肯定有更好的方法！当然，有，我们将在本章的第一节中很快开发出来。

我们想强调，在本章中，我们还将开发一种新的证明风格。与之前我们研究的问题和技术相比，组合学的证明在很大程度上依赖于语言的清晰性和具体性。

一些你在这些章节中的练习证明可能完全由英语句子组成，几乎没有数学符号！这乍一看可能很奇怪，甚至可能似乎与我们迄今为止强调的精确性、清晰性和数学严谨性相矛盾。但这绝对不是情况；组合数学在有限集合理论中有一个严谨的基础，我们将努力指出每当相关时这种关系。组合数学的这一特性还要求你在撰写证明时格外小心，确保你的措辞选择适当，以避免歧义并清晰易懂。比以往任何时候都要更加确信，在写完证明后，假装你是另一个人，以确保你想要表达的观点实际上在证明中得到了体现。

一个最后的介绍性观点可以通过以下引用来表达，这是我的一位朋友在我们讨论如何教授组合数学时说过的。我发现它很好地总结了从我们迄今为止所进行的证明（可能感觉相当正式）到组合数学证明（可能感觉相当非正式）的有时奇怪的过渡。

有限基数很无聊。这与组合学很难的事实并不矛盾。

您现在可能不知道这是什么意思，但如果你在阅读完这一章后回顾这句话，你就会明白他的意图。这意味着，在抽象和理论的意义上，有限的基数 {v*} 很无聊；所有结果都是你所期望的——就像 $|A \cup B| = |A| + |B|$ 当 $A \cap B = \varnothing$ 时——而且技术都是一样的——找到一个适当的集合的双射。*Infinite* 的基数要奇怪和令人惊讶得多——$|A \cup B| = |A| + |B|$ 可以是 False，即使 $A \cap B = \varnothing$，更进一步，加法 $|A| + |B|$ 在数学上很难理解！

如何组合数学有所不同呢？嗯，在我们所有的组合数学工作中，我们都被给了一个有限集；区别在于它的元素只是以某种方式对我们来说是 *described*。我们不是直接与集合的元素打交道并要求计数它们。（那会很容易：“一，二，三，……”）我们必须想出相关且有帮助的策略来识别 *many* 个对象具有某种规定的属性列表。*That* 就是组合数学困难的地方。当我们说，“考虑从一副标准扑克牌中抽取的所有5张牌的手牌”，你可以立即理解这个集合的概念，但你当然无法想象 *all* 它的元素在你面前展开，更不用说开始逐个计数了。从这个意义上说，组合数学很难；这也是为什么它如此有趣和受欢迎的原因！

8.2 Basic Counting Principles

8.2.1 The Rule of Sum

回顾我们在上一章中证明的定理7.6.7。它说当我们取两个不相交的有限集合（即它们没有共享的元素）时，{v*}

它们的并集大小是它们各自大小的总和。这对于有限集合来说直观上是合理的，我们使用双射数学上证明了这一结果。这一结果构成了组合学第一个、基本有用的原理的基础。注意，这使我们牢固地立足于集合论的原则。

Partitions

我们首先回顾定义3.6.9，该定义是在我们讨论集合时引入的。

Definition 8.2.1. *Let A be a set. A* **partition** *of A is a collection of sets that are pairwise disjoint and whose union is A.*

That is, a partition is formed by an index set I and non-empty sets S_i (defined for every $i \in I$) that satisfy the following conditions:

(1) For every $i \in I$, $S_i \subseteq A$.

(2) For every $i, j \in I$ with $i \neq j$, we have $S_i \cap S_j = \varnothing$.

(3) $\bigcup_{i \in I} S_i = A$

本质上，一个划分是将一个集合分解成不重叠的较小集合的方法。在继续之前，让我们看看几个例子。

Example 8.2.2. 设A为当前房间内的人的集合。设$I = \{1, 2\}$，设S_1为左撇子的集合，设S_2为右撇子的集合。那么$S = \{S_1, S_2\}$是A的一个划分。注意区分写作“$\{S_1, S_2\}$划分A”，这是正确的，和“S_1, S_2划分A”，这是不正确的。在这个上下文中说S_1, S_2是什么意思？我们真正意思是说这两个集合，作为一个集合，形成A的划分。这就是为什么我们必须记住要在括号中写出元素S。

为了严谨起见，我们应该 *prove* 为什么 S 是 A 的一个划分。为此，我们指出 $S_1 \cap S_2 = \varnothing$ 因为这里每个人要么是左撇子要么是右撇子，但不是两者都是。（让我们假设这里没有“特殊情况”，比如真正双手灵巧的人或没有手的人。如果这样的人在场，将他们包含在集合 S_3 中，并将该集合包含在我们的划分集合 S 中。）我们还指出 $S_1 \cup S_2 = A$ 因为房间里每个人必须是左撇子或右撇子，因此 *cannot* 存在一个元素 $x \in A$ 满足 $x \notin S_1$ 和 $x \notin S_2$。这表明 S 是一个划分。

如果我们想根据他们名字的第一个字母将这个房间里的人分成几组呢？尝试用数学符号定义这个划分，就像之前的例子一样。

Example 8.2.3. 现在，让我们看看一个非有限划分。考虑集合 $A = \mathbb{N}$ 和指标集 $I = \mathbb{N}$。对于每一个 $i \in \mathbb{N}$，定义集合

$$S_i = \{2i - 1, 2i\}$$

是集合 $S = \{S_i \mid i \in \mathbb{N}\}$ 是集合 $\mathbb{N}$ 的划分吗？我们认为是的；让我们来调查一下原因。我们可以从写出前几个集合的样子开始（实际上，这通常是一个好的第一步策略：只写出前几个情况，看看会发生什么）：

$$\begin{aligned} S_1 &= \{1, 2\} \\ S_2 &= \{3, 4\} \\ S_3 &= \{5, 6\} \\ &\vdots \end{aligned}$$

等等。这似乎是到目前为止 $\mathbb{N}$ 的一个划分，不是吗？让我们证明它确实是吧！

首先，让我们证明集合 S_i 是 *pairwise-disjoint* (，即任意两个集合没有共享的元素)。我们通过反证法来证明这一点。假设 $\exists i, j \in \mathbb{N}$ 与 $i \neq j$ 满足 $S_i \cap S_j \neq \varnothing$。这意味着（至少）$S_i$ 中的一个元素也是 S_j 的一个元素；我们发现这种情况有四种可能的情况：

1. $2i - 1 = 2j - 1$
2. $2i - 1 = 2j$ 33.
$2i = 2j - 1$4. $2i =$
$2j$

第一个和第四个情况立即表明，通过一些简单的代数运算，$i = j$与我们的给定条件$i \neq j$相矛盾。第二个和第三个情况本身就是矛盾，因为它们涉及一个奇自然数和一个偶自然数相等。无论如何，我们都会找到一个矛盾。因此，$\forall i, j \in \mathbb{N}$与$i \neq j$一起，$S_i \cap S_j = \varnothing$的情况成立。

其次，让我们证明所有 S_i 集合的并集是 $\mathbb{N}$。也就是说，让我们证明

$$\bigcup_{i \in \mathbb{N}} S_i = \mathbb{N}$$

记住，左侧的集合由所有满足$x \in S_i$的元素x组成。$\exists i \in I$（思考一下为什么这有意义，即使I是无限的。这仅仅意味着并集包含属于至少一个集合S_i的所有元素。）注意，对于每个$i \in \mathbb{N}$，元素$2i - 1, 2i \in S_i$都是自然数。因此，

$$\mathbb{N} \supseteq \bigcup_{i \in I} S_i$$

接下来，我们证明反向集合包含。设$n \in \mathbb{N}$。我们需要考虑两种情况。（1）如果n是偶数，那么$\exists k \in \mathbb{N}$使得$n = 2k$。因此，$n \in S_k$。（2）如果n是奇数，那么$\exists \ell \in \mathbb{N}$使得$n = 2\ell - 1$。因此，$n \in S_\ell$。在任何情况下，我们都已经证明了$n \in \bigcup_{i \in I} S_i$.

因此，S 是 $\mathbb{N}$ 的一个划分。特别是，它是一个无限划分。

现在我们看到了一个有限和无限的例子 {v*}。 投标。
(您能否识别一个$\mathbb{N}$的无限划分，使得该划分的所有分量集都是*also*无限的？)

Statement

对于本章剩余部分，我们只考虑有限集的 *finite* 个划分。特别是，求和规则仅适用于这个特定情况。

Proposition 8.2.4. *Let A be a finite set, let $n \in \mathbb{N}$, and let $S = \{S_i \mid i \in [n]\}$ be a finite partition of A. The* **Rule of Sum** *states that*

$$|A| = \sum_{i \in [n]} |S_i|$$

求和法则告诉我们，可以通过将集合划分为有限个更小的集合并求和它们的尺寸来找到集合的大小。注意，这正是我们在上一章讨论有限集合时看到的推论7.6.10！在那里，我们要求你在7.6.5节的练习2中通过归纳法证明这个命题。有了这个结果，我们将继续看一些例子。

Examples

Example 8.2.5. 在独特活动大学，每个学生每年都必须参加*exactly*一项大学体育项目。参加多项会占用太多时间，而不参加则会使他们变得懒惰，所以每个人都必须参加以下非传统但仍然是体育项目的其中一项：高尔夫、板球、羽毛球和象棋。体育部门发布了今年每个运动队名单的以下统计数据：

- 高爾夫：12名球員
- 板球：18名球员
- 羽毛球：23名球员
- 国际象棋：33名选手

有多少学生参加UAU?

好的，这是一个简单的例子，因为我们确保了大学提供的运动项目构成了学生集的一个划分。（与句子“大学提供的运动项目构成了学生集的一个划分。”进行比较，两者都是正确的。）因此，我们可以通过相加来找到S的基数，即所有学生的集合；

$$|S| = 12 + 18 + 23 + 33 = 86$$

一所小型大学，确实，而且非常奇特。不要去那里。

当我们将求和法则与其他计数原则结合时，将出现更多有趣的求和法则应用示例。目前，它是一个简单的想法，决定了如何计数可以分解为不相交部分的集合。一般来说，使用求和法则最难的部分是决定应用它的 $which$ 分区，并在这方面发挥创造力。

下一个计数原理同样，如果不是更有帮助，但定义和证明稍微复杂一些。

8.2.2 The Rule of Product

Motivation

我们将通过一个例子来解释这个原理。

Example 8.2.6. 假设房间里有三个人。我们还有三个贴纸，上面分别写着数字1、2和3（每个贴纸上的数字都是唯一的）。我们有多少种方法可以将这些贴纸放在三个人身上？为了方便讨论，我们假设这三个人分别叫Andy、Brendan和Carl，方便地简称为A、B和C。为了回答这个问题，我们可以以有组织的方式列出所有贴纸分配，以确保不遗漏任何一种。具体来说，我们将它们按照Andy的分配、然后是Brendan的、最后是Carl的顺序进行排序：我们有 $(A, B, C) =$

1. (1, 2, 3)
2. (1, 3, 2)
3. (2, 1, 3)
4. (2, 3, 1)
5. (3, 1, 2)
6. (3, 2, 1)

因此，共有6种方式分配贴纸。

如果我们有四个人——Andy、Brendan、Carl和Dave——以及四个贴纸？我们能列出所有这些分配吗？当然可以，为什么不呢？

$$
\begin{array}{cccc}
(1,2,3,4) & (1,2,4,3) & (1,3,2,4) & (1,3,4,2) \\
(1,4,2,3) & (1,4,3,2) & (2,1,3,4) & (2,1,4,3) \\
(2,3,1,4) & (2,3,4,1) & (2,4,1,3) & (2,4,3,1) \\
(3,1,2,4) & (3,1,4,2) & (3,2,1,4) & (3,2,4,1) \\
(3,4,1,2) & (3,4,2,1) & (4,1,2,3) & (4,1,3,2) \\
(4,2,1,3) & (4,2,3,1) & (4,3,1,2) & (4,3,2,1)
\end{array}
$$

好的，所以有24种总方法来分配贴纸。如果是五个人呢？我不知道你们，但我的手臂在写下所有这些分配变得很累。一定有更好的方法来做这件事！是的！这就是

产品法则来拯救这一天。（旁注：你可能会注意到我们上面的列表中有一个模式；你能推断出我们是如何确保我们实际上列出了*all*种可能性吗？你能写一个小程序来生成所有可能性，对于任何数量的元素？试试吧！）

Statement

我们将实际上对乘法法则做出两个单独的陈述。第一个是对何时以及如何应用它以及它所声称的内容的直观陈述。第二个是一个更严谨、数学化的陈述，它基于我们一直使用的集合论语言。我们强调，这两个定义理想情况下都应被理解；然而，真正理解第一个定义更为重要，第二个定义主要提出是因为它是可以且将被严格证明的那个。

Proposition 8.2.7. *Consider a process that is completed in n distinct steps. Assume that the i-th step, for every $i \in [n]$, has exactly w_i different ways to be completed; moreover, assume that this number $w_i \in \mathbb{N}$ does* 非 *depend on the choices made in the previous steps. Also, assume that no two distinct choices at any step yield the same outcome. Then the Rule of Product states that the total number of outcomes, N, of this n-step process is*

$$N = \prod_{i \in [n]} w_i$$

让我们将这个陈述与之前关于人和贴纸的例子联系起来，然后再继续并更严格地陈述乘法法则。

Example 8.2.8. 我们可以将将贴纸分配给Andy、Brendan和Carl视为一个三步过程。让我们按字母顺序从左到右排列三位绅士，然后沿着行移动。在每一步中，我们将通过选择一个尚未分配的贴纸来放置在我们面前的绅士。在第一步中，我们接近Andy，有3种可能的贴纸可以放在他身上。在第二步中，我们接近Brendan，有2种可能的贴纸可以放在他身上。注意，这是真的 *no matter what sticker was chosen for Andy*。我们实际上并不关心 *which* 贴纸被选为Andy——无论是1、2还是3——只是当我们面对Brendan时，我们的 *number*选择数量是*always* 2。在第三步中，我们接近Carl，发现无论前两步的选择如何，我们只有1种贴纸选项。

产品法则告诉我们，完成这个过程的方法数是每一步选项数的乘积：$3 \cdot 2 \cdot 1 = 6$。这与我们的“穷举法”程序一致。太棒了！

关于4个人呢？使用相同的逻辑，我们可以看到有$4 \cdot 3 \cdot 2 \cdot 1 = 24$种可能的贴纸分配方式。再次，这与我们之前的程序一致。双倍的欢呼！

关于5个人呢？嗯，$5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$。我们发现了我们之前不知道的事情。三声欢呼！6个人呢？7个人呢？

使用 n 人，$n \in \mathbb{N}$? 我们现在可以非常容易和精确地回答所有这些问题，多亏了乘法法则。无限欢呼!

Tree Diagrams

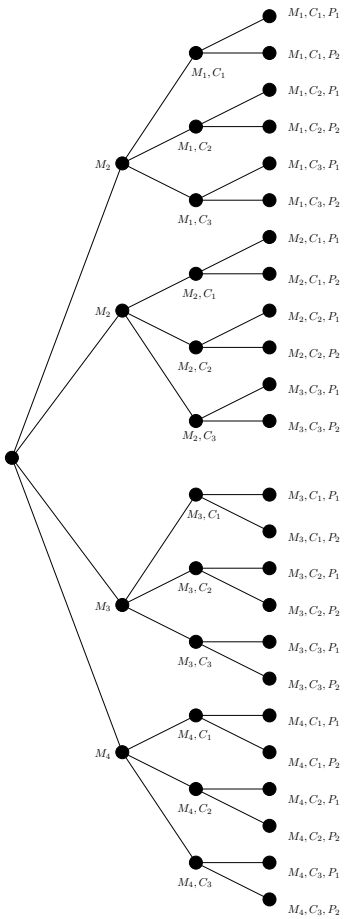
一个有趣的、有帮助的乘法法则解释可以通过一个 *tree diagram* 来证明。*tree* 的概念出现在被称为 *graph theory* 的数学分支中，该分支研究由顶点（点）通过边（点之间的线）连接的数学对象，我们只关心线是否 *present*，而不关心它在纸上“看起来”如何。树是一种特殊的图，它在计算机科学中也很常见，尤其是在研究 *branching processes* 时。在我们的语境中，我们可以使用树来表示 *procedure* 的决策点，其最终产品将通过乘法法则来计数。此外，这种方法将为我们提供对乘法法则数学上 *rigorous* 陈述和证明的一些见解。（我们将这些最终目标留给练习，但对于那些有兴趣并愿意尝试的人来说，我们强烈建议阅读这一部分；它将给你一些直觉并引导你完成这些练习。）

Example 8.2.9. 让我们通过一个例子来说明树状图以及它们如何与乘法法则相关。假设我们正在为下个学期的课程表做规划。根据我们的专业和时间限制（当然，还有个人兴趣），我们必须从每个三个系中各选一门课程：数学、计算机科学和哲学。我们可以在每个系选择的课程数量取决于我们在任何其他系的选择；具体来说，我们有4门数学课程可供选择，3门计算机科学课程，以及2门哲学课程，任何课程组合都将适合我们的课程表（前提是每个系恰好被代表一次）。

我们如何将乘法法则应用于我们的情况? 我们需要定义一个 *process* 以及该过程的 *steps*，然后确定每个步骤有多少 *choices* 可用。自然地，这里的整体过程是确定下个学期的课程表。由于我们被限制在每个系中恰好选择一门课程，让我们确定三个步骤：（1）选择一门数学课程；（2）选择一门计算机科学课程；（3）选择一门哲学课程。（注意：这些步骤的 *order* 是否重要? 如果我们首先选择哲学课程会怎样? 我们的过程会从根本上 *different* 吗? 我们认为不会，但在继续阅读之前确保你明白为什么。）

接下来，让我们表示每一步我们可以做出的选择。假设可供选择的4门数学课程集合是$\mathcal{M} = \{M_1, M_2, M_3, M_4\}$，3门计算机科学课程集合是$\mathcal{C} = \{C_1, C_2, C_3\}$，2门哲学课程集合是$\mathcal{P} = \{P_1, P_2\}$。这立即为我们确定了每一步的可选方案数*number*：(1)有$|\mathcal{M}| = 4$种选择；(2)有$|\mathcal{C}| = 3$种选择；(3)有$|\mathcal{P}| = 2$种选择。因此，乘法原理告诉我们，我们可以为下学期创建24种总课程表。但是，

真的，*why*这是真的吗？那些*are*日程表是什么？让我们用树状图来表示它们吧！



从左到右阅读图中的内容，我们正在遵循我们建立的三个步骤程序。最左边的单个顶点（或节点）代表我们过程的开始——尚未做出任何决定——从这个顶点发出的四个边（或分支）代表我们可以选择的四门数学课程。我们已将每个边标记为 $\mathcal{M}$ 中的一个元素。无论我们跟随哪条边（即无论我们选择哪门数学课程），下一个顶点都会出现三条边（即我们仍然有三个计算机科学课程可以选择）。我们已将这些边全部标记为来自 $\mathcal{C}$ 的相应元素。按照同样的思路，该列中的每个顶点都有两条发出的边，这些边由 $\mathcal{P}$ 中的相应元素标记。

这个图表的好处是，我们可以通过跟随边上的标签来看到 *exactly* 这个过程的24个结果。例如，看看最右边列顶部的顶点。这对应于选择 M_1 和

C_1 和 P_1；或者，我们可以将其表示为有序三元组 (M_1, C_1, P_1)。在该列的下方，我们看到一个与有序三元组 (M_2, C_3, P_1) 对应的顶点，例如。每个顶点都有一个有序三元组表示！当我们应用乘积规则时，我们实际上是在识别一些 *set* 的基数，它是几个构成集合的 *Cartesian product*。*process* 对应于识别构成集合的元素并将它们排列在有序元组中。乘积规则告诉我们，通过识别由 *all* 这样的元组组成的乘积集合的 *cardinality*，我们可以进行多少次这样的操作。在这个特定例子中，我们有

$$|\mathcal{M} \times \mathcal{C} \times \mathcal{P}| = |\mathcal{M}| \cdot |\mathcal{C}| \cdot |\mathcal{P}| = 4 \cdot 3 \cdot 2 = 24$$

现在这更有意义了吗？这让你对乘法法则实际上是如何工作的有任何洞察吗？

More Formal Statement

参见练习8.9.1，该练习要求证明以下定理。这是对乘积法则的更正式的数学表述。在陈述之后，我们将描述它如何与之前的版本相关。

Theorem 8.2.10. Rule of Product (Set-Theoretic Version)

Let $n \in \mathbb{N}$. Suppose that $\forall i \in \mathbb{N}$. T_i is a finite set. Then,

$$\left| \prod_{i \in [n]} T_i \right| = |T_1 \times T_2 \times \cdots \times T_n| = |T_1| \cdot |T_2| \cdots |T_n| = \prod_{i \in [n]} |T_i|$$

与之前所述的乘积规则的关系如下。集合 T_1 的元素是过程中第一步可以选择的选项。对于 T_1 的每个元素，我们定义集合 T_2 为过程中第二步可以选择的选项集合，这些选项是在第一步中做出的选择。根据假设，无论第一步的选择如何，此类选择的数量都是相等的 *number*。因此，定理的结论只包含 $|T_2|$ 是有意义的，因为这个值是明确定义的。同样，T_3 是可以跟随第一步和第二步选择的第三步的选项集合，并且根据假设，$|T_3|$ 是明确定义的。

最终，我们可以通过一个有序的 n-元组来描述这个过程的 **outcome**，其中坐标 i 是集合 T_i 的一个元素。实际上，这个元素可能是什么确实取决于之前的坐标，但这个元素的选择 **number** 与之前的选项无关。由于最终我们真正关心的是可能结果的数量 **number**，所以这个结果是有意义的。实际上，要分析所有结果都需要对每个步骤进行仔细分析，看看一个特定的选择如何影响下一步（以及之后的步骤）的选择，但这并不是这个结果的重点。这就是为什么，本质上，这个结果相当于证明有限集合的乘积的大小等于它们大小的乘积。

Example: Applying the Rules of Sum and Product (Together)

让我们练习使用这两条组合规则。你也会注意到，我们将开始将这些规则缩写为ROS和ROP，这样我们就可以轻松引用它们。是的，当我们使用它们时，我们会用*need*来引用它们!

Example 8.2.11. **License Plates:**

假设车牌字符串由6或7位组成，每个位置都填充了一个字母（从A到Z）或一个数字（从0到9）。

(1) 有多少个车牌号？我们必须根据字符串长度进行划分，是6位还是7位。在每一部分中，我们有一个6步或7步的过程。在第 i 步，我们在字符串中的位置 i 用36种选项之一进行填充（有26个字母和10个数字）。因此，通过ROP，有36^6个6位字符串和36^7个7位字符串。通过ROS，总共有$36^6 + 36^7$个车牌号字符串。

(2) 至多有多少个车牌号只有1位数字?

我们必须根据是否有0个数字或1个数字进行划分。

使用0个数字，我们过程中的每一步都将一个字母放置在相应的位置。我们或者有6个字母——产生26^6种可能性——或者有7个字母——产生26^7种可能性，通过ROP。

通过ROS，有36^6或36^7这样的结果。

使用1位数字，步骤1a选择哪个位置填充数字，步骤1b选择该位置的数字，其余步骤仅用字母填充剩余位置。

有6种选择来确定哪个位置是数字，然后有10种选择来填充*that*位置（无论它在何处），其他位置各有26种选择。应用ROS和ROP，我们发现存在$6 \cdot 10 \cdot 36^5$或$7 \cdot 10 \cdot 36^6$这样的结果。

总共，通过ROS，有

$$(36^6 + 6 \cdot 10 \cdot 36^5) + (36^7 + 7 \cdot 10 \cdot 36^6)$$

总结果。

(3) 至少有2个数字的牌照有多少个?

我们可以遵循与上一个问题相同的方法，将这组车牌分为3位数、4位数、5位数、6位数和7位数。然后我们需要计算每个这样的集合的大小并将它们相加。但是，有多少车牌有4位数？有6个位置需要填充，有多少种选择4个位置作为数字的方法？这正是*binomial coefficients*将很快派上用场的地方

(在定义它们并推导出一个公式)之后。

相反，让我们利用我们刚刚完成的工作！让我们将 all 牌照集合（称为集合 Y）分为最多1位数的那些（称为集合 X_1）和至少2位数的那些（称为集合 X_2）。注意，这是一个 is 分区，所以 ROS告诉我们 $|Y| = |X_1| + |X_2|$。通过代数减法，这告诉我们我们想要的表达式是

$$\begin{aligned} |X_2| &= |Y| - |X_1| \\ &= (36^6 + 36^7) - \left[(36^6 + 6 \cdot 10 \cdot 36^5) + (36^7 + 7 \cdot 10 \cdot 36^6)\right] \end{aligned}$$

只需代入我们已推导出的表达式。多么方便!

一般来说，这是一个好的策略：要计算一个集合，我们可以计算它的 $comple\text{-}ment$ (即集合外的所有“其他”元素，并从“总数”中减去这个计数。然而，请记住，我们只有一条 Sum 规则可用，没有减法规则，因此我们应该始终小心（至少目前如此）用 $partition$ 和 sum 的术语来表述这样的步骤。之后，我们可以减去数字或代数变量。最终，一旦我们在数学上更加成熟，我们可以轻松地跳过这种形式，只谈论“减去”一个计数；然而，现在，我们想要强调这些计数论证的基础，因此我们将要求这种谨慎的表述和 Sum 规则的应用。

(4) 有多少车牌既没有元音也没有偶数?

这个条件只是限制了每一步的选择数量。可供选择的字母和数字只有21个，所以我们可以得到

$$26^6 + 26^7$$

总结果，按ROP和ROS。

8.2.3 Fundamental Counting Objects and Formulas

让我们回到我们计数扑克牌手的激励例子。记住，我们想知道每种牌型的数量 $how\ many$，以及从一副新洗过的52张牌中我们可能被发到的同花牌有多少张。让我们先回答一个相关但更简单的问题：有多少种 $total$ 扑克牌手？另一种表述这个问题的方式——实际上这会暗示我们回答它的方法——如下：有多少种方式可以洗一副52张牌，以及其中有多少种方式在顶5张牌中产生相同的扑克牌？也就是说，让我们确定有多少种不同的（即完全不同的）洗牌方式；让我们称这些方式为 $shufflings$。然后，让我们考虑一个特定的手牌，比如 $T\clubsuit\ J\clubsuit\ Q\clubsuit\ K\clubsuit\ A\clubsuit$，并计算有多少种洗牌具有这样的特性：牌堆顶部的5张牌按照 any 的顺序组成那个特定的手牌（因为我们不关心 how 我们收到的5张牌是什么，我们只关心我们手中的牌！）。

我们有的是什么？没错，是加法和乘法规则。基本上就是这样，除了我们的数学智慧和直觉之外，所以让我们直接开始。洗牌如何对应于一个划分，或者一个多步骤过程？好吧，有趣的是，我们实际上并不关心*how*牌是否被洗过，我们只关心*outcomes*过程的数量。关于一副牌真正重要的是什么？没错，从上到下*order*的顺序。有了这个想法，让我们考虑*constructing*一个任意的洗牌，通过分配牌的顺序。

让我们通过手中的一副牌，一张一张地，将牌面朝下放在我们面前的堆叠中，来创建一个洗牌。在第一步，我们手中有一副52张牌，没有堆叠，所以我们有52种选择。在第二步，无论第一张牌是什么，我们手中剩下51张牌可供选择。（记住：这是乘法法则的重要部分，即选择的可能性*number*与实际做出的选择无关。）在第三步，我们剩下50张牌，以此类推。最终，在第52步，我们手中只剩下一张牌可以放在桌上51张牌的堆叠上。完成这一步后，我们面前就有一副洗好的牌，牌面朝下堆叠。第一步的牌在最下面，最后一步的牌在最上面。此外，我们注意到，对于任何任意的洗牌，都有一个*exactly one*序列的选择可以产生那个洗牌。（这满足了乘法法则的另一部分，即有不同结果。仔细思考一下，为什么这是必需的。）

这些观察使我们能够直接引用乘积法则来回答问题：标准一副扑克牌有多少种洗牌方式？这个数字是 ...

$$52 \cdot 51 \cdot 50 \cdots 3 \cdot 2 \cdot 1 = \prod_{k \in [52]} k = 8.06581752 \times 10^{67}$$

哇塞！这是一个很大的数字。为了比较，阿伏伽德罗常数（摩尔中的原子数）的数量级为10^{23}。对于这种乘积有一种更好的表示方法，即“将所有自然数从52乘到1”，你可能之前见过，但现在我们将定义它。

Definition 8.2.12. *Let $n \in \mathbb{N}$. The natural number $n!$, read as n* **factorial***, is given by*

$$n! = \prod_{k \in [n]} k = k \cdot (k-1) \cdot (k-2) \cdots 3 \cdot 2 \cdot 1$$

By definition, $0! = 1$.

(回忆一下，我们曾在2.5.1节中以计算阶乘为例，展示了如何将归纳原理应用于递归编程。请再次阅读该节！)

让我们想想我们实际上取得了什么成就。在这种情况下，数字52有什么特别之处？除了它是我们牌组中的卡片数量之外，没有其他！如果我们提出这样的问题：将 $[n]$ 的元素放入有序列表中有多少种方法？如果我们用52替换 n，这实际上就是

与之前相同的问题！（我们可以在卡片集合和集合[52]之间找到一个自然的双射。你能做到吗？你能看出这为什么表明问题属于*equivalent*吗？）

Permutations

这种问题——将 n 个对象排列成有序列表有多少种方法——非常常见，以至于我们为这些有序列表专门有一个术语。我们严格地用 *functions* 来定义它们，但请注意它们与其他数学对象（例如有序列表）之间的关系。

Definition 8.2.13. *Let $n \in \mathbb{N}$. A* **permutation** *of $[n]$ is a function $f : [n] \to [n]$ that is a bijection.*

Equivalently, a permuation of $[n]$ is an ordered n-tuple of elements from $[n]$ such that every element appears exactly once.

Proposition 8.2.14. *Let $n \in \mathbb{N}$. Let S be the set of all permuations on $[n]$. Then $|S| = n!$.*

Proof. 我们通过选择有序列表中哪个元素首先出现来构造一个任意的 $[n]$ 排列。有 n 种选择。然后，从已经选择的元素 *except* 中选择一个作为列表的第二位。有 $n-1$ 种选择。一般来说，在第 k 步，我们从尚未选择的 $n-(k-1) = n-k+1$ 个元素中选择一个作为下一个出现的元素。这会持续到第 $n-1$ 步，此时我们只有一个选择。通过 ROP，总共有 $n(n-1)(n-2)\cdots 2\cdot 1 = n!$ 种结果。 □

（注意：这促使我们选择将0!定义为1的惯例。因为$n!$表示排列n个对象的方式，而排列空集的所有元素恰好有1种方式——我们刚刚就是这样做的！——因此，$0! = 1$是有意义的。当我们不久后定义*binomial coefficients*时，这个想法将再次出现；对于相应的公式，$0! = 1$将非常有帮助。）

Selections

这从数学上证明了关于洗牌的观察的一般版本，并且它使我们更接近回答我们最初关于扑克牌手排名的问题。记住，我们希望确定有多少种不同的洗牌方式会在前五张牌中产生某种类型的五张牌手牌，所以让我们先解决一个稍微更一般的问题。想象一个*specific*五张牌手牌，五张特定的牌。我们正在考虑 $T\clubsuit$ $J\clubsuit$ $Q\clubsuit$ $K\clubsuit$ $A\clubsuit$，所以让我们使用它。现在，让我们计算有多少种牌组洗牌会将这张特定的手牌放在前五张牌中。

我们怎么能有这种情况呢？我们不关心我们手中牌的顺序，也不关心牌堆中其他47张牌的顺序。重要的是那些特定的牌是否在顶部。所以，让我们遵循之前使用过的相同思路，*construct*洗牌

使用此属性。我们想使用乘法法则，因此我们需要识别一个特定的过程，该过程构建具有所需属性的洗牌。我们如何做到这一点?

实际上我们只需要满足两个属性，所以让我们确定一个两步过程来确保这些属性成立。第一步应该以某种顺序将我们手中的47张牌放在牌堆底部。第二步应该以某种顺序将我们手中的五张牌放在那堆牌的顶部。乘法原理适用，因为无论我们如何洗牌底部的47张牌，这都不会影响我们洗牌顶部五张牌的方式数量。（一般来说，在应用乘法原理之前，请注意{v*}在特定情况下适用；这通常是微妙的，并不明显！）现在，我们只需要计算执行每一步的方法数量。

第一步涉及创建47张牌的排列。命题8.2.14告诉我们有47!种方法来做这件事。第二步涉及创建五张牌的排列。命题8.2.14告诉我们有5!种方法来做这件事。然后，乘法原理告诉我们依次完成这些步骤的方法数是$47! \cdot 5!$。就是这样!

这个情况下我们选择 $T\clubsuit$ $J\clubsuit$ $Q\clubsuit$ $K\clubsuit$ $A\clubsuit$ 有什么特别之处? 没错，没有! 再次应用乘法法则，这个事实将告诉我们有关牌组洗牌次数的更多信息。具体来说，假设 X 是选择一副扑克牌中五张牌作为一手牌的方法数。现在，考虑从牌组中取出五张特定的牌，以某种顺序排列它们，然后排列下面的其他47张牌的三个步骤过程。乘法法则在这里适用，因为执行每个步骤的方法数不依赖于之前步骤的选择。此外，从牌组中产生的 *every* 洗牌方式正好对应于这个程序中的 *one* 个特定实例。（想想为什么这是真的。考虑一副牌的任意洗牌。最上面的五张牌决定了我们在第一步选择了哪一手牌，它们的顺序决定了第二步是如何执行的，其他牌的顺序决定了第三步是如何执行的。）因此，我们找到了两个特定的公式来计算同一组对象——即一副牌的洗牌方式——因此，这必须是真的

$$X \cdot 5! \cdot 47! = 52!$$

因此

$$X = \frac{52!}{5! \cdot 47!}$$

考虑这个公式告诉我们什么。我们让 X 表示从一副52张牌中选择5张牌的组合方式的数量。5张或52张有什么特别之处? 没错，什么也没有! 我们实际上推导出了一个从更大的对象集合中选择任意数量对象的组合方式的公式。这看起来可能不像，但我们现在非常接近解决扑克牌手牌问题。在我们完成那个项目之前，让我们做一个评论。

首先，我们刚才提出的论证类型是组合数学中一种常见且极其有用的证明技术。它被称为 *counting in two ways*。什么

我们做的是确定一组特定的对象——在这种情况下，一副牌的洗牌组合——然后描述了两种不同的程序，这些程序使我们能够计算该集合的大小。每种程序都导致一个不同的公式，因为我们正在计算相同的对象集合，我们知道这些公式是相等的。我们将在第8.4节中更明确地探讨这种论证类型，并看到许多例子。现在，我们希望你能看到为什么这是一种有效的论证类型，尤其是因为我们期望你用它来证明下面的命题8.2.16！在这样做的时候，你将推广我们在这里提出的论证。为了说明，让我们总结一下我们做了什么：

Argument Summary: 我们寻求从一副52张牌中抽取5张牌的方法数。设N为我们所寻找的该数。我们将识别两个涉及N的表达式的不同公式。这将使我们能够解这些代数表达式以得到N的公式。

(1) 选择一个任意且固定的五张牌的手牌。我们将确定如何洗牌使得牌堆顶部的五张牌是那固定的五张牌手牌，无论顺序如何。

请注意，有 N 种方法来完成这一步。我们寻求一个关于 N 的公式。

(2) 计算一副52张牌的全排列数量。

(3) 计算得到顶部固定五张牌的牌组排列数。这分为三个步骤：

(i) 计算这五张牌的排列方式数量。 (ii) 计算其他47张牌的排列方式数量。 (iii) 计算将这5张排列好的牌放在那47张排列好的牌上面的方式数量。（注意：这只有一种方式，但重要的是将其作为一个单独的步骤指出。）

(4) 总体来说，请注意我们以两种不同的方式计算了牌组排列（即洗牌）的数量，因此它们必须是相同的数字。

(5) 简化涉及 N 的表达式，以找到 N 的公式。

现在，让我们将我们刚刚推导出的公式进行推广。首先，我们进行一个定义并引入一些符号，然后我们陈述一个公式。

Definition 8.2.15. *Let $k, n \in \mathbb{N}$ with $n \geq k$. A* **k-selection** *from $[n]$ is an unordered set of k elements from $[n]$.*

The number of k-selections from $[n]$ is represented by $\binom{n}{k}$. This is known as a **binomial coefficient***, and is read as "n choose k".*

Proposition 8.2.16. *Let $k, n \in \mathbb{N}$ with $n \geq k$. The number of k-selections from $[n]$ is given by*

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

Proof. 作为第8.2.4节中的练习2留给读者 □

Binomial Coefficients

上述公式中你可能觉得令人惊讶的一点是，无论 k 和 n 是什么，这个分数实际上都是一个自然数！这通过证明中描述的它代表完成一个程序的方式的数量来证明，这必须是一个自然数。

我们想指出这个公式的一个特殊情况，这个情况可能不会出现在你的脑海中。如果 k = 为 0，会怎样呢？$\binom{n}{0}$ 应该是多少？你可能会惊讶地发现 $\binom{n}{0}$ = 为 1。这为什么有道理呢？直观上，我们认为 $\binom{n}{k}$ 是从一组 n 个对象中选择 k 个对象的方式的数量；那么，我们如何从，比如说，3 个对象中选择 0 个对象呢？在你的桌子上放 3 支笔。现在，不选择任何一支。就这样！你刚刚完成了一种选择——也就是选择 0 个对象的一种方式。当 n = 为 0 时，这个论点同样适用！在你的桌子上不放任何笔。现在，不选择任何一支。就这样！你再次以一种方式完成了它。因此，

$$\forall n \in \mathbb{N} \cup \{0\}. \binom{n}{0} = 1$$

存在“更好”的、更数学化的理由来解释这个结果，我们将在下一节中证明帕斯卡恒等式时指出这些理由。现在，我们希望这个带有选择的启发式解释能够让你理解并信服这个结果。

另一个事实是，当 $K > n$ 时，$\binom{n}{K} = 0$。这是因为有 no 种选择方式，例如，从只有 3 个对象的集合中选择 5 个对象。这一事实在我们的上述推导中得到证实，因为在其中一步，我们会尝试（不可能地）为一张手牌抽取比该牌堆中卡片 in 更多的牌，这样做有 0 种方式。然后，当我们应用 ROP 时，该乘积将评估为 0。

如果你在 k 和 n 的某些值上玩弄，你会注意到 $\binom{n}{k}$ 的值遵循所谓的 **unimodal distribution**。也就是说，如果我们固定 n 并让 k 从 0 增加到 n，我们会发现数字在上升，达到峰值在 $\lfloor \frac{n}{2} \rfloor$ 和 $\lceil \frac{n}{2} \rceil$（，注意如果 n 是偶数），那么它们是相同的，然后再次下降。此外，分布是围绕那个中间 $symmetric$ 的！你能证明这些属性成立吗？试试吧！

Arrangements

我们现在拥有了计数扑克牌手牌（以及其他许多对象）所需的所有工具。我们知道有多少种方式可以对集合的元素进行排列，也知道有多少种方式可以从更大的集合中选择一个特定大小的子集。在这两个工具之间，我们知道如何计数任何牌的组合。例如，要计数一个$ordered$牌的子集，我们可以计数选择子集和$then$排列其元素的方式，将乘法原理应用于这个两步过程。事实上，这个想法足够常见，我们将给它一个定义名称。

Definition 8.2.17. *Let $k, n \in \mathbb{N}$ with $n \geq k$. A* **k-arrangement** *from* [v2] *is an ordered k-tuple of elements from* [v5] *with no repeated elements.*

Equivalently, a k-arrangement from $[n]$ is a function $f : [k] \to [n]$ that is an injection.

Proposition 8.2.18. *Let $k, n \in \mathbb{N}$ with $n \geq k$. The number of k-arrangements from $[n]$ is given by $\binom{n}{k} \cdot k! = \frac{n!}{(n-k)!}$.*

Proof. 作为第8.2.4节中的练习3留给读者 □

Repetition

在继续计数扑克牌手之前，实际上，我们应该指出，在本节中我们看到的所有标准计数公式只考虑了不允许对象为 *repeated* 的程序。也就是说，当我们从一副牌中抽取五张牌时，我们不能有两张 $A\clubsuit$，例如。有些情况下，我们希望允许对象被多次选择。回顾一下上一节中的车牌号码示例。我们允许重复任何数字/字母；例如，111AAA 是一个有效的车牌号码。这里我们再看一个例子：

Example 8.2.19. 考虑一枚标准、公平的正面和反面都有的硬币。连续抛掷硬币6次，并记录每次的结果，每次结果为 H 或 T。

Question: 有多少可能的结果序列?

要回答这个问题，我们注意到每次翻转都有2种可能的结果，无论之前的翻转结果如何。因此，乘法原理适用，我们可以说有$2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$种可能的翻转序列。

这个想法与选择和排列（当然，除了使用乘法法则之外）相关的原因是，我们还可以将这些序列表示为从集合 $\{H, T\}$ 中选取4个对象的排列，其中对象可以重复出现。（$\{H, T\}$ 与 [2] 之间存在自然对应关系，因此这就像我们在 [2] 中排列4个对象，其中对象可以重复出现。）

这个一般概念由以下定义传达：{v*}

Definition 8.2.20. *Let $k, n \in \mathbb{N}$. A* **k-arrangement with repetition** *from $[n]$ is a k-tuple of elements from $[n]$ where elements are allowed to appear more than once.*

注意，因为允许元素出现多次，所以有 *no restriction* 在 k 上。在此之前，如果没有重复的 k 排列，从8个对象中选择10个对象是没有意义的！然而，这里允许这样做，因此 k 和 n 可以是 *any* 个自然数。

Proposition 8.2.21. *Let $k, n \in \mathbb{N}$. The number of k-arrangements with repetition from $[n]$ is given by n^k.*

Proof. 作为第8.2.4节中的练习4留给读者。 □

您可能预计会有一个与重复排列类似的定义和命题，用于 *k-selections*，我们将讨论这些内容在8.5节中，但用于计算这些内容的技巧比我们现在所用的更高级，所以我们将稍后讨论。

Summarizing Counting Formulas

让我们总结一下到目前为止我们定义和推导出的标准计数对象和公式：假设我们有 n 个对象，并想要从中选择 k 个。我们有多少种方法可以做到这一点？答案取决于 *two questions:*。

- 允许重复吗?
- 是否顺序区分了结果?

每个这些问题都可以用 Yes 或 No 来回答，并且回答它们的四种方式会产生原始问题的不同表述。

		Repeats? Yes	Repeats? No
Order Matters?	Yes	n^k	$\frac{n!}{(n-k)!}$
	No	???	$\binom{n}{k}$

(注意：有时，在问题中n和k的角色会颠倒。请注意这一点！我们将尽量遵守这些约定，但一般来说，字母并不重要；重要的是它们*represent*.)

Combinatorics Definitions in terms of Functions

记住，这些计数思想在*functions*方面也有等效的表达形式，记住这一点很有帮助。也许用函数来表示问题会帮助我们解决问题。至少，通过思考和确保你理解例如*permutations*和*bijections*之间的关系是一种很好的心理锻炼。我们将只陈述这些公式（以及一些相应的公式），并要求你自己思考。试图弄清楚这些概念是如何和为什么相关的；试图向只了解其中一种解释的朋友解释它们；与你的同学合作，也许可以提出不同的公式！

- 一个 **permutation** 的 n 元素是双射 $f : [n] \to [n]$。
  存在从集合 $[n]$ 到自身的 $n!$ 个可能的双射。

- 一个从 n 个元素中选取 k 个元素的 **arrangement** 是一个注入 $f : [k] \to [n]$。从 $[k]$ 到 $[n]$ 有 $\frac{n!}{(n-k)!}$ 个注入。

- 一个从 n 个元素中选取 k 个元素的 **arrangement with repetition** 是一个函数 $f : [k] \to [n]$。

  存在从 $[k]$ 到 $[n]$ 的 n^k 个可能函数。

8.2.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) **selection** 和 **arrangement** 之间的区别是什么?

(2) 如何用选择和排列来定义一个 **permutation**?

(3) 什么是 $\binom{10}{15}$?

(4) 排列与**bijection**这一概念有何关联?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 代数验证 $\binom{n}{k} = \binom{n}{n-k}$。

(2) 证明命题8.2.16，即证明

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

通过调整我们用于计算标准牌组中5张牌手牌数量的论点来完成此操作。

(3) 证明命题8.2.18。也就是说，证明存在

$$\frac{n!}{(n-k)!}$$

可能的 {v*} 排列从 $[n]$。

(4) 证明命题8.2.21。也就是说，证明存在

$$n^k$$

可能的重复 k 从 $[n]$ 的排列。

8.3 Counting Arguments

现在我们完全准备好解决本章的激励性问题了！我们将使用我们开发的计数技术——乘法规则和加法规则——以及选择和排列的公式。重要的是，我们将向您展示一些标准的计数论证和证明策略。在过程中，我们将指出一些一般性指南和证明技术，并通过几个例子来激励和实施这些技术。这些就是我们期望你在未来使用的类型的技术。

8.3.1 Poker Hands

Example 8.3.1. **One Pair**

让我们从排名底部开始计数，对应于 *one pair* 的扑克手牌数量。我们强调，我们只想计数包含 *exactly* 一对的手牌，并排除两对、三张同花和葫芦以及四张同花。这个想法很快就会在我们的计数论证中显现出来。（这也暗示了为什么计数“高牌”手牌实际上相当困难，远比只是选择五张随机牌要复杂得多！我们如何保证手牌有 *no* 匹配的牌，不是顺子，也不是同花？我们将在本节稍后解答这个问题。）

在这个例子中——以及我们在这里将解释的每一个其他例子，以及你将完成的每一个其他练习（你有没有感觉到这很重要？）——我们寻求一个 *process*，其中我们 *construct* 一个具有所需属性的对象（在这个案例中，是一副扑克牌手牌）（在这个案例中，恰好有一对牌且没有其他匹配的牌）。通过计算过程中每一步的选择数量，并确保每个所需的对象只能通过过程中的一组选择获得，我们可以应用乘法原理并确定具有所需属性的对象数量！

这里有一个有用的策略来想出这些过程：假装你的朋友手里拿着你正在数的一个物体，但你看不见它。你会问什么问题来识别他/她手中的特定属性？这些问题可以是是/否问题，或者更常见的是，询问物体具有的特定属性。在我们的特定情况下，计算一对手牌，我们可能会问以下问题：（1）“这对牌里有两张是什么？”和（2）“不在对里的三张牌是什么？”有了这些问题的答案，我们就可以完全指定朋友手中的牌。不幸的是，按照这种方式提出这些问题，很难计算答案的数量。我们应该更加具体地

将我们的问题分解成更小的部分。这样，我们可以计算每个问题的答案数量，并使用这些数字在乘法法则中。

我们如何更具体？如何将问题一分解成几个部分？想象一下我们的朋友可能会对问题一给出的答案类型。我们可能会听到像“红桃A和黑桃A”或“方片7和梅花7”这样的答案。这表明了问题一的答案的重要属性：我们需要知道一对牌的$rank$（它们都是A吗？K吗？Q吗？等等）以及所代表的$two\ suits$。我们知道牌堆中有13个花色和4个花型。有了这些信息，我们可以确定如何$construct$一对牌并计算选项数量。

1. 选择对牌中两张牌的等级：13种选项
2. 选择这些牌的两种花色：$\binom{4}{2} = 6$种选择

请注意，我们使用了二项式系数 $\binom{4}{2}$ 来表示从4种花色中选择2种花色，因此有 $\binom{4}{2}$ 种方法来做这件事。

注意：$\binom{4}{2}$是一个数字。它代表要做的$ways$的数量，并且not实际上对应于执行该动作。也就是说，我们不会说些愚蠢的话，比如“$\binom{4}{2}$从4种花色的牌组中选出2种花色。”一个数字怎么能从一副牌中选出牌呢？

也请注意：在这种情况下，我们为了说明的目的写下了 $\binom{4}{2} = 6$，但一般来说，我们期望（甚至可能必须）您评估二项式系数。算术运算往往涉及非常大的数字，坦白说，数字 $\binom{4}{2}$ 比起 6 来更具说明性。它向读者表明，您在这个过程中这一步涉及从包含 4 个元素的集合中选择 2 个元素，而 6 可能代表 $\binom{6}{1}$ 或 $2 \cdot \binom{3}{2}$ 等等。有了这个观察，我们不妨在第一步就写下数字 $\binom{13}{1}$，对吧？

现在，我们观察到在这些步骤中做出的任何选择都会产生一个 $unique$ 对。也就是说，我们不可能有一个可能由这个过程的两个不同版本产生的对。因此，乘法原理适用，我们可以得出结论，有 $\binom{13}{1} \cdot \binom{4}{2}$ 种选择一对卡片的方法。

如果我们以相反的顺序执行这两个步骤会怎样？我们可以通过询问哪两种花色被代表以及$then$询问它们的共同点数来识别一对牌吗？（当然，这只有在事先知道牌有共同点数的情况下才有效。）在这种情况下，乘积法则会告诉我们有$\binom{4}{2} \cdot \binom{13}{1}$这样的对。嘿，这是同一个数字！实数乘法的交换律（即，$x \cdot y = y \cdot x$对于任何$x, y \in \mathbb{R}$）证实了我们的直觉，即这些步骤是可逆的。

我们还没有完全构建好一对$poker\ hand$。我们需要再选择三张牌。它们应该有什么属性？除了“它们是什么？”之外，我们还能向朋友提出什么更具体的问题？我们需要知道这三张牌的$ranks$和它们的$suits$。它们的花色有约束吗？没有！（因为我们已经有一对，所以不可能出现同花顺。）它们的等级有约束吗？是的！我们知道这三张牌的等级都不同，并且它们都不匹配已经选定的对子的等级。有了这些观察，我们可以反转这个过程，$construct$剩余的手牌。

1. 从剩余的12个等级中选择3个等级（即不与对子牌相同的等级）：$\binom{12}{3}$种选择 2. 将这3个等级按升序排列：1种选择 3. 选择最低等级牌的花色：$\binom{4}{1}$种选择 4. 选择中间等级牌的花色：$\binom{4}{1}$种选择 5. 选择最高等级牌的花色：$\binom{4}{1}$种选择

为什么我们需要第二步？回顾一下 $selection$ 的定义；它是一个 $unordered$ 列表，或者一个 set。因此，通过说“为那些选中的第一张牌选择一副牌”来跳到第二步是没有意义的，因为，嗯，没有 $1st$ 牌！我们需要在卡片上 $impose$ 一种排序，以便单独引用它们。你可能想按照我们从牌堆中移除它们的顺序来排序。这将把第一步分解为 3 个子步骤：(a) 选择第一张牌：$\binom{12}{1}$ 选项；(b) 选择第二张牌：$\binom{11}{1}$ 选项；(c) 选择第三张牌：$\binom{10}{1}$ 选项。将乘法原理应用于这一步会产生比第一步更多的 $different$ 数。

$$\binom{12}{1}\cdot\binom{11}{1}\cdot\binom{10}{1}=12\cdot 11\cdot 10\neq\binom{12}{3}=\frac{12!}{3!\cdot 9!}=\frac{12\cdot 11\cdot 10}{6}$$

这是因为(a)-(b)-(c)步骤对这三张牌的顺序进行了规定，但这在我们扑克手中的实际顺序并不重要。在玩牌时，你不在乎how你收到牌的顺序，只在乎它们是什么！（然而，请注意，如果我们“除以”3张牌的排列方式的数量，即3!，我们会得到相同的数字。这暗示了一个有趣的概念，一种“逆”乘法法则的概念。我们将在本节末尾讨论这一点。）这就是为什么我们无法在步骤2中提到“第一张牌”的原因。相反，我们找到了一种$inherent$的牌序，这是一种它们所具有的特定属性，使我们能够在不应用外部排序的情况下引用它们中的特定牌。

再次，乘法规则适用，因为从不同花色的3张牌的选择只能来自这些步骤中做出的一个选择集。此外，我们可以将选择一对作为第一步，选择三张不同花色的其他牌作为第二步，并将乘法规则应用于此 $entire$ 过程。这最终给出了“一对”扑克牌手牌数量的答案：

$$\binom{13}{1}\cdot\binom{4}{2}\cdot\binom{12}{3}\cdot\binom{4}{1}^3$$

注意，我们将上面最后几步中的三个数字合并成了一个系数的三次方。现在，这种数值答案是 $totally\ \ acceptable$，比仅仅写下 1, 098, 240 要好得多。如果你在作业中犯了一个“错误”或者计算器出错，我们如何识别错误并提供评论？☺

我们之前已经注意到乘法的交换律以及以不同顺序进行步骤的想法。然而，我们希望你会同意解释像{v*} 这样的乘积

$$\binom{4}{1}^3 \cdot \binom{13}{1} \cdot \binom{12}{3} \cdot \binom{4}{2}$$

尽管它代表的是相同的过程，但结构要复杂得多，而且是不必要的。

我们选择在上一个子节中特别详细地解释。我们不会期望你写很多*nearly*。我们只是正式介绍了一种应用我们在上一节中开发计数规则和公式的正式方法，同时提到了一些启发式规则和策略来解决问题。所以，有了这些话，让我们以更简洁的形式提出这个问题的典型解决方案。这是我们期望你写出的解决方案类型：

Question: 有多少5张牌的扑克手牌是“一对”手牌?

Answer: 我们声称存在

$$\binom{13}{1} \cdot \binom{4}{2} \cdot \binom{12}{3} \cdot \binom{4}{1}^3$$

这样的手。为了展示这一点，我们将识别一个四步过程并应用ROP。此过程的成果是一个“一对”扑克手牌：

(1) 选择一个等级来构成一对。有 $\binom{13}{1}$ 种方法来做这件事。(2) 选择在(1)中出现的两张牌的花色。有 $\binom{4}{2}$ 种方法来做这件事。(3) 选择三个 *other* 等级出现。有 $\binom{12}{1}$ 种方法来做这件事。(4) 对于在(3)中选择的每个等级，选择该牌的花色出现在手中。有 $\binom{4}{1}$ 种方法来做这件事，每个三次；因此，总共有 $\binom{4}{1}^3$ 种方法。

应用ROP，我们发现上述答案。 □

这有什么意义吗？注意它比我们上面的解释要短得多。这很好！我们有时会继续在这里的书面例子中写出一些细节（帮助你了解如何*approach*这些问题，然后再把它们写出来），但你的书面解答可以稍微简略一些，只要它们能识别出问题解决方案的所有关键要素。注意，我们指出了ROP的一个用法，引用了它，并确定了过程中的所有步骤；对于每一步，我们注意到了完成这一步有多少种方法。恰好这些步骤都很简单，并且

每种执行方式在每个情况下都很清楚。一般来说，我们可能会期望一个更详细的描述。例如，我们会考虑写步骤（3）的执行方式有$\binom{12}{1}$，因为我们不允许重新选择步骤（1）中选择的排名。然而，我们认为这一点从描述中已经很清楚了，所以我们省略了它。这是一个判断问题，尽管如此，我们（一如既往地）建议留出你的证明，并像没有写一样重新阅读它们。如果你记不起，或者并不完全确定为什么某事是正确的，考虑在那里添加一些额外的描述。

在再举一个例子之前，让我们指出这个相同问题的另一个 $different$ 解决方案!

$Question:$ 有多少5张牌的扑克手牌是“一对”手牌?

$Answer:$ 我们声称存在

$$\binom{13}{4}\binom{4}{1}\binom{4}{2}\binom{4}{1}^3$$

“一对”扑克牌型。我们将确定一个六步流程并应用ROP。主要思想是可以通过选择所有出现的四个花色并确定哪个花色重复两次（其余花色只出现一次）来识别一对牌型。

(1) 选择将出现在我们手中的4个等级。

有 $\binom{13}{4}$ 种方法来做这件事。

(2) 在步骤（1）中选出的4个花色中，选择其中一个。该花色的两张牌将出现在我们的手中。

有 $\binom{4}{1}$ 种方法来做这件事。

(3) 在步骤(2)中选择的那个等级，选择2个花色。这些将出现在我们的手中。有$\binom{4}{2}$种方法可以做到这一点。

(4) 对于在步骤(2)中选择的3个等级中的最低等级 not，选择一个花色。

有 $\binom{4}{1}$ 种方法来做这件事。

(5) 对于步骤(2)中选择的3个等级的中间 not，选择一个花色。

有 $\binom{4}{1}$ 种方法来做这件事。（6）在步骤（2）中选择的3个等级中的最高等级 not，选择一个花色。有 $\binom{4}{1}$ 种方法来做这件事。

通过ROP，并简化 $\binom{4}{1}\binom{4}{1}\binom{4}{1} = \binom{4}{1}^3$，我们已经证明了上述表达式是正确的。

□

这不是很整洁吗？我们将留给你来验证

$$\binom{13}{4}\binom{4}{1}\binom{4}{2}\binom{4}{1}^3 = 1098240 = \binom{13}{1}\binom{4}{2}\binom{12}{3}\binom{4}{1}^3$$

是正确的，从数值上来说。尽管如此，如果不计算中间的那个数字，我们就可以确定，左右两个表达式是绝对相同的$equal$表示，因为它们计算的是$same$：一对扑克牌手牌的数量。这是我们在构建的“两种方式计数”想法的另一个例子。

Example 8.3.2. **Flush**

让我们直接跳到另一个问题并解决它。让我们计算扑克牌中顺子的数量。顺子手牌由两个特性定义：所有5张牌共有的$suit$，以及这些牌的5个花色。因此，顺子可以通过两步过程生成：

(1) 从手中的五张牌中选择一套。有 $\binom{4}{1}$ 种方法可以这样做。(2) 从该套中选择五张牌出现在手中。有 $\binom{13}{5}$ 种方法可以这样做。

由于每手洗牌都是由这两个步骤唯一确定的，我们可以应用ROP并得出结论，存在

$$\binom{4}{1} \cdot \binom{13}{5} = 5148$$

扑克牌中的顺子

这个例子中给出的证明（除了最后的数字5148，我们只在这里为了与“一对”答案进行比较，该答案比 $much$ 大），是完全正确和严谨的，并且会得到满分。将其用作使用乘法法则的简单计数问题的范例。

Example 8.3.3. **Straight**

牌的顺序在顺子中由“起始牌面”，即手中的最低牌唯一确定。如果我告诉你我有一手以7开始的5张顺子，你就会立刻知道我有一手789TJ顺子。由于我们可以有像A2345这样的顺子，或者像23456这样的顺子，... 一直到TJQKA（注意：顺子中没有“绕弯”的情况，如QKA23），这意味着我们在顺子中有10种可能的$lowest\ ranks$。因此，有十种顺子类型，在确定我们拥有的类型后，我们只需要分配花色，确保它们不是全部相同（在这种情况下，我们会有同花顺）。

我们声称存在

$$\binom{10}{1}\left[\binom{4}{1}^5 - \binom{4}{1}\right] = 10 \cdot (4^5 - 4)$$

5 张顺子牌手

Proof. 我们将通过两步过程描述5张牌的手牌，这些手牌是顺子：

1. 从10个等级中选择一个作为直线上的 *lowest* 等级。这些选项是 A,2,3,4,5,6,7,8,9,T，因此这一步有 **10 options** 个选项。

   注意：这是 *determines* 手中的其他 4 个等级，因为 5 个等级必须是连续的，而且我们知道最低的是哪一个。

2. 将花色分配给5张牌，以确保它们不是*all*同一花色。

   假设 X 是以这种方式分配花色的所有可能方式的集合，因此在这一步有 $|X|$ 种选择。

我们现在将通过建立一个划分来找到 $|X|$。设 Y 为所有分配 5 种花色的分配集合，使得它们 *are* 都相同。注意，集合 X 和 Y 构成了 U 的划分，即所有可能的 5 种花色的分配集合。（也就是说，任何 5 种花色的分配要么选择所有相同的花色，要么不选择。）因此，根据 ROS，我们有 $|U| = |X| + |Y|$。

我们可以通过5个步骤找到$|U|$，其中在第i步，我们从手中的i最高牌中选择4种花色之一。在每一步都有4个选项，因此我们有$|U| = 4^5$。

我们可以通过注意到任何这样的选择都相当于从4种花色中选择一种，并将该花色分配给手中的5张牌来找到$|Y|$。因此，$|Y| = 4$。

相应地，我们可以重新排列上述等式并写出

$$|X| = |U| - |Y| = 4^5 - 4$$

由于 $|X|$ 是上述步骤（2）中的选项数量，通过ROP，我们已经证明了该主张。

□

Note: 在这个证明中，我们提出了所有相关步骤来证明有$10 \cdot 4 = 40$种可能的 *straight flushes* (同花顺)，其中只有$1 \cdot 4 = 4$是 *royal straight flushes* (同花TJQKA)。试着为自己写出这些论据!

8.3.2 Other Card-Counting Examples

让我们看看一些相关示例，以拓宽我们应用的技术类别。

Example 8.3.4. **At least 3 Aces**

对于这个例子，让我们计算至少有三张A的扑克牌手牌的数量。再次，让我们应用上面使用的技术，并考虑这种手牌的必要*properties*。试着自己提出几个问题，目标是答案确定一个*unique*手牌，并且对于任何答案，我们都可以精确地计算出构造出该答案的手牌方式数量。

你注意到困难了吗？对问题 *directly affects* 其他问题的性质的回答之一！这表明存在一些更深层次的数学问题。也许让那个决定性问题先出现是有意义的，然后考虑从那里必须做出的决定。

首先，如果手中恰好有3个A，那么我们需要确定其他两张牌的特征。这两张牌要么是（a）相同的点数，要么是（b）两个不同的点数。因此，对于这种情况有两个子情况。这导致以下程序：

1. 为3个A选择3种花色：$\binom{4}{3}$种选择

   (a) 剩下的两张牌花色不同：

      i. 从剩余的12张牌中选择2张牌：$\binom{12}{2}$

      选项 ii. 选择第2步中选择的最低等级的牌的花色：$\binom{4}{1}$

      选项 iii. 选择第2步中选择的最高等级的牌的套装：$\binom{4}{1}$

      选项

   (b) 剩下的两张牌是同一等级的：

      i. 从12个非王牌花色中选择1个等级：$\binom{12}{1}$种选择 ii. 为此等级选择2个花色：$\binom{4}{2}$种选择

然后，根据乘法规则 and 求和（因为我们在一个过程中有单独的情况），我们发现存在

$$\binom{4}{3}\left[\binom{12}{2}\binom{4}{1}^2+\binom{12}{1}\binom{4}{2}\right]$$

手与$exactly\ 3\ Aces$。

其次，如果手中恰好有4张A，我们需要确定手中第五张牌的特征。这产生了以下步骤

1. 选择4个花色的4个A：$\binom{4}{4}$种选择

2. 从剩余的12个中选择1个等级作为另一张牌：$\binom{12}{1}$个选项

3. 选择第2步中选定的牌的花色：$\binom{4}{1}$种选项

我们可以应用乘法法则并得出结论，然后有 $\binom{4}{4}\binom{12}{1}\binom{4}{1}$ 张手牌，每张手牌有 $exactly\ 4\ Aces$。现在，我们必须应用加法法则！我们这里有一个 $partition$ 的集合，即至少有三张A的手牌，分为两个子集——恰好有三张A的手牌和恰好有四张A的手牌。由于这些子集将更大的集合分割开来（即，每张至少有三张A的手牌要么有三张A，要么有四张A，不可能两者都有或两者都没有），我们可以应用加法法则并得出结论，有

$$\binom{4}{3}\left[\binom{12}{2}\binom{4}{1}^2+\binom{12}{1}\binom{4}{2}\right]+\binom{4}{4}\binom{12}{1}\binom{4}{1}$$

扑克牌手牌至少有三张A

回忆一下，求和法则的严谨表述涉及有限集合的基数，然而在前一个例子中，我们实际上并没有详细探讨这些细节。这些类型的组合论证需要一定程度的自由裁量权和技巧。对于 *every poker hand with at least three Aces has either exactly three or exactly four Aces, not both and not neither* 是否显而易见，对你来说明显吗？我们并不是说它应该完全显而易见，你因为没立刻看出而显得愚蠢！远非如此！我们想说的是，这种类型的陈述可能足以作为证明中的解释。是的，我们可以进一步深入细节，用集合术语重新表述扑克牌手，并将扑克游戏完全用集合符号严格化。但这真的有什么好处吗？通过上面的斜体陈述来解释似乎更容易。如果被困惑的读者追问细节，我们可以提供进一步的解释，但对于一般受众来说，这种论证就足够了。希望这个经验法则——说服一般受众，但在被进一步追问时能够进一步解释——能指导你决定在计数论证中包含多少细节。这里的基本观察是，我们指出 *why* 我们的选择与所讨论的手牌集合的划分有关。不，我们没有严格证明这两个集合是互斥的，但我们解释了为什么。

另一种解决这个问题的方法涉及考虑非王牌牌的花色。相反，我们可以按照以下步骤构建至少包含3个王牌的扑克手牌：

1. 如果恰好有3个A：

   (a) 为3个A选择3个花色：$\binom{4}{3}$种选择 (b) 从剩余的48张非A牌中选出2张以“填满”5张牌的手牌：$\binom{48}{2}$

2. 如果恰好有4个A：

   (a) 从4个A中选择4个花色：$\binom{4}{4} = 1$种选择 (b) 从剩余的48张非A牌中，选择1张来“填满”5张牌的手牌：$\binom{48}{1}$

因此，根据求和法则（因为我们已经根据手牌中的A的数量对手牌进行了划分）以及在每个两种情况下的乘法法则，我们有

$$\binom{4}{3}\binom{48}{2} + \binom{4}{4}\binom{48}{1}$$

总共有至少3个A的扑克牌手。您将更频繁地看到（并使用）这种方法。之前的论点与涉及同花牌的先前的例子更相似，所以我们首先展示了这一点。这个论点稍微短一些，也更“巧妙”，因此更常用。但是等等，这些答案看起来不同！我们在计算相同的扑克牌手集合，所以

我们不应该期望相同的 *final number* 吗？嗯，是的，我们建议您进行必要的代数操作，以使您自己相信

$$\binom{4}{3}\binom{48}{2}+\binom{48}{1}=\binom{4}{3}\left[\binom{12}{2}\binom{4}{1}^2+\binom{12}{1}\binom{4}{2}\right]+\binom{4}{4}\binom{12}{1}\binom{4}{1}$$

只需一分钟，值得。

在继续探讨另一个问题之前，让我们先看看关于这个问题的 *false argument* 。查看错误答案可能看起来很奇怪，但根据经验，尝试 *find the flaw* 一个有缺陷的论点可能非常有帮助和具有教育意义。当然，我们完全可以比较两个大整数，然后说，“嘿，看，它们是不同的！”但这并不具有启发性。相反，我们希望遵循组合论论证，并找出导致逻辑错误或以错误方式改变我们计数对象集合的步骤。我们强烈推荐这种方法，原因有几个。首先，它可以帮助你练习阅读证明和理解他人的论证。当你学习更多数学并阅读其他可能不会以完全相同方式解释事物的书籍时，这将对你有所帮助。其次，它有助于你成为自己证明的更好编辑。在写完一个作业问题后，把它放一边半小时，然后用全新的心态回到它。就像你没有写它一样（尽可能做到，我们理解你不可能假装你没有做！）它有道理吗？是否有某些步骤在你写的时候看起来很显然，但现在你却忘记了细节？答案甚至正确吗？你被它说服了吗？第三，认识到在证明中何时出现错误步骤，可以巩固你对论证基本原理的理解。通过组合论论证并识别错误，将真正有助于你的直觉和对求和规则与乘积规则的理解。相信我们。

你对这个论点有什么看法？记住，这个答案是 *incorrect*，我们想知道为什么！

Example 8.3.5. **Find the Flaw!** 至少有三张A的5张扑克牌手有多少种？

1. 对于有三张A的手牌：
   (a) Choose 3 of the 4 Aces: $\binom{4}{3}$ options
   (b) From the remaining 49 cards, choose 2 more: $\binom{49}{2}$ options
2. 对于有四个A的手牌：
   (a) Choose 4 of the 4 Aces: $\binom{4}{4}=1$ option
   (b) From the remainign 48 cards, choose 1 more: $\binom{48}{1}$ options

因此，有

$$\binom{4}{3}\binom{49}{2}+\binom{4}{4}\binom{48}{1}$$

扑克牌手牌至少有3个A

这里有什么问题？你看到任何错误吗？产品法则是否被不适当地应用？求和法则是否被应用于实际上不是划分的东西？我们是否多算了？少算了？我们是否计算了一些不具有所需属性的手牌？在继续阅读之前，请考虑这些问题。

这里是我们注意到的：这个答案是 *too large*。我们通过在计数中多次包含某些手来 *overcounted*。也就是说，我们试图计数的每一手都至少通过上述步骤被包括一次，但某些手可以通过那些步骤在 *multiple ways* 中构建。这些观察结果保证了我们的数字太大。

我们是如何知道这个的？我们建议积极尝试通过以上步骤识别可以以不同方式构建的手牌。如果你正在阅读一个证明并且能够做到这一点，你就知道整个证明现在是有缺陷的。在这种情况下，让我们考察一个恰好有4个A的手牌；具体来说，让我们看看手牌$A\clubsuit A\spadesuit A\diamondsuit A\heartsuit 2\clubsuit$。我们可以通过以下步骤通过以下路径构建这个手牌：

1. 从4个A中选择3个：$A\clubsuit A\spadesuit A\diamondsuit$
2. 从剩余的49张牌中再选择2张：$A\heartsuit 2\clubsuit$

或者，我们可以选择这条路径：

1. 从4张A中选择4张：$A\clubsuit A\spadesuit A\diamondsuit A\heartsuit$ 2. 从剩余的48张牌中再选择1张：$2\clubsuit$

你现在看到问题了吗？通过上述过程，这只手以（至少）两种不同的方式被生产出来。因此，答案是过度计数。我们还有其他方法可以构建出同样的手吗？有多少种？尝试识别另一种被过度计数的手。我们能否可能确定每种手被过度计数的次数，并以此方式修正我们的答案？这是一个有趣（实际上非常具有挑战性！）的想法，我们稍后会回到这个话题。

Potential Flaws in Arguments

目前，我们想强调阅读组合证明的技术以及寻找一些标准缺陷的方法：

- **Misuse of Rule of Product**:
  证明错误地将乘法规则应用于不需要这种情况。也许在程序的每一步中，选项的数量以某种方式改变，这取决于前一步的完成情况。或者，也许不同的步骤序列会产生相同的结果。

- **Misuse of Rule of Sum**:
  证明错误地将求和规则应用于不需要这种情况。或许“划分”的集合实际上并不是不相交的。

或者，也许“划分”的集合的并集实际上并没有覆盖整个所讨论的集合。

- **Overcount**:
  每个所需的对象至少被计数一次，但有些对象被计数多次。也就是说，在证明步骤中，某些集合的元素可以通过多种方式被计数。

- **Undercount**:
  一些期望的对象根本未被计算。也就是说，所讨论的集合中的某些元素没有被证明的步骤所计算。

- **Extraneous Count**:
  一些不希望的对象被计算在内。也就是说，证明的步骤计算了不属于所讨论集合的一些对象。

我们建议仔细阅读你的手写证明，并尝试识别这些缺陷，即使它们可能不存在。或许通过 *struggling* 来找到一个过度计数论证，比如说——通过尝试以多种方式通过你的步骤构建某些对象——你实际上发现了一个你不知道存在的缺陷！如果你没有发现任何缺陷，你可以更有信心地认为你的证明是完全正确的。

Example 8.3.6. 这是一个标准的朴素 **overcount** 的例子。我们将展示它是一个过度计数，然后通过不同的计数方式来修复它！问题是：

至少每种花色都有一张牌的5张牌手有多少种?

这里是一个 **incorrect** 论点：

> 有 $\binom{13}{1}^4 \cdot \binom{48}{1} = 1370928$ 种这样的手。我们可以使用一个五步过程。在第1步中，我们从13张红心中选择一张。在第2步中，我们从13张方块中选择一张。在第3步中，我们从13张黑桃中选择一张。在第4步中，我们从13张梅花中选择一张。完成这些步骤的每种方法有 $\binom{13}{1}$ 种。接下来，从剩余的48张牌中，我们选择一张来完成我们的5张牌手。根据ROP，上述说法成立。

有什么问题吗？在继续阅读之前仔细想想。看看上面的潜在错误列表；其中之一适用于这里吗？你会如何展示这个?

我们认为这是一个 **overcount**。为了证明这一点，我们将展示一个特定的5张牌手牌，该手牌应该只计算一次，但实际上按照上述论点中概述的程序被计算了 *at least twice*。

考虑手 $A\heartsuit, A\diamondsuit, A\spadesuit, A\clubsuit, K\heartsuit$。注意，可以通过上述程序以两种方式实现此手：

(1) 步骤 1：选择 $A\heartsuit$。步骤 2：选择 $A\diamondsuit$。步骤 3：选择 $A\spadesuit$。步骤 4：选择 $A\clubsuit$。步骤 5：选择 $K\heartsuit$。 (2) 步骤 1：选择 $K\heartsuit$。步骤 2：选择 $A\diamondsuit$。步骤 3：选择 $A\spadesuit$。步骤 4：选择 $A\clubsuit$。步骤 5：选择 $A\heartsuit$。

由于一只手是 *unordered*，这两个程序产生 *same outcome*。然而，上述论点会将这两个结果分别计算。因此，这个论点是过度计算的。

要修复这个论点，让我们更仔细地思考每种花色中必须出现的 **how many**。有5张牌可供选择，只有4种花色，我们发现要求每种花色至少出现一次意味着我们有三种花色各出现一次，一种花色出现两次。这就是 *only* 这种情况可能发生的方式。换一种说法，花色的 *distribution* 必须看起来像（1, 1, 1, 2）。

为了计算此类手牌的数量，我们确定一个过程：

- 选择四个花色中哪两个会各出现两次。（其他三个花色各出现一次。）有 $\binom{4}{1}$ 种方法可以这样做。
- 从那副牌中选出两张牌。有 $\binom{13}{2}$ 种方法可以这样做。
- 从其他三副牌中各选一张牌。共有 $\binom{13}{1}^3$ 种方法。

通过ROP，我们发现存在

$$\binom{4}{1}\binom{13}{2}\binom{13}{1}^3 = 685464$$

许多包含每种花色至少一张牌的5张牌手牌。

Example 8.3.7. **At most 2 Aces**

现在让我们提出一个类似的问题。有多少5张牌的扑克手牌中有*at most* 2个A? 在继续阅读之前，先自己尝试几分钟。如果你有困难，试着用我们上一个问题中提出的类似论据来思考。这两个问题有哪些相似之处和不同之处?

这里是我们处理这个问题的方法：

1. 对于恰好有2个A的手牌：
   (a) Select 2 of the 4 Aces: $\binom{4}{2}$ options
   (b) From the 48 remaining non-Aces, select 3: $\binom{48}{3}$ options
2. 对于恰好有1个A的手牌：

(a) 选择4张A中的一张：$\binom{4}{1}$ 选项

(b) 从剩余的48张非A牌中选出4张：$\binom{48}{4}$选项

3. 对于恰好有0个A的手牌：

(a) Select 0 of the 4 Aces: $\binom{4}{0} = 1$ options

(b) From the 48 remaining non-Aces, select 5: $\binom{48}{5}$ options

由于1、2和3个案例不重叠（即一副扑克牌有特定数量的A），我们可以应用求和规则；此外，由于我们在每个案例中连续执行两个步骤，因此我们还可以在每个案例中应用乘法规则。因此，有

$$\binom{4}{2}\binom{48}{3} + \binom{4}{1}\binom{48}{4} + \binom{48}{5}$$

(注意：在二项式系数之间省略 · 乘号是常见的；乘法是隐含的.)

你记得要计算没有Aces的手牌吗？忘记这种情况是一个常见的错误！你也避免了我们在上一个问题中看到的多计算论点吗？我们需要通过识别三个不重叠的情况来划分所讨论的手牌集合，具体取决于手牌中有多少个Aces。

另一种完全合理的解决方法是利用我们在前一个例子中已经完成的工作。也许你已经想到了这种方法？如果是这样，恭喜你的聪明才智！主要思想是将all扑克牌手牌集分为两个不同的案例。每个扑克牌手牌必须要么最多有2个Aor，要么至少有3个A。对吧？让我们让S表示所有最多有2个A的扑克牌手牌集，T表示至少有3个A的扑克牌手牌集，H表示所有扑克牌手牌集。我们的解释说$H = S \cup T$和$S \cap T = \varnothing$。因此，可以应用求和规则来推断$|H| = |S| + |T|$。此外，由于我们需要识别$|S|$，我们可以将其写成

$$|S| = |H| - |T|$$

因此

$$|S| = \binom{52}{5} - \left(\binom{4}{3}\binom{49}{2} + \binom{4}{4}\binom{48}{1}\right)$$

我们能够写下这个解，而无需计算其他任何东西！我们需要的只是将它们分成两个集合，其基数已经是 $known$。

这个策略表明了一个更深层次的原则在起作用。本质上，我们应用了“减法规则”来找到我们关心的答案。这相当于应用了“加法规则”，正如之前所述，然后从那里操纵表达式。确实，这是“正确”思考它的方式，从意义上说，这是应用基本数学原理的方式。然而，在数学证明中，更直接地应用“减法规则”是很常见的。证明者可能会假设读者对“加法规则”的复杂运作有一定了解，并“跳”到结论，而没有明确识别分区或

严格解释求和法则的应用。例如，一位高级数学家可能会通过写下以下内容来为这个当前示例提供一个证明：

从所有扑克牌手牌中去除包含三张或四张A的牌，得到

$$\binom{52}{5} - \binom{4}{3}\binom{48}{2} - \binom{48}{1}$$

一位数学家，稍加思考后，会接受这个证明。然而，我们同意你可能的想法：这难道不是太 *short* 了吗？这不会让读者想得太难吗？目前，在你数学生涯的这个阶段，我们强烈建议（并且 **require**）你在这类证明中提供更多 *explicit* 的细节。我们希望你应用求和规则，并指出为什么有 *partition* 的应用基础，然后操纵任何代数表达式以得出结论。以后，在课程之外，你可以根据需要使用“减法规则”。不过，现在，我们希望你能正确掌握基本原理，这就是为什么需要求和规则。

这是最后一个手工计数问题。它涉及求和规则和乘积规则，并需要仔细思考你的步骤

Example 8.3.8. **Exactly 1 Queen and exactly 1 ♠**

有多少副扑克牌手牌恰好有一张皇后和一张黑桃？

尝试一下，自己思考一会儿。想想是否可以向握着这样手的你的朋友提问？有没有哪些问题能决定你的未来提问方向？你会如何反转这些问题并确定一个建设性的过程？

这里是我们建设性的步骤。它与你的相比如何？它是否完全相同？它以某种方式等价吗？我们只是以不同的顺序划分了手牌集合吗？我们得到了相同的最终答案吗？为什么或为什么不呢？认真地说，如果我们步骤或最终答案不同，*not*是否会气馁？坐下来思考我们的答案为什么不同，而不是仅仅阅读我们的正确解决方案，这对您来说将更有教育意义。认真地说。

1. Q♠ 当前：

   (a) 选择黑桃皇后：1种选择 (b) 从剩余的51张非皇后牌（其中3张是皇后）和非黑桃牌（其中12张非皇后是黑桃）中选择4张：$\binom{51-3-12}{4} = \binom{36}{4}$ 或者

2. Q♠不存在：

   (a) 选择一张非黑桃王后：$\binom{3}{1}$ 种选择

(b) 选择一张非王后黑桃牌：$\binom{12}{1}$ 种选择（c）从剩余的50张非王后牌（其中3张是王后）和非黑桃牌（其中11张非王后且未被选择）中，选择3张：$\binom{50-3-11}{3} = \binom{36}{3}$ 种选择

由于每一步的选择都产生独特的结果，因此适用乘法原理；由于具有这些属性的每一手牌要么有 $Q\spadesuit$，要么没有，因此适用加法原理。因此，恰好有一张王和一张黑桃的手牌数量是

$$\binom{36}{4} + \binom{3}{1}\binom{12}{1}\binom{36}{3} = 58,905 + 257,040 = 315,945$$

这是一个比前几个例子更复杂的问题，所以我们鼓励你多次阅读这个证明，直到你完全熟悉它。事实上，你可以问问你的朋友他们是否能解决这个问题，然后通过遵循这个证明的步骤来试图说服他们你的答案。你理解得足够好，可以解释给别人听吗？如果是这样，你就是组合论证的大师！

在下一个小节中，我们寻求进一步发展你对组合论证和证明的舒适度。在这个过程中，我们还将介绍一些标准的组合对象，以便我们可以计算除了扑克牌手以外的其他事物。关于一副牌的计算问题是常见且容易提出的，但我们还想谈谈其他内容！

8.3.3 Other Counting Objects

n-Tuples from $[k]$

一副扑克牌是一组很好的、标准的 *physical* 物体，用于计数。大多数人熟悉它们，并且每张牌都有 *two* 属性——花色和等级——这使得可以提出许多有趣的组合问题。一个更“抽象”的计数标准物体集合的例子涉及具有指定长度的自然数列表。我们将做出以下定义，以便我们可以以简洁的形式引用这些集合。

Definition 8.3.9. *Let $n, k \in \mathbb{N}$ be given. Then*

$$T_{k,n} = [k]^n = \{(a_1, a_2, \ldots, a_n) \mid \forall i.\ a_i \in [k]\}$$

That is, $T_{k,n}$ is the set of all n-tuples whose elements belong to $[k]$.

注意：我们选择字母 T 因为这些对象是 *n-tuples*，即长度为 n 的有序列表。我们还将指出，当 k 是一个小的数字，如 2 或 3 时，通常用 $[k-1] \cup \{0\}$ 替换集合 $[k]$。例如，数学中的 *binary* n-元组概念相当常见，部分原因是它在计算机科学中的普遍性。考虑到这一点，$k = 2$ 的情况通常考虑长度为 n 的有序列表，其元素来自集合 $\{0, 1\}$。

代替 $\{1, 2\}$。由于我们关注这些集合的 $combinatorial$ 方面（即“有多少具有属性 P 的 $many$ 序列？”），实际上我们并不关心选择哪种惯例。实际上，证明这一点是一个简单的练习。

$$|T_{k,n}| = |[k]^n| = k^n = |([k-1] \cup \{0\})^n|$$

通过在底层集合 $[k]$ 和 $[k-1] \cup \{0\}$ 之间建立双射，我们将把这个任务留给你来完成 ☺

许多我们在下一节将要看到的计数论证可以通过识别适当的 k 和 n 以及有序列表必须具有的附加属性，方便地用这个框架表达。现在，让我们研究几个简单的情况，并探讨一些应用。在每种情况下，我们将关注一些子集，$S \subseteq T_{k,n}$，其元素具有某种（或某些）属性；具体来说，我们将通过计数 S 的元素来寻找 $|S|$。我们将首先研究一些非常简单的情况，然后进入一些更具挑战性的情况。本节中的练习将进一步探讨这些想法。

Example 8.3.10. 让 $n = 4$ 和 $k = 3$。

(1) 什么是 $|T_{3,4}|$?

要计算$T_{3,4}$的所有元素，我们可以通过以下四个步骤构建这个集合，其中第i步对应于选择4元组中的第i个元素。在每一步中，我们有3个选项（每个元素是$\{1, 2, 3\}$中的一个），因此乘法原理告诉我们有$3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3$共81个$T_{3,4}$元素。（注意：参见练习，其中要求证明$|T_{n,k}| = n^k$，一般而言。）

(2) $T_{3,4}$中有多少个元素没有1?

要计算 $T_{3,4}$ 中没有 1 的元素数量，我们可以通过限制每一步的选择数量来改变我们的 4 步过程。也就是说，$T_{3,4}$ 中任何没有 1 的元素的 4 个位置中，每个位置只能从集合 $\{2, 3\}$ 中填充。因此，乘法原理表明，有 $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$ 这样多的元素。

(3) 有多少个恰好有一个1? 恰好有两个1? 恰好有三个1? 恰好有四个1?

要计算具有恰好一个1的$T_{3,4}$中的元素数量，我们能否使用上一段提到的相同思路？不完全是这样！在每一步过程中可用的选项数量可能$change$，这取决于是否已经在我们的4元组中放置了一个1。我们必须找到一种新的方法。相反，让我们考虑在4元组中的某个位置放置一个1，然后使用$\{2, 3\}$中的元素填充剩余的位置。也就是说，我们的四个步骤过程来构建一个具有恰好一个1的4元组如下：

(a) 从4个位置中选择一个由1：$\binom{4}{1} = 4$个选项占据。然后，对于剩余的3个未填位置，从左到右读取。

(b) 对于第一个未填空位，从 $\{2,3\}$ 中选择一个元素：2个选项（c） 对于第二个未填空位，从 $\{2,3\}$ 中选择一个元素：2个选项（d） 对于第三个未填空位，从 $\{2,3\}$ 中选择一个元素：2个选项

因此，存在4个 $\cdot\, 2^3 = 32$这样的 $T_{3,4}$ 元素。

也许我们在这次争论中说得有点啰嗦。我们本可以分两步进行，第一步确定1的位置，第二步从$\{2,3\}$中选择每个剩余的3个位置。但这只是语义问题，本质上是对同一事实的相同证明。我们提供这些额外细节是为了确保你们能理解我们的论点并理解其背后的原理。这将帮助你们将这些想法应用到自己的证明中！

我们可以使用类似的论据来计算具有恰好2个1的$T_{3,4}$的元素数量。唯一的不同在于第一步：我们必须从4个位置中选择2个位置来填充1。有$\binom{4}{2}$种方法来做这件事。然后，从$\{2,3\}$中选择两个位置来填充。因此，有

$$\binom{4}{2} \cdot 2^2 = 24$$

此类 $T_{3,4}$ 的元素。

我们将把它留给你来验证，$T_{3,4}$中有8个元素恰好有三个1，以及1个元素恰好有四个1。我们也将把它留给你来验证并解释为什么$16 + 32 + 24 + 8 + 1 = 81$是有意义的。（挑战问题：你能将这个结果推广到任意的 n 和 k 吗？）

Example 8.3.11. 让 $n \geq 3$. 计算具有以下性质的二进制 n-元组的数量：(a) 恰好有三个 1；(b) 至少有三个 1；(c) 1 的个数为偶数。

我们的上下文是所有元素来自基集 $\{0,1\}$ 的 n-元组的集合 $\{0,1\}^n$。请注意，这并不是上面定义的集合 $T_{2,n}$，但我们解释了这些集合在某种意义上是等价的，即我们可以在它们之间找到一个双射。

要回答问题（a），我们采用与上一个例子相同的技术。首先，我们从总共 n 个位置中选择 3 个位置用 1 填充；其次，我们将剩余的 $n-3$ 个位置用 0 填充。完成第一步有 $\binom{n}{3}$ 种方法，从那里开始，第二步是确定的（即只有 1 种方法），因此有 $\binom{n}{3}$ 个二进制 n-元组恰好包含三个 1。（注意：我们只指定了 $n \geq 3$ 来确保我们的答案是零的。如果 $1 \leq n \leq 2$，那么我们当然不能有任何这样的元组！实际上，这“验证了”$\binom{n}{\ell} = 0$ 当且仅当 $\ell > n$。））

为了回答问题（b），我们采用与（a）中相同的技术，但将范围从3推广到任意自然数ℓ。也就是说，我们可以按照以下方式计算恰好有ℓ个1的二进制n-元组数量：从n个位置中选择ℓ个位置填充1，然后剩余的位置填充0。为了至少有3个1，我们必须有恰好3个1，或者恰好4个1，或者...，或者恰好n个1。更严格地说，对于3和n（（含）之间的每个ℓ，令A_ℓ为集合

二进制 n-元组，恰好有 ℓ 个 1。每个至少有三个 1 的二进制 n-元组属于 *exactly* A_ℓ 个集合之一。因此，我们根据恰好有多少个 1 来识别了我们想要计数的元组集合中的一个 *partition*。根据求和规则，我们寻求的数字是

$$\sum_{\ell=3}^{n} |A_\ell| = \sum_{\ell=3}^{n} \binom{n}{\ell}$$

您可能想知道这个答案，用求和符号表示，是否是 *acceptable*。在某种意义上，是的；就在10分钟前，我们还不知道有多少至少有三个1的二进制 n-元组，而现在我们对这个数字有了更好的认识。然而，所提出的解决方案更多的是一种寻找精确数字的 *method*。如果有人在街上走到你面前说，“快！告诉我至少有三个1的二进制 n-元组的数量！”你会怎么做？你会说，“等等，我需要逐个评估每个项并求和 ...” 这并不理想，对吧？如果有一个简单的解决方案形式，那就更方便了；也许我们可以将其写成只有一个二项式系数，或者两个、三个或一些 *small* 个这样的系数的和、差、积或商。这样，无论 n 是什么（即无论它变得有多大），我们都能知道我们总是可以在几个简短的步骤中高效地计算出答案；此外，我们希望知道这些 *number* 步骤的数量会随着 n 的增加而 *not* 增加。在上面的求和形式中，求和项的数量会随着 n 的增加而增加。这并不理想。

我们将细节留给你验证和解释，但我们声称可以建立一个适当的 *all* 二元 k-元组集合的划分，以证明

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \sum_{\ell=3}^{n} \binom{n}{\ell}$$

通过调用求和规则。（实际上，这个等式的证明涉及到我们将在下一节讨论的一些技术，但我们相信你可以理解这个方程的术语含义以及为什么这个等式必须成立。）然而，我们想要强调的是，我们可以重新排列这个方程，以获得某种意义上的原始所求解的 *better* 形式，在 *qualitative* 某种意义上：

$$\sum_{\ell=3}^{n} \binom{n}{\ell} = 2^n - \binom{n}{0} - \binom{n}{1} - \binom{n}{2}$$

看看我们取得了什么成就！无论N有多大，我们只需要评估四个项。这个数字是*fixed*的事实是关键点。事实上，由于我们非常喜欢这种形式的解，因此给它起了一个名字：**closed form**。其思想是没有“不必要的”求和，并且项数是固定的，无论其中包含的变量的值如何。

一般来说，在组合数学问题中，我们总是尽可能地寻找解决方案的 **closed form**。有时，想出

一个非封闭（有些人可能会说“开放”）的解的形式，但可能需要一些巧妙的方法才能将其简化为封闭形式。在这个特定例子中，我们依赖于我们的观察，即所有二进制 n-元组都可以被分类为恰好零个、恰好一个、恰好两个或至少三个1。这个解的封闭形式不仅使我们能够更快、更轻松地评估表达式，而且还为我们提供了对问题潜在结构的更多见解。出于这些原因，我们总是会要求封闭形式的解。

现在，让我们不要忘记问题（c）！为了回答它，我们采用与（b）中类似的技术，将具有偶数个1的二进制n-元组集划分为具有恰好零个1的，具有恰好两个1的，具有恰好四个1的，依此类推。然而，我们必须注意上限，因为n本身不一定是偶数！回想一下*floor function*，它将一个数向下舍入到小于该数的最大整数；一个例子是$\lfloor 5.7 \rfloor = 5$。考虑到这一点，我们声称有

$$\sum_{\ell=0}^{\lfloor n/2 \rfloor} \binom{n}{2\ell}$$

二进制 n-元组，其中1的个数为偶数。我们将把这个说法的解释留给你们来完成。试着向你的朋友展示并说服他们这是正确的。直到他们完全信服，不要放弃！我们将放弃尝试找到这个解决方案的 *closed form*，因为它超出了我们的掌握 . . .，或者不是吗？看看你能从这个求和中推断出什么！当 n 为偶数时会发生什么？当 n 为奇数时会发生什么？你能将这个表达式与类似的和联系起来吗？你能得出什么结论？

Example 8.3.12. 计算二进制4元组的数量，其中1以成对出现。为了澄清，我们希望将（1, 1, 0, 0）和（1, 1, 1, 1）包括在我们的计数中，但*neither* (1, 0, 1, 1) 以及（0, 1, 1, 1），例如。将此论点调整为计算二进制5元组的数量，其中1以成对出现。你能继续并找到一个一般模式吗？

要在一个4元组中有成对的1，这意味着我们总共可以有0个、2个或4个1。让我们定义集合S_0, S_2,和S_4为包含成对1的4元组的集合，这些4元组分别恰好有0个、2个或4个总1。注意：我们不是定义S_2为只包含恰好两个1的二进制字符串的集合。那样会错误地计算像(1, 0, 1, 0)这样的字符串。）这些集合构成了我们想要计数的元素集的一个划分，因此我们只需要计算这三个集合的元素，并应用加法规则将这些数字相加。

- 要找到 $|S_0|$，我们需要计算没有1的二进制4元组，并且只有一个这样的元组：(0, 0, 0, 0)。
- 要找到 $|S_2|$，我们需要计算包含两个连续1的二进制4元组，其余位置由0填充。通过手工列出情况，

(1, 1, 0, 0) (0, 1, 1, 0) (0, 0, 1, 1)

很明显，只有3个这样的元组。（你能找到一个更巧妙的论据来解释为什么是3个吗？当我们查看5元组时，我们会回到这个问题。）

- 要找到 $|S_4|$，我们需要计算包含四个 1 的二进制 4-元组。当然（1, 1, 1, 1）是唯一的这样的元组。

根据求和规则，因此，存在$1 + 3 + 1 = 5$个二进制4元组，其1位以成对出现。

要回答关于5元组的相同查询需要一点更多的独创性。我们将定义相同的集合，S_0, S_2, S_4，修改定义以包括5元组（而不是4元组）。然而，这三个集合的集合构成了我们寻求计数的二进制5元组集合的一个划分。只需计算每个集合的元素并应用求和规则即可。

- $|S_0| = 1$ 因为只有 1 个二进制 5-元组没有 1：(0, 0, 0, 0, 0).
- 要找到$|S_2|$，我们又可以手动写出情况，但最好能提出一个我们可以轻松适应k-元组的论点，对于任何$k \in \mathbb{N}$。要有一对1和剩余位置填0，我们可以将块“1, 1”视为一个单一单元，放置在三个0之间。因此，我们实际上是在计算将一个特殊单元放置在长度为4的有序列表中的方法数，然后确定性地用另一个固定元素填充剩余的位置。当然，有4种方法可以做到这一点，手动列出情况可以验证这一说法。（我们真正做的是注意到一个连续的1对由该对*first* 1的索引在元组中确定；该索引可以是{1, 2, 3, 4}中的任何一个，因此有$\binom{4}{1} = 4$种选择。）

- 此技术适用于我们考虑 $|S_4|$ 的情况。在这里，我们有两个独立的连续的1对，因此我们可以将每一对视为一个单独的块，“1, 1”。因此，我们实际上有两个“1, 1”块和一个0要放置在长度为3的有序列表中。由于1, 1块是相同的，我们可以通过选择1, 1块的两个位置来计数这些有序列表。因此，有 $\binom{3}{2} = 3$ 个这样的元组。（等价地，我们可以考虑选择0的位置，即 $\binom{3}{1} = 3$ 个选项。）

因此，存在$1 + 4 + 3 = 8$个二进制5元组，其1位以成对出现。

Alphabets and Words

与从 $[n]$ 中抽取元素的 k-元组的概念相关的是从给定的 *alphabet* 中创建 *words* 的概念。这两个概念之间没有太大的区别（在数学上，它们实际上是 *equivalent*，所以没有什么新东西！）但它允许使用不同的术语，并将一些“现实世界”的概念和问题联系起来。因此，以及你可能发现使用其中一个公式比另一个更容易，我们介绍了这个子节，并将其与前面的子节联系起来。

我们将通过一些例子来介绍和激发本小节的思想。在每个例子中，我们将指定一个 $alphabet$，其元素是我们可以用它来构建 $words$ 的允许的 $letters$。然而，“单词”一词实际上是指从给定字母表中抽取的有序字母 any 的字符串。例如，在第一个例子中，我们使用标准的英语字母表；在这种情况下，ZPQ 是一个完全可接受的三字母单词（但尝试发音它可能很幸运！）。我们允许这种通用性的主要原因是为了避免任何语义或词源上的争论，例如 REALISE 是否应该是一个可接受的 REALIZE 变体，或者 ZZZ 是否真的属于拟声词。这意味着我们必须剥离围绕“单词”一词的一些含义，将其视为仅由字母及其顺序组成的字符串，没有其他固有的含义。

Example 8.3.13. 让我们考虑这个例子中的标准26个字母的英语字母表。

1. 这个字母表可以组成多少个三个字母的单词?

   考虑这是否等同于询问 $identical$。我们有 26 个允许的字母，并希望形成长度为 3 的有序列表。通过在集合 $\{A, B, C, \ldots, Z\}$ 和 [26] 之间建立双射（这实际上是一种常见且简单的儿童游戏中的替换密码），我们可以严格地展示这个问题等同于询问 $|T_{26,3}|$ 是什么。

   无需必然建立这种联系，我们仍然可以轻松地数出三个字母的单词，注意到构建一个这样的单词相当于一个三步过程（从左到右填入三个字母）的每个步骤都有26种选择。因此，共有26^3个三个字母的单词。

2. 可以组成多少个四字母单词?

   根据前一个示例的相同逻辑，有26^4个四字母单词。

3. 有多少个 n-字母的词?

   我们将让您处理这个 ☺

4. 有多少个以元音开头的4个字母的单词?

   注意：我们将 {A,E,I,O,U} 视为元音字母集（即，尽管字母歌可能告诉你，但Y从不包括在内）。考虑到这一点，我们可以修改构建四字母词的四个步骤，以确保元音出现在左侧的第一个位置。这一步有5种完成方式，接下来每一步都有26种方式。因此，共有$5 \cdot 26^3$ 个以元音开头的四字母词。

5. 至多有2个辅音的4个字母单词有多少个?

   辅音是非元音，因此根据我们的定义，字母表中总共有26个−5个=21个辅音。至多有两个辅音意味着我们恰好有0个、恰好有1个或恰好有2个，因此我们可以将集合划分为

将问题中的单词分为三个相应的集合，S_0, S_1, S_2，并分别计数。通过应用乘法法则，我们发现

$$\begin{aligned} |S_0| &= 5^4 \\ |S_1| &= \binom{4}{1} \cdot 21 \cdot 5^3 \\ |S_2| &= \binom{4}{2} \cdot 21^2 \cdot 5^2 \end{aligned}$$

因此，有

$$5^4 + 4 \cdot 21 \cdot 5^3 + \binom{4}{2} \cdot 21^2 \cdot 5^2$$

四个字母的单词，最多有两个辅音。（挑战问题：有多少个四个字母的单词至少有三个辅音？用这个来对26^4的数量提出一个说法。）

以下关于 S_2 的论点有什么问题？通过选择两个辅音，然后选择第一个辅音的位置，然后选择第二个辅音的位置，最后用元音填充剩下的两个空位，得到

$$\binom{21}{2} \cdot 4 \cdot 3 \cdot 5^2$$

这样的词。

仔细思考这个问题。记住，这些“找出错误”问题并不仅仅是让你识别出存在错误，而是要解释为什么它是错误以及如何修复它。

6. 有多少个由4个不同字母组成的4个字母的单词?

没有预先思考，我们可以通过描述一个从左到右填充四个字母的四步过程，并在每一步减少一个选项的数量来回答这个问题。因此，有

$$26 \cdot 25 \cdot 24 \cdot 23$$

四个字母的不同字母的四字词。

这个看起来熟悉吗？回顾一下我们定义了 *arrange- ments* 的地方。这正是我们在这里使用的方法！从一个包含26个元素的集合中，我们想要构建一个长度为4的无重复的有序列表，即从26个元素中构造一个4-排列。我们推导出的公式告诉我们，恰好有

$$\binom{26}{4} \cdot 4! = \frac{26!}{4!\ 22!} 4! = \frac{26!}{22!} = 26 \cdot 25 \cdot 24 \cdot 23$$

这样的安排。这就是这个例子的教训：通过利用先前定义的术语和推导出的公式，并将当前问题与这些想法联系起来，我们可以“跳跃”到解决方案。

7. 有多少个四字母单词恰好有一个字母重复两次?

   为了构建具有这些特性的单词，我们需要知道哪个字母被重复，以及它的两个实例出现在哪里，还需要知道单词中出现的其他两个字母。因此，我们确定了一个三步过程：(1) 选择重复的字母；(2) 为该字母选择4个空位中的2个；(3) *arrange* 在剩余的两个空位中选择剩余的25个字母中的两个：

$$\binom{26}{1}\binom{4}{2}\binom{25}{2}\cdot 2!$$

8. 有多少个5个字母的单词恰好有两个字母各重复两次?

   按照前一个例子中的类似逻辑，我们可以（1）选择两个要重复的字母；（2）从5个空位中选择两个作为第一个（按字母顺序）重复字母的位置；（3）从剩余的3个空位中选择两个作为第二个（按字母顺序）重复字母的位置；（4）从剩余的24个字母中选择一个来填充最后一个，第五个位置。因此，总共有

$$\binom{26}{2}\binom{5}{2}\binom{3}{2}\binom{24}{1}$$

Example 8.3.14. 字母表中把U和ME放在一起有多少种排列（即排列）？ ☺

您可能会想到用“减法”思路来解决这个问题；也就是说，您可能会尝试计算所有将字母U *not* 放在字母ME旁边（按此顺序）的字母表的排列。您应该尝试解决这个问题，看看它会带您走向何方。不过，我们将提供一个 *different*，我们认为这是一个更简短的解决方案。这个解决方案背后的思想在其他问题中也会很有用，它归结为将两个字母组成的单词ME视为一个单独的 *block*，就像任何其他单个字母一样。

要稍微反转一下问题，而不是询问从给定的字母表中有多少个某种类型的单词，我们可能会想知道有多少个给定的单词的重新排列（即 *anagrams*）。在考虑这些问题时必须小心，因为当字母重复时，事情可能会变得复杂！例如，单词 A 有多少个排列？对于单词 AAAAA 呢？对于 AABBBCCCCDD 呢？正好！

Example 8.3.15. 让我们从简单的情况开始。HEART 这个单词有多少个排列组合？记住，我们将字母的排列组合 *all* 计算为可接受的单词，所以放下你的 Scrabble 思维过程 ☺(顺便说一句，Scrabble 对这个问题的答案是 4–HEART，HATER，EARTH，RATHE.) 由于这个单词中的每个字母都是 *distinct*，所以答案很简单：我们只需计算 5 个字母的所有排列组合。因此，有 $5! = 120$ 个 HEART 的排列组合。

现在，有多少个APPLE的排列？注意字母P出现了两次，所以我们不能真正考虑一个*five*元素集合的排列。如果我们这样做，每个单词实际上会以*twice*出现；也就是说，APPLE和APPLE都会被计算。你看到这两个单词之间的区别了吗？我们只是交换了P的位置！当然，这些是*same*个单词，所以我们必须将这一点考虑在我们的排列考虑中。

我们如何做到这一点？一个有用的技巧是“标记”重复的P。在从左到右阅读APPLE时，让我们称第一个为P_1，第二个为P_2。这将帮助我们区分重复的排列。现在我们的单词中有五个不同的元素——A，P_1，P_2，L，E——因此我们可以考虑这些元素的5!排列。我们知道这个*overcounts*，但我们都想弄清楚如何*by how much*这个过度计数。定义G为APPLE的排列（因此我们试图识别$|G|$），让M为上面列出的五个不同元素的排列。$|G|$和$|M|$之间有什么关系？

为了回答这个问题，我们可以考虑从 G 的元素构造 M 的元素。具体来说，我们可以通过首先取 G (的一个元素——APPLE 的一个字母排列) 并标记 Ps 来构造 M (的任何元素，即 5 个不同元素) 的一个排列。然而，这不会生成 M 的 *all* 个元素。为了做到这一点，我们必须取 G 的元素，并从中构造两个元素；具体来说，我们必须标记 Ps，然后考虑 Ps 在单词中的排列 *both*。让我们看一个例子：

- 取G中的一个元素，例如PAPEL。
- 标记 Ps 从左到右：P_1AP_2EL
- 构建 Ps 的两种排序，并将这两个词都视为 M 的元素：$P_1AP_2EL \in M$ 和 $P_2AP_1EL \in M$

自有两个排列两个P的方法，我们在单词内展示了$|G| \cdot 2! = |M|$。我们描述了一个两步过程来生成M的元素并应用了乘法规则。因此，我们可以重新排列这个方程以找到我们想要的数量：

$$|G| \cdot 2! = |M| \implies |G| = \frac{|M|}{2!} = \frac{5!}{2!} = 60$$

对于稍微困难一点的例子，让我们计算 COMBINATORICS 的排列。我们希望应用与上一个例子相同的策略，并标记重复的字母，以便将排列与 13 个不同元素的排列联系起来。再次，让我们定义 G 为 COMBINATORICS 的排列集合，M 为 $\{C_1O_1MBI_1NATO_2RI_2C_2S\}$ 中 13 个不同元素的排列集合。我们可以描述一个生成 M 的元素的四步过程：

1. 从G中取一个元素，并标注重复的字母，从左到右读取：$|G|$选项

2. 对两个重复的C进行排列：2!种选择。

3. 对两个重复的O进行排列：2!种选择。

4. 对两个重复的I进行排列：2! 选项。

因此，根据乘法法则，我们可以得出结论

$$|M| = |G| \cdot 2! \cdot 2! \cdot 2! \implies |G| = \frac{|M|}{2! \cdot 2! \cdot 2!} = \frac{13!}{2! \cdot 2! \cdot 2!}$$

您可能会想知道为什么我们选择写成$2! \cdot 2! \cdot 2!$而不是仅仅8。我们发现将答案以阶乘的形式呈现更为启发性和说明性，因为它表明了那些项 $came\ from$ 也位于何处。

如果字母重复超过两次会发生什么？唯一的区别在于当我们考虑重复字母的排列时。我们将让您填写论证的细节，但我们声称单词AABBBCCCCDD有

$$\frac{11!}{2! \cdot 2! \cdot 3! \cdot 4!}$$

无序词. 你能“看到”为什么还没有完全通过细节吗？你能填补这些细节来证实你的直觉吗？你能证明这个事实并说服一个朋友吗？试试吧！

存在几个更多的字母排列问题在练习中。稍后，我们甚至将证明一个结果，该结果将推广这种标记重复字母并计算它们的排列的技术。

在继续之前，我们应该指出一个与之前所见类似的现象。在一些例子中，我们最终从总数中得出一个计数 $subtracting$，并指出一个复杂的证明作者会直接陈述减法思想，尽管我们要求你用 $partition$ 的术语来表达并应用求和规则。同样，在之前的例子中，我们最终得出一个计数 $dividing$ 来消除一些过度计数，但我们确保用 $process$ 的术语来表达并应用乘积规则；之后，我们可以通过代数除法来简化。一个复杂的证明作者可能会通过考虑过度计数并论证我们可以“除掉”过度计数来写出相同的解决方案。我们说这是危险的，我们要求你 not 这样做（目前，在我们的语境中）。如果你让自己提出这类论点，很容易在不需要或不正确的情况下错误地“除掉”！强迫自己“从头开始”提出这些论点将更牢固地确立这些基本原理，并允许你在数学生涯的后期更自信地应用“减法”和“除法”原则。只需记住，我们要求你只在我们语境中使用ROS和ROP！

让我们看看两个基于标准英语字母表之外的字母和单词的快速示例。

Example 8.3.16. 美国电话号码由区号（3位数字）和本地号码（7位数字）组成。这些数字来自集合

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}，但区号和本地号码都不能以0开头。有多少种可能的电话号码?

这是一个通过建立10个步骤的过程来计数，对应于电话号码的10个总数字。其中8个数字有10种选择，而另外两个数字有9种选择（不含0），因此乘法原理告诉我们有

$$10^8 \cdot 9^2 = 8,100,000,000$$

可能的电话号码。这个数字略大于当前世界人口，所以目前来看，我们的系统似乎是安全的!

Example 8.3.17. 假设一家餐厅有三种不同的类别：开胃菜、主菜和甜点。有5种开胃菜，9种主菜和4种甜点。你带你的约会对象去这家餐厅，在等待服务员出现的时候，通过计算在满足某些条件下你可以下多少种可能的订单来打发时间。（不幸的是，你忘记决定要吃什么，最后你随机选择了一个订单，但这不是重点。）

(1) 假设你必须点一份开胃菜、一份主菜和一份甜点，你能点多少种不同的组合?

这是一个简单的ROP应用。有$5 \cdot 9 \cdot 4 = 180$种可能的订单。这像字母和单词一样吗? 嗯，你可以把它想象成构建一个三字母单词，但单词中每个“槽位”的字母表都不同。

(2) 假设你们每人订购一个应用、一棵树和一个zert，但你们两人不能在任何类别中订购$same$这个物品，你们可以做出多少种可能的订单?

这是一个3步过程，每步分为2部分。首先，你点一份开胃菜，然后你的约会对象也点（确保从你挑选的开胃菜中选择）。其次，你点一份主菜，然后你的约会对象挑选一个不同的。第三，你点一份甜点，然后你的约会对象挑选一个不同的。显然，那么，有

$$(5 \cdot 4) \cdot (9 \cdot 8) \cdot (4 \cdot 3) = 20 \cdot 72 \cdot 12 = 17280$$

可能性。将此与每个类别中不同物品排序的限制所具有的可能性 $without$ 进行比较，我们可以通过使用我们在问题（1）上的工作来找到这个限制：{v *}

$$180 \cdot 180 = 32400$$

再次，我们可以将这个问题视为一个限制性字母/单词问题。

Balls and Bins

这是更高级课程中组合问题的一种常见公式。在讨论 $probability$ 并使用组合事实和思想来探索概率时尤其有帮助。我们希望在这里提出它

因为引入了*distinguishable*和*indistinguishable*对象之间的重要区别。为了激发这次讨论，让我们提出一个看似简单的问题：

考虑一个包含 n 个球的箱子；我们有多少种方式可以选出 k 个球?

你的答案是什么？如果你说了“$\binom{n}{k}$”，你可能是对的。如果你说了“1”，你也可能是对的。这怎么可能？！好吧，我们没有指定箱子里的n个球是否是*distinguishable*；也就是说，我们没有说明它们是否都是不同的，我们是否能够区分出任意两个球。

想象一个里面有100个网球的水桶。如果我们抽出两个球给你看，你能分辨出它们吗？也许它们上面有不同的模糊黄色毛发数量，或者也许它们是不同的品牌，或者类似的东西……但是也许我们做不到。也许所有的球都是完全相同的。在这种情况下，我们抽出的“哪个”k球并不重要，因为我们无法分辨它们。所有“可能的”k球的选择都归结为同一件事，所以“1”这个答案是完全合理的。然而，如果所有的球都有一个独特的数字，或者它们都是不同的颜色，或者……想象任何你想要的区分属性。在任何这些情况下，“$\binom{n}{k}$”都是正确的答案。出于这些原因，最初提出的问题是一个糟糕的问题；我们应该具体说明球是否是*distinguishable*。

这个关于*distinguishability*的想法之前已经出现过。记得我们在第8.2.3节中建立的计数公式网格吗？网格中的一个基本问题是选择/排列*distin- guished*的顺序是否会影响结果。例如，选择不考虑顺序。选择{1, 3, 4}和{3, 4, 1}是相同的（你也应该把它们看作*sets*来理解这一点），因为元素书写的顺序并不能区分它们。相反，*arrangements* (1, 3, 4)和(3, 4, 1)是不同的，因为元素的顺序可以区分它们。

在“球和箱子”问题的背景下，我们将通过说它们以某种方式编号或着色来指定物品的可区分性。然而，这也可能涉及可区分/不可区分特征的混合，所以请小心！下一个例子说明了这种相互作用。

Example 8.3.18. 假设我们有一个包含红色、蓝色或绿色球（即每个球都有这三种颜色中的一种）的箱子。箱子里每种颜色的球都有3个，任何两种*same*颜色的球都是无法区分的。我们抽出四个球。有多少种可能的结果?

在阅读我们的解决方案之前，试着玩玩这个问题。你可能会想出自己解决问题的方法！

一种可能的方法是先列举所有可能性，然后

尝试推断一个模式。我们可能开始写下输出 mes as:

3个红色和1个蓝色 3个红色和1个绿色 2个红色和2个蓝色 2个红色和2个绿色 2个红色和1个蓝色和1个绿色 ...

等等。注意我们是如何跟踪这些信息的；每个结果都由以下特征来描述：（a）我们挑选了多少个 red 球，（b）有多少个蓝色球，以及（c）有多少个绿色球。本质上，我们可以用形式为 (r, b, g) 的有序三元组来描述每个结果，其中 r 是红色球的数量，对于 b 和 g 也是如此。我们唯一需要满足的条件是 $r+b+g = 4$，并且每个值都满足 $0 \leq r \leq 3$，$0 \leq b \leq 3$，$0 \leq g \leq 3$。我们实际上只需要计算满足这些条件的 3-元组的数量！我们可以将这个计数分解为有多少个非零项，并分别分析每种情况。

- 如果两个项为0，则第三个项必须是4。有 $\binom{3}{1} = 3$种选择哪个项不为零，因此有3种这样的可能性。

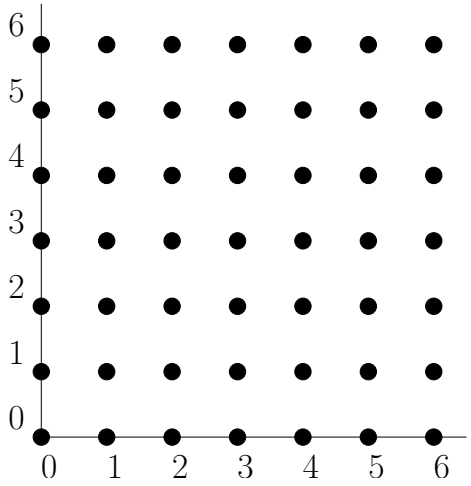
- 如果一个项为0，则其他两项之和必须为4，且两项均不为零。共有3种方法：$1 + 3$ 和 $2 + 2$ 和 $3 + 1$。由于有3种选择哪一项为0，根据ROP，共有 $3 \cdot 3 = 9$种可能性。

- 如果所有三个项都不为零，那么我们可以看到，唯一的这样的和是$1 + 1 + 2$，以某种顺序。对于哪一项是2，有3种选择，然后其他项必须是1。因此，有3种这样的可能性。

通过ROS，共有$3 + 9 + 3 = 15$种可能性。

Lattice Paths

考虑由所有自然数或0组成的有序对 $\mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\} = (\mathbb{N} \cup \{0\})^2$ 组成的集合。实际上，让我们在平面上直观地表示这个集合：



这个平面上的“点阵”被称为一个 *lattice*。这里有一个自然的问题：给定晶格中的任何一点，从原点 $(0,0)$ 到达该点的有多少种方法？让我们更具体一些。让我们定义一个 **lattice path** 为从 $(0,0)$ 到特定点的路径，该路径在任何一步只允许移动 *rightwards* 或 *upwards*。这就是下一个定义所传达的内容：

Definition 8.3.19. *Let $(x,y) \in (\mathbb{N} \cup \{0\})^2$. A* **lattice path** *to (x,y) is an ordered tuple of points in the plane lattice where the first element of the tuple is $(0,0)$, the last element of the tuple is (a,b), and every element in the tuple only differs from the previous one by having exactly one coordinate that is exactly one larger than the corresponding coordinate of the previous element.*

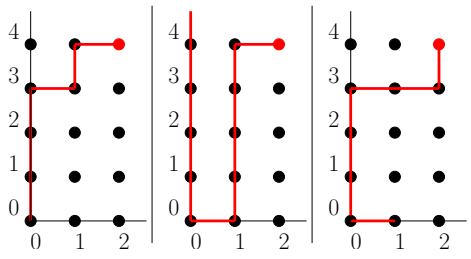
More rigorously, given (x,y) a lattice path is an n-tuple $(P_1, P_2, \ldots, P_n)$, for some $n \in \mathbb{N}$, where each $P_i = (x_i, y_i)$ is a point in the lattice, and

$$\forall i \in [n-1] \bullet (x_{i+1}, y_{i+1}) = (x_i + 1, y_i) \ \vee \ (x_{i+1}, y_{i+1}) = (x_i, y_i + 1)$$

and, furthermore, $(x_1, y1) = (0,0)$ and $(x_n, y_n) = (x,y)$.

That is, a lattice path is a sequence of points in the lattice from $(0,0)$ to (n,n) where we are only allowed to move 向右 *or* 向上 *by one grid point at every step.*

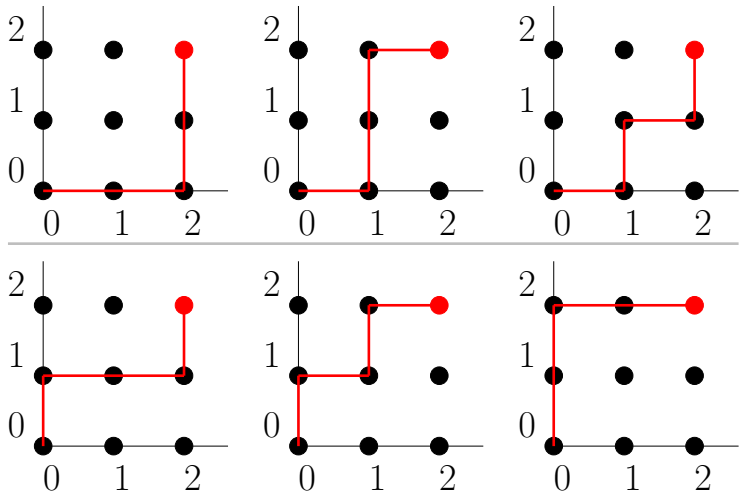
Example 8.3.20. 考虑平面格点上的点 (2, 4)。在下图中，我们绘制了几条到 (2, 4) 的样本格点路径。



我们的问题是这样的：

> 给定 $(a, b) \in (\mathbb{N} \cup \{0\})^2$，有多少 *many* 个不同的晶格路径到达 (a, b) ？

为了开始回答这个问题，让我们考虑一个简单的、值较小的情况，这样我们实际上可以枚举出所有路径。让我们考虑到（2, 2）的格点路径：



如何以 *combinatorial* 的方式表示格点路径？也就是说，我们如何以方便计数某些对象的方式表示它们？考虑格点路径的定义特征：格点路径构建中的每一次“移动”必须是 *rightwards* 或 *upwards*。那么，以某种方式表示我们何时进行“向右”移动和何时进行“向上”移动是有意义的。然后，我们只需要计数有多少“向右”和“向上”的选择序列实际上带我们到达所问的点 (x, y)。

这很简单，尽管如此！平面上点(x, y)有什么特征？嗯，它在(0, 0)右边有x个网格点，并且从(0, 0)向上有y个网格点。因此，无论我们的路径*looks like*如何，我们知道必须有x次向右移动和y次向上移动。回顾上面到(2, 2)的6个格点路径。想想沿着路径走，从(0, 0)开始，并在每个网格点上写下R或U，具体取决于我们下一步去哪里。这产生了以下6个R和U的序列

$$RRUU\,,\ RUUR\,,\ RURU\,,\ URRU\,,\ URUR\,,\ UURR$$

这些序列有哪些共同属性？每个序列都有2个 R 和2个 U，因为我们必须以 (2, 2) 结束，因此每个序列总共有4项。注意，这很像一个受限字母表/单词问题：我们想要找到长度为4的单词，这些单词是从字母表 {R,U} 中选取的，并且每个字母恰好出现两次！

一般来说，我们知道任何到(x, y)的晶格路径都可以表示为R和U的$(x + y)$-元组，其中恰好有x R个和y U个。为了确定有多少个这样的序列$many$，我们有一个两步过程：

1. 从 $x + y$ 个空槽中，选择 x 个用 R 填充： $\binom{x+y}{x}$
   选项 2. 用 U 填充剩余的 $(x + y) - x = y$ 插槽：1 个选项（确定性）

Thus, 我们有以下结果。

Proposition 8.3.21. *For every* $(x, y) \in (\mathbb{N} \cup \{0\})^2$*, there are exactly* $\binom{x+y}{x}$ *lattice paths from* $(0, 0)$ *to* (x, y)*.*

我们将探讨在练习中格点路径的一些有趣的应用和性质。目前，我们想要指出它们的存 在以及与序列和选择的关系。但关于它们还有一个观察：为什么我们选择计算长度为 $x+y$ 且恰好有 x Rs 的序列的数量？计算长度为 $x + y$ 且恰好有 y U s 的序列的数量会有所不同吗？想想看：每个到 (x, y) 的格点路径需要恰好 x Rs 和恰好 y U s，确保其中一个性质成立也保证了另一个性质成立。因此，我们可以提出以下结果：

Proposition 8.3.22. *For every* $(x, y) \in (\mathbb{N} \cup \{0\})^2$*, there are exactly* $\binom{x+y}{y}$ *lattice paths from* $(0, 0)$ *to* (x, y)*.*

这不仅 *proves* 以下事实

$$\binom{x+y}{x} = \binom{x+y}{y}$$

但是，它还向我们介绍了一种新的、有用的证明策略：**Counting in Two Ways**。我们识别了一个对象（从（0, 0）到（x, y）的格路径集合）并继续解释了计算该对象集合的两种方法。每种方法都给出了该集合的基数的一个不同表达式，因此我们可以宣布这两个表达式是相等的。这个第一个例子说明了“两种方式计数”背后的主要思想，我们将在下一节中探讨更多示例和一般技术。

8.3.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 如何识别一个提出的计数论点是 **under- count**？如何证明它是 **overcount**？(2) 解释“[n]中的 $k-$元组”与“字母表和单词”之间的关系。它们在本质上有什么相同之处？(3) 假设我们从有 n 个球的箱子中选取 k 个球。为什么球是否 $distinguishable$ 有关系？(4) 为什么从 (0, 0) 到 (x, y) 的格点路径数等于 $both$ $\binom{x+y}{x}$ 和 $\binom{x+y}{y}$?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 找出所有5张牌的扑克手牌中**two pair**的数量，并证明你的说法。(2) 找出所有5张牌的扑克手牌中是**full house**的数量，并证明你的说法。(3) COMBINATORICS这个单词有多少个排列？MASSACHUSETTS有多少个排列?

(4) 考虑找出从 {1, 2, 3} 中包含至少每个数字的一个的 4-元组的数量。对于以下提出的“证明”，通过展示被该论证计数的对象来证明它是 **incorrect**。

(a) 从元组中选择一个位置给1，然后选择一个位置给2，再选择一个位置给3。然后，从三个元素中选择一个出现在第4个空位上。

$$\binom{4}{1}\binom{3}{1}\binom{2}{1}\binom{3}{1} = 72$$

(b) 从4个空位中选择3个来填充元素1、2、3。将这些元素排列在所选位置。为第4个空位选择一个数字。

$$\binom{4}{3}3! \cdot 3 = 72$$

(5) 对于这个问题，考虑一个 $word$ 是任何由英文字母组成的字符串，无论它实际上是否在字典中拼写出某个词。例如，$ZYQFIB$ 是一个长度为6的有效的 $word$。

(a) 有多少个长度为2的单词？(以*two*种方式回答这个问题：用指数数和两个项的和。) (b) 长度为7的单词中有多少个恰好有3个A？ (c) 长度为7的单词中最多有多少个元音？(注意：A, E, I, O, U是元音。Y不是。)

考虑所有长度为 n 的二进制字符串的集合 S_n。对于以下所述的每个属性，计算 S_n 中有多少个元素具有该属性。（注意：每个属性是独立的；不要考虑同时满足所有属性，例如。）

(a) 精确有3个位置是0。

(b) 最多3位是0。 (c) 至少4位是0。 注意：使用最后两部分将2^n写成二项式系数的和！

(d) 0的位置比1的位置多。

(6) 设 $n \in \mathbb{N}$ 已知。有多少个格点路径从 (0, 0) 到 $(2n, 2n)$？有多少条这样的路径 *also* 通过 (n, n)？

(7) 考虑以下解释：

> 6张牌的手牌数量，从一副标准扑克牌中抽取，每个花色有 *at least one*张牌的是
>
> $$\binom{13}{1}\binom{13}{1}\binom{13}{1}\binom{13}{1}\binom{48}{2}$$
>
> 因为我们从每种花色中选一张牌，然后从剩余的48张未使用的牌中再选两张。

这是计数正确吗？如果你认为它是一个 *overcount*，展示一个特定的手并展示如何以两种方式计数。如果你认为它是一个 *undercount*，展示一个特定的手并展示它为何不计数。

8.4 Counting in Two Ways

如果您刚刚进入这一节，请重新阅读上一节中的最后一个例子，因为它为“两种计数方法”提供了一个完美的介绍和示例。在那个例子中，我们以不同的方式计算了到达 *two* 中特定点的格点路径数量，推断出我们找到的两个表达式必须相等。具体来说，我们推断出 $\binom{x+y}{x} = \binom{x+y}{y}$。有了这个例子作为基础，我们在这里将概述一种一般策略并将其应用于几个示例。在这个过程中，我们不仅将练习这种技术，还将证明一些有用的组合结果，我们可以将这些结果应用于其他问题！

让我们首先实际展示一个来自上一节的 *alternative* 证明。有一个更简短的论证，根本不涉及格路径，并且是对这个结果更易于记忆和理解的解释。

Proposition 8.4.1. *Let* $n, k \in \mathbb{N} \cup \{0\}$. *Then* $\binom{n}{k} = \binom{n}{n-k}$.

Proof. 设 S 为 $[n]$ 的所有大小为 k 的子集的集合，即

$$S = \{T \subseteq [n] \mid |T| = k\}$$

根据 k-选择的定义，$|S| = \binom{n}{k}$，因为构造一个包含 $T \subseteq [n]$ 的集合 $|T| = k$ 等于从包含 n 个元素的集合中选择 k 个元素。

等效地，我们可以通过选择 $n-k$ 个元素到 *not* 包含在 T 中来构建一个集合 $T \subseteq [n]$，其中包含 $|T| = k$；这意味着已经选择了 $n-(n-k) = k$ 个元素属于 T。这样做的方法数是 $\binom{n}{n-k}$。由于每个这样的集合 T 都可以通过这种方式构建，我们已经证明了 $|S| = \binom{n}{n-k}$。

因此，$\binom{n}{k} = \binom{n}{n-k}$。 □

我们发现这更是一个令人难忘的事实证明，因为我们能非常简洁地用一句话总结整个证明

> 统计 $[n]$ 中的 k-元素子集，通过识别要包含的元素 *or* 和要省略的元素。

This 这是我们要记住的想法；从它，我们可以重建证明。试图逐句“记住”一个证明是没有意义的；相反，记住证明主要思想的 *kernel* 然后填充细节是有帮助的。

8.4.1 Method Summary

Why It Works

让我们抽象一个层次，并讨论计数两种方式作为证明技术。让我们谈谈 *why* 它是如何工作的以及 *how* 如何应用它。然后，我们将通过

几个更多示例。我们在上一节的末尾提到了 *why* 这个想法，所以我们将在这里重申这些想法。“两种方式计数”是这个证明技术的最佳名称，因为它在其名称中就解释了策略！任何遵循此技术的证明都识别一组有限元素，并提供 *two ways* 来计数这些元素。通过使用求和规则和乘积规则，以及我们看到的其他组合结果，这两种方式为相同的数字产生了不同的代数表达式，即所讨论的元素集合的 *cardinality*。

一个好的证明清楚地确定了要计数的有限集合以及计数其元素的两个不同方法，然后通过等式得出两个代数表达式。因此，通过这种方法证明的任何结果都将是某种涉及二项式系数、求和和其他代数表达式的*identity*或*equation*。证明的要点是用计数论来清楚地解释这些表达式，而不是对项进行严格的代数简化。

看看我们刚才证明的结果：是的，我们可以直接验证 $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$，但那样有什么乐趣呢？这无论如何都不能算是一个 *interesting* 证明，也不提供任何 *insight* 来解释结果为什么是正确的。此外，随着我们研究越来越多、越来越具有挑战性的这类问题，代数验证变得相当困难，在某些情况下，几乎是不可能的！

How To Use It

我们将在此节后面继续展示几个例子（以及非例子），但首先我们想介绍“两种计数方法”的概要。这将为我们提供一个标准，用以衡量未来此类证明；我们可以阅读它们，确保它们遵循结构、清晰度和正确性的重要要点。我们将以此标准要求自己，并期望你们也这样做。我们还向你们介绍一些在“两种计数方法”证明中使用的标准组合对象，随着例子的进行，我们将指出何时考虑使用特定的对象集合进行计数。

现在，这里有一骨骼结构 *every good Counting in Two Ways* *proof*！

1. 陈述要证明的结果。（注意：记得量化表达式中出现的任何变量！）2. 定义一个集合——让我们称其为 S——要计数的对象。3. 通过遵循适当的组合论论证，以某种方式计数 S 的元素。将所得表达式与 $|S|$ 等式。4. 通过遵循适当的组合论论证，以另一种方式计数 S 的元素。将所得表达式与 $|S|$ 等式。5. 结论是，由于两个导出表达式都等于 $|S|$，它们必须相等。

那就可以了！就像我们说的，技术的名字就是技术本身，所以应该很容易记住。然而，多年来阅读了许多这些证明后，我们注意到某些错误是常见的。我们在这里列出了最常见的。想想为什么做这些中的任何一项在某种程度上都会构成一个“不好的”证明。每个错误未能满足一个好的证明的哪个属性？正确性？清晰性？简洁性？

Common mistakes to avoid:

- 忘记定义要计数的对象集。
- 定义一个集合，但以两种方式计数其他事物。
- 计算一组对象，但然后用另一种方式计算一个 *different* 组对象。
- 未在结论中将两个表达式等同起来

其他错误可能在实际的组合证明中产生，而不是整个技术，但也要留意这些！

8.4.2 Examples

让我们详细地通过几个例子。这将帮助您了解如何应用“两种计数方法”，为您提供一些可以回顾和重新阅读的典型例子，并为您提供一些可以在未来问题中应用的基本组合结果。在每个例子中，我们不仅试图证明所提出的结果，还解释我们如何得出证明，我们的思维过程可能是什么，以及您如何尝试自己解决这类问题。两种计数方法证明的美丽之处在于，在证明结束时，我们通常可以清楚地总结证明的主要思想。我们将对每个证明都这样做，并鼓励您在写完任何这样的证明后尝试同样的总结。这使得证明思想更容易记住，并允许您仅从一句话中重建整个证明。

Proposition 8.4.2 (帕斯卡恒等式)**.** *For any* $n, k \in \mathbb{N}$*,*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

*Proof strategy*看到二项式系数，如 $\binom{n}{k}$，表明我们可能想要计数具有特定大小的 $[n]$ 的子集。这个恒等式的左边容易表示（计数所有大小为 k 的子集），但右边呢？看到两个项的 *sum* 指示某种类型的划分。我们必须识别 $[n]$ 中大小为 k 的子集的某个特定属性，以便某些子集 *do* 具有该属性，其中一些 *don't*。

仅术语之间的区别在于“底部系数”，我们可以找出一个有成效的划分 . . . 在继续阅读之前，看看你能否自己想出来！

Proof. 让 $S = \{T \subseteq [n] \mid |T| = k\}$。根据 k-选择的定义，我们知道 $|S| = \binom{n}{k}$。接下来，定义集合

$$A = \{T \subseteq [n] \mid |T| = k \wedge 1 \in T\}$$
$$B = \{T \subseteq [n] \mid |T| = k \wedge 1 \notin T\}$$

当然，$A \cap B = \varnothing$，因为对于任何集合 T，$1 \in T$ 和 $1 \notin T$ 都不能同时为真。同样地，$S = A \cup B$，因为对于任何集合 T，$1 \in T$ 或 $1 \notin T$ 至少有一个为真。因此，$\{A, B\}$ 是 S 的一个划分，那么我们知道 $|S| = |A| + |B|$。

要找到 $|A|$，我们确定了一个两步构建元素 $T \in A$ 的过程：(1) 将元素 1 包含在 T 中；(2) 从剩余的 $n-1$ 个元素中，再选择 $k-1$ 个来形成一个包含 k 个元素的集合。根据乘法原理，我们得出

$$|A| = 1 \cdot \binom{n-1}{k-1} = \binom{n-1}{k-1}$$

类似地，为了找到 $|B|$，我们确定了一个两步构建元素 $T \in B$ 的过程：(1) 从 T 中省略元素 1；(2) 从剩余的 $n-$ 个 1 元素中，选择 k 个元素。根据乘法原理，我们得出

$$|B| = \binom{n-1}{k}$$

根据求和规则，我们得出结论

$$|S| = |A| + |B| = \binom{n-1}{k-1} + \binom{n-1}{k}$$

通过将 $|S|$ 的两个表达式相等，我们得出结论

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

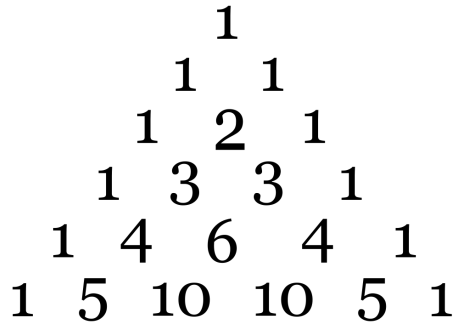
□

*Proof summary*计算基于特定元素（例如，1）是否属于子集的划分，来计算 $[n]$ 的 k-元素子集。

*Question*如果我们用元素 n 而不是 1 来构建我们的划分，证明会有任何 *different* 结构上的变化吗？不会！重要的是我们识别了一个 *specific* 元素，并基于该元素定义了划分集合，A 和 B。

*Historical note*这个命题是以法国数学家布莱士·帕斯卡命名的。也许你也听说过帕斯卡三角形吧？这个自然数三角形是通过写下两行1，所有行都是1来构建的

周长，然后填充其他每个数字为它上面的两个数字之和。基于我们刚刚证明的命题，这给你任何关于三角形中包含的数字的提示吗？没错，它们是二项式系数！n行代表所有形式为$\binom{n}{k}$的数字，其中系数k在从左到右读取时是递增的。帕斯卡三角形的性质有很多有趣之处，我们将在我们的例子和练习中探讨其中的一些。



Proposition 8.4.3 (主席身份)**.** *For any $n, k \in \mathbb{N}$,*

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Proof strategy: 该方程式的两边都是两个项的 *products*，因此我们正在寻找两个两步过程来构建相同的元素集。左边的项可以被视为 $\binom{n}{k} \cdot k$，因为乘法是交换的。这表示从 $[n]$ 中选择 k 项，然后 ... 另一件事。如果我们把 k 重新写成 $\binom{k}{1}$，这会使第二步变得清晰：我们随后从第一步中选择的 k 个元素中选择一个。

这提出了一种描述子集及其包含的特定元素的新策略：*committees* 和 *leaders*。这在组合证明中相当流行，因为它减少了使用的技术、数学语言和符号的数量，并使对证明关键思想的通俗理解更好。我们将在下面的证明中向您展示如何使用这种策略，然后我们将将其与用更数学化的语言编写的证明进行比较。在继续阅读之前，看看您能否预测我们如何描述所讨论恒等式的右侧 ...

Proof. 设 $k, n \in \mathbb{N}$ 已知，设 S 为从 n 人中选出的 k 人的委员会，并指定一名委员会主席。构建 S 的元素的一种方法首先选择一个 k 人的委员会，然后从委员会中选择一名成员担任主席。根据乘法原理，我们得出

$$|S| = \binom{n}{k} \cdot \binom{k}{1} = k\binom{n}{k}$$

另一种构建 S 元素的方法是首先从 n 人员中选出委员会主席，然后从剩余的 $n-1$ 人中选出 $k-1$ 人来填补委员会。根据乘法原理，我们得出结论：

$$|S| = \binom{n}{1} \cdot \binom{n-1}{k-1} = n\binom{n-1}{k-1}$$

通过将这两个关于 $|S|$ 的表达式等同起来，我们得出结论

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

□

*Proof summary*统计由n人组成的、有主席的k-委员会，通过先选择委员会然后选择主席，或者先选择主席再选择委员会的其他成员。

Comments: 如果我们尝试用纯数学术语来描述这个证明，即用集合来描述，会怎样呢？在集合论语言中，“主席”究竟对应什么？从总共 n 人的 k 人规模的委员会只是一个包含 n 的集合 $T \subseteq$，但我们如何区分这个集合与所有选择其成员之一作为主席的 k 种不同的方式？一种合理的方法是定义一个 *ordered pair*，其中第一个坐标是委员会成员的集合，第二个坐标是特定的主席。有了这种策略，我们就可以定义

$$\hat{S} = \{(T, x) \mid T \subseteq [n] \wedge |T| = k \wedge x \in T\}$$

这个集合$\hat{S}$ 与我们在上述证明中定义的集合 S 是 *equivalent* 的，因为它包括了拥有一个主席的 k-委员会的所有方式。然而，在描述$\hat{S}$ 的两种计数方式时，我们可能会发现自己不得不求助于对委员会和主席的相同口语描述！（试试看用这种方法计数$\hat{S}$ *without* 的元素。）这样做更自然，也更易于理解。简而言之，没有真正的原因要严格写出这些关于委员会集合的集合论描述；然而，重要的是要指出我们 *can*。这证实了上述证明中的描述确实是足够严格的；它们基于数学概念，但在用其他术语描述时更容易理解和跟随。

本节练习中探讨了涉及委员会和子委员会的两种计数方式的几个例子。在此，我们将再举一个例子以供练习。

Proposition 8.4.4 (所有规模的委员会)**.** *Let* $n \in \mathbb{N}$*.* T *hen,*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

*Proof strategy*右侧可能代表许多事物，但似乎它涉及一个n-步过程，其中每一步有2个选项。让我们稍后再重新审视这个术语。左侧代表一个*partition*，因为我们有几个项的*sum*。求和中每个单独的项，形式为$\binom{n}{k}$，代表从n个人中选择一个委员会的k人的方法数。当我们允许k从0到n变化时，我们正在考虑委员会的*all possible sizes*。这表明我们正在计算从一组n个人中选择*all*个可能的委员会。现在我们知道右侧必须计算什么，我们可以为那个...构建一个论点。在阅读我们的证明之前，试着自己来做！

Proof. 设 $n \in \mathbb{N}$ 和设 S 为从 n 个人中选择的任何大小的所有委员会的集合。S 的每个元素是从 0 到 n（含）的某个大小的委员会；对于每个 $k \in [n] \cup \{0\}$，设 S_k 为大小恰好为 k 的委员会的集合。那么集合 $\{S_k \mid k \in [n] \cup \{0\}\}$ 是 S 的一个划分。因此，根据求和规则，我们得出

$$|S| = \sum_{k=0}^{n} |S_k| = \sum_{k=0}^{n} \binom{n}{k}$$

wh因为 S_k 是从所有 k-选择中组成的集合 $[n]$。

我们还可以按以下方式计算S的元素：取我们的n人集合，并为他们分配从1到n的数字。（例如，可以通过给每个人一件带有其唯一编号的T恤来实现。）为了构建一个委员会，我们按数字顺序排列每个人，沿着队伍前进，对每个人说“是”或“否”，以表明他们是否属于我们正在创建的委员会。每个n个“是”和“否”分配的序列产生一个独特的委员会。由于这是一个每步有两个选择的n步过程，乘法原理告诉我们有2^n种完成此过程的方法，所以$|S| =^n$。通过将这两个关于$|S|$的表达式相等，我们得出结论：

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

□

*Proof summary*计算基于大小的划分下 $[n]$ 的所有子集。（注意：这个总结是以 *sets* 为基础的，但证明本身以 *committees* 为基础写起来更容易理解，我们感觉如此。）

也许这个证明在你看来有点冗长，尤其是因为我们已经通过归纳法证明了 $|\mathcal{P}([n])| = 2^n$。由于我们正在考虑所有大小的 *all* 委员会，所以我们等价地说“设 $S = \mathcal{P}([n])$”，然后以两种方式计算 S。然而，当我们开始用 *committees* 的术语来写证明时，我们不能在不写一两句话关于 *why* 那些公式等价的情况下，切换到谈论 $[n]$ 的子集。作为一个练习，尝试完全用集合符号重写这个证明，而不提及委员会。你更喜欢哪一种?

The Summation Identity

下一个组合恒等式非常有用，它将出现在本章后续的证明和练习中，因此我们在这里呈现结果。此外，我们将以两种方式呈现 *two different* 计数证明，第三种在练习中介绍，甚至！这两种证明我们呈现涵盖了更多标准计数对象，正如它们出现在两种方式计数证明中。我们鼓励你阅读这两个证明，并尝试理解它们是如何 *related* 的。也许你正在想为什么我们甚至要呈现 *same* 事实的两个证明。（“一个不就够了吗？我们已知它是真的？”）通过理解证明结构和它们是如何 *equivalent* 的，你将获得对这些证明技术的更深入理解，并能更好地应用它们。相信我们！此外，我们将将这些技术与我们在前一个问题中使用的委员会方法进行比较，并研究这三种方法是如何相关的。

Theorem 8.4.5 (求和恒等式)**.** *Let* $n, k \in \mathbb{N}$*. Then,*

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}$$

*Proof 1 strategy*看到右侧只有一个二项式项表示我们正在查看大小恰好为 k+1 的 [n+1] 的子集。左侧有求和符号时，我们根据某些属性将所有此类子集的集合进行划分。由于求和符号内的二项式系数在最后一项中有一个 k，而不是 k+1，这意味着索引 i 以某种方式代表一个被包含在子集中的特定元素。在继续阅读之前，看看你能否填写这个划分的细节 ...

Proof 1. 让 $n, k \in \mathbb{N}$ 和 定义

$$S = \{T \subseteq [n+1] \mid |T| = k+1\}$$

根据 $[n+1]$ 中的 $(k+1)$-选择的定义，我们知道 $|S| = \binom{n+1}{k+1}$。接下来，对于每个 $i \in [n] \cup \{0\}$，定义集合

$$S_i = \{T \in S \mid i+1 \in T \wedge (\forall j \in T.\, j \leq i+1)\}$$

这意味着 S_i 是 $[n+1]$ 的所有大小为 $k+1$ 的子集的集合，其 *maximally-indexed* 元素是 $i+1$。我们声称 $\{S_i \mid i \in [n] \cup \{0\}\}$ 是 S 的一个划分。

首先，观察当 $i \neq j$ 时 $S_i \cap S_j = \varnothing$。这是因为 $T \in S_i$ 意味着 $i+1 \in T$；进一步地，如果 $i > j$，则任何 $U \in S_j$ 的最大索引元素是 $j+1$，这小于 $i+1$，如果 $i < j$，则任何 $U \in S_j$ 包含 $j+1$ 但 $j+1 \notin T$。

其次，请注意每个 $T \in S$ 都在 1 和 $n+1$ 之间有一个最大索引元素，因此属于 S_i 个集合之一。（作为本证明部分的指南，我们下面包含了一个图，说明了 $n = 4$ 的情况）

并且 $k = 2$。注意，其中几个集合是空的。一般来说，对于每个 $i \in [k-1] \cup \{0\}$，但这是有意义的，因为对于所有这些 i 的值，$\binom{i}{k} = 0$（也是一样）。

接下来，我们必须为每个 $i \in [n] \cup \{0\}$ 识别 $|S_i|$。为了构建一个元素 $T \in S_i$，我们采用两步过程：（1）我们包括元素 $i+1 \in T$，然后（2）从 i 较小索引的元素中，我们选择 k 个来包括。根据乘法原理和选择定义，有 $\binom{i}{k}$ 种方法来做这件事。

因此，根据求和规则，我们得出结论：

$$|S| = \sum_{i=0}^{n} |S_i| = \sum_{i=0}^{n} \binom{i}{k}$$

通过将这两个关于 $|S|$ 的表达式等同起来，我们得出结论

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}$$

□

Diagram for $n = 4$ *and* $k = 2$:

$$S = \Big\{ \{1,2,3\},\ \{1,2,4\},\ \{1,2,5\},\ \{1,3,4\},\ \{1,3,5\},\ \{1,4,5\},\ \{2,3,4\},\ \{2,3,5\},\ \{2,4,5\},\ \{3,4,5\} \Big\}$$

$$S_1 = \varnothing$$

$$S_2 = \varnothing$$

$$S_3 = \Big\{ \{1,2,3\} \Big\}$$

$$S_4 = \Big\{ \{1,2,4\},\ \{1,3,4\},\ \{2,3,4\} \Big\}$$

$$S_5 = \Big\{ \{1,2,5\},\ \{1,3,5\},\ \{1,4,5\},\ \{2,3,5\},\ \{2,4,5\},\ \{3,4,5\} \Big\}$$

*Proof 1 summary*计算基于任何子集的最大索引元素的划分，统计 $[n+1]$ 的 $(k+1)$-元素子集。

这个证明策略是从我们的初始观察中发展而来的，即像 $\binom{n+1}{k+1}$ 这样的二项式系数代表一个 *selection*，识别出 $[n+1]$ 的一个子集。然而，我们也可以通过另一个标准的计数对象集来解释这个系数：二元元组。这将导致对左侧求和的不同考虑。现在让我们深入这个证明！

Proof 2. 让 $n, k \in \mathbb{N}$ 和让 S 为所有恰好有 $k+$ 个 1 的二进制 $(n+1)$ 元组的集合。也就是说，$S \subset \{0,1\}^{n+1}$，并且每个 $T \in S$ 由恰好 $k+$ 个 1 和 $(n+1) - (k+1) = n-k$ 0 个组成。

我们可以直接通过注意到构造 S 的一个元素相当于从 $n+$ 中选择 1 个开放位置，$k+1$ 个位置用 1 填充（然后确定性地将剩余位置用 0 填充）来识别 $|S|$。因此，$|S| = \binom{n+1}{k+1}$。

接下来，我们可以通过根据 *right-most* 1 出现的位置来分类元组来识别 S 的一个划分。具体来说，对于 $i \in [n+1]$，令 S_i 是由那些最右边的 1 出现在位置 i 的元组组成的 S 的子集（从左到右自然读取）。（见证明下面的图，其中展示了 n 和 k 的具体值的情况。）要计算 S_i 的元素数量，我们在位置 i 放置一个 1，然后从左侧的 $i-$ 个 1 位置中选择 k 个作为 1。剩余的位置以确定的方式填充 0。根据乘法原理，$|S_i| = \binom{i-1}{k}$。

现在，我们验证 $\{S_i \mid i \in [n+1]\}$ 是 S 的一个划分。首先，观察当 $i \neq j$ 时，$S_i \cap S_j = \varnothing$；如果 $i < j$，则 S_i 中任何元素的 j-th 位置为 0，但 S_j 中任何元素的 j-th 位置为 1，因此任何 $(n+1)$-tuple 都不能属于两个集合之一。同样地，如果 $j < i$，i-th 位置要么是 1（对于 S_i 的元素），要么是 0（对于 S_j 的元素）。其次，观察 S 的任何元素都有一个最右边的 1，这必须在 1 和 $n+1$ 之间的某个位置发生，因此 S 的每个元素都属于 S_i 个集合之一。

因此，根据求和规则

$$|S| = \sum_{j=1}^{n+1} |S_j| = \sum_{j=1}^{n+1} \binom{j-1}{k}$$

通过将求和索引重新定义为 $i = j-1$，我们可以写出

$$|S| = \sum_{i=0}^{n} \binom{i}{k}$$

and equating the two expressions for $|S|$, we have proved the result. □

Diagram for $n = 4$ *and* $k = 2$:

$$S = \Big\{ \{11100\},\ \{11010\},\ \{11001\},\ \{10110\},\ \{10101\},\ \{10011\},\ \{01110\},\ \{01101\},\ \{01011\},\ \{00111\} \Big\}$$

$$S_1 = \varnothing$$

$$S_2 = \varnothing$$

$$S_3 = \Big\{ \{11100\} \Big\}$$

$$S_4 = \Big\{ \{11010\},\ \{10110\},\ \{01110\} \Big\}$$

$$S_5 = \Big\{ \{11001\},\ \{10101\},\ \{10011\},\ \{01101\},\ \{01011\},\ \{00111\} \Big\}$$

*Proof 2 summary*计算恰好有 $k+$ 个 1 的二进制 $(n+1)$-元组，通过根据最右边的 1 出现的位置进行划分。

我们希望这已经让您对如何以两种方式呈现计数论证有了很好的了解，以及如何通过观察恒等式的形式来尝试提出这样的论证。本小节应为您提供一些练习，并让您尝试本节末尾的练习。如果您发现自己需要更多帮助，我们建议阅读下一节。它描述了一些启发式方法来观察以两种方式计数的问题，并为证明找到一个“合适的”集合 S。这些方法基于我们在本章 earlier 提出的标准计数对象及其相应的公式。

在继续之前，我们想以两种方式呈现一个最终的计数证明，因为我们发现它极其启发人心、巧妙且优雅。我们不期望你能提出这种论点——尤其是因为它不符合我们迄今为止开发的“两种方式计数”证明中对*exactly*的描述——但我们认为它值得一读并为之惊叹，所以请这样做。

Proposition 8.4.6 (高斯配对和)**.** *For any* $n \in \mathbb{N}$*,*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Proof. 首先，观察$\frac{n(n+1)}{2} = \binom{n+1}{2}$。

现在，考虑一个由 $n+$ 行组成的规则三角形点阵，其中第 k 行有 k 个点。左侧的求和表示该数组的“面积”，即这些 n 行中的点总数。

接下来，我们在这些点之间建立一一对应关系，以及 $(n+1)$ 行中的 *pairs* 个点的对应关系。对于任意一对点，向上绘制指向内部的斜线

通过数组获得上一行中的一个唯一点。相反，对于数组中的任何一点，通过数组向下绘制向外指的斜线，以获得底部行中的一对唯一点。因此，$(n+1)$-行中点的对数，即 $\binom{n+1}{2}$，等于上数组的点数，即 $\sum_{k=1}^{n} k$。

□

8.4.3 Standard Counting Objects

我们已经在前一节讨论了几个标准的组合对象。然而，在两种计数方法证明中的一个困难是确定要计数哪些对象！这些练习通常如下提出：“这里有一个恒等式；通过两种计数方法来证明它。” 这并没有给你任何关于要计数什么的想法，只是你需要计数！在本节中，我们将尽力提供一个实用的指南来“解开”组合恒等式并创建两种计数方法的证明。这些想法基于我们的经验和组合学家使用的某些标准论证。

Binomial Coefficients and Multiple Interpretations

这些对象以及任何相应的计数公式已在上一节中介绍，因此我们鼓励您重新阅读任何感觉不熟悉的部分。我们在这里能做的就是强调何时将某个计数对象以某种方式视为与计数两步问题“相关”。例如，回忆一下主席身份，但假装我们还没有证明它：

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

观察到身份只包含二项式系数的乘积（并记住我们总是可以将 k 写作 $\binom{k}{1}$，例如），这表明我们应该尝试计数一些可以用简单的二项式系数轻松描述的东西。最自然的选择是 $[n]$ 的子集；等价地，我们也可以使用从一组人中选出的某个大小的委员会，或者具有 k 个 1 的二进制 n-元组。这三个选择中的任何一个都会为我们提供对表达式中各个项的相对容易的描述，并允许我们将它们联系起来。在那个时刻，我们需要选择我们感觉最舒适的解释，也就是我们最能轻松解释所有项的那个解释。

如果我们选择使用人员和委员会，那么我们可以遵循上面证明中使用的论点。如果我们选择 $[n]$ 的子集，那么我们需要提出一个合理的两步过程来描述等式两边项的乘积。在选择了大小为 k 的子集之后，$\binom{k}{1}$ 项可能代表什么？本质上，我们正在挑选出已经选择的子集中的一个“特殊”元素。这类似于右侧的 $\binom{n}{1}$ 项，我们首先挑选出一个“特殊”元素，然后填充其余的子集。然而，当我们的上下文是 $[n]$ 的子集时，我们不再有“委员会主席”这个术语。（这就是我们感觉

委员会的解释是合理的且易于使用。只需唯一编号所有人，然后我们可以安全地使用这些术语。）这个术语的常见解释可能包括，例如，“圈出”一个元素，以表示它是特殊的。也就是说，等式的两边都会计算包含一个圈出元素的子集 $[n]$ 的大小为 k 的子集。在左侧，我们选择子集然后分配圆圈；在右侧，我们圈出一个元素并将其包含在子集中，然后填写其余的子集。还有其他简单易懂的方法来完成这个论证，但我们想确保指出，“委员会”的术语不适用，除非我们从证明的开始就选择那个设置。（挑战问题：你如何在二进制 n-元组的情况下处理这个证明？提示：考虑允许“特殊”位置被除0或1以外的符号填充。）

也常见到二项式系数的乘积，其中“顶部项”是相同的。例如，考虑如何在两种计数方法的证明中描述如下项，(假装它只是方程的一边；另一边对此讨论无关紧要。)

$$\binom{n}{k}\binom{n}{\ell}$$

有两种合理的方式来描述这类产品，决定使用哪一种将取决于等式的另一侧，或涉及的其它项。我们将在这里展示这两种解释，并让您通过考察上下文来确定使用哪一种。

考虑委员会的上下文，因此每个项以某种方式代表从总共 n 人中选择一个特定规模的委员会（k 或 ℓ）。一种解释是我们从总共 n 人的 $same$ 集合中选择两个委员会。也就是说，也许我们有一个系的 n 名教授，我们需要从中选择 k 名来监督预算和 ℓ 名来监督课程，教授可以可能同时服务于两个委员会。另一种解释是我们从 $different$ 个集合中选择两个委员会，但这两个集合的大小都是 n。也就是说，也许我们有一个班级有 n 名男生和 n 名女生，我们想要从中选择 k 名男生和 ℓ 名女生来组建一个俱乐部。这两种解释中的任何一种都是“正确”的，并且合理使用，但“正确的选择”肯定会取决于所讨论问题的其余部分。

一个在委员会类型论证中很有用的术语是子委员会的概念。由于从n人中选择出的k人组成的委员会已经代表了一个$subset$，子委员会实际上代表了一个子集的子集。因此，如果我们找到一个像这样的术语

$$\binom{a}{b}\binom{b}{c}$$

在一个身份中，我们可能选择将其解释为从 a 总人数中选择 b 人的委员会，然后从这些人中选择 c 人的子委员会 $then$。这可以描述为选择一个俱乐部及其官员，或者一个运动队及其首发阵容，或者类似的事情。

Exponents and Processes

其他术语，除了二项式系数外，在组合恒等式中频繁出现的是指数项：n^3，2^n，n^{k-1}，等等。通常，这些术语的解释将由如何根据恒等式中的其他术语分配上下文来决定。我们在这里介绍一些标准、常见且易于解释的术语解释方法。有趣的是，有时解释可能取决于基数或指数哪个更大！

考虑一个像这样的术语

$$\binom{n}{k}2^k$$

让我们假设我们已经将“委员会”这一解释分配给问题，基于身份的其余部分，并且我们已经声明二项式系数 $\binom{n}{k}$ 代表从 n 名学生中选出 k 人的委员会的选择。那么 2^k 项又代表什么呢？记住，这个项可能来自一个 k 步的过程，其中每一步可以用两种方式之一来完成。由于 k 是所选委员会的大小，因此我们可以简单地描述一个针对委员会每个成员的 2 步决策过程。例如，我们可以给每个委员会成员分配一顶红帽子或蓝帽子；或者，对于每个委员会成员，我们可以选择是否给他/她一颗金星；或者，我们可以强迫委员会成员选择是否成为共和党人或民主党人。如果你愿意，可以发挥创意！当然，所选的解释必须与身份的其余部分相匹配，因此有时一种解释比另一种解释更容易解释。请记住这一点，并且如果你发现难以传达你的想法，愿意回到并更改你的解释。

现在，考虑一个像这样的项

$$\binom{n}{k}2^n$$

再次，假设我们将“委员会”解释应用于这个问题。这与上述情况有何不同？在这种情况下，指数与二项式系数的“最高项”相匹配。因此，选择委员会与随后的 n-步过程没有必然联系。这个项可能描述从 k 个官员中选出的一个，然后是每个学生被分配到A组或B组（无论官员的分配情况）。如果我们 $weren't$ 使用“委员会”解释，这个项可能描述一个恰好有 k 个1的二进制 n-元组，其中一些0和1被圈出。解释的选择将取决于问题的其余部分以及你对解释这些术语的舒适度。

考虑如何使用略有不同的数字来修改这些解释。对于一个像{v*} 这样的术语

$$\binom{n}{k}4^n$$

我们可能描述一个由 k 名成员组成的委员会，每位成员都戴着红色、蓝色、绿色或黄色的帽子。用这样的术语

$$\binom{n}{k}5^n$$

我们可能描述一个恰好有 k 个 1 的二进制 n-元组，其中每个 0 和 1 都有 1、2、3、4 或 5 个圆圈围绕它。

接下来，让我们考察一些基数是变量而指数是固定的术语。例如，考虑一个像这样的项

$$\binom{n}{k}k^2$$

在这种情况下，我们以某种方式从 n 个总对象中选择 k 个对象，并在每一步进行具有 k 个选择的 2 步过程。也就是说，首先选择 k 个对象会影响 2 步过程的第二部分的结果。如果我们处于“委员会”的背景下，我们可能会将这个术语解释为选择一个由 k 人组成的委员会，然后选择委员会的 2 名官员——比如说，一名发言人和一名财务主管——任何委员会成员都可以被选为官员，而且，任何成员都有可能担任这两个官职。

如果我们想使用“元组”解释，我们可能会将这个术语描述为选择一个恰好有 k 个 1 的二进制 n-元组，其中有一个 1 周围有一个圆圈，有一个 1 周围有一个方框（并且可能同一个 1 同时有一个圆圈和一个方框）。我们还可以使用“字母表”解释来描述这个术语。从一个包含 n 个总字母的字母表中，我们可以选择一个包含 k 个字母的子集，然后仅使用这 k 个字母构造双字母词。思考这三种解释以及为什么它们都适用，以及它们是如何相互关联的。尝试用这三种解释之一重写我们的一个证明。还要考虑这些解释在 k^3 或 k^4 的情况下会有何不同。

现在，考虑一个像这样的项

$$\binom{n}{k}n^3$$

在一个“委员会”的上下文中。由于指数项的底数与二项式系数的“最高项”相同，因此$\binom{n}{k}$项所代表的委员会与随后的3步过程之间不一定存在关系。因此，我们可能描述一个k人委员会的选择，然后分配一条红带、一条蓝带和一条绿带，其中一个人可能收到多条带子，任何人（无论是否在委员会中）都可能收到带子（或带子）。我们将把它留给你去构建一个在“二进制n元组”解释下的这种术语的适当解释。试着做一下吧！

Summation means Partition

在组合恒等式中找到 *summation* 是相当常见的。在两种计数方式证明中处理这一点稍微复杂一些，因为一个求和符号代表好几个项。然而，最重要的规则是：一个求和符号始终代表一个 *partition*。特别是，它代表一个划分，并告诉我们所有划分集合的基数。为了在两种计数方式证明中解释这一点，我们始终需要描述三个属性：

- 分区的集合是什么。
- 为什么在总和的索引 *limits* 中的含义是合理的。
- 对于任意索引，为什么对应集合的大小是求和中的项。

我们将通过一个例子来说明这些。

Example 8.4.7. **Pro/Con Committee Identity:**

$$\binom{n}{k}2^{n-k} = \sum_{i=k}^{n}\binom{n}{i}\binom{i}{k}$$

Intuition: 创建一个由k人组成的委员会，从n人中选出。然后，确定非委员会成员是支持还是反对委员会的决定。我们也可以通过首先选出至少k人，他们将加入/支持委员会，并将其他人设定为不加入和反对。然后，从这些人中选出k人实际加入委员会，将其他人设定为支持它。（注意：在构建中，我们必须说明我们将执行的所有步骤。不要假设读者会认为任何事都是显而易见的。）

Proof. 考虑一组 n 人。设 S 为从 n 人中选择 k 人组成委员会的方法，每个不在委员会上的人对委员会有明确的观点，认为 For 或 Against 委员会。

首先，我们可以通过多步骤过程找到 $|S|$：

- 选择 k 名 n 人进入委员会。

  $\mathbf{\binom{n}{k}}$ **options**
- 对于剩余的每个 $n-k$ 人，让他们决定是 For 还是 Against。这是一个有 $n-k$ 个步骤且每步有两个选择的过程，所以通过 ROP ... $\mathbf{2^{n-k}}$ **options**

通过ROP，我们有 $|S| = \binom{n}{k}\cdot 2^{n-k}$。

其次，我们可以通过根据有多少人来建立一个分区来找到 $|S|$。

For 委员会。根据 S 的定义，非委员会成员中的任何一个人到所有人都可以是 For 委员会成员。因此，总的来说，在委员会成员及其 For 支持者之间，我们可以有从 k 到 $k + (n - k) = n$ 的人，包括在内。

对于满足 $k \leq i \leq n$ 的每个 i，令 $S_i \subseteq S$ 为拥有 k 个委员会成员和 $i - k$ For 个支持者的方法集合。（注意 $0 \leq i - k \leq n - k$，这与之前提到的限制相匹配。）

注意 $\{S_i \mid k \leq i \leq n\}$ 是 S 的一个划分。这是因为，对于 S 的任意一个元素，该元素可以通过有多少 For 委员会支持者来表征，这必须是一个特定的数字。现在，我们可以通过一个多步骤的过程找到每个这样的 i 的 $|S_i|$：

- 从所有 n 人中，选择 i 人。这些人是有潜力的委员会候选人。

  $\binom{\mathbf{n}}{\mathbf{i}}$ **options**
- 指定 $n - i$ *other* 人明确成为我们正在构建的委员会的 Against。（这一步是确定性的，所以只有一种方法，但我们需要指出这一点，以完全描述一个属于 S 的结果。）

- 在第一步中选出的 i 人中，选出 k 人作为实际委员会成员。 $\binom{\mathbf{i}}{\mathbf{k}}$ **options**

- 指定上一步未选中的 $i - k$ 人作为委员会的 For 支持者，但不是委员会成员。

  (再次，有一种方法可以做到这一点，但需要完全描述结果。)

通过ROP，我们发现$|S_i| = \binom{n}{i}\binom{i}{k}$。

通过ROS，因此，我们发现$|S| = \sum_{i=k}^{n} |S_i| = \sum_{i=k}^{n} \binom{n}{i}\binom{i}{k}$。

由于我们以两种方式找到了 $|S|$，我们可以将它们等同起来。这证明了该主张。□

注意，在证明中识别出划分后，我们做了几件事情。我们解释了为什么它是一个划分。我们解释了它与求和的索引之间的关系。我们解释了求和中的 *limits* 如何对应于划分并代表所有可能性。然后，对于任意的 i，我们解释了为什么 $|S_i|$ 是求和中的对应项。

8.4.4 Binomial Theorem

我们可以使用这种证明技术证明一个强大且重要的定理，两种方式计数。这将是对该技术的一个有趣应用，但这也是一个有用的结果，正如我们将看到的！

Theorem 8.4.8. *Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. Then,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

我们将解释几种证明此结论的不同方法。

Proof 1. 考虑证明这一点，其中我们假设 $x, y \in \mathbb{N}$。

在这个情况下，想象有一组 $x+y$ 符号；例如，假设我们有 x 个小写字母和 y 个大写字母。那么 $(x+y)^n$ 是由这些符号组成的长度为 n 的字符串的数量。

在右侧，我们根据字符串中有多少位置被小写字母填充来划分所有此类长度 n 的字符串集合。将有从 0 到 n（包含）的位置被从 x 个小写字母集合中的选择填充。对于每个此类 k，其中 $0 \leq k \leq n$，长度为 n 且恰好有 k 个小写字母的字符串数量为 $\binom{n}{k} \cdot x^k \cdot y^{n-k}$，因为我们选择了那些 k 位置用于小写字母，选择如何填充这些位置，然后使用大写字母填充剩余的 $n-k$ 位置。

□

Proof 2. 让我们通过计算“FOILed”展开式中与k个x (选择相对应的项的数量，从而计算从乘积中的因子中选择$n-k$个y)的选择数量，来证明这一点。

考虑乘积

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdots(x+y)}_{n \text{ factors}}$$

考虑通过反复应用分配律来展开这些 {v*} 因子。例如，对于 $n=2$，我们有

$$\begin{aligned}(x+y)^2 &= (x+y)(x+y) = x(x+y)+y(x+y) = x\cdot x + x\cdot y + x\cdot y + y\cdot y \\ &= x^2 + 2xy + y^2\end{aligned}$$

并且，当 $n =$ = 3 时，我们有

$$(x+y)^3 = (x+y)(x+y)(x+y) = x(x+y)(x+y)+y(x+y)(x+y) = \cdots$$

通用思路是这样的：为了在最终产品中找到一个项，我们从每个因子（$x+y$）中选择一个x或一个y。每个这样的项看起来像$x^k \cdot y^{n-k}$，其中k是介于0和n之间的某个数。我们所需做的就是确定有多少个$ways$可以创建一个像$x^k \cdot y^{n-k}$这样的项。这相当于找出从n个因子中选择k个因子的方法数，并说我们从这些因子中选择了“x”，从其他$n-k$个因子中选择了“y”。根据选择的定义，有恰好$\binom{n}{k}$种这样做的方法！

□

Proof 3. 我们也可以通过归纳法来证明这一点！**Pascal's Identity**在归纳步骤中是必不可少的。这将在练习8.9.14中向您展示。 □

Example 8.4.9. 让我们展示这个定理的用途。

- 应用二项式定理以证明

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Proof. 使用 $x = 1$ 和 $y = 1$。 □

这就可以了！我们已经通过归纳法证明，然后通过两种方法的计数论证，现在从这个强大的定理中得出一个结果 *immediately*。

- 证明 $[n]$ 中奇数个数的子集数量等于 $[n]$ 中偶数个数的子集数量；即，

$$\sum_{k=0}^{\lceil n/2 \rceil - 1} \binom{n}{2k+1} = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}$$

可以通过找到偶数个元素子集集合与奇数个元素子集集合之间的双射来证明这一点。我们甚至可以用计数论来解释这一点。

相反，让我们在两边都减去，并将等式重写为

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

注意这正是二项式定理所说的，其中 $x = -1$ 和 $y = 1$。太惊人了！

8.4.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 什么是 **counting in two ways** 参数的整体方法?

(2) 为本节每个例子证明写一个简短的 *proof summary*。

(3) 当在拟证明的恒等式中存在求和时，在随后的两种方式证明中我们必须讨论什么?

(4) 我们证明了求和恒等式的不同方法有哪些？它们在本质上有什么相同之处?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 设 $\ell, k, n \in \mathbb{N}$ 已知。证明

$$\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{-\ell}$$

通过两种计数方式的论证。

(2) 证明以下公式：{v*}

$$n \cdot 2^{n-1} = \sum_{k=1}^{n} \binom{n}{k} \cdot k$$

通过两种计数方式的论证。

(3) 证明

$$3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} = \sum_{k=0}^{n} \binom{n}{k} 2^k$$

通过两种计数方式的论证。

(Hint: 考虑使用三元字符串集合。**)**

然后，解释它如何从二项式定理中得出，也是如此。

(4) 通过两种计数方法论证 $k^2 = \binom{k}{1} + 2\binom{k}{2}$。

应用 **Summation Identity** 以推导出

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

(5) 用两种方法计数证明以下 **Geometric Series Formula**：

$$\forall q \in \mathbb{N} - \{1\}\,.\, \forall n \in \mathbb{N}\,. \quad 1 + q + q^2 + q^3 + \cdots + q^{n-1} = \sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}$$

(注意：此公式实际上对任何 *real* 数 $q \neq 1$ 都成立，但两种计数方式的证明我们只适用于 *natural* 数 $q \neq 1$。要证明实值版本，使用归纳法.)

(**Hint:** 考虑由 q 个元素组成的所有 n-元组集合，除了一个特定的……)

8.5 Selections with Repetition

8.5.1 Motivation

当我们推导出 *arrangements* 和 *selections* 的公式时，我们注意指出是否允许我们 **repeat** 对象。当时，我们省略了推导选择对象 *with repetition* 的方法数公式。具体来说，在解决这个问题之前，我们需要开发——并且熟悉——*counting in two ways* 的技术。现在，我们准备好了！

Example 8.5.1. 假设我在厨房的柜台上有一个装满水果的盒子。里面有一堆苹果、香蕉和桃子。让我们假设每种至少有10个。我伸手进去，拿出5个水果，在学校的一天里享用。我可能有多少种不同的组合可以拿?

为了这个例子，我们假设任何两个苹果，比如，对我来说都是 *indistinguishable*。它们没有一个是偏色的，也没有比其他苹果小得多，或者类似的情况。在这个假设下，这个问题是关于从3 **types** 个对象中选取 **selecting** 个对象。结果是 *unordered* (，所以这是一个选择，而不是排列)，并且我们可以从任何类型中选择对象（即我可以挑选几个香蕉）。

例如，我们可以挑选4个苹果和1个桃子，或者5个香蕉，或者1个苹果和2个香蕉以及2个桃子。

这代表了这类问题最一般的形式。给定若干个 **types**，我如何从这些类型中选出一些总数量的对象？在找到这类问题的公式之前，让我们看看另一个例子。实际上，这就是我们将用来推导公式的解释！

Example 8.5.2. 假设我们有 n 枚不可区分（相同的）金币要分给 k 个可区分（不同且标记的）海盗。我们有多少种分法?

尝试用这个方法处理 n 和 k 的较小值。实际上，拿一些五分硬币和一些朋友，试着解决它。如果你有 $n = 5$ 枚硬币和 $k = 3$ 个朋友，有多少种分配硬币的方法?

请注意，海盗是 *distinguishable*。例如，给红胡子船长2枚硬币和黑胡子船长10枚硬币与给红熊10枚和黑胡子2枚的结果相同。我们应该单独计算这些。

同时，请注意硬币是 *indistinguishable*。这意味着我们分发硬币的方式，或者在哪里分发，或者类似的事情，都无关紧要。重要的是最终结果，他们最终都去了哪里。例如，给红胡子5个硬币，然后给黑胡子5个，然后给红胡子另外2个……这和只给红胡子7个硬币，黑胡子5个是一样的。我们应该将这些视为相同的结果。

尝试使用这些示例，并找到一个解决这些问题的公式。你能推广到任意的 n 和 k 吗？你能证明你的说法吗?

试试吧！然后，阅读下一节以了解我们的公式和 p 屋顶。

8.5.2 Formula

我们将通过考虑海盗与黄金的例子来推导出重复选择的公式。首先，让我们解释为什么这类似于重复选择：

假设我们是这个场景中的 *gold distributor*。我们坐在一张桌子旁，周围坐着 k 个海盗，旁边放着一个装满 n 金币的袋子。我们可以通过逐个分发金币来选择如何分配金币。当我们选择将一枚金币给海盗 #i (，出于某种 $i \in [n]$) 的原因时，我们是在从 k 个不同的 *types* 海盗中挑选这个海盗。最终，要分发 n 枚金币，我们需要做出 n *selections*。因此，我们总共从 k 种类型中选择了 n 个对象，并且允许我们 *repeatedly* 选择一个类型。

Derivation

想象一下，把我们的 n 枚硬币摆放在桌子上，排成一行。为了将它们分给 k 名海盗，我们需要放置“分隔符”或“条杠”，将金币分成 k 堆。然后，海盗1将拿走左边的堆，海盗2将拿走下一堆，以此类推。

这个“分隔符”参数使我们能够方便地计算完成此过程的方法数量！为了将n块金币分配给k个不同的海盗，我们需要有n枚金币，由$k-$个分隔符分开。想想为什么我们在这里只需要$k-$个分隔符。很容易看出为什么我们只需要1个分隔符来将一排金币分成两堆。然后，我们可以看到2个分隔符将它们分成3堆。一般来说，一旦我们已经放置了$k-$个分隔符，就有k堆已经建立；我们不需要在行的end处放置一个最终的分隔符来表示最右边的堆属于海盗#k。

Example 8.5.3. 例如，当 $k = 3$ 和 $n = 7$ 时，我们可能会有如下分布：

○ | ○ ○ ○○ | ○○

在这种情况下，海盗#1获得1金币，海盗#2获得4金币，海盗#3获得2金币。

请注意，这是以下结果中的 *different*：

○ ○ ○○ | ○○ | ○

在这个情况下，海盗#1获得4金币，海盗#2获得2金币，海盗#3获得1金币。

我们也可以让一些海盗获得0金币：

○ ○ ○ ○ ○ | ○○ |

这里，海盗#1获得5金币，海盗#2获得2金币，海盗#3获得0金币。

这些观察告诉我们什么？嗯，这意味着任何金币分配都对应于长度为 $n+k-$ 的字符串，其中恰好有 n 枚金币和恰好 $k-$ 个分隔符。这两个对象（金币分布和分隔符放置）之间存在一个 $bijection$ 关系：给定一个金币分布方案，我们可以构建相应的分隔符排列。（例如，如果我们被告知海盗1将获得5枚金币，海盗2将获得2枚金币，海盗3将获得0枚金币，我们将在上面最后一个例子中构建分隔符排列。）同样，给定一个分隔符排列，我们可以读取它并确定它对应的金币分布方案。

这个双射告诉我们，要计算分配黄金的方法数，我们只需要计算可能的分隔符排列的数量。我们可以很容易地计算这些！分隔符排列只是一个长度为 $n+k-$ 的 1 的字符串，恰好有 $k-$ 个分隔符。这是因为我们需要 n 个黄金和 $k-$ 个分隔符，所以 $n+k-$ 个位置，总共。因此，根据选择的定义，有

$$\binom{n+k-1}{k-1}$$

构建此类安排的方法！

（你可能也听说过这个论点被称为“星星和条形”。这只是对这个问题的另一种常见解释，其中金币被星星所代替，分隔符被条形所代替。）

由于这种排列集合与黄金分配集合之间的双射，我们得出结论，$\binom{n+k-1}{n}$ 是我们可以分配黄金的方式数量！

我们已经知道$\binom{n}{k} = binn-k$在一般情况下，因此我们可以将其应用于此处，并推断出黄金分配的数量也是

$$\binom{n+k-1}{n}$$

但我们已经在我们的推导中看到了这一点。我们需要构造一个长度为 $n+k-$ 的 1 字符串，其中包含 $k-$ 个 1 分隔符（剩余位置为金币）。等价地，我们需要一个长度为该长度的字符串，其中包含 n 个金币（剩余位置为分隔符）。

8.5.3 Equivalent Forms

在继续解决这个新公式的一些问题之前，让我们考虑一下基本 $selections\ with\ repeti\text{-}\ tion$ 问题的一些 **equivalent formulations**。无论你遇到涉及这些概念或公式的任何问题，你可能都会考虑应用我们刚刚推导出的公式，以某种方式。

Pirates & Gold

这是我们推导公式的原始公式，所以当然适用于这种情境。一般来说，我们只需要知道海盗的数量和金币的数量。

金子 n 个相同件在 k 个可区分的海盗之间分配的方法数是 $\binom{n+k-1}{k-1}$。

在我们的推导中隐含的是，海盗可能实际上会收到0金币，请注意这一点。有些问题可能会要求你考虑分布中的其他*conditions*。例如，如果每个海盗都必须收到*at least one*金币怎么办?

Integer Sums

考虑将海盗与金币问题重新表述如下。让我们定义 $x_i \in \mathbb{N} \cup \{0\}$ 为海盗 #v12 在分配中获得的金币数量。问题的条件要求

$$\forall i \in [k] \text{.}\ x_i \in \mathbb{N} \cup \{0\}$$

并且那

$$\sum_{i=1}^{k} x_i = x_1 + x_2 + x_3 + \cdots + x_k = n$$

啊！如果我们询问关于方程中 **solutions** 的数量会怎样呢? 这正好（以 *bijective* 的方式）对应于解决海盗与黄金问题的方法。给定这个方程的解，我们只需给海盗 #i 精确 x_i 份黄金。这给我们提供了另一种表述问题的方法:

方程 $x_1 + x_2 + \cdots + x_k = n$ 的解的个数满足条件 $\forall i \in [k]$。 $x_i \in \mathbb{N} \cup \{0\}$ is $\binom{n+k-1}{k-1}$.

Balls and Bins

如果我们被给出 n 个相同的球，并被要求将它们放入 k 个不同的箱子中。（箱子是可区分的，所以让我们说它们被标记为从 1 到 k。）我们有多少种方法可以做到这一点? 这很容易与前面的公式联系起来！设 $x_i \in \mathbb{N} \cup \{0\}$ 为最终落在编号为 i 的箱子中的球的数量。那么，与上面的问题相同的条件也适用于这里。

n 个相同的球分配到 k 个可区分的箱子中的方法数是 $\binom{n+k-1}{k-1}$ 。

Indistinguishable Dice

考虑掷n *identical*个骰子。有多少种结果？这与掷可区分的骰子（例如，骰子颜色不同）是相同的。相反，这个过程的结果是一个*unordered*显示在面上的数字列表。

例如，如果我们掷了3个不可区分的6面骰子，这个过程的一个结果可能是**unordered**列表（1, 3, 3）。为了思考这个问题，假设你的朋友走进另一个房间掷了3个骰子，然后回来告诉你发生了什么。如果他这么说“我掷了一个1和两个3”，那么你并没有了解到*which*个骰子显示了哪个数字。（这与他说“我在第一个骰子上掷了一个1，然后在第二个和第三个骰子上各掷了一个3”的情况形成对比。）通过询问不可区分的骰子的结果数量，我们实际上是在询问你的朋友可能给你多少种不涉及*order*中掷骰子出现的可能回答。

我们可以将此与“球和箱子”公式联系起来，通过掷所有骰子并将它们根据点数放入6个编号的箱子中。等价地，为了描述此过程的输出，我们需要知道有多少个骰子显示了1，有多少显示了2，等等。我们不在乎（也无法知道！）*which*个骰子显示了哪些数字；我们只需要知道*how many*显示了每个数字。

掷n个不可区分的k面骰子的结果数量是$\binom{n+k-1}{k-1}$。

8.5.4 Examples

让我们练习使用这个新推导的公式来解决一些问题！在这个过程中，我们将考察几个基本结果的不同表述。

Example 8.5.4. 假设我们有 $n = 20$块金币要分给 $k = 3$个海盗。假设海盗是红胡子船长（哈利尔·阿丁，奥斯曼人）、黑胡子船长（爱德华· Teach，英国人）和基德船长（苏格兰人）。

让我们找出在特定条件下分配金币的多少种方式：

(1) 总共有多少种方法?

这就像从3种类型中选择20个对象，允许重复。每次我们选择一个海盗，就意味着我们给他一块金币。

根据上述选择公式，有

$$\binom{20+3-1}{20} = \binom{22}{20} = \frac{22 \cdot 21}{2} = 231$$

方法来完成这个。

(2) 有多少种方法可以确保每个海盗至少得到2件物品?

让我们立即每人给两块金币。然后，我们剩下$20-6=14$块金币要分给所有3个海盗，所以有

$$\binom{14+2}{14} = \binom{16}{14} = \frac{16 \cdot 15}{2} = 120$$

这种方法。想想为什么这样做有效。我们实际上是在重新定义“获得0金币”的含义。我们不是从20枚金币开始，担心是否每个人都能得到$at\ least$两枚金币，我们只需立即确保满足这个条件，然后分配剩余的金币。

(3) 有多少种方法可以确保红胡子和大胡子至少得到2个，基德至少得到6个?

就像上一个一样，让我们给Redbear和Blackbeard每人2件，给Kidd 6件。这样我们就剩下$20-4-6=10$件要分给所有3个海盗，所以有

$$\binom{10+2}{10} = \binom{12}{10} = \frac{12 \cdot 11}{2} = 66$$

方法来完成这个。

(4) 有多少种方法可以确保Redbeard和Blackbeard至少得到2个，而Kidd不超过2个?

有几种方法可以处理这个问题。

(i) 基于基德获得0、1或2枚金币的情况建立案例。在每种情况下，我们立即给红胡子和大胡子每人2枚金币，然后给基德相应数量的金币（0、1或2）。这让我们剩下16、15或14枚金币要分给前两个海盗$only$，因此有

$$\binom{16+1}{16} + \binom{15+1}{15} + \binom{14+1}{14} = 17+16+15 = 48$$

(ii) 让我们考虑确保Redbeard和Blackbeard每人至少获得2枚金币的方法有all种，然后从这些方法中找出Kidd获得过多金币，即至少3枚金币的方法有$remove$种。

如果我们给红/黑胡子每人2金币，那么我们就剩下16个金币要分给所有3个海盗，所以有

$$\binom{16+2}{16} = \binom{18}{16} = \frac{18 \cdot 17}{2} = 153$$

步骤的做法。

然后，如果我们给红/黑胡子每人2金币，给基德3个金币，然后将剩余的13个金币分给所有3个海盗，那么就有

$$\binom{13+2}{13} = \binom{15}{13} = \frac{15 \cdot 14}{2} = 105$$

步骤的做法。我们想要从之前的计数中 $remove$ 这些可能性。因此，总共

$$\binom{18}{16} - \binom{15}{13} = 153 - 105 = 48$$

给Redbeard和Blackbeard每人至少两个，但给Kidd不超过2个。

(看，两种方法都得到相同的答案！)

Example 8.5.5. 考虑以下方程:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 25$$

让我们确定这个方程的解的数量，其中每个变量 x_i 是一个非负整数。我们将施加某些条件，并计算满足这些条件的解的数量。

(1) 总共有多少个解?

应用我们推导出的公式，我们看到有

$$\binom{25 + (5-1)}{5-1} = \binom{29}{4}$$

(2) 满足 $x_1 \geq 4$ 的有多少个解?

这正是要求红发船长获得$at\ least$ 4枚金币。我们将预先将4个“计数”分配给变量x_1，然后将剩余的21个“计数”分配给所有五个变量。

更正式地，我们定义 $y_1 = x_1 - 4$。条件只需要 $y_1 \geq 0$。因此，我们正在尝试解这个方程

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 = 25 &\iff (x_1 - 4) + x_2 + x_3 + x_4 + x_5 = 21 \\ &\iff y_1 + x_2 + x_3 + x_4 + x_5 = 21 \end{aligned}$$

应用公式，我们看到有

$$\binom{21+(5-1)}{5-1} = \binom{25}{4}$$

这样的解决方案。

(3) 满足 $x_1, x_2 \geq 5$ 和 $x_3, x_4, x_5 \geq 2$ 的解有多少个?

使用与上次完全相同的方法，我们看到我们正在尝试解决

$$y_1 + y_2 + y_3 + y_4 + y_5 = 9$$

在 $y_i = x_i - 5$ 对 $i = 1, 2$，以及 $y_i = x_i - 2$ 对 $i = 3, 4, 5$。右侧已更改为 $25 - 5 - 5 - 2 - 2 - 2 = 9$。根据公式，我们知道有

$$\binom{9+(5-1)}{5-1}$$

这样的解决方案。

(4) 满足 $x_2 \leq 5$ 的解有多少个?

我们可以用两种方式之一来做这件事。首先，让我们取总的解的数量（在示例的第一部分找到）和 *remove* 满足这个所需条件的解的数量。也就是说，让我们取满足 $x_2 \geq 6$ 的解的数量，这将是

$$\binom{(25-6)+(5-1)}{5-1} = \binom{23}{4}$$

从总数中移除它，得到

$$\binom{29}{4} - \binom{23}{4}$$

其次，我们可以将其写成求和形式，找出满足 $x_2 = \ell$，对于 $0 \leq \ell \leq 5$ 的解的数量：

$$\sum_{\ell=0}^{5} \binom{28-\ell}{3} = \binom{28}{3} + \binom{27}{3} + \binom{26}{3} + \binom{25}{3} + \binom{24}{3} + \binom{23}{3}$$

有趣的是，如果我们只想到用第二种方法解决这个问题，我们仍然可以将表达式 *reduce* 到第一种。我们只需要使用求和恒等式！观察一下

$$\begin{aligned}\sum_{\ell=0}^{5} \binom{28-\ell}{3} &= \binom{28}{3} + \binom{27}{3} + \binom{26}{3} + \binom{25}{3} + \binom{24}{3} + \binom{23}{3} \\ &= \sum_{k=0}^{28} \binom{k}{3} - \sum_{k=0}^{22} \binom{k}{3} \\ &= \binom{29}{4} - \binom{23}{4}\end{aligned}$$

整洁，对吧?

8.5.5 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 选择与带重复的选择有什么区别?

(2) 从 k 个对象中选择 n 个对象的方法数是多少？（注意这里的字母！）

(3) 从 k 种类型的对象中选择 n 个对象的方法有多少种?

(4) “海盗与黄金”和“整数和”公式 *equivalent* 是如何的?

(5) 修改我们用来推导公式 $\binom{n+k-1}{k-1}$ 的论点，并使用它来证明相同的公式计算“整数和”公式的解的数量。

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 一家服装店制作5种不同颜色的衬衫（红色、绿色、蓝色、白色和黑色）。

(a) 我们需要购买10件衬衫。我们如何做这件事，假设我们可以订购每种颜色的任意数量的衬衫（即每种颜色的供应量是无限的）？(b) 我们需要获得一些衬衫，10件、11件或12件，我们还不确定。我们如何做这件事，再次假设每种颜色的供应量是无限的？(c) 我们需要获得10件、11件或12件衬衫，但在每种情况下，我们每种颜色至少需要1件衬衫。我们如何做这件事？(d) 现在，我们需要订购25件衬衫，但被告知只剩下3件红色衬衫（而其他颜色仍然有无限的供应）。我们如何做这件事？(e) 现在，我们仍然需要订购25件衬衫，但被告知只剩下3件红色衬衫和5件蓝色衬衫（而其他颜色仍然有无限的供应）。我们如何做这件事?

(2) 考虑掷20个不可区分的骰子。

(a) 总共有多少种结果？(b) 每个数至少出现两次的有多少种？(c) 至多有三个6的有多少种？(d) 至少有四个6的有多少种？

(3) 以下主张的“证明”有什么问题?

考虑4个硬币桶：一个桶里有便士，一个桶里有镍币，一个桶里有一角硬币，还有一个桶里有25美分硬币。每个桶里都有超过50枚硬币（所以我们不必担心任何类型的硬币会用完）。

我们想要从这些桶中选出50枚硬币；我们想要确保至少选出10枚便士和至少10枚镍币，但最多只能有10枚一角硬币和最多10枚25美分硬币。

Claim: 这个方法的方式数量是

$$\binom{53}{3} - \binom{11}{3} = 23261$$

Proof: 考虑从4种类型中选择50枚硬币的总方法数，没有任何附加限制。这是从4种类型中选择$k = 50$个对象，因此有$\binom{53}{3}$种方法可以这样做。

现在，我们想要从这个总数中减去选择硬币的方式数量，其中我们确实选择了至少10个便士和至少10个镍币，但也至少有11个一角硬币和至少11个五分硬币。为了计算这些选择，我们实际上只需要选择所有这些硬币（总共有42个），然后从四种类型中选择另外8个。我们知道有$\binom{11}{3}$种方式从$n = 4$种类型中选择$k = 8$个对象。

从第一个数减去第二个数，我们得到所声称的数。

8.6 Pigeonhole Principle

8.6.1 Motivation

这是我们在之前暗示过的一个结果。我们甚至在我们第一次学习证明技术时，就证明了它的一个特定 $version$！（参见示例4.9.2。）一般思路是这样的：

如果我们把太多的“东西”放进太少的“箱子”里，那么某些箱子就会装满“东西”。

这当然非常非正式，但它应该能帮助你看到它可能在哪里有用。

鸽巢原理在以下情况下很有用，例如，当我们有一堆落入一定数量类别的对象时。如果我们知道我们有多少个对象，以及有多少可能的类别，那么我们可以保证某些类别中有 *existence* 个对象，其中包含 *at least* 个特定数量的对象。

Example 8.6.1. 这里是一个应用该原则的典型示例：

Of any 3 people, two must have the same sex.

注意，这并不是说 *which* 性别至少出现两次。它只是保证了此类 *existence* 的存在。为了使你自己相信这个事实，你可以列出所有可能性（其中 M 代表男性，F 代表女性）：MMM, MMF, MFF, FFF。在每种情况下，*at least one* 性别的出现次数都是两次（或更多）。

这里是一个与上述陈述逻辑等价版本 nt:

如果我们抛3枚硬币，至少有两枚必须显示相同的面。

这里是一个与上面类似的陈述：

如果我们掷7个骰子，至少有两个必须显示相同的数字 r.

你开始看到这个一般想法了吗？这里是对这些主张的另一个版本，以及过渡到下一部分，在那里我们陈述并证明一个通用版本。

如果我们有 $n+1$ 张纸要放入 n 个不同的抽屉中，一些抽屉最终会至少有 2 张纸。

这是“鸽笼”一词的词源起源：它是指你会在老式翻盖桌上找到的抽屉。我们宁愿不去想将温顺的生物粗暴地塞进小小的盒子！

8.6.2 Statement and Proof

有两个版本的这一原则，所以我们将分别陈述和证明它们。第一个版本是我们将在组合问题中使用的方式。

Theorem 8.6.2 (鸽巢原理)**.** *(1) If a set S with $|S| = n$ is partitioned into k disjoint subsets whose union is S, and if $k < n$, then* 至少一个 *of the subsets in the partition has more than one element. Furthermore, that part actually has at least $\lceil \frac{n}{k} \rceil$ elements.*

(That is, if we separate n objects into k piles, there must be one pile with at least $\frac{n}{k}$ objects in it.)

(2) If $x_1, x_2, \ldots, x_n$ are real numbers with the property that $\sum_{i=1}^{n} x_i \geq z$, then there is at least one index i such that $x_i \geq \frac{z}{n}$.

(That is, if we have n real numbers, there must be one number that is at least as large as the average).

Proof. AFSOC $k < n$ 和 S 被划分为 $S_1, \ldots, S_k$，这些划分也满足 $|S_i| < \frac{n}{k}$ 对于每个 i。由于这些集合构成了 S 的划分，因此我们有

$$n = |S| = \sum_{i=1}^{k} |S_i| < \sum_{i=1}^{k} \frac{n}{k} = n$$

所以 $n < n$。这是一个矛盾！※

AFSOC 所有数字 x_i 都满足 $x_i < \frac{z}{n}$。然后，

$$z = \sum_{i=1}^{n} x_i < \sum_{i=1}^{n} \frac{z}{n} = n \cdot \frac{z}{n} = z$$

所以 $z < z$。这是一个矛盾。※ □

注意这些证明多么相似！它们在代数上看起来完全相同。确实，它们代表了相同的基本思想。

8.6.3 Examples

让我们直接深入探讨如何在使用组合数学问题中应用鸽巢原理。我们将通过一些练习示例向您展示它是如何工作的。一般来说，关于使用鸽巢原理的 *hardest* 部分实际上是在决定“鸽巢”究竟是什么！

Example 8.6.3. 在8个人中，今年一定有两个人的生日在同一天。另外，在13个人中，一定有两个人的生日在同一个月。

对于第一个主张，我们可以将我们的“鸽巢”视为一周的7天。将8个人根据他们今年生日所在的星期几进行划分，我们发现有8个对象进入7个部分。因此，至少有一个部分有$\frac{8}{7}$个对象。由于我们正在处理*whole*个对象，这实际上意味着某个部分至少有2个对象。

一个类似的论点适用于第二个主张。我们只需使用年份的12个月作为我们的“鸽巢”。

Example 8.6.4. 在纽约市，至少有8个人的头发数量完全相同。

这是从知道一些事实中得出的。首先，科学家估计人类头部有10万到15万根头发。让我们保守一些，将这个范围扩大到0到100万。其次，纽约市大约有8

百万人。通过将我们的“鸽巢”定义为从0到100万（基于每个人头上的毛发数量），我们得到结果。

(事实上，这个论点可能并不必要。我打赌我们很快就能在城市里找到8个秃头的人！）

Example 8.6.5. 回顾第1.4.4节，我们调查了在更大的群体中找到一组共同朋友的问题。在那个问题的解决方案中，我们实际上使用了鸽巢原理！我们有5个对象被任意地分成了2个类别。这使得我们推断出$some$类别至少有3个对象。

Example 8.6.6. 假设有 n 名高尔夫球手 ($n \geq 2$) 在一场循环赛制的比赛中竞争，问有多少场比赛？在这些比赛之后，是否必须存在两名高尔夫球手拥有完全相同的胜负次数？如果不是，你能提出哪些条件来保证这一点？

使用计数论证，我们发现 $\frac{n(n-1)}{2}$ 场比赛被进行。（为什么？你能填补细节吗？试试！）然而，我们无法 $guarantee$ 记录相同的人。例如，假设 $n = 3$，并且玩家1输给了其他人，玩家2打败了玩家1但输给了玩家3，玩家3打败了其他人。这分别产生了 0-2、1-1 和 2-0 的记录，我们看到没有任何一个是相同的。

现在，如果我们施加条件 $no\ one\ is\ undefeated$，那么我们 can 保证两名玩家有相同的战绩。每位玩家打 $n - 1$ 场比赛（与除自己外的每个人打一场比赛）。由于没有人是无敌的，没有人有 $n - 1$ 胜。因此，每位玩家可能的胜利次数是 0 或 1 或 2 或 ... 或 $n - 2$。这里有 $n - 1$ 种选择。根据鸽巢原理，在 n 名玩家中，必然有两个这些胜利次数是重复的！

Example 在任意一组 m 个不同的自然数中，至少存在两个这样的数，它们的和或差是10的倍数。

找到使此声明有效的小于等于 m 的最小值。

通过尝试一些小案例，我们可以看到$m \leq$6将会not工作。即使有$m =$6，我们也可以选择数字集合$\{1, 2, 3, 4, 5, 10\}$。注意，其中任意两个数的和/差都不是10的倍数。（注意：我们不允许简单地重复选择相同的数字，比如$5 - 5 = 0$或$5 + 5 = 10$，以得到10的倍数。）

可能是 $m = 7$ 是我们要找的数字吗？让我们来证明它！

假设我们有一个任意的7个自然数的集合。让我们将它们分配到按最后一位数字分类的鸽巢盒中（即，根据满足 $x \equiv n \bmod 10$ 的最小正值 x 将每个数字 n 放入一个盒子中，如下所示：$\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}, \{0\}$。也就是说，我们有6个盒子。

因为我们有7个数字，所以某个盒子中有两个数字。这意味着这些数字的最后一位数字相加除以10余数为0（例如2和8或5和5），或者这些数字的最后一位数字相同，因此它们的差除以10余数为0。无论如何，我们都有一个除以10余数为0的和或差，即10的倍数。

8.6.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 空心原理的两个版本是什么?

(2) Wh 在证明技术中，我们使用了将 $prove$ 鸽巢原理的证明技术 原则?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你!

(1) 假设数学系有5位教授。每年选择2位教授教授《数学概念》。系里可以连续多少年不重复选择相同的两位教授? 通过展示这样一个长度的序列，以及引用鸽巢原理来证明，任何比any更长的序列必然使用到重复的配对。 (2) 考虑 $n \in \mathbb{N}$和集合[2n]。假设我们有一个大小为$|S| = n + 1$的集合$S \subseteq$ [2n]。证明必须存在两个元素$x, y \in S$是$relatively\ prime$的。 (3) 假设我们有一个边长为1 km $\times$ 1 km的正方形公园。我们想在公园上建一个高尔夫球场，但我们只有5个洞的空间。特别是，出于安全考虑，我们需要考虑实际杯子的位置（地面上的洞）之间的距离。证明无论我们如何放置5个洞，必然存在两个洞之间的距离d满足 $d \leq \frac{\sqrt{2}}{2}$ km。 （注意：我们可以在公园的边界上放置一个洞。）

接下来，证明这个界限是 $optimal$; 也就是说，展示一种放置5的方法

公园地面上有孔（再次，允许边界）使得任意两个孔之间的距离大于或等于 $\frac{\sqrt{2}}{2}$ 公里。

8.7 Inclusion/Exclusion

8.7.1 Motivation

包含-排除原理是一个实用的结果，有助于确定如何从大集合中提取*remove*个集合并计算剩余的元素。我们已经在简单形式中看到了它的应用。如果我们有 $A \subseteq U$，并且我们想找到$|U - A|$，我们只需计算$|U|$和$|A|$并从中减去。这是通过对集合U的划分$\{A, U - A\}$应用求和规则得出的。

如果我们从一个较大的集合中移除两个集合会发生什么？如果它们以某种方式重叠呢？我们必须考虑这一点吗？如果我们移除三个集合呢？或者四个集合？或者 n 个集合？我们能否写出一个通用的表达式来表示剩余元素的数量？我们能否用它来解决计数问题？

这里是一些描述“小案例”的表述。假设我们有一个全集 U 和一些子集 $A_1, A_2, \ldots, A_n \subseteq U$。我们想要计算所有 A_i 集合的 *outside* 的 U 的元素数量。我们可以通过以下方式实现：{v*} 保持不变。

$$\begin{aligned} |U - A_1| &= |U| - |A_1| \\ |U - (A_1 \cup A)2)| &= |U| - |A_1| - |A_2| + |A_1 \cap A_2| \\ |U - (A_1 \cup A_2 \cup A_3)| &= |U| - |A_1| - |A_2| - |A_3| \\ &\quad + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| \end{aligned}$$

你看到为什么这些方法有效吗？试着想一个元素 $x \in U$，并考虑它属于多少个 A_i 集合。这个元素在左右两边的表达式中会被计算在哪里？它在两边是否被正确地计算了适当次数？你能看到如何推广这个想法吗？

可能有助于将这些表达式视为“猜测”正确的计数，然后不断“修正”以调整过度/不足计数。例如，我们可以如下推导出上面的最后一个表达式：

> 让我们找到 $|U - (A_1 \cup A_2 \cup A_3)|$。让我们取 U 中的元素数量并减去集合 A_1, A_2, A_3 中的元素数量。
>
> 哦，糟糕！关于属于集合 *two* 的元素怎么办。我们已经多次从我们的计数中移除了这些元素，所以我们应该将属于两个集合交集的元素数量加回来。
>
> 哦，糟糕！关于属于所有 *three* 集合的元素。我们现在已经多次将它们添加回去了，所以我们需要再次移除它们。

您现在可能已经看到如何将这些表达式推广到任意数量的集合，并证明它们。这就是我们在下一节将要做的。

8.7.2 Statement and Proof

Theorem 8.7.1 (包含/排除). *Suppose we have a universal set U and some subsets $A_1, A_2, \ldots, A_n \subseteq U$. Then,*

$$|U - (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{S \subseteq [n]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right| \qquad \text{where} \quad \bigcap_{i \in \varnothing} A_i = U$$

(尝试将上述表达式在 $n =$ = 1、$n =$ = 2 和 $n =$ = 3 的情况下写出来，以了解为什么它们与我们在上一节中写下的相同。

为了 *prove* 这个定理，我们将应用两种方式的计数论证。具体来说，我们将考虑一个元素 $x \in U$ 并论证它在上述方程的两侧被计数了 *correct* 次。

Proof. 设 $x \in U$ 为任意且固定的。我们将考虑两种 案例。

首先，假设对于每个 $i \in [n]$，有 $x \notin A_i$。那么左侧恰好计算 x 一次，因为 x 不是 A_i 集合的并集的元素。右侧只计算项中的 x，因为 x 不是任何 A_i 集合的元素，因此它不是任何 *intersections* 的元素。因此，右侧也恰好计算 x 一次。

其次，假设 x 是一个集合中的一个元素（或多个）的 A_i 集合之一）。这意味着，在左侧被一次计数，为了帮助说明也在右侧被 次计数，让我们定义 [] 为满足 ，即 的索引集合 。

考虑求和项中的本质 这些术语将 *not* 对 x 。对于任何 $S \subseteq [n]$，如果 $S \not\subseteq B$（即存在 $i \in S$ 使得 $i \notin B$，这是因为存在某个 $i \in S$ 使得 $x \notin A_i$，但并非所有满足 $x \in A_i$ 的索引 ）这意味着 x 在求和项中被计算了 0 次，这些项满足 $S \not\subseteq B$。

接下来，根据之前已证明的结果，我们知道 B 的奇数大小子集与偶数大小子集的数量相等。对于任何这样的子集 $T \subseteq B$，我们知道 $x \in \bigcap_{i \in T} A_i$。现在，如果 $|T|$ 是偶数，那么这个项将是正的，所以 x 会被计算一次；如果 $|T|$ 是奇数，那么这个项将是负的，所以 x 会被从计数中减去一次。由于这些项的数量相等，我们可以看到 x 由这些项计算了 0 次。

总体而言，我们已经表明任意元素在方程的两边均被计数了*same* (和*correct*)次，无论如何。 □

有时，会出现所有 k-许多 A_i 集合的交集都具有 *same size* 的情况。在下一节中，我们将看到一些例子是这样的。在这种情况下，上述表达式中的许多项可以 *combined*，因为它们是相同的。具体来说，我们不是对集合 A_i 的所有可能的交集的子集 $S \subseteq [n]$ 求和来考虑，而是对被交集的集合的 *number* 求和，而不是 *which* 集合被交集。

Corollary 8.7.2. *Suppose we have a universal set U, and suppose we have some sets $A_1, A_2, \ldots, A_n$ that are all subsets of U. Furthemore, suppose that the intersection of any k of the A_i sets has a fixed size—call it $S(k)$—independent of, 其中 sets are intersected. Then,*

$$|U - (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} S(k)$$

Proof. 此结果由定理8.7.1的结果通过合并相同项得出。具体来说，我们知道存在满足$|S| = k$的$\binom{n}{k}$集合$S \subseteq [n]$。根据本推论的假设，所有这样的集合与$|S| = k$|结合将产生

$$\left| \bigcap_{i \in S} A_i \right| = S(k)$$

将那些项合并在一起，并对 S 的可能大小进行求和，我们得到上述结果。

□

这将有助于我们下面要解决的某些例子！

8.7.3 Examples

Example 8.7.3. **Bridge hands:**

一副牌中至少有一张每种花色的牌，共有多少种这样的牌组?

回忆一下，对于扑克牌手牌（即5张牌）来说，这很容易！我们只需注意到花色的分布必须遵循1112，即某些花色出现两次，其他花色各出现一次。（回顾第8.3.6例以了解此论证的细节。）

使用13张牌时，尽管如此，要写下所有这些情况，将这些13的零非项划分：(1,1,1,10)和(1,1,2,9)和(1,2,3,7)等等，要难得多！情况有很多！

让我们使用包含/排除法以提高效率。

设 U 为从一副52张标准牌中所有13张牌手组成的集合。

让 A_H 为 *don't* 中有任意红桃的13张牌手组成。

设 A_S 为 *don't* 中有任意梅花牌的13张牌手

Let A_C 是包含任何 Cl 的 13 张牌手牌集合 *don't* 瑞士银行。

让 A_D 为 *don't* 有任何红桃的13张牌手牌集合。

然后我们寻求一个表达式来

$$\text{☺} = \left|U - \left(A_H \cup A_S \cup A_C \cup A_D\right)\right|$$

考虑所有可能的交集，我们有

$$\begin{aligned}\text{☺} = \ & |U| - |A_H| - |A_S| - |A_C| - |A_D| \\ & + |A_H \cap A_S| + |A_H \cap A_C| + |A_H \cap A_D| \\ & + |A_S \cap A_C| + |A_S \cap A_D| + |A_C \cap A_D| \\ & - |A_H \cap A_S \cap A_C| - |A_H \cap A_S \cap A_D| \\ & - |A_S \cap A_C \cap A_D| - |A_H \cap A_D \cap A_C| \\ & + |A_H \cap A_S \cap A_C \cap A_D|\end{aligned}$$

自因为有4个“坏集合”，我们需要考虑它们所有可能的交集方式。然而，计算这些交集实际上非常方便，因为交集的大小 *only* 取决于 *how many* 集合的交集，而不是 *which* 集合的交集。

请注意 $|A_H| = |A_S| = |A_C| = |A_D| = \binom{39}{13}$。要有一副包含 *avoids* 一组的 13 张牌手牌，我们只需从 *other* 39 张牌中选出 13 张即可。

同样，请注意 $|A_H \cap A_S| = \binom{26}{13}$，因为我们需要避免2种花色。这一点适用于 *every* 这两个集合的交集。

同样，请注意 $|A_H \cap A_S \cap A_D| = \binom{13}{13}$，因为我们需要避免3种花色，所以我们只有13张牌可供选择（第4种花色）。这一点适用于这些集合的每个三重交集。

因此，我们有

$$\text{☺} = \binom{52}{13} - \binom{4}{1}\binom{39}{13} + \binom{4}{2}\binom{26}{13} - \binom{4}{3}\binom{13}{13} + \binom{4}{4}\binom{0}{13}$$

总此类手牌。

(注意，最后一项为0；我们怎么可能有一副没有任何花色的13张牌的手牌？！)

One Lesson: 注意我们在这个例子中选择如何定义集合 U 和 A_i。我们想计算具有特定属性的手牌 *with* 的数量，因此我们定义了具有该属性的手牌集合，并考虑了如何从总数中计算它们的数量。

Example 8.7.4. **Counting surjections:** 计算函数 f 的数量：$[5] \to [3]$。计算是单射的数量。计算是满射的数量。

设 U 为从 [5] 到 [3] 的所有函数的集合。

我们知道 $|U| = 3^5$，因为我们有 3 种输出选择，针对域中的每个 5 个元素。

存在 *no* 个这样的函数是单射的。如果一个函数 $f : [5] \to A$ 是单射的，那么 $|\mathrm{Im}_f([5])| = 5$，但在这里，值域的大小是 3。因此，这是不可能的。

现在，让我们来计算满射!

设 A_1 为具有性质 $1 \notin \text{Im}_f([5])$ 的所有此类函数的集合。设 A_2 为具有性质 $2 \notin \text{Im}_f([5])$ 的所有此类函数的集合。设 A_3 为具有性质 $3 \notin \text{Im}_f([5])$ 的所有此类函数的集合。然后我们寻求 $N = |U - (A_1 \cup A_2 \cup A_3)|$ 的一个表达式。我们有

$$N = |U| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|$$

记住，一般来说，函数 $f : [m] \to [n]$ 的数量是每个 m 输入) 的 n^m (n 个输出选择，我们有

$$N = 3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5 - \binom{3}{3}0^5 = 3^5 - 3 \cdot 2^5 + 3 = 243 - 96 + 3 = 150$$

Example 8.7.5. 找出从1到1000的自然数中，既不是完全平方数，也不是立方数，也不是四次幂的数的个数。

让 $U = [1000]$。对于 $i \in \{2, 3, 4\}$，让 A_i 是 U 中某些自然数的完美 i-次幂的元素集合。也就是说，定义

$$A_i = \left\{x \in U \mid \exists b \in \mathbb{N}\text{.}\ x = b^i\right\}$$

然后我们寻求数字 $M = |U - (A_2 \cup A_3 \cup A_4)|$。

注意 $|U| = 1000$。

请注意，U中的最大平方是$31^2 = 961$（因为$32^2 = 1024$）。因此，$|A_2| = 31$。

注意，U 中最大的立方体是 $10^3 = 1000$。因此，$|A_3| = 10$。

注意，U 中最大的四次方是 $5^4 = 625$（因为 $6^4 = 1296$）。因此，$|A_4| = 5$。

考虑到交集，请注意，例如，$A_2 \cap A_3$ 是六次幂集合，因为 LCM$(2, 3) = 6$。（LCM 是最小公倍数。）

注意，U 中最大的六次方是 $3^6 = 729$（因为 $4^6 = 4096$）。因此，$|A_2 \cap A_3| = 3$。

我们已经找到了U中的最大四次方是5^4，所以$|A_2 \cap A_4| = |A_4| = 5$。

注意，U 中最大的12次方是 $1^{12} = 1$（因为 $2^{12} = 4096$）。因此，$|A_3 \cap A_4| = 1$。

这也告诉我们 $|A_2 \cap A_3 \cap A_4| = |A_3 \cap A_4| = 1$。

将所有这些放在一起，我们发现

$$N = 1000 - 31 - 10 - 5 + 3 + 5 + 1 - 1 = 962$$

8.7.4 Questions & Exercises

Remind Yourself

简要回答以下问题，无论是口头还是书面。这些问题都是基于您刚才阅读的部分，所以如果您无法回忆起特定的定义、概念或例子，请返回并重新阅读该部分。确保您能够自信地回答这些问题，然后再继续，这将有助于您的理解和记忆！

(1) 排除/包含原理何时适用?

(2) 我们使用了什么策略来证明包含-排除原理?

(3) 为什么我们需要对每个 i 要求 $A_i \subseteq U$? 如果这些条件不满足，你认为结果仍然成立吗?

Try It

尝试回答以下简答题。这些问题需要你实际写下或大声描述（可能是一个朋友/同学），目的是让你练习使用新概念、定义和符号。虽然它们旨在简单，但确保你能完成它们将有助于你！

(1) 有多少个小于100的自然数不是2或5的倍数?

(2) 有多少个小于1000的自然数不是2、3或5的完全幂?

(3) 从 (0, 0) 到 (10, 10) 经过 (3, 3) 的格点路径有多少条?

(4) 从 (0, 0) 到 (10, 10) 经过 (3, 3) 或 (6, 8) 的格点路径有多少条?

(5) 有多少个函数 $f : [6] \to [3]$ 是满射?

8.8 Summary

我们现在已经开发了几种基本的计数技术，并将它们发展成为更高级的技术。我们首先简单地讨论了求和规则和乘积规则，这些规则基于前一章关于有限集的基数的结果。我们能够利用这些来开发一些基本的计数对象，并描述如何计数它们。这包括非常有用的 **binomial coefficients**。我们为自己推导了二项式系数的公式，实施了一种计数策略。然后，我们将这些原则应用于大量例子，以使我们自己在处理计数论证的细微差别方面得到实践：有时涉及许多情况，

有时我们得巧妙地应用乘法法则，有时我们得担心计数过多或过少。在这方面，我们讨论了如何判断一个提出的论点是否错误，并*demonstrate*。

*counting in two ways*的证明技术非常重要，你将在许多其他数学领域看到它的应用。我们看到了一些有教育意义的例子——它们本身也是有用的定理——并在练习中提出了许多这类问题，以供你充分练习。我们使用了两种计数方法来后来证明一些进一步的结果和技术，包括二项式定理、重复选择的公式。

我们简要讨论了一些更高级的计数技术，鸽巢原理和包含/排除原理。这些被认为更高级的部分原因是因为很难看到 *when* 和 *how* 来应用它们。通过解决一些示例，我们希望我们已经给了你更好的直觉，了解这些技术如何有用，以便你在解决问题时知道何时使用它们。

8.9 Chapter Exercises

这些问题涵盖了本章的所有内容，以及我们之前看到的任何内容，以及可能的一些假设的数学知识。当然，我们不期望你解决其中的**all**，但工作得越多，你将学到越多！记住，没有*doing*数学，你无法真正*learn*数学。动手解决一个问题。阅读几个陈述，四处走走，思考它们。尝试写一个证明，并向朋友展示，看看他们是否信服。继续练习以清晰、精确和逻辑的方式将你的想法*write*出来。写完证明后，编辑它，使其更好。最重要的是，继续*doing*数学！

简答题，只需解释或陈述答案，无需严格的 *proof*，已用 ► 标记。

特别具有挑战性的问题已用 ⋆ 标记。

Problem 8.9.1. 在这个问题中，你将 *prove* 查看**Rule of Product**（定理8.2.10）。

证明，通过在 n 上的归纳，n 个有限集合的笛卡尔积的大小等于这些集合大小的乘积。

Problem 8.9.2. 设$n \in \mathbb{N}$ (具有$n \geq 3$)，并设S为所有长度为n的二进制字符串的集合。

每个以下表达式都是S的某个子集的大小。对于每一个，确定这样的子集并解释为什么它有效。

例如，如果我被呈现以下内容

$$\binom{n}{3} + \binom{n}{4} + \binom{n}{5}$$

我会说，

> 设 $S_1 \subseteq S$ 为所有具有 3 或 4 或 5 个位置的 0 的字符串集合。我们可以将这个集合划分为具有恰好 k 个 0 的字符串集合，对于每个 $k = 3, 4, 5$。在每种情况下，我们可以通过选择 k 个 n 个总位置为 0，并将其余的固定为 1 来找到该部分的尺寸。通过 ROS，因此，我们发现 $|S_1|$ 是上述总和。

(a) 2^{n-2}

(b) $2^n - \binom{n}{n} - \binom{n}{n-1} - \binom{n}{n-2} - \binom{n}{n-3}$

(c) $\binom{n}{2} - \binom{n-1}{1}$

(d) $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k}$

Problem 8.9.3. 一个学生组织每周举行会议，由一位选出的领导者和两位助手来高效地主持会议。如果学期中有14周，为了保证每次会议都能有不同的领导者和助手组合，组织内必须有多少名学生?

Problem 8.9.4. 假设我们有50块万圣节糖果要分给4个不同的孩子。我们有多少种分配方式？如果所有的糖果都是相同的呢？如果有5种不同种类的糖果，每种各有10块呢?

Problem 8.9.5. 设 U 为所有从一副标准扑克牌中抽取的、恰好包含两张王和一张红桃的5张牌的手牌集合。求 $|U|$。

Problem 8.9.6. 对于以下每个条件，考虑从一副标准扑克牌中抽取7张牌的手牌。

(a) 有多少种7张牌的手牌组合?

(b) 有多少7张牌的手牌中没有高于8点的牌？（注意：A是最高点数。）

(c) 有多少7张牌的手牌恰好有两张国王?

(d) 有多少7张牌的手牌恰好包含一对？（即一对和五张不同花色的牌。）

(e) 至少有多少种7张牌的手牌包含3 ♡s?

Problem 8.9.7. 从 {0, 1, 2, . . . , 9} 中找出5 *distinct* 位有序排列的数字。然后，找出其中5和6相邻排列的数量。

Problem 8.9.8. 设 $T_{5,4}$ 为从集合 [4] 中抽取的所有 5-元组的集合。

（例如，（1, 4, 4, 1, 2）$\in T_{5,4}$。）

(a) 什么是 $|T_{5,4}|$? (b) $T_{5,4}$ 中有多少个元素没有奇数? (c) $T_{5,4}$ 中有多少个元素没有重复数字? (d) $T_{5,4}$ 中有多少个元素恰好有 2 个不同的数字?（例如，(1, 2, 2, 1, 2) 应该计算，但 (1, 1, 1, 1, 1) 不应该计算，(1, 2, 3, 3, 3) 也不应该计算。）(e) $T_{5,4}$ 中有多少个元素没有相邻的相同数字?（例如，(1, 3, 1, 3, 4) 应该计算，但 (2, 3, 1, 1, 3) 不应该计算，(1, 1, 1, 4, 3) 也不应该计算。）

Problem 8.9.9. 对于以下每个属性，找出掷5 *distinguishable* 个骰子使该属性成立的方法数。（不考虑属性组合；每个属性都是独立的）。

(a) 面上没有出现偶数。

(b) 正好有两个偶数出现在面上。

(c) 所有面的和为奇数。

(d) 面牌上的数字组成一个“满堂红”。（即，恰好有三个相同的数字和恰好两个相同的数字。）

(e) 面上的数字组成一个“直线”。

Problem 8.9.10. 有多少个单词MILLIMETER的排列? 有多少这样的排列中两个M相邻? 有多少这样的排列中M是*non*-相邻的?

Problem 8.9.11. 在1到1000（含）之间有多少个自然数，其各位数字都不是偶数? 有多少个数的各位数字都不重复? 有多少个数的各位数字之和是偶数?

(贝 c areful: 记住，像 0011 这样的字符串实际上是 num 关于11.)

Problem 8.9.12. 考虑从一副牌的顶部抽取两张牌 **in order**。有多少种结果使得第一张牌是A，第二张牌是红桃?

Problem 8.9.13. 至少每种花色都有一张牌的15张牌手有多少种?

Problem 8.9.14. 通过 **induction** 在 n 上证明二项式定理（参见定理8.4.8）。

Problem 8.9.15. 证明

$$\binom{n}{k}2^k = \sum_{i=0}^{k}\binom{n}{i}\binom{n-i}{k-i}$$

Problem 8.9.16. 设 $a, b, k \in \mathbb{N}$ 为 $a + b \geq k$。证明

$$\binom{a+b}{k} = \sum_{i=0}^{k}\binom{a}{i}\binom{b}{k-i}$$

Problem 8.9.17. 三个人走进浴室，发现墙上排成一行的七个小便池。这些人以不违反“兄弟准则”的方式排列自己的方法有多少种？（也就是说，他们必须确保没有两个相邻的小便池被占用。）

Problem 8.9.18. 设 $n \in \mathbb{N}$ 已知。通过 *counting in two ways* 论证证明以下恒等式。

(Hint: 很可能您可以在所有部分使用相同的“故事”或公式；也就是说，尝试稍微修改您的论证从（a）来证明（b）和（c）。）

(a) $\displaystyle\sum_{i=1}^{n}(i-1) = \binom{n}{2}$

(b) $\displaystyle\sum_{i=1}^{n}(i-1)(n-i) = \binom{n}{3}$

(c) $\displaystyle\sum_{i=1}^{n}\binom{i-1}{2}\binom{n-i}{2} = \binom{n}{5}$

Problem 8.9.19. 证明

$$\sum_{i=0}^{n}\binom{r+i}{i} = \binom{r+n+1}{n}$$

通过两种计数方式的论证。

Problem 8.9.20. 证明

$$\binom{n}{k} - \binom{n-2}{k} = 2\binom{n-2}{k-1} + \binom{n-2}{k-2}$$

通过两种计数方式论证。使用给定的确切形式；不要代数简化。

Problem 8.9.21. 证明

$$\binom{n}{k} - \binom{n-2}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1}$$

通过两种计数方式论证。使用给定的确切形式；不要代数简化。

Problem 8.9.22. 证明

$$\binom{n}{k} - \binom{n-3}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \binom{n-3}{k-1}$$

通过两种计数方式论证。使用给定的确切形式；不要代数简化。

Problem 8.9.23. 证明

$$4^n = \sum_{k=0}^{n} \binom{n}{k} 3^k$$

通过两种计数方式的论证。

Problem 8.9.24. 设 $p \in \mathbb{N}$ 为素数。设 $k \in \mathbb{N}$ 给定，满足 $1 \leq k < p$。证明 $\binom{p}{k}$ 能被 p 整除。

Problem 8.9.25{v*} 设 $p \in \mathbb{N}$ 为素数。使用前一个问题 8.9.24 来证明

$$\forall x, y \in \mathbb{Z}\text{.}\ (x+y)^p \equiv x^p + y^p \mod p$$

(回顾一下问题6.7.22，我们之前在那里研究过这个问题。你刚刚在一般性上证明了它！)

Problem 8.9.26. 设 $p \in \mathbb{N}$ 为素数，并设 $a \in \mathbb{Z}$。使用问题 8.9.24 的结果和二项式定理来证明

$$a^p \equiv a \mod p$$

这个结果被称为 **Fermat's Little Theorem**。

Problem 8.9.27. 通过考虑 *lattice paths* 的两种计数方式论证来证明求和恒等式（参见定理8.4.5）。具体来说，我们建议根据第一次向右移动发生的位置将 (0, 0) 到 $(k+1, n-k)$ 的格路径集合进行划分。

Problem 8.9.28. 在这个问题中，你将证明以下求和公式，你之前已经通过归纳法证明了它！

$$\forall n \in \mathbb{N}\text{.}\quad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

(a) 设 $k \in \mathbb{N}$ 已知。通过一个 *counting in two ways* 论证证明以下等式：

$$\forall k \in \mathbb{N}\text{.}\quad k^3 = 6\binom{k}{3} + 6\binom{k}{2} + \binom{k}{1}$$

(提示：考虑从一个包含 k 个字母的字母表中计算长度为 3 的单词数量.)

(b) 使用 **Summation Identity** 以及你在 (a) 中刚刚证明的等式来证明问题陈述中给出的上述断言！

奖励你能将这种方法推广到找到 $\sum k^4$ 的公式吗?

Problem 8.9.29. 设 $n \in \mathbb{N}$ 已知。有多少个格点路径从 (0, 0) 到 (3n, 3n) 而不经过 (n, n) 或 (2n, 2n)?

Problem 8.9.30. 设 $n \in \mathbb{N}$ 已知。假设我们有 n 位CMU学生和 n 位Pitt学生。（当然，假设没有人同时就读于这两所学校，因此这两组 n 学生是互斥的。）

(a) 我们有多少种方法将这些2n名学生分成n对？（注意：对之间以及对内的人员顺序不应考虑。）(b) 我们有多少种方法将这些2n名学生分成n对，其中每对必须包含一名CMU学生和一名Pitt学生？（同样，对之间以及对内的人员顺序不考虑。）

Problem 8.9.31. 设 $n \in \mathbb{N}$，并设 $S \subseteq \mathbb{N}$ 的大小为 $|S| = n + 1$. 证明存在 $\exists x, y \in S$ 使得 $x \neq y$ 和 $x - y$ 是 n 的倍数。

Problem 8.9.32. 考虑集合 [22]。设 $S \subseteq$ [22] 满足 $|S| = 7$。在这里，你将证明必须存在两个不相交的非空子集 $X, Y \subseteq S$，它们的元素具有相同的 sum。

1. S中有多少个非空子集?

2. 设 $T \subseteq S$ 已知。T元素之和的最小可能值是多少？最大可能值是多少？ 3. 使用 (a) 和 (b) 推导出存在两个集合 $X, Y \subseteq S$，它们的元素具有相同的和。4. 进一步解释，你可以使 X 和 Y成为 $disjoint$。

Problem 8.9.33. 考虑一个边长为1厘米的等边三角形。假设有10个点被放置在三角形内部（且不在边界上）。证明必须存在两个点，它们之间的距离 d 小于 $\frac{1}{3}$ 厘米。

Problem 8.9.34. 设 $n \in \mathbb{N}$ 已知。通过一个 $counting\ in\ two\ ways$ 论证证明以下恒等式：

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Problem 8.9.35. 设 $n \in \mathbb{N}$ 已知。考虑以下恒等式：

$$4^n = \sum_{k=0}^{n} \binom{n}{k} 2^n$$

从二项式定理中推导它。然后，通过一个 $counting\ in\ two\ ways$ 论证来证明它。

Problem 8.9.36. 设 $n, k \in \mathbb{N}$ 已知。考虑方程 n ⋆:

$$\sum_{i \in [k]} x_i = x_1 + x_2 + \cdots + x_k = n$$

在这个问题中，我们将讨论从 *solutions* 到 ⋆，其中解是对 $x_1, x_2, \ldots, x_k$ 的赋值，使得它们的和为 n，并且每个都满足 $x_i \in \mathbb{N} \cup \{0\}$。

(a) ⋆存在多少个解?

(b) 有多少个解同时满足 ⋆ 和 $x_1 \geq 3$?

(c) 有多少个解满足 ⋆ 也满足 $\forall i \in [k]$。 $x_i \geq 2$?

(d) 有多少个解同时满足 ⋆ 4?

(e) 考虑以下对 ⋆ 的修改:

$$x_1 + x_2 + \cdots + x_k \leq n$$

这个 *inequality* 有多少个解存在? （再次，一个解需要 $x_i \in \mathbb{N} \cup \{0\}$。）

Problem 8.9.37. 假设有10个海盗需要分配100块金币。

假设红胡子船长和黑胡子船长是10名海盗中的一员。

(a) 有多少种方式分配金币，使得红胡子至少得到5枚金币但黑胡子至多得到5枚？(b) 有多少种方式分配金币，使得红胡子至少得到10枚金币但黑胡子得到5到15（含）之间的金币？(c) 有多少种方式分配金币，使得红胡子得到0到10（含）之间的金币，而黑胡子得到10到20（含）之间的金币?

(使用包含/排除法。){v*}

8.10 Lookahead

目前没有太多可以期待的内容！至少，*this*这本书里没有其他内容。我们希望这仅仅是为了激发你对数学知识和解决问题的渴望。想想我们是从哪里开始的：我们不过是在提出有趣的谜题，并尝试通过应用我们的现有知识和逻辑技巧来解决它们。实际上，我们现在做的就是这些！只是我们现在已经发展了如此多的数学

术语和如此多的结果以及如此多的解决问题的技能，使我们能够处理和讨论更高级的问题。当你开始阅读这本书时，你是否想过你会解决像这样的问题？你是否觉得你对数学家所从事的工作以及他们如何看待世界有了更好的理解，有了更深的欣赏？我们希望如此！☺

我们还在数学之外的生活中也开发了几项基本技能。你很可能在日常生活中不会遇到正式的 *symbolic* 逻辑，但你肯定会不得不处理包含合取、析取和条件语句的复杂陈述。我们每天都在做这件事，作为相互交谈并传达复杂思维过程的人类。通过研究形式逻辑的一些基础方面，我们现在都更擅长分析复杂陈述并评估它们的真实性，以及能够写下或以其他方式分享我们自己的思想。

同样，你可能不会在日常生活中遇到组合恒等式的正式陈述，但我们对两种计数方式的证明工作将有助于提高你的分析思维能力。有时我们不得不在如何发展一个“故事”来描述要按两种方式计数的元素集方面发挥创意。这需要一些创造力和机智，锻炼这些大脑肌肉只会有所帮助。此外，阅读一个提出的“证明”并分析它是否实际上是一个过度/不足计数，使我们更擅长理解和批评他人的论点。当然，这是你每天都在做的事情，但可能不是用数学术语。

总体而言，我们已经发展出了一种用数学方式思考的能力。我们学会了：如何阅读和理解问题；如何从多个角度接近问题，并愿意追寻可能的死胡同以深化我们的理解；如何识别不同问题背后的共同结构，并利用这些相似性采用某些技术；最终，如何将我们对问题的所有理解整理成书面、可呈现的论点供他人阅读。这个过程将使我们所有人不仅成为更好的问题解决者，而且成为更好的*communicators*。在一个快速变化的世界里，沟通变得越来越重要（因为与他人的快速连接变得越来越容易），有效地、正确地、清晰地分享我们的思想是一种基本的生活技能。

但无论如何，不要让这成为我们数学之旅的终点！勇往直前，繁荣昌盛，传播你对数学的知识和喜悦。与其他人一起解决这些问题以及其他问题。寻找那些能激发你兴趣的数学领域。看看你是否可以用这些概念来解决你面临的现实世界问题。最重要的是，只是出去 **do mathematics**。

Appendix A

Definitions and Theorems

A.1 Sets

A.1.1 Standard Sets

- **natural numbers** 是

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

  注意：$0 \notin \mathbb{N}$。

- 对于每个 $n \in \mathbb{N}$，集合 $[n]$（“**brackets** n”）被定义为

$$[n] = \{x \in \mathbb{N} \mid 1 \leq x \leq n\} = \{1, 2, 3, \dots, n\}$$

- **integers** 是

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

- **rational numbers** 是

$$\mathbb{Q} = \left\{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z}\text{.}\ b \neq 0 \text{ and } \frac{a}{b} = x\right\}$$

- **real numbers**表示为$\mathbb{R}$。每个实数要么是**ratio- nal**，要么是**irrational**。

- 空集是没有任何元素的集合。我们将其写作 $\varnothing$ 或 $\{\ \}$。

A.1.2 Set-Builder Notation

- 如果 U 是一个集合，并且 $P(x)$ 是某种对于任何给定的 x 要么成立要么不成立的 **property**，那么我们总可以通过以下方式定义一个新的集合：

$$S = \{x \in U \mid P(x) \text{ holds}\}$$

- 这是称为 **set-builder notation**。识别 **uni- versal set** U 和 **property** $P(x)$ 是至关重要的。

A.1.3 Elements and Subsets

- 要表示“x 是集合 S 的一个元素”，我们写作 $x \in S$ 要表示“x 不是集合 S 的一个元素”，我们写作

$$x \notin S$$

- 要说“S 是 T 的子集”，我们写

$$S \subseteq T$$

这是由条件语句“S的每个元素也是T的元素”定义的。这可以表示为

$$\forall x \in U \,.\, x \in S \implies x \in T$$

这意味着，对于全集（假设$S, T \subseteq U$）中的每个元素x，每当$x \in S$，我们也知道$x \in T$。

- 为了证明一个集合是另一个集合的子集，例如 $S \subseteq T$，我们需要做类似这样的事情：让 $x \in S$ 是任意且固定的... 咕噜咕噜... 因此，$x \in T$ 也是如此。这表明 $S \subseteq T$。

- 要表示“S 是 T 的真子集”，我们写作 $S \subset T$

这意味着 $S \subseteq T$ 和 $S \neq T$。

- 这是真的，对于任何集合 S，都有 $\varnothing \subseteq S$。
- 这是真的，对于任何集合 S，都有 $S \subseteq S$。

A.1.4 Power Set

- 设 S 为一个集合。**power set of** S 表示为 $\mathcal{P}(S)$，并由以下定义：

$$\mathcal{P}(S) = \{A \mid A \subseteq S\}$$

这是，$\mathcal{P}(S)$是**set of all subsets of** S。

- 这是真的，对于任何集合 S，有 $\varnothing \in \mathcal{P}(S)$ 和 $S \in \mathcal{P}(S)$。

A.1.5 Set Equality

- 要说“S 和 T 是 **equal** 集合”，我们写作 $S = T$。这由 $S = T$ 定义，当且仅当 $S \subseteq T$ 和 $T \subseteq S$

- 要使两个集合 **prove** 相等，例如 $S = T$，我们需要做如下事情：首先，我们将证明 $S \subseteq T$。设 $x \in S$ 为任意且固定的。. . . 咕咕咕 . . . 因此，$x \in T$。这表明 $S \subseteq T$。其次，我们将证明 $T \subseteq S$。设 $y \in T$ 为任意且固定的。. . . 咕咕咕 . . . 因此，$x \in S$。这表明 $T \subseteq S$。因此，$S = T$。这被称为一个 **double-containment argument**。

A.1.6 Set Operations

假设 S, T, U 是集合，$S \subseteq U$ 和 $T \subseteq U$。

- 两个集合的 **union** 定义为

$$S \cup T = \{x \in U \mid x \in S \text{ or } x \in T\}$$

它是属于两个集合 **at least one**、S 和 T 的所有元素的集合。

- 两个集合的 {v*} 定义为

$$S \cap T = \{x \in U \mid x \in S \text{ and } x \in T\}$$

它是属于 **both** 集合、S 和 T 的所有元素的集合。

- 两个集合的 **difference** 定义为

$$S - T = \{x \in U \mid x \in S \text{ and } x \notin T\}$$

它是集合 S 中所有不是 T 元素的元素集合。

- 集合的 **complement** 定义为

$$\overline{S} = \{x \in U \mid x \notin S\} = U - S$$

它是全集所有不属于S的元素的集合。

- 两个集合的 {v*} 定义为

$$S \times T = \{(x, y) \mid x \in S \text{ and } y \in T\}$$

它是所有 **ordered pairs** 的集合，其中第一个坐标是 S 的一个元素，第二个坐标是 T 的一个元素。

A.1.7 Indexed Set Operations

假设 I 是一个指标集，U 是一个全集，并且我们为每个 $i \in I$ 定义了一些集合 $A_i \subseteq U$。

- 所有 A_i 集合的 **indexed union** 定义为

$$\bigcup_{i \in I} A_i = \{x \in U \mid \exists k \in I \,.\, x \in A_k\}$$

  它是包含在全集中的所有元素x的集合，使得x是索引集合的并集中 **at least one**的元素。

- 所有 A_i 集合的 **indexed intersection** 定义为

$$\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I \,.\, x \in A_i\}$$

  它是包含在交集的索引集中，使得 x 是 **all** 的元素的所有元素 x 的集合。

A.1.8 Partition

- 设 S 为一个集合。**partition** 的 S 是一组互斥的集合，它们的并集是 S。也就是说，一个划分由索引集 I 和为每个 $i \in I$) 定义的 *non-empty* 集合 S_i (形成，这些集合满足:
  - $\forall i \in I \,.\, S_i \neq \varnothing$
  - $\forall i \in I \,.\, S_i \subseteq S$
  - $\forall i, j \in I \,.\, i \neq j \implies S_i \cap S_j = \varnothing$
  - $\bigcup_{i \in I} S_i = S$

A.2 Logic

A.2.1 Statements and Propositions

- True 并且 False 是我们考虑的唯一两个真值。
- 一个 **mathematical statement** (或 **logical statement**) 是一个语法正确的句子，它具有 **exactly** 一个真值。
- 一个 **variable proposition** 是一个语法正确的句子，它涉及一个或多个变量，当为这些变量分配值时，它恰好获得一个真值。
- 当我们定义一个陈述或命题时，我们给它分配一个字母名称，指明任何对变量的依赖（以及给它们分配字母），并用引号括起实际的陈述/命题。这里有两个 **good examples**:

  定义 P 为“每个实数 x 满足 $x^2 \geq 0$”。定义 $Q(x, y)$ 为“$xy \leq \left(\frac{x+y}{2}\right)^2$”，对于每个 $x, y \in \mathbb{R}$。

- **Law of the Excluded Middle** 是我们假设每个陈述要么是 True 要么是 False。它表明，当我们有一个陈述 P 时，我们保证要么 P 是 True 要么 P 是 False，并且这些情况中有 **only one** 个成立。

A.2.2 Quantifiers

- 对于“对于每个”或“对于所有”，我们使用 **universal quantifier** $\forall$

  “$\forall x \in S$**.** $P(x)$” says that “For every element $x \in S$, the property $P(x)$ holds true”.

- 存在或至少有一个，我们使用 **existential quantifier** $\exists$

  “$\exists x \in S$**.** $P(x)$” says that “There exists an element $x \in S$ with the property $P(x)$”

- 我们使用“点”**.** 来分隔量化陈述的各个部分。 **.** dot to separate parts of a quantified statement.
- 当大声朗读一个量化陈述时，我们在一个量化词之后说“使得”**only**。

- 我们使用“！”来表示存在是 {v*}；也就是说，断言“$\exists!\, x \in S$”

  $P(x)$” says that “There exists an element $x \in S$ with property $P(x)$, and there is *exactly* one such x”.

A.2.3 Connectives

假设 P和 Q 是数学陈述。它们可能由带有量词的变量命题组成。

- 要表示“P和 Q”，我们写
$$P \wedge Q$$
这只有在 **both** P和 Q 是 True 时才具有真值 True。
- 要说“P或 Q”，我们写
$$P \vee Q$$
这只有在陈述 **at least one**、P和 Q 都为真时才具有真值 True。 (这是 **inclusive** 或，因此允许 P和 Q 都为真。)
- 如果说“如果 P则 Q”，我们写作
$$P \implies Q$$
这只有在 P成立时，Q 也成立的情况下，才有真值 True。

  注意，$P \implies Q$ 本身就是一个逻辑陈述。它有一个真值，True 或 False 。它关于构成陈述的真值，P和 Q 的真值。

  我们称这为 **conditional statement**；我们说 P是 **hypothesis**，Q 是 **conclusion**。

  注意，当 P是 False 时，$P \implies Q$ 是 True。这是因为这是一个“如果⋯⋯那么⋯⋯”的陈述；它使 **no claim** 关于 P是 False 的情况，因此我们不能声明条件语句是 False，所以它必须是 True (根据“排中律”)。
- 一个表示 $P \implies Q$ 的等价方法是
$$\neg P \vee Q$$
- 条件语句 **contrapositive** 的 $P \implies Q$ 是
$$\neg Q \implies \neg P$$
保证与$P \implies Q$具有相同的真值。即,
$$(P \implies Q) \iff (\neg Q \implies \neg P)$$
- 条件语句 **converse** 的 $P \implies Q$ 是
$$Q \implies P$$

它保证与 **not** 具有相同的真值，与 $P \implies Q$。存在语句 P, Q 使得 $P \implies Q$ 成立，并且逆命题也成立，存在语句 P, Q 使得 $P \implies Q$ 成立，但逆命题不成立。

- 要说“P和 Q 是 **logically equivalent**”，我们写

$$P \iff Q$$

并且我们大声朗读为“P当且仅当 Q”。

我们也可以将其写为

$$(P \implies Q) \wedge (Q \implies P)$$

这意味着无论发生什么，都是指 P和 Q **have the same truth value**。

A.2.4 Logical Negation

- 我们使用“$\neg$”来表示语句的 **logical negation**。
- 声明 $\neg P$来自声明 P的 **opposite truth value** 。
- **Negating a $\forall$ claim:**

$$\neg\big(\forall x \in S\text{.}\ P(x)\big) \iff \exists x \in S\text{.}\ \neg P(x)$$

- **Negating a $\exists$ claim:**

$$\neg\big(\exists x \in S\text{.}\ P(x)\big) \iff \forall x \in S\text{.}\ \neg P(x)$$

- **Negating a $\vee$ claim:**

$$\neg\big(P \vee Q\big) \iff \neg P \wedge \neg Q$$

这是**DeMorgan's Laws for Logic**之一。

- **Negating a $\wedge$ claim:**

$$\neg\big(P \wedge Q\big) \iff \neg P \vee \neg Q$$

这是**DeMorgan's Laws for Logic**之一。

- **Negating a $\implies$ claim:**

$$\neg\big(P \implies Q\big) \iff \neg(\neg P \vee Q) \iff P \wedge \neg Q$$

- **Negating a $\iff$ claim:**

$$\neg\big(P \iff Q\big) \iff \neg\left[(P \implies Q) \wedge (Q \implies P)\right] \iff (P \wedge \neg Q) \vee (Q \wedge \neg P)$$

- 使用这些事实，我们可以否定 **any** 数学陈述，因为一个陈述只是由量词、连接词和变量命题组成的。

我们可以从左到右读取该语句并否定每一部分。

A.2.5 Proof Strategies

我们使用短语AFSOC表示“为了反驳的目的而假设”。

- **Proving a $\exists$ claim:** $\exists x \in S$**.** $P(x)$ D

  Direct proof:
  efine a specific example, $y =$ _____.

  Prove that $y \in S$.

  Prove that $P(y)$ holds true.
  Find a contradiction.
Indirect proof:

  AFSOC that for every $y \in S$, $\neg P(y)$ holds.

- **Proving a $\forall$ claim:** $\forall x \in S$**.** $P(x)$ L

  Direct proof:
  et $y \in S$ be arbitrary and fixed.

  Prove that $P(y)$ holds true.
  Find a contradiction.
Indirect proof:

  AFSOC that $\exists y \in S$ such that $\neg P(y)$ holds.

- **Proving a $\vee$ claim:** $P \vee Q$

  Direct proof:

  证明 P成立，否则证明 Q 成立。*Indirect proof 1:* 假设 $\neg P$成立。证明 Q 成立。*Indirect proof 2:* AFSOC $\neg P \wedge \neg Q$ 成立。找到一个矛盾。

- **Proving a $\wedge$ claim:** $P \wedge Q$

  Direct proof:

  证明 P成立。证明 Q 成立。

  Indirect proof:

AFSOC что $\neg P \vee \neg Q$ удерживается. Рассмотрим первый случай, где $\neg P$удерживается. Найдите противоречие. Рассмотрим второй случай, где $\neg Q$ удерживается. Найдите противоречие.

- **Proving a $\implies$ claim:** $P \implies Q$

  Direct proof:

  假设 P成立。证明 Q 成立。

  Contrapositive proof:

  假设 $\neg Q$ 成立。证明 $\neg P$成立。

  Indirect proof:

  AFSOC что Pудерживает и предположим, что Q не выполняется. Найти противоречие.

- **Proving a $\iff$ claim:** $P \iff Q$

  Direct proof:

  证明 $P \implies Q$ (使用上述方法之一)。证明 $Q \implies P$ (使用上述方法之一)。

  Indirect proof:

  AFSOC that $\neg(P \implies Q) \vee \neg(Q \implies P)$.

  考虑第一种情况，其中 $P \wedge \neg Q$ 成立。找到一个矛盾。考虑第二种情况，其中 $Q \wedge \neg P$成立。找到一个矛盾。

A.3 Induction

A.3.1 Principle of Specific Mathematical Induction

- **Theorem:** 假设 $P(n)$ 是对所有 $n \in \mathbb{N}$ 定义的变量命题。假设 $P(1)$ 成立。

  假设 $\forall k \in \mathbb{N}$。 $P(k) \implies P(k+1)$.
  然后 $\forall n \in \mathbb{N}$。 $P(n)$.
- **Proving a claim by induction:** 假设我们有一个对所有 $n \in \mathbb{N}$ 定义的变量命题 $P(n)$，并且我们想要证明 $P(n)$ 对每个 $n \in \mathbb{N}$ 都成立。 **Base Case:** 证明 $P(1)$ 成立。 **Induction Hypothesis:** 假设 k 是一个任意且固定的自然数，并且假设 $P(k)$ 成立。 **Induction Step:** 证明 $P(k+1)$ 成立。 **Conclusion:** 通过归纳，$\forall n \in \mathbb{N}$。 $P(n)$.

A.3.2 Principle of Strong Mathematical Induction

- **Theorem:** 假设 $P(n)$ 是对所有 $n \in \mathbb{N}$ 定义的变量命题。假设 $P(1)$ 成立。假设 $\forall k \in \mathbb{N}$。 $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \implies P(k+1)$. Then $\forall n \in \mathbb{N}$。 $P(n)$.
- **Proving a claim by strong induction:** 假设我们有一个对所有 $n \in \mathbb{N}$ 定义的可变命题 $P(n)$，我们想要证明 $P(n)$ 对每个 $n \in \mathbb{N}$ 都成立。 **Base Case(s):** 证明 $P(1)$ 成立。（根据归纳步骤中发生的情况，你可能需要多个基本情形。） **Induction Hypothesis:** 假设 k 是一个任意且固定的自然数，它满足某些不等式（$k \geq$,__ 取决于归纳步骤中发生的情况），并且假设 $P(1) \wedge \cdots \wedge P(k)$ 成立。 **Induction Step:** 证明 $P(k+1)$ 成立。 **Conclusion:** 通过归纳，$\forall n \in \mathbb{N}$。 $P(n)$.

A.3.3 "Minimal Criminal" Argument

- 假设归纳原理的第二条件是一个条件语句，因此我们可以通过逆否命题来证明它。逆否命题说

$$\neg P(k) \implies \neg P(1) \vee \neg P(2) \vee \cdots \vee \neg P(k-1)$$

这意味着，"如果命题在某些特定值 k 上失败，那么我们可以找到一个命题的某些 *prior* 实例（从 1 到 $k-1$）也失败了。"

- **Proving a claim by a "minimal criminal" argument:** 假设我们有一个对所有 $n \in \mathbb{N}$ 定义的变量命题 $P(n)$，并且我们想要证明 $P(n)$ 对每个 $n \in \mathbb{N}$ 都成立。

Base Case(s): 证明 $P(1)$ 成立。

(根据归纳步骤中发生的情况，可能需要多个基本情形。)

Induction Hypothesis: 假设 k 是一个任意且固定的自然数，它满足某些不等式（$k \geq$, 取决于归纳步骤中的情况），并且假设 $\neg P(k)$ 成立；也就是说，假设 $P(k)$ 不成立。

Induction Step: 证明 $\neg P(1) \vee \neg P(1) \vee \neg P(2) \vee \cdots \vee \neg P(k-1)$，即证明该命题在某些先前的实例中不成立。

Conclusion: 通过归纳，$\forall n \in \mathbb{N}$ $P(n)$.

A.4 Relations

- 设 A, B 为集合。**relation** 在 A 和 B 之间是一个 *ordered pairs* 的 $R \subseteq A \times B$ 集合。

  给定元素 $a \in A$ 和 $b \in B$，我们称 a 和 b 为 **related**，当且仅当 $(a, b) \in R$ 。

  集合 A 被称为 **domain**，集合 B 被称为 **codomain**。

  集合 R 被称为 **relation set**。

  我们称 R 是一个关系 **between** A **and** B。

  当 $A = B$ 时，我们称 R 是一个 **on the set** A 关系。

A.4.1 Properties of Relations

设 A 为一个集合，设 R 为 A 上的一个关系，即 $R \subseteq A \times A$。

(注意：这些属性 *only* 在此情况下适用，而不是适用于两个 *different* 集合 A 和 B 之间的关系。)

- 我们称 R 为 **reflexive**，如果 $\forall x \in A \circ \quad (x, x) \in R$

  (i.e. every element is related to itself).
- 我们称 R 为 **symmetric**，如果

  $$\forall x, y \in A \bullet (x, y) \in R \implies (y, x) \in R$$

  (即比较的顺序无关紧要)。
- 我们称 R 为 **transitive**，如果 $\forall x, y, z \in A$

  $\circ \quad [(x, y) \in R \land (y, z) \in R] \implies (x, z) \in R$

  (i.e. the relation always "transitions through a middle-man")
- 我们称 R 为 **anti-symmetric**，如果

  $$\forall x, y \in A \bullet [(x, y) \in R \land (y, x) \in R] \implies x = y$$

  (即，两个在两个方向上相关的元素必须相同)。

A.4.2 Equivalence Relations

让 A 为一个集合，让 R 为 A 上的一个关系。

- 我们称 R 是一个 **equivalence relation**，当且仅当 R 是自反的、对称的和传递的。

- 如果 R 是一个等价关系，并且 $x \in A$，那么 **equivalence class corresponding to x (under the relation R)** 是

$$[x]_R = \{y \in A \mid (x, y) \in R\}$$

这是与x相关的所有元素的集合。

- 如果 R 是一个等价关系，那么 A/R 是 A **modulo** R；它是所有等价类的集合：

$$A/R = \{[x]_R \mid x \in A\}$$

- **Theorem:** 如果 R 是 A 上的等价关系，那么等价类（即 A/R 的元素）构成 A 的 *partition*。

- **Theorem:** 如果 I 是某个指标集，并且 $\{S_i \mid i \in I\}$ 是 A 的一个 *partition*，那么这对应于在 A 上定义的唯一 *equivalence relation*，通过关联 A 的两个元素，如果且仅如果它们属于同一个 *part* 的划分。

A.4.3 Modular Arithmetic

Congruence mod n

- 设 $n \in \mathbb{N}$ 已知。对于任意的 $x, y \in \mathbb{Z}$，我们称 x 和 y 是 **congruent modulo** n，当且仅当 $n \mid x - y$。

  等效地，这意味着 x 和 y 在除以 n 时的余数相同。（这种等价性不是 *definition* 的部分；相反，它遵循下面所述的除法引理。）

  我们将其写作 $x \equiv y \bmod n$。

  (注意：$\bmod n$ 不是一个 *operator* 或 *function*；它是一个 *modifier*，我们将其放置在算术/代数行的末尾，以表示所有操作都已执行模 n。)

- $\equiv$ 是一个 *equivalence relation*，对于每一个 $n \in \mathbb{N}$。

- **Division Lemma:** 设 $n \in \mathbb{N}$ 已知。设 $x \in \mathbb{Z}$ 已知。然后

  $$\exists!\, k, r \in \mathbb{Z}.\ \big[(x = kn + r)\ \wedge\ (0 \le r \le n - 1)\big]$$

  注意，“$\exists!$ ”表示将x表示为n的倍数加上余数的形式是*unique*。

- **Modular Arithmetic Lemma:** 设 $n \in \mathbb{N}$ 已知。设 $a, b \in \mathbb{Z}$ 已知。

  假设 $a \equiv r \bmod n$ 和 $b \equiv s \bmod n$。那么，

  $$a + b \equiv r + s \mod n \text{ 和 } a \cdot b \equiv r \cdot s \bmod n$$

Multiplicative Inverses in $\mathbb{Z}$ mod n

- 设 $x, y \in \mathbb{Z}$ 已知。我们称 x 和 y 是 **relatively prime**，当且仅当它们除了 1 以外没有公共因子（除数）。

- **MIRP Lemma:** (乘法逆元对于互质数)

  假设 $n \in \mathbb{N}$ 和 $a \in \mathbb{Z}$，并且 a 和 n 互质。考虑同余 $ax \equiv 1$ 模 n。那么存在一个解 x 来满足这个同余。

  (事实上，这个同余方程有无限多解，并且它们在模 n 下都是同余的。)

- 当 $ax \equiv 1 \bmod n$ 时，我们称 x 是 a 在 $\mathbb{Z}$ 模 n 下的 **multiplicative inverse**。我们将其写作 $x \equiv a^{-1} \bmod n$。

  实际上，任何与 y 同余于 x 模 n 的整数都将满足 $ay \equiv 1$ 模 n，因此我们实际上考虑等价类 $[x]_{\bmod n}$ 是等价类 $[a]_{\bmod n}$ 的乘法逆元。

- 假设 a^{-1} 首先存在，$(a^{-1})^{-1} \equiv a \bmod n$。
- 设 p 为一个素数。那么所有数字 1, 2, 3, $\ldots, p-1$ 都保证与 p 互质，因此它们在 $\mathbb{Z}$ 模 p 的上下文中都有乘法逆元。
- 如果 a 在 $\mathbb{Z}$ 模 n 的上下文中有乘法逆元，则可以保证在 1 和 $n-$ 之间存在这样的逆元。在实践中，我们只需逐个检查这些候选者，直到找到逆元。

Results

- **Chinese Remainder Theorem:** 假设 $r \in \mathbb{N}$，并且我们有一些自然数 r，$n_1, n_2, \ldots, n_r$，它们两两互质。（也就是说，除了1之外，这些数没有其他公共因子。）假设我们还有 r 个整数，$a_1, a_2, \ldots, a_r$。那么，存在一个解 X 满足由 n_i 和 a_i 定义的同余方程组；即，

$$\exists X \in \mathbb{Z} \centerdot \forall i \in [r] \centerdot X \equiv a_i \mod n_i$$

此外，如果我们定义 $N = \prod n_i$，那么所有无限多个满足同余方程组的解 Y 都满足 $X \equiv Y \bmod N_{\circ^{i \in [r]}}$

A.5 Functions

- 设 A, B 为集合。设 f 为 *relation* 之间的 A 和 B，因此 $f \subseteq A \times B$。

  此外，假设 f 具有如下性质

  $$\forall a \in A \,.\, \exists!\, b \in B \,.\, (a, b) \in f$$

  即，假设定义域 A (的“输入”集合) 的每个元素都有 *ex- actly one* 个与值域 B (的“输出”集合) 中相应元素相对应，使得这两个元素在 f 下相关。

  另一种说法是，“每个输入恰好对应一个输出。”

  这样的关系被称为从 A 到 B 的 **function**。

  我们称 A 为函数的 **domain**，称 B 为函数的 **codomain**。我们写

  $$f : A \to B$$

  表示 f 是一个函数 **from** A **to** B。

  如果 a 与 b 相关，即 $(a, b) \in f$，那么我们写

  $$f(a) = b$$

  知道对于每个 a 都存在这样的 b *exactly one*。

- 给定一个提议的域集 A，一个提议的值域集 B，以及一个提议的“规则” f，该规则说明给定 A 的一个元素时应该输出什么，那么我们说 f 是一个 **well-defined function**，如果规则在 A 的 *all* 个元素上定义，并且对于每个 $a \in A$，规则输出一个实际位于集合 B 中的 *exactly one* 元素。

  (注意：每个函数都是一个定义良好的函数；当我们试图确定给定的“规则”实际上是否是一个函数时，此规则适用。)

- 设 $f : A \to B$ 和 $g : A \to B$ 为函数。我们说 f 和 g 在函数) 的意义上是 **equal** (，当时，我们写 $\forall a \in$ **Images and Pre-Images** $f(a) = g(a)$. That is, $f = g$ when the two functions yield the same output for every input.

- 设 $f : A \to B$ 为一个函数，设 $X \subseteq A$，在函数 f 下 X 的 **image** 是

  $$\mathrm{Im}_f(X) = \{b \in B \mid \exists a \in X \,.\, f(a) = b\}$$

  这是一个等价的集合表示方法:

  $$\mathrm{Im}_f(X) = \{f(a) \mid a \in X\}$$

(直观上，这是所有被 X.) 中元素“击中”的值域元素的集合。

- 设 $f : A \to B$ 为一个函数。设 $Z \subseteq B$。在函数 f 下 Z 的 **pre-image** 是

$$\text{PreIm}_f(Z) = \{a \in A \mid f(a) \in Z\}$$

(直观上，这是所有输出“落在” Z.)的“输入”的集合。

- 注意：$\text{Im}_f(\varnothing) = \varnothing$ 和 $\text{PreIm}_f(\varnothing) = \varnothing$。

A.5.2 Jections

- 设 $f : A \to B$ 为一个函数。如果 $\text{Im}_f(A) = B$，那么我们称 f 为 **surjective**，或者它是一个 **surjection**。

定义　　图像的表示给出了这个等价公式：{v*}　　活动：

$$f \text{ is surjective} \iff \forall b \in B \,.\, \exists a \in A \,.\, f(a) = b$$

(直观上，当值域元素中的 *all* 被函数“击中”时，f 是满射的.)

- 让 $f : A \to B$ 为一个函数。如果 f 具有如下性质

$$\forall a_1, a_2 \in A.\ a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

然后我们说 f 是 **injective**，或者它是一个 **injection**。

这个条件语句的逆否命题得到一个等价的注入性公式：

$$\forall a_1, a_2 \in A.\ f(a_1) = f(a_2) \implies a_1 = a_2$$

(直观上，当两个不同的输入总是产生不同的输出时，f 是单射的，或者等价地说，当输出相等意味着它们来自相同的输入时。)

- 如果一个函数 f 既是单射又是满射，那么我们称 f 为 **bijective**，或者它是一个 **bijection**。

A.5.3 Composition of Functions

- 让 $f : A \to B$ 和 $g : B \to C$ 为函数。

函数 $g \circ f : A \to C$ 定义为

$$\forall a \in A \,.\, (g \circ f)(a) = g(f(a))$$

是 **composition** 与 g 的 f，或“g 与 f 组合而成”　　.

注意：将“$\circ$”读作“之后”有助于提醒您运算顺序：$g \circ f$表示g应用于 *after* f。我们找到$f(a)$，然后找到$g(f(a))$。

- 符号：我们写$(g \circ f)(x) = g(f(x))$。我们*not*写$g \circ f(x)$。括号很重要！

- 让 $f : A \to B$ 和 $g : B \to C$ 以及 $h : C \to D$ 为函数。那么 $(h \circ g) \circ f = h \circ (g \circ f)$。这意味着 **composition is associative**。

- 假设 $f : A \to B$ 和 $g : B \to C$ 都是满射/单射/双射。那么 $g \circ f$ 也是一个满射/单射/双射。

A.5.4 Inverses

- 设 X 为任意集合。**identity function** Id_X：定义为

- 设 $f : A \to B$ 为一个函数。如果存在函数 $F : B \to A$，使得 $f \circ F : B \to B$ 满足 $f \circ F = \mathrm{Id}_B$ 且 $F \circ f : A \to A$ 满足 $F \circ f = \mathrm{Id}_A$，那么我们称 F 是 *inverse* 的 f，并写为 $F = f^{-1}$。

  注意，形式定义明确包括了检查两种函数组合的 *both* 种方式是否产生恒等函数的必要性。存在一些例子，其中一种方式有效而另一种方式无效！

  （注意：当 *proving* 是另一个函数的逆函数时，我们还不允许写 f^{-1}，因为我们实际上正在证明 f 甚至 *has* 也是一个逆。）

  如果 f 有逆元，我们称 f 为 **invertible**。

- **Theorem:** $f : A \to B$ 是双射 $\iff$ f 有逆 $f^{-1} : B \to A$。

- **Theorem:** 设 $f : A \to B$ 和 $g : B \to C$ 均为双射。那么 $g \circ f : A \to C$ 也是一个双射，因此它有一个逆；这个逆是 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。

A.5.5 Proof Techniques for Functions

- 证明 f 是 **surjective**：

  – 设 $b \in B$ 为任意且固定的。– 定义 $a =$ 。– 证明 $a \in A$。– 证明 $f(a) = b$。– 这表明 $b \in \mathrm{Im}_f(A)$，因此 $B \subseteq \mathrm{Im}_f(A)$。– 由于 $\mathrm{Im}_f(A) \subseteq B$ 根据定义，这表明 $\mathrm{Im}_f(A) = B$，因此 f 是满射的。

- 证明 f 是 **not surjective**：

– 定义 $b =$. – 证明 $b \in B$. – 令 $a \in A$ 为任意且固定的. – 证明 $f(a) \neq b$. （或者，假设 $f(a) = b$ 并找出矛盾。）– 这表明

$\exists b \in B.\ b \notin \mathrm{Im}_f(A)$, so f is not surjective.

- 证明 f 是 **injective**：

  – 设 $x, y \in A$ 为任意且固定的。– 假设 $f(x) = f(y)$。– 推导出 $x = y$。

  或者：

  – 设 $x, y \in A$ 为任意且固定的。– 假设 $x \neq y$。– 推导出 $f(x) \neq f(y)$。

- 证明 f 是 **not injective**：

  – 定义 $x =$ 和定义 $y =$ ○ – 证明 $x \in A$ 和 $y \in A$○ – 证明 $x \neq y$○ – 证明 $f(x) = f(y)$ ○ – 这表明 $\exists x, y \in A$○

  $x \neq y \ \wedge \ f(x) = f(y)$, so f is not injective.

- 证明 f 是 **bijective**：

  – 证明 f 是单射的。– 证明 f 是满射的。

  或者：

  – 定义一个函数 $F\colon B \to A$。– 证明 $F \circ f = \mathrm{Id}_A$。– 证明 $f \circ F = \mathrm{Id}_B$。– 这表明 $F = f^{-1}$，因此 f 是可逆的，所以它是双射的。

- 证明 f 是 **not bijective**：– 证明 f 不是单射的，或者证明 f 不是满射的。或者

  - AF SOC f 是双射的，因此它有一个逆 f^{-1}。找到一个反　　词典。

- 对于某些 $X \subseteq A$，求其像 $\text{Im}_f(X)$：
  - 定义一个集合 S。声称 $S =$ 属于 $_f(X)$。

    （注意：提出这个定义是难点，需要大量草稿工作。无需将此作为证明的一部分展示。只需从定义开始。）

    - 证明 $\text{Im}_{f(X)} \subseteq S$。　∗ 设 $y \in \text{Im}_{f(X)}$ 为任意且固定的。∗ 这意味着 $\exists a \in X$。　$f(a) = y$.
      - ∗ Use the properties of f to show that $f(a) \in S$.
    - ∗ This shows that $y \in S$.
  - Prove that $S \subseteq \text{Im}_f(X)$.
    - ∗ Let $z \in S$ be arbitrary and fixed.
    - ∗ Define $x =$ _____.
    - ∗ 通过双重包含论证得出 $\text{Im}_f(X) = S$。
    - ∗ Show that $f(x) = z$.
    - ∗ This shows that $z \in \text{Im}_f(X)$.
- 对于某些 $Z \subseteq B$，找到前像 $\text{PreIm}_f(Z)$：– 定义一个集合 T。声称 $T =$ 是 $\text{PreIm}_f(Z)$ 的前像。（注意：提出这个定义是难点，需要大量草稿工作。无需将此作为证明的一部分展示。只需从定义开始。）–

  证明 $\text{PreIm}_f(Z) \subseteq T$. ∗ 设 $a \in \text{PreIm}_f(Z)$ 为任意且固定的。∗ 这意味着 $f(a) \in Z$。∗ 使用 f 的性质来证明 $a \in T$。

  – 证明 $T \subseteq \text{PreIm}_f(Z)$。∗ 令 $x \in T$ 为任意且固定的。∗ 使用 f 的性质来证明 $f(x) \in Z$。∗ 这表明 $x \in \text{PreIm}_f(Z)$。– 通过双重包含论证得出结论：$\text{PreIm}_f(Z) = T$。

- 找到 **inverse** 的 f。
  - 定义一个函数 $F\colon B \to A$。

    （注意：提出这个定义是难点，需要大量草稿工作。无需将此作为证明的一部分展示。只需从定义开始。）

– 证明 F 是一个定义良好的函数：证明来自 B 的每个输入都有且只有一个输出属于 A。– 证明 $F \circ f = \mathrm{Id}_A$。– 证明 $f \circ F = \mathrm{Id}_B$。– 推导出 $F = f^{-1}$。（由于 f 有逆元，因此它是一个双射。）

A.6 Cardinality

A.6.1 Definitions

设 S 为任意集合。

- 我们称 S 为 **finite**，如果存在一个双射 $f\colon S \to [n]$，使得 $\exists n \in \mathbb{N} \cup \{0\}$ 成立。注意：空集 $S = \varnothing$ 是有限的，因为 $[0] = \varnothing$。

- 我们称 S 是 **infinite**，如果 S 是 *not finite*；也就是说，如果 $\forall n \in \mathbb{N} \cup \{0\}$，每个函数 $f\colon S \to [n]$ 都无法成为双射。

- 我们称 S 为 **countably infinite**（或简称为 **countable**），如果存在一个双射 $f\colon S \to \mathbb{N}$。

- 我们称 S 为 **uncountably infinite**（或简称为 **uncountable**），如果每个函数 $f\colon S \to \mathbb{N}$ 都无法成为双射。

- 我们使用 $|S|$ 来表示 **cardinality** 的 S。当 S 是有限的，因此存在某个 $n \in \mathbb{N} \cup \{0\}$ 和一个双射 $f\colon S \to [n]$，我们写 $|S| = n$ 来表示 S 有 n 个元素。我们说 n 是 S 的 **size**。当 S 是无限的，我们只使用 $|S|$ 来 **compare** S 的基数与其他集合的基数。也就是说，我们不写像 $|S| = \infty$ 这样的东西；而是写像 $|S| = |T|$ 这样的东西来表示 S 和 T 有相同的基数，无论这个基数是什么，或者写像 $|S| < |T|$ 这样的东西来表示 T 的基数比 S 大。

- 我们写 $|S| = |T|$ 并说 S 具有作为 T 的 **same cardinality** 当且仅当存在一个双射 $f\colon S \to T$。

A.6.2 Results

一般来说，以下结果成立。一些剩余的结果可从这些一般性陈述中得出。

- 假设 $|A| = |C|$ 和 $|B| = |D|$。然后 $|A \times B| = |C \times D|$。

- 假设 $|A| = |C|$ 和 $|B| = |D|$，并且假设 $A \cap B = \varnothing$ 和 $C \cap D = \varnothing$。然后 $|A \cup B| = |C \cup D|$。

- 假设存在一个注入 $f\colon A \to B$。然后 $|A| \leq |B|$。

- 假设存在一个满射 $f\colon A \to B$。那么 $|A| \geq |B|$。

Finite Sets

- 如果 A 和 B 是有限的，那么 $A \cup B$ 也是有限的。
- 如果 A 和 B 是有限的，并且 $A \cap B = \varnothing$，那么 $|A \cup B| = |A| + |B|$。
- 如果 A 和 B 是有限的，那么 $|A \times B| = |A| \cdot |B|$。

Infinite Sets

- 如果 A 是可数无穷大且 B 是有限或可数无穷大，那么 $A \cup B$ 是可数无穷大。
- 如果 A 是可数无穷大且 B 是有限或可数无穷大，那么 $A \times B$ 是可数无穷大。
- 如果 A 是不可数无穷的，并且 B 是任何集合，那么 $A \cup B$ 是不可数无穷的。
- 如果 A 是不可数无穷的，并且 B 是任何集合，那么 $A \times B$ 是不可数无穷的。
- 如果 $A \subseteq B$，则 $|A| \leq |B|$。（注意：这适用于有限集和无限集。）
- $|A| < |\mathcal{P}(A)|$ 对于任何集合 A。(注意：这适用于有限集和无限集！)
- 如果 A 是无穷的，那么存在一个可数无穷的集合 $C \subseteq A$。
- A 是无限 $\iff$ $\exists C \subset A$，使得存在一个双射 $f\colon A \to C$。（注意 *strict* 子集不等式。）
- 可数无限个可数无限集的并集也是可数无限的。
- 一个有限集的可数无穷乘积是不可数无穷的。（注意，这表明任何非空集的可数无穷乘积都是不可数无穷的。）
- **Cantor-Schröder-Bernstein Theorem:** 假设 A 和 B 是集合，并且存在函数 $f\colon A \to B$ 和 $g\colon B \to A$，它们都是 *injections*。那么实际上存在一个 *bijection* $h\colon A \to B$，因此特别地，$|A| = |B|$。

A.6.3 Standard Catalog of Cardinalities

- **Finite sets:**
  - $\varnothing$
  - $[n]$，对于任意的 $n \in \mathbb{N}$
- **Countably Infinite sets:**
  - $\mathbb{N}$
  - $\mathbb{Z}$
  - 奇数自然数/整数，偶数自然数/整数
  - 所有二进制字符串的集合
  - $\mathbb{Q}$
  - $\mathbb{N} \times \mathbb{N}$
  -
- **Uncountably Infinite sets:**
  - $\mathbb{R}$
  - 区间 $\mathbb{R}$；即，对于任何 $a, b \in \mathbb{R}$，有 $\{y \in \mathbb{R} \mid a \leq y \leq b\}$。（注意：区间中的“$\leq$”也可以分别替换为“$<$。”）
  - $\mathcal{P}(\mathbb{N})$ 所有 *infinite* 二进制字符串的集合
  - $\mathcal{P}(\mathbb{Z})$
  -

A.7 Combinatorics

A.7.1 Definitions

- 集合 $[n]$ 中的一个 **permutation** 是一个双射 $f : [n] \to [n]$。
- 一个 k**-selection** 来自集合 $[n]$，是子集 $S \subseteq [n]$，包含 $|S| = k$。
- 一个 k**-arrangement** 来自集合 $[n]$，是 $[n]$ 中 k 元素的有序列表，其中没有重复的元素。
- 一个 k**-selection with repetition** 来自集合 $[n]$，是无序的 k 元素列表 [n]，其中元素可以重复。
- 一个 k**-arrangement with repetition** 来自集合 $[n]$，是 $[n]$ 中 k 个元素的有序列表，其中元素可以重复。

A.7.2 Counting Principles

- **Rule Of Sum:** 设 A 为一个有限集。设 $n \in \mathbb{N}$。假设 $\{S_i \mid i \in [n]\}$ 是 A 的一个划分。那么

$$|A| = \sum_{i=1}^{n} |S_i| = |S_1| + |S_2| + \cdots + |S_n|$$

- **Rule Of Product:** 假设我们有一个在 n 个步骤中完成的进程。假设步骤 i (其中 $1 \leq i \leq n$) 可以以 w_i 种方式完成，独立于前一步的选择。那么这个进程的结果数是

$$\prod_{i=1}^{n} w_i = w_1 \cdot w_2 \cdots w_n$$

A.7.3 Formulas

- 有 $n!$ 种 $[n]$ 的排列方式。
- 存在从 $[n]$ 中选出的 k 的 $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ 种选择。
- 存在 $\binom{n}{k}\, k!$ 有 $= \frac{n!}{(n-k)!}$ 多个 k-排列从 $[n]$。
- 存在 $\binom{k+n-1}{k}$ 个有重复的 k-选择，从 $[n]$ 中。
- 存在 n^k 个重复的 k 安排从 $[n]$。

A.7.4 Standard Counting Objects

- **Cards:** 一副标准扑克牌有52张牌。每张牌都有花色（要么是♡要么是♢要么是♣要么是♠）和点数（要么是2要么是3要么是4……要么是10要么是Jack要么是Queen要么是King要么是Ace）。

- **Tuples:** 设 $k, n \in \mathbb{N}$。集合 $T_{n,k}$ 是从 $[k]$ 中所有 n-元组的集合。也就是说，它是所有长度为 n 且坐标为 $[k]$ 中元素的有序列表的集合。

- **Words:** 这是等价于元组，其中 $[k]$ 代表字母表，n 代表单词的长度。

- **Lattice Paths:** 设 $x, y \in \mathbb{N}$。到 (x, y) 的一个格点路径是平面上自然数点网格上的点序列，从 $(0, 0)$ 出发，到 (x, y) 结束，其中每次移动要么向右，要么向上。到 (x, y) 有 $\binom{x+y}{x} = \binom{x+y}{y}$ 条格点路径。

A.7.5 Counting In Two Ways

这是一个使用组合论证证明恒等式标准方法。

Method Outline:

1. 陈述要证明的结果。注意：记得量化表达式中出现的任何变量！2. 定义一个要计数的对象集合（让我们称其为S）。3. 通过遵循适当的组合论论证，以某种方式计数S的元素。将所得表达式与$|S|$相等。4. 通过遵循适当的组合论论证，以另一种方式计数S的元素。将所得表达式与$|S|$相等。5. 结论是，由于两个导出表达式都等于$|S|$，它们必须相等。

A.7.6 Results

这些在讲座中通过两种方式计数论证得到了证明。（您可以在没有证明的情况下引用这些结果，但记住计数论证的主要思想也是有帮助的，这样您就可以在不只是记住它的情况下重建公式。）

- **Pascal's Identity:** $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

- **Chairperson Identity:** $\binom{n}{k} \cdot k = n \cdot \binom{n-1}{k-1}$
- **Binomial Theorem:** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
- **Summation Identity:** $\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$

A.7.7 Inclusion/Exclusion

我们有全集 U 和一些子集 $A_1, A_2, \ldots, A_n \subseteq U$。我们想要计算所有 A_i 集合的 *outside* 的 U 的元素数量。

$$\begin{aligned} |U - A_1| &= |U| - |A_1| \\ |U - (A_1 \cup A_2)| &= |U| - |A_1| - |A_2| + |A_1 \cap A_2| \\ |U - (A_1 \cup A_2 \cup A_3)| &= |U| - |A_1| - |A_2| - |A_3| \\ &\quad + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \\ &\quad - |A_1 \cap A_2 \cap A_3| \end{aligned}$$

等等。

通常，对于 n 许多集合，我们有

$$|U - (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{S \subseteq [n]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right| \qquad \text{where} \quad \bigcap_{i \in \varnothing} A_i = U$$

在（方便的）情况下，当*size*的交集仅依赖于该值k (而不是我们交集的*which*集合时，我们可以写出

$$|U - (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} |S_1 \cap S_2 \cap \cdots \cap S_k|$$

A.7.8 Pigeonhole Principle

如果将包含 $|S| = n$ 的集合 S 划分为 k 个不相交的子集，其并集为 S，并且如果 $k < n$，那么划分中的至少一个子集包含多于一个元素。此外，该部分实际上至少有 $\lceil \frac{n}{k} \rceil$ 个元素。

（即，如果我们把 n 个对象分成 k 堆，其中必定有一堆至少有 $\frac{n}{k}$ 个对象。）

A.8 Acronyms

A.8.1 General Phrases

- **WWTS**我们想展示
- **AFSOC**假设为了反证
- **WOLOG**无失一般性

A.8.2 Induction

- **PMI**数学归纳法原理
- **BC**基本情形
- **IH**归纳假设
- **IS**归纳步骤