.

经典数论选讲

宗传明

.

问题1. 你学过的最好的数学结论是什么？为什么你认为最好？

问题2. 你读过的最有收获的数学参考书是什么？最重要的收获是什么？

课程简介

- **课程目的：**通过介绍数论的一些重要分支、重要结论和重要数学家，让同学们对这一学科有所了解。

- **上课形式：**正常上课+课外学习研讨。

- **考核形式：**作业20+期中30+期末50+课外学习研讨（参考）。

目录

第三章. 自然数的表示

第四章. 素数的分布

第五章. 丢番图方程

第六章. 丢番图逼近

第七章. 超越数

第八章. 数的几何

第一章. 数论简介

§ 1. 数论的研究对象

数论是研究数字系统的一门学问, 是数学中最基础的一个分支. 做为一个学科, 很难确定数论是何时诞生的. 但是, 自数字诞生以来人们就开始探索研究它们的规律, 也就孕育了数论.

做为数学中最富悠久历史的一个学科, 她经历了几百年乃至上千年的发展. 直到今天, 她仍是数学中最有生机的分支之一. 在这种情况下, 我们很难概括数论的研究对象. 但是, 我们可以用几个典型的例子来说明数论学家做了些什么.

例1.1. 每一个自然数都可以表示成四个自然数的平方和. 也就是：

$$n = a^2 + b^2 + c^2 + d^2.$$

注1.1. 这一著名的论断最早出现在Fermat写给Carcavi的信中. 当然, 他没有给出证明. 这一命题的第一个证明是由Lagrange给出的. 据历史记载, Euler曾研究这一问题长达四十年之久. 当他听说Lagrange证明了这一结论时, 他很快明白了他的问题所在, 并给出了一个新证明. 由于这一结论是如此的重要， Jacobi, Cauchy等多位大数学家也给出了它的新证明。

在此基础上，你有和联想？

例1.2. 用$\pi(x)$表示不大于x的素数的个数. 那么,

$$\pi(x) \sim \frac{x}{\log x}.$$

注1.2. 这就是著名的素数分布定理. 这一渐近公式是由Legendre和Gauss于1800年前后分别提出的. 但是, 这一断言直到1896年才由de la Vallée Poussin 和Hadamard独立证明. 1949年, Selberg与Erdös给出了这一定理的一个初等证明. 为此Selberg获得了Fields奖, Erdös没有.

例1.3. 当$n \geq 3$时, $x^n + y^n = z^n$无整数解.

注1.3. 这就是著名的Fermat 大定理. 几百年来, 它一直吸引着许多大数学家和无数数学爱好者为之如醉如痴. Euler, Kummer都曾做出了不懈的努力并得到过部分结果. Hilbert也曾将其列入他的23个数学问题. 但是, 直到1995年才由Wiles在Taylor的帮助下, 在Taniyama, Shimura, Frey, Mazur, Ribet等人的工作的基础上证明了这一定理.

例1.4. e **和**π **都是超越数.**

注1.4. 1766年前后, 瑞士数学家Lambert证明了e和π都是无理数. 1873年, Hermite证明了e是超越数. 10年后, Lindeman证明了π也是超越数. 许多大数学家对相关的问题做过进一步的研究. 例如, Hilbert就给出过e和π的超越性的新证明, 并在他的23个数学问题中提出了系统研究的新问题.

一百年以前, 几乎所有的数学家都曾研究过数论并做出过重要贡献. 这中间包括Dedekind, Dirichlet, Euler, Fermat, Gauss, Hermite, Hilbert, Jacobi, Kronecker, Kummer, Lagrange, Legendre, Minkowski, Riemann 等. 在过去的一百多年中, 共有六十四位数学家 获得过Fields奖. 其中十六位(Selberg, Serre, Roth, Baker, Bombieri, Deligne, Faltings, Drinfeld, Lafforgue, Tao, Ngo Bao Chau, Bhargava, Scholze, Venkatesh, Maynard, Viazovska) 主要因为对数论的杰出贡献而获奖. 做为一个学科, 数论是Fields获得者最多的数学领域之一.

数论是纯数学中的纯数学, 以它的深奥与艰难使人们望而生畏. 但它是人类知识与思想的精华, 也是数学中最优美的领域之一. 同时, 在现代科技中数论具有重要的应用——例如在密码通讯技术中的重要应用.

§ 2. 近代数论的主要分支

通过Gauss, Dirichlet, Riemann, Kummer, Hilbert, Minkowski, Hadamard, Hardy, Littlewood 和Vinogradov等许多大数学家的工作, 许多新思想和新方法被引入数论的研究中. 这样, 在研究对象和方法的基础上, 数论被分成了几个既相互关联又自成体系的分支. 这里, 我们简单介绍其中的几个.

解析数论

这一分支主要研究自然数的表示以及与素数相关的一些问题, 例如Waring问题和Goldbach猜想. Riemann假设和孪生素数问题也都属于这一分支. 顾名思义, 这一分支的主要方法是**分析**, 更确切地说是复变函数论. 这一分支系统地发展了筛法, 圆法, 三角和法等强有力的分析工具.

Dirichlet, Riemann, Hadamard, Hardy, Littlewood, Vinogradov, Ramanujan, Landau, Selberg和Bombieri 等著名数学家在这一分支的发展中起了重要作用. Selberg, Bombieri, Tao, Maynard因解析数论的工作荣获Fields奖. 我国数学家, 特别是华罗庚和陈景润, 在这一领域也做出了重要贡献. 近年来，华裔数学家张益唐在孪生素数问题作出了重要贡献.

代数数论

近两个世纪以来, Galois, Abel, Jacobi, Kummer等人在数论的研究中引入了系统的代数方法, 也就逐渐形成了代数数论. 近年来, 这是最活跃的数学研究领域之一. Fermat大定理的证明（Wiles 和Taylor）是数学史上最耀眼的成就之一.

当代许多著名数学家在这一领域做出了不朽的贡献, 例如Weil, Langlands, Deligne, Faltings, Wiles, Taylor, Shirmura等等. 继Fermat大定理和Taniyama-Shimura猜想之后, 该领域最有代表性的问题可能要算Birsh-Swinnerton-Dyer猜想了. Serre, Deligne, Faltings, Drinfeld, Lafforgue, Ngo Bao Chau, Bhargava, Scholze因代数数论的工作荣获Fields奖.

丢番图逼近

这一分支是研究用有理数来逼近其它数的一门学问. 这一分支与连分数和超越数轮密切相关. 最早是由Dirichlet 和Kronecker等做出了奠基性的工作.

上个世纪六, 七十年代由Roth 和Schmidt等杰出的数学家将这一学科发展到最高潮. 其中Roth因在这一领域的杰出贡献荣获Fields奖. 一致分布这一学科也是在丢番图逼近的基础上发展起来的. 这一分支中的Thue-Siegel-Dyson-Roth定理是最完美的数学结论之一.

超越数论

如何判定和构造超越数是这一分支的主题. 早在19世纪末, Lambert, Hermite和Lindeman就开始研究e和π的无理性和超越性. Hilbert也曾将某些数的超越性判别列入他的23个著名问题（第七）：$\alpha \neq 0, 1$是一个代数数, β是一个非有理代数数, 是否可以断定 α^β一定是超越数. 这一问题的一个特例是e^π, 因为

$$e^\pi = \left(e^{\pi i}\right)^{-i} = (\cos\pi + i\sin\pi)^{-i} = (-1)^{-i}.$$

Hilbert第七问题是由Gelfond和Schneider独立解决的. 但对推动这一学科的发展做出最系统和最重要贡献的当属Baker. 他荣获Fields奖. 另外, Liouville, Siegel, Mahler也都做出了重要贡献.

数的几何

这是由Minkowski在Kepler, Newton, Gauss, Lagrange, Hermite等人的工作的基础上创立的一个分支, 其目的是用几何的思想方法来研究数论的某些问题, 例如整数的表示. 后来, 经过Mordell, Davenport, Mahler, Siegel, Hlawka和Rogers等许多杰出数学家的工作将其发展成为一个具有丰富内容的独立分支.

近四十年来, 离散化与几何化的思想使这一分支有了突飞猛进的发展, Desarte, Levenstein, Elkies, Cohn, Viazovska等作出了重要贡献. Viazovska荣获Fields奖. 这一分支的许多核心问题至今远未解决, 其中有些问题堪称整个数学中的基本问题. 例如高维球堆积的最大密度问题. 该分支在现代密码学中具有重要应用。

第二章. 素数与同余

§1. 整除与素数

自然数: $1, 2, 3, \cdots\cdots$. 通常我们用N表示所有自然数构成的集合.

整数: $0, \pm1, \pm2, \pm3, \cdots\cdots$. 通常我们用$Z$表示所有整数构成的集合.

定义2.1. 设a与b为两个自然数. 我们称a整除b (记做$a \mid b$)当且仅当存在一个自然数c使得$b = ac$.

定义2.2. 不能被1和它自身以外的任何自然数整除的自然数被称为素数, 否则称其为合数. 例如：$2, 3, 5, 7, \cdots$ 都是素数.

定理 2.1. 素数无限.

证明思路一. 观察

$$m = 1 + \prod p.$$

这一想法是由Euclid发现的.

证明思路二. 因为

$$\left(1 - \frac{1}{p}\right)^{-1} = 1 + \sum_{i=1}^{\infty} \frac{1}{p^i},$$

我们得到

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 - \frac{1}{p}\right)^{-1}.$$

这一想法是由Euler发现的. 事实上, 他由此导出了$\sum \frac{1}{p}$的发散性.

证明三. 用P表示所有素数构成的集合. 如果$a, b \in Z$, $b > 0$, 我们定义

$$N_{a,b} = \{a + nb : \ n \in Z\}.$$

我们称O是Z的一个开集如果O空或者它满足条件：对任一$a \in O$都存在一个$b > 0$使得$N_{a,b} \subseteq O$.

- 显然, 每个$N_{a,b}$都是开集且两个开集的并集仍是一个开集.

- 如果O_1和O_2是两个开集, $a \in O_1 \cap O_2$, $N_{a,b_1} \subseteq O_1$, $N_{a,b_2} \subseteq O_2$, 那么

$$N_{a,b_1 b_2} \subseteq O_1 \cap O_2.$$

所以$O_1 \cap O_2$也是Z中的一个开集.

这样定义的开集导出了Z的一个拓扑.

我们注意到两个事实：

A. 每一个非空开集包含有无穷多个元素.

B. 由于

$$N_{a,b} = Z \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

每一个$N_{a,b}$都是闭集.

由于任一非 ± 1的整数都有素因子, 所以

$$Z \setminus \{1, -1\} = \bigcup_{p \in P} N_{0,p}$$

假如P有限, 那么$\bigcup_{p \in P} N_{0,p}$是一个闭集, 因为它是有限个闭集的并. 这样我们得到 $\{1, -1\}$是一个开集, 与A矛盾. 定理得证.

注 2.1. 数学中有些证明之所以重要, 并不是因为它第二次、 第三次证明了某个结论. 更重要的是它所体现出来的思想方法. Euler的证明就体现出这种重要性.

注 2.2. Aigner和 Ziegler 的畅销书Proofs from THE BOOK的第一个问题就是证明素数的个数为无穷多. 其中列了6个证明.

自然思考. 既然有无穷多素数, 那素数多还是合数多？ 能不能导出一个类似测度形式的结论？

定理2.2. 几乎所有的自然数都不是素数.

基本思路. 设p_1和p_2是2个素数, X是一个很大的自然数. 在$[2, X]$中我们有如下三列与p_1和p_2有关的合数:

$$2p_1, 3p_1, \cdots, \left\lfloor \frac{X}{p_1} \right\rfloor p_1,$$

$$2p_2, 3p_2, \cdots, \left\lfloor \frac{X}{p_2} \right\rfloor p_2$$

和

$$p_1p_2, 2p_1p_2, \cdots, \left\lfloor \frac{X}{p_1p_2} \right\rfloor p_1p_2.$$

这三列的个数分别是

$$\left\lfloor \frac{X}{p_1} \right\rfloor - 1, \quad \left\lfloor \frac{X}{p_2} \right\rfloor - 1, \quad \left\lfloor \frac{X}{p_1p_2} \right\rfloor.$$

由此可以导出, 在$[2, X]$中的素数以及与p_1和p_2无关的合数的个数为

$$\begin{aligned} & X-1-\left(\left\lfloor\frac{X}{p_1}\right\rfloor-1+\left\lfloor\frac{X}{p_2}\right\rfloor-1\right)+\left\lfloor\frac{X}{p_1 p_2}\right\rfloor \\ \leq & \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) X+3. \end{aligned}$$

作业 2.1. 将定理证明补充完整.

定理2.3. 如果n是一个合数, 那么它一定有一个素因子不超过 $\sqrt{n}$.

例 2.1. 判定97是一个素数.

作业2.2. 任给一个自然数k, 总能构造出k个相继的合数.

问题2.1. 寻找未知素数.

§ 2. 整数的模

算术基本定理. 任一自然数都可以分解为素数幂次的乘积, 也就是

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}.$$

且分解是唯一的.

注2.3. 这是非常古老的一个定理. 据说Euclid知道这一定理. 当然, 严格证明是后人给出的.

这一定理的存在性是很容易证明的(你能做到吗？), 关键是唯一性. 为此, 我们需要介绍一个新概念.

定义2.3. 我们称整数的一个子集M为一个模如果它具有以下性质：

如果$x,\ y \in M$, 那么 $x - y \in M$.

注2.4. 显然, 只有一个元素0的集合和所有整数构成的集合都是模. 通常称之为平凡模. 模是一个非常简单的概念. 但是, 通过它的一些基本性质, 却很容易导出算术基本定理.

定理2.4. 任一非平凡模M必为某一正整数的所有倍数构成的集合.

证明要点. 首先, 如果$a \in M$, 那么$na \in M$.

假定d为该模中的最小正整数, 则有

$$M = \{zd : \ z \in Z\}.$$

否则, 由

$$x = zd + r,$$

我们可以得到

$$r = x - zd \in M$$

且$0 < r < d$, 与假定矛盾.

定理2.5. 任给两个正整数a和b. 我们用(a,b) 表示它们的最大公因数, 用M表示模$\{z_1a+z_2b:\ z_1,z_2\in Z\}$, 那么

$$M=\{(a,b)z:\ z\in Z\}.$$

证明思路. 由定理2.4, 我们得到

$$M=\{mz:\ z\in Z\}.$$

从而我们得到$m|a$, $m|b$, 也就得到了 $m|(a,b)$. 反过来, 由

$$m=ax+by$$

可以得到$(a,b)|m$. 所以, 一定有

$$m=\pm(a,b).$$

注2.5. 两个自然数的最大公因数可以表示为它们的整数线性组合. 也就是

$$(a, b) = xa + yb.$$

作业2.3. 推广这一结论.

注2.6. 注2.5中的结论也可以由欧几里得算法得出.

定理2.6. p为一个素数. 若$p \mid ab$, 则有$p \mid a$ 或 $p \mid b$.

证明要点. 假如$p \nmid a$, 则有

$$(a, p) = 1.$$

由注2.5, 我们有

$$xa + yp = 1.$$

所以得到

$$xab + ypb = b.$$

由此可导出$p \mid b$.

注2.7. 算术基本定理中的唯一性可由定理2.6导出. 事实上, 它们是等价的.

作业2.4. 试从定理2.6导出基本定理.

设$a_1, a_2, \cdots, a_n$为n个自然数. 通常我们用$(a_1, a_2, \cdots, a_n)$ 表示它们的最大公因数, 用$[a_1, a_2, \cdots, a_n]$表示它们的最小公倍数. 基于算术基本定理, 我们有以下结论.

定理2.7. 如果

$$a_i = \prod p_j^{\alpha_{ij}},$$
$$\alpha_j^* = \max_i\{\alpha_{ij}\},$$
$$\alpha_j' = \min_i\{\alpha_{ij}\},$$

那么

$$(a_1, a_2, \cdots, a_n) = \prod p_j^{\alpha_j'} \qquad [a_1, a_2, \cdots, a_n] = \prod p_j^{\alpha_j^*}.$$

§ 3. 同余与同余方程

定义2.4. m为一给定自然数. 如果$a-b$是m的倍数, 我们就称a与b相对m是同余的, 记为

$$a \equiv b \pmod{m}.$$

反之, 则记为

$$a \not\equiv b \pmod{m}.$$

同余是一个非常重要的概念, 它有如下基本性质：

1. $a \equiv a \pmod{m}$
2. 如果$a \equiv b \pmod{m}$, 则$b \equiv a \pmod{m}$
3. 如果$a \equiv b,\ b \equiv c \pmod{m}$, 则$a \equiv c \pmod{m}$
4. 如果$a \equiv b,\ a_1 \equiv b_1 \pmod{m}$, 则有

$$a + a_1 \equiv b + b_1 \pmod{m},$$
$$a - a_1 \equiv b - b_1 \pmod{m}$$

和

$$aa_1 \equiv bb_1 \pmod{m}$$

5. 如果$ac \equiv bd \pmod{m}$, $c \equiv d \pmod{m}$ 并且$(c, m) = 1$, 那么

$$a \equiv b \pmod{m}.$$

作业2.5. 证明性质5. 并举出没有$(c, m) = 1$限制条件时的反例。

作业2.6. 用归纳法证明$n^5 - n$总能被5整除。

定义2.5. 通常集合$\{0, 1, \cdots, m-1\}$被称为是模m的一个剩余系； 其中与m互素的元素构成的子集合被称为缩剩余系, 它们的个数被记为$\varphi(m)$.

注2.8. 同余将数论的运算变成了代数运算. 由以上性质, 不难看出剩余系是 一个有限环, 而缩剩余系则构成一个乘法群.

定理2.8. 如果$(k, m) = 1$, 那么

$$k^{\varphi(m)} \equiv 1 \pmod{m}.$$

证明1. 假定

$$\{a_1, a_2, \cdots, a_{\varphi(m)}\}$$

为模m的一个缩剩余系. 因为$(k, m) = 1$,

$$\{ka_1, ka_2, \cdots, ka_{\varphi(m)}\}$$

仍为模m的一个缩剩余系. 所以,

$$\prod_{i=1}^{\varphi(m)} a_i \equiv \prod_{i=1}^{\varphi(m)} ka_i \equiv k^{\varphi(m)} \prod_{i=1}^{\varphi(m)} a_i \pmod{m}.$$

由性质5可得

$$k^{\varphi(m)} \equiv 1 \pmod{m}.$$

证明2. 假定

$$M = \{a_1, a_2, \cdots, a_{\varphi(m)}\}$$

为模m的一个缩剩余系. 我们不妨假设$a_1 = 1$. 显然, 我们有

$$a_i a_j \in M.$$

另外, 如果$a_i \in M$, 那么 $(a_i, m) = 1$. 由注2.5, 我们得到

$$1 = a_i x + my,$$

$$a_i x \equiv 1 \pmod{m}.$$

换句话说a_i有逆元素. 这样, M是一个具有 $\varphi(m)$个元素的乘法群. 所以对任一元素 a_i都有

$$a_i^{\varphi(m)} \equiv 1 \pmod{m}.$$

注2.9. 取m为一素数p, 可得

$$k^{p-1} \equiv 1 \pmod{p}$$

对$1 \leq k \leq p-1$都成立. 这就是Fermat小定理.

作业2.7. 如果$(m,n)=1$, 则有

$$\varphi(mn) = \varphi(m)\varphi(n).$$

试证之. 并由此导出

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

作业2.8. 证明

$$\sum_{d|m} \varphi(d) = m.$$

注2.10. Abel曾提出是否存在p和a满足

$$a^{p-1} \equiv 1 \quad (mod\ p^2)?$$

Jacobi证明数对$[p, a] = [11, 3]$, $[11, 9]$, $[29, 14]$和$[37, 19]$即可. 实际上这一问题与 Fermat大定理密切相关. 如果

$$x^p + y^p + z^p = 0, \quad (xyz, p) = 1 \qquad (*)$$

成立, 那么

$$q^{p-1} \equiv 1 \quad (mod\ p^2)$$

对2与89间的所有素数q都成立. 由此可以导出当

$$p < 8.858 \times 10^{20}$$

时$(*)$确实无解.

讨论补充:

1977年，R. Rivest，A. Shamir和L. Adleman提出了基于大整数分解的加密算法(RSA)。这一加密方案使他们荣获2002年度图灵奖。

密钥的产生: 1. 选取两个保密的大素数p和q. **2.** 计算$n = pq$, $\varphi(n) = (p-1)(q-1)$. **3.** 选取一个整数e满足$1 < e < \varphi(n)$以及$(\varphi(n, e) = 1$. **4.** 计算d使得

$$ed \equiv 1 \mod \varphi(n).$$

我们取$\{e, n\}$为公开密钥，$\{d, n\}$为秘有密钥.

加密: $m \longmapsto c$

$$c \equiv m^e \mod n.$$

解密: $c \longmapsto m$

$$c^d = m^{ed} \equiv m \mod n.$$

讲到同余式, 我们不能不讲**孙子定理**. 这是少有的几个以中国人的名字命名的定理之一.

定理2.9. 如果$(m_i, m_j) = 1$, $i \neq j$, 那么

$$x \equiv a_i \pmod{m_i}, \quad 1 \leq i \leq n$$

对任意给定的一组a_i都有唯一解$(mod\ m_1 \cdots m_n)$.

证明想法. 记 $m = m_1 \cdots m_n$, 并定义

$$M = \{0, 1, 2, \cdots, m-1\}$$

和

$$M' = \{(a_1, \cdots, a_n) : \ 0 \leq a_i < m_i\}.$$

验证M和M'为$1-1$对应.

求解的基本思路: 令

$$d_i = m/m_i$$

和

$$d_i d_i^{-1} \equiv 1 \pmod{m_i},$$

那么

$$x \equiv \sum_{i=1}^{n} d_i d_i^{-1} a_i \pmod{m}$$

即为所求的解.

作业2.9. 详细写清楚求解过程.

作业2.10. 假设b是一个大于1的整数。那么，任一正整数n都可以唯一地表示为 $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, 其中$0 \leq a_i \leq b-1$并且 $a_k \neq 0$.

思考研讨：

问题1. 上次课我们介绍了凯撒密码和RSA密码，你回顾、思考、尝试过吗？

问题2. 你思考过为什么RAS密码是安全的吗？

$$n = \sum_{i=1}^{m} a_i 2^i.$$

$$m \sim \log_2 n.$$

$$\sqrt{n} \sim 2^{m/2}.$$

§4. 二次互反律

我们的目标是判定二次同余方程

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{2.1}$$

是否有解？显然, 我们可以假定p既不是2也不整除a (这些情况要么方程退化，要么判别显然). 这时，它等价与判定同余方程

$$y^2 \equiv b^2 - 4ac \pmod{p} \tag{2.2}$$

是否有解？

由于p既不是2也不整除a，所以

$$(4a, p) = 1.$$

在(2.2)中做线性变换

$$y = 2ax + b$$

我们得到

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p},$$
$$4a^2x^2 + 4abx + b^2 \equiv b^2 - 4ac \pmod{p},$$
$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

由同余方程的性质5，我们得到

$$(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

这样，我们得到：二次同余方程(2.1)是否有解等价于(2.2)是否有解，且他们的解由$y = 2ax + b$关联。

为了判定(2.2)是否有解，我们引进Legendre符号：

$$\left(\frac{d}{p}\right)=\begin{cases}1, & \text{如果 } x^2\equiv d \pmod p \text{ 有非零解,}\\ -1, & \text{如果 } x^2\equiv d \pmod p \text{ 无解,}\\ 0, & \text{如果} p\mid d.\end{cases}$$

这一定义有许多好的性质, 例如

$$\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right) \tag{2.3}$$

$$\left(\frac{d}{p}\right)=d^{(p-1)/2} \pmod p \tag{2.4}$$

$$\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{c}{p}\right) \tag{2.5}$$

(2.4)的证明： 如果d是模p的二次剩余, 即存在a满足

$$a^2 \equiv d \pmod{p}.$$

那么我们得到

$$d^{(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod{p}. \tag{2.a}$$

如果d不是模p的二次剩余, 对任一给定j,一次同余方程

$$j \cdot x \equiv d \pmod{p} \tag{2.b}$$

的解x_j一定满足

$$x_j \neq j.$$

这样, $\{1, 2, \cdots, p-1\}$ 被分成了$(p-1)/2$个数对$\{j, x_j\}$满足$(2.b)$. 所以我们得到(根据Wilson定理)

$$d^{(p-1)/2} \equiv (p-1)! \equiv -1 \pmod{p}. \tag{2.c}$$

综合(2.a)和(2.c),我们得到(2.4).

注2.11. $(2.c)$中的最后一步即Wilson定理. 试证之(提示：互逆配对).

注2.11'. 由(2.5)可知，最最基本的二次同余方程是

$$x^2 \equiv q \pmod{p}$$

型的，其中p和q均为素数.

二次互反律. 如果p和q均为奇素数且$p \neq q$, 那么

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

另外

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

基本引理. 设素数$p > 2, p \nmid d, 1 \leq j \leq (p-1)/2,$

$$t_j \equiv jd \pmod{p}, \quad 0 < t_j < p. \tag{2.6}$$

以n表示这$(p-1)/2$个t_j 中大于$p/2$ 的个数. 那么

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

证明思路. 首先由t_j的定义(2.6)可以导出

$$t_i \not\equiv \pm t_j \pmod{p}, \quad i \neq j. \tag{2.7}$$

否则，可以推出矛盾

$$(i \pm j)d \equiv 0 \pmod{p}.$$

用$r_1, r_2, \cdots, r_n$表示 $\{t_j : 1 \le j \le (p-1)/2\}$中大于$p/2$的数, 用$s_1, s_2, \cdots, s_k$表示其中小于$p/2$的数. 由(2.7)可以导出

$$\{s_1, s_2, \cdots, s_k, p-r_1, p-r_2, \cdots, p-r_n\} = \{1, 2, \cdots, (p-1)/2\}. \quad (2.8)$$

由(2.6)和(2.8)我们可以得到

$$d^{(p-1)/2} \prod_{j=1}^{(p-1)/2} j \equiv \prod_{j=1}^{(p-1)/2} t_j \equiv (-1)^n \prod_{j=1}^{(p-1)/2} j \qquad (mod\ p).$$

所以，由同余方程的性质5我们得到

$$d^{\frac{p-1}{2}} \equiv (-1)^n \quad (mod\ p),$$

也就是(由(2.4))

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

基本引理得证.

二次互反律的证明思路. 由于

$$jq = p\left\lfloor \frac{jq}{p} \right\rfloor + t_j$$

我们得到

$$q\sum_{j=1}^{(p-1)/2} j = p\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{(p-1)/2} t_j = pT + \sum_{j=1}^{(p-1)/2} t_j, \tag{2.9}$$

其中

$$T = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor. \tag{2.10}$$

另一方面, 由(2.8)可以导出

$$\sum_{i=1}^{\lfloor p/2\rfloor-n} s_i + \sum_{i=1}^{n}(p-r_i) = \sum_{j=1}^{(p-1)/2} j,$$

$$\sum_{j=1}^{(p-1)/2} t_j = \sum_{i=1}^{n} r_i + \sum_{i=1}^{\lfloor p/2\rfloor-n} s_i = \sum_{j=1}^{(p-1)/2} j - np + 2\sum_{j=1}^{n} r_j.$$

代入(2.9)我们得到

$$(q-1)\sum_{j=1}^{(p-1)/2} j = p(T-n) + 2\sum_{j=1}^{n} r_j,$$

$$\frac{p^2-1}{8}(q-1) = p(T-n) + 2\sum_{j=1}^{n} r_j. \tag{2.11}$$

当$q=2$时, 由(2.10)我们得到$T=0$. 所以

$$n \equiv (p^2-1)/8 \pmod 2.$$

由基本引理我们得到

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

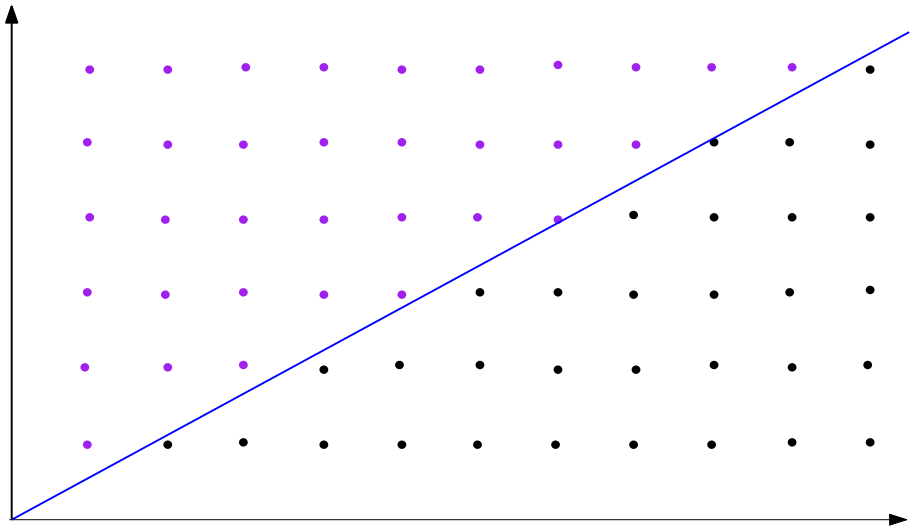
当$q>2$时, 因为$8|(p^2-1)$, 由(2.11)我们得到

$$n \equiv T \pmod 2.$$

所以, 由(2.10)我们得到

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{(p-1)/2}\lfloor\frac{jq}{p}\rfloor+\sum_{j=1}^{(q-1)/2}\lfloor\frac{jp}{q}\rfloor} = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

二次互反律得证.



$p = 23 \quad q = 13$

思考研讨：

思考1. 请总结一下二次互反律的思想。

思考2. 你能提出什么研讨问题？

作业2.11. 判定以下同余方程是否有解：

1. $x^2 \equiv 7\ (mod\ 227)$.
2. $11x^2 \equiv -6\ (mod\ 91)$.

作业2.12. 设素数$p \geq 3$并且 $(p, a) = 1$. 试证

$$\sum_{x=1}^{p} \left(\frac{ax + b}{p} \right) = 0$$

作业2.13. 当素数$p \geq 7$,总存在两个相继的二次剩余数(提示：2, 5, 10).

作业2.14. 当素数$p \geq 7$,总存在两个相差2的二次剩余数(提示：2, 3, 6).

§ 5. 几类著名的自然数

Mersenne 素数. 我们称型如$M_p = 2^p - 1$的素数为 Mersenne素数.

注2.12. 如果$n > 1$并且$m^n - 1$是素数, 那么$m = 2$且n为一素数. 试证之.

注2.13. 当$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937$时, 可以证明$M_p$是Mersenne素数.

例2.1(Frank Cole, 1903). $M_{67} = 193707721 \times 761838257787$.

Fermat 数. 我们称型如$F_n = 2^{2^n} + 1$的数为 Fermat数.

注2.14. Fermat曾猜测F_n全为素数. 不幸的是, 1732年Euler证实了

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417.$$

问题2.3. 是否有无穷多个Fermat数为素数?

注2.15. Gauss曾证明, 如果F_n是素数, 那么我们就可以用圆规和直尺做出正F_n边形. 这也就是他做出正17边形($F_2 = 17$)的基础.

完全数. 用$\sigma(n)$表示n的所有因子之和. 如果

$$\sigma(n) = 2n,$$

我们称n为一个完全数.

注2.16. 如果M_p是一个Mersenne素数, 那么$M_p(M_p+1)/2$是一个完全偶数. 相反, 每一个完全偶数都是这种形式. 试证之.

问题2.4. 是否有完全奇数？若有, 是否无穷？

Fibonacci数. 令$f_1 = 1$, $f_2 = 1$, 并定义

$$f_n = f_{n-1} + f_{n-2}.$$

那么f_1, f_2, f_3, ... 被称为Fibonacci数列.

命题. 令$\alpha = (1 + \sqrt{5})/2$. 当$n \geq 3$, 我们有$f_n > \alpha^{n-2}$.

证明. 容易验证, 当$n = 3, 4$时命题成立. 假设命题对所有$k \leq n$都成立, 我们证明它对$k = n + 1$也成立。

容易验证$\alpha = (1 + \sqrt{5})/2$是$x^2 = x + 1$的一个根。所以，我们得到

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

由归纳假设我们进而得到

$$f_{n+1} = f_n + f_{n-1} > \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-1}.$$

附. Möbius函数与Möbius变换

Möbius函数.

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ (-1)^r & if\ n = p_1 p_2 \dots p_r \\ 0 & otherwise. \end{cases}$$

性质1. Möbius 函数是一个乘积函数. 即, 如果$(m, n) = 1$, 那么

$$\mu(mn) = \mu(m) \cdot \mu(n).$$

性质2.

$$\sum_{d|n}\mu(d)=\begin{cases}1 & if\ n=1,\\ 0 & if\ n>1.\end{cases}$$

证明思路. 令

$$f(n)=\sum_{d|n}\mu(d).$$

可以验证，如果$(m,n)=1,$那么

$$f(mn)=f(m)f(n).$$

另一方面，假设$n=p^k,$其中p是一个素数，k是一个正整数，那么

$$f(n)=1-1=0.$$

所以，由整数的因子分解定理，性质2成立。

Möbius反演公式. $f(n)$ 和 $F(n)$是定义在正整数集的函数。如果

$$F(n) = \sum_{d|n} f(d)$$

对所有的n都成立，那么

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

证明.

$$\sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \left(\mu(d) \sum_{e|(n/d)} f(e) \right) = \sum_{d|n} \left(\sum_{e|(n/d)} \mu(d) f(e) \right)$$

$$= \sum_{e|n} \left(\sum_{d|(n/e)} f(e) \mu(d) \right) = \sum_{e|n} \left(f(e) \sum_{d|(n/e)} \mu(d) \right) = f(n).$$

第三章. 自然数的表示

§1. Fermat–Lagrange定理

定理3.1. 每一个自然数都可以表示成四个自然数的平方和. 也就是

$$n = a^2 + b^2 + c^2 + d^2.$$

注3.1. 很显然, 7 不能表示成三个自然数的平方和. 所以, 该命题是最佳的.

注3.2. 这就是著名的Fermat-Lagrange定理. 它是由Fermat提出, 后来由Lagrange证明的. 历史上, 许多著名数学家曾研究过这一问题并给出过新证明. 例如, Euler, Cauchy, Jacobi和Davenport. 下面, 我们简单介绍两种想法：模函数与二次剩余.

模函数方法: 模函数是研究自然数分拆的最基本的工具之一.

首先，我们熟知

$$\frac{1}{(1-x^k)}=\sum_{i=0}^{\infty}x^{ik}.$$

例3.1. 用$p_r(n)$表示可以将n表示为不大于r的自然数的和的不同种数. 当$|x|<1$时, 我们有

$$1+\sum_{n=1}^{\infty}p_r(n)x^n=\frac{1}{\prod_{i=1}^{r}(1-x^i)}.$$

然后将右式表示为简单形式并求导, 从而求出$p_r(n)$.

例3.2. 我们知道，人民币纸币有1元，2元，5元，10元，20元，50元和100元面值。假设银行支付客户m元人民币（不用角和分）的不同支付方式数为$g(m)$, $g(0) = 1$, 那么

$$\sum_{m=0}^{\infty} g(m)x^m = \frac{1}{(1-x)(1-x^2)(1-x^5)(1-x^{10})(1-x^{20})(1-x^{50})(1-x^{100})}.$$

例3.3. 用$q(n)$表示可以将n表示为奇数和的不同种数. 当$|x| < 1$时, 我们有

$$1 + \sum_{n=1}^{\infty} q(n)x^n = \frac{1}{\prod_{i=1}^{\infty}(1-x^{2i-1})}.$$

思考研讨：

思考1. 针对整数分拆你能提出什么研讨问题？

这方面最著名的结论是以下Jacobi等式：

当$|x|<1$和$y\neq 0$时, 恒有

$$\prod_{n=1}^{\infty}\left[(1-x^{2n})(1+x^{2n-1}y)(1+x^{2n-1}y^{-1})\right]=\sum_{n=-\infty}^{\infty}x^{n^2}y^n.$$

我们定义

$$f(x)=\sum_{i=0}^{+\infty}x^{i^2}$$

并且假定

$$f(x)^4=\sum_{n=0}^{+\infty}\tau(n)x^n.$$

如果能证明$\tau(n)>0$对所有的n成立, 那么我们就导出了 Fermat-Lagrange 定理.

注3.3. 这一美妙的想法是由Euler提出来的. 但是他未能实现它. 最 终证明

$$\tau(n) > 0$$

是由Jacobi通过对椭圆函数的深入研究完成的.

所谓的椭圆函数是一类非常特殊的函数, 例如,

$$f_1(x) = \prod_{n=1}^{\infty}(1 - x^{2n}),$$

$$f_2(x) = \prod_{n=1}^{\infty}(1 + x^{2n}),$$

$$f_3(x) = \prod_{n=1}^{\infty}(1 + x^{2n-1})$$

和

$$f_4(x) = \prod_{n=1}^{\infty}(1 - x^{2n-1}).$$

实际上, Jacobi证明了

$$f_1^4 f_3^8 = \left(\sum_{n=-\infty}^{\infty} x^{n^2}\right)^4 = 1 + 8\sum{}^* \frac{mx^m}{1 - x^m},$$

这里$\sum^*$表示不含4的倍数的和.

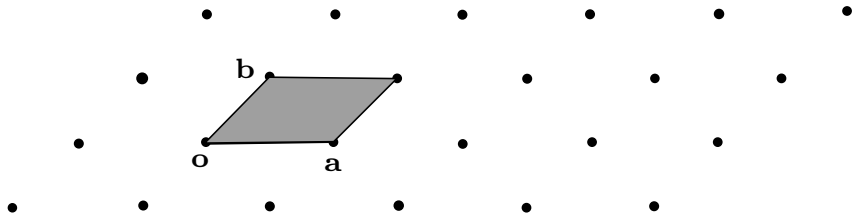
作业3.1. 试证, 将n分为每份不超过m的分拆数等于把n分为不超过m份的分拆数.

2. 二次剩余方法

定义3.1. 设$\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_n$为$E^n$中的$n$个线性无关的向量, 我们称

$$\Lambda = \left\{ \sum_{i=1}^{n} z_i \mathbf{a}_i : \ z_i \in Z \right\}$$

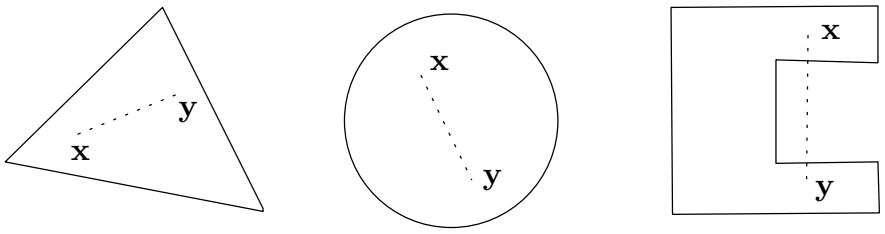
为一个格. 由这些向量构成的矩阵的行列式记为$det(\Lambda)$.



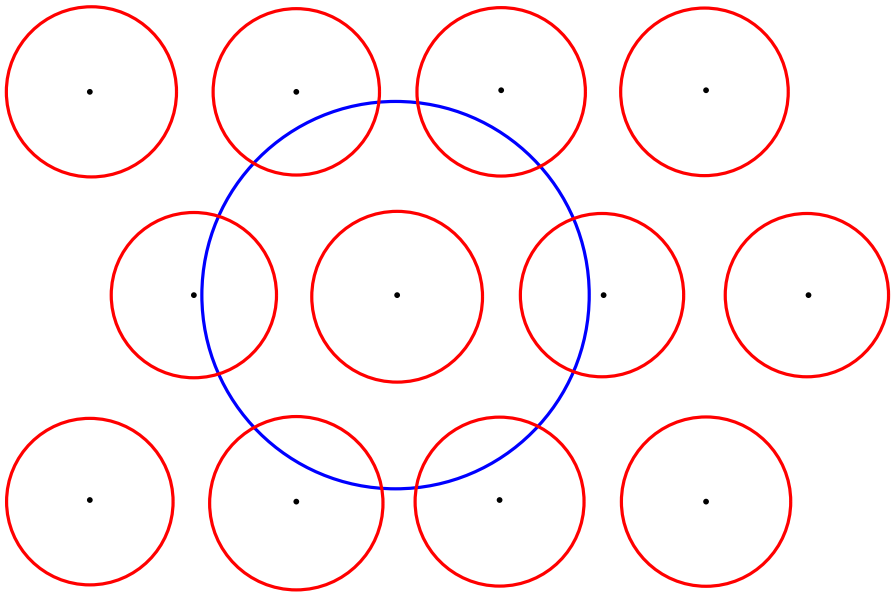
引理3.1 (Minkowski). C为一个n维的中心对称凸体, Λ为一个格. 如果

$$v(C) \geq 2^n \ det(\Lambda),$$

那么C含有Λ的一个非零点.



注3.4. 这是数的几何中的Minkowski基本定理. 证明非常简单, 将在第七章中给出. 你能证明吗?



引理3.2. 对任意给定的素数p总可以找达两个自然数a和b使得

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

证明思路. 首先, 可以证明

$$\left\{0^2, 1^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\} \tag{3.1.1}$$

$(mod\ p)$两两不同余. 同理, 可以证明

$$\left\{-1-0^2, -1-1^2, \cdots, -1-\left(\frac{p-1}{2}\right)^2\right\} \tag{3.1.2}$$

$(mod\ p)$两两不同余. 因为(3.1.1）和（3.1.2)共有$p+1$各自然数, 所以在(3.1.1)中可以找到一个a^2, 在 (3.1.2)中可以找到一个$-1-b^2$满足

$$a^2 \equiv -1 - b^2 \pmod{p}.$$

引理得证。

引理3.3. 令

$$c_1 = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4,$$
$$c_2 = a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3,$$
$$c_3 = a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4$$

和

$$c_4 = a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2,$$

我们有

$$\sum_{i=1}^{4} a_i^2 \sum_{j=1}^{4} b_j^2 = \sum_{k=1}^{4} c_k^2.$$

注3.5. 这就是著名的Euler恒等式. 类似的, 我们有

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

通常它被称为Fibonacci恒等式.

Fermat-Lagrange定理的证明： 由引理3.3可知, 我们只需证明n为素数的情况. 假设p为一个素数, a和 b为满足引理3.2的两个自然数. 我们定义 $\mathbf{a}_1 = (1, 0, a, -b)$, $\mathbf{a}_2 = (0, 1, b, a)$, $\mathbf{a}_3 = (0, 0, p, 0)$, $\mathbf{a}_4 = (0, 0, 0, p)$ 和

$$\Lambda = \left\{ \sum_{i=1}^{4} z_i \mathbf{a}_i : \ z_i \in Z \right\}$$

由引理3.1可以导出：存在不全为零的四个整数z_1, z_2, z_3 和z_4满足

$$\sum_{i=1}^{4} z_i \mathbf{a}_i \in rB^4,$$

其中$r = 2^{5/4} p^{1/2} \pi^{-1/2}$. 也就是说,

$$\mathbf{p} = (z_1, z_2, az_1 + bz_2 + pz_3, -bz_1 + az_2 + pz_4)$$

在该球中. 所以有

$$z_1^2 + z_2^2 + (az_1 + bz_2 + pz_3)^2 + (-bz_1 + az_2 + pz_4)^2 \leq (4\sqrt{2}/\pi) \cdot p < 2p.$$

令

$$k = z_1^2 + z_2^2 + (az_1 + bz_2 + pz_3)^2 + (-bz_1 + az_2 + pz_4)^2,$$

因为(注3.5)

$$(az_1 + bz_2)^2 + (-bz_1 + az_2)^2 = (a^2 + b^2)(z_1^2 + z_2^2),$$

由引理3.2我们得到

$$\begin{aligned} k &\equiv z_1^2 + z_2^2 + (az_1 + bz_2 + pz_3)^2 + (-bz_1 + az_2 + pz_4)^2 \\ &\equiv (z_1^2 + z_2^2)(1 + a^2 + b^2) \equiv 0 \pmod{p}. \end{aligned}$$

综上所述, 我们得到

$$0 < k < 2p \quad and \quad k \equiv 0 \pmod{p},$$

也就是说,

$$p = k = z_1^2 + z_2^2 + (az_1 + bz_2 + pz_3)^2 + (-bz_1 + az_2 + pz_4)^2.$$

思考题. 试探讨将一个自然数n可表示为四个非负整数的平方和的种数.

作业3.2. 任一被4除余3的自然数都不能表示为两个自 然数的平方和. 试证并推广之.

1910年, Ramanujan列出了54种无交叉项, 且能表示所有自然数的四元正定二次型. 其中包括

$$x^2+y^2+z^2+2w^2,$$
$$x^2+2y^2+4z^2+7w^2$$

和

$$x^2+2y^2+5z^2+5w^2.$$

注. 事实上，最后一个不能表示15. 假设能表示，那么$x \le 3$, $y \le 2$, $z \le 1$, $w \le 1$.

Conway-Schneeberger定理(1997). 一个交叉项全为偶数的整系数正定四元二次型若能表示$1, 2, 3, \ldots, 15$， 那么它就能表示所有的自然数。

Bhargava定理(1999). 一个整系数四元正定二次型若能表示$1, 2, 3, \ldots, 290$, 那么它就能表示所有的自然数。

Bhargava-Hanke定理(2005). 有且仅有6436个整系数四元正定二次型能表示所有的自然数。其中无交叉项的共有53种 (即Ramanujan发现的53种)。

思考研讨：

思考1. 针对整数的四元正定二次型表示理论你能提出什么研讨问题？

参考. Conway, Bhargava 文献。

§2. Waring-Hilbert定理

如何推广Fermat-Lagrange定理？

定理3.2. 任意给定一个自然数k, 存在一个最小的$g(k)$使得每一个自然数都能表示为不多于$g(k)$个k次幂之和. 也就是, 对任意自然数n,

$$n = \sum_{i=1}^{g(k)} x_i^k$$

总有非负整数解.

注3.8. 这就是著名的Waring-Hilbert定理. 这一断言是由Waring于1770年提出来的. 他当时已明确地指出

$$g(2) = 4,$$

$$g(3) = 9$$

和

$$g(4) = 19.$$

一百多年以后, 这一一般性断言由Hilbert所证明. 与$g(k)$相类似, 存在一个最小的$G(k)$使得每一个充分大的自然数都可以表示为不多于$G(k)$个k次幂之和. 显然,

$$G(k) \leq g(k).$$

确定或估计$g(k)$和$G(k)$是解析数论中的重要问题.

例3.3. 证明

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

证明要点. 令

$$q = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$$

以及

$$n = 2^k q - 1.$$

因为$n < 3^k$, 所以它只能表示为若干个1^k和2^k之和, 即

$$n = i \cdot 2^k + j \cdot 1^k.$$

这时显然有

$$i + j \geq q - 1 + 2^k - 1.$$

所以,

$$g(k) \geq q - 1 + 2^k - 1 = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

注3.9. 由例3.3可以得出

$$g(2) \geq 4,$$
$$g(3) \geq 9,$$
$$g(4) \geq 19,$$
$$g(5) \geq 37.$$

事实上, 以上等号全成立. 其中$g(5)$是由陈景润定出的.

例3.4. 当$k \geq 2$时, 我们有

$$G(k) \geq k + 1.$$

证明要点. 令$A(N)$表示不大于N的正整数中能表示为k个k次幂之和

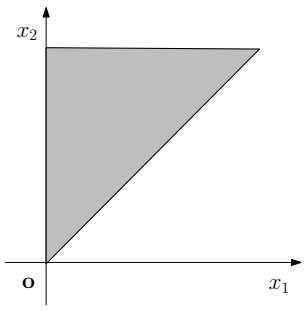
$$x_1^k + x_2^k + \cdots + x_k^k$$

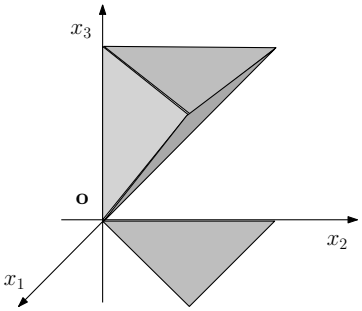
的个数. 不妨假定

$$0 \leq x_1 \leq x_2 \leq \cdots \leq x_k \leq \lfloor N^{1/k} \rfloor. \tag{3.2}$$

那么$A(N)$不超过适合上式的整数组的个数.

.





在k维空间，通过估计满足(3.2)的几何体的体积我们得到

$$\begin{aligned} A(N) &\leq \sum_{x_k=0}^{\lfloor N^{1/k}\rfloor} \sum_{x_{k-1}=0}^{x_k} \cdots \sum_{x_1=0}^{x_2} 1 = \frac{1}{k!} \prod_{i=1}^{k} \left(\left\lfloor N^{1/k} \right\rfloor + i \right) \\ &\sim \frac{N}{k!} \ll \frac{2}{3} N. \end{aligned}$$

所以

$$G(k) \geq k + 1.$$

注3.10. 用初等方法可以证明

$$g(3) \leq 13,$$

$$g(4) \leq 50,$$

$$g(6) \leq 2451,$$

$$g(8) \leq 42273.$$

Hilbert原始的证明是非常复杂的. 后来, 通过利用Schnirelman的密率概念 Linik将这一定理的证明得以大大地简化.

Schnirelman密率. T表示一个由互不相同的非负整数j 所构成的集合. 令$f(n)$表示T中不大于n的正整数的个数, 也就是

$$f(n) = \sum_{1 \le j \le n,\ j \in T} 1.$$

如果有（最大的）正数α存在, 使的

$$f(n) \ge \alpha n$$

对所有的正整数n都成立. 那么, 我们称该集合有正密率α.

例3.5. 令

$$T_1 = \{1, 4, 8, \cdots, 4k, \cdots\}$$

和

$$T_2 = \{1, 4, 9, \cdots, k^2, \cdots\}.$$

它们的密率分别是0.25和0.

数集的和. T_1和T_2表示两个非负整数集合. 我们定义

$$T = T_1 + T_2 = \{a + b : \ a \in T_1, \ b \in T_2\}.$$

引理3.4. 如果T（定义如上）, T_1和T_2 分别具有密率α, α_1和α_2 并且$0 \in T_1$, 那么

$$\alpha \geq \alpha_1 + \alpha_2 - \alpha_1\alpha_2.$$

证明要点. 假设N 为一个给定的自然数,

$$T_1 \cap [0, N] = \{0, a_1, a_2, \cdots, a_{f(N)}\},$$

$$T_2 \cap [1, N] = \{b_1, b_2, \cdots, b_{g(N)}\}$$

我们有如下论断：

I. 首先, 由于$0 \in T_1$, 我们有

$$T_2 \cap [1, N] = \{b_1, b_2, \cdots, b_{g(N)}\} \subseteq T$$

以及

$$card\{T_2 \cap [1, N]\} = g(N).$$

II. 对任一满足$1 \leq v \leq g(N)-1$的v, 如果$a \in T_1$并且$1 \leq a \leq b_{v+1}-b_v-1$, 那么

$$1 + b_v \leq a + b_v \leq b_{v+1} - 1.$$

它们不仅互不相同, 且与I中所列的数不同. 对所考虑的v, 共 有$f(b_{v+1} - b_v - 1)$个相应的$a + b_v$.

III. 如果$a \in T_1$, $1 \leq a \leq N - b_{g(N)}$, 那么 $a + b_{g(N)} \in T \cap [1, N]$且它们两两不同. 另外, 由于$a + b_{g(N)} \geq 1 + b_{g(N)}$, 所以本项所列的$f(N - b_{g(N)})$个数与I 和II所列的数都不相同.

由以上所讨论的三种情况可知,

$$\begin{aligned} card\{T \cap [1,N]\} &\geq g(N) + \sum_{v=1}^{g(N)-1} f(b_{v+1} - b_v - 1) + f(N - b_{g(N)}) \\ &\geq g(N) + \sum_{v=1}^{g(N)-1} \alpha_1(b_{v+1} - b_v - 1) + \alpha_1(N - b_{g(N)}) \\ &= g(N) + \alpha_1(b_{g(N)} - b_1 - (g(N) - 1) + N - b_{g(N)}) \\ &= g(N) + \alpha_1(N - g(N)) \geq (1 - \alpha_1)\alpha_2 N + \alpha_1 N \\ &= N(\alpha_1 + \alpha_2 - \alpha_1\alpha_2). \end{aligned}$$

所以,

$$\alpha \geq \alpha_1 + \alpha_2 - \alpha_1\alpha_2.$$

注3.11. 这一引理不是最佳结果. 最佳结果是

$$\alpha \geq \min\{1, \alpha_1 + \alpha_2\}.$$

这一结论是由Mann证明的, 由此他获得了美国数学会的数论奖.

只有引理3.4还不能证明Waring-Hilbert定理 (为什么？). 我们还需要如下引理.

引理3.5. 在引理3.4的假设下, 如果 $\alpha_1 + \alpha_2 \geq 1$, 那么

$$\alpha = 1.$$

证明要点. 假设$\alpha < 1$, 且n为满足$n \notin T$的最小自然数. 因为 $\alpha_2 > 0$ 可得$1 \in T_2$, 又因$0 \in T_1$ 可知$1 \in T$. 所以 $n \geq 2$. 另外, 由$0 \in T_1$可得 $n \notin T_2$.

如果

$$a \in T_1 \cap [1, n-1],$$

$$b \in T_2 \cap [1, n-1],$$

可得

$$a \neq n - b.$$

(否则, 可以导出$n \in T$, 矛盾.) 所以,

$$card\{T_1 \cap [1, n-1]\} + card\{T_2 \cap [1, n-1]\} \leq n - 1. \tag{3.3}$$

另一方面, 我们有

$$\begin{aligned} card\{T_2 \cap [1, n-1]\} &= card\{T_2 \cap [1, n] \\ &\geq \alpha_2 n > \alpha_2(n-1), \end{aligned}$$

$$\begin{aligned} &card\{T_1 \cap [1, n-1]\} + card\{T_2 \cap [1, n-1]\} \\ &> \alpha_1(n-1) + \alpha_2(n-1) \geq n-1. \end{aligned} \tag{3.4}$$

显然, (3.3)与(3.4)矛盾. 由此矛盾, 引理得证.

引理3.6. 对给定的$k \geq 2$, 我们定义

$$m = \frac{1}{2}8^{k-1}$$

和

$$T = \{x_1^k + x_2^k + \cdots + x_m^k : \ x_i = 0, 1, \cdots\}.$$

那么T具有正密率α

注3.12. 这一引理的证明是非常复杂的. 它是由Schnirelman 首先证明的, 后来Linik又给出了简化证明.

证明思路. 令$r(a)$表示不定方程

$$x_1^k + x_2^k + \cdots + x_m^k = a$$

的解的个数, 令$f(n)$表示1到n之间可以表示为m个k次幂之和的数的个数. 那么, 由 Buniyakowski-Schwarz不等式可以导出

$$\Big(\sum r(a)\Big)^2 \le \sum r(a)^2 \sum 1^2 = f(n)\sum r(a)^2,$$

也就是

$$\frac{f(n)}{n} \ge \frac{(\sum r(a))^2}{n\sum r(a)^2}.$$

所以这一引理可以由

$$\sum_{1\le a\le n} r(a) \ge c_1(k) n^{m/k}$$

和

$$\sum_{1\le a\le n} r(a)^2 \le c_2(k)n^{2m/k-1}$$

导出. 证明以上最后一个公式的关键是

$$\int_0^1 \left|\sum_{x=0}^{p} e^{2\pi i x^k \alpha}\right| d\alpha \le c_3(k)p^{2m-k}.$$

注3.13. 容易看出, Waring-Hilbert定理可以马上从以上3个引理导出.

As for the values of $g(k)$, among many partial results, it was shown by K. Mahler that

$$g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2 \tag{7}$$

holds when k is sufficiently large. It was conjectured by Euler that (7) holds for all $k \geq 2$. The exact values of $g(k)$ for small k are listed in the following table.

k	$g(k)$	Authors
2	4	J. L. Lagrange
3	9	A. Wieferich
4	19	R. Balasubramanian, F. Dress, J.M. Deshouiller
5	37	J.R. Chen
6	73	S.S. Pillai

关于$G(k)$, 我们有

$$G(k) \leq k(2\log k + 4\log\log k + 2\log\log\log k + 13).$$

这中间有I.M. Vinogradov和华罗庚的重要贡献。

作业3.3. 若$1 \in T$且

$$d(T) = \lim_{n\to\infty} \frac{f(n)}{n}$$

存在并大于零. 那么T具有正密率. 试证之.

思考研讨. 比较一下$G(k)$和$g(k)$的结果。

§3. Goldbach猜想

Goldbach猜想. 1. 任一奇数都可以表示为三个素数之和.
2. 任一偶数都可以表示为两个素数之和.

注3.14. 这一猜想最早出现在Goldbach写给Euler的一封信中. 前半部分已由Vinogradov基本上证明. 严格地说, 他证明了：**每一个充分大的奇数都可以表示为三个素数之和**. 在证明Goldbach猜想的探索中, Hardy, Littlewood, Vinogradov和Bombieri等在思想方法上做出了杰出的贡献.

这里, 我们既不试图介绍Vinogradov的证明, 也不介绍Hardy和Littlewood的著名方法, 而只是通过密率的方法介绍如下定理：

定理3.3. 存在一个常数h使得每一个自然数都可以表示为不多于h个素数之和.

注3.15. 这一定理首先是由Schnirelman证明的, 后来Selberg简化了他的证明. 如果Goldbach 猜想成立, 那么$h = 3$. 现在我们只知道$h \leq 27$.

引理3.7. 由1和所有能表示成两个素数之 和的自然数构成的集合具有正密率.

证明思路. 这一引理的证明是非常复杂的. 类似于Waring问题我们定义

$$r'(a) = \begin{cases} 1 & a = 1 \\ \sum_{p_1+p_2=a} 1 & a \geq 2 \end{cases}$$

那么以上引理可以从

$$\sum_{1\leq a\leq n} r'(a) \geq c_1 n^2/\log^2 n,$$

$$\sum_{1\leq a\leq n} r'(a)^2 \leq c_2 n^3/\log^4 n$$

和Buniyakowski-Schwarz不等式导出.

假定它成立, 我们可以这样导出以上定理：

由引理3.4, 3.5可以证明$n-2$可以表示为不多于h^*个素数和$f(n)$个1之和, 其中h^*是由引理3.7中的正密率所确定的一个正常数, $f(n) \leq h^*$. 显然$2+f(n)$可以表示为不多于$f(n)$个素数之和. 所以n可以表示为不多于$h=2h^*$个素数之和.

课外研讨：

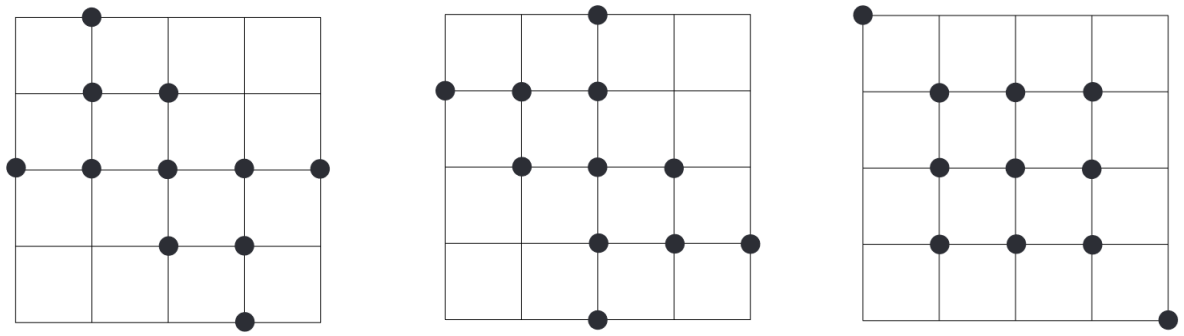


Fig. 4. Noncongruent origin-symmetric convex lattice sets with equal projection counts.

第四章. 素数的分布

§1. Tchebycheff 定理

我们已经知道自然数中有无限多个素数. 通常我们用$\pi(n)$表示不大于n的素数的个数. 很自然人们会问：**当n趋向无穷大时, $\pi(n)$的阶是多大？有无渐近公式？**

定理4.1. 当$n \geq 2$时,

$$\frac{1}{8} \cdot \frac{n}{\log n} \leq \pi(n) \leq 12 \cdot \frac{n}{\log n}.$$

注4.1. 这就是著名的Tchebycheff 定理. 它基本上确定了$\pi(n)$的阶.

这一定理的证明是富有思想和技巧的. 它基于以下两个简单引理：

引理4.1. 当$k \geq 0$时,

$$\pi(2^{k+1}) \leq 2^k.$$

主要想法. 当$n > 9$时,

$$\pi(n) \leq \frac{n}{2}.$$

引理4.2. 当$l \geq 1$时,

$$\frac{1}{2}l \leq \sum_{i=2}^{2^l} \frac{1}{i} \leq l.$$

主要想法. 事实上, 我们有

$$\begin{aligned}\sum_{i=2}^{2^l}\frac{1}{i} &= \frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\cdots \\ &> \frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\cdots \geq \frac{1}{2}l\end{aligned}$$

和

$$\begin{aligned}\sum_{i=2}^{2^l}\frac{1}{i} &= \left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)\cdots \\ &< \left(\frac{1}{2}+\frac{1}{2}\right)+\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right)\cdots \leq l.\end{aligned}$$

引理4.3. 假设w是满足$p^w | n!$的最大整数，那么

$$w = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor .$$

验证.

$$p, 2p, \ldots, \left\lfloor \frac{n}{p} \right\rfloor p; \qquad \left\lfloor \frac{n}{p} \right\rfloor ,$$

$$p^2, 2p^2, \ldots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2; \qquad \left\lfloor \frac{n}{p^2} \right\rfloor ,$$

$$\ldots .$$

证明Tchebycheff定理的主要想法. 最关键的想法是研究$\binom{2m}{m}$的分解. 首先, 容易证明

$$\prod_{m<p\leq 2m} p \Bigg| \binom{2m}{m}. \tag{4.1}$$

另一方面, 我们有

$$\binom{2m}{m} \Bigg| \prod_{p^r\leq 2m<p^{r+1}} p^r, \tag{4.2}$$

因为，由引理4.3可以证明$\binom{2m}{m}$中p的次数为

$$\sum_{j=1}^{r} \left(\left\lfloor \frac{2m}{p^j} \right\rfloor - 2 \left\lfloor \frac{m}{p^j} \right\rfloor \right) \leq r.$$

由(4.1)和(4.2)我们得到

$$m^{\pi(2m)-\pi(m)} < \prod_{m<p\leq 2m} p \leq \binom{2m}{m}$$

$$\leq \prod_{p^r\leq 2m<p^{r+1}} p^r \leq (2m)^{\pi(2m)}. \tag{4.3}$$

另外我们有

$$2^m \leq \frac{2m\ldots(m+1)}{m\ldots 1} = \binom{2m}{m} \leq (1+1)^{2m} = 2^{2m}. \tag{4.4}$$

由(4.3)和(4.4)我们分别得到

$$m^{\pi(2m)-\pi(m)} < 2^{2m} \tag{4.5}$$

和

$$2^m \leq (2m)^{\pi(2m)}. \tag{4.6}$$

取$m = 2^k$, 由(4.5)和(4.6)我们分别得到

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \tag{4.7}$$

和

$$2^k \leq (k+1)\pi(2^{k+1}). \tag{4.8}$$

由(4.7)引理4.1我们得到

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k,$$

也就是

$$(k+1)\pi(2^{k+1}) < 3\sum_{i=0}^{k} 2^k < 3 \cdot 2^{k+1}. \tag{4.9}$$

由(4.8) 和(4.9)可以得到

$$\frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \leq \pi(2^{k+1}) < 3 \cdot \frac{2^{k+1}}{k+1}. \tag{4.10}$$

假设$2^{k+1} \leq n < 2^{k+2}$并记$H(n) = \sum_{i=2}^{n} \frac{1}{i}$, 由(4.10)和引理4.2我们得到

$$\pi(n) \leq \pi(2^{k+2}) < 3 \cdot \frac{2^{k+2}}{k+2} \leq 6 \cdot \frac{2^{k+1}}{H(2^{k+2})} \leq 6 \cdot \frac{n}{H(n)},$$

$$\pi(n) \geq \pi(2^{k+1}) \geq \frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \geq \frac{1}{8} \cdot \frac{2^{k+2}}{H(2^{k+1})} \geq \frac{1}{8} \cdot \frac{n}{H(n)}$$

也就是

$$\frac{1}{8} \leq \pi(n) \cdot H(n)/n < 6. \tag{4.11}$$

另外, 当$n \geq 4$时可以证明

$$\frac{1}{2} \log n \leq \log \frac{n}{2} = \int_2^n \frac{dt}{t} < H(n) < \int_1^n \frac{dt}{t} = \log n. \tag{4.12}$$

Tchebycheff定理可从(4.11)和 (4.12)导出.

定理4.2. 在n和$2n$之间, 总存在素数.

注4.2. 这就是历史上有名的Bertrand假设. 它是由Tchebycheff 首先证明的. 其证明与前一定理相似, 也是基于对$\binom{2n}{2}$的深入分析, 但更精细.

作业4.1. 若$n > 1$, 证明$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ 一定不是整数。

§2. 素数的分布

定理4.3. 当n趋向无穷大时,

$$\pi(n) \sim \frac{n}{\log n}.$$

注4.5. 这就是著名的素数分布定理. 这一渐近公式是由Legendre和Gauss于1800年左右分别提出的. 直到1896年, 这一结论才由de la Vallée Poussin 和Hadamard独立证明. 1949年, Selberg与Erdös对此分别给出了一个初等证明. 为此Selberg获得了Fields奖, 但Erdös没有.

当$x > 0$时, 我们定义

$$\vartheta(x) = \sum_{p \le x} \log p$$

和

$$\psi(x) = \sum_{p^m \le x} \log p.$$

通常它们被称为Tchebycheff函数.

引理4.3.

$$\limsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = \limsup_{x\to\infty} \frac{\vartheta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x},$$

$$\liminf_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = \liminf_{x\to\infty} \frac{\vartheta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x}.$$

注4.6. 显然我们有

$$\psi(x) = \sum_{i=1}^{\infty} \vartheta(x^{1/i})$$

和

$$\psi(x) = \sum_{p \le x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

所以

$$\begin{aligned} \vartheta(x) &\le \psi(x) \le \sum_{p \le x} \frac{\log x}{\log p} \log p \\ &= \pi(x) \log x. \end{aligned}$$

由此可以导出

$$\limsup_{x \to \infty} \frac{\vartheta(x)}{x} \le \limsup_{x \to \infty} \frac{\psi(x)}{x} \le \limsup_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}}$$

反过来, 对任意$0 < \alpha < 1$可得

$$\begin{aligned}\vartheta(x) &\geq \sum_{x^\alpha \leq p \leq x} \log p \geq (\pi(x) - \pi(x^\alpha)) \log x^\alpha \\ &\geq \alpha(\pi(x) - x^\alpha) \log x\end{aligned}$$

以及

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \geq \alpha \limsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}}.$$

所以我们有

$$\limsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = \limsup_{x\to\infty} \frac{\vartheta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

思考题4.1. 如何证明引理中的第二式.

在de la Vallée Poussin 和Hadamard的证明中, Riemann ζ函数起了重要的 作用. 所谓的Riemann ζ函数也就是

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

其中$s = \sigma + it$并且$\sigma > 1$. 实际上, 通常所说的 Riemann ζ函数是指它解析延拓到全平面上的一个亚纯函数. 它只有一个单极点$s = 1$, 其留数为1, 并且满足

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

伽马函数的定义：

$$\Gamma(z) = \int_0^{+\infty} t^{z-1}e^{-t}dt.$$

Riemann 假设. $\zeta(s)$在 $0 < \sigma < 1$中的零点都在直线 $\sigma = \frac{1}{2}$上.

在深入研究 $\zeta(s)$的基础上, de la Vallée Poussin 和Hadamard证明以上零点都在$\epsilon < \sigma < 1 - \epsilon$中, 从而可以导出

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$$

从而导出定理. 如果Riemann 假设成立, 可以导出

$$\pi(x) = li(x) + O(\sqrt{x}\log x), \tag{4.13}$$

$$li(x) = \int_2^x \frac{dt}{\log t}.$$

反之, 从(4.13)也可以导出Riemann 假设.

Landau符号解释。

注4.7. Selberg与Erdös的证明从工具上讲是简单, 但是从技巧上讲却更繁琐复杂. 令$R(x)=\vartheta(x)-x$. 那么, 素数定理与

$$\lim_{x\to\infty}\frac{R(x)}{x}=0$$

是等价的. Selberg 与Erdös的初等方法包括许多对 $\vartheta(x)$和 $R(x)$的精细估计. 例如

$$\vartheta(x)+\sum_{pq<x}\frac{\log p\log q}{\log pq}=2x+O\left(\frac{x}{\log x}\right)$$

$$R(x)\log x=\sum_{pq<x}\frac{\log p\log q}{\log pq}R(x/pq)+O(x\log\log x)$$

$$|R(x)|\le\frac{1}{\log x}\sum_{n\le x}|R(x/n)|+O\left(\frac{x\log\log x}{\log x}\right)$$

$$\sum_{n\le x}\frac{\vartheta(n)}{n^2}=\log x+O(1)$$

$$\sum_{n\le x}\vartheta(x/n)=x\log x+O(x)$$

$$\sum_{n\le x}\frac{\log n}{n}R(n)=-\sum_{n\le x}\frac{1}{n}R(n)R(x/n)+O(x)$$

在这样一些准备的基础上, 试图证明

$$\frac{|R(x)|}{x}\le\sigma_n$$

其中$\sigma_n\to 0$.

作业4.2. 用p_n表示第n个素数, 证明

$$\lim_{n\to\infty} \frac{p_n}{n\log n} = 1.$$

附. Riemann ζ函数的几个恒等式

$\tau(n)$： n 的所有正除数的个数.

$\varphi(n)$： 所有小于n且与n无公因子的自然数的个数.

$\mu(n)$： Möbius函数：

$$\mu(n)=\begin{cases}1, & n=1\\ (-1)^r, & n\text{是}r\text{个互不相等的素数的积}\\ 0, & \text{其它}\end{cases}$$

$\Lambda(n)$： Mangoldt函数：

$$\Lambda(n)=\begin{cases}\log p, & n\text{是素数}p\text{的幂},\\ 0, & \text{其它}.\end{cases}$$

命题4.1. 若$s > 1$, 那么

$$\sum_{n=1}^{\infty} \mu(n) n^{-s} = \frac{1}{\zeta(s)},$$

$$\sum_{n=1}^{\infty} \mu(n)^2 n^{-s} = \frac{\zeta(s)}{\zeta(2s)}.$$

和

$$\sum_{n=1}^{\infty} \tau(n) n^{-s} = \zeta(s)^2.$$

证明. 首先，我们回顾$\mu(n)$的性质

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if\ n = 1, \\ 0 & if\ n > 1. \end{cases}$$

所以，我们得到

$$\zeta(s)\sum_{n=1}^{\infty}\mu(n)n^{-s}=\sum_{n=1}^{\infty}n^{-s}\sum_{n=1}^{\infty}\mu(n)n^{-s}=\sum_{n=1}^{\infty}\left(\sum_{d|n}\mu(d)\right)n^{-s}=1.$$

第一个恒等式得证。

其次，容易导出：每一个自然数n都可以唯一地表示为一个无平方因子的自然数P与一个平方数Q 的乘积。所以，由$\mu(n)$的定义

$$\zeta(2s)\sum_{n=1}^{\infty}\mu(n)^2n^{-s}=\sum Q^{-s}\sum P^{-s}=\sum_{n=1}^{\infty}n^{-s}=\zeta(s).$$

第二个恒等式得证。

最后，我们有

$$\zeta(s)^2 = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)^2 = \sum_{n=1}^{\infty} \left(\frac{1}{n^s} \sum_{d|n} 1\right) = \sum_{n=1}^{\infty} \tau(n) n^{-s}.$$

第三个恒等式得证。

命题4.2. 若$s > 2$, 则有

$$\sum_{n=1}^{\infty} \varphi(n) n^{-s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

证明. 回顾作业2.8，我们有

$$\sum_{d|n} \varphi(d) = n.$$

所以，我们得到

$$\zeta(s) \sum_{n=1}^{\infty} \varphi(n) n^{-s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \left(\frac{1}{n^s} \sum_{d|n} \varphi(d) \right) = \zeta(s-1).$$

命题得证。

命题4.3. 若$s > 1$, 则有

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

证明. 由Mangoldt函数的定义可以导出

$$\sum_{d|n} \Lambda(d) = \log n.$$

一方面，由导数公式我们可以算出

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

另一方面，我们可以得到

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=\sum_{n=1}^{\infty}\left(\frac{1}{n^s}\sum_{d|n}\Lambda(d)\right)=\sum_{n=1}^{\infty}\frac{\log n}{n^s}.$$

比较前面两个公式，命题得证。

E. C. Titchmarsh, *The theory of functions*, Oxford University Press, 1932.
E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Clarendon Press, Oxford, 1951.

讨论思考题4.1. 在素数分布定理的基础上，你会提问思考什么问题？

讨论思考题4.2. 围绕黎曼假设，你会试验思考什么问题？

§3. Dirichlet定理

例4.1. 有无限多个形如$4k+3$的素数.

证明要点. 假如只有$m+1$个形如$4k+3$的素数, 记作$p_0=3$, p_1, p_2, $\cdots$, p_m. 我们令

$$n = 4p_1p_2\cdots p_m + 3,$$

并将其分解为素数幂的乘积

$$q_1^{l_1}q_2^{l_2}\cdots q_r^{l_r}.$$

显然, 所有的q_i不可能都是$4K+1$形的, 也不可能是2或3. 所以必有一个素因子 q_i是$4k+3$形的. 同时, 它不可能是p_0, p_1, $\cdots$, p_m中的任何一个. 由此矛盾可以得出$4k+3$形的素数有无限个.

为了介绍Dirichlet定理, 我们先来介绍一个基本概念：

定义4.1. 我们用$\varphi(n)$表示不大于n且与n互素的整数的个数. 通常它被称为Euler函数.

注4.9. 这是一个非常重要的函数, 在许多数论问题的研究中起着重要的作用. 它有许多重要性质. 例如：如果$(a,b)=1$, 那么

$$\varphi(ab)=\varphi(a)\varphi(b).$$

定理4.4. 假定a和m为互素的两个自然数. 我们用$\pi(x,m,a)$表示形如$km+a$且不大于x的素数的个数. 那么

$$\pi(x,m,a)\sim\frac{x}{\varphi(m)\log x}$$

注4.10. 这就是著名的Dirichlet定理, 也叫等差级数中的素数分布定理. 通过比较定理 4.3和定理4.4, 可见素数分布还是较有规律的.

定义4.2. m是一个给定的自然数, $\chi(n)$是在所有整数上定义的 一个复值函数. 如果$\chi(n)$满足如下条件：

1. 如果$(n,m)\neq 1$, 那么$\chi(n)=0$；
2. $\chi(1)\neq 0$;
3. 如果$a\equiv b\ (mod\ m)$, 那么$\chi(a)=\chi(b)$;
4. $\chi(ab)=\chi(a)\chi(b)$.

我们称它为对模m的一个特征函数.

注4.11. 特征函数是非常重要的一个概念. 它对证明Dirichlet定理 尤为重要. 如果m是一个素数, 那么总存在一个小于m的自然数α（通常叫做原根）使的

$$\alpha^x \equiv n \ (mod \ m)$$

对任一$n < m$都有不大于m的自然数解. 通常这一解被记为$ind(n)$. 对任意给定的a,

$$\chi(n) = e^{2\pi i a \ ind(n)/(m-1)}$$

就是一个特征函数.

基本性质一. 对给定的自然数m, 有且仅有$\varphi(m)$个互不相同的 特征函数.

由定义中的第(4)条可以导出：$\chi(a)^{\varphi(m)} = 1$ 对所有满足$(a, m) = 1$的a都成立. 所以, 对给定的m特征函数的个数是有限的.

为了证明这一性质, 可以先证m为一个素数的情况, 再证m为一个素数幂的情况, 最后导出一般情况.

基本性质二.

$$\sum_{n\in\{1,\cdots,m\}}\chi(n)=\begin{cases}\varphi(m), & \text{如果 } \chi=I\\ 0, & \text{如果 } \chi\neq I\end{cases}$$

这里

$$I(a)=\begin{cases}0, & \text{如果 } (a,m)\neq 1\\ 1, & \text{如果 } (a,m)=1\end{cases}.$$

基本性质三.

$$\sum_{\chi}\chi(n)=\begin{cases}\varphi(m), & \text{如果 } n\equiv 1\ (mod\ m)\\ 0, & \text{如果 } n\not\equiv 1\ (mod\ m)\end{cases}.$$

Dirichlet定理的证明思路. 令

$$L(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}.$$

在这些性质的基础上, 可以证明

$$\sum_{p\le x}\frac{\chi(p)\log p}{p}=\begin{cases}O(1) & \text{若}L(\chi)\neq 0\\ -\log x+O(1) & \text{若}L(\chi)=0\end{cases}$$

和

$$\varphi(m)\sum_{p\le x,\ p\equiv a\ mod\ m}\frac{\log p}{p}=\log x+O(1).$$

类似于素数定理的证明，当$x>0$时, 我们定义

$$\vartheta_a(x)=\sum_{p\le x,\ p\equiv a\ mod\ m}\log p,$$

$$\psi_a(x) = \sum_{p \le x,\ p \equiv a \ mod \ m} \Lambda(p)$$

以及

$$R_a(x) = \vartheta_a(x) - \frac{x}{\varphi(m)}.$$

在此基础上证明

$$\limsup_{x\to\infty} \frac{\pi(x,m,a)}{\frac{x}{\varphi(m)\log x}} = \limsup_{x\to\infty} \frac{\vartheta_a(x)}{\frac{x}{\varphi(m)}} = \limsup_{x\to\infty} \frac{\psi_a(x)}{\frac{x}{\varphi(m)}},$$

$$\liminf_{x\to\infty} \frac{\pi(x,m,a)}{\frac{x}{\varphi(m)\log x}} = \liminf_{x\to\infty} \frac{\vartheta_a(x)}{\frac{x}{\varphi(m)}} = \liminf_{x\to\infty} \frac{\psi_a(x)}{\frac{x}{\varphi(m)}},$$

$$\dots$$

$$\lim_{x\to\infty} \frac{R_a(x)}{x} = 0.$$

与素数相关的几个著名问题.

问题4.1（孪生素数问题）. 差为2的素数对是否有无限个？

问题4.2. 形如n^2+1的素数是否有无限多？

问题4.3. 在$(n+1)^2$和n^2之间是否总有素数？

你可以试试n^2+n+41形状的数。

作业4.3. 若χ为模m的一个特征函数且$\chi \neq I$, 那么对任意 自然数j和k, $(j \leq k)$, 我们有

$$\left| \sum_{i=j}^{k} \chi(i) \right| \leq \frac{\varphi(m)}{2}.$$

作业4.4. 若χ_1和χ_2是模m的两个特征函数, 那么$\chi_1\chi_2$ 和$\overline{\chi_1}$都是模m的特征函数.

作业4.5. 证明：除3，5，7外，没有其他形如$p, p+2, p+4$的三素数。

第五章. 丢番图方程

§1. 线性方程

丢番图方程是指系数和变量都是整数的方程. 而方程的次数是指变量的最高次数.

定理5.1. 方程

$$ax + by = n$$

有解的充分必要条件是$(a, b) \mid n$. 当$(a, b) = 1$, 且x_0和y_0是它的一组 解, 那么它的任一解都可以表示为

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak. \end{cases}$$

证明要点. 显然, 前半部分可由定理2.4导出. 如果

$$ax + by = n$$

和

$$ax_0 + by_0 = n$$

同时成立, 则有

$$a(x - x_0) + b(y - y_0) = 0.$$

由$(a, b) = 1$可得$a \mid (y - y_0)$,

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak. \end{cases}$$

定理5.2. 若$a_1, a_2, \cdots, a_n$是满足$(a_1, a_2, \cdots, a_n) = 1$ 的一组正整数.我们用$A(N)$表示

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$$

的非负解的个数. 那么

$$\lim_{N\to\infty} \frac{A(N)}{N^{n-1}} = \frac{1}{a_1a_2\cdots a_n(n-1)!}.$$

证明要点. 令

$$f(x) = \frac{1}{1-x^{a_1}} \cdot \frac{1}{1-x^{a_2}} \cdots \frac{1}{1-x^{a_n}}.$$

那么$A(N)$即$f(x)$的无穷级数展开式中x^N项的系数.

若$1, \tau_1, \tau_2, \cdots, \tau_t$表示

$$(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})$$

的根, 且次数分别为

$$n, l_1, l_2, \cdots, l_t,$$

那么我们可以得到

$$l_i \leq n-1$$

且

$$\begin{aligned} f(x) \ = \ & \frac{A_n}{(1-x)^n} + \cdots + \frac{A_1}{1-x} + \\ & + \cdots + \\ & \frac{Z_{l_t}}{(\tau_t - x)^{l_t}} + \cdots + \frac{Z_1}{\tau_t - x}. \end{aligned}$$

令

$$g(x) = \frac{A}{(\alpha - x)^k}$$

并用$C(N)$表示$g(x)$的无穷级数展开式中x^N项的系数, 我们得到

$$g^{(N)}(x) = \frac{A \cdot k(k+1)\cdots(k+N-1)}{(\alpha - x)^{k+N}},$$

$$C(N) = \frac{g^{(N)}(0)}{N!} = \frac{A \cdot (N+1)\cdots(N+k-1)}{(k-1)!\alpha^{k+N}}$$

以及

$$\lim_{N\to\infty} \frac{C(N)\alpha^{k+N}}{N^{k-1}} = \frac{A}{(k-1)!}.$$

由此可以得出

$$\lim_{N\to\infty} \frac{A(N)}{N^{n-1}} = \frac{A_n}{(n-1)!},$$

$$\begin{aligned} A_n &= \lim_{x\to 1} \frac{(1-x)^n}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})} \\ &= \frac{1}{a_1\cdots a_n}. \end{aligned}$$

证毕.

注5.1. 在以上两定理的基础上, 可以得出若$(a,b) = 1$, $a > 0$, $b > 0$, 那么任一大于$ab - a - b$的自然数都可以表示为 $ax + by$的形式, 其中$x > 0$和$y > 0$. 但是$ab - a - b$不能. 多变量的类似问题是数 论中的一个著名难题.

练习5.1. 如果$a > 0$, $b > 0$并且 $(a,b) = 1$, 那么

$$xa + yb = n$$

的非负整数解的个数是$\lfloor n/ab \rfloor$或 $\lfloor n/ab \rfloor + 1$.

§2. Pell方程与连分数

通常所说的Pell方程是指形如

$$x^2 - dy^2 = 1 \tag{5.1}$$

或

$$x^2 - dy^2 = -1 \tag{5.2}$$

的方程.

注5.3. 事实上, 并不是一个叫Pell的数学家最早研究过这类方程或曾在 这一问题做出过杰出 的贡献. 历史上, 最早系统地研究这一问题的是Fermat, 而做出最重要贡献的是Lagrange 和Euler. 是Lagrange和Euler为研究这一问题而系统地发展了连分数这一重要工具.

a_0为一整数, a_1, a_2, $\cdots$ 皆为正整数. 我们称

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

为一连分数. 通常简记为

$$[a_0, a_1, \cdots].$$

另外我们定义

$$\frac{p_n}{q_n} = [a_0, a_1, \cdots, a_n]$$

并称之为以上连分数的n级近似.

注5.4. 连分数有许多重要的性质, 它不仅对Pell方程的研究起了 最关键的作用, 对丢番图逼近的一些问题也是最重要的工具之一.

定理5.3. 对一个连分数的n级近似, 我们有

$$p_0 = a_0, \quad q_0 = 1;$$

$$p_1 = a_1 a_0 + 1, \quad q_1 = a_1;$$

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

证明要点. 用归纳法,

$$\begin{aligned}
\frac{p_{n+1}}{q_{n+1}} &= [a_0, a_1, \cdots, a_{n+1}] = \left[a_0, a_1, \cdots, a_n + \frac{1}{a_{n+1}}\right] \\
&= \frac{(a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}})q_{n-1} + q_{n-2}} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\
&= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}
\end{aligned}$$

定理5.4.

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1};$$
$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_nq_{n-1}};$$
$$p_nq_{n-2} - p_{n-2}q_n = (-1)^n a_n.$$

证明要点. 由定理5.3和归纳法,我们得到

$$\begin{aligned} p_nq_{n-1} - p_{n-1}q_n &= (a_np_{n-1} + p_{n-2})q_{n-1} \\ &\quad -p_{n-1}(a_nq_{n-1} + q_{n-2}) \\ &= (-1)^{n-1}. \end{aligned}$$

第二个公式是第一个公式的简单推论。类似地可以得到

$$p_nq_{n-2} - p_{n-2}q_n = a_n(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = (-1)^n a_n.$$

由前面两个定理，我们容易得到下面两个重要推论：

定理5.5.

$$\begin{aligned} &q_n \geq q_{n-1} + 1; \\ &\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}; \\ &\frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}. \end{aligned}$$

定理5.6. 命

$$\alpha_n = [a_0, a_1, \cdots a_n],$$

则α_n的极限存在.

给定一个正实数a, 定义

$$\begin{aligned} a_0 &= [a], \qquad & b_0 &= \{a\}, \\ a_1 &= [1/b_0], \qquad & b_1 &= \{1/b_0\}, \\ &\cdots \\ a_n &= [1/b_{n-1}], \qquad & b_n &= \{1/b_{n-1}\}, \\ &\cdots \end{aligned}$$

当然, 如果$b_i = 0$则定义停止. 这样我们得到一个连分数

$$a' = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

容易证明：

命题5.1. 假如a是一个有理数，那么a'是一个有限连分数。

命题5.2. 假如a是一个正实数，那么$a' = a$.

在生成连分数的过程中, 如果存在两个非负整数m和k, 当$n \geq m$时

$$a_{n+k} = a_n$$

我们就称它为一循环连分数. 满足这一性质的最小k被称为它的周期. 我们记为

$$a = [a_0; a_1, a_2, \ldots, a_{m-1}, \overline{a_m, a_{m+1}, \ldots, a_{m+k-1}}].$$

例5.1. 记$\alpha = [1, 1, 1, \cdots] = [1; \overline{1}]$. 可以得出

$$\alpha = 1 + \frac{1}{\alpha},$$

也就是

$$\alpha^2 - \alpha - 1 = 0.$$

所以,

$$\alpha = (1 \pm \sqrt{5})/2.$$

再由$\alpha > 1$, 我们得到

$$\alpha = (1 + \sqrt{5})/2.$$

例5.2.

$$\begin{aligned} \sqrt{8} &= [2, (\sqrt{8}+2)/4] = [2, 1, \sqrt{8}+2] = [2, 1, 4, (\sqrt{8}+2)/4] \\ &= [2, 1, 4, 1, 4, \cdots] = [2; \overline{1, 4}]. \end{aligned}$$

定理5.7 (Euler-Lagrange). 每一个循环连分数都是二次无理数； 反过来，每一个二次无理数都可以被表示为一个循环连分数.

第一部分证明 (Euler, 1737). 假设

$$\alpha = [a_0; a_1, a_2, \ldots, a_{m-1}, \overline{a_m, a_{m+1}, \ldots, a_{m+k}}]. \tag{5.3}$$

我们取

$$\beta = [\overline{a_m; a_{m+1}, \ldots, a_{m+k}}].$$

这样，我们得到

$$\beta = [a_m; a_{m+1}, \ldots, a_{m+k}, \beta],$$

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}$$

以及

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0.$$

所以，β是一个二次无理数。再由(5.3)我们得到

$$\alpha = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}}.$$

即，α也是一个二次无理数。

定理5.8 (Euler, Lagrange). 若$\sqrt{d}$ 的循环连分数的周期是l, 渐近分数是 $\frac{p_n}{q_n}$, 那么

1. 当l为偶数时, (5.2)无解, (5.1)的全部正解为

$$x = p_{jl-1}, \quad y = q_{jl-1} \quad j = 1, 2, 3, \cdots .$$

2. 当l为奇数时, (5.2)的全部正解为

$$x = p_{jl-1}, \quad y = q_{jl-1} \quad j = 1, 3, 5, \cdots$$

(5.1)的全部正解为

$$x = p_{jl-1}, \quad y = q_{jl-1} \quad j = 2, 4, 6, \cdots .$$

练习5.2. 通过确定$\sqrt{11}$的循环连分数求解不定方程

$$x^2 - 11y^2 = 1$$

和

$$x^2 - 11y^2 = -1.$$

练习5.3. 设$u_1 = u_2 = 1$, $u_{i+1} = u_{i-1} + u_i$, 那么$\{u_1, u_2, \cdots, \}$被称为Fibonacci列. 试证 $(1+\sqrt{5})/2$的第n个渐进分数为 u_{n+2}/u_{n+1}.

§3. Fermat 定理

定理5.9. 若$n \geq 3$, 那么

$$x^n + y^n = z^n$$

无自然数解.

Euler研究过$n = 3$的情况. 它可由如下两个引理导出：

引理5.1. 设p为一个大于3的素数, 那么

$$x^2 + 3y^2 = p$$

有解的充分必要条件是$(\frac{-3}{p}) = 1$.

引理5.2. 设s为一个奇数, 那么

$$s^3 = a^2 + 3b^2, \qquad (a, b) = 1$$

成立的充分必要条件是存在α, β满足

$$s = \alpha^2 + 3\beta^2, \qquad (\alpha, 3\beta) = 1,$$
$$a = \alpha^3 - 9\alpha\beta^2, \qquad b = 3\alpha^2\beta - 3\beta^3.$$

注5.7. 这两个引理以及定理的证明都非常繁琐. 我们注意到引理5.2与毕达哥拉斯定理(引理5.3)的相似性.

引理5.3. 方程$x^2+y^2=z^2$满足$2|x$和$(x,y)=1$的所有正整数解都可表示为

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2,$$

$(a,b)=1$, $a>b>0$, a和b一奇一偶.

证明思路. 从$2|x$和$(x,y)=1$可以导出$(y,z)=1$并且y和z均为奇数. 我们进而得到$z-y$和$z+y$均为偶数且

$$x^2=(z-y)(z+y). \tag{5.4}$$

若

$$((z-y)/2,(z+y)/2)=k\neq 1,$$

则可以导出$(y,z)=k$. 所以, 由(5.4)可以导出$(z+y)/2=a^2$与$(z-y)/2=b^2$均为平方数. 亦即

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2.$$

情形$n = 4$的证明. 假设$x^4 + y^4 = z^2$有解, 并假定u是其正解中z的最小值. 显然, 这时$(x, y) = 1$.

由引理5.3, 我们可设

$$x^2 = 2ab, \qquad y^2 = a^2 - b^2, \qquad u = a^2 + b^2,$$

$$a > 0, \quad b > 0, \quad (a, b) = 1, \quad a + b \equiv 1 \pmod 2.$$

若a偶b奇, 则可以导出

$$y^2 \equiv -1 \pmod 4.$$

显然不可能. 故a奇b偶. 命$b = 2c$, 则有

$$(x/2)^2 = ac, \qquad (a, c) = 1.$$

所以, 我们得到

$$a = d^2, \quad c = f^2, \quad d > 0, \quad f > 0, \quad (d, f) = 1, \quad 2 \dagger d,$$

$$y^2 = a^2 - b^2 = d^4 - 4f^4,$$

亦即

$$(2f^2)^2 + y^2 = (d^2)^2,$$

其中(因为$(d, 2f) = 1$)

$$(2f^2, y, d^2) = 1.$$

再由引理5.3, 我们有

$$2f^2 = 2lm, \quad d^2 = l^2 + m^2, \quad (l, m) = 1.$$

由于

$$f^2 = lm, \quad (l, m) = 1$$

可得

$$l = r^2, \quad m = s^2$$

以及

$$d^2 = r^4 + s^4,$$

其中

$$d \leq d^2 = a \leq a^2 < a^2 + b^2 = u.$$

这与u的最小假设矛盾。所以，$x^4 + y^4 = z^4$无整数解。

注5.8. 这就是Fermat的递降法.

注5.9. 这一猜想是由Fermat于1637年提出. Euler和Kummer等大数学家曾研究过$n = 3, 5$的情况. 后来, Faltings证明了Mordell的一个猜想从而推出**这类方程最多只有有限个解**. 由于这一工作, Faltings于1982年获得了Fields奖. 直到1995年前后, 才由Wiles在Taylor 的帮助下, 在Taniyama, Shimura, Frey等人的工作的基础上证明了这一定理.

附：abc猜想 如果a, b和c为两两互素的自然数且满足 $a+b=c$, 那么

$$h < (1+\epsilon)n + d,$$

其中$h = \log c$, $n = \sum_{p|abc} \log p$, ϵ为任意正数, d为一个绝对常数.

注5.8. 从这一猜想可以导出Fermat大定理.

第六章. 丢番图逼近

§1. Dirichlet 逼近定理

定理6.1. 对任意给定的实数α和任意给定的自然数N总能找到 一个自然数$n \leq N$和一个整数p满足

$$|n\alpha - p| \leq \frac{1}{N},$$

也就是

$$\left|\alpha - \frac{p}{n}\right| < \frac{1}{nN}.$$

证明要点. 观察有限数列$\{0\alpha\},\{\alpha\},\{2\alpha\},\cdots,\{N\alpha\}$. 显然, 它们都在半闭半开区间$[0,1)$内. 将该区间分成$N$个长为$1/N$的区间

$$U_j=\left[\tfrac{j-1}{N},\tfrac{j}{N}\right),\quad j=1,2,\cdots,N.$$

以上数列中必有两个$n_1\alpha$和$n_2\alpha$ (假定$n_1>n_2$) 在同一个小区间中. 所以

$$|(n_1-n_2)\alpha-[n_1\alpha]+[n_2\alpha]|<1/N.$$

这样, 取

$$n=|n_1-n_2|$$

和

$$p=[n_1\alpha]-[n_2\alpha]$$

即可.

注. 这就是抽屉原理的出处。

定理6.2. 对每一个给定的无理数α总能找到无穷多个整数对 (m,n)满足

$$\left|\alpha-\frac{m}{n}\right|<\frac{1}{n^2}.$$

证明要点. 假定只有k对这样的数对(m_i,n_i), $i=1,2,\cdots,k$. 我们取

$$\delta=\min_i\{|n_i\alpha-m_i|\}$$

以及

$$N=[1/\delta]+1.$$

由定理6.1, 存在一对 (m,n)满足

$$n\le N$$

和

$$|n\alpha-m|<1/N<\delta.$$

显然(m,n)不是以上k个数对中的任何一个. 但是它满足

$$\left|\alpha-\frac{m}{n}\right|<\frac{1}{nN}\leq\frac{1}{n^2}.$$

所以有无限对.

注6.1. 如果α为有理数, 则至多有有限个整数对(m,n)满足

$$\left|\alpha-\frac{m}{n}\right|<\frac{1}{n^2}.$$

注6.2. 通过这一定理也可以证明Pell方程有无限组整数解.

定理6.3. α_{ij} $(i = 1, 2, \cdots, M; j = 1, 2, \cdots, L)$ 是ML个实数. N为任一给定的自然数. 我们总能找到M个整数$p_1, p_2, \cdots, p_M$ 和L个整数$n_1, n_2, \cdots, n_L$同时满足$|n_j| \leq N^{M/L}$和

$$\left| \sum_{j=1}^{L} n_j \alpha_{ij} - p_i \right| < \frac{1}{N}, \quad i = 1, 2, \cdots, M.$$

注6.3. 这一定理是定理6.1的推广, 通常被称为Dirichlet联立逼近定理.

§2. Hurwitz 定理

定理6.4. 在α的任意两个连续的渐近连分数中必有一个满足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

证明要点. 由连分数的性质我们知道α介于$\frac{p_{n+1}}{q_{n+1}}$与 $\frac{p_n}{q_n}$之间. 所以,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right|.$$

若定理不对，我们可以导出

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2},$$

$$2q_n q_{n+1} \geq q_{n+1}^2 + q_n^2,$$

$$(q_{n+1} - q_n)^2 \leq 0.$$

显然，这与连分数的性质

$$q_{n+1} = a_{n+1} q_n + q_{n-1}$$

相矛盾。定理得证。

定理6.5 (Hurwitz). 在α的任意三个连续的渐近连分数中必有一个满足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

证明要点1. 记$\alpha_i' = [a_i, a_{i+1}, \cdots]$, 并且记$q_{n-1}/q_n = \beta_{n+1}$. 由连分数的定义（参见定理5.3的证明）我们有

$$\alpha = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}, \qquad n \geq 2.$$

所以，由定理5.4我们得到(注意α'的下指标),

$$\left|\frac{p_n}{q_n} - \alpha\right| = \frac{1}{q_n(\alpha_{n+1}' q_n + q_{n-1})} = \frac{1}{q_n^2(\alpha_{n+1}' + \beta_{n+1})}.$$

下面, 我们证明

$$\alpha_i' + \beta_i \leq \sqrt{5} \tag{6.1}$$

对$i = n-1, n, n+1$不可能同时成立.

若它对$i = n-1$和$i = n$都成立. 由α_i'和 β_i的定义,我们得到

$$\alpha_{n-1}' = a_{n-1} + \frac{1}{\alpha_n'} \tag{6.2}$$

和

$$\frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = \frac{a_{n-1}q_{n-2} + q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1}. \tag{6.3}$$

由(6.2),(6.3),(6.1)我们得到

$$\frac{1}{\alpha_n'} + \frac{1}{\beta_n} = \alpha_{n-1}' - a_{n-1} + a_{n-1} + \beta_{n-1} = \alpha_{n-1}' + \beta_{n-1} \leq \sqrt{5}. \tag{6.4}$$

由(6.4),(6.1)我们得到

$$1 = \frac{1}{\alpha'_n} \cdot \alpha'_n \leq \left(\sqrt{5} - \frac{1}{\beta_n}\right)(\sqrt{5} - \beta_n) \tag{6.5}$$

和

$$\beta_n + \frac{1}{\beta_n} \leq \sqrt{5}. \tag{6.6}$$

因为β_n是有理数, 所以我们有

$$\beta_n^2 - \sqrt{5}\beta_n + 1 < 0,$$

$$\left(\beta_n - \frac{\sqrt{5}}{2}\right)^2 < \frac{1}{4}.$$

又因为$\beta_n < 1$, 我们得到

$$\beta_n > \frac{1}{2}(\sqrt{5} - 1). \tag{6.7}$$

同理, 若(6.1)对$i = n$和$i = n + 1$都成立则可以得到

$$\beta_{n+1} > \frac{1}{2}(\sqrt{5} - 1). \tag{6.8}$$

由(6.3), (6.6), (6.7)和 (6.8)我们得到

$$a_n = \frac{1}{\beta_{n+1}} - \beta_n < \sqrt{5} - \beta_{n+1} - \beta_n < \sqrt{5} - (\sqrt{5} - 1) = 1,$$

这与a_n是正整数相矛盾. 定理得证.

引理6.1. 如果$x \geq 1$且满足 $x + x^{-1} < \sqrt{5}$, 那么必有

$$1 \leq x < (\sqrt{5}+1)/2.$$

证明方法2. 用反证法, 假设定理不正确, 对$j = n,\ n+1$我们得到

$$\frac{1}{q_j q_{j-1}} = \left|\frac{p_j}{q_j} - \frac{p_{j-1}}{q_{j-1}}\right| = \left|\frac{p_j}{q_j} - \alpha\right| + \left|\alpha - \frac{p_{j-1}}{q_{j-1}}\right| \geq \frac{1}{\sqrt{5}q_j^2} + \frac{1}{\sqrt{5}q_{j-1}^2}.$$

为了方便, 我们取$k_j = q_j/q_{j-1}$. 由上式我们得到

$$k_j + k_j^{-1} \leq \sqrt{5}, \qquad j = n,\ n+1.$$

由连分数的基本性质和引理6.1我们得到

$$1 \le k_j < (\sqrt{5}+1)/2, \qquad j = n,\ n+1. \tag{6.9}$$

另一方面, 我们又有

$$k_{n+1} = \frac{a_{n+1}q_n + q_{n-1}}{q_n} = a_{n+1} + k_n^{-1} \ge 1 + k_n^{-1}.$$

由此以及$k_n < (\sqrt{5}+1)/2$可以导出

$$k_{n+1} > (\sqrt{5}+1)/2.$$

这与(6.9)矛盾. 证毕.

注6.4. 这一结论是最佳的. 当$\alpha = (\sqrt{5}-1)/2$且$A > \sqrt{5}$时,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$$

最多有有限解.

§3. Kronecker 逼近定理

定理6.6. 对任意给定的无理数α, 实数β, 任意小的数 $\epsilon > 0$和任意大的数N, 总能找到两个整数p和n(其中$|n| \geq N$)满足

$$|n\alpha - \beta - p| < \epsilon.$$

证明要点. 由定理6.2可知, 存在两个整数p和q满足

$$|p| \geq N$$

和

$$0 < |p\ \alpha - q| < \epsilon.$$

注6.5. 如果α是有理数, 这一定理则不成立. 这一点与Dirichlet 逼近定理是一致的. 类似的, 我们也有如下的联立逼近定理.

定理6.7. $\alpha_1, \alpha_2, \cdots, \alpha_l$ 为l 个整线性无关的无理数, $\beta_1, \beta_2, \cdots, \beta_l$为$l$个实数, ϵ和N为两个任意正数. 那么总能找到$l+1$个整数$p_1, p_2, \cdots, p_l$ 和n (其中$|n| \geq N$)满足

$$|n\alpha_i - \beta_i - p_i| < \epsilon, \quad i = 1, 2, \cdots, l.$$

注6.6. 在Dirichlet逼近定理和Kronecker逼近定理的基础上, Weyl, van der Corput, Hlawka等发展了一致分布理论: 若p_i为$(0,1)$中的一个点集, 对任意给定的自然数n及两个正数a和b, $(0 \leq a < b \leq 1)$, 在$p_1\ p_2 \cdots\ p_n$中落入区间(a,b)中的个数$N(n,a,b)$总满足

$$\lim_{n\to\infty} \frac{N(n,a,b)}{n} = b - a,$$

我们就称点集$p_1\ p_2 \cdots$在$(0,1)$中是一致分布的.

命题6.1. 如果α为一无理数, 那么$\{n\alpha\}$在$(0,1)$中是一致分布的.

命题6.2. 数列$x_1,\ x_2,\ \cdots$在$(0,1)$中是一致分布的充分必要条件是对任意在该区间上Riemann可积的函数$f(x)$都有

$$\lim_{n\to\infty} \frac{\sum_{i=1}^{n} f(x_i)}{n} = \int_0^1 f(x)dx.$$

§4. Roth定理

首先, 我们介绍两个基本概念：

定义6.1. 如果实数α是某个整系数多项式的根, 我们就称它是一个代数数；否则就称它是一个超越数。更进一步，如果满足$f(\alpha)=0$的整系数多项式$f(x)$的最低次数是n，我们称α是一个n次代数数。

思考6.1. 把整系数多项式换成有理多项式会更广泛吗？

思考6.2. 超越数存在吗？

定理6.8 (Liouville). 若α 是一个n次代数数. 那么对任一$\epsilon > 0$及$A > 0$, 适合不等式

$$\left|\alpha - \frac{x}{y}\right| < \frac{A}{y^{n+\epsilon}}$$

的有理数解$\frac{x}{y}$ 的个数是有限的.

证明思路. 如果α适合

$$f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

其中a_i均为整数，$a_0 > 0$, $a_n \neq 0$。可以找到适当的$M > 0$, 当 $|x| \leq 1$时总有

$$|f'(x)| \leq M.$$

一方面, 容易得到

$$|f(\tfrac{p}{q})| = \frac{|\sum_i a_i p^i q^{n-i}|}{q^n} \geq \frac{1}{q^n}. \tag{6.10}$$

另一方面，由微分中值定理我们得到

$$f(\tfrac{p}{q}) = f(\tfrac{p}{q}) - f(\alpha) = \left(\frac{p}{q} - \alpha\right) f'(\eta).$$

所以，我们得到

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f(\frac{p}{q})}{f'(\eta)}\right| > \frac{1}{Mq^n}.$$

所以，对任一$\epsilon > 0$及$A > 0$只有有限个q满足

$$\frac{1}{Mq^n} < \frac{A}{q^{n+\epsilon}}.$$

进一步分析(6.10)，重复上面的推导，可以得到p也只能有有限个。定理得证。

推论6.1. 如果$a_1, a_2, \cdots$ 是满足$|a_i| = 1$的一个数列, 那么

$$\gamma = \sum_{i=1}^{\infty} \frac{a_i}{10^{i!}}$$

为一个超越数.

证明. 命

$$\alpha_n = \sum_{i=1}^{n} \frac{a_i}{10^{i!}} = \frac{p}{q}, \quad q = 10^{n!}.$$

容易导出, 对所有的n均有

$$0 < \left|\gamma - \frac{p}{q}\right| \leq \sum_{i=n+1}^{\infty} \frac{1}{10^{i!}} < \frac{2}{10^{(n+1)!}} = \frac{2}{q^{n+1}}.$$

所以，根据Liouville定理，γ一定是一个超越数。

练习6.1. 如果α是一个首项系数为1的整系数多项式的根，那么它一定是一个整数或无理数。

练习6.2. 试证：所有的实代数数构成的集合是一个可数集，从而导出实超越数构成的集合不可数。

分析. 1、首先，一次代数数（有理数）是可数的。

2、 二次整系数多项式是可数的，所以二次代数数是可数的。

3、 n次整系数多项式是可数的，所以n次代数数是可数的。

根据可数集合的性质，我们得到所有的代数数构成的集合是可数的。因为实数集合是不可数的，所以实超越数构成的集合不可数。

定理6.9. 若α 是一个非有理的代数数. 那么对任一$\epsilon > 0$, 适合不等式

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\epsilon}}$$

的有理数解$\frac{x}{y}$的个数是有限的.

注6.8. 这就是著名的Roth定理, 有时也被称为Thue-Siegel-Dyson-Roth定理. 由于这一工作, Roth 获得了1958年的Fields奖. Siegel 是这样评价Roth的这一工作的： **只要数学还存在, 人们就该记住这一工作.** 后来, Schmidt将Roth定理推广到联立逼近的形式.

注6.9. 在Roth的工作之前，Thue, Siegel和Dyson曾先后将Liouville定理中的n改进为$\frac{1}{2}n+1$, $\min\limits_{1\le s\le n-1}(s+\frac{n}{s+1})$ 和$\sqrt{2n}$。但人们普遍认为最佳下界应该与n有关。

定理6.9. 设$n \geq 3$,

$$f(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i$$

为一不可约整系数齐次多项式,

$$g(x,y) = \sum_{i+j \leq n-3} g_{ij} x^i y^j$$

为一有理多项式. 那么, 方程

$$f(x,y) = g(x,y) \tag{6.11}$$

最多有有限对整数解(x,y).

证明. 不失一般性，我们假设$|x| \le y$，假定$\alpha_1, \alpha_2, \ldots, \alpha_n$ 是方程

$$f(x,1) = 0$$

的n个根，并记

$$G = \max\{|g_{ij}| : i + j \le n - 3\}.$$

这时，由方程(6.11)我们得到

$$a_0(x - \alpha_1 y)(x - \alpha_2 y) \cdots (x - \alpha_n y) \le n^2 G y^{n-3}. \tag{6.12}$$

所以，必有一个适当的下指标v使得

$$|x - \alpha_v y| < c_1 y^{1-\frac{3}{n}}.$$

c_i均表示正常数。这时，对任一$u \ne v,$ 当y足够大时$(\ge c_2)$我们得到

$$|x - \alpha_u y| = |(\alpha_v - \alpha_u)y + (x - \alpha_v y)| > c_3 y - c_1 y^{1-\frac{3}{n}} > c_4 y. \tag{6.13}$$

所以，由(6.12)和(6.13)我们得到

$$|x - \alpha_v y| < \frac{c_5}{y^2}$$

亦即

$$\left|\alpha_v - \frac{x}{y}\right| < \frac{c_5}{y^3}.$$

由Roth定理我们知道上式仅有有限多组解。定理得证。

第七章. 超越数

§1. 超越数的存在性

如定义6.1 所说, 如果α是某一有理多项式的根我们就称其为一个代数数； 否则就称其为一超越数.

定理7.1. 所有的代数数所构成的集合是可数的.

证明要点. 对任给的一个正整数n, 所有的n次有理多项式所构成的集合是可 数的. 所以, 所有的n次代数数构成的集合是一个可数集合. 根据集

合论的基本定理, 可数个可数集合的并集合仍然 是一个可数集合. 所以, 所有的代数数构成的集合是一个可数集合.

反过来, 我们知道实数集合时不可数的. 所以, 超越数集合是不可数的.

推论7.1. 所有的超越数所构成的集合是不可数的.

注7.1. 虽然具有不可数的超越数, 我们却很难判定某一给定的数是超越数, 例如$\sin 1$, π和e. 直到今天我们仍不知道$\pi + e$ 和Euler常数

$$\gamma = \lim_{n\to\infty} \left(\sum_{i=1}^{n} \frac{1}{i} - \log n \right)$$

是否为超越数.

§2. 某些数的超越性

定理7.3. π 和e都是无理数.

基本想法 e**.**

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = \alpha_n + \beta_n,$$

$$\alpha_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!},$$

$$\beta_n = \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}.$$

那么

$$\begin{aligned}(-1)^{n+1}\beta_n &= \frac{1}{(n+1)!}-\frac{1}{(n+2)!}+\cdots\\ &< \frac{1}{(n+1)!}\end{aligned}$$

所以

$$0<n!\beta_n(-1)^{n+1}<\frac{1}{n+1}$$

也就是

$$\{n!e^{-1}\}=\{n!\beta_n(-1)^{n+1}\}\neq 0.$$

基本想法 π**.** 若$\pi = b/a$, 令

$$f(x) = \frac{x^n(b-ax)^n}{n!}$$

及

$$\begin{aligned} F(x) \ &= \ f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots \\ &\quad +(-1)^n f^{(2n)}(x). \end{aligned}$$

可以验证$f(x)$及其导数当$x = 0$和π时均为整数. 即$F(0)$和$F(\pi)$均为整数. 因为

$$\begin{aligned} &(F'(x)\sin x - F(x)\cos x)' \\ &= (F"(x) + F(x))\sin x = f(x)\sin x \end{aligned}$$

所以

$$\int_0^\pi f(x)\sin x dx = F(\pi) - F(0)$$

是一整数. 但是当$0 < x < \pi$及n充分大时有

$$0 < f(x)\sin x < \frac{\pi^n b^n}{n!} < \frac{1}{\pi},$$

$$0 < \int_0^\pi f(x)\sin x dx < 1$$

得出矛盾. 定理证毕。

定理7.4 (Hermite). e**是超越数.**

证明. 如果$f(x)$是一个 m次实多项式并且定义

$$I(t) = \int_0^t e^{t-u} f(u) du,$$

其中t是一个复数，且积分沿线段从 0积到t。由分部积分我们可以得到

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t). \tag{7.1}$$

用$\overline{f}(x)$ 表示f的各项系数取绝对值，那么

$$|I(t)| \leq \int_0^t |e^{t-u} f(u)| du \leq |t| e^{|t|} \overline{f}(|t|). \tag{7.2}$$

假设e是一个代数数且满足

$$q_0 + q_1 e + \cdots + q_n e^n = 0. \tag{7.3}$$

我们将对

$$J = q_0 I(0) + q_1 I(1) + \cdots + q_n I(n)$$

取得矛盾,其中$I(t)$中的f按如下定义

$$f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p,$$

p为一个大素数。由 (7.1)和 (7.3)，我们得到

$$J = -\sum_{j=0}^{m} \sum_{k=0}^{n} q_k f^{(j)}(k),$$

其中$m = (n+1)p - 1$.

由于

$$f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p,$$

容易验证，如果$j < p,\ k > 0$或者$j < p-1,\ k = 0$，我们有 $f^{(j)}(k) = 0.$ 所以，除非$j = p-1$，$k = 0$，我们都有 $f^{(j)}(k)$是一个能被 $p!$整除的整数。更进一步，我们得到

$$f^{(p-1)}(0) = (p-1)!(-1)^{np}(n!)^p.$$

所以,如果$p > n,$ 那么$f^{(p-1)}(0)$能被$(p-1)!$整除,但不能被 $p!$整除. 这样我们得到,如果 $p > |q_0|$,那么 J是一个能被 $(p-1)!$整除的非零整数, 所以

$$|J| \geq (p-1)!. \tag{7.4}$$

另一方面,由于$\overline{f}(k) \leq (2n)^m$ 以及(7.2),我们得到

$$|J| \leq |q_1|e\overline{f}(1) + \cdots + |q_n|ne^n\overline{f}(n) \leq c^p$$

其中c与p无关, 与（7.4）矛盾。定理证毕。

定理7.4* (Lindemann). π是超越数。

证明. 假设π是一个代数数，那么 $\theta = i\pi$也是一个代数数。假设 θ的次数为 d，记 $\theta_1\ (=\theta), \theta_2, \ldots, \theta_d$为与$\theta$相伴的代数数， 记$l$为 θ的极小多项式的（正）首项系数。 由欧拉恒等式$e^{i\pi} = -1$，我们得到

$$\prod_{i=1}^{d}(1 + e^{\theta_i}) = 0.$$

显然，这一乘积可以表达为2^d项形如e^{Θ}的和，其中

$$\Theta = \sum_{i=1}^{d} \epsilon_i \theta_i, \qquad \epsilon_i = 0, 1.$$

假设，其中恰好有n项非零，记为$\alpha_1, \alpha_2, \ldots, \alpha_n$。我们得到

$$q + \sum_{i=1}^{n} e^{\alpha_i} = 0, \tag{7.5}$$

其中$q = 2^d - n > 0$.

假设p是一个大素数，我们定义

$$f(x) = l^{np} x^{p-1} (x - \alpha_1)^p \ldots (x - \alpha_n)^p,$$

$$I(t) = \int_0^t e^{t-u} f(u) du$$

以及

$$J = \sum_{i=1}^{n} I(\alpha_i).$$

我们将通过估计J得到矛盾。

类似于e的情况，当J展开成二重和时，关于 k指标的和是关于 $l\alpha_1$, ..., $l\alpha_n$的一个整系数对称多项式，进而可以导出它是一个整数。

容易验证（**请按照e的情况补充完整**），当 $j < p$时$f^{(j)}(\alpha_k) = 0$。另外，对所有$j \neq p-1$， $f^{(j)}(0)$是一个能被 $p!$ 整除的整数，并且

$$f^{(p-1)}(0) = (p-1)!(-l)^{np}(\alpha_1 \dots \alpha_n)^p.$$

显然,$f^{(p-1)}(0)$能被$(p-1)!$整除,但不能被 $p!$整除。所以，如果$p > q$，我们有

$$|J| \geq (p-1)!. \tag{7.6}$$

但是，由(7.2)我们可以得到

$$|J| \leq \sum_{i=1}^{n} |\alpha_i| e^{|\alpha_i|} \overline{f}(|\alpha_i|) \leq c^p.$$

显然，它与（7.6）相矛盾。定理证毕。

Hilbert第七问题： 若α是一个非0非1的代数数, β 是一个非有理数的代数数. 那么是否 α^β一定是一个代数数？做为特例, 是否能证明$2^{\sqrt{2}}$及$e^\pi = (-1)^{-i}$是超越数？

注7.5. 1929年, Gelfond首先证明了e^π的超越性. 一年以后, Linik证明了$2^{\sqrt{2}}$的超越性. 在1934, Gelfond和Schneider独立解决了这一问题. 后来, Baker证明了如下定理并由此而获得了Fields奖.

定理7.5. 1. 若$\alpha_1, \cdots, \alpha_n, \beta_0, \beta_1, \cdots, \beta_n$ 为一组 非零代数数, 那么$e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$为一超越数.

2. 若$\alpha_1, \cdots, \alpha_n$为一组非 0非 1的代数数, $\beta_1, \cdots, \beta_n$为一组与1在有理数域上线性无关的代数数. 那么$\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$是一个超越数.

注7.6. 超越数论是一个深奥的领域, 其中不乏一流的问题. 例如$e+\pi$是否为 一个超越数？Euler的γ常数是否为一超越数？事实上, 我们都不知道γ是否为一无理数？

练习7.1. 推广推论7.2, 构造出更多的超越数.

第八章. 数的几何

基本问题. 假设

$$F(\mathbf{x}) = \sum_{1 \le i,j \le n} c_{ij} x_i x_j$$

是一个n变元的整系数正定二次型。研究刻画

$$m(F) = \min_{\mathbf{z} \in Z^n \setminus \mathbf{o}} F(\mathbf{z})$$

和

$$k(F) = \sharp\{\mathbf{z} : F(\mathbf{z}) = m(F)\}.$$

§1. Minkowski基本定理

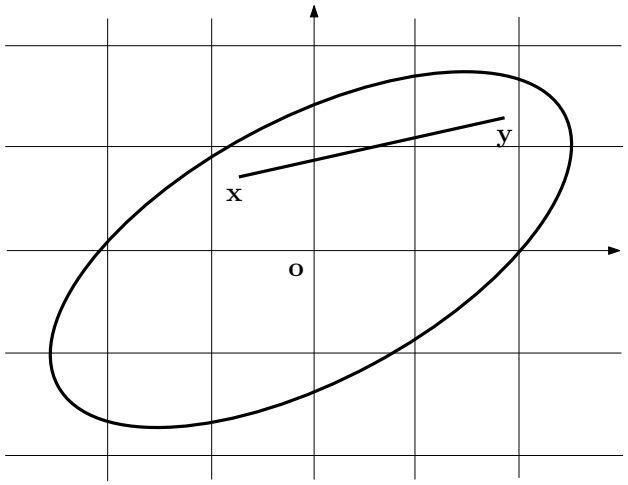
定义8.1. 我们称n维欧氏空间的一个子集 C为一个中心对称的凸体如果它满足

1). 若$\mathbf{x} \in C$, 则 $-\mathbf{x} \in C$;

2). 若$\mathbf{x}, \mathbf{y} \in C$和$0 \leq \lambda \leq 1$, 那么

$$\lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in C.$$

3). C是一个紧集.



例8.1. 可以验证单位球

$$B^n = \left\{ \mathbf{x} : \left(\sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}} \leq 1 \right\}$$

和单位立方体

$$I^n = \left\{ \mathbf{x} : |x_i| \leq \tfrac{1}{2} \right\}$$

都是中心对称凸体.

定理8.1 (Minkowski). C为一个n维的中心对称凸体. 如果

$$v(C) \geq 2^n,$$

那么它含有一个坐标全为整数且非原点的点.

证明要点. 用Z^n表示E^n中所有具有整数坐标的点构成的集合, 用C'表示C 的内部. 如果定理不成立, 那么

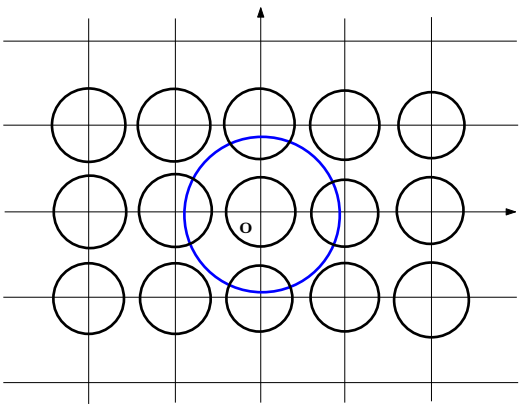
$$\left(\tfrac{1}{2}C' + \mathbf{z}_1\right) \cap \left(\tfrac{1}{2}C' + \mathbf{z}_2\right) = \emptyset.$$

也就是说, $\frac{1}{2}C + Z^n$在E^n中构成一个密度小于1的堆积. 所以,

$$\frac{v(\frac{1}{2}C)}{det(Z^n)} < 1,$$

$$v(C) = 2^n v(\tfrac{1}{2}C) < 2^n det(Z^n) = 2^n.$$

由此矛盾定理得证.



例8.1. 设α, β, γ 和 δ均为实数且定义

$$\xi = \alpha x + \beta y, \quad \eta = \gamma x + \delta y, \quad \Delta = \alpha\delta - \beta\gamma.$$

那么，

$$|\xi\eta| \leq \frac{1}{2}|\Delta|$$

一定有非零整数解。

证明. 显然，区域$A = \{(x, y) : \ |\xi\eta| \leq \frac{1}{2}|\Delta|\}$非凸。但是，由于

$$|\xi\eta| \leq \left(\frac{|\xi| + |\eta|}{2}\right)^2,$$

可以导出$B = \{(x, y) : \ |\xi| + |\eta| \leq (2|\Delta|)^{\frac{1}{2}}\}$ 是一个中心对称凸集并且$B \subset A$. 容易导出

$$area(B) = 4.$$

所以，由Minkowski定理可以得出B一定含有非零整点。

例8.2. 假设a_{ij} 是n^2个实数，且定义

$$\xi_j = \sum_{i=1}^{n} a_{ij}x_i, \quad j = 1, 2, \ldots, n,$$

$$\Delta = |a_{ij}| \neq 0, \quad J_n = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}.$$

那么，

$$\sum_{i=1}^{n} \xi_i^2 \leq 4\left(\frac{|\Delta|}{J_n}\right)^{\frac{2}{n}}$$

一定有非零整数解。

证明. 我们定义

$$E = \left\{(x_1, x_2, \ldots, x_n) : \sum_{i=1}^{n} \xi_i^2 \leq 4\left(\frac{|\Delta|}{J_n}\right)^{\frac{2}{n}}\right\}.$$

可以验证E是一个中心对称凸体，其实它是一个n维椭球。令

$$r = 2\left(\frac{|\Delta|}{J_n}\right)^{\frac{1}{n}}.$$

可以证明

$$\begin{aligned} v(E) &= \underset{\xi_1^2+\cdots+\xi_n^2\le r^2}{\int\cdots\int} dx_1\cdots dx_n = \underset{\xi_1^2+\cdots+\xi_n^2\le r^2}{\int\cdots\int} \left|\frac{\partial(x_1,\cdots,x_n)}{\partial(\xi_1,\cdots,\xi_n)}\right| d\xi_1\cdots d\xi_n \\ &= \frac{1}{|\Delta|}\underset{\xi_1^2+\cdots+\xi_n^2\le r^2}{\int\cdots\int} d\xi_1\cdots d\xi_n = \frac{1}{|\Delta|}J_n r^n = 2^n. \end{aligned}$$

由Minkowski定理可以得出E一定含有非零整点。

§2. Minkowski-Hlawka定理

定义8.2. $\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_n$为$n$维欧氏空间 中的一组线性无关的向量. 那么我们称

$$\Lambda = \left\{ \sum_{i=1}^{n} z_i \mathbf{a}_i : \ z_i \in Z \right\}$$

为一个n维格. 并称

$$P = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{a}_i : \ 0 \leq \lambda_i \leq 1 \right\}$$

为Λ的基本方体. 显然,

$$v(P) = det(a_{ij}).$$

定义8.3. 如果

$$(int(C)+\mathbf{u}_1)\cap(int(C)+\mathbf{u}_2)=\emptyset$$

对Λ的两个任意不相同的点都成立. 我们就称

$$C+\Lambda=\bigcup_{\mathbf{u}\in\Lambda}(C+\mathbf{u})$$

为一个格堆积. 这时, 我们称$v(C)/v(P)$为$C+\Lambda$的堆积密度, 并定义

$$\delta^*(C)=\max_{\Lambda}\frac{v(C)}{v(P)}.$$

注8.2. 如果将格换成一般的离散点集, 可类似地定义$\delta(C)$. 这也是一个非常重要的几何量. 另外，$\delta^*(B^n)$与正定二次型的$m(F)$和$det(C)$密切相关。

定理8.2. 对任意的n维中心对称凸体C, 我们有

$$\delta^*(C) \geq \frac{\zeta(n)}{2^{n-1}},$$

其中

$$\zeta(n) = \sum_{k=1}^{\infty} \frac{1}{k^n}$$

为Riemann-zeta函数.

注8.3. 这就是著名的Minkowski-Hlawka定理. 它首先是由 Minkowski 做为一个 猜想提出来的. 直到1941才由Hlawka用均值达的方法得以证明. 后来虽经 T. Schneider, Siegel, Rogers, Davenport, Schmidt等许多大数学家的多次该进, 但主项仍然没变.

§3. Newton-Gregory问题

Newton-Gregory问题: 一个球是否能跟13个内部互不相交的同样的球相接触?

注8.4. 这是Newton与Gregory在1696的一次辩论中提出的一个问题. Newton认为一个球最多只能与12个同样的球相接触; Gregory 则认为13是可能的. 直到1956年前后, 这一问题才由 Schutte, Van der Waerden 和 Leech 所解决. 一个球最多只能跟12个内部互不相交的同样的球相接触. 证明是初等但复杂的.

定义8.4. K是一个n维凸体. 假定K最多能与$m(K)$个内部互不相交的它的 平移体相接触. 我们称$m(K)$为K的Newton数.

定理8.3. 对任意的n维凸体K, 我们有

$$m(K) \leq 3^n - 1.$$

证明要点. A是一个任意给定的凸集合. 我们定义

$$D(A) = \{\mathbf{x} - \mathbf{y} : \ \mathbf{x}, \ \mathbf{y} \in A\}.$$

通常, $D(A)$被称为A的差集. 可以证明, $D(A)$总是一个中心对称的凸集, 并且

$$(A + \mathbf{u}) \cap (A + \mathbf{v}) = \emptyset$$

当且仅当

$$(\tfrac{1}{2}D(A) + \mathbf{u}) \cap (\tfrac{1}{2}D(A) + \mathbf{v}) = \emptyset.$$

所以我们不妨假定K是中心对称的, 且以坐标原点为中心.

假定$K+\mathbf{u}_i$, $i=1,2,\cdots,m(K)$, 与K在表面接触, 那么

$$K+\mathbf{u}_i \subset 3K.$$

由于它们内部互不相交, 我们有

$$((m(K)+1)v(K) \leq v(3K) = 3^n v(K).$$

所以

$$m(K) \leq 3^n - 1.$$

注8.5. 早在一个世纪以前, Minkowski利用同余式证明了: 在K的任一格堆积中它最多只能与3^n-1个相接触。 后来Hadwiger将Minkowski的结果推广到了以上定理的形式。

假设

$$F(\mathbf{x}) = \mathbf{x}C\mathbf{x}'$$

是一个n元正定二次型。则存在一个非奇异矩阵A使得

$$C = AA'.$$

定义

$$\Lambda = \{\mathbf{z}A : \ \mathbf{z} \in \mathbb{Z}^n\}.$$

显然，Λ是一个n维的格, 其中

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}), \quad i = 1, 2, \ldots, n$$

构成Λ的一组基。这时，我们看到

$$F(\mathbf{z}) = \mathbf{z}C\mathbf{z}' = \mathbf{z}AA'\mathbf{z}' = \langle \mathbf{z}A, \mathbf{z}A \rangle.$$

$\{F(\mathbf{z}) : \ \mathbf{z} \in \mathbb{Z}^n\}$ 即Λ的所有格点的自内积。

定义

$$m(F) = \min_{\mathbf{z} \in Z^n \setminus \mathbf{o}} F(\mathbf{z})$$

和

$$k(F) = \sharp\{\mathbf{z} : F(\mathbf{z}) = m(F)\}.$$

显然，$\sqrt{m(F)}$就是Λ的最短非零向量的长度。在Λ的每一个点放置一个以 $\frac{1}{2}\sqrt{m(F)}$为半径的球则构成一个球堆积。 这时，$k(F)$就是在上述球堆积中的牛顿数。

§4. 堆球的故事

在所有的凸体中, 毫无疑问单位球是最特殊的, 尤其是在与堆积有关的问题中. 为方便起见, 我们用 B^n表示n维单位球. 在研究n维单位球的Newton数和堆积密度的历史上, 最出人意外和最重要 的方法应该算是线性规划方法. 所谓的线性规划方法是指在一组线性不等式的限制下求某一函数的 极大或极小值. 在1975年前后, 由Delsarte等人证明了如下引理从而将球的Newton数和堆积密度与线性 规划方法密切地连了起来.

设α和β均为大于-1的给定实数。那么由

$$P_k^{\alpha,\beta}(x) = \frac{1}{2^k}\sum_{i=0}^{k}\binom{k+\alpha}{i}\binom{k+\beta}{k-i}(x+1)^i(x-1)^{k-i}$$

所定义的一系列函数被称为Jacobi多项式。这是一类非常重要的特殊多项式，有许多好的性质。1972 年，P. Delsarte发现 了如下结论：

Delsarte引理. 取$\alpha = (n-3)/2$并且定义

$$f(x) = \sum_{i=0}^{k} c_i P_i^{\alpha,\alpha}(x),$$

其中c_i均非负且$c_0 > 0$. 如果当$-1 \le x \le 1/2$时均有$f(x) \le 0$, 那么

$$m(B^n) \le \frac{f(1)}{c_0}.$$

1979年，Levenštein, Odlyzko和Sloane证明了下面的结论。其方法之精妙，结论之意外， 让几乎所有的专家都目瞪口呆。

定理 8.4 (Levenštein, Odlyzko, Sloane). 一个8维单位球能且仅能跟 240个单位球同时相切。换句话说

$$m(B^8) = 240.$$

注. 通过构造容易得到$m(B^8) \geq 240$. 关键是证明上界.

证明思路. 取$\alpha = (8-3)/2 = 2.5$,并且将$P_i^{\alpha,\alpha}(x)$简写为P_i. 定义

$$\begin{aligned} f(x) &= \tfrac{320}{3}(x+1)\left(x+\frac{1}{2}\right)^2 x^2\left(x-\frac{1}{2}\right) \\ &= P_0 + \frac{16}{7}P_1 + \frac{200}{63}P_2 + \frac{832}{231}P_3 \\ &\quad + \frac{1216}{429}P_4 + \frac{5120}{3003}P_5 + \frac{2560}{4641}P_6. \end{aligned}$$

可以验证$f(x)$满足Delsarte引理且$f(1) = 240$. 所以,

$$m(B^8) \leq \frac{f(1)}{c_0} = 240.$$

定理 8.5 (Levenštein, Odlyzko, Sloane). 一个24维单位球能且仅能跟 196560个单位球同时相切。换句话说

$$m(B^{24}) = 196560.$$

证明思路. 取$\alpha = (24-3)/2 = 10.5$,并且将$P_i^{\alpha,\alpha}(x)$简写为P_i. 定义

$$\begin{aligned} f(x) &= \tfrac{1490944}{15}(x+1)\left(x+\tfrac{1}{2}\right)^2\left(x-\tfrac{1}{16}\right)^2 x^2\left(x-\tfrac{1}{2}\right) \\ &= P_0 + \tfrac{48}{23}P_1 + \tfrac{1144}{425}P_2 + \tfrac{12992}{3825}P_3 + \tfrac{73888}{22185}P_4 \\ &\quad + \tfrac{2169856}{687735}P_5 + \tfrac{59062016}{25365285}P_6 + \tfrac{4472832}{2753575}P_7 \\ &\quad + \tfrac{23855104}{28956015}P_8 + \tfrac{7340032}{20376455}P_9 + \tfrac{7340032}{80848515}P_{10}. \end{aligned}$$

容易验证，$f(x)$满足Delsarte引理的全部条件且$f(1) = 196560$。所以，

$$m(B^{24}) \le f(1)/c_0 = 196560.$$

由Leech格的构造,我们知道$m(B^{24}) \ge 196560$. 所以, 我们得到

$$m(B^{24}) = 196560.$$

定理8.6 (Gauss, Hales, Cohn, ... Viazovska).

$$\delta(B^3) = \frac{\pi}{\sqrt{18}}$$

$$\delta(B^8) = \frac{\pi^4}{384}$$

$$\delta(B^{24}) = \frac{\pi^{12}}{12!}$$

定理8.7.

$$2^{0.2075n(1+o(1))} \leq m(B^n) \leq 2^{0.401n(1+o(1))}.$$

注8.7. 这一定理的下界部分是分别由Shannon和Wyner于1960年前后证明的. 假定 $B^n + \mathbf{u}_1, B^n + \mathbf{u}_2, \cdots, B^n + \mathbf{u}_{m(B^n)}$是$m(B^n)$个内部互 不相交且都与$B^n$相接触的单位球. 将这些球向$B^n$的表面做球面投影, 我们就得到了一组内部 互不相交的球冠. 比较这些球冠与单位球的面积就可导出以上下界. 上界是由Kabatjanski和Levenstein通过线性规划的方法得到的.

定理8.8.

$$2^{-n} \leq \delta(B^n) \leq 2^{-0.599n(1+o(1))}.$$

注8.8. 这一上界是由Kabatjanski和Levenstein通过利用Delsarte引理得到的. 通过与Minkowski-Hlawka定理做比较, 我们可以看出已知的关于$\delta(B^n)$的上下界之间的差别 是很大的.

问题8.1. 确定$m(B^n)$和$\delta(B^n)$的渐近公式.

注8.9. 这是数的几何中最核心的问题之一.

练习8.1. 若$\mathbf{y}_i = \sum_{j=1}^{n} a_{ij}x_j$, $i = 1, 2, \cdots, n$, 且

$$J_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)}.$$

那么总有一组不全为0的整数$x_1, x_2, \cdots, x_n$满足

$$\sum_{i=1}^{n} y_i^2 \leq 4(|A|/J_n)^{2/n}.$$

参考文献:

1. W. Scharlau & H. Opolka, *From Fermat to Minkowski*, Springer-Verlag, 1985.
2. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1954.
3. 华罗庚, 数论导引, 科学出版社, 1979.
4. A. Wiles, https://www.bilibili.com/video/BV1py4y1V7ba?from_spmid=666.9.0.0
5. 张益唐, https://v.qq.com/x/page/x0163z5gzjn.html