平方和问题（Sum of squares problem)

作者： Jiahai Wang

时间： November 27, 2024

目录

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。补充了三平方和定理，这些是为我们之后讨论 $Waring's\ problem$ 做铺垫

之后从笔记的这些初等结果出发，看到之后更为深刻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。

第 1 章 经典平方和

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

定理 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 $p\equiv 1 \pmod 4$。

首先，这个命题的必要性是显然的（组合性质决定）。**这个定理的证明有很多，一些奇奇怪怪的证明放在附录。下面是第一种初等证明**

证明 $\exists a\in\mathbb{Z}$ 满足 $a^2\equiv -1\pmod p$. 考察形如 $as+t$ 的 $\left(\lfloor\sqrt{p}\rfloor+1\right)^2$ 个整数，其中 $0\le s,t\le\sqrt{p}, s,t\in\mathbb{Z}$. 根据鸽笼原理，必有两个数模 p 同余，设 $as_1+t_1\equiv as_2+t_2\pmod p$. 记 $x=|s_1-s_2|, y=|t_1-t_2|$，则 $1\le x,y\le\lfloor\sqrt{p}\rfloor$，且 $a^2x^2\equiv y^2\pmod p$，于是 $x^2+y^2\equiv 0\pmod p$. 而 $2\le x^2+y^2\le 2\lfloor\sqrt{p}\rfloor^2<2p$，故 $x^2+y^2=p$.

另一边，它的证明核心是一个**无穷递降 (infinite descent)** 的过程。为实现这一过程，我们先证明一个引理：

引理 1.1

如果 N 可以写成两个互素整数的平方和的形式，q 是 N 的一个素因子，同时它也可以写成 $q=x^2+y^2$ 的形式，则 $\frac{N}{q}$ 也可以写成互素整数的平方和的形式。

证明 设 $N=a^2+b^2$，其中 $(a,b)=1$。由于 $q=x^2+y^2$ 且 $q\mid N$，于是

$$q\mid x^2N-a^2q=x^2(a^2+b^2)-a^2(x^2+y^2)=(bx+ay)(bx-ay)$$

由于 q 是一个素数，不妨设 $q\mid bx-ay$，于是可以设

$$bx-ay=dq$$

注意到

$$x\mid (a+dy)y=ay+dy^2=bx-dq+dy^2=x(b-xd)$$

且 x,y 是互素的，于是

$$x\mid a+dy$$

记 $a+dy=cx$，则

$$bx=ay+d(x^2+y^2)=y(a+dy)+dx^2=cxy+dx^2,\quad b=cy+dx.$$

则

$$\begin{cases}a=cx-dy,\\ b=dx+cy.\end{cases}$$

于是

$$N=a^2+b^2=(cx-dy)^2+(cy+dx)^2=(c^2+d^2)(x^2+y^2)=q(c^2+d^2).$$

于是 $\frac{N}{q}$ 可以写成两个整数的平方和的形式。由于 $(a,b)=1$，于是 $(c,d)=1$。因此我们就说明了 $\frac{N}{q}$ 可以写成两个互素整数的平方和的形式。

定理 1.2 (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 $p\equiv 1 \pmod 4$。

证明

设 p 为 $N=a^2+b^2$ 的一个素因子。将 a,b 对 p 进行带余除法，设

$$a=mp\pm a',\quad b=np\pm b'$$

易得 $p\mid a'^2+b'^2$。由于 a' 与 b' 可能不是互素的，于是同时除以它们的最大公因数 $d=(a',b')$，显然 $p\nmid d$，于是

$$p\mid \left(\frac{a'}{d}\right)^2+\left(\frac{b'}{d}\right)^2$$

因此我们不妨在一开始假设 $|a|<\frac{p}{2},|b|<\frac{p}{2}$。

于是

$$N=a^2+b^2<\frac{p^2}{2}$$

由此 p 是 N 最大的一个素因子。若 q 为 N 异于 p 的一个素因子且能够写成两个整数平方和的形式，则由引理 1 我们可知 $\frac{N}{q}$ 也可以写成互素整数的平方和形式。如果对于 N 的所有异于 p 的素因子均能够写成两个整数平方和的形式，则不断利用引理 1 我们可知 p 也能写成两个整数平方和的形式。

假设 p 无法写成两个整数平方和的形式，则由上述分析可得必存在 N 的素因子 $q<p$ 使得 q 也无法写成两个整数平方和的形式。这就导致了一串严格递减的素数序列 $\{q_n\}$，它们都无法写成两个整数平方和的形式，这引发了矛盾。

于是接下来我们只需找到 N 使其能够写成两个互素整数的平方和且它是 p 的倍数，就可以说明 p 能够写成两个整数的平方和 x^2+y^2 的形式了。

由于 $p\equiv 1\pmod 4$，于是记 $p=4k+1$，由费马小定理知：

$$(x^{2k}+1)(x^{2k}-1)=x^{4k}-1\equiv 0\pmod p$$

于是我们选定适当的 x 使得 $x^{2k}-1\not\equiv 0\pmod p$（这是可以做到的，因为 $x^{2k}-1$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中至多有 $2k<p-1$ 个解）。于是

$$p\mid x^{2k}+1$$

令

$$N=x^{2k}+1$$

这样我们就找到了满足要求的 N，也就证明了费马平方和定理。

如何表示 x^2+ny^2 的素因子？

我们引入勒让德符号 $\left(\frac{a}{p}\right)$，其中 a 为一个整数，p 为一个奇素数，具体定义如下：

$$\left(\frac{a}{p}\right)=\begin{cases}0 & p\mid a,\\ 1 & p\nmid a\text{ 且}a\text{ 为}p\text{ 的二次剩余},\\ -1 & p\nmid a\text{ 且}a\text{ 不为}p\text{ 的二次剩余}.\end{cases}$$

这样我们就可以通过下列的引理给出 x^2+ny^2 的素因子需要满足的条件。

定理 1.3

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

定理 1.4

设 n 是一个非零整数，而 p 是一个奇素数且不整除 n，则

$$p \mid x^2+ny^2,(x,y)=1 \Leftrightarrow \left(\frac{-n}{p}\right)=1 \tag{1.1}$$

♡

这一块算类域论，简单说明一下，详细理论见互反率

证明 必要性：若 $x^2+ny^2\equiv 0 \pmod p$ 且 $(x,y)=1$，于是 p 必然不整除 y，否则将推出 p 将是 x,y 的公因子。于是存在 $y^*\in\mathbb{Z}$ 使得

$$y^*y\equiv 1 \pmod p,$$

因此

$$((xy^*)^2+n(y^*y)^2\equiv (xy^*)^2+n\equiv 0 \pmod p$$

$$(xy^*)^2\equiv -n \pmod p$$

因此 $-n$ 为 p 的二次剩余。于是

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

充分性：若 $\left(\frac{-n}{p}\right)=1$，则存在 $x\in\mathbb{Z}$，使得

$$x^2+n\equiv 0 \pmod p$$

因此令 $y=1$，知道充分性是成立的。

利用上述引理，我们想要寻找的确定 x^2+ny^2 素因子性质的命题就转化为："$p\equiv \alpha,\beta,\cdots \pmod{4n}$ 可以推出 $\left(\frac{-n}{p}\right)=1$"。

通过计算我们可以发现：

据此我们提出猜想：若 p 与 q 为不同的奇素数，则

$$\left(\frac{q}{p}\right)=1 \Leftrightarrow p\equiv \pm\beta^2 \pmod{4q} \tag{1.2}$$

对于某些奇数 β 成立。

事实上，这一猜想和我们通常表述的二次互反律是等价的

定理 1.5

假设 p 与 q 为互异的奇素数，则猜想（1.2）式等价于

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}} \tag{1.3}$$

♡

证明 令 $p^*=(-1)^{\frac{p-1}{2}}p$，则我们有如下的等式：

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},\quad \left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

于是根据上面的性质可得

$$\left(\frac{p^*}{q}\right)=\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right)=\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right).$$

得

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

于是

$$\left(\frac{q}{p}\right)=1 \Leftrightarrow \left(\frac{p^*}{q}\right)=1.$$

于是我们只需证明

$$\left(\frac{p^*}{q}\right) = 1 \Leftrightarrow p \equiv \pm\beta^2 \pmod{4q} \tag{1.4}$$

其中 β 为奇数。

而（1.4）式是容易证明的，这样我们就证明了（1.2）式事实上是二次互反律（1.3）式的一个等价形式。

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。

定理 1.6 (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

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(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

其实后面的思想, 用数学归纳法并不本质，很难透彻理解，可以通过下面两个 Lemma 来看到, 为什么不可以。详细可见附录, 来自 GTM164 加性数论

引理 1.2

If n is a positive integer and $n \equiv 2 \pmod 4$, then n can be represented as the sum of three squares. ♡

引理 1.3

If n is a positive integer such that $n \equiv 1, 3$, or 5 (mod 8), then n can be represented as the sum of three squares. ♡

定理 1.7 (Gauss)

A positive integer N can be represented as the sum of three squares if and only if N is not of the form

$$N = 4^a (8k + 7).$$

♡

笔记 由三平方和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

定理 1.8

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，第一块是乘法封闭，从 N 转化到 P 上。可以从四元数考虑 z 的构造

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

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。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 $1<m\le n<p$ 成立。令 $y_i=x_i \pmod m$ 对于 $i\in\{1,2,3,4\}$ 成立，并且 $-\frac{m}{2}<y_i\le\frac{m}{2}$。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，$mr\le 4\left(\frac{m}{2}\right)^2=m^2$。

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 $1\le r<m\le n<p$ 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 $z_i=w_im$，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 $1\le r<m$，这与 m 的极小性假设相矛盾。

$m=1$ 证明完成！

第 2 章 从 Jacobi theta 到平方和问题

定义 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

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

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

定理 2.1 (Jocabi)

$$r_k(n) = 8 \sum_{4\nmid d,\, d\mid n} d \tag{2.1}$$

♡

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）

引理 2.1 (jocabi 三重积)

$$\prod_{n=1}^{\infty}(1+aq^{2n-1})(1+a^{-1}q^{2n-1})(1-q^{2n}) = \sum_{n=-\infty}^{\infty} a^n q^{n^2} (*) \tag{2.2}$$

♡

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

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

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

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

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

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

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

四次方后再把 q 换成 $-q$，得

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

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 $8\sum_{4\nmid d,\,d\mid n} d$。

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

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

定理 2.2

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

♡

附录 A 二平方和其他证明

证明 利用 Euler 判别法说明 -1 是模 p 的平方剩余, 事实上由 Wilson 定理, 易得 $-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$. 设正整数 a 满足 $p \mid a^2+1$, 考查平面向量 $\mathbf{v}_1=(p,0), \mathbf{v}_2=(a,1)$. 显然它们线性无关, 且在格 $L=\mathbb{Z}\mathbf{v}_1+\mathbb{Z}\mathbf{v}_2$ 上的任一点 (x,y) 处满足 $p \mid x^2+y^2$. $\mathbf{v}_1, \mathbf{v}_2$ 对应基本平行四边形面积为 $\left\|\mathbf{v}_1 \wedge \mathbf{v}_2\right\|=p$, 而以原点为中心, $\sqrt{2p}$ 为半径的圆面积为 $2\pi p>4p$, 于是根据 Minkowski 定理, 这个圆内必定存在除原点外的属于格 $L=\mathbb{Z}\mathbf{v}_1+\mathbb{Z}\mathbf{v}_2$ 的格点 (x,y), 它满足 $p \mid x^2+y^2$ 且 $x^2+y^2<2p$, 于是 $p=x^2+y^2$,

下面是一个《数学天书》的证明

证明 考虑所有满足 $x^2+4yz=p$ 的自然数数组 (x,y,z) 构成的集合 S, 显然 S 是一个有限集. 容易验证 S 上存在以下两组对合映射: (1) $(x,y,z) \mapsto (x,z,y)$ $(x,y,z) \mapsto \begin{cases} (x+2z,z,y-x-z), \text{ if } x \leq y-z \\ (2y-x,y,x-y+z), \text{ if } y-z<x \leq 2y \\ (x-2y,x-y+z,y), \text{ if } x>2y \end{cases}$ 容易验证 (2) 中有唯一不动点 $(1,1,n), n=\frac{p-1}{4}$, 故 S 的元素个数为奇数, 那么 (1) 中也至少有一个不动点 (x,y,y), 即 $x^2+(2y)^2=p$.

附录 B 三平方和详细说明

GTM164 原文

引理 B.1

If n is a positive integer and $n \equiv 2 \pmod 4$, then n can be represented as the sum of three squares. ♡

Proof. Since $(4n, n-1) = 1$, it follows from Dirichlet's theorem that the arithmetic progression $\{4nj + n - 1 : j = 1, 2, \ldots\}$ contains infinitely many primes.

Choose $j \geq 1$ such that

$$p = 4nj + n - 1 = (4j + 1)n - 1$$

is prime. Let $d' = 4j + 1$. Since $n \equiv 2 \pmod 4$, we have

$$p = d'n - 1 \equiv 1 \pmod 4.$$

By Lemma 1.7, it suffices to prove that $-d'$ is a quadratic residue modulo p. Let

$$d' = \prod_{q_i | d'} q_i^{k_i}$$

where the q_i are the distinct primes dividing d'. Then

$$p = d'n - 1 \equiv -1 \pmod{q_i}$$

for all i, and

$$d' \equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \equiv 1 \pmod 4.$$

Therefore,

$$\prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = 1.$$

By quadratic reciprocity we have

$$\left(\frac{-1}{p}\right) = 1$$

since $p \equiv 1 \pmod 4$, and

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$$

$$= \left(\frac{d'}{p}\right)$$

$$= \prod_{q_i} \left(\frac{q_i}{p}\right)^{k_i}$$

$$= \prod_{q_i | d'} \left(\frac{p}{q_i} \right)^{k_i}$$

$$= \prod_{q_i | d'} \left(\frac{-1}{q_i} \right)^{k_i}$$

$$= \prod_{\substack{q_i | d' \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}$$

$$= 1 .$$

This completes the proof.

引理 B.2

If n is a positive integer such that $n \equiv 1, 3$, or 5 (mod 8), then n can be represented as the sum of three squares. ♡

Proof. Clearly,1 is a sum of three nonnegative squares. Let $n \geq 2$. Let

$$c = \begin{cases} 3 & \text{if } n \equiv 1 \pmod 8 \\ 1 & \text{if } n \equiv 3 \pmod 8 \\ 3 & \text{if } n \equiv 5 \pmod 8 . \end{cases}$$

If $n \equiv 1$ or 3 (mod 8), then

$$\frac{cn-1}{2} \equiv 1 \pmod 4 .$$

If $n \equiv 5 \pmod 8$, then

$$\frac{cn-1}{2} \equiv 3 \pmod 4 .$$

In all three cases,

$$\left(4n, \frac{cn-1}{2} \right) = 1$$

By Dirichlet' s theorem, there exists a prime number p of the form

$$p = 4nj + \frac{cn-1}{2}$$

for some positive integer j . Let

$$d' = 8j + c.$$

Then

$$2p = (8j + c) n - 1 = d'n - 1.$$

By Lemma 1.7, it suffices to prove that $-d'$ is a quadratic residue modulo $2p$.
If $-d'$ is a quadratic residue modulo p , then there exists an integer x_0 such that

$$(x_0 + p)^2 + d' \equiv x_0^2 + d' \equiv 0 \pmod{p}.$$

Let $x = x_0$ if x_0 is odd, and let $x = x_0 + p$ if x_0 is even. Then x is odd and $x^2 + d'$ is even. Since

$$x^2 + d' \equiv 0 \pmod{2}$$

and

$$x^2 + d' \equiv 0 \pmod{p}$$

it follows that

$$x^2 + d' \equiv 0 \pmod{2p}.$$

Therefore, it suffices to prove that $-d'$ is a quadratic residue modulo p.
Let

$$d' = \prod_{q_i | d'} q_i^{k_i}$$

be the factorization of the odd integer d' into a product of powers of distinct odd primes q_i. Since

$$2p \equiv -1 \pmod{d'},$$

it follows that

$$2p \equiv -1 \pmod{q_i}$$

and

$$(p, q_i) = 1$$

for every prime q_i that divides d'.
If $n \equiv 1$ or 3 (mod 8), then $p \equiv 1 \pmod{4}$ and

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$$

$$= \left(\frac{d'}{p}\right)$$

$$= \prod_{q_i | d'} \left(\frac{q_i}{p}\right)^{k_i}$$

$$= \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i}$$

If $n \equiv 5 \pmod{8}$, then $p \equiv 3 \pmod{4}$ and $d' \equiv 3 \pmod{8}$. From the factorization of d', we obtain

$$d' = \prod_{\substack{q_i \mid d' \\ q_i \equiv 1 (\bmod\ 4)}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3\ (\bmod\ 4)}} q_i^{k_i}$$

$$\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3\ (\bmod\ 4)}} (-1)^{k_i} \ (\bmod\ 4)$$

$$\equiv -1 \ (\bmod\ 4)$$

and so

$$\prod_{\substack{q_i \mid d' \\ q_i \equiv 3\ (\bmod\ 4)}} (-1)^{k_i} = -1.$$

It follows from quadratic reciprocity that

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right)$$

$$= -\left(\frac{d'}{p}\right)$$

1. Sums of polygons

$$= -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 (\bmod\ 4)}} \left(\frac{q_i}{p}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3 (\bmod\ 4)}} \left(\frac{q_i}{p}\right)^{k_i}$$

$$= -\prod_{\substack{q_i \mid d' \\ q_i \equiv 1 (\bmod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3^{q_i \mid d'}}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3^{q_i \mid d'}}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i \mid d' \\ q_i \equiv 1\ (\bmod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3\ (\bmod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i}$$

$$= \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i}$$

In both cases,

$$\left(\frac{-d'}{p}\right) = \prod_{q_i \mid d'} \left(\frac{p}{q_i}\right)^{k_i}$$

$$= \prod_{q_i \mid d'} \left(\frac{2}{q_i}\right)^{k_i} \left(\frac{2p}{q_i}\right)^{k_i}$$

$$= \prod_{q_i \mid d'} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i \mid d'} \left(\frac{-1}{q_i}\right)^{k_i}$$

$$= \prod_{\substack{q_i \mid d' \\ q_i \equiv 3.5 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3.7 \pmod 8}} (-1)^{k_i}$$

$$= \prod_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i}.$$

Therefore, $-d'$ is a quadratic residue modulo $2p = d'n - 1$ if

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2.$$

This is what we shall prove. We have

$$d' = \prod_{\substack{q_i \mid d' \\ q_i \equiv 3'}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 3'}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ \pmod 8}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5' \pmod 8}} q_i^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 7' \pmod 8}} q_i^{k_i}$$

$$\equiv \prod_{q_i \equiv 3^{q_i \mid d'_i}} 3^{k_i} \prod_{q_i \equiv 5^{q_i \mid d'_i}} (-3)^{k_i} \prod_{q_i \equiv 7^{q_i \mid d'_i}} (-1)^{k_i} \prod_{q_i \equiv 7^{q_i \mid d'_i}} \left((-1)^{k_i}\right) \pmod 8$$

$$\equiv \prod_{\substack{q_i \mid d' \\ q_i \equiv 3.5^{(q_i \mid d'_8)}}} 3^{k_i} \prod_{\substack{q_i \mid d' \\ q_i \equiv 5.7^{(q_i)} \pmod 8}} (-1)^{k_i} \pmod 8.$$

If $n \equiv 1$ or 5 (mod 8), then $c = 3$ and

$$d' = 8j + 3 \equiv 3 \pmod 8.$$

This implies that

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 1 \pmod 2$$

and

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2.$$

If $n \equiv 3 \pmod 8$, then $c = 1$ and

$$d' = 8j + 1 \equiv 1 \pmod 8.$$

It follows that

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 0 \pmod 2$$

and

$$\sum_{\substack{q_i \mid d' \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2 .$$

This completes the proof.

定理 B.1 (Gauss)

A positive integer N can be represented as the sum of three squares if and only if N is not of the form

$$N = 4^a (8k + 7) .$$

♡

Proof. Since

$$x^2 \equiv 0, 1, \text{ or } 4 \pmod 8$$

for every integer x , it follows that a sum of three squares can never be congruent to 7 modulo 8 . If the integer $4m$ is the sum of three squares, then there exist integers

x_1, x_2, x_3 such that

$$4m = x_1^2 + x_2^2 + x_3^2.$$

This is possible only if x_1, x_2, x_3 are all even, and so

$$m = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2.$$

Therefore, $4^a m$ is the sum of three squares if and only if m is the sum of three squares. This proves that no integer of the form $4^a (8k + 7)$ can be the sum of three squares.

Every positive integer N can be written uniquely in the form $N = 4^a m$, where $m \equiv 2 \pmod 4$ or $m \equiv 1, 3, 5$, or $7 \pmod 8$. By Lemma 1.8 and Lemma 1.9, the positive integer N is the sum of three squares unless $m \equiv 7 \pmod 8$. This completes the proof.

Bibliography

[1] GTM7

[2] 数论 I–Fermat 的梦想和类域论🄵川信重，栗原将人，🄵藤毅

[3] 数论 II——岩澤理論と保型形式🄵川信重，栗原将人，🄵藤毅

[4] GTM164 加性数论