Sum of squares

Jiahai Wang

2024 年 9 月 1 日

Beauty is the first test:there is no permanment place in the world for ugly mathematics——G.H.Hardy

目录

Chapter 0

Introduction

本笔记旨在探讨数论中平方和相关的经典定理。我们从初等数论入手，首先回顾费马两平方和定理和拉格朗日四平方和定理，这些定理在数论的历史上占据了重要位置，揭示了整数与平方和之间的深刻联系。

笔记从这些初等结果出发，揭示这些更为深奥的理论是如何从平方和问题的研究中逐步发展出来的。通过引入 Jacobi theta 函数和自守形式等工具，我们将看到这些经典问题如何在更为抽象的数学框架下得到统一的理解。

在整个笔记中，我们将以逐步加深的方式介绍平方和问题的不同方面，从初等的二平方和和三平方和问题，到最终的四平方和问题，再到更高维度的平方和问题。

Chapter 1

初探平方和

本章尽量用初等的证明，展示平方和的一些经典定理

1.1 二平方和

Theorem 1.1 (费马二平方和定理)**.** 一个奇素数 p 可以表示为两个平方数之和，当且仅当 $p \equiv 1 \pmod 4$。

这小节都是大家熟知的理论，略过

1.2 三平方和

三平方和在数学结构上缺乏某种对称性或统一性。比如，四平方和可以通过二次型理论和模形式理论自然地处理，而三平方和的问题并没有同样简单或广泛的理论框架支撑。我们用一个定理来说明三平方和研究价值的局限性。Serre 在 gtm7 中用二次型理论给出了这个证明

Theorem 1.2 (Legendre 1798)**.** 正整数 n 不能表示成三平方和的充要条件是，n 可以表示为 $4^a(8b+7)$ 的形式，其中 a, b 为任意非负整数。

证明. 对任意整数 x 有

$$x^2 \equiv 0, 1 \text{ 或} 4 (\mathrm{mod}\, 8).$$

因此，对任意整数 x_1, x_2, x_3 必有

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 7 (\mathrm{mod}\, 8).$$

由此推出，n 是形如 $8k+7$ 的正整数时不能表为三个整数的平方和，即

定理当 $\alpha = 0$ 时成立. 假设定理当 $\alpha = l (l \geqslant 0)$ 时成立. 当 $\alpha = l + 1$ 时，

若有 $n = 4^{l+1}(8k_1 + 7)$ 可表示为

$$n = 4^{l+1}(8k_1 + 7) = x_1^2 + x_2^2 + x_3^2,$$

则必有 $x_1^2 + x_2^2 + x_3^2 \equiv 0$ 或 $4(\mathrm{mod}\ 8)$, 进而推出

$$x_1 \equiv x_2 \equiv x_3 \equiv 0(\mathrm{mod}\, 2).$$

所以有

$$4^1(8k_1 + 7) = (x_1/2)^2 + (x_2/2)^2 + (x_3/2)^2.$$

但这和归纳假设矛盾，所以定理对 $\alpha = l + 1$ 也成立 □

由定理立即推出下面定理中的 “四” 是最佳结果. 由于 8k+7 形式的素数有无穷多个 (Dirichlet theorem)

1.3 四平方和

Theorem 1.3. 每个正整数均可表示为四个整数的平方和

证明. 这个证明可以分成两块来考虑，只需要一点点注意力可以直接验证如下恒等式

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

其中

$$\begin{cases} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ z_2 = x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3, \\ z_3 = x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2, \\ z_4 = x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2. \end{cases}$$

由于 1 与 2 都明显满足这个定理，那么只需要考虑大于 2 的正整数。而这些正整数都可以分解成素数的乘积，因此，只需要证明该定理对所有的素数成立，则使用以上恒等式就可以得到最终的结论。

至此第一块结束证明现假设 p 是一个奇素数。由于 $\{a^2 : a \in \{0, 1, \cdots, (p-1)/2\}\}$ 里面有 $(p+1)/2$ 个不同的同余类，$\{-b^2 - 1 : b \in \{0, 1, \cdots, (p-1)/2\}\}$ 里面也有 $(p+1)/2$ 个不同的同余类，但是素数 p 的同余类只有 p 个，因此存在正整数 $a, b \in \{0, 1, \cdots, (p-1)/2\}$ 满足 $a^2 \equiv -b^2 - 1 \pmod{p}$。也就是说 $a^2 + b^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$。令 $n \in \mathbb{Z}$ 满足 $np = a^2 + b^2 + 1$，则有 $p \le np \le \frac{2(p-1)^2}{4} + 1 < p^2$。于是，$1 \le n < p$。

因此存在一个 $1 \le n < p$ 使得 $np = a^2 + b^2 + 1^2 + 0^2$ 是四个整数的平方和。于是必定存在一个最小的正整数 m 使得 $1 \le m \le n < p$ 使得 mp 为四个整数的平方和，不妨设为 $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$。

下面证明 $m = 1$。反证法，假设 $1 < m \leq n < p$ 成立。令 $y_i = x_i \pmod m$ 对于 $i \in \{1, 2, 3, 4\}$ 成立，并且 $-\frac{m}{2} < y_i \leq \frac{m}{2}$。因此，$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv (x_1^2 + x_2^2 + x_3^2 + x_4^2) \equiv mp \equiv 0 \pmod m$。令 $mr = y_1^2 + y_2^2 + y_3^2 + y_4^2$。因此，$mr \leq 4\left(\frac{m}{2}\right)^2 = m^2$。

如果 $r = m$，通过以上不等式得知 $r = m$ 等价于 $y_i = \frac{m}{2}$ 对于 $i \in \{1, 2, 3, 4\}$ 都成立。此时，$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4\left(\frac{m}{2}\right)^2 \equiv 0 \pmod{m^2}$。因此，$p$ 是 m 的倍数，这与 p 是素数，$m > 1$ 矛盾。所以，$r < m$ 成立。即 $1 \leq r < m \leq n < p$ 成立。

进一步地，$(mp)\cdot(mr) = (x_1^2+x_2^2+x_3^2+x_4^2)\cdot(y_1^2+y_2^2+y_3^2+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2$，这里的 z_i 正如恒等式里面所定义的。由于 $y_i \equiv x_i \pmod m$ 并且 $\sum_{i=1}^4 x_i^2 \equiv 0 \pmod m$。因此，对所有 $i \in \{1, 2, 3, 4\}$ 有 $z_i \equiv 0 \pmod m$。所以，对所有 $i \in \{1, 2, 3, 4\}$ 有 $z_i = w_i m$，其中 $w_i \in \mathbb{Z}$。由等式 $(mp) \cdot (mr) = \sum_{i=1}^4 z_i^2$，我们得到 $pr = \sum_{i=1}^4 w_i^2$。然而，由于 $1 \leq r < m$，这与 m 的极小性假设相矛盾。

$m = 1$ 证明完成! □

Chapter 2

从 Jacobi theta 到平方和问题

Definition 2.1. $\mathrm{r}_k(n) = \#\{(n_1, \cdots, n_k) \in \mathbb{Z}^k | n_1^2 + \cdots + n_k^2 = n\}$. 这是将 n 表示成 k 个平方和的方法的总个数 (算上符号), 利用 ϑ 级数

$$\vartheta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z} = \sum_{n=-\infty}^{\infty} q^{\frac{n^2}{2}} \quad (q = e^{2\pi i z}),$$

则因为

$$\begin{aligned}
\vartheta(z)^k &= \left(\sum_{n=-\infty}^{\infty} q^{\frac{n^2}{2}} \right)^k \\
&= \left(\sum_{n_1=-\infty}^{\infty} q^{\frac{n_1^2}{2}} \right) \cdots \left(\sum_{n_k=-\infty}^{\infty} q^{\frac{n_k^2}{2}} \right) \\
&= \sum_{n_1, \cdots, n_k = -\infty}^{\infty} q^{\frac{n_1^2 + \cdots + n_k^2}{2}} \\
&= \sum_{n=0}^{\infty} r_k(n) q^{\frac{n_2^2}{2}},
\end{aligned}$$

于是, 求 $r_k(n)$ 的问题变成了求权 $\frac{k}{2}$ 的自守形式 $\vartheta(z)^k$(2 级) 的表示问题了

2.1 二平方和

$k = 2$ 的情形, 由 Dedekind ζ 的计算

$$\zeta_{\mathbb{Q}(\sqrt{-1})}(s) = \zeta(s) L(s, \chi_{-1})$$

知道有

$$r_2(n) = 4 \sum_{\substack{d|n \\ d:\text{奇數}}} \chi_{-1}(d) = 4 \sum_{\substack{d|n \\ d:\text{奇數}}} (-1)^{\frac{d-1}{2}}.$$

注意，这个关系式可写为

$$\vartheta(z)^2=\left(\sum_{n=-\infty}^{\infty}q^{\frac{n^2}{2}}\right)^2=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\frac{q^{(2m-1)/2}}{1-q^{(2m-1)/2}}.$$

这是个 “ϑ 级数 =Eisenstein 级数” 的等式. 实际上，我们有

$$\begin{aligned}\left(\sum_{n=-\infty}^{\infty}q^{n^2/2}\right)^2&=1+\sum_{n=1}^{\infty}r_2(n)q^{n/2}\\&=1+4\sum_{n=1}^{\infty}\left(\sum_{d|n}(-1)^{\frac{d-1}{2}}\right)q^{n/2}\\&=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\sum_{n=1}^{\infty}q^{(2m-1)n/2}\\&=1+4\sum_{m=1}^{\infty}(-1)^{m-1}\frac{q^{(2m-1)/2}}{1-q^{(2m-1)/2}}.\end{aligned}$$

2.2 四平方和

Theorem 2.2 (Jocabi)**.**

注：这是最重要的定理，有多种角度的证明，下面给出椭圆函数论的一种组合证明，此证明较为初等（模形式的证明可以参考 stein 《complex analysis》或李文威《模形式》，后者更加深刻）

Lemma 2.3 (jocabi 三重积)**.** $\prod_{n=1}^{\infty}(1+aq^{2n-1})(1+a^{-1}q^{2n-1})(1-q^{2n})=\sum_{n=-\infty}^{\infty}a^nq^{n^2}(*)$

证明. 把引理中 a 换成 $-a^2q$，再把 q^2 换成 q，两边再乘 a，可得

$$(a-a^{-1})\prod_{n=1}^{\infty}(1-a^2q^n)(1-a^{-2}q^n)(1-q^n)=\sum_{n=-\infty}^{\infty}(-1)^na^{2n+1}q^{n(n+1)/2}$$

对 a 求导，再令 $a=1$，然后两边除以 2，得

$$\prod_{n=1}^{\infty}(1-q^n)^3=\frac{1}{2}\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)q^{n(n+1)/2}$$

两边平方得

$$\prod_{n=1}^{\infty}(1-q^n)^6=\frac{1}{4}\sum_{m,n=-\infty}^{\infty}(-1)^{m+n}(2m+1)(2n+1)q^{(m(m+1)+n(n+1))/2}$$

$$=\frac{1}{4}\left(\sum_{2|m-n}(2m+1)(2n+1)q^{(m(m+1)+n(n+1))/2}-\sum_{2\nmid m-n}(2m+1)(2n+1)q^{(m(m+1)+n(n+1))/2}\right)$$

在第一个和式中令 $(m,n)=(r+s,r-s)$，在第二个和式中令 $(m,n)=(s+r,s-r-1)$，得

$$\prod_{n=1}^{\infty}(1-q^n)^6=\frac{1}{2}\sum_{r,s=-\infty}^{\infty}\left((2r+1)^2-(2s)^2\right)q^{r(r+1)+s^2}$$

$$=\frac{1}{2}\left(\sum_{s=-\infty}^{\infty}q^{s^2}\sum_{r=-\infty}^{\infty}(2r+1)^2q^{r(r+1)}-\sum_{r=-\infty}^{\infty}q^{r(r+1)}\sum_{s=-\infty}^{\infty}(2s)^2q^{s^2}\right)$$

$$=\frac{1}{2}\left(\sum_{s=-\infty}^{\infty}q^{s^2}\left(1+4q\frac{\mathrm{d}}{\mathrm{d}q}\right)\sum_{r=-\infty}^{\infty}q^{r(r+1)}-\sum_{r=-\infty}^{\infty}q^{r(r+1)}\left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right)\sum_{s=-\infty}^{\infty}q^{s^2}\right)$$

再次应用恒等式 (*) 得

$$\prod_{n=1}^{\infty}(1-q^n)^6=\frac{1}{2}\left(\prod_{n=1}^{\infty}(1+q^{2n-1})^2(1-q^{2n})\cdot\left(1+4q\frac{\mathrm{d}}{\mathrm{d}q}\right)2\prod_{n=1}^{\infty}(1+q^{2n})^2(1-q^{2n})\right.$$

$$\left.-2\prod_{n=1}^{\infty}(1+q^{2n})^2(1-q^{2n})\cdot\left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right)\prod_{n=1}^{\infty}(1+q^{2n-1})^2(1-q^{2n})\right)$$

$$=\prod_{n=1}^{\infty}(1+q^{2n-1})^2(1+q^{2n})^2(1-q^{2n})^2\cdot\left(1-8\sum_{n=1}^{\infty}\left(\frac{(2n-1)q^{2n-1}}{1+q^{2n-1}}-\frac{2nq^{2n}}{1+q^{2n}}\right)\right)$$

两边除等式右边的乘积，得

$$\prod_{n=1}^{\infty}\left(\frac{1-q^n}{1+q^n}\right)^4=1-8\sum_{n=1}^{\infty}\left(\frac{(2n-1)q^{2n-1}}{1+q^{2n-1}}-\frac{2nq^{2n}}{1+q^{2n}}\right)$$

由恒等式 (*) 可得

$$\sum_{n=-\infty}^{\infty}(-1)^nq^{n^2}=\prod_{n=1}^{\infty}(1-q^{2n})(1-q^{2n-1})^2=\prod_{n=1}^{\infty}(1-q^{2n})\prod_{n=1}^{\infty}\frac{(1-q^n)^2}{(1-q^{2n})^2}$$

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

四次方后再把 q 换成 $-q$，得

$$\left(\sum_{n=-\infty}^{\infty}q^{n^2}\right)^4=1+8\sum_{n=1}^{\infty}\left(\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}}+\frac{2nq^{2n}}{1+q^{2n}}\right)$$

$$=1+8\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}-8\sum_{n=1}^{\infty}\left(\frac{2nq^{2n}}{1-q^{2n}}-\frac{2nq^{2n}}{1+q^{2n}}\right)$$

$$=1+8\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}-8\sum_{n=1}^{\infty}\frac{4nq^{4n}}{1-q^{4n}}=1+8\sum_{n\geq1,4\nmid n}\frac{nq^n}{1-q^n}$$

把右边的 $(1-q^n)^{-1}$ 展开成级数，再比较系数，可得把 n 表示成四平方和的方法数是 $8\sum_{4\nmid d,\, d|n} d$。

□

2.3 八平方和

建议读者自行思考后再看

对于 $\theta(\tau)^8 = \sum_{n\geq 0} r_8(n)q^n \in M_4(\Gamma_0(4))$，算出 $\dim_{\mathbb{C}} M_4(\Gamma_0(4)) = 3$ 和 Eisenstein 级数

$$\mathscr{G}_4 := \frac{E_4}{240} = \frac{1}{240} + \sum_{n\geq 1} \sigma_3(n)q^n$$

如法炮制, 可得

$$\theta(\tau)^8 = 16\mathscr{G}_4(\tau) - 32\mathscr{G}_4(2\tau) + 256\mathscr{G}_4(4\tau),$$

$$r_8(n) = 16\sum_{d|n}(-1)^{n-d}d^3.$$

参考文献

[1] Gtm7

[2] GTM164

[3] 数论 I–Fermat 的梦想和类域论Ⓕ川信重，栗原将人，Ⓕ藤毅

[4] 数论 II——岩澤理論と保型形式Ⓕ川信重，栗原将人，Ⓕ藤毅