中国科学(A 辑)
第 31 卷 第 10 期 SCIENCE IN CHINA (Series A) 2001 年 10 月

3/2 权的 Eisenstein 级数和 Kaplansky 的一个猜想*

王学理 裴定一

(广州大学数学系,广州 510405;中国科学院研究生院信息安全国家重点实验室,北京 100039)

摘要 利用 3/2 权的 Eisenstein 级数方法,证明三元二次型:$f_1(x,y,z)=x^2+y^2+7z^2$能够表示所有除形如:14×7^{2k}之外的模 3 同余于 2 的合格数. 这是 Kaplansky (1995 年)猜测的. 该方法也可以应用到其他的三元二次型.

关键词 Eisenstein 级数 Kaplansky 猜想 三元二次型

本文研究问题:如何找出被一个正定三元二次型表示的整数. Jones 指出:在一个簇中的全体三元二次型能够表示除满足某些对应的同余式之外的所有正整数[1]. 借用 Kaplansky 的说法,称这些数为该簇的合格数[2]. 但是,一般来说,要决定在一个簇中的某个形式到底表示哪些合格数,是非常困难的事情. 这即使对于十分简单的情形,也难于解决.

在文献[2]中,Kaplansky 就研究了 $f_1=x^2+y^2+7z^2$ 与 $g_1=x^2+2y^2+4z^2+2yz$ 组成的一个簇的代表元集. f_1 和 g_1 的合格数是那些不为 7 的奇数次幂和模 7 同余于 3, 5 或 6 的数之积者. 但无法完全确定它们中哪一些能够由 f_1 表示,哪一些可以由 g_1 表示. Kaplansky 证明了下面定理和列表:

定理 1 形式 f_1 表示所有是 9 的倍数的合格数,也表示所有模 3 同余于 2,但不具有形式 $14t^2$ 的合格数.

表 Ⅰ: 直到 100000 为止,仅有 27 个与 7 互素的合格数不能被 f_1 表示:3, 6, 19, 22, 31, 51, 56, 66, 94, 139, 142, 159, 166, 214, 235, 283, 439, 534, 559, 670, 874, 946, 1726, 2131, 2419, 3559, 4759.

表 Ⅱ: 直到 100000 为止,仅有 26 个模 7 同余于 1, 2 或 4 的合格数不能被 $f_2=x^2+7y^2+7z^2$ 表示:2, 22, 46, 58, 85, 93, 102, 205, 298, 310, 330, 358, 466, 478, 697, 862, 949, 1222, 1402, 1513, 1957, 1978, 2962, 3502, 7165, 10558.

显然,$14\times 7^{2k}\equiv 2 \pmod 3$,且由归纳法可知 f_1 不能表示形如 14×7^{2k}的合格数,其中 k 是任意非负整数. 称形如 14×7^{2k}为平凡型的数,因此,确实存在形如 $14t^2$ 的合格数不能被 f_1 表示. 这促使 Kaplansky 猜想:

猜想 1 f_1 表示所有模 3 同余于 2 的非平凡型的合格数.

2000-07-04 收稿,2001-03-19 收修改稿

* 国家自然科学基金资助项目(批准号:19871017)

本文的主要结果是上述猜想成立,即

定理 2 f_1 表示所有模 3 同余于 2 的非平凡型的合格数.

本文中的方法也可以应用到其他的三元二次型,在此不作考虑,有兴趣的读者可参见文献[3].

1 定理 2 的证明

为了证明定理 2,需要引进某些记号和结果. 有关的详细的证明可参见文献[3].

设 α,β,γ 是无平方因子奇正整数,且 $(\alpha,\beta,\gamma)=1$. 记 $D=[\alpha,\beta,\gamma]$, $\lambda_{4m}(m\mid D)$ 和 $\lambda_m(1\neq m\mid D)$ 是下述线性方程组的惟一解:

$$\begin{cases}\displaystyle\sum_{m\mid D}(C_{4m}\cdot\mu(m/d)m^{-1})+\sum_{1\neq m\mid D}(C_m\cdot\mu(m/d)m^{-1})\\ \displaystyle\quad=\frac{1}{D}\left(\frac{-1}{d}\right)\left(\frac{\alpha\beta/(\alpha,\beta)^2}{(d,\alpha,\beta)(d,l,\gamma)}\right)\left(\frac{\beta\gamma/(\beta,\gamma)^2}{(d,\beta,\gamma)(d,l,\alpha)}\right)\left(\frac{\gamma\alpha/(\gamma,\alpha)^2}{(d,\gamma,\alpha)(d,l,\beta)}\right),\\ \displaystyle\sum_{m\mid D}C_{4m}\cdot\mu(m/d)m^{-1}\\ \displaystyle\quad=\frac{1}{D}\left(\frac{-1}{D/d}\right)\left(\frac{\alpha\beta/(\alpha,\beta)^2}{\gamma(\alpha,\beta)(\alpha,\beta,d)^{-1}(\gamma,\alpha\beta d)^{-1}}\right)\left(\frac{\beta\gamma/(\beta,\gamma)^2}{\alpha(\beta,\gamma)(\alpha,\beta\gamma d)^{-1},(\beta,\gamma,d)^{-1}}\right)\\ \displaystyle\quad\times\left(\frac{\gamma\alpha/(\gamma,\alpha)^2}{\beta(\gamma,\alpha)(\beta,\alpha\gamma d)^{-1}(\gamma,\alpha,d)^{-1}}\right),\end{cases}\qquad(*)$$

其中 $l=\alpha\beta\gamma/((\alpha,\beta)^2(\alpha,\gamma)^2(\beta,\gamma)^2)$. 对于正整数 n,D,l,定义:

$$\alpha(n)=\begin{cases}3\times2^{-(1+v_2(n))/2}, & 若\ 2\nmid v_2(n),\\ 3\times2^{-(1+v_2(n)/2)}, & 若\ 2\mid v_2(n),n/2^{v_2(n)}\equiv1\ (\mathrm{mod}\ 4),\\ 2^{-v_2(n)/2}, & 若\ 2\mid v_2(n),n/2^{v_2(n)}\equiv3\ (\mathrm{mod}\ 8),\\ 0, & 若\ 2\mid v_2(n),n/2^{v_2(n)}\equiv7\ (\mathrm{mod}\ 8),\end{cases}$$

$$\beta_{l,p}(n)=\begin{cases}(1+p)p^{(1-v_p(ln))/2}, & 若\ 2\nmid v_p(ln),\\ 2p^{1-v_p(ln)/2}, & 若\ 2\mid v_p(ln),\ \left(\dfrac{-ln/p^{v_p(ln)}}{p}\right)=-1,\\ 0, & 若\ 2\mid v_p(ln),\ \left(\dfrac{-ln/p^{v_p(ln)}}{p}\right)=1,\end{cases}$$

$$\beta_3(n,\chi_D,4D)=\sum_{\substack{(ab)^2\mid n,(a,b,2D)=1\\ a,b正整数}}\mu(a)\left(\frac{-n}{a}\right)(ab)^{-1},$$

其中 μ 为 Möbius 函数. 注意到,如果 n 是无平方因子的正整数,$\beta_3(n,\chi_D,4D)=1$,其中 $v_p(n)$. 记 n 的 p-adic 赋值,即 $v_p(n)$ 是最大非负整数 h 使得 $p^h\mid n$.

引理 1 假设 α,β,γ 是无平方因子奇正整数且 $(\alpha,\beta,\gamma)=1$, $f=\alpha x^2+\beta y^2+\gamma z^2$,又假设 $A=\{f_1=f,f_2,\cdots,f_t\}$ 是 f 所在簇中等价类的代表元之全体的集合,则对任意正整数 n,有

$$G(n)=r(\alpha,\beta,\gamma;n)\cdot h(-ln),$$

其中 $l=\alpha\beta\gamma/((\alpha,\beta)^2(\alpha,\gamma)^2(\beta,\gamma)^2)$，$h(-ln)$是二次域$\mathbb{Q}(\sqrt{-ln})$的类数，而

$$r(\alpha,\beta,\gamma;n)=\frac{32}{\omega_{ln}}\alpha(ln)(1-2^{-1}\chi_{-ln}(2))\left(\frac{ln}{\delta_{ln}}\right)^{1/2}\beta_3(ln,\chi_D,4D)\times\left(\sum_{i=1}^{t}\frac{1}{O(f_i)}\right)$$
$$\times\left(\sum_{m\mid D}(-1)^{t(m)}\lambda_{4m}\prod_{p\mid D/m}\frac{(1-\chi_{-ln}(p)p^{-1})p^2}{p^2-1}\prod_{p\mid m}\frac{(1-\chi_{-ln}(p)p^{-1})}{p^2-1}\beta_{l,p}(n)\right.$$
$$\left.+\sum_{1\neq m\mid D}(-1)^{t(m)}\lambda_m\prod_{p\mid D/m}\frac{(1-\chi_{-ln}(p)p^{-1}}{p^2-1}\prod_{p\mid m}\frac{(1-\chi_{-ln}(p)p^{-1}}{p^2-1}\beta_{l,p}(n)\right),$$

$G(n)=\sum_{i=1}^{t}\frac{r_i(n)}{O(f_i)}$，$r_i(n)$ 是 n 由f_i 表示的表示数，$O(f_i)$是 f_i 的自同构的数目，其中 ω_{ln}是$\mathbb{Q}(\sqrt{-ln})$中单位根的数目，$t(m)$记 m 的不同素因子的数目，χ_{-ln}是如下定义的特征：

$$\chi_{-ln}(\cdot)=\left(\frac{-ln}{\cdot}\right),$$

而 δ_{ln}是χ_{-ln}的导子．

证　参见文献[3]，这里略．

引理 2　（ⅰ）记 $r_1(n)$是 n 由$f_1=x^2+y^2+7z^2$ 表示的表示数，$r'_1(n)$是 n 由 $g_1=x^2+2y^2+4z^2+2yz$ 表示的表示数，则

$$G_1(n)=\frac{r_1(n)}{8}+\frac{r'_1(n)}{4}=\frac{1}{4}\omega_{7n}^{-1}(2-\alpha(7n))\beta_{7,7}(n)\gamma_7(n)h(-7n).$$

（ⅱ）记 $r_2(n)$是 n 由$f_2=x^2+7y^2+7z^2$ 表示的表示数，$r'_2(n)$是 n 由 $g_2=2x^2+4y^2+7z^2-2yz$ 表示的表示数，则

$$G_2(n)=\frac{r_2(n)}{8}+\frac{r'_2(n)}{4}=\frac{1}{4}\omega_n^{-1}(2-\alpha(n))\beta_{1,7}(n)\gamma'_7(n)h(-n),$$

其中

$$\gamma_7(n)=(1-2^{-1}\chi_{-7n}(2))(7n/\delta_{7n})^2\sum_{\substack{(ab)^2\mid n\\(ab,14)=1}}\mu(a)\chi_{-7n}(a)(ab)^{-1},$$

$$\gamma'_7(n)=(1-2^{-1}\chi_{-n}(2))(1-\chi_{-n}(7)7^{-1})(n/\delta_n)^{1/2}\sum_{\substack{(ab)^2\mid n\\(ab,14)=1}}\mu(a)\chi_{-n}(a)(ab)^{-1}.$$

证　（ⅰ）注意到 $O(f_1)=8$，$O(g_1)=4$，且此时对应的线性方程组（＊）有惟一解

$$\begin{pmatrix}\lambda_4\\\lambda_{28}\\\lambda_7\end{pmatrix}=\begin{pmatrix}0\\1\\-2\end{pmatrix}.$$

于是利用引理 1 立得．

（ⅱ）与（ⅰ）的证明完全类似．

推论 1　（ⅰ）f_1 和 g_1 的合格数是所有不为 7 的奇数次幂和模 7 同余于 3,5 或 6 的数之积者；

（ⅱ）f_2 和 g_2 的合格数是所有不为 7 的偶数次幂和模 7 同余于 3, 5 或 6 的数之积者．

证　（ⅰ）由引理 2 知，正整数 n 是f_1 和 g_1 的合格数当且仅当 $G_1(n)>0$，不难证明此时

引理 2(ⅰ)中的 $G_1(n)$ 的右边表达式中除 $\beta_{7,7}(n)$ 外都是正数，故 n 不是合格数当且仅当 $\beta_{7,7}(n)=0$，由 $\beta_{7,7}(n)$ 的定义，这当且仅当 $v_7(n)\equiv 1 \pmod 2$ 且 $\left(\frac{-n/7^{v_7(n)}}{7}\right)=1$，这正是推论 1 的结果.

(ⅱ) 证明与(ⅰ)完全类似.

引理 3　$f_1=x^2+y^2+7z^2$ 不能表示 $7A$ 当且仅当 $f_2=x^2+7y^2+7z^2$ 不能表示 A.

由推论 1 知 f_2 和 g_2 的合格数正好是那些不是 7 的偶数次幂和模 7 同余于 3, 5 或 6 之积者，因此由引理 3 知，为了证明定理 2，仅需要证明 f_2 表示所有模 7 同余 1,2,4 且形如 $2t^2$($t\neq 1$ 且 $7\nmid t$) 的合格数. 这表明，如果能够证明与 7 互素且不能被 f_2 表示的合格数均是无平方因子的，则定理 2 得证. 事实上，有

定理 3　假设 $f_2=x^2+7y^2+7z^2$，如果 n 是一个与 7 互素的合格数，且 n 不能被 f_2 表示，则 n 是无平方因子的.

证　由引理 2(ⅱ)及 n 是一个合格数，有

$$0 < G_2(n) = \frac{r_2(n)}{8} + \frac{r'_2(n)}{4} = \frac{1}{4}\omega_n^{-1}(2-\alpha(n))\beta_{1,7}(n)\gamma'_7(n)h(-n), \tag{1}$$

此处 $r_2(n)$ 和 $r'_2(n)$ 分别记 n 被 f_2 和 $g_2=2x^2+4y^2+7z^2-2yz$ 表示的表示数. 由直接计算，易知

$$\tilde{f}_2(z) := \sum_{n=1}^{\infty} b(n)\mathrm{e}^{2\pi inz} = \frac{1}{2}\sum_{n=1}^{\infty}(r_2(n)-r'_2(n))\mathrm{e}^{2\pi inz} \tag{2}$$

是尖点模形式空间 $S_{3/2}(28,\chi_1)$ 中所有 Hecke 算子 T_{n^2} 的特征函数，并且其 Shimura 提升 $F_2(z)=S(\tilde{f}_2(z))$ 是一个权为 2，特征为 χ_1 且水平为 14 的新形式. 即 $F_2(z)\in S_{3/2}^{new}(14,\chi_1)$. 因此，存在复数 α_n，使得 $T_{n^2}(\tilde{f}_2(z))=\alpha_n\tilde{f}_2(z)$. 但 Hecke 算子与 Shimura 提升可交换，故有

$$\begin{aligned} T_n(F_2(z)) &= T_n(S(\tilde{f}_2(z))) = S\circ T_{n^2}(\tilde{f}_2(z)) \\ &= S(\alpha_n\tilde{f}_2(z)) = \alpha_n S(\tilde{f}_2(z)) = \alpha_n F_2(z). \end{aligned}$$

这表明 α_n 也是 T_n 对于 $F_2(z)$ 的特征值. 但 $F_2(z)$ 是一个权为 2 的新形式，这意味着对任意正整数 m，$(m,14)=1$，有 $\alpha_m=B(m)$，此处 $F_2(z)=\sum_{n=1}^{\infty}B(n)\mathrm{e}^{2\pi inz}$ 是 $F_2(z)$ 的 Fourier 展开式. 所有这些事实表明

$$B(p)b(n) = \alpha_p b(n) = b(p^2n) + \left(\frac{-n}{p}\right)b(n) + pb(n/p^2) \tag{3}$$

对任意素数 p，$(p,14)=1$，及任意正整数 n 成立. 注意到 $b(n)=\frac{r_2(n)-r'_2(n)}{2}$，则

$$r_2(p^2n)-r'_2(p^2n) = \left(B(p)-\left(\frac{-n}{p}\right)\right)(r_2(n)-r'_2(n)) + p(r_2(n/p^2)-r'_2(n/p^2)). \tag{4}$$

特别地，如果 n 是无平方因子的正整数，则对任意素数 p，$(p,14)=1$，有

$$r_2(p^2n)-r'_2(p^2n) = \left(B(p)-\left(\frac{-n}{p}\right)\right)(r_2(n)-r'_2(n)). \tag{5}$$

对于素数 $p\mid 14$，由 Hecke 算子的定义，得知 $T_{p^2}(\tilde{f}_2(z))=\sum_{n=1}^{\infty}b(p^2n)\mathrm{e}^{2\pi inz}$，这表明：

$$\alpha_p b(n) = b(p^2 n),$$

即

$$r_2(p^2 n) - r'_2(p^2 n) = \alpha_p(r_2(n) - r'_2(n)). \tag{6}$$

直接计算易知 $\alpha_2 = -1$，$\alpha_7 = 1$.

现在证明：如果 n_0 是一个无平方因子的正整数，且不能被 f_2 表示（即 $r_2(n_0)=0$），则 $p^2 n_0$ 一定能被 f_2 表示（即 $r_2(p^2 n_0) \neq 0$），其中 p 是任意素数，且 $(p,7)=1$. 假设不然，则由(4)和(6)式知：

$$\frac{r'_2(p^2 n_0)}{r'_2(n_0)} = B(p) - \left(\frac{-n_0}{p}\right), \quad \frac{r'_2(2^2 n_0)}{r'_2(n_0)} = -1. \tag{7}$$

另一方面，由(1)式，有

$$\frac{r'_2(p^2 n_0)}{r'_2(n_0)} = \frac{G_2(p^2 n_0)}{G_2(n_0)} = \frac{\omega_{p^2 n_0}^{-1}(2-\alpha(p^2 n_0))\beta_{1,7}(p^2 n_0) r'_7(p^2 n_0) h(-p^2 n_0)}{\omega_{n_0}^{-1}(2-\alpha(n_0))\beta_{1,7}(n_0) r'_7(n_0) h(-n_0)}$$

$$= \frac{(2-\alpha(p^2 n_0))\beta_{1,7}(p^2 n_0) r'_7(p^2 n_0)}{(2-\alpha(n_0))\beta_{1,7}(n_0) r'_7(n_0)}. \tag{8}$$

现设 $p \neq 2,7$，则由 $\alpha(n)$，$\beta_{1,7}(n)$ 和 $r'_7(n)$ 的定义，及 n_0 为无平方因子正整数这个事实，易得

$$\alpha(p^2 n_0) = \alpha(n_0), \quad \beta_{1,7}(p^2 n_0) = \beta_{1,7}(n_0),$$

$$r'_7(p^2 n_0) = (p+1) r'_7(n_0), \quad \alpha(2^2 n_0) = \frac{1}{2}\alpha(n_0),$$

$$\beta_{1,7}(2^2 n_0) = \beta_{1,7}(n_0), \quad r'_7(2^2 n_0) = \frac{3}{1 - 2^{-1}\chi_{-n_0}(2)} r'_7(n_0),$$

$$\alpha(7^2 n_0) = \alpha(n_0), \quad \beta_{1,7}(7^2 n_0) = \frac{1}{7}\beta_{1,7}(n_0), \quad r'_7(7^2 n_0) = \frac{8}{1 - \chi_{-n_0}(7) 7^{-1}} r'_7(n_0).$$

因此，有

$$\frac{r'_2(p^2 n_0)}{r'_2(n_0)} = \begin{cases} p+1, & 若\ p \neq 2,7, \\ 5, & 若\ p = 2,\ v_2(n_0) = 1, \\ 15, & 若\ p = 2, n_0 \equiv 1 \pmod 4, \\ 9, & 若\ p = 2, n_0 \equiv 3 \pmod 8, \\ 6, & 若\ p = 2, n_0 \equiv 7 \pmod 8, \\ \dfrac{8}{7 - \chi_{-n_0}(7)}, & 若\ p = 7. \end{cases} \tag{9}$$

对任意素数 $p \neq 2,7$，由(7)和(9)式，有

$$B(p) \geqslant p, \tag{10}$$

且

$$0 < \frac{r'_2(2^2 n_0)}{r'_2(n_0)} = -1 < 0. \tag{11}$$

(11)式是不可能的，因为 n_0 是合格数，而(10)式也是不可能的，因为由模形式 Fourier 系数的

Deligne 估计,知 $B(p)\leqslant 2\sqrt{p}$,从而对于 $p>3$,不可能有 $B(p)\geqslant p$. 又直接计算表明 $B(3)<3$.

由上面已经证明了:如果 n 是 f_2 和 g_2 的任意无平方因子的合格数,且 n 不被 f_2 表示,则对任意不等于 7 的素数 p, p^2n 一定被 f_2 表示. 这当然等价于说,如果 n 是与 7 互素的合格数,且 n 不被 f_2 表示,则 n 是无平方因子的. 这就完成了定理 3 的证明. 从而完成了定理 2 的证明.

注 1 如果 n 不是与 7 互素的,则定理 3 的结论不正确. 例如 $n=98=2\times 7^2$ 就是一个有平方因子的合格数,但不能被 f_2 表示. 事实上,对于 $p=7$,上面的证明并不适应,因为不能获得一个相应于 $p\neq 7$ 类似的矛盾. 因为若假设 n_0 是一个合格数,使得 $r_2(n_0)=r_2(7^2n_0)=0$,则上面的计算表明有

$$\frac{8}{7-\chi_{-n_0}(7)}=\frac{r'_2(7^2n_0)}{r'_2(n_0)}=\alpha_7=1.$$

这是可能的,例如取 $n_0=2$,就使上式成立.

注 2 本文的方法能用于更多的三元二次型,例如,可以完全类似地证明

定理 4 假设 $f_p=x^2+py^2+pz^2$, p 为奇素数,又设 f_p 的簇由两个等价类组成,其代表元为 f_p 和 g_p,记

$$\tilde{f}_p(z):=\sum_{n=1}^{\infty}b(n)e^{2\pi inz}=\frac{1}{2}(r(n)-r'(n))e^{2\pi inz},$$

此处 $r(n)$ 和 $r'(n)$ 分别是 n 被 f_p 和 g_p 表示的表示数,假定 $\tilde{f}_p(z)$ 的 Shimura 提升 $F_p(z)=S(\tilde{f}_p(z))$ 是一个权 2 的新形式,则 f_p 和 g_p 的每一个与 $2p$ 互素的不能被 f_p 表示的合格数,一定是无平方因子的.

例 每一个与 34 互素且不能被 $f_{17}=x^2+17y^2+17z^2$ 表示的合格数均是无平方因子的. 这是因为 f_{17} 和 $g_{17}=2x^2+9y^2+17z^2+2xy$ 组成一个簇的全体代表元, $\tilde{f}_{17}(z)$ 的 Shimura 提升是对应于模椭圆曲线(34A)的新形式.

参考文献

1 Jones B. The regularity of a genus of positive ternary quadratic forms. Trans Amer Math Soc, 1931, 33: 111 ~ 124

2 Kaplansky I. The first nontrivial genus of positive definite ternary forms. Math Comp, 1995, 64: 341 ~ 345

3 Pei Dingyi, Rosenberger G, Wang Xueli. The eligible numbers of positive definite ternary quadratic forms. Math Zeitschriften, 2000, 235: 479 ~ 497