SUM OF THREE SQUARES

JIANG ZIHANG

Abstract. We are going to follow following theorems one by one to prove our goal.
1. law of quadratic reciprocity:
for p and q odd prime numbers, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

2. Dirichlet's theorem on arithmetic progressions:
For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is a non-negative integer.

3. Every positive-definite binary (or ternary) quadratic form of discriminant 1 is equivalent to the form

$$x_1^2 + x_2^2 \ (or\ x_1^2 + x_2^2 + x_3^2)$$

4. Let $n \geq 2$. If there exists a positive integer d' such that $-d'$ is a quadratic residue modulo $d'n-1$, then n can be represented as **the sum of three squares**.
5. A positive integer n can be represented as **the sum of three squares** if and only if n is not of the form

$$n = 4^a(8k + 7)$$

6. (Davenport-Cassels) Assume

$$f(X) = \sum_{p}^{i,j=1} a_{ij}X_iX_j$$

is positive-definite quadratic form with $a_{ij} \in \mathbb{Z}$, we also assume that for all $x = (x_1, x_2, ..., x_p) \in \mathbb{Q}^p$, we have $y \in \mathbb{Z}^p$ s.t.

$$f(x - y) < 1$$

Then if f can represent $n \in \mathbb{Z}$ in $\mathbb{Q}$,it can also represent n in $\mathbb{Z}$.

1. Notation

$$\textit{Legendre symbol}: \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

2. Introduction

Let's view the problem through another point of view:

In number theory, natural density (or asymptotic density) is one of the posibility to measure how large a subset of the set of natural numbers is.

Let A be a subset of the set of natural numbers $\mathbb{N} = \{1, 2, \ldots\}$ For any $n \in \mathbb{N}$,put $A(n) = \{1, 2, \ldots, n\} \cap A$ and $a(n) = |A(n)|$.

Define the upper asymptotic density $\overline{d}(A)$ of A by

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{a(n)}{n}$$

Similarly, $\underline{d}(A)$, the lower asymptotic density of A, is defined by

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{a(n)}{n}$$

One may say A has asymptotic density $d(A)$ if $\underline{d}(A) = \overline{d}(A)$, in which case $d(A)$ is equal to this common value.

This definition can be restated in the following way:

$$d(A) = \lim_{n\to\infty} \frac{a(n)}{n} d(A) = \lim_{n\to\infty} \frac{a(n)}{n}$$

if the limit exists.

An interesting fact:

Square-free integers has density

$$d(SFI) = \frac{6}{\pi^2}$$

Hint:For any p, consider integer $p^2|n$ can be rewrite as $n = p^2k$,we know there are $\frac{1}{p^2}$ integers in all that satisfy $p^2|n$, and this, for each p is independent event.i.e.

$$d(SFI) = \prod_p (1 - \frac{1}{p^2}) = \prod_p \frac{1}{1 + \frac{1}{p^2} + \ldots + \frac{1}{p^{2k}} + \ldots} = \frac{1}{\sum_{k=1}^{\infty} \frac{1}{k^2}} = \frac{6}{\pi^2}$$

Now we go back to our squares.

Density of squares:

$$d(\mathscr{B}^2) = \lim_{n\to\infty} \frac{\sqrt{n}}{n} = 0$$

And by Landou-Ramanujan, we have:

$$d(\mathscr{B}^2 \bigoplus \mathscr{B}^2) = \lim_{n\to\infty} \frac{c}{\sqrt{ln(n)}} = 0$$

where $c \approx 0.76422365358$

But by Lagrange,we have:

$$d(\mathscr{B}^2 \bigoplus \mathscr{B}^2 \bigoplus \mathscr{B}^2 \bigoplus \mathscr{B}^2) = 1$$

How does it change?

$$d(\mathscr{B}^2 \bigoplus \mathscr{B}^2 \bigoplus \mathscr{B}^2) =?$$

One the one hand,we consider it by mod 8: Since $p^2 \equiv 0, 1, 4 \ (mod\ 8)$, obviously, 7 can't be represented by sum of 3 squares.

Moreover, if

$$n = x^2 + y^2 + z^2 \equiv 0 \ (mod\ 4)$$

then all of them must be even, which means

$$\frac{n}{4} = \frac{x}{2}^2 + \frac{y}{2}^2 + \frac{z}{2}^2$$

This implies that all integer of form $n = 4^a(8k + 7)$ can't be represented.

Now, we can estimate the density of $\mathscr{B}^2 \bigoplus \mathscr{B}^2 \bigoplus \mathscr{B}^2$

$$d(\mathscr{B}^2 \bigoplus \mathscr{B}^2 \bigoplus \mathscr{B}^2) \leq 1 - \frac{1}{8} \times \frac{1}{1 - \frac{1}{4}} = \frac{5}{6}$$

In order to show it is exactly $\frac{5}{6}$, we have to show

$$n \equiv 1, 2, 3, 5, 6 \ (mod\ 8)$$

can be represented by sum of 3 squares.

Tool we need:law of quadratic reciprocity (Gauss),Dirichlet's Theorem.

Here we would give the prove of law of quadratic reciprocity,the other one will be referred to Zhang Sicong's report.

Law of Quadratic Reciprocity

Here we define the Legendre symbol in a seemingly different way. Later we'll check this is nothing but the former one.
Consider $x \in \mathbb{F}_p^*,\ p \neq 2$, then the Legendre symbol of x is

$$x^{\frac{p-1}{2}} (= \pm 1)$$

First, we prove that it is equivalent to the former one.

Proof. On the one hand, if $x^{\frac{p-1}{2}} = -1$ and $\exists y^2 = x$, then we have $y^{p-1} = 1$, a contradiction. That is to say $x^{\frac{p-1}{2}} = -1 \ \Rightarrow x$ is a quadratic non-residue modulo p.
On the other hand, if x is a quadratic non-residue modulo p,consider $a\dot{a}^{-1}x = x$, then we have $a \neq a^{-1}x$. Takeing it in pairs, we get $x^{\frac{p-1}{2}} = (p-1)! = -1$ □

Now for convenience, we denote $\left(\frac{0}{p}\right) = 0$ and $\epsilon(n) = \pm 1 \equiv \frac{n-1}{2} (mod\ 2)$. And there is some basic observation: $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$,$\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$, if x is inversible, $\left(\frac{x}{p}\right) = \left(\frac{x^{-1}}{p}\right)$

Theorem 2.1. *(Gauss) p,q are different odd prime numbers,the equation holds*

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

Proof. Consider Ω to be the algebra closure of $\mathbb{F}_p$, $\omega \in \Omega$ is the primitive root of order q in Ω. Then $\omega^q = 1$, in which case for all $x \in \mathbb{F}_p$ the definition of ω^x is well-defined.
Consider the Gauss sum:

$$y = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x$$

we claim the following two equation hold:

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

if these hold, we could immediately draw to a conclusion:

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

Proof of equations
1.

$$(-1)^{\epsilon(q)}y^2 = (-1)^{\epsilon(q)}\sum_{x,z\in\mathbb{F}_q}\left(\frac{xz}{q}\right)\omega^{x+z} = (-1)^{\epsilon(q)}\sum_{u\in\mathbb{F}_q}\omega^u\left(\sum_{t\in\mathbb{F}_q}\left(\frac{t(u-t)}{q}\right)\right)$$

While for $t=0$, $\left(\frac{t(u-t)}{q}\right)=0$, and for $t\neq 0$, $\left(\frac{t(u-t)}{q}\right)=\left(\frac{-t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right)=(-1)^{\epsilon(q)}\left(\frac{1-ut^{-1}}{q}\right)$

$$So,\ (-1)^{\epsilon(q)}y^2 = \sum_{u\in\mathbb{F}_q}\omega^u\left(\sum_{t\in\mathbb{F}_q^*}\left(\frac{1-ut^{-1}}{q}\right)\right) = q-1+\sum_{u\in\mathbb{F}_q^*}-\omega^u = q$$

2.

$$y^p = \sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^{xp} = \sum_{z\in\mathbb{F}_q}\omega^z\left(\frac{zp^{-1}}{q}\right) = \left(\frac{p^{-1}}{q}\right)\sum_{z\in\mathbb{F}_q}\omega^z\left(\frac{z}{q}\right) = y\left(\frac{p}{q}\right)$$

So by reducing y in both side we get the equation.

□

By this mean,we can also deal with the case $q=2$.We shall prove the following

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases}1 & p\equiv\pm1 \pmod 8,\\ -1 & p\equiv\pm3 \pmod 8.\end{cases}$$

Proof. Choose Ω as the closure of $\mathbb{F}_p$, α be one of the primitive root of order 8 in Ω.Then $\alpha^8=1, \alpha^4=-1$.Let

$$y=\alpha+\alpha^{-1}$$

Then $y^2=\alpha^2+\alpha^{-2}+2=2$, in the meanwhile,

$$y^p=\alpha^p+\alpha^{-p} = \begin{cases}\alpha+\alpha^{-1}=y & p\equiv\pm1 \pmod 8,\\ \alpha^5+\alpha^{-5}=-y & p\equiv\pm5 \pmod 8.\end{cases}$$

$$So, \left(\frac{2}{p}\right) = y^{p-1} = \begin{cases}1 & p\equiv\pm1 \pmod 8,\\ -1 & p\equiv\pm3 \pmod 8.\end{cases}$$

□

3. Main Lemma

Notation : we say two quadratic form F_A, F_B is equivalent if

$$\exists U \in SL_n(\mathbb{Z}) \ s.t. \ A = U^T BU$$

Here, F_A is the quadratic form generated by the matrix A.

Theorem 3.1. *Every positive-definite binary quadratic form of discriminant= 1 is equivalent to the form*

$$x_1^2 + x_2^2$$

In order to prove this,we give a generalized lemma.

Lemma 3.2. *Every equivalent class of positive-definite binary quadratic form of discriminant d contains at least one form*

$$F_A(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 \quad s.t. \ 2|a_{12}| \leq a_{11} \leq \frac{2}{\sqrt{3}}\sqrt{d}$$

Proof. Assume that $F_B(x_1, x_2) = b_{11}x_1^2 + 2b_{12}x_1x_2 + b_{22}x_2^2$, then $det(B) = b_{11}b_{22} - b_{12}^2$. Let a_{11} be the smallest positive integer represented by F_B (we can assume that $a_{11} = F_B(r_1, r_2)$).Obviously, $(r_1, r_2) = 1$, otherwise we can divide it to make a_{11} smaller. so

$$\exists s_1, s_2 \ s.t. \ r_1s_2 - r_2s_1 = 1 = r_1(s_2 + r_2t) - r_2(s_1 + r_1t) \ \forall t$$

That is:

$$\forall t \in \mathbb{Z}, U_t = \begin{pmatrix} r_1 & s_1 + r_1t \\ r_2 & s_2 + r_2t \end{pmatrix} \in SL_n(\mathbb{Z})$$

Let

$$A_t = U_t^T BU_t = \begin{pmatrix} F(r_1, r_2) & (\star) + F(r_1, r_2)t \\ (\star) + F(r_1, r_2)t & F(s_1 + r_1t, s_2 + r_2t) \end{pmatrix}$$

here,$(\star) = b_{11}r_1s_1 + b_{22}r_2s_2 + b_{12}(r_1s_1 + r_2s_2)$

Choose t to make $|a_{12}| = |(\star) + F(r_1, r_2)| \leq \frac{a_{11}}{2}$,since by definition of $a_{11}, F(s_1 + r_1t, s_2 + r_2t) \geq a_{11}$,thus,we have

$$d = a_{11}a_{22} - a_{12}^2 \geq a_{11}^2 - \frac{1}{4}a_{11}^2 \geq \frac{3}{4}a_{11}^2$$

So,$2|a_{12}| \leq a_{11} \leq \frac{2}{\sqrt{3}}d$ □

We say similarly, we have the theorem for ternary quadratic form.

Theorem 3.3. *Every positive-definite ternary quadratic form of discriminant= 1 is equivalent to the form*

$$x_1^2 + x_2^2 + x_3^2$$

In order to prove this,we also give a generalized lemma.

Lemma 3.4. *Every equivalent class of positive-definite binary quadratic form of discriminant d contains at least one form*

$$F_A(x_1,x_2,x_3)=\sum_{i,j=1}^{3}a_{ij}x_ix_j \quad s.t.\ 2max\{|a_{12}|,|a_{13}|\}\le a_{11}\le\frac{4}{3}\sqrt[3]{d}$$

Proof. Assume that $F_C(x_1,x_2,x_3)=\sum_{i,j=1}^{3}c_{ij}x_ix_j$, then again we let a_{11} be the smallest positive integer represented by F_C (we can assume that $a_{11}=F_C(u_{11},u_{21},u_{31})$).
Obviously, $(u_{11},u_{21},u_{31})=1$.

Here we'd give the another lemma:

Lemma 3.5. $\forall(u_{11},u_{21},u_{31})=1$, *we have a* $U\in SL_3(\mathbb{Z})$ *s.t. the first column of* U *is exactly* $(u_{11},u_{21},u_{31})^T$.

Proof. Denote $a=(u_{11},u_{21})$,then $\exists u_{12},u_{22}$ s.t. $u_{11}u_{22}-u_{21}u_{12}=a$, also since $(a,u_{31})=1$, $\exists u_{33},b$ s.t. $au_{33}-bu_{31}=1$.It is easy to check $\begin{pmatrix}u_{11}&u_{12}&\frac{u_{11}b}{a}\\u_{21}&u_{22}&\frac{u_{21}b}{a}\\u_{31}&0&u_{33}\end{pmatrix}\in SL_3(\mathbb{Z})$

□

Since we get the U we want, we can denote $B=U^TCU=(b_{ij})$, we can see that $b_{11}=F_C(u_{11},u_{21},u_{31})=a_{11}$, and $det(B)=det(C)=d$.Considering

$$b_{11}F_B(y_1,y_2,y_3)=(b_{11}y_1+b_{12}y_2+b_{13}y_3)^2+G_{B^*}(y_2,y_3)$$

$$\text{where } B^*=\begin{pmatrix}b_{11}b_{22}-b_{12}^2&b_{11}b_{23}-b_{12}b_{13}\\b_{11}b_{23}-b_{12}b_{13}&b_{11}b_{33}-b_{13}^2\end{pmatrix} \text{ and } det(B^*)=b_{11}d$$

So, how does the change of B^* influence B. We can see in the following lemma.

Lemma 3.0.1. $\forall\ V^*=(v_{ij}^*)\in SL_2(\mathbb{Z})$, *let* $A^*=(V^*)^TB^*V*$, *we say* $\forall\ r,s$, *Let* $V_{r,s}=\begin{pmatrix}1&r&s\\0&v_{11}^*&v_{12}^*\\0&v_{21}^*&v_{22}^*\end{pmatrix}$, *then for* $A_{r,s}=V_{r,s}^TBV^{r,s}$, *we have*

$a_{11}^{r,s}=b_{11}$ *and* $a_{11}F_{A_{r,s}}(x_1,x_2,x_3)=(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+G_{A^*}(x_2,x_3)$ *which is equivalent to say* $A_{r,s}^*=A^*$

Proof. Simply calculation can prove $A_{r,s}^*=A^*$

□

Now for the former B^*, since we have $det(B^*) = b_{11}d$, so we have a equivalent class

$$A^* = (V^*)^T BV^* \text{ s.t. } a_{11}^* \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}d}$$

That is to say in $A_{r,s}^* = A^*$, we have $a_{11}^{(rs)}a_{22}^{(rs)} - (a_{12}^{(rs)})^2 = a_{11}^* \ \forall r, s$
By computing

$$a_{12}^{(rs)} = a_{11}r + b_{12}v_{11}^* + b_{13}v_{21}^*, a_{13}^{(rs)} = a_{11}s + b_{12}v_{12}^* + b_{13}v_{22}^*$$

we know that we can make both of them smaller than $\frac{a_{11}}{2}$ by choosing r, s properly.Then,as

$a_{22}^{(rs)} = F_C(ru_{11}+v_{11}^*u_{12}+v_{21}^*u_{13}, ru_{21}+v_{11}^*u_{22}+v_{21}^*u_{23}, ru_{31}+v_{11}^*u_{32}+v_{21}^*u_{33}) \geq a_{11}$

we have

$$a_{11}^2 \leq a_{11}a_{22}^{(rs)} = a_{11}a_{22}^{(rs)} - (a_{12}^{(rs)})^2 + (a_{12}^{(rs)})^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}d} + \frac{a_{11}^2}{4}$$

That is $a_{11} \leq \frac{4}{3}\sqrt[3]{d}$

□

Main Lemma: Let $n \geq 2$. If there exists a positive integer d' such that $-d'$ is a quadratic residue modulo $d'n-1$, then n can be represented as **the sum of three squares**.

Proof. Since $-d' = a_{12}^2 - a_{11}(d'n-1)$, denoting $a_{22} = d'n-1$, we have $0 < d' = a_{11}a_{22} - a_{12}^2$.
Consider

$$A = \begin{pmatrix} a_{11} & a_{11} & 1 \\ a_{11} & a_{11} & 0 \\ 1 & 0 & n \end{pmatrix}, \ det(A) = n(a_{11}a_{22} - a_{12}^2) - a_{22} = nd' - (d'n-1) = 1$$

and it is easy to check it is positive. Then by **Theorem 3.3**, F_A has an equivalent class

$$F_A(x_1, x_2, x_3) = F_{U^TIU}(x_1, x_2, x_3) = F_I(y_1, y_2, y_3) = y_1^2 + y_2^2 + y_3^2$$

But since $F_A(0, 0, 1) = n$, we have $n = y_1^2 + y_2^2 + y_3^2$ can be represented as **the sum of three squares**. □

4. Main Theorem

Theorem 4.1. *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. With the discussion before, we only have to deal with the case $n \equiv 1, 2, 3, 5, 6 \pmod 8$

Case 1: For $n \equiv 2 \pmod 4$, $(4n, n-1) = 1$, by Dirichlet theorem, we have prime $p = 4nj + n - 1 = (4j+1)n - 1$. We let d' is exactly $4j+1$, then we have $p = d'n - 1 \equiv 1 \pmod 4$,claim that $\left(\frac{-d'}{p}\right) = 1$, then by main lemma we know n can be represented as the sum of three squares.
In fact,denote

$$d' = \prod_{q_i | d} q_i^{k_i}, \text{we have } p = d'n - 1 \equiv -1 \pmod{q_i}$$

So,

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

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

Case 2: For $n \equiv 1 \pmod 8$, $(4n, \frac{3n-1}{2}) = 1$, by Dirichlet theorem, we have prime $p = 4nj + \frac{3n-1}{2} = \frac{(8j+3)n-1}{2}$. We let d' is exactly $8j+3$, then we have $p = \frac{d'n-1}{2} \equiv 1 \pmod 4$,claim that $-d'$ is a quadratic residue modulo $2p$, then by main lemma we know n can be represented as the sum of three squares.Here we argued that we only need to prove $\left(\frac{-d'}{p}\right) = 1$, because if there exists $-d' = x^2 + kp$, while k is even, we know $-d'$ is a quadratic residue modulo $2p$, or else, we have $-d' = (x+p)^2 + k'p$ where k' is even. Thus, in all, $-d'$ is a quadratic residue modulo $2p$
In fact,denote

$$d' = \prod_{q_i | d} q_i^{k_i}, \text{we have } 2p = d'n - 1 \equiv -1 \pmod{q_i}$$

So,

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

$$\prod_{q_i \equiv 3,7 \pmod 8} (-1)^{k_i} \prod_{q_i \equiv 3,5 \pmod 8} (-1)^{k_i} \equiv \prod_{q_i \equiv 5,7 \pmod 8} (-1)^{k_i}$$

Reconsidering

$$3 \equiv d \equiv \prod_{q_i \equiv 3 \pmod 8} 3^{k_i} \prod_{q_i \equiv -3 \pmod 8} (-3)^{k_i} \prod_{q_i \equiv -1 \pmod 8} (-1)^{k_i}$$
$$\equiv \prod_{q_i \equiv \pm 3 \pmod 8} 3^{k_i} \prod_{q_i \equiv -3,-1 \pmod 8} (-1)^{k_i} \pmod 8$$

Comparing both sides, we get

$$\prod_{q_i \equiv 5,7 \pmod 8} (-1)^{k_i} = 1$$

.

Case 3: For $n \equiv 3 \pmod 8$, $(4n, \frac{n-1}{2}) = 1$, by Dirichlet theorem, we have prime $p = 4nj + \frac{n-1}{2} = \frac{(8j+1)n-1}{2}$. We let d' is exactly $8j+1$, then we have $p = \frac{d'n-1}{2} \equiv 1 \pmod 4$,claim that $-d'$ is a quadratic residue modulo $2p$.And we only need to prove $\left(\frac{-d'}{p}\right) = 1$

Denote

$$d' = \prod_{q_i | d} q_i^{k_i}, \text{we have } 2p = d'n - 1 \equiv -1 \pmod{q_i}$$

Again,

$$\left(\frac{-d'}{p}\right) \equiv \prod_{q_i \equiv 5,7 \pmod 8} (-1)^{k_i}$$

Reconsidering

$$1 \equiv d \equiv \prod_{q_i \equiv \pm 3 \pmod 8} 3^{k_i} \prod_{q_i \equiv -3,-1 \pmod 8} (-1)^{k_i} \pmod 8$$

Comparing both sides, we get

$$\prod_{q_i \equiv 5,7 \pmod 8} (-1)^{k_i} = 1$$

.

Case 4: For $n \equiv 5 \pmod 8$, $(4n, \frac{3n-1}{2}) = 1$, by Dirichlet theorem, we have prime $p = 4nj + \frac{3n-1}{2} = \frac{(8j+3)n-1}{2}$. We let d' is exactly $8j+3$, then we have $p = \frac{d'n-1}{2} \equiv 3 \pmod 4$,claim that $-d'$ is a quadratic residue modulo $2p$. Again we only need to prove $\left(\frac{-d'}{p}\right) = 1$

Denote

$$d' = \prod_{q_i | d} q_i^{k_i}, \text{we have } 2p = d'n - 1 \equiv -1 \pmod{q_i}$$

Now there's a little difference,

$$\left(\frac{-d'}{p}\right) \equiv - \prod_{q_i \equiv 3,5 \pmod 8} (-1)^{k_i}$$

Reconsidering

$$3 \equiv d \equiv \prod_{q_i \equiv 3 \pmod 8} 3^{k_i} \prod_{q_i \equiv -3 \pmod 8} (-3)^{k_i} \prod_{q_i \equiv -1 \pmod 8} (-1)^{k_i}$$
$$\equiv \prod_{q_i \equiv \pm 3 \pmod 8} 3^{k_i} \prod_{q_i \equiv -3,-1 \pmod 8} (-1)^{k_i} \pmod 8$$

Comparing both sides, we get

$$\prod_{q_i \equiv \pm 3 \pmod 8} 3^{k_i} = 3 \pmod 8$$

which means

$$\sum_{q_i \equiv \pm 3 \pmod 8} k_i \equiv 1 \pmod 2$$

so

$$\left(\frac{-d'}{p}\right) = - \prod_{q_i \equiv 3,5 \pmod 8} (-1)^{k_i} = 1$$

□

5. Another Point Of View

Theorem 5.1. *(Davenport-Cassels) Assume*

$$f(X) = \sum_{p}^{i,j=1} a_{ij} X_i X_j$$

is positive-definite quadratic form with $a_{ij} \in \mathbb{Z}$, we also assume that for all $x = (x_1, x_2, ..., x_p) \in \mathbb{Q}^p$, we have $y \in \mathbb{Z}^p$ s.t.

$$f(x - y) < 1$$

Then if f can represent $n \in \mathbb{Z}$ in $\mathbb{Q}$,it can also represent n in $\mathbb{Z}$.

The last theorem listed is another way to look at the problem.

And in order to solve it in $\mathbb{Q}$, it is claimed that it's equivalent to say it is solvable in each localization of $\mathbb{Q}$, namely $\mathbb{Q}_p$, where $p \in V = \{\text{All Prime}\} \cup \{\infty\}$.

Further proof will be found in [2], but anyway, this will show us a new field, a new view to see these kind of problems.

References

[1] Additive Number Theory (The Classical Bases).**Melvyn B.Nathansn** *Springer*
[2] A Course in Arithmetic . **Jean-Pierre Serre** *Springer*

School of Mathematical Sciences, University of Science and Technology of China, Hefei, 230026, P.R. China,
E-mail address: jzh0103@mail.ustc.edu.cn