每周定理

BY WHZECOMJM

July 1, 2020

我很早就是每周定理（Theorem of the week）这一博客的读者，不过之前并没有系统的去看完所有的博文，做一个忠实的读者。最近，我在看过它关于随机图的概率证明（即Erdos关于拉姆齐数的一个下界的证明）之后，突然意识到这一博客的语言很自然，且会以很多简单的例子入手，因此值得推广它的做法。博客的作者维姬尼尔（Vicky Neale）是一位牛津大学的Whitehead Lecturer。然而遗憾的是，这一博客现在已经停止更新多年。但是得益于它对我的帮助，我决定把它的每周定理做一个简单的翻译和改写，这样有利于我自己偶尔复习查阅，也方便其他中文读者阅读。

目录

1 裴蜀定理

你是否遇到过用有限数量的容器测量一定量水的问题？或者类似的有限砝码天平测量物体的问题。以下是一个例子。

假设我有两个桶。一个满了水是3升，另一个盛满是5升。我希望从花园用这两个桶打水，使得能往我的池塘里装上17升水。如果仅仅用这两个桶这可能吗？

简单的思考，我们可以得到一个答案，即用3升桶打4次，5升桶打1次即可。因为 $17 = 4 \times 3 + 5$。

如果我们仅仅需要1升水呢？我们可以考虑先用3升水桶打两次，再用5升水桶从其中取出一次。也就是有方程：$1 = 2 \times 3 - 5$.

如果我们把水桶的规格换为3升和6升，还能得到一升水吗？答案是不能，因为无论我们是打水进水池还是从中打水出来，每次操作改变的水量都是3升的倍数。也就是说，我们有 $3m + 6n = 3(m + 2n)$。这里的 3 称为 3 和 6 的最大公约数，记为 $3 = \gcd(3, 6)$。

现在我们把上述过程数学化，也就有了Bezout定理。

定理 1.1. (Bezout) 令h, k为整数。则存在整数m, n满足方程

$$hm + kn = 1 \tag{1.1}$$

当且仅当$\gcd(h, k) = 1$。

上述等式称为Bezout等式。我们需要用到欧几里得算法（即辗转相除法）。辗转相除法给出了一个求两个数的最大公约数的办法，同时还给出了一个解 Becout 等式的办法。

辗转相除法此处不再赘述，网上有大量资料，也是中小学生学习过的内容。它恰好给出了解等式的方法。另一方面如果方程满足，则必然最大公约数是1，否则等式右边只能得到最大公约数的倍数。

上述定理的一个自然的推论如下：

定理 1.2. 令h, k为整数。则存在整数m, n满足方程

$$hm + kn = \gcd(h, k). \tag{1.2}$$

2 中值定理

第二周的定理更多的是讲述作者的修钟表的故事。他讲述了调整了摆钟以后每周会快40分钟，之后往回调又慢了60分钟。如果假定调节是连续的，则一定存在一个调节使得时间刚刚好。这就是中值定理。

定理 2.1. (中值定理) 令 $f:\mathbb{R}\to\mathbb{R}$的函数，若$f$在 $[a,b]$ 中连续，且 $f(a)<0, f(b)>0$，则存在点c，满足$a<c<b$使得$f(c)=0$。

作者仅仅介绍了这一定理，并没有给出证明和进一步的结果。不过一个很自然的推论是，如果 $h\in(f(a),f(b))$，则必然存在 $a<c<b$使得 $f(c)=h$。

3 三素数定理

大概哥德巴赫不会想到他在1727年给欧拉的信奠定了他的数学名声。哥德巴赫猜想是当今数学中著名的未解问题之一。 它出名的主要原因之一也许是因为它很容易表述，但显然非常难。

猜想 3.1. (哥德巴赫) 每一个大于2的偶数均等于两个素数之和。

比如，$18=11+7, 92=89+3$。这一猜想被称为**（强）哥德巴赫猜想**。另一个哥德巴赫提出的三素数之和的相关猜想，似乎没那么有名，但是显然是上述猜想的一个推论。

猜想 3.2. (哥德巴赫) 每一个大于5的奇数均等于三个素数之和。

比如，$7=2+2+3, 91=3+5+83$。这一猜想又被称为**弱哥德巴赫猜想**或**三元哥德巴赫猜想**。对于奇数的猜想，最著名的结果来自于俄罗斯数学家维诺格拉多夫 （Ivan Vinogradov）。

> 他的主要贡献在解析数论方面。 1934年提出了估计外尔三角和的新方法， 对华林问题作了重大改进。 1937年他引进了线性素变数三角和的概念， 从而证明了三素数定理 。即： 存在正数c使得每个大于c的奇数是3个奇素数之和。他一生不断完善和发展估计各种三角和的方法， 在许多数论问题上得到重要结果。他的方法已成为解析数论的强有力的工具， 并在分析学、 近似计算、 概率论及数学物理等领域得到应用。 他的初等数论这本书在中国很有名。
>
> —— 百度百科，维诺格拉多夫

维诺格拉多夫证明了如下著名的三素数定理：

定理 3.3. (维诺格拉多夫) 任何一个足够大的奇数可以写成三个素数之和。

这个足够大的奇数并没有确切的指定，不过维诺格拉多夫证明了存在性。这距离哥德巴赫猜想的证明十分接近，因为三素数定理表明不满足哥德巴赫猜想（奇数）的整数是有限个的。

最近， H. A. Helfgott 在2014年的文章中证明了**三元哥德巴赫猜想**（Ternary Goldbach Conjecture）。他先基于圆法、大筛法、三角和估计等方法证明了对 $n \geq 10^{27}$ 的一切奇数 n 该猜想成立（也就是上述提到的足够大的奇数）， 同时又对 $n \leq 8.875 \times 10^{30}$ 进行了计算机的验证，最终得到了如下的三元哥德巴赫定理

定理 3.4. (Goldbach-Helfgott) 每一个大于5的奇数均等于三个素数之和。

至于强哥德巴赫猜想，目前最好的结果仍然是陈景润的 $(1+2)$。其无法攻克的难度即使在今天仍然存在， 实际上， H. A. Helfgott 在证明了三元哥德巴赫定理之后说过： *The strong conjecture remains out of reach*。

------ 具体关于三素数定理的证明可以参见三素数定理的证明及其方法（一）以及潘承洞和潘承彪的专著《哥德巴赫猜想》。

维诺格拉多夫不是第一个在这个定理上取得进展的人。 早在1923年， G.H. Hardy 和J.E. Littlewood便奠定了基础。 他们用所谓的圆法(现在通常被称为Hardy-Littlewood圆法)证明了,如果广义黎曼假设是正确的,那么每一个足够大的奇数可以写成三个素数之和。 (广义黎曼假设为他们提供了一些质数分布所需的信息。 不过这一假设直到今天仍未被证明)然后在1937年维诺格拉多夫提出了一种方法，也使用了圆法，但它不需要广义黎曼假设的假设。

圆法已被用于许多其他问题。Hardy和 Srinivasa Ramanujan用它来研究将数字N写成和(划分函数)的方法的个数， Hardy和Littlewood用它给出了Waring问题的一个新的证明(David Hilbert给出了第一个证明)。

不幸的是，圆法似乎不能用来证明著名的强哥德巴赫猜想——尽管这当然并不意味着该猜想是假的!

4 范德瓦尔登定理

范.德.瓦尔登(Van der Waerden, Bartel Leendert,1903-1996)荷兰数学家、 数学史家.生于阿姆斯特丹， 1926年获阿姆斯特丹大学博士学位。先后在哥罗宁根(Groningen)、莱比锡、阿姆斯特丹、苏黎世等地的各大学任教。

范.德.瓦尔登的主要贡献在代数、代数几何、群论方法在量子物理和数理统计中的应用等方面. 他撰写的《近世代数》(上、下册，1930-1931)对代数学的发展起了重要影响， 它的出版标志着“抽象”代数的初创时期已经结束.这部著作从某种程度上确定了后来代数研究的特点和方向.其修订本后来改名为《代数学》(1955)，增加了许多新的研究成果.范 .德.瓦尔登还是一位数学史家， 他对古埃及、 巴比伦和希腊的数学和天文学颇有研究.著作有《 代数几何导论》 (1939), 《 量子力学中的群论方法》(1932), 《科学的觉醒》(1954)和《代数学史》(1985)等。

——《数学辞海》第六卷

这是组合数学和数论的一个定理，在拉姆齐理论的课程中已经接触。作者在生活中是观察到英语诗歌的头韵来引出这一问题和定理。简而言之，这一定理是指：

定理 4.1. (范德瓦尔登) 对于任意给定的正整数 r和 k，总存在正整数N，使得把数 $\{1,\ldots,N\}$ 染成r种颜色时，至少存在 k 个组成等差数列的正整数是同一种颜色的。这个最小的N叫做**范德瓦尔登数**$V(r,k)$。

这一定理可以由数学归纳法证明，或者作为拉姆齐理论的一个直接推论。此处，我们不再重述作者的故事和对这定理的说明例子。

5 根号二是无理数

这一定理想必大多数中国学生从小就学习过，并且了解其中的故事。证明的方法也很著名，是最初讲述反证法的一个例子。因此，在这里不再赘述。

6 二项式定理

你有注意过如下的事实吗？即

$$\begin{aligned} 11^0 &= 1 \\ 11^1 &= 11 \\ 11^2 &= 121 \\ 11^3 &= 1331 \\ 11^4 &= 14641 \end{aligned}$$

等式的右边恰好是帕斯卡三角（杨辉三角）。不过我们继续写下去，似乎出现了一些问题，因为

$$11^5 = 161051 \neq 15101051.$$

事实上，这是因为两个连续进位 $11^5 = 146410 + 14641$ 导致的。

事实上右边是二项式公式给出的结果，因为

$$11^n = (10+1)^n = 11^{n-1} \times 10 + 11^{n-1}.$$

这一递归方法的推广是

$$(x+y)^n = (x+y)^{n-1}x + (x+y)^{n-1}y.$$

这里的递归思想很宝贵，可以用数学归纳法证明二项式定理

$$(x+y)^n = \sum_{k=1}^{n} \binom{n}{k} x^k y^{n-k}.$$

7 巴拿赫-塔斯基定理

巴拿赫-塔斯基定理又被称为**分球怪论**，是一条数学定理。1924年，斯特凡**.**巴拿赫和阿尔弗雷德**.**塔斯基首次提出这一定理，指出在选择公理成立的情况下，可以将一个三维实心球分成有限（不可测的）部分，然后仅仅通过旋转和平移到其他地方重新组合，就可以组成两个半径和原来相同的完整的球。我们称这一过程为**等度分解**。

在现实生活中这种变形之所以不可行是因为原子的体积不是无限小，数量不是无限大，但其几何形状确实可以这样变形的。如果知道总是可以存在从一个几何体的内部点一一映射到另一个的方法，也许这个悖论看上去就不那么怪异了。例如两个球可以双射到其自身同样级别的无限子集（例如一个球）。同样我们还可以使一个球映射到一个大点或者小点的球，只要根据半径放大系数即可将一个点映射到另一个。然而，这些变换一般来说不能保积，或者需要将几何体分割成不可数无限块。巴拿赫 - 塔斯基悖论出人意料的地方是仅用有限块进行旋转和平移就能完成变换。

> 巴拿赫和塔斯基提出这一定理原意是想拒绝选择公理，但该证明很自然，因此数学家认为这仅意味着选择公理可以导致少数令人惊讶和反直觉的结果。有些叙述中这条定理被看成是悖论，但是定理本身没有逻辑上不一致的地方，实际上不符合悖论的定义。

这听起来不可思议。因为在现实生活中，把一个实心球打碎重新组合是不可能得到两个和原来一样大的球的，原因是它们的质量不相等。

但是在数学是，如果允许"质量为0"的点概念的出现，定义一个"完美的质量"函数是不可能的。也就是说，存在无法定义质量的集合。这又被称为不可测集（Lebesgue 测度）。

事实上，更强的结果是五块就能够做到一个球和它自身的两个拷贝等度分解。

这个悖论甚至有个更强的版本：任意两个三维欧几里得空间具有非空内部的子集是等度分解的。换句话说，一块大理石可以分成有限块然后重新组合成一个行星。

对于三维以上的情形这个悖论依然成立。但对于欧几里得平面它不成立。同时，也有一些悖论性的分解组合在平面上成立：一个圆盘可以分割成有限块并重新拼成一个面积相同的实心正方形。参见塔斯基分割圆问题。

冯纽曼研究这个悖论时，创出了可均群（Amenable Group）的概念。他发现三维以上情形之所以产生悖论，和这些空间的旋转群的非可均性有关。

证明的方法是分四步：

1. 找到把一个具有两个生成元的自由群进行分割的特殊方法

2. 找到一个3维空间中同构于这两个生成元的旋转群

3. 利用这个群的特殊分割方法和选择公理对单位球面进行分解

4. 把这个单位球面的分解推广到实心球

我们在这着重讲讲第一步：

考虑由 a, b 生成的自由群 F_2。 令 $S(a)$为所有以a开头的字符串， 同理定义$S(a^{-1})$、$S(b)$和$S(b^{-1})$。显然我们有

$$F_2 = e \cup S(a) \cup S(a^{-1}) \cup S(b) \cup S(b^{-1})$$

且

$$F_2 = S(a) \cup aS(a^{-1}) = S(b) \cup bS(b^{-1}).$$

简而言之，我们把F_2分解为四块（e忽略也没问题），然后乘上一个 a或者b来"旋转"它们，其中两个重新组合成 F_2，另外两个重新组合成另一个 F_2。这样的事情，放在球体上就是我们想要证明的东西了。

8 欧拉一笔画定理

康德（Immanuel Kant）的故乡是普鲁士的城市柯尼斯堡（Konigsberg，现在是俄罗斯的加里宁格勒）。著名的七桥问题的故事就是发生在这里。七桥问题是指，是否存在一条路能通过有且仅有一次所有的桥。

这一问题最早被瑞士数学家欧拉（Leonhard Euler）解决。欧拉在他在1736年发表的论文《柯尼斯堡的七桥》中不仅解决了七桥问题，也提出了**一笔画定理**，顺带解决了一笔画问题。一般认为，欧拉的研究是图论的开端。

与一笔画问题相对应的一个图论问题是哈密顿路径问题，即通过每个点有且仅有一次的通路或回路。

定理 8.1. (欧拉一笔画定理) 一个连通图有欧拉路径当且仅当奇数度的点的个数为0或2。

9 巴切特公式

今天我们考虑一类被称为巴切特方程的丢番图方程：对一固定整数 c，下列方程的有理数解是哪些

$$y^2 - x^3 = c \tag{9.1}$$

我们将看到它的几何解释，且这一解释给出生成解的钥匙。这个方程的一个惊人的性质是存在一个所谓的重复公式（Duplication Formula），由巴切特（Bachet）于1621年发现：

定理 9.1. 如果 (x, y) 是方程(9.1)的有理数解，则

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

是另一组有理数解。

想要验证这一定理是简单的，我们只需要将新的解带入方程(9.1)即可。但是，现在我们的问题是如果找到这一重复公式的呢？显然新解和原来的解不是线性的。线性关系的一个简单例子是，在 Bezout 等式中，如果 $aX + bY = c$，则有线性解 $a(X + b) + b(Y - a) = c$，亦即 $(X + b, Y - a)$ 是另一组解。

如果仅仅是迭代这一巴切特公式，我们可能会感受到其越来越复杂的形式，从而需要使用计算机来辅助完成，这和当时巴切特的初衷渐行渐远。

我们来做一个简单的解释。对于一给定方程的一个解 $P = (x, y)$，我们做过 P 点的切线。如果 $y \neq 0$(否则切线斜率不存在，切线垂直于x)，带入切线方程 $Y = mX = c$ 到三次曲线方程。我们将证明这个切线与三次曲线交于另一点 Q是有理点，且恰好是巴切特公式给出的新点。（可通过下列代码查看相应的曲线图）

```
>>> from sympy import plot_implicit, Eq, symbols
>>> x, y=symbols('x y')
>>> plot_implicit(Eq(y**2-x**3,5))
>>>
```

我们可以知道，因为巴切特方程的所有系数都是有理数，因此其曲线上有理点的斜线斜率也是有理数，从而过有理点的切线是一个有理直线。而新的点Q正是有理曲线和有理直线的交点，虽然这不能保证Q是有理点。不过计算可知其就是有理点。

因为 $\frac{dy}{dx} = \frac{3x^2}{2y}$. 于是切线方程为 $Y = \frac{3x^2}{2y}X + \left(y - \frac{3x^3}{2y}\right)$，带入巴切特方程得到

$$Y^2 = X^2\frac{9x^4}{4y^2} + X\frac{3x^2}{y}\left(y - \frac{3x^3}{2y}\right) + \left(y^2 - 3x^3 + \frac{9x^6}{4y^2}\right) = x + X^3$$

由此可得 $Q = (\alpha, \beta)$，利用韦达定理，可得 $\alpha = \frac{x^4 - 8xc}{4y^2}$.

10 群的拉格朗日定理

群是一个拥有闭合的满足结合率的乘法的集合，并且这个集合有乘法的单位元和任意元素的逆元。拉格朗日定理表明子群的阶都整除于有限群的阶。

定理 10.1. (拉格朗日) 有限群的任意子群的阶均整除于有限群本身的阶。

11 抽屉原理与狄利克雷定理

抽屉原理又称为鸽子洞原理（the pigeonhole principle）。它讲述的是很基础的原理，即把n+1只鸽子放入n个鸽子洞，必然有一个洞至少有两只鸽子。推广的形式是 $\mathrm{kn}+1$ 个鸽子放入 n 个洞里，必然有一个洞有至少 $k+1$只鸽子。这一原理在数学中大量应用，尤其是组合数学。

狄利克雷使用这一原理证明了一个关于使用有理数逼近无理数的结论。我们知道，每个无理数都能用有限小数来逼近，只需要取其小数形式的前n位即可。但是我们重新考虑一个问题就是用既约分数逼近无理数。

定理 11.1. (狄利克雷) 令 α 为一无理数，N是一正整数。则存在一个有理数 p/q 使得分母 $1 \leqslant q \leqslant N$ 且满足

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{qN}.$$

证明. 上述结论等价于存在 $1 \leqslant q \leqslant N$ 使得 $q\alpha$ 的左右$\frac{1}{N}$的邻域中存在一个整数。我们现在使用区间 $[0,1)$，并将其N等分，于是得到N个子区间

$$\left[0, \frac{1}{N}\right), \left[\frac{1}{N}, \frac{2}{N}\right), \ldots, \left[\frac{N-1}{N}, 1\right).$$

这些子区间就是我们要用到的"鸽子洞"。

我们知道任意实数x的小数部分，记为$\{x\}$，它是一个位于 $[0,1)$的实数。

现在我们考虑这$N+1$个数 $0, \{\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\}$。根据抽屉原理，必然存在至少两个数 $\{r\alpha\}, \{s\alpha\}$ 位于同一$[0,1)$的上述子区间内。这说明 $(s-r)\alpha$ 的左右$\frac{1}{N}$的邻域中存在一个整数。我们定义 $q = s - r$。则显然有 $1 \leqslant q \leqslant N$，使得 $q\alpha$ 半径大小为$\frac{1}{N}$的邻域存在一个整数。 □

12 素数无限定理

素数有无穷多个，伟大的希腊数学家欧几里得给出了著名的反证法证明。欧拉的证明也很有意思，他证明了级数 $\sum_{p\text{prime}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \dots$ 是发散的，因此素数是无穷多的。否则有限个素数的导数必然收敛到一个常数。事实上，欧拉证明了这一级数的增长速度和 $\log\log n$ 相当，具体地，

$$\sum_{p\text{prime}\leqslant n} \frac{1}{p} \geqslant \ln\ln(n+1) - \ln\frac{\pi^2}{6}.$$

详情参见维基百科Divergence of the sum of the reciprocals of the primes 或 Aigner 和 Zagier 的Proofs from the BOOK。

13 算术基本定理

算数基本定理是指任何大于1的整数都能唯一表达为素数的乘积。 此处的唯一是不考虑素数之间的顺序的。

算数基本定理解释了为什么不把1看成素数。 在证明这一结论之前， 我们需要一个重要引理即：$p|ab \Rightarrow p|a$ 或 $p|b$。

这一结论可以使用 Bezout定理来得到。 假设 $p \nmid a$，即 p, a 互素，因此有 Bezout 等式 $ph + ak = 1$。

我们知道 $p|ab$，因此需要添加点b的信息，把上述等式两边同乘以 b，我们得到 $bph + abk = b$。我们知道 $p|bph, p|abk$，因此必然有 $p|b$。

现在我们来证明算数基本定理：

证明. （存在性）存在性的证明看起来没那么直接， 我们需要使用最小反例(minimal counterexample)来证明。 假设这一结论不正确， 则必然存在一个最小的数使得无法被分解为素数的乘积，我们不妨设为n。

n 显然不能为素数，否则它本身就是素因子。因此n是一个合数，也就是说，存在 $n = ab$。于是 a, b是两个小于n的整数， 由n的最小性， 因此a, b均可以表示为素因子的乘积，从而n也有素因子分解。

（唯一性）我们不妨设 $n = p_1 \cdots p_r = q_1 \cdots q_s$ 其中 $p_i \neq q_j$，否则我们可以约去它们得到一个新的数，如果可以一直约去则必然相等。实际上，完全不同的分解这也是不可能的，因为我们知道 $p_1|n = q_1 \cdots q_s$，因此根据上述引理可知 $p_1|q_1$ 从而 $p_1 = q_1$ 或者 $p_1|q_2 \cdots q_s$，继续下去可知必然存在一 q_i 使得 $p_1 = q_i$。这与p_i, q_j的互异性矛盾。 □

14 费马小定理

定理 14.1. (费马小定理) 若p为素数，a为不被p整除的整数，则 $a^{p-1} \equiv 1 \bmod p$.

上述定理还有一个等价形式，即

定理 14.2. 若 p 为素数，a为任一整数，则 $a^p \equiv a \bmod p$.

首先我们说明它们两者为什么是等价的。

$\Longrightarrow$. 如果 a 不被p 整除，则 $a^{p-1} \equiv 1 \bmod p$，两遍同乘以 p 可得 $a^p \equiv a \bmod p$。如果 a 被p整除，即 $a \equiv 0 \bmod p$，因此等式当然成立。

$\Longleftarrow$. 如果 a 不被 p 整除，则说明 a 存在一个 $\bmod p$ 的逆，即 a^{-1}。将 $a^p \equiv a \bmod p$ 等式两边同乘以 a^{-1} 即可。

上述证明过程也能帮助我们记忆两种形式对 a 要求的区别。因为如果 $a \equiv 0 \bmod p$ 是不可能找到幂和1同余。

让我们来证明费马小定理。我们将提供三种证明方法。

证明.

方法一. 我们考虑 $p-1$ 个数 $a, 2a, 3a, \ldots, (p-1)a$. 如果我们把它们相乘，可以得到 $(p-1)!a^{p-1}$。

注意到 $a, 2a, \ldots, (p-1)a$ 它们模p均不相等且不等于0。因此它们也同余于 $1, \ldots, p-1$ 的某个数，因此

$$(p-1)!a^{p-1} \equiv (p-1)! \bmod p.$$

而显然 $p \nmid (p-1)!$，因此有 $a^{p-1} \equiv 1 \bmod p$.

方法二. (归纳法) 我们将对a使用数学归纳法，证明 $a^p \equiv a \bmod p$。事实上 $0^p \equiv 0 \bmod p$ 和 $1^p \equiv 1 \bmod p$ 的情况是显然的。我们现在假设 $a^p \equiv a \bmod p$，我们想推出 $(a+1)^p \equiv a+1 \bmod p$。我们可以使用二项式公式得到：

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

根据归纳假设， $(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p$。

方法三. （拉格朗日定理）考虑群去除0的所有模p数构成的群 $G \cong \mathbb{Z}_p \setminus \{0\}$。我们需要一个由$a$生成的子群 $H = \langle a \rangle$。我们断言 $H = \{a, a^2, \ldots, a^k = 1\}$，$k$为最小的整数，使得 $a^k = 1$。于是根据拉格朗日定理， $k | p-1$，也就是说 $p-1 = km$。因此，

$$a^{p-1} = a^{km} = (a^k)^m = 1^m = 1$$

亦即， $a^{p-1} \equiv 1 \bmod p$. □

如果p不是素数呢？ 使用上述证明的方法一方法三可以推广到任意情况， 这就是著名的费马欧拉定理：

定理 14.3. (费马-欧拉) 令 n 为任一大于1的整数， $(a, n) = 1$， 令 $\phi(n)$ 为所有小于n且与之互素的正整数的个数，则 $a^{\phi(n)} \equiv 1 \bmod n$.

$\phi(n)$又被称为欧拉函数(Euler totient function)或者欧拉ϕ函数。注意到，如果n是素数，则该定理正是费马小定理。

我们上文已经提到可以推广方法一和方法三得到这一定理的证明。比如，我们可以取所有与 n 互素的比n小的正整数构成一个群。考虑它的子群即可得解。

15 拉格朗日四平方和定理

费马的一个定理给出了描述哪些自然数能写为两个自然数的平方和。对于所有的奇素数能写为两个数的平方和当且仅当模4余1。 因为任意平方数mod4余1或0。 任意奇数 mod 4 余1或者3.

艾伯特.吉拉德(Albert Girard)是第一个观察到这个现象的人，他描述了所有可以表示为两个正整数平方数的和的正整数(不一定是素数)；这本书出版于1625年。4n+1形式的每一个素数p都是两个平方的和，这一表述有时被称为**吉拉德定理**。

费马在一封1640年圣诞节给马林梅森（Marin Mersenne）的信中， 写了一个精心制作的版本的陈述(包括一些 p的幂作为两个正方形的总和的表达式)。 因为这个原因这个版本的定理有时被称为**费马圣诞节定理**(参见Fermat's theorem on sums of two squares)。

完整的两平方和的充要条件如下（参见 sum of two squares theorem）：

定理 15.1. (Fermat) 任意大于一的正整数能写为二平方和当且仅当其素因子分解中不包含某个形如$4n + 3$的素因子的奇数次幂。

大于一的整数的素因子中每个$4n + 3$的素数的次数是偶数。

一些自然数还能写为更多自然数的平方和，比如三平方和。在1-20的所有整数中，只有7和15不能写成三平方和。对于三平方和，我们不再考虑mod 4，转而考虑 mod 8. 事实上， 所有的平方 mod 8 要么为 0， 1要么为4。 因此所有mod 8余7的数都不能写为三平方和。 这也是为什么 7， 15不能写为三平方和的原因。 事实上， 勒朗德（Legendre） 在1798年给出了如下的三平方和定理：

定理 15.2. (Legendre) 任意正整数能写为三平方和当且仅当它不能写为$4^k(8m+7)$的形式。

如果是四平方和呢？巴切特（Bachet）猜想任何自然数都能表示为四平方和。拉格朗日给出令人惊讶的结论的证明:

定理 15.3. (拉格朗日 1770) 任意正整数都是四个自然数的平方和。

证明这个定理之前，我们需要知道任何两个可以写为四平方和的数的乘积也是四平方和。以下结果由欧拉给出，

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)\,(b_1^2+b_2^2+b_3^2+b_4^2) \;=\; & (a_1\,b_1-a_2\,b_2-a_3\,b_3-a_4\,b_4)^2+\\ & (a_1\,b_2+a_2\,b_1+a_3\,b_4-a_4\,b_3)^2+\\ & (a_1\,b_3-a_2\,b_4+a_3\,b_1+a_4\,b_2)^2+\\ & (a_1\,b_4+a_2\,b_3-a_3\,b_2+a_4\,b_1)^2.\end{aligned}$$

另一种思考方式是考虑四元数的范数。因此，我们只需要证明每个素数都能表示为四平方和。详细证明参见 Lagrange's four-square theorem.

这一类平方和问题还能推广到立方和、四次方和等等，它们称为华林问题（Waring's problem）。

16 容斥原理

定理 16.1. (inclusion-exclusion principle) 令 $A,B,C\subseteq X$ 均有有限集，则

$$|A\cup B|=|A|+|B|-|A\cap B|,$$

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|C\cap A|+|A\cap B\cap C|.$$

这一结果可以推广到n个集合，我们可以用数学归纳法证明，作者使用了集合的示性函数1_A来证明。

$1_A(x):=\begin{cases}1, & x\in A\\ 0, & x\notin A\end{cases}$. 于是我们有 $|A|=\sum_{x\in X}1_A(x)$. 进一步地， $A\cap B$ 的示性函数是 $1_{A\cap B}=1_A1_B$. 而 $1_{A\cup B}=1_A+1_B-1_A1_B$. 由此可得到$1_{A\cup B\cup C}=1_A+1_{B\cup C}-1_A1_{B\cup C}$. 并进一步展开得到完整的表达式。由此对应的 $|A\cup B\cup C|=\sum_{x\in X}1_{A\cup B\cup C}(x)$.

17 狄利克雷定理

定理 17.1. (狄利克雷) 若a, q为互素的两个自然数，则存在无穷多个形如 $a+kq\,(k\in\mathbb{N})$ 的素数。

狄利克雷于1837年发表的结果实际上比上述论述更加强。 对于任意互素正整数对$(a,\ q)$， 模q同余a的素数集合$\{x|x\equiv a \bmod q;\ x \text{ is prime}\}$相对所有素数集合的密度为$\frac{1}{\phi(q)}$，即 $\lim_{x\to\infty}\frac{\pi(x;a,q)}{\pi(x)}=\frac{1}{\varphi(q)}$，其中 $\phi(q)$ 为欧拉函数。

类似于证明无穷多个素数， 狄利克雷得到欧拉方法的启发， 考虑如下级数的发散性。这个定理的证明中引入了狄利克雷L函数， 应用了一些解析数学的技巧， 是解析数论的重要里程碑。

$$\sum_{p:p\equiv a \bmod q}\frac{1}{p}.$$

这个定理有一些推广形式，但是都还只是未被证明的猜想而已。比如

- 布尼亚科夫斯基猜想，推广至>=2次的多项式。
- 狄克森猜想，推广至>=2个一次多项式，比如孪生素数猜想是一特例。
- 欣策尔假设H，上述两个推广合并。

18 有理数是可数的

有理数是可数的，这一定理相比我们都很熟悉，就是要找到有理数和整数的对应，不再详述。

19 存在超越数

早期比较著名的超越数是刘维尔数，$L=\sum_{n=1}^{\infty}10^{-n!}=0.1100010\ldots$

刘维尔注意到无理代数数不能很好地被有理数逼近，反而超越数能很好的被有理数逼近。更确切地说，如果α是一个无理代数数，且若n是α的极小多项式的次数，则存在某个常数C，使得 $\left|\alpha-\frac{p}{q}\right|>\frac{C}{q^n}$ 对任意整数 $p, q>0$ 成立。

而刘维尔数的定义说明了它可以很好地被逼近，只要取 $\sum_{n=1}^{\infty} 10^{-n!}$ 即可。因此 L 是超越数。

更多的超越数参见维基百科词条Transcendental number。

20 波尔查诺-魏尔斯特拉斯定理

我们知道分析基本公理（fundamental axiom of analysis）是任何递增的序列，如果有上界则有极限的（收敛的）。同理一个有下界的递减的序列也有极限。

但是一个有意思的序列，比如 $-1, 1, -1, 1, \ldots$ 是不收敛的，但是我们可以把它拆成奇数偶数两个（递增）序列，收敛于1和-1。

波尔查诺-魏尔斯特拉斯定理给出了上述情况的结论：

定理 20.1. (Bolzano-Weierstrass) 有界的实数序列必有收敛子序列。

我们介绍两个证明方法。

证明. 第一种方法是分割有界区间，利用二分法，放大每个极限子序列中每个点为区间。假设实数序列 $\{x_n\}$ 的界为 $[a_0, b_0]$. 设 $c_0 = \frac{a_0+b_0}{2}$，我们考虑子区间 $[a_0, c_0], [c_0, b_0]$。显然必然存在一个区间有无穷多个序列 $\{x_n\}$ 的数。否则，两个区间都只有有限个数，会导致序列也是有限的。不妨设 $[a_0, c_0]$ 有无限个数，令$[a_1, b_1] = [a_0, c_0]$. 我们可以继续定义这样的区间，得到一系列区间 $[a_i, b_i]$，每个区间都有无穷多个数。

我们知道它们是嵌套的，因此有 $a_i \leqslant a_{i+1} \leqslant b_{i+1} \leqslant b_i$ $(\forall i)$. 因此 $\{a_i\}$ 是一个递增序列，且它们有上界 b_0. 根据分析基本原理，$a_i \to a$ 拥有极限。

我们也可以在每个区间中任意取值。

第二种方法是证明有界实数序列必然存在递增或递减的子序列。 x_n称为顶峰(summit)是指$\forall m \geqslant n$，$x_n \geqslant x_m$。

我们列出所有的顶峰，$x_{n_1}, x_{n_2}, \ldots$ 我们需要知道顶峰序列是否是无限的。我们将此分为两种情况：

1. 如果顶峰序列是无限的，则这一序列就是一个递减子序列，因此根据分析基本原理有极限；

2. 如果顶峰是有限的。设 x_M 是最后一个顶峰，令 $x_{m_1} = x_{M+1}$（最后顶峰下一个数，如果没有顶峰则 $x_{m_1} = x_1$.）我们知道 x_{m_1} 不是顶峰，因此必然存在 $x_{m_2} \geqslant x_{m_1}$。同理，由于之后都没有顶峰，必然存在 $x_{m_3} \geqslant x_{m_2}$等等。继续这一过程，则必然存在一个递增序列。根据分析基本原理有极限。 □

21 实数是不可数的

使用康托的对角线原理可以证明实数更确切的说$(0,1)$是不可数的。

22 塞迈雷迪定理

塞迈雷迪.安德烈(Szemerédi Endre)是当代匈牙利数学家，主要研究组合数学与理论计算机科学。塞迈雷迪定理是个关于自然数集子集中的等差数列的结论。

一个自然数的子集 A 被称为有正自然密度是指

$$\limsup_{n\to\infty}\frac{|A\cap\{1,2,3,\ldots,n\}|}{n}>0.$$

1936年，爱多士（Erdos）和图兰（Turan）猜想：

定理 22.1. (Szemerédi) 若整数集 A 具有正的自然密度，则对任意的正整数 k, 都可以在 A 中找出一个 k 项的等差数列。

塞迈雷迪.安德烈于 1975 年证明了此结论。这一定理

1. $k=1,2$：显然的；
2. $k=3$：Klaus Roth, 1953
3. $k=4$：Szemeredi, 1969; Roth, 1972
4. general：Szemeredi, 1975; Hillel Furstenberg 1977; Timothy Gowers 2001.

2004年 Ben Green 和陶哲轩（Terence Tao）的格林-陶定理的一个著名推论是质数序列包含任意长的等差数列。

定理 22.2. (Green-Tao) 对于任意的素数集合的子集A，若A相对于素数集合的上密度（upper density）为正，即：

$$\limsup_{n\to\infty}\frac{|A\cap\{1,\ldots,n\}|}{\pi(n)}>0,$$

那么对于任意的正整数k，A中的元素可以组成任意多个长度为k的等差数列。

23 华林问题

1770年，爱德华.华林（Edward Waring）猜想，

猜想 23.1. 对于每个非1的正整数k，皆存在正整数$g(k)$，使得每个正整数都可以表示为至多$g(k)$个k次方数（即正整数的k次方）之和。

1909年，大卫.希尔伯特首先用复杂的方法证明了$g(k)$的存在性。1943年，U.V.林尼克给出了关于$g(k)$存在性的另一个证明。

然而，尽管g(k)的存在性已被证明，人们尚且无法知晓$g(k)$与k之间的关系。

- 1770年，拉格朗日证明了四平方和定理，指出$g(2)=4$。
- 1770年，华林发表了《代数沉思录》（Meditationes Algebraicae），其中说，每一个正整数至多是9个立方数之和；至多是19个四次方之和。
- 1909年，亚瑟.韦伊费列治证明了$g(3)=9$。
- 1859年，刘维尔证明了$g(4)\leqslant 53$。后来哈代和李特尔伍德得到$g(4)\leqslant 21$，1986年巴拉苏布拉玛尼安证明了$g(4)=19$。
- 1896年马力特得到$g(5)\leqslant 192$；1909年韦伊费列治将结果改进为$g(5)\leqslant 59$；1964年陈景润证明了$g(5)=37$。
- 欧拉之子 J.A. Euler猜想 $g(k)=2^k+\lfloor (3/2)^k \rfloor -2$。至1990年，对于$6\leqslant k\leqslant 471600000$此式已经被计算机验证为正确。

24 中国剩余定理

中国剩余定理，又称中国余数定理，是数论中的一个关于一元线性同余方程组的定理，说明了一元线性同余方程组有解的准则以及求解方法。也称为孙子定理。

定理 24.1. 同余方程组(S)

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \quad\vdots \\ x \equiv a_n (\mathrm{mod}\, m_n) \end{cases}$$

有解当且仅当对任意 $1 \leqslant i \neq j \leqslant n$，$(m_i, m_j) = 1$ 。特别地，令 $M = \prod_{i=1}^{n} m_i$， $M_i = M/m_i$。设 $t_i = M_i^{-1}$为M_i模m_i的数论倒数（即$t_i M_i \equiv 1 \,(\mathrm{mod}\, m_i)$）。则方程组 (S) 的通解形式为：

$$x = kM + \sum_{i=1}^{n} a_i t_i M_i,$$

对任意 $k \in \mathbb{Z}$. 在模M意义下方程组的解唯一。

25 拉姆齐数的爱多士下界

拉姆齐定理表明在二染色中对任意整数 r 一定存在 n，使得完全图 K_n 必然包含的同色子完全图K_s。

$R(s) := R(s,s)$. 我们已经知道 $R(1) = 1$, $R(2) = 2$, $R(3) = 6$, 以及 $R(4) = 18$. 然后寻找确切的拉姆齐数十分困难, 事实上, $R(5)$ 及其以上的确切值仍然没有确定. 因此, 自然的想法就是不断缩小上下界. P. Erdös 在其1947年的文章中开创性的利用概率方法给出第一个拉姆齐数的下界.

定理 25.1. The Ramsey number $R(s)$ is bigger than $2^{(s-1)/2}$.

上述定理的证明是概率性而非构造性证明。我们选择 K_n 边的一个随机着色。然后我们将得到一个同色完全图K_s的概率的一个上界。我们将证明如果我们非常小心地选取 n，我们可以令这个概率（严格）小于1。如果这个概率小于1，则必然存在某些着色方式使得不存在同色的 K_s。

那么如何选择一个随机着色呢？我们将K_n 的每条边染为红色或者蓝色，每次染色都是独立事件，且任意一次染色两种颜色的概率为$1/2$。那么我们得到一个同色的完全图K_s 的概率如何？利用简单粗暴的估计，我们知道这等于所有使得 K_s 是同色的概率的和。我们可以通过计算 K_s 的所有数量乘以每一个 K_s 是同色的概率。

K_s 的数量显而易见是 $\binom{n}{s}$. 那么每一个 K_s 同色的概率为多少？我们知道每条边为红色概率是 $1/2$，K_s 有 $\binom{s}{2}$ 个边。因此，K_s 是红色的概率是 $2^{-\binom{s}{2}}$，因此这个 K_s 同色的概率为 $2^{1-\binom{s}{2}} = 2 \times 2^{-\binom{s}{2}}$。

因此，K_s 同色的概率是 $\binom{n}{s} 2^{1-\binom{s}{2}}$. 我们想选择足够大的 n，使得这一概率小于1。如果我们选择 $n = \lfloor 2^{(s-1)/2} \rfloor$，则我们得到

$$2^{1-\binom{s}{2}} \binom{n}{s} \leq 2^{1-\binom{s}{2}} \frac{n^s}{s!} < 2^{-s(s-1)/2}\, 2^{s(s-1)/2} = 1.$$

这正是我们想要的结果。注意到在 Erdos 最初的证明中，他使用的是计数而非概率，而现在概率是现代的语言。

26 第一同构定理

定理 26.1. 令G_1, G_2为群，$f: G_1 \to G_2$是一群同态，则$G_1/\ker(f) \cong \mathrm{Im}(f)$.

27 威尔孙定理

我们在费马小定理的介绍中提到的证明方法中利用了 $(p-1)!$。事实上，我们有

定理 27.1. (Wilson) 设p为素数，则 $(p-1)! \equiv -1 \bmod p$.

证明的思路是找配对（除去$1, p-1$），使得乘积模p为1，最后剩下 $p-1 \equiv -1 \bmod p$.

28 卡迈克尔数有无穷多个

根据费马小定理我们知道对一素数p和任意自然数a满足 $(a,p)=1$，$a^{p-1} \equiv 1 (\bmod p)$。一个自然的问题是，这一结论是充分必要的吗？即是否可以作为判断p为素数的条件。事实上，存在合数也满足上述关系，这一类合数我们称之为卡迈克尔数。

定义 28.1. (Carmichael number) 卡迈克尔数是满足如下同余关系的合数n

$$b^{n-1} \equiv 1 (\bmod n),$$

其中b为满足$(b,n)=1$的任意自然数。

或者等价的，是否存在一个合数n，满足对任意自然数b，使得 $b^n \equiv b (\bmod n)$成立。

Alford, Granville 和 Pemerance在1994年发表在 Annals of Mathematics 的论文中证明了有无穷多个卡迈克尔数。

定理 28.2. (Alford, Granville, Pemerance) 存在无穷多个卡迈克尔数。

29 二次互反律

二次互反律的英文为 the lay of quadratic reciprocity，念起来非常有意思，有一种疯狂卷舌的味道。同时这也是一个非常有意思的定理。

令 p, q 为不相等的奇素数，则可以定义勒让得（Legendre）符号如下：

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } n^2 = q \bmod p \text{ for some integer } n \\ -1 & \text{otherwise} \end{cases}$$

定理 29.1. (高斯)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

30 勾股数

欧几里得在几何原本中得到了所有勾股数的形式：

定理 30.1. 一组互素正整数(a, b, c)是勾股数当且仅当它满足如下形式：

$$(r^2 - s^2, 2rs, r^2 + s^2),$$

其中 $(r, s) = 1$，$r > s$，且r, s有且仅有一个偶数。

31 非零整数模p得到一个乘法群

定理 31.1. 非零整数模p得到一个阿贝尔乘法群。

这一结果可以自然地推广到模任意整数 n， 其中的元素是小于n且与之互素的整数，因此$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$。

32 圆心角等于圆周角的两倍

定理 32.1. 圆心角等于圆周角的两倍。

这一定理算是非常早学习的一个定理，现在也没有记得完整的证明。不过，稍微一想也很简单，只要连接圆心和圆周角的顶点即可：分为两种情况，一种是圆心在圆周角内，一种是圆周角外。之后分类讨论即可。

33 高斯和的大小

设 $e(\theta)$ 为一个逆时针角度为360 $\times$ θ的单位步子， 在复平面中 $e(\theta)=\exp(2\pi i\theta)=\cos(2\pi\theta)+i\sin(2\pi\theta)$。容易知道

$$\sum_{n=0}^{N-1} e(n/N)=0.$$

高斯考虑的是一组特殊的步子，且关注素数和平方，$\sum_{n=0}^{p-1} e(n^2/p)$，其中 p 是奇素数。我们称之为高斯和(Gauss sums)。

定理 33.1. 令p为奇素数，则有

$$\sum_{n=0}^{p-1} e(n^2/p)=\epsilon_p\sqrt{p},$$

其中 $\epsilon_p=\begin{cases}1 & p\equiv 1 \bmod 4\\ i & p\equiv 3 \bmod 4\end{cases}$.

34 霍尔的结婚定理

霍尔的结婚定理（Hall's marriage theorem）由 Philip Hall 在1935年证明了等价的两种形式：

- （组合形式）处理一系列有限集：它给出了能够从每个集合中选择不同元素的充要条件。
- （图论形式）处理二分图（偶图）：给出找到至少覆盖图一侧的匹配的充要条件。

令 S 为X的有限子集的类，且某些子集可以重复出现（因此S不是集合，而是类）。

S的一个截线（transversal）是指一个**单射**函数 $f\colon S\to X$的像，使得 $f(s)$是S的任意一个集合的一个元素。也就是说，f 从每个S的集合内选择一个代表元使得S内的任意两个集合的代表元都不相同。截线也被称为互异代表元的系统。

一个类S满足结婚条件（marriage condition）是指对任意子类 $W\subseteq S$，都有

$$|W|\le\left|\bigcup_{A\in W} A\right|.$$

如果结婚条件不成立，则 f 不是一个截线。反过来，Hall 证明了也是正确的：

定理 34.1. (Hall's marriage theorem) 有限集合的类S拥有截线当且仅当S满足结婚条件。

35 最好的有理逼近来自于连分式

因为连分式的求解是使用欧几里得算法，因此

定理 35.1. 最好的有理逼近来自于连分式。

更多关于连分式的求法，可以看我的笔记《数学的源与流》。

36 康托集是零测度的不可数集

首先康托集是不可数的。因为存在一个满射 $C \to [0,1]$。因为康托集每次都是三等分，因此我们考虑三进制（ternary system）。康托集的三进制表示是所有仅有0和2的小数，比如 $0.020020220\ldots$。我们只要把康托集的数的三进制表示中的2映射到1，生成的新数我们看成是二进制，则显然表示了所有的$[0,1]$的实数，因此得到这一满射。所以康托集是不可数集。

定理 36.1. 康托集的测度为0.

因为在通常测度中，被挖去的测度为 $\sum_{n=1}^{\infty} \frac{2^{n-1}}{3^n} = \frac{1}{2} \times 2 = 1$。

37 斯皮纳引理

我最早接触斯皮纳引理（Sperner's lemma）是在高中奥数时期，当时知道了这一引理的威力，同时也对此一知半解。

现在我们自然的引进它。令$[n] = \{1,2,\ldots,n\}$。它一共有2^n个子集。因此我们可以把它的所有子集对应到 n 维欧几里得空间，比如 $n=3$时我们有：

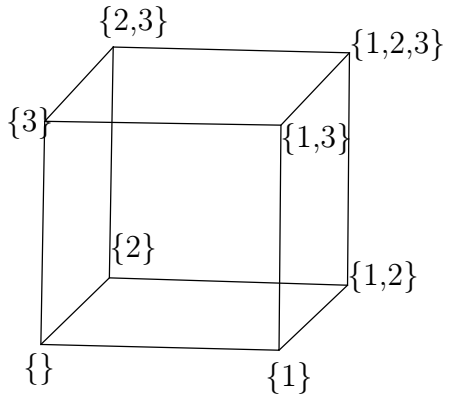

图 37.1. 分层模型（*layered model*）

由此我们可以把所有集合依据到原点$\{\} = \varnothing$的距离，得到如下分层

$$\{1,2,3\}$$

$$\{1,2\}\,\{2,3\}\,\{1,3\}$$

$$\{1\}\,\{2\}\,\{3\}$$

$$\varnothing$$

这一分层的大小（集合个数）看起来是先增大后减小，而且在 $n/2$ 附近最大。

在这里我们要引入链的概念，链即是一系列的嵌套的（nested）集合 C_i，使得 $C_i \subseteq C_{i+1}$. 注意到上述分层就是一个链的概念，即从每层中可以挑一个合适的集合构成一条链，比如 $\varnothing, \{2\}, \{2,3\}, \{1,2,3\}$。显然$[n]$的链的最长长度是 $n+1$

反过来，如果没有一个集合是另一个集合的子集，我们为反链（antichains）,有时也称为斯皮纳类（Sperner families）。比如这个例子 $\{1,2,3\}, \{1,2,4\}, \{2,3,4\}$。我们也可以扩充这一反链，但是只能增加一个即 $\{1,3,4\}$. 那问题来了？$[n]$的反链的最长长度是多少？

斯皮纳引理给出了答案：

引理 37.1. (Sperner) $[n]$的子集类的最长反链的大小为 $\binom{n}{\lfloor n/2 \rfloor}$。

作者也觉得奇怪为什么不叫定理，反正她与我首次接触时，老师都叫它引理。

这一引理的直观感觉就是，分层模型中每一层都是一个反链，最长的反链在最中间，大小为$\binom{n}{\lfloor n/2 \rfloor}$。

我们要证明这一引理，需要明确两点。首先任意反链都至多和链有一个交集（一个公共的集合），比如 $\{1,2\}, \{2,3\}, \{1,3\}$ 和 $\varnothing, \{1\}, \{1,3\}, \{1,2,3\}$只有一个交集 $\{1,3\}$。这是显然的，否则和反链定义矛盾。

第二点就是利用到 Hall 的结婚定理。因为最长链和反链也只有一个交集，反链在中间层最大。

另一种证明方法是使用 LYM 不等式。

38 存在一个模p的本原根

定理 38.1. 令p为素数，则存在一个一个模p的本原根，即在 $(\mathbb{Z}/p\mathbb{Z})^\times$存在一个 a 使得a的阶为$p-1$。

这是群论中的一个简单的定理。

39 欧拉准则

欧拉准则（Euler's criterion）是关于二次互反律的一个结果。我们首先根据费马小定理可得到 $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \bmod p$，因此 $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$。如何确定这个正负呢？欧拉给出如下判定准则：

定理 39.1. (Euler) 令p为奇素数，令a为一与p互素的自然数，则

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

40 染色三角形的斯皮纳引理

这是另一个斯皮纳引理。这是一个有意思的游戏：

定理 40.1. (Sperner) 令 T 为一个三角形且被随意分割为一系列三角形（三角形化）。我们给每个顶点着三种颜色，规则如下：

1. T 的三个顶点着三种不同的颜色；
2. 如果三角形的顶点在 T 的一条边上，则只能着这条边的两个（大三角形T的）顶点的颜色；
3. 内部的顶点着色任意

则在三角化中必然存在一个小三角形使得恰好三个顶点不同色。

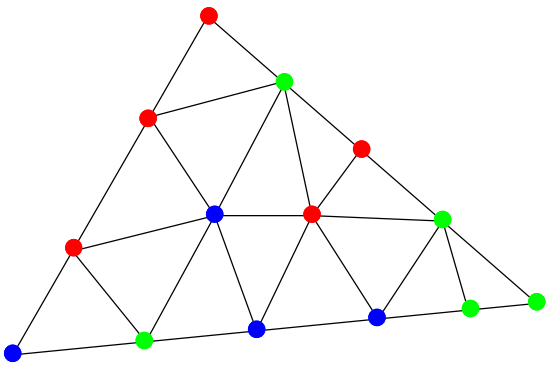

图 40.1. 三角化的例子

41 高斯引理

$\langle a\rangle$是a模p以后是在 $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ 之间的某个数。例如 $p=7, a=2$，则有

$\langle a\rangle = 2, \langle 2a\rangle = \langle 4\rangle = -3, \langle 3a\rangle = \langle 6\rangle = -1$。

定理 41.1. (Gauss's lemma) 令p为奇素数，且令 $(a, p)=1$。则

$$\left(\frac{a}{p}\right) = (-1)^{\nu},$$

其中 $\nu = \#\left\{k \in \left\{1, 2, \ldots, \frac{p-1}{2} | \langle ka \rangle < 0\right\}\right\}$。

42 费马大定理

本节是语音博客，介绍的是著名的费马大定理：

定理 42.1. 当$n \geqslant 3$时，$x^n + y^n = z^n$ 无整数解。

此定理由Wiles于1995年证明。

43 斯坦尼茨交换引理

定理 43.1. (Steinitz Exchange Lemma) 令 $v_1, \ldots, v_m$ 为线性空间 V 的一系列线性不相关的向量。令 $w_1, \ldots, w_n$ 为一组 V 的基。则 $m \leqslant n$，且在给 w_i 适当的重新排序后， $v_1, \ldots, v_m, w_{m+1}, \ldots, w_n$ 也是一组基（或者说全部 v_i 加上 合适的 $n-m$ 个w_i也组成一组新基）。