A talk given at Institute of Mathematics, Chinese Academy of Sciences (Beijing, 2017)

THE THREE-SQUARE THEOREM AND ITS APPLICATIONS

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

1. The Three-Square-Theorem

What integers can be written as the sum of three squares ? This was answered by the following classical theorem which is called the Three-Square-Theorem or the Gauss-Legendre Theorem (cf. M. B. Nathanson [N96]).

Three-Square-Theorem (Legendre, 1797; Gauss, 1801)**.** $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ *can be written as the sum of three squares if and only if it is not of the form* $4^k(8l + 7)$ *with* $k, l \in \mathbb{N}$.

The "only if" direction is easy. If $x, y, z \in \mathbb{Z}$ and $x^2 + y^2 + z^2 \equiv 3 \pmod 4$, then $2 \nmid xyz$ and thus $x^2+y^2+z^2 \equiv 3 \not\equiv 7 \pmod 8$. If $4^k(8l+7) = x^2 + y^2 + z^2$ with $k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, $l \in \mathbb{N}$ and $x, y, z \in \mathbb{Z}$, then x, y, z are all even and

$$4^{k-1}(8l + 7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2.$$

Thus

$$4^{k-1}(8l+7) \notin \{x^2+y^2+z^2 : x, y, z \in \mathbb{Z}\} \Longrightarrow 4^k(8l+7) \notin \{x^2+y^2+z^2 : x, y, z \in \mathbb{Z}\}.$$

So, by induction we see that $4^k(8l + 7)$ with $k, l \in \mathbb{N}$ cannot be written as the sum of three squares.

The "if" direction is much more difficult. It involves the theory of quadratic forms.

Let $M_n(\mathbb{Z})$ be the ring of all $n\times n$ matrices over $\mathbb{Z}$, and $\mathrm{SL}_n(\mathbb{Z})$ be the special linear group consisting of those $U\in M_n(\mathbb{Z})$ with $\det U=1$. For $A,B\in M_n(\mathbb{Z})$, we say that A is equivalent to B (which is denoted by $A\sim B$) if $U'AU=B$ for some $U\in M_n(\mathbb{Z})$, where U' is the transpose of U. Clearly, $A\sim B$ implies that $\det A=\det B$, and the relation $\sim$ is an equivalent relation over $M_n(\mathbb{Z})$.

For a symmetric matrix $A\in M_n(\mathbb{Z})$, its associated quadratic form is

$$F_A(x_1,\ldots,x_n)=\sum_{i=1}^n\sum_{j=1}^n a_{ij}x_ix_j=\sum_{i=1}^n a_{ii}x_i^2+2\sum_{1\leqslant i<j\leqslant n}a_{ij}x_ix_j=xAx',$$

where x denotes the vector $(x_1,\ldots,x_n)$. The discriminant of F_A is defined by $d(F_A)=\det A$. If $F_A(x_1,\ldots,x_n)=N$ for some $x_1,\ldots,x_n\in\mathbb{Z}$, then we say that F_A represents N.

For two symmetric matrices $A,B\in M_n(\mathbb{Z})$, if $A\sim B$ then we write $F_A\sim F_B$ (and say that F_A is equivalent to F_B), and in this case $d(F_A)=d(F_B)$. If $F_A\sim F_B$, then $U'AU=B$ for some $U\in\mathrm{SL}_n(\mathbb{Z})$ and hence

$$F_B(x)=xBx'=xU'AUx'=(Ux')'A(Ux')=F_A(Ux').$$

Thus, if $F_A\sim F_B$ then the integers represented by F_A coincide with the integers represented by F_B.

Let $A\in M_n(\mathbb{Z})$ be symmetric. If $F_A(x_1,\ldots,x_n)>0$ for all $x_1,\ldots,x_n\in\mathbb{Z}$ with $x_1,\ldots,x_n$ not all zero, then we call the quadratic form F_A *positive-definite*. For the linear algebra, we know that F_A is positive-definite if and only if $\det(a_{ij})_{1\leqslant i,j\leqslant k}>0$ for all $k=1,\ldots,n$.

Using the auxiliary results in Sections 2 and 3 on binary and ternary quadratic forms, we give the first proof of the Three-square Theorem in Section 4 (based on some treatments from Nathanson [N96]). In Section 5 we give another proof of the Three-square Theorem via Legendre's theorem (based on some materials from P. Pollack [P]. In the last section we present several applications of the Three-Square Theorem.

2. Binary quadratic forms

Lemma 2.1. *Each positive-definite binary quadratic form of discriminant d has an equivalent form*

$$F_A(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$$

with $a_{11}, a_{12}, a_{22} \in \mathbb{Z}$ and $2|a_{12}| \leqslant a_{11} \leqslant 2\sqrt{d/3}$.

Proof. Let $B = (b_{ij})_{i,j=1,2}$ be a symmetric matrix in $M_2(\mathbb{Z})$ with the quadratic form $F_B(x_1, x_2) = b_{11}x_1^2 + 2b_{12}x_1x_2 + b_{22}x_2^2$ positive-definite and $d(F_b) = \det B = d$. Let a_{11} be the least positive integer represented by F_B. Then $F_B(r_1, r_2) = a_{11}$ for some $r_1, r_2 \in \mathbb{Z}$. Let $r = \gcd(r_1, r_2)$. Then

$$a_{11} \leqslant F_B\left(\frac{r_1}{r}, \frac{r_2}{r}\right) = \frac{F_B(r_1, r_2)}{r^2} = \frac{a_{11}}{r^2} \leqslant a_{11}$$

and thus $r = 1$. Hence, $r_1s_2 - r_2s_1 = 1$ for some $s_1, s_2 \in \mathbb{Z}$.

Let $t \in \mathbb{Z}$. Then

$$U = \begin{pmatrix} r_1 & s_1 + r_1t \\ r_2 & s_2 + r_2t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

It is easy to check that

$$U'BU = A := \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$$

where $a_{12} = a'_{12} + a_{11}t$ with $a'_{12} = b_{11}r_1s_1 + b_{12}(r_1s_2 + r_2s_1) + b_{22}r_ss_2$, and $a_{22} = F(s_1 + r_1t, s_2 + r_2t)$. Since $1 = r_1(s_2 + r_2t) - r_2(s_1 + r_1t)$, $s_1 + r_1t$ and $s_2 = r_2t$ are not all zero and thus $a_{22} \geqslant a_{11}$.

Now choose $t \in \mathbb{Z}$ with $|a_{12}| = |a'_{12} + a_{11}t| \leqslant a_{11}/2$. As $A \sim B$, we have $F_A(x_1, x_2) \sim F_B(x_1, x_2)$. Note that $a_{11}a_{22} - a_{12}^2 = \det A = \det B = d(F_B) = d$. Thus

$$a_{11}^2 \leqslant a_{11}a_{22} = d + a_{12}^2 \leqslant d + \frac{a_{11}^2}{4}$$

and hence $a_{11} \leqslant 2\sqrt{d/3}$. This ends the proof. $\square$

Theorem 2.1. *Each positive-definite binary quadratic form $F(x_1,x_2)$ of discriminant 1 is equivalent to $x_1^2+x_2^2$.*

Proof. By Lemma 2.1, $F(x_1,x_2)\sim a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2$ for some $a_{11},a_{12},a_{22}\in\mathbb{Z}$ with

$$a_{11}a_{22}-a_{12}^2=d(F)=1\ \text{ and }\ 2|a_{12}|\leqslant a_{11}\leqslant 2\sqrt{\frac{1}{3}}<2.$$

Thus $a_{11}=1$, $a_{12}=0$ and $a_{22}=1$. So $F\sim x_1^2+x_2^2$. □

3. Ternary quadratic forms

Lemma 3.1. *Let $A=(a_{ij})_{1\leqslant i,j\leqslant 3}$ be a symmetric matrix in $M_3(\mathbb{Z})$, and let F_A be the corresponding ternary quadratic form of discriminant $d=d(F_A)=\det A$. Let*

$$A^*=\begin{pmatrix} a_{11}a_{22}-a_{12}^2 & a_{11}a_{23}-a_{12}a_{13}\\ a_{11}a_{23}-a_{12}a_{13} & a_{11}a_{33}-a_{13}^2\end{pmatrix}.$$

Then

$$a_{11}F_A(x_1,x_2,x_3)=(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{A^*}(x_2,x_3)\tag{3.1}$$

and

$$d(G_{A^*})=\det A^*=a_{11}d,\tag{3.2}$$

where G_{A^*} is the binary quadratic form associated with A^*. Also, G_{A^*} is positive-definite if F_A is positive-definite.

Proof. We can verify (3.1) and (3.2) directly.

Now suppose that F_A is positive-definite. Then $a_{11}=F_A(1,0,0)>0$. If $G_{A*}(x_2,x_3)\leqslant 0$ with $x_2,x_3\in\mathbb{Z}$, then for $x_1=-(a_{12}x_2+a_{13}x_3)$ we have

$$\begin{aligned}&a_{11}F_A(x_1,a_{11}x_2,a_{11}x_3)\\ =&(a_{11}x_1+a_{12}(a_{11}x_2)+a_{13}(a_{11}x_3))^2+G_{A^*}(a_{11}x_2,a_{11}x_3)\\ =&a_{11}0^2+a_{11}^2G_{A^*}(x_2,x_3)\leqslant 0\end{aligned}$$

and hence $x_1=x_2=x_3=0$. Therefore G_{A^*} is positive-definite. □

Lemma 3.2. *Each positive-definite ternary quadratic form of discriminant d is equivalent to a ternary quadratic form $\sum_{i=1}^{3}\sum_{j=1}^{3} a_{ij}x_ix_j$ with $a_{ij} = a_{ji}$ for which*

$$2\max\{|a_{12}|, |a_{13}|\} \leqslant a_{11} \leqslant \frac{4}{3}\sqrt[3]{d}.$$

Proof. Let $F_C(x_1, x_2, x_3)$ be a positive-definite ternary quadratic form with $C = (c_{ij})_{1\leqslant i,j\leqslant 3}$ a symmetric matrix in $M_3(\mathbb{Z})$ and $d(F_c) = \det C = d$. Let a_{11} denote the least positive integer represented by F_C. Then $F_C(u_{11}, u_{21}, u_{31}) = a_{11}$ for some $u_{11}, u_{21}, u_{31} \in \mathbb{Z}$. For $u = \gcd(u_{11}, u_{21}, u_{31})$, we have

$$a_{11} \leqslant F\left(\frac{u_{11}}{u}, \frac{u_{21}}{u}, \frac{u_{31}}{u}\right) = \frac{a_{11}}{u^2} \leqslant a_{11}$$

and hence $u = 1$.

Let $a = \gcd(u_{11}, u_{21})$. Then there are $u_{12}, u_{22} \in \mathbb{Z}$ such that

$$u_{11}u_{22} - u_{21}u_{12} = a.$$

Since $\gcd(a, u_{31}) = u = 1$, there are $u_{33}, b \in \mathbb{Z}$ such that

$$au_{33} - bu_{31} = 1.$$

Define

$$U = (u_{ij})_{1\leqslant i,j\leqslant 3} = \begin{pmatrix} u_{11} & u_{12} & bu_{11}/a \\ u_{21} & u_{22} & bu_{21}/a \\ u_{31} & 0 & u_{33} \end{pmatrix}.$$

It is easy to check that $\det U = 1$. So $U \in \mathrm{SL}_3(\mathbb{Z})$. Write

$$B := U'CU = (b_{ij})_{1\leqslant i,j\leqslant 3}.$$

Then $F_B \sim F_C$ and $d(F_B) = d(F_c) = d$. Note that

$$b_{11} = \sum_{j,k=1}^{n} u_{j1}c_{jk}u_{k1} = F_C(u_{11}, u_{21}, u_{31}) = a_{11}.$$

By Lemma 3.1,

$$a_{11}F_B(x_1, x_2, x_3) = (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + G_{B^*}(x_2, x_3)$$

with G_{B^*} a binary quadratic form of discriminant $a_{11}d$. Since F_B is positive-definite, so is G_{B^*} by Lemma 3.1. In view of Lemma 2.1, $G_{B^*}(x_2,x_3)$ is equivalent to certain

$$G_{\hat{A}}(x_2,x_3)=\hat{a}_{11}x_2^2+2\hat{a}_{12}x_2x_3+\hat{a}_{22}x_3^2$$

with

$$2|\hat{a}_{12}|\leqslant\hat{a}_{11}\leqslant 2\sqrt{\frac{a_{11}d}{3}}.$$

As $\hat{A}\sim B$, we have $\hat{A}=\hat{V}'B\hat{V}$ for some $V=(\hat{v}_{ij})_{1\leqslant i,j\leqslant 3}\in \mathrm{SL}_2(\mathbb{Z})$.

Let $r,s\in\mathbb{Z}$ and set

$$V_{r,s}=(v_{ij})_{1\leqslant i,j\leqslant 3}=\begin{pmatrix}1&r&s\\0&\hat{v}_{11}&\hat{v}_{12}\\0&\hat{v}_{21}&\hat{v}_{22}\end{pmatrix}\in \mathrm{SL}_3(\mathbb{Z}).$$

Define $A_{r,s}=V_{r,s}'BV_{r,s}$. It is easy to see that the $(1,1)$-entry of $A_{r,s}$ is $b_{11}=a_{11}$. Write $A_{r,s}=(a_{ij})_{1\leqslant i,j\leqslant 3}$.

Let $x=(x_1,x_2,x_3)$ and $y=(y_1,y_2,y_3)=xV_{r,s}'$. Then

$$y_2=v_{21}x_1+v_{22}x_2+v_{23}x_3=0x_1+\hat{v}_{11}x_2+\hat{v}_{12}x_3$$

and

$$y_3=v_{31}x_1+v_{32}x_2+v_{33}x_3=0x_1+\hat{v}_{21}x_2+\hat{v}_{22}x_3.$$

It follows that

$$G_{B^*}(y_2,y_3)=G_{\hat{V}'B\hat{V}}(x_2,x_3)=G_{\hat{A}}(x_2,x_3).$$

We also have

$$\sum_{j=1}^3 a_{1j}x_j=\sum_{j=1}^3\left(\sum_{i=1}^3 b_{1i}v_{ij}\right)x_j=\sum_{i=1}^3 b_{1i}\sum_{j=1}^3 v_{ij}x_j=\sum_{i=1}^3 b_{1i}y_i$$

and

$$F_{A_{r,s}}(x_1,x_2,x_3)=xA_{r,s}x'=xV_{r,s}'BV_{r,s}x'=yBy'=F_B(y_1,y_2,y_3).$$

Thus, in light of Lemma 3.1, we obtain

$$\begin{aligned}&(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{A^*_{r,s}}(x_2,x_3)\\ =&a_{11}F_{A_{r,s}}(x_1,x_2,x_3)=b_{11}F_B(y_1,y_2,y_3)\\ =&(b_{11}y_1+b_{12}y_2+b_{13}y_3)^2+G_{B^*}(y_2,y_3)\\ =&(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{\hat{A}}(x_2,x_3)\end{aligned}$$

and hence $A^*_{r,s}=\hat{A}$. In view of this and Lemma 3.1,

$$\begin{aligned}\hat{a}_{11}=&a_{11}a_{22}-a_{12}^2,\\ \hat{a}_{12}=&a_{11}r+b_{12}\hat{v}_{11}+b_{13}\hat{v}_{21},\\ \hat{a}_{13}=&a_{11}s+b_{12}\hat{v}_{12}+b_{13}\hat{v}_{22}.\end{aligned}$$

Choose $r,s\in\mathbb{Z}$ such that $|a_[12|\leqslant a_{11}/2$ and $|a_{13}|\leqslant a_{11}/2$, and write $A_{r,s}$ as A. Then

$$a_{22}=F_A(0,1,0)\geqslant a_{11}$$

and hence

$$a_{11}^2\leqslant a_{11}a_{22}=\hat{a}_{11}+a_{12}^2\leqslant 2\sqrt{\frac{a_{11}d}{3}}+\Big(\frac{a_{11}}{2}\Big)^2.$$

It follows that $a_{11}\leqslant\frac{4}{3}\sqrt[3]{d}$. This ends the proof. □

Theorem 3.1. *Any positive-definite ternary quadratic form $F(x_1,x_2,x_3)$ with discriminant one is equivalent to $x_1^2+x_2^2+x_3^2$.*

Proof. By Lemma 3.2, F is equivalent to certain $F_A(x_1,x_2,x_3)=\sum_{i,j=1}^3 a_{ij}x_ix_j$ with $A=(a_{ij})_{1\leqslant i,j\leqslant 3}\in M_3(\mathbb{Z})$ symmetric and

$$2\max\{|_{12}|,|a_{13}|\}\leqslant a_{11}\leqslant\frac{4}{3}.$$

Clearly, $a_{12}=a_{13}=0$. Since $\det A=d(F)=1\neq 0$, we have $a_{11}\neq 0$ and hence $a_{11}=1$. Let

$$A_*=\begin{pmatrix}a_{22}&a_{23}\\ a_{23}&a_{33}\end{pmatrix}.$$

Then $\det A_* = \det A = 1$ and hence $A_* \in \mathrm{SL}_2(\mathbb{Z})$. Since F_A is positive-definite,

$$a_{22} = \det\begin{pmatrix} 1 & 0 \\ 0 & a_{22}\end{pmatrix} = \det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}\end{pmatrix} > 0.$$

Now we see that F_{A_*} is positive-definite with discriminant one. By Theorem 2.1, $F_{A_*} \sim x_1^2 + x_2^2$, i.e., for some

$$U_* = \begin{pmatrix} u_{22} & u_{23} \\ u_{23} & u_{33}\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

we have

$$U_*' A_* U_* = I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}.$$

Set

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u_{22} & u_{23} \\ 0 & u_{23} & u_{33}\end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z}).$$

Then $U'AU = I_3$ and thus $A \sim I_3$. Therefore

$$F(x_1,x_2,x_3) \sim F_A(x_1,x_2,x_3) \sim F_{I_3}(x_1,x_2,x_3) = x_1^2 + x_2^2 + x_3^2.$$

This concludes the proof. □

4. Proof of the Three-Square Theorem

Lemma 4.1. *Let $n > 1$ and $d > 0$ be integers with $-d$ a quadratic residue modulo $dn - 1$. Then $n = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$.*

Proof. By the condition, there are $a_{11}, a_{12} \in \mathbb{Z}$ such that

$$a_{12}^2 + d = a_{11}(dn-1) = a_{11}a_{22},$$

where $a_{22} = dn - 1 \geqslant 2d - 1 > 0$. As $d > 0$ we must have $a_{11} > 0$. For

$$A = \begin{pmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n\end{pmatrix},$$

we have

$$\det A = 1 \times \begin{vmatrix} a_{12} & 1 \\ a_{22} & 0\end{vmatrix} + n \times \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22}\end{vmatrix} = -a_{22} + dn = 1.$$

Now F_A is positive-definite and of discriminant one. By Theorem 3.1, $F_A(x_1,x_2,x_3) \sim x_1^2+x_2^2+x_3^2$. Since $n = F_A(0,0,1)$ is represented by $F_A(x_1,x_2,x_3)$, n is also represented by $x_1^2+x_2^2+x_3^2$. We are done. $\square$

Proof of the "if" part of the Three-Square-Theorem. Clearly $1 = 1^2+0^2+0^2$. Let $n>1$ be an integer not of the form $4^k(8l+7)$ $(k,l \in \mathbb{N})$. We want to prove that n can be written as the sum of three squares.

Case 1. $n \equiv 2 \pmod 4$.

As $\gcd(4n, n-1) = 1$, by Dirichlet's theorem there is a positive integer j such that $p = 4nj+n-1 = (4j+1)n-1$ is prime. Let $d = 4j+1$. Then $p = dn-1 \equiv 1 \pmod 4$ and hence

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

So $-d$ is a quadratic residue modulo $p = dn-1$. Applying Lemma 4.1, we see that n can be written as the sum of three squares.

Case 2. $2 \nmid n$ and $n \not\equiv 7 \pmod 8$.

Let $c = 2+(-1)^{(n-1)/2}$. Then $c \equiv -n \pmod 4$ and $(cn-1)/2 \equiv 1 \pmod 2$. Note that

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

By Dirichlet's theorem, $p = 4nj + (cn-1)/2$ is prime for some positive integer j. Let $d = 8j+c$. Then $2p = dn-1$ and thus

$$\begin{aligned}\left(\frac{-d}{p}\right) =& (-1)^{\frac{p-1}{2}}(-1)^{\frac{d-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{d}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d+1}{2}}\left(\frac{2}{d}\right)\left(\frac{2p}{d}\right)\\ =& (-1)^{\frac{p-1}{2}\cdot\frac{c+1}{2}}(-1)^{\frac{c-1}{2}}\left(\frac{dn-1}{d}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{c+1}{2}}(-1)^{\frac{c-1}{2}} = 1.\end{aligned}$$

So there is an integer x_0 with $x_0^2+d \equiv 0 \pmod p$. Choose $x \in \{x_0, x_0+p\}$ such that $x^2+d \equiv 0 \pmod{2p}$. Then $-d$ is a quadratic residue modulo $2p = dn-1$. Applying Lemma 4.1 we see that $n \in \{x^2+y^2+z^2 : x,y,z \in \mathbb{Z}\}$.

Case 3. $4 \mid n$.

Write $n = 4^k n_0$ with $k, n_0 \in \{1, 2, 3, \dots\}$ and $4 \nmid n_0$. Then $n_0 \not\equiv 7 \pmod 8$. By our discussions in cases 1 and 2, $n_0 = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$, and hence

$$n = (2^k x)^2 + (2^k y)^2 + (2^k z)^2.$$

Combining the above, we have completed the proof. □

5. Another proof via Legendre's theorem

Legendre's Theorem. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ be squarefree and pairwise coprime. Suppose that a, b, c don't have the same sign. Then*

$$\begin{aligned} &ax^2 + by^2 + cz^2 = 0 \text{ for some } x, y, z \in \mathbb{Z} \text{ not all zero} \\ \iff &-bc \ R \ a,\ -ac \ R \ b \text{ and } -ab \ R \ c, \end{aligned}$$

where $r \ R \ m$ means that r is a quadratic residue modulo m.

Proof. $\Rightarrow$: Suppose that $ax^2 + by^2 + cz^2 = 0$ for some integers x, y, z not all zero. Let $d = \gcd(x, y, z)$. Then $a(x/d)^2 + b(y/d)^2 + c(z/d)^2 = 0$ with $\gcd(x/d, y/d, z/d) = 1$. Without loss of generality we simply assume that $d = 1$. If p is a prime dividing both c and y, then p divides $ax^2 = -by^2 - cz^2$ and hence $p \mid x$ since $\gcd(a, c) = 1$, thus p^2 divides $cz^2 = -ax^2 - by^2$ and hence $p \mid z$ (since c is squarefree), so p divides $\gcd(x, y, z) = 1$ which leads a contradiction. As $(ax)^2 \equiv -aby^2 \pmod c$ and $\gcd(y, c) = 1$, we have $-ab \ R \ c$. Similarly, $-bc \ R \ a$ and $-ac \ R \ b$.

$\Leftarrow$: Since $-bc \ R \ a$, $u^2 \equiv -bc \pmod a$ for some $u \in \mathbb{Z}$, and hence

$$ax^2+by^2+cz^2 \equiv b^{-1}(b^2y^2+bcz^2) = b^{-1}(b^2y^2-u^2z^2) = (y-b^{-1}uz)(by+uz) \pmod a.$$

So there are $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}$ such that

$$ax^2 + by^2 + cz^2 \equiv (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z) \pmod a.$$

Similarly, there are $a_3, b_3, c_3, a_4, b_4, c_4, a_5, b_5, c_5, a_6, b_6, c_6 \in \mathbb{Z}$ such that

$$ax^2 + by^2 + cz^2 \equiv (a_3x + b_3y + c_3z)(a_4x + b_4y + c_4z) \pmod b$$

and

$$ax^2+by^2+cz^2 \equiv (a_5x+b_5y+c_5z)(a_6x+b_6y+c_6z) \pmod{c}.$$

As a,b,c are pairwise coprime, by the Chinese Remainder Theorem there are $A_1,B_1,c_1,A_2,B_2,C_2\in\mathbb{Z}$ such that

$$ax^2+by^2+cz^2 \equiv (A_1x+B_1y+C_1z)(A_2x+B_2y+C_2z) \pmod{abc}.$$

(For example, we may choose $A_1\in\mathbb{Z}$ such that $A_1\equiv a_1 \pmod{a}$, $A_1\equiv a_3 \pmod{b}$ and $A_1\equiv a_5 \pmod{c}$.)

As a,b,c don't have the same sign. Without loss of generality we simply assume that $a\geqslant b>0>c$. If $|abc|=1$, then $a=b=1$ and $c=-1$. Obviously $x^2+y^2-z^2=0$ for some integers x,y,z not all zero. Below we assume that $|abc|>1$.

If the squarefree numbers $|bc|,|ac|,|ab|$ are all squares, then $|bc|=|ac|=|ab|=1$ which contradicts $|abc|>1$. Thus

$$\lceil\sqrt{|bc|}\rceil\lceil\sqrt{|ac|}\rceil\lceil\sqrt{|ab|}\rceil > \sqrt{|bc|}\sqrt{|ac|}\sqrt{|ab|}=|abc|.$$

By the Pigeon-hole Principle, two of the numbers

$$A_1x+B_1y+C_1z \ (0\leqslant x<\lceil\sqrt{|bc|}\rceil,\ 0\leqslant y<\lceil\sqrt{|ac|}\rceil\ 0\leqslant z\leqslant\lceil\sqrt{|ab|}\rceil)$$

are congruent modulo abc. So, there are integers x,y,z not all zero for which

$$|x|<\sqrt{|bc|},\ |y|<\sqrt{|ac|},\ |z|<\sqrt{|ab|}$$

and

$$A_1x+B_1y+C_1z\equiv 0 \pmod{abc}.$$

Now,

$$ax^2+by^2+cz^2 \equiv (A_1x+B_1y+C_1z)(A_2x+B_2y+C_2z)\equiv 0 \pmod{abc}$$

and

$$-|abc|=abc<cz^2\leqslant ax^2+by^2+cz^2\leqslant ax^2+by^2<a|bc|+b|ac|=2|abc|.$$

So $ax^2+by^2+cz^2$ is 0 or $|abc|=-abc$. If $ax^2+by^2+cz^2=-abc$, then $ax^2+by^2+c(z^2+ab)=0$ and hence

$$0=(ax^2+by^2)(z^2+ab)+c(z^2+ab)^2=a(xz+by)^2+b(yz-ax)^2+c(z^2+ab)^2$$

with $z^2+ab>0$. This ends the proof. $\square$

Lemma 5.1. *Suppose that n is a positive integer which can be written as the sum of three squares of rational numbers. Then $n \in \{x^2+y^2+z^2 : x,y,z\in\mathbb{Z}\}$.*

Proof. (Aubry) By the condition, there is a rational point $a=(a_1,a_2,a_3)$ on the sphere $x^2+y^2+z^2=n$. Take such a point $a=(a_1,a_2,a_3)$ with the common denominator d of the rationals a_1,a_2,a_3 minimal. It suffices to show that $d=1$.

Suppose that $d>1$. Take $a'=(a_1',a_2',a_3')\in\mathbb{Z}^3$ with $|a_i-a_i'|\leqslant 1/2$ for all $i=1,2,3$. The distance between the points a and a' (or the norm of $a-a'$) is given by

$$\|a-a'\|=\sqrt{(a_1-a_1')^2+(a_2-a_2')^2+(a_3-a_3')^2}\leqslant\sqrt{\frac{3}{4}}=\frac{\sqrt{3}}{2}<1.$$

Note that $A_i:=da_i\in\mathbb{Z}$ for all $i=1,2,3$ and

$$\sum_{i=1}^3(A_i-da_i')^2\equiv\sum_{i=1}^3A_i^2=d^2n\equiv 0\pmod d.$$

Write $\sum_{i=1}^3(A_i-da_i')^2=dd'$ with $d'\in\mathbb{Z}$. Then

$$0<\|a-a'\|^2=\frac{1}{d^2}\sum_{i=1}^3(A_i-da_i')^2=\frac{d'}{d}$$

and hence $1\leqslant d'<d$.

Let $A=(A_1,A_2,A_3)=(da_1,da_2,da_3)\in\mathbb{Z}^3$. The line $l=\{P_\lambda=a'+\lambda(A-da'):\ \lambda\in\mathbb{R}\}$ passes the points a' and $a=a'+\frac{1}{d}(A-da')$. If P_λ is an intersection point of the line l and the sphere, then

$$(a_1'+\lambda(A_1-da_1'))^2+(a_2'+\lambda(A_2-da_2'))^2+(a_3'+\lambda(A_3-da_3'))^2=n,$$

i.e.,

$$\|a'\|^2-n+2\lambda(a'\cdot A-d\|a'\|^2)+\|A-da'\|^2\lambda^2=0,\qquad(5.1)$$

where $a'\cdot A:=a_1'A_1+a_2'A_2+a_3'A_3$. Note that $\|A-da'\}\neq 0$ since $a\neq a'$. As a is an intersection point of the line l with the sphere, $\lambda=1/d$ is a root

of the equation (5.1). Let P_{λ_0} be another intersection point of the line l and the sphere. Then

$$\frac{1}{d}\lambda_0 = \frac{\|a'\|^2 - n}{\|A - da'\|^2} = \frac{\|a'\|^2 - n}{dd'}$$

and thus $\lambda_0 = (\|a'\|^2 - n)/d'$. Note that the common denominator of all the three coordinates of the point P_{λ_0} is at most $d' < d$. This contradicts the choice of d.

In view of the above, we have completed the proof of Lemma 5.1. □

Another Proof of the Three-Square Theorem. Let n be a positive integer not of the form $4^k(8l+7)$ $(k, l \in \mathbb{N})$. We may write n as $4^k a^2 m$, where $k \in \mathbb{N}$, $a, m \in \mathbb{Z}^+$, a is odd and m is squarefree. Note that $m \equiv a^2 m \not\equiv 7 \pmod 8$. If $m = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$, then $n = (2^k ax)^2 + (2^k ay)^2 + (2^k az)^2$. So it suffices to show that the squarefree number $m \not\equiv 7 \pmod 8$ can be written as the sum of three squares.

Write $m = 2^\alpha m_1$ with $\alpha \in \{0, 1\}$ and $2 \nmid m_1$. By the Chinese Remainder Theorem and Dirichlet's theorem, there is a prime p for which $p \equiv -2^\beta \pmod{m_1}$ and $p \equiv 3 + 2(-1)^{(m_1+1)/2} \pmod 4$, where

$$\beta = \begin{cases} 1 & \text{if } \alpha = 0 \text{ and } m_1 \equiv 3 \pmod 8, \\ 0 & \text{if } \alpha = 1 \text{ or } (\alpha = 0 \ \&\ m_1 \equiv 1 \pmod 4). \end{cases}$$

Set $r = 2^\beta p$. As $p \equiv 1 \pmod 4$, r can be written as the sum of two squares. Clearly, $\gcd(r, m_1) = 1$ and

$$\left(\frac{m}{p}\right) = \left(\frac{2}{p}\right)^\alpha \left(\frac{m_1}{p}\right) = \left(\frac{2^\alpha}{p}\right)\left(\frac{p}{m_1}\right) = \left(\frac{2^\alpha}{p}\right)\left(\frac{-2^\beta}{m_1}\right) = 1.$$

So, m is a quadratic residue modulo p and also a quadratic residue modulo $r = 2^\beta p$. (If $\beta = 1$ and $x^2 \equiv m \pmod p$, then the odd number in $\{x, x+p\}$ is a quadratic residue modulo $r = 2p$.) If $\alpha = 1$, then $\beta = 0$ and $2 \nmid r$. Thus $-r$ is a quadratic residue modulo 2^α. For any prime divisor q of m_1, we have

$$\left(\frac{-r}{q}\right) = \left(\frac{-2^\beta p}{q}\right) = \left(\frac{(-2^\beta)^2}{q}\right) = 1$$

since $p \equiv -2^\beta \pmod q$. Therefore, $-r$ is a quadratic residue modulo $m = 2^\alpha m_1$.

As m and r are squarefree, m is a quadratic residue modulo r and $-r$ is a quadratic residue modulo m, by Legendre's theorem there are integers x, y, z not all zero with $mx^2 - y^2 - rz^2 = 0$. If $x = 0$, then obviously $y = z = 0$. So $x \neq 0$ and

$$m = \left(\frac{y}{x}\right)^2 + r\left(\frac{z}{x}\right)^2.$$

Since $r = r_1^2 + r_2^2$ for some $r_1, r_2 \in \mathbb{Z}$, we see that m is the sum of three squares of rational numbers. Applying Lemma 5.1, we get $m \in \{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{Z}\}$. This concludes our proof. $\square$

6. Some Applications of the Three-Square-Theorem

For positive integers a, b, c, we define

$$E(a, b, c) = \mathbb{N} \setminus \{ax^2 + by^2 + cz^2 : \ x, y, z \in \mathbb{Z}\}.$$

The Three-Square Theorem indicates that

$$E(1, 1, 1) = \{4^k(8l + 7) : \ k, l \in \mathbb{N}\}.$$

Theorem 6.1. *We have*

$$E(1, 1, 2) = E(1, 2, 4) = \{4^k(16l + 14) : \ k, l \in \mathbb{N}\}.$$

Proof. For any $n \in \mathbb{N}$, clearly

$$n = x^2 + y^2 + 2z^2 \iff 2n = (x + y)^2 + (x - y)^2 + (2z)^2.$$

Suppose that $2n = u^2 + v^2 + w^2$ for some $u, v, w \in \mathbb{Z}$. If there is a unique even number among u, v, w, without loss of generality we may assume that $2 \mid w$ and $2 \nmid uv$, hence

$$n = \left(\frac{u + v}{2}\right)^2 + \left(\frac{u - v}{2}\right)^2 + 2\left(\frac{w}{2}\right)^2$$

with

$$\frac{u + v}{2} \cdot \frac{u - v}{2} = \frac{u^2 - v^2}{4} \equiv 0 \pmod 2.$$

If u, v, w are all even, then two of them, say u and v, are congruent modulo 4, and thus

$$n = \left(\frac{u+v}{2}\right)^2 + 4\left(\frac{u-v}{4}\right)^2 + 2\left(\frac{w}{2}\right)^2.$$

By the above,

$$\begin{aligned} E(1,1,2) =& E(1,2,4) = \{n \in \mathbb{N} :\ 2n \notin E(1,1,1)\} \\ =& \{n \in \mathbb{N} :\ 2n = 4^{k+1}(8l+7) \text{ for some } k, l \in \mathbb{N}\} \\ =& \{4^k(16l+14) :\ k, l \in \mathbb{N}\}. \end{aligned}$$

This concludes the proof. □

Remark 6.1. By Theorem 6.1, any positive odd number can be written as $x^2 + 2y^2 + 4z^2$ with $x, y, z \in \mathbb{Z}$. It is also known that any positive odd integer can be written as $x^2 + 2y^2 + 3z^2$ with $x, y, z \in \mathbb{Z}$ and furthermore

$$E(1,2,3) = \{4^k(16l+10) :\ k, l \in \mathbb{N}\}.$$

There are totally 102 regular diagular form $ax^2 + by^2 + cz^2$ with $1 \leqslant a \leqslant b \leqslant c$ and $\gcd(a,b,c) = 1$ for which $E(a,b,c)$ is completely determined (cf. [D39, pp. 112-113]). For example,

$$\begin{aligned} E(1,1,5) =& \{4^k(8l+3) :\ k, l \in \mathbb{N}\}, \\ E(1,2,6) =& \{4^k(8l+5) :\ k, l \in \mathbb{N}\}, \\ E(1,1,6) =& \{9^k(9l+3) :\ k, l \in \mathbb{N}\}. \end{aligned}$$

Those integers $T_x = x(x+1)/2$ with $x \in \mathbb{Z}$ are called *triangular numbers.*

Theorem 6.2. (Conjectured by Fermat and proved by Gauss) *Any $n \in \mathbb{N}$ can be written as the sum of three triangular numbers.*

Proof. By the Three-Square Theorem, $8n + 3 = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$. It is easy to see that x, y, z must be all odd. Write $x = 2u+1$, $y = 2v+1$ and $z = 2w+1$ with $u, v, w \in \mathbb{Z}$. Then

$$8n+3 = (2u+1)^2+(2v+1)^2+(2w+1)^2 = (8T_u+1)+(8T_v+1)+(8T_w+1)$$

and hence $n = T_u + T_v + T_w$. □

The following result can be found in L. E. Dickson [D99].

Theorem 6.3. (i) (Euler) *Each $n\in\mathbb{N}$ can be written as $x^2+y^2+T_z$ with $x,y,z\in\mathbb{Z}$.*

(ii) (Conjectured by Lionnet and proved by Lebesgue and Réalis in 1872) *Each $n\in\mathbb{N}$ can be written as $x^2+T_y+T_z$ with $x,y,z\in\mathbb{Z}$.*

Proof. (i) By the Three-Square Theorem, we can write $8n+1=u^2+v^2+w^2$ with $u,v,w\in\mathbb{Z}$. It is easy to see that there is a unique odd number among u,v,w. Without loss of generality, we assume that $u=2x$, $v=2y$ and $w=2z+1$ with $x,y,z\in\mathbb{Z}$. As $4(x^2+y^2)=8n+1-(2z+1)^2\equiv 0\pmod 8$, we have $x\equiv y\pmod 2$. Thus

$$n=\frac{(2x)^2+(2y)^2}{8}+\frac{(2z+1)^2-1}{8}=\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+T_z.$$

(ii) As observed by Euler (cf. [D99]),

$$\begin{aligned}&m\in\{T_y+T_z:\ y,z\in\mathbb{Z}\}\\ \iff&4m+1\in\{(y+z+1)^2+(y-z)^2:\ y,z\in\mathbb{Z}\}\\ \iff&4m+1\in\{u^2+v^2:\ u,v\in\mathbb{Z}\text{ and }u\not\equiv v\pmod 2\}\\ \iff&4m+1\in\{(2y)^2+(2z+1)^2:\ y,z\in\mathbb{Z}\}\\ \iff&m\in\{y^2+2T_z:\ y,z\in\mathbb{Z}\}.\end{aligned}$$

On the other hand, By the Three-Square Theorem there are $x,y,z\in\mathbb{Z}$ such that $4n+1=(2x)^2+(2y)^2+(2z+1)^2$ and hence $n=x^2+y^2+2T_z$. Therefore, n can be written as the sum of a square and two triangular numbers. □

Remark 6.2. In 1939, B. W. Jones and G. Pall [JP] showed that $8n+1$ with $n\in\mathbb{N}$ can be written as $32x^2+8y^2+z^2$ with $x,y,z\in\mathbb{Z}$. It follows that each $n\in\mathbb{N}$ can be written as the sum of a square, an even square and a triangular number. In 2007, Z.-W. Sun [S07] proved that any $n\in\mathbb{N}$ can be written as the sum of an even square and two triangular numbers; He conjectured, and proved with B.-K. Oh [OS] in 2009 that any positive integer can be written as the sum of a square, an odd square and a triangular number.

References

[D39] L. E. Dickson, *Modern Elementary Theory of Numbers*, University of Chicago Press, Chicago, 1939.

[D99] L. E. Dickson, *History of the Theory of Numbers,* Vol. II, AMS Chelsea Publ., 1999.

[JP] B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. **70** (1939), 165–191.

[N96] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Grad. Texts in Math., Vol. 164, Springer, New York, 1996.

[OS] B.-K. Oh and Z.-W. Sun, *Mixed sums of squares and triangular numbers (III)*, J. Number Theory **129** (2009), 964–969.

[P] P. Pollack, *Not Always Buried Deep – A Second Course in Elementary Number Theory*, Amer. math. Soc., Providence, RI, 2009.

[S07] Z.-W. Sun, *Mixed sums of squares and triangular numbers*, Acta Arith. **127** (2007), 103–113.