一个二次型引理以及应用

曾卫国

(湖南省雅礼中学, 410007)

在笔者学生时代, 曾经遇到过一道难题, 就是下面给出的引理. 本文将利用引理去解决一些颇有难度的关于数论的平方和问题.

引理 设 $a>0, c>0, \Delta=4ac-b^2>0$, $f(x,y)=ax^2+bxy+cy^2$, 则存在不全为 0 的 整数 x,y, 使得

$$f(x,y)\le\sqrt{\frac{\Delta}{3}}.$$

证明 首先, 因为 $a>0, c>0, \Delta=4ac-b^2>0$, 所以

$$ax^2+bxy+cy^2=\frac{1}{a}\left(\left(ax+\frac{by}{2}\right)^2+\frac{\Delta}{4}y^2\right)=\frac{1}{c}\left(\left(\frac{bx}{2}+cy\right)^2+\frac{\Delta}{4}x^2\right)\ge 0$$

恒成立, 注意到 $f(1,0)=a$, 所以当 x,y 是整数且不全为 0 时, $f(x,y)$ 的最小值 $\le a$.

又 $f(x,y)\le a\Rightarrow \Delta y^2\le 4a^2, \Delta x^2\le 4ac$, 说明此时整数对 (x,y) 有限, 从而存在不全为 0 的整数对 (u,v), 使得 $f(u,v)$ 取最小值, 记为 M. 显然 u,v 是互质的, 由裴蜀定理: 存在整数 s,t, 使得 $us-vt=1$.

另一方面, 令 $x=uz+t, y=vz+s$, 解得 $z=sx-ty, 1=uy-vx$, 从而 x,y 不全为 0. 则

$$\begin{aligned}
f(x,y)&=ax^2+bxy+cy^2=a(uz+tw)^2+b(uz+t)(vz+s)+c(vz+s)^2\\
&=z^2M+z(2aut+btv+bus+2cvs)+\left(at^2+bst+cs^2\right)\\
&=M\left(z+\frac{(2aut+btv+bus+2cvs)}{2M}\right)^2+\left(at^2+bst+cs^2\right)\\
&\quad-\frac{(2aut+btv+bus+2cvs)^2}{4M}\\
&=M\left(z+\frac{w(aut+btv+bus+cvs)}{M}\right)^2+\frac{\Delta}{4M}.
\end{aligned}$$

修订日期: **2019-04-20.**

所以存在整数 z, 使得

$$\left|z+\frac{w(aut+btv+bus+cvs)}{M}\right| \leq \frac{1}{2},$$

此时,

$$M \leq f(x,y) \leq \frac{M}{4}+\frac{\Delta}{4M},$$

从而 $M \leq \sqrt{\frac{\Delta}{3}}$. 引理得证. □

推论 对于正整数 m,n,k,l, 若 $mn=k^2+l$, 则存在不全为 0 的整数 x,y, 使得

$$0<mx^2+2kxy+ny^2 \leq \sqrt{\frac{4l}{3}}.$$

从而可以得到如下命题:

命题 1 若 $m \mid k^2+1$, 则存在整数 x,y, 使得 $m=x^2+y^2$.

证明 事实上, 在推论中取 $l=1$ 即知存在存在不全为 0 的整数 u,v, 使得

$$mu^2+2kuv+nv^2=1,$$

即 $m=m^2u^2+2kmuv+mnv^2=(mu+kv)^2+v^2$ 为两个整数的平方和. □

命题 2 若 $m|k^2+2$, 则存在整数 x,y, 使得 $m=x^2+2y^2$.

证明 在推论中取 $l=2$ 即知存在存在不全为 0 的整数 u,v, 使得

$$mu^2+2kuv+nv^2=1,$$

即

$$m=m^2u^2+2kmuv+mnv^2=(mu+kv)^2+2v^2.$$

令 $x=mu+kv, y=v$ 即可. □

命题 2* 若奇质数 p 满足 $p \equiv 1,3 \pmod 8$, 则存在整数 x,y, 使得 $p=x^2+2y^2$.

证明 若奇质数 p 满足 $p \equiv 1,3 \pmod 8$, 则由二次剩余可以知 $\left(\frac{-2}{p}\right)=1$, 从而存在正整数 k, 使得 $p|k^2+2$, 从而由命题 2 即知结论成立. □

命题 3 若 $m \mid k^2+3$, 则存在整数 x,y, 使得 $m=x^2+3y^2$ 或者 $2m=x^2+3y^2$.

证明 在推论中取 $l=3$, 知存在整数 u,v, 使得

$$0<mu^2+2kuv+nv^2 \leq 2,$$

从而 $mu^2+2kuv+nv^2=t, t=1$ 或者 2, 从而

$$tm=m^2u^2+2kmuv+mnv^2=(mu+kv)^2+3v^2,$$

令 $x=mu+kv, y=v$ 即可. □

命题 3* 若质数 p 满足 $p\equiv 1 \pmod 3$, 则存在整数 x,y, 使得 $p=x^2+3y^2$.

证明 质数 p 满足 $p\equiv 1 \pmod 3$, 由二次剩余知存在正整数 k, 使得 $p|k^2+3$. 从而由命题 3 可知存在整数 x,y, 使得 $p=x^2+3y^2$ 或者 $2p=x^2+3y^2$, 又因为 $x^2+3y^2\equiv 0,1 \pmod 3$, 所以 $2p=x^2+3y^2$ 不成立, 从而 $p=x^2+3y^2$. □

命题 4 若 $m\mid k^2+5$, 则存在整数 x,y, 使得 $m=x^2+3y^2$ 或者 $2m=x^2+3y^2$.

命题 4 的证明和命题 3 的证明类似, 推论中取 $l=5$ 即可.

有兴趣的读者可以进一步思考 l 取更大值的情形.

下面再给出两个例子.

例 1 求所有的质数 p, 使得存在正整数 x,y, $p=x^2+5y^2$.

解 所求 p 是模 20 余 1 或者 9 的质数.

显然, 若存在正整数 x,y, $p=x^2+5y^2$, 则 x,y 一定是一奇一偶并且 x,y 互质, 从而

$$p\equiv x^2+y^2\equiv 1 \pmod 4,\quad p\equiv x^2\equiv \pm 1 \pmod 5,$$

所以 $p\equiv 1,9 \pmod{20}$.

另一方面, 当 $p\equiv 1,9 \pmod{20}$ 时, 勒让德符号

$$\left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)=(-1)^{\frac{5-1p-1}{2}}\left(\frac{p}{5}\right)=1,$$

所以存在整数 m, 使得 $p|m^2+5$, 设 $m^2+5=pq$.

考虑函数 $f(u,v)=pu^2+2muv+qv^2, \Delta=4pq-4m^2=20>0$.

由引理可知, 存在不全为 0 的整数 u_0,v_0, 使得

$$0<f\left(u_0,v_0\right)\leq\sqrt{\frac{20}{3}}<3,$$

从而 $f\left(u_0,v_0\right)=1$ 或 2.

若 $f\left(u_0,v_0\right)=1$, 则

$$p=pf\left(u_0,v_0\right)=p^2u_0^2+2mpu_0v_0+pqv_0^2=\left|pu_0+mv_0\right|^2+5v_0^2,$$

令 $x=\left|pu_0+mv_0\right|, y=\left|v_0\right|, x\neq 0, y\neq 0$, 从而 $p=x^2+5y^2$.

若 $f(u_0,v_0)=2$, 则

$$2p=pf(u_0,v_0)=p^2u_0^2+2mpu_0v_0+pqv_0^2=|pu_0+mv_0|^2+5v_0^2,$$

从而 $2p\equiv |pu_0+mv_0|^2\equiv \pm 2 \pmod 5$, 矛盾.

综上, 所求 p 是模 20 余 1 或者 9 的质数. □

例 2 (2006 CMO) 正整数 m,n,k 满足 $mn=k^2+k+3$, 证明: 方程 $4m=x^2+11y^2$ 和 $4n=x^2+11y^2$ 至少有一个方程有奇数解 (x,y).

证明 设 $f(x,y)=mx^2+(2k+1)xy+ny^2, \Delta=4mn-(2k+1)^2=11>0$, 由引理, 存在不全为 0 的整数对 (x_0,y_0) 使得

$$0<f(x_0,y_0)\le\sqrt{\frac{11}{3}}<2,$$

所以 $f(x_0,y_0)=1$. 即

$$1=mx_0^2+(2k+1)x_0y_0+ny_0^2,$$

显然 x_0,y_0 中至少有一个奇数.

若 y_0 是奇数,

$$4m=(2mx_0+(2k+1)y_0)^2+11y_0^2, x=2mx_0+(2k+1)y_0, y=y_0,$$

则 $4m=x^2+11y^2$ 符合.

若 x_0 是奇数,

$$4n=(2ny_0+(2k+1)x_0)^2+11x_0^2, x=2ny_0+(2k+1)x_0, y=x_0,$$

则 $4n=x^2+11y^2$ 符合.

综上, 结论成立. □

注 这是一道非常难的题, 此题在当年考试时只有一位同学完整做出. 对此题可以进行一些简单的推广:

(1) 正整数 m,n,k 满足 $mn=k^2+k+1$, 证明: $4m=x^2+3y^2$ 和 $4n=x^2+3y^2$ 至少有一个方程有奇数解 (x,y).

(2) 正整数 m,n,k 满足 $mn=k^2+k+2$, 证明: $4m=x^2+7y^2$ 和 $4n=x^2+7y^2$ 至少有一个方程有奇数解 (x,y).

(3) 正整数 m,n,k 满足 $m\mid k^2+k+n, n\in\{4,5,6\}$, 证明: $4m=x^2+(4n-1)y^2$ 和 $8m=x^2+(4n-1)y^2$ 至少有一个方程有整数解 (x,y).

有兴趣的读者可以做更多的推广.