数论

2023 年 4 月 9 日

目录

1 数论

数论是代数的基础，所以我们今天先整点数论。

1.1 数学归纳法

数学归纳法是一种非常常用的证明方法，我们先来看归纳法适合什么样的东西。

在自然科学中，归纳推理是用来断言频繁观察到的现象一直发生的，因此，我们经常说太阳早上会升起，是因为太阳每天都有升起。但在数学中这并不是合格的证明，例如火鸡悖论。

指的是假设你是一只火鸡，被农夫养在美国的农场。在过去的120天里，你都很幸福，因为农夫每天都给你吃的。所以，随着时间的推移，你的幸福指数直线上升，是线性发展的。绝大多数人都会像这只火鸡一样，站在过去看现在，站在现在预测未来。作为一只火鸡，你认为这种幸福会永远地延续下去。但很不幸，明天就是感恩节了，大家知道会发生什么事。火鸡的幸福指数戛然而止，因为火鸡不知道要过感恩节，感恩节人们要烤火鸡吃。

起初这是罗素在批判滥用归纳法的行为，但这也说明了，直觉不一定是对的，就像这只火鸡一样。为此我们需要严格的证明方法。

在进一步的叙述之前，我们需要给一些标准术语的含义：数$0, 1, -1, 2, -2, 3, \cdots$我们称为整数，整数的集合我们记作$\mathbb{Z}$

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

然后是我们熟悉的自然数集，自然数集合是由所有满足$n \geq 0$的整数n构成的

$$N = \{n \in Z, n \geq 0\} = \{0, 1, 2, 3, \cdots\}$$

1.1.1 素数

素数是一种奇怪的数，除了自身和1外没有别的因数分解。为此我们给出如下定义

定义：设n, d为两个整数，现在如果存在整数a，使得$n = da$，则称d为n的一个因子，一个自然数n称为素数，当且仅当$n \geq 2$的时候因子只有± 1和$\pm n$

如果$n \leq 2$的时候自然数不是素数，那么我们称为合数。对于任意大于0的合数n，则存在分解为$n = ab$，其中$a, b < n$。现在我们就存在了两个问题：1、表达式$f(n) = n^2 - n + 41$能够表达每一个素数吗；2、素数是有限的吗？

我们先来看第一个问题。我们假设成立，就可以对其使用归纳法，因为根据假设，每个素数都可以被表达式$f(n)$所表达，那么我们对$n = 1, 2, 3, \cdots, 40$带入表达式看看结果。

$$41, 43, 47, 53, 61, 71, 83, 97, 113, 131$$
$$151, 173, 197, 223, 251, 281, 313, 347, 383, 421$$
$$461, 503, 547, 593, 641, 691, 743, 797, 853, 911$$
$$971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.$$

好的，现在看起来没问题，但是$n = 41$的时候$f(41) = 1681 = 41^2$不是素数，为此不能使用归纳，这也暴露了一个问题，归纳假设不适用于数学证明。

第二个问题我们将在等一下做解答。

上述例子已经说明归纳法不适用于在什么方面，现在我们则要来讨论归纳法能用在什么方面

最小整数公理　对于自然数集$\mathbb{N}$的每个非空子集C，都含有一个最小整数。对于这个公理，实际上就是遍历集合的元素，先检查0，看是否属于C，如果是，那么0就是最小的，否则检查数1，然后持续这个步骤。所以我们最终都能找到一个最小整数。

命题：最小反例　对上述公理我们可以做这么一个拓展。

设k是一个自然数，$S(k), S(k+1), \cdots, S(n)$是一组命题，若命题中存在一些假命题，那么一定能找到第一个假命题

证明：我们设C为一个由命题S中为假命题构成的集合，根据假设有：C是$\mathbb{N}$的一个子集，为此由最小整数公理可知，一定存在一个最小整数m，使得$S(m)$为假命题。

1.1.2 定理：每个整数$n \geq 2$或是素数或是素数的乘积。

这其实挺好理解的，对每个分解$n = ab$，假设a是素数，那么$b = cd$，若c, d里面都是合数，则进一步的分解即可，这样子就有因为偶数是一些可以除以2的数，只需要做如下操作可得：$d = 2 \times 2 \times \cdots \times d_n$，其中$d_n$为素数。

证明：我们假设结论不成立，则存在反例使得当整数$n \geq 2$时既不是素数也不是一些素数的乘积，则根据最小反例可知，我们令m为这些数中最小的一个，由于m不是素数，则m为合数，而合数存在分解$m = ab$，其中$2 \leq a < m$和$2 \leq b < m$，那么由于m是最小反例，则a, b都可以使得定理成立有

$$a = pp'p'' \cdots ,\ \ b = qq'q'' \cdots$$

其中p, q是素数。由于m是最小反例，但$m = ab$且a, b都是素数的乘积。那么m就可以表示成素数的乘积，我们得到矛盾。

1.1.3 命题：设$m \geq 2$为正整数，若m不能被任何满足$p \leq \sqrt{m}$的数整除，则m为素数

证明：若m不是素数，那么$m = ab$，其中a, b是正整数，且$a, b < m$。若$a, b > \sqrt{m}$。那么就有$m = ab > \sqrt{m}\sqrt{m} = m$矛盾。为此，假设$a \leq \sqrt{m}$，由定理1.1.2可知，$a$是一个素数，或者是素数的乘积。那么$a$的任何素因子$p$也是$m$的一个因子，那么$m$在这种情况就不是素数，则存在一个最小素因子。有$p \leq \sqrt{m}$，否则$m$自己就是一个素数。

现在，利用该命题我们可以来证明991是一个素数。$\sqrt{991} \approx 31.48$，若991不能被$2, 3, 5, \cdots, 31$整除，那么就是一个素数。里面包含11个素数，但是都不能整除991。所以991是一个素数。

1.1.4 定理数学归纳法

给定一组关于自然数$n \geq 1$的命题$S(n)$，假设

1. 基础步骤：$S(1)$成立。

2. 归纳步骤：若$S(n)$成立，则$S(n+1)$成立。那么对一切$n \geq 1$，$S(n)$成立

证明：依然是设C为一组命题$S(n)$中假命题的集合。我们要证C是空集。

我们假设C是非空的集合，那么存在一个假命题$S(m)$，现在因为$S(1)$是成立的，所以$m \geq 2$，因为不存在$S(0)$这种东西，那么$m-1 \geq 1$，现在，由于m为最小反例，那么$m-1$就是成立的，因为$m-1$成立，那么$S(m) = S(m-1+1)$是成立的。这是个矛盾，为此$S(n)$所有的命题是成立的。

1.1.5 命题：证明对正整数$n \geq 1$，$2^n > n$成立

证明：运用归纳法，首先有

$$S(1) = 2^1 > 1$$

成立，我们假设$S(n)$成立，有

$$S(n) = 2^n > n$$

要利用归纳假设，我们要证明$S(n+1) = 2^{n+1} > n+1$。那么因为$S(n)$成立，则

$$S(n+1) = S(n) \times 2 = 2^n \times 2 > 2n$$

又因为$2n > n+1$，所以由归纳假设有

$$S(n+1) > n+1$$

证毕

1.2 平均数

给定一组正数$a_1, a_2, \cdots, a_n$，则它们的算术平均数是$(a_1 + \cdots + a_n)/n$，而几何平均数指的是$\sqrt[n]{a_1 a_2 \cdots a_n}$

几何平均数肯定是比算术平均数小的，因为两者的累加不是一个级别的东西。

考虑恒等式

$$(x+y)^2 = (x-y)^2 + 4xy$$

有

$$\begin{aligned}\left[\frac{1}{2}(x+y)\right]^2 =& xy + \left[\frac{1}{2}(x-y)\right]^2 \\ \frac{1}{2}(x+y) =& \sqrt{xy} + \frac{1}{2}(x-y)\end{aligned}$$

从式子中不难发现

$$\frac{1}{2}(x+y) > \sqrt{xy}$$

所以几何平均数比算术平均数小。

1.2.1 引理：如若$0 < m < 1 < M$，那么$m + M > 1 + mM$

证明：设$f = m + M - 1 - mn$，则有$f = (1-m)(M-1)$，由于$1 > m$和$M > 1$，那么$1-m$和$M-1$是正数，也就有

$$M - 1 - mM + m > 0 \iff m + M > 1 + mM$$

1.2.2 引理：若$k_1, \cdots, k_n$都是正数且$k_1 \cdots k_n = 1$，那么$k_1 + \cdots + k_n > n$

直观上来说，考虑任意小的分数x，在考虑一个y，只要令 $xy \geq 1$就行，等式成立就只有$x = y = 1$，选择其他的任意都有$2 + \frac{1}{2} > 2$，或者考虑任意小的数有

$$1.0000000000000000001 + \frac{1}{1.0000000000000000001} = 2.00000000000000000000000000000000000009$$

证明：若$k_1 = \cdots = k_n = 1$显然有$k_1 + \cdots + k_n = n$，考虑对于不完全的$k_i = 1$有$k_1 + k_2 + \cdots + k_n$。我们利用归纳法

现在有$k_1 k_2 = 1$，如果$k_1, k_2 > 1$，则$k_1 k_2 > 1$或者$k_1, k_2 < 1$则有$k_1 k_2 < 1$，为此，可能的取值范围是$0 < k_1 < 1 < k_2$，利用引理1.2.1有$k_1 + k_2 > 1 + k_1 k_2 = 2$成立。

假设$k_1\cdots k_{n+1}=1$，由引理1.2.1可知有

$$k_1+k_{n+1}>1+k_1k_{n+1}$$

两边加$k_2+\cdots+k_n$有

$k_1+\cdots+k_n > 1+k_1k_{n+1}+k_2+\cdots+k_n$ 现在我们的工作就是证明$1+k_1k_{n+1}+k_2+\cdots+k_n\geq n+1$。

现在有$k_1k_{n+1}k_2\cdots k_n=1$，若$k_1k_{n+1}=1=k_2=\cdots=k_n$，那么等式$1+k_1k_2+\cdots+k_n=n+1$成立。否则，我们对其使用归纳假设，刚才已经证明了当k_1+k_2的时候成立，现在设对$k_1k_n+\cdots+k_{n-1}$成立，那么有

$$k_1k_{n+1}+\cdots+k_n>n$$

成立,有

$$1+k_1k_{n+1}+\cdots+k_{n-1}+k_n>n+1$$

证毕。

1.2.3 定理：平均不等式

因为算术平均数大于几何平均数，那么我们可以给出一个不等式

若$a_1,\cdots,a_n$均为正数，则

$$(a_1+\cdots+a_n)/n\geq\sqrt[n]{a_1a_2\cdots a_n}$$

在刚才我们只是给出了一个直观上的理解并且证明了对于两个元素的不等式成立。即$\frac{1}{2}(x+y)\geq\sqrt{xy}$，另外，等式成立当且仅当$k_1=\cdots=k_n=1$。

证明：我们定义$G=\sqrt[n]{a_1a_2\cdots a_n}$，现在，要使用之前的引理，我们只需要令每个$k_i=a_i/G$，那么就存在

$$k_1k_2\cdots k_n=\frac{a_1a_2\cdots a_n}{G^n}=1$$

再由引理1.2.2有$k_1+k_2+\cdots+k_n\geq n$，那么就有

$$k_1+k+2+\cdots+k_n\geq n\iff\frac{a_1+\cdots+a_n}{G}\geq n\Rightarrow a_1+\cdots+a_n\geq nG$$

为此，就得到了平均不等式$(a_1+\cdots+a_n)/n\geq\sqrt[n]{a_1a_2\cdots a_n}$

1.3 第二归纳法

第二归纳法也是一种比较方便的方法，只不过形式与第一归纳法有些许差别

设$S(n)$是关于正整数n的一组命题，设

1. **$S(1)$成立且**

2. **若对n之前的全部条件$1, 2, \cdots, n-1$成立，那么$S(n)$成立则$S(n)$对一切整数$n \geq 1$都成立。**

不难看出，第二归纳法只是在归纳法上做了些许改变。

1.3.1 命题：对于每个整数$n \geq 1$都存在唯一分解$n = 2^k m$，其中$k \geq 0$，而$m \geq 1$为奇数。

这是一个比较平凡的性质，由于整数除了奇数就是偶数，那么每个偶数a都能被2整除，那么每个部分都是$a = 2m$，如果m为偶数则我们继续做分解，直到不能被2整除。

为了证明这个平凡的性质，我们首先对$n \geq 1$引用第二归纳法来证明k, m的存在性

首先，对于$n = 1$的时候，$k = 0, m = 1$成立。现在，我们假设对$n \geq 1$，则n有两种情况，奇数或者偶数，对于奇数，取$k = 0, m = n$即可，当n为偶数，我们取$n = 2b$，因为$b < n$，所以b可以取一个满足假设的条件，即$b = 2^t m$，其中$t \geq 0, m$是奇数。整合起来就有$n = 2b = 2^{t+1}m$证毕

现在我们来证明唯一性，若$n = 2^k m = 2^t m'$，t, k非负。且m, m'都是奇数，对于第一种情形，只需要令$t = k, m = m'$就有结论了，但是对于第二种，不妨设$k > t$，我们从两边消去2^t得到2^{k-t}，那么就有$2^{k-t}m = m'$得到左边是偶数，右边是奇数，矛盾。为此分解是唯一的。

黄金比率是古希腊人很喜欢的一组数，他们认为满足这种关系的长方形都很漂亮。即

$$a : b = b : (a + b)$$

那么就有$a(a+b) = b^2$，那么有$b^2 - ab - a^2 = 0$我们可以从中解得

$$b/a = \gamma = \frac{1}{2}(1 + \sqrt{5}) \text{ 或 } b/a = \delta = \frac{1}{2}(1 - \sqrt{5})$$

我们讨论这种比率的原因是，它和斐波那契数列相关。

1.4 定义:斐波那契数列

斐波那契数列指的是$F_0, F_1, \cdots$指的是

$$F_0 = 0, F_1 = 1\text{对所有整数}n > 2\text{存在}F_n = F_{n-1} + F_{n-2}$$

1.4.1 命题：斐波那契数列的通项

我们用F_n表示斐波那契数列的第n项，则对于所有的$n \geq 0$有

$$F_n = \frac{1}{\sqrt{5}}(\gamma^n - \delta^n)$$

其中$\gamma = \frac{1}{2}(1+\sqrt{5})$，$\delta = \frac{1}{2}(1-\sqrt{5})$

该通项不是通过归纳法得到的，但是我们可以通过归纳法证明公式的正确性。验证$n = 0$的情况，有$F_0 = \frac{1}{\sqrt{5}}(\gamma^0 - \delta^0) = 0$成立，在验证$F_1 = \frac{1}{2\sqrt{5}}(2\sqrt{5}) = 1$成立

因为我们要证明的含有两个命题，F_{n-1}, F_{n-2}，只有一个F_{n-1}或者F_{n-2}都是不够的，所以我们才证明了当$n = 0, 1$的情况。

首先有$\gamma + 1 = \gamma^2$, $\delta + 1 = \delta^2$。则

$$\begin{aligned}
F_n =& F_{n-1} + F_{n-2} \\
=& \frac{1}{\sqrt{5}}(\gamma^{n-1} - \delta^{n-1}) + \frac{1}{\sqrt{5}}(\gamma^{n-2} - \delta^{n-2}) \\
=& \frac{1}{\sqrt{5}}(\gamma^{n-1} + \gamma^{n-2}) + \frac{1}{\sqrt{5}}(\delta^{n-1} + \delta^{n-2}) \\
=& \frac{1}{\sqrt{5}}(\gamma^{n-2}(\gamma+1) + \delta^{n-2}(\delta+1)) \\
=& \frac{1}{\sqrt{5}}(\gamma^{n-2}(\gamma^2) + \delta^{n-2}(\delta^2)) \\
=& \frac{1}{\sqrt{5}}(\gamma^n - \delta^n)
\end{aligned}$$

斐波那契数列的通项最令人惊讶的实际上是，我们由一堆无理数得到了一个个整数。

最后由斐波那契数列给出一个推论来结束这章

1.4.2 推论：对所有整数$n \geq 3$，有$F_n > \gamma^{n-2}$

若$n = 3$，那么有$F_3 = 2 > \gamma, \gamma \approx 1.618$成立，现在假设$F_n > \gamma^{n-2}$成立，则

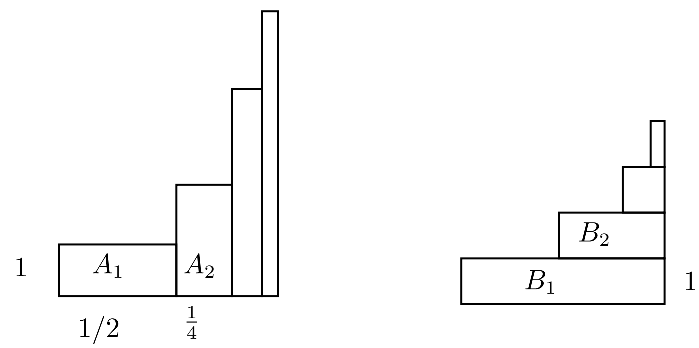
$$F_{n+1} = F_n + F_{n-1} > \gamma^{n-2} + \gamma^{n-3} = \gamma^{n-3}(\gamma^2) = \gamma^{n-1}$$

推论成立。

顺便写两道习题

1.5 习题

大约在1350年，奥雷姆（N.Presme）就通过下图的分割用两种方法求级数$\sum_{n=1}^{\infty} \frac{n}{2^n}$的和，设$A_n$是底为$\frac{1}{2^n}$，高为$n$的直角三角形。不难算出$A_n$的面积为$n/2^n$。设$B_n$是以底为$\frac{1}{2^n} + \frac{1}{2^{n+1}} \cdots$，高1的矩形。证明：$\sum_{n=1}^{\infty} \frac{n}{2^n} = 2$



解：图片的给出是因为一个提示，我们要给出一个证明来解决这个问题，即阿贝尔求和公式。

阿贝尔求和公式：设$a_i, b_i, i = 1, 2, 3, \cdots$为两组实数，令$B_k = b_1 + \cdots + b_k$，则下面公式成立

$$\sum_{i=1}^{n} a_i b_i = (a_1 - a_2)B_1 + (a_2 - a_3)B_2 + \cdots + (a_{n-1} - a_n)B_{n-1} + a_n B_n$$

给出两组实数$a_i, b_i, i = 1, 2, 3, \cdots$，令

$$B_k = b_1 + \cdots + b_k$$

而$B_k - B_{k-1} = b_k$ 那么我们就可以把公式给变成

$$\begin{aligned}\sum_{i=1}^{n} =& a_1b_1 + \cdots + a_nb_n \\ =& B_1a_1 + (B_2 - B_1)a_2 + \cdots + (B_{n-1} - B_{n-2})a_{n-1} + (B_n - B_{n-1})a_n \\ =& B_1(a_1 - a_2) + B_2(a_2 - a_3) + \cdots + B_n(a_{n-1} - a_n) + B_na_n\end{aligned}$$

证毕。

现在重新看题目，题目要求的是求$\sum_{n=1}^{\infty}\frac{n}{2^n}$的和，为此我们应用阿贝尔求和公式有

令$a_i = n_i$, $b_i = \frac{1}{2^i}$有

$$\begin{aligned}\sum_{i=1}^{n}\frac{i}{2^i} =& (1-2)\frac{1}{2} + (2-3)\left(\frac{1}{2}+\frac{1}{4}\right) + \cdots + (n-1-n)\left(\sum_{i=1}^{n-1}\frac{1}{2^i}\right) + n(1-\frac{1}{2^n}) \\ =& n(1-\frac{1}{2^n}) - \left(\sum_{i=1}^{n-1}B_i\right), \qquad \text{其中}B_k = \sum_{i=1}^{k}\frac{1}{2^i} = 1 - \frac{1}{2^n} \\ =& n - \frac{n}{2^n} - (n-1) + \frac{1}{2}\frac{1-\frac{1}{2^{n-1}}}{1-\frac{1}{2}} \\ =& -\frac{n}{2^n} + 1 + \left(1 - \frac{1}{2^{n-1}}\right)\end{aligned}$$

现在，因为题目要求给的是无穷级数，我们需要做最后一件事情做极限

$$\lim_{n\to\infty} -\frac{n}{2^n} + 1 + \left(1 - \frac{1}{2^{n-1}}\right) = 2$$

其中$\frac{n}{2^n}$的极限为0由命题1.15可推出。

所以

$$\sum_{n=1}^{\infty}\frac{n}{2^n} = 2$$