REFERENCES

1. N. Bourbaki, *Espaces vectoriels topologiques*, Chaps. 1–2 Actualités Scientifiques et Industrielles no. 1189, Paris, Hermann.

2. Seth Warner, *Weak locally multiplicatively-convex algebras*, Pacific Journal of Mathematics vol. 5 (1955) pp. 1025–1032.

DUKE UNIVERSITY

---

# SUMS OF THREE SQUARES

N. C. ANKENY[1]

**Introduction.** I would like to present here a short and elementary proof of the following theorem.

THEOREM 1. *If $m$ is a positive integer not of the form $4^a(8n+7)$, then $m$ is the sum of three squares.*

We make use of an elegant method of Professor H. Davenport [1] in the Geometry of Numbers.

Without loss of generality we will prove Theorem 1 only when $m$ is square free. (In the following $m$ will be assumed to be square free.) In §1 we shall prove Theorem 1 when $m \equiv 3 \pmod 8$. In §2 we will merely outline the proof when $m \equiv 1, 2, 5, 6 \pmod 8$, as the proof is almost identical except for minor changes.

We shall only assume the reader is familiar with the elementary facts of the law of quadratic reciprocity, Minkowski's Theorem on lattice points contained within convex symmetric bodies; and when a positive integer is the sum of two squares.

1. Let $m$ be a positive square free integer $\equiv 3 \pmod 8$, and $m = p_1 p_2 \cdots p_r$ where $p_j$'s are primes.

Denote by $q$ a positive prime which satisfies

$$(-2q/p_j) = +1, \qquad j = 1, 2, \cdots, r, \tag{1}$$

$$q \equiv 1 \pmod 4 \tag{2}$$

with $(a/b)$ denoting the Jacobi Symbol. We see that such a prime exists by Dirichlet's theorem regarding primes in an arithmetic pro-

Received by the editors April 26, 1956.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract No. AF 18 (603)-90. Reproduction in whole or in part is permitted for any purpose of the United States Government.

gression, as (1) and (2) merely necessitate that $q$ lie within certain relatively prime residue classes (mod $4m$).

By (1) and (2)

$$
\begin{aligned}
1 &= \prod_{j=1}^{r} (-2q/p_j) = \prod_{j=1}^{r} (-2/p_j)(q/p_j) \\
&= (-2/m) \prod_{j=1}^{r} (p_j/q) \qquad (3) \\
&= (-2/m)(m/q) = (-2/m)(-m/q) \\
&= (-m/q)
\end{aligned}
$$

as $m \equiv 3 \pmod 8$.

Hence, as $q$ is an odd prime we can find an odd integer $b$ such that $b^2 \equiv -m \pmod q$, or

$$b^2 - qh_1 = -m. \qquad (4)$$

Considering (4) (mod 4) yields $1 - h_1 \equiv +1 \pmod 4$, or $h_1 = 4h$ where $h$ is a rational integer and

$$b^2 - 4qh = -m. \qquad (5)$$

Utilizing (1) we can find an integer $t$ such that

$$t^2 \equiv -1/2q \pmod m. \qquad (6)$$

We now consider the figure

$$R^2 + S^2 + T^2 < 2m \qquad (7)$$

where

$$
\begin{aligned}
R &= 2tqx + tby + mz, \\
S &= (2q)^{1/2}x + b/(2q)^{1/2}y, \qquad (8) \\
T &= m^{1/2}/(2q)^{1/2}y
\end{aligned}
$$

In the $(R, S, T)$ space (7) defines a convex, symmetric (about the origin) body of volume $4/3\pi(2m)^{3/2}$. The determinant of the transformations (8) is $m^{3/2}$. Hence, in the $(x, y, z)$ space, (7) represents a convex symmetric body of volume $1/3(2^{7/2}\pi)$, and certainly $1/3(2^{7/2}\pi) > 8$.

Hence, by Minkowski's Theorem on convex symmetric body in three dimensions of volume $>8$, we know there exist integer values of $x, y, z$ not all zero which satisfy (7). Let $x_1, y_1, z_1$ be the integers which satisfy (7) and (8), $R_1, S_1, T_1$ the corresponding values of $R, S, T$.

By (8)

$$
\begin{aligned}
R_1^2 + S_1^2 + T_1^2 &= (2tqx_1 + tby_1 + mz_1)^2 \\
&\quad + ((2q)^{1/2}x_1 + b/(2q)^{1/2}y_1)^2 + (m^{1/2}/(2q)^{1/2}y_1)^2 \\
&\equiv t^2(2qx_1 + by_1)^2 + 1/2q(2qx_1 + by_1)^2 \qquad (9) \\
&\equiv 0 \pmod{m}
\end{aligned}
$$

by (6), the selection of $t$.

Furthermore,

$$
\begin{aligned}
R_1^2 + S_1^2 + T_1^2 &= R_1^2 + ((2q)^{1/2}x_1 + b/(2q)^{1/2}y_1)^2 + (m^{1/2}/(2q)^{1/2}y_1)^2 \\
&= R_1^2 + 1/2q(2qx_1 + by_1)^2 + m/2qy_1^2 \qquad (10) \\
&= R_1^2 + 2(qx_1^2 + bx_1y_1 + hy_1^2).
\end{aligned}
$$

Let $v$ be the positive rational integer defined by

$$v = qx_1^2 + bx_1y_1 + hy_1^2. \qquad (11)$$

We note that $R_1$ is a rational integer and by (9), (10), and (11) that $m \mid R_1^2+2v$, but by (7) $R_1^2+2v<2m$. Furthermore $R_1^2+2v\neq 0$, by the nondegenerate triangular transformation (8) and the fact that not all $x_1$, $y_1$, $z_1$ equal zero. Hence,

$$R_1^2 + 2v = m. \qquad (12)$$

Let $p$ be an odd prime which exactly divides $v$ to an odd power, i.e. $p^{2n+1} \| v$.

If $p$ does not divide $m$, then by (12),

$$(m/p) = +1. \qquad (13)$$

By (11)

$$4qv = (2qx_1 + by_1)^2 + my_1^2. \qquad (14)$$

If $p/q$, then (5), $(-m/p)=1$.

If $p\nmid q$, then by (14)

$$p^{2n+1} \| e^2 + mf^2, \text{ or } (-m/p) = 1.$$

Thus, in either case,

$$(-m/p) = +1 \qquad (15)$$

which combined with (13) implies

$$(-1/p) = 1 \text{ or } p \equiv 1 \pmod 4. \qquad (16)$$

If $p/v$, $p/m$, then by (11) and (12)

$$R_1^2 + 2v = m$$

or

$$R_1^2 + \frac{1}{2q}((2qx_1 + by_1)^2 + my_1^2) = m \tag{17}$$

which implies $p/R_1$, $p/(2qx_1+by_1)$, and thus as $m$ is square free by dividing both sides of (17) by $p$, yields

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

or

$$y_1^2 \equiv 2q \pmod{p}, \quad \left(\frac{2q}{p}\right) = +1$$

which combined with (1) gives $(-1/p) = +1$ or $p \equiv 1 \pmod 4$.

Thus all odd primes which exactly divide $v$ to an odd power are $\equiv 1 \pmod 4$. Thus $2v$ is the sum of two square integers. By (12) this implies $m$ is the sum of three square integers, which proves Theorem 1 when $m \equiv 3 \pmod 8$.

2. If $m \equiv 1, 2, 5$ or $6 \pmod 8$, we alter the proof in §1 in the following ways. Let $q$ be a prime, $(-q/p_j) = +1$ for all odd prime divisors of $m$, $q \equiv 1 \pmod 4$, and if $m$ is even,

$$m = 2m_1, \quad (-2/q) = (-1)^{(m_1-1)/2}, \quad t^2 \equiv -1/q \pmod{p_j},$$
$$t \text{ odd}, \quad b^2 - qh = -m$$

and

$$R = tqX + tby + mz,$$
$$S = q^{1/2}x + b/q^{1/2}y,$$
$$T = m^{1/2}/q^{1/2}y.$$

The proof will proceed exactly as in §1, which will complete the proof when $m \equiv 1, 2, 3, 5, 6 \pmod 8$, and thus for all square free $m$.

## Bibliography

1. H. Davenport, *The geometry of numbers*, Mathematical Gazette vol. 31 (1947) pp. 206–210.

Massachusetts Institute of Technology