PROOF OF LAGRANGE'S 3-SQUARE THEOREM AND OTHER RELATED RESULTS

JONATHAN SY

1. Introduction

In this paper, we give a proof of Legendre's three-square theorem and a few consequences of it.

Theorem 1.1 (Legendre)**.** *A natural number n can be represented as a sum of three squares*

$$n = x^2 + y^2 + z^2$$

if and only if n is not of the form $4^a(8b + 7)$.

We will assume that n is square free, since we can always factor out a square factor from each of x, y, and z. Hence, it suffices to show that for any square free n, $n = x^2 + y^2 + z^2$ if and only if $n \not\equiv 7 \pmod 8$. It's easy to show the only if direction. The only residues modulo 8 of x^2 are $0, 1, 4$. Since there's no way to make 7 out of $0, 1, 4$, $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$, proving the "only if" direction.

Thus, it suffices to show that for any $n \equiv 1, 2, 3, 5, 6 \pmod 8$, n can be represented as a sum of three squares.

2. Preliminaries

We will assume the following theorems in the rest of the proof.

Theorem 2.1 (Dirichlet's theorem on primes in arithmetic progression)**.** *For any relatively prime integers a and p, the infinite arithmetic sequence $\{a + np : n \in \mathbb{N}\}$ contains infinitely many primes.*

Theorem 2.2 (Fermat's Two-Square Theorem)**.** *A positive integer n can be represented as a sum of two squares if and only if every odd prime p in its factorization that has odd power is congruent to $1 \pmod 4$.*

Theorem 2.3 (Minkowski's Convex Body Theorem)**.** *Let $\Omega \subset \mathbb{R}^N$ be a convex body with volume 2^N. Then Ω contains a nonzero lattice point.*

In particular, we will use the case of when $N = 3$, which is the statement that every convex body in three dimensions with volume greater than 8 contains a nonzero lattice point.

Date: December 10, 2018.

3. Proof, $n \equiv 3 \pmod 8$

Given an $n \equiv 3 \pmod 8$, we will construct a solution to $x^2 + y^2 + z^2 = n$, albeit in a rather unmotivated fashion. The first step in doing this is to find a prime q such that $-m$ is a quadratic residue modulo q, as from this we'll be able to obtain a set of equations that is easier to work with.
It is clear that if m contains a square factor, then it can be simply be factored out of every term, so assume that m is square free. Let $m = p_1 p_2 \dots p_r$ where the p_i's are prime. We claim that we can construct a q such that $q \equiv 1 \pmod 4$ and that $-2q$ is a quadratic residue modulo each of p_1, p_2, …, p_r; that is, $(\frac{-2q}{p_i}) = 1$ for $1 \le i \le r$ where $(\frac{a}{b})$ denotes the Jacobi symbol. Note that $(\frac{-2q}{p_i}) = 1$ implies that there exists an x such that $x^2 \equiv -2q \pmod{p_i}$, and since -2 is relatively prime to p_i, we can write $q \equiv \frac{x^2}{-2} \pmod{p_i}$, where the right hand side is really just one equivalence class modulo p_i. Doing this for every prime p_i, we obtain a series of congruences with pairwise relatively prime mods, so by CRT we can construct a single congruence from these congruences. By Dirichlet's theorem, there exists a prime satisfying the latter congrunce. This is our desired q.

Multiplying the equations involving the Jacobi symbols yields

$$1 = \prod_{i=1}^{r} \left(\frac{-2q}{p_i}\right).$$

Using properties of the Jacobi symbol, we have

$$\prod_{i=1}^{r} \left(\frac{-2q}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right)$$

By definition of the Jacobi symbol, we can combine the denominators of $\left(\frac{-2}{p_i}\right)$ to get

$$\prod_{i=1}^{r} \left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)$$

Since $q \equiv 1 \pmod 4$, $(\frac{q}{p_i}) = (\frac{p_i}{q})$, so

$$\left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right) = \left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right)$$

Now the product just simplifies to $(\frac{m}{q})$, so we have

$$\left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right) = \left(\frac{-2}{m}\right)\left(\frac{m}{q}\right)$$

Finally, it is easy to check that for $m \equiv 3 \pmod 8$, $(\frac{-2}{m}) = 1$ and for $q \equiv 1 \pmod 4$, $(\frac{-1}{q}) = 1$, so we have

$$\left(\frac{-2}{m}\right)\left(\frac{m}{q}\right) = \left(\frac{-m}{q}\right)$$

Putting this all together, we get $(\frac{-m}{q}) = 1$.

Thus, $-m$ is a quadratic residue modulo q, so there exists an odd b such that $b^2 \equiv -m \pmod q$. Equivalently, $b^2 + m = qh'$. Rearranging gives $b^2 - qh' = -m$. Now note that since

b is odd, $b^2 \equiv 1 \pmod 4$. Since $-m \equiv -3 \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$, it follows that $4|h'$, so $h' = 4h$ for some integer h, and thus

$$b^2 - 4qh = -m$$

By our construction of q, we can find an integer t such that $t^2 \equiv -\frac{1}{2q} \pmod m$.
The next few steps are a bit hairy and the verifications will be swept under the rug. Let

$$R = 2tqx + tby + mz$$
$$S = (2q)^{1/2}x + \frac{b}{(2q)^{1/2}}y$$
$$T = \frac{m^{1/2}}{(2q)^{1/2}}y$$

and consider the figure $R^2 + S^2 + T^2 < 2m$. In the space of (R, S, T), this defines a convex, symmetric body of volume $\frac{4}{3}\pi(2m)^{\frac{3}{2}}$... worried about plagiarism now, since I'm not certain about this and the next couple of sentences...

Thus, by Minkowski's theorem on convex symmetric bodies in 3 dimensions, there exists a nonzero point (R_1, S_1, T_1) satisfying $R^2 + S^2 + T^2 < 2m$. Let x_1, y_1, z_1 be the corresponding x, y, z. By definition of R, S, and T, we have

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= (2tqx_1 + tby_1 + mz_1)^2 + \left((2q)^{1/2}x_1 + \frac{b}{(2q)^{1/2}}y_1\right)^2 + \left(\frac{m^{1/2}}{(2q)^{1/2}}y\right)^2 \\ &= t^2(2qx_1 + by_1)^2 + \frac{1}{2q}(2qx_1 + by_1)^2 \\ &= 0 \pmod m \end{aligned}$$

where the last equality comes from the definition of t. If we expand only S_1^2 and T_1^2, we obtain

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= R_1^2 + \left((2q)^{1/2}x_1 + \frac{b}{(2q)^{1/2}}y_1\right)^2 + \left(\frac{m^{1/2}}{(2q)^{1/2}}y_1\right)^2 \\ &= R_1^2 + 2qx_1^2 + 2bx_1y_1 + \frac{b^2}{2q}y_1^2 + \frac{m}{2q}y_1^2 \\ &= R_1^2 + 2(qx_1^2 + bx_1y_1 + hy_1^2) \\ &= R_1^2 + 2v \end{aligned}$$

where $h = \frac{b^2+m}{4q}$ and $v = qx_1^2 + bx_1y_1 + hy_1^2$. Hence, $m|R_1^2 + 2v$. But $R_1^2 + 2v \neq 0$ because of the definitions of R, S, T. Also, $R^2 + S^2 + T^2 < 2m$, so $R_1^2 + 2v = m$. Thus, as the definition of R_1 implies that R_1 is an integer, it remains to show that $2v$ can be written as a sum of 2 squares, which is our last step.

In order to show that $2v$ is representable as a sum of two squares, we only need to show that any odd prime p whose exponent is odd in the factorization of v is congruent to 1 (mod 4), so consider such a p with exponent k in the prime factorization of v.
If $p \nmid m$, then because $R_1^2 + 2v = m$ and $p|v$, $\left(\frac{m}{p}\right) = 1$.
By definition of v, we know that $4qv = 4q^2x_1^2 + 4qbx_1y_1 + 4qhy_1$, or $4qv = (2qx_1 + by_1)^2 + my_1^2$.

Now recall that $b^2 - 4qh = -m$. Hence, $\left(\frac{-m}{p}\right) = 1$.

Now, if $p \nmid q$, then we have p^k divides an expression of the form $e^2 + mf^2$, so $\left(\frac{-m}{p}\right) = 1$ here too. In both cases, $\left(\frac{-m}{p}\right) = 1$. Combining this with the fact that $\left(\frac{m}{p}\right) = 1$, we know that $\left(\frac{-1}{p}\right) = 1$, which by quadratic reciprocity means that $p \equiv 1 \pmod 4$.

Now suppose that $p|v$ and $p|m$. Dividing $4qv = (2qx_1 + by_1)^2 + my_1^2$ by $2q$ gives $2v = \frac{1}{2q}((2qx_1 + by_1)^2 + my_1^2)$. Plugging this into $R_1^2 + 2v = m$ gives

$$R_1^2 + \frac{1}{2q}((2qx_1 + by_1)^2 + my_1^2) = m.$$

But since $p|v$ and $p|m$, this means that $p|R_1$ and $p|(2qx_1 + by_1)$, so dividing both sides by p and taking modulo p gives

$$\frac{1}{2q}\frac{m}{p}y_1^2 \equiv \frac{m}{p} \pmod p,$$

or

$$y_1^2 \equiv 2q \pmod p.$$

This implies that $2q$ is a quadratic residue modulo p, so $\left(\frac{2q}{p}\right) = 1$. But recall that we defined q to be a positive prime that satisfied $\left(\frac{-2q}{p}\right) = 1$ for all p in the prime factorization of m. Hence, once again, $\left(\frac{-1}{p}\right) = 1$, or that $p \equiv 1 \pmod 4$.

Thus, any prime that divides v to an odd power satisfies $p \equiv 1 \pmod 4$, so $2v$ is a sum of two squares.

4. Proof, $m \equiv 1, 2, 5, 6 \pmod 8$

The proofs for when $p \equiv 1, 2, 5, 6 \pmod 8$ are nearly identical, with the following modifications.

Instead of $\left(\frac{-2q}{p_i}\right) = +1$, we instead have $\left(\frac{-q}{p_i}\right) = +1$. $q \equiv 1 \pmod 4$ still. Now, if m is even, let $m = 2m_1$, so that m_1 is odd (since we're assuming m to be squarefree). Then we can find an odd integer t such that $t^2 \equiv \frac{-1}{q} \pmod{p_i}$, resulting in $b^2 - qh = -m$. Finally, we alter the definitions of R, S, and T as follows:

$$R = tqx + tby + mz$$
$$S = q^{1/2}x + \frac{b}{q^{1/2}}y$$
$$T = \frac{m^{1/2}}{q^{1/2}y}$$

Then the proof for these congruence classes proceeds exactly the same as for $m \equiv 3 \pmod 8$. Thus, we have finished the proof.

5. Some Applications of the Three Square Theorem

Theorem 5.1. *An number n can be written as a sum of 3 triangular numbers.*

Proof. By the three-square theorem, there exists a solution to $8n+3 = x^2+y^2+z^2$. The only possible residues of a square modulo 8 are 0, 1, and 4. Thus, $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 8$, so they are all odd. Writing $x = 2a+1$, $y = 2b+1$, and $z = 2c+1$, we obtain $8n+3 = 4(a^2+a)+4(b^2+b)+4(c^2+c)+3$, or $n = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}$. Thus, any number n can be written as a sum of 3 triangular numbers. ■

Theorem 5.2. *Every natural number can be written as a sum of two squares and a triangular number.*

Proof. By the Three-Square Theorem, every number congruent to $1 \pmod 8$ can be written as a sum of three squares, so for any integer n, $8n+1 = x^2+y^2+z^2$ for some x, y, z. Now recall that $0, 1, 4$ are the only quadratic residues modulo 8. Thus, at most one of x, y, z can be odd. WLOG, let $z = 2c+1$, and let $y = 2b$, $x = 2a$. Then we have $8n+1 = 4(a^2+b^2)+(2c+1)^2$. Rearranging, and taking $\pmod 8$, we have $4(a^2+b^2) = 8n+1-(2c+1)^2 \equiv 0 \pmod 8$, as $(2c+1)^2 \equiv z^2 \equiv 1 \pmod 8$. Hence, $a^2+b^2 \equiv 0 \pmod 2$. Therefore, $a \equiv b \pmod 2$, so we can write ■

Theorem 5.3. *We have the following characterization of the $x^2+y^2+2z^2$:*

$$\{x^2+y^2+2z^2 : x, y, z \in \mathbb{Z}\} = \mathbb{N} \backslash \{4^a(16b+14) : a, b \in \mathbb{N}\}$$

Proof. First, suppose that $n = x^2+y^2+2z^2$. Then, after multiplying both sides by 2 and rearranging, we get $2n = 2x^2+2y^2+4z^2 = (x+y)^2+(x-y)^2+(2z)^2$. This process is clearly reversible, so if $x \notin \{2(x^2+y^2+z^2) : x, y, z \in \mathbb{Z}\}$, then $x \notin \{x^2+y^2+2z^2 : x, y, z \in \mathbb{Z}\}$. But $x \notin \{2(x^2+y^2+z^2) : x, y, z \in \mathbb{Z}\} = \{4^a(16b+14) : a, b \in \mathbb{N}\}$, which means that

$$\{x^2+y^2+2z^2 : x, y, z \in \mathbb{Z}\} = \mathbb{N} \backslash \{4^a(16b+14) : a, b \in \mathbb{N}\},$$

as desired. ■

References

[1] N. C. Ankeny. Sums of Three Squares. *Proc. Amer. Math. Soc.* 008:316-319, 1957
[2] Zhi-Wei Sun. The Three-Square Theorem And Its Applications.

Euler Circle, Palo Alto, CA 94306