COLLOQUIUM MATHEMATICUM

VOL. XXIV 1971 FASC. 1

ON SUMS OF THREE SQUARES

BY

JAN WÓJCIK (WARSZAWA)

N. C. Ankeny [1] gave a proof of Gauss theorem on sums of three squares based on Minkowski convex body theorem. This proof has been subsequently simplified by L. J. Mordell [4]. The aim of this note is to give another proof of Gauss theorem based on the geometry of numbers and on a theorem of Legendre on a representation of zero by ternary forms (for a simple proof see [3], p. 157-158; the case considered there is almost identical with that which we need below).

GAUSS THEOREM. *A positive integer is a sum of three squares of integers if and only if it is not of the form* $4^h\,(8k+7)$.

LEMMA 1. *Let* x, y, z *be rational number such that* $x^2+y^2+z^2$ *is an integer. Then there exist rational numbers* a, b, c *such that* $a^2+b^2+c^2 = 1$ *and that* $ax+by+cz$ *is integer.*

Proof. Let $x = x_1/d$, $y = y_1/d$, $z = z_1/d$, where x_1, y_1, z_1, d are relatively prime integers. Let M denote the lattice $(u+tx, v+ty, w+tz)$ and Λ the lattice (u, v, w), where u, v, w, t, $ux+vy+wz$ are integers, $0 \leqslant t \leqslant d-1$. Let $d(M)$ and $d(\Lambda)$ be the determinants of M and Λ, respectively, $[M:\Lambda]$ be the index of Λ in M. Clearly,

$$[M:\Lambda] = d. \tag{1}$$

The lattice Λ is characterized by the congruence $ux_1+vy_1+wz_1 \equiv 0 \bmod d$. Hence, by (1), by formula (2) and Lemma 1 of Chapter I of [2], and by Lemma 9 of Chapter III of [2], there is

$$d(M) = d(\Lambda)/[M:\Lambda] = d(\Lambda)/d \leqslant 1.$$

Thus

$$V = \tfrac{4}{3}\pi(\sqrt{2})^3 > 8 \geqslant 8d(M),$$

where V is the volume of the all $\xi^2+\eta^2+\zeta^2 < 2$.

In virtue of Minkowski convex body theorem there exists a vector (a, b, c) in M such that

$$(a, b, c) = (u+tx, v+ty, w+tz), \qquad 0 < a^2+b^2+c^2 < 2.$$

Since $a^2+b^2+c^2 = u^2+v^2+w^2+2t(ux+vy+wz)+t^2(x^2+y^2+z^2)$ is an integer, it follows that $a^2+b^2+c^2 = 1$, and that $ax+by+cz = ux+ +vy+wz+t(x^2+y^2+z^2)$ is an integer, which completes the proof.

LEMMA 2. *If an integer is the sum of three squares of rationals, then it is the sum of three squares of integers.*

Proof. Let $x^2+y^2+z^2$ be an integer, x, y, z be rationals. Let a, b, c be rationals the existence of which is asserted in Lemma 1. We may assume $b^2+c^2 \neq 0$. Then we have the identity

$$x^2+y^2+z^2 = (ax+by+cz)^2+U^2+V^2,$$

where

$$U = bx-\frac{ab+c^2}{b^2+c^2}y+\frac{-abc+bc}{b^2+c^2}z, \qquad V = cx+\frac{-abc+bc}{b^2+c^2}y-\frac{ac^2+b^2}{b^2+c^2}z.$$

The integer U^2+V^2 is the sum of two squares of rational numbers and so it is also the sum of two squares of integers (see [5], p. 352). This proves Lemma 2.

Proof of the theorem. The necessity of the condition is easy to verify. To prove the sufficiency we may assume that $m \not\equiv 7 \bmod 8$ is squarefree. In virtue of Lemma 2 it is enough to show that m is the sum of three squares of rational numbers.

Let $m = 2^a m_1$, where $a = 0$ or 1, m_1 odd, $m_1 = p_1 \ldots p_r$, p_i primes. Let

$$\beta = \begin{cases} 0 & \text{if either } a = 0,\ m_1 \equiv 1 \bmod 4 \text{ or } a = 1, \\ 1 & \text{if } a = 0,\ m_1 \equiv 3 \bmod 8. \end{cases}$$

By a theorem of Dirichlet on primes in arithmetic progression there exists a prime q such that

$$\left(\frac{q}{p_i}\right) = \left(\frac{-2^\beta}{p_i}\right) \quad \text{and} \quad q \equiv \begin{cases} 1 \bmod 8 & \text{if } m_1 \equiv 1 \bmod 4, \\ 5 \bmod 8 & \text{if } m_1 \equiv 3 \bmod 4. \end{cases}$$

Hence, in virtue of the quadratic reciprocity law,

$$\left(\frac{-2^\beta q}{p_i}\right) = 1, \quad \left(\frac{m}{q}\right) = \left(\frac{2}{q}\right)^a \left(\frac{m_1}{q}\right) = \left(\frac{2}{q}\right)^a \left(\frac{q}{m_1}\right)$$
$$= \left(\frac{2}{q}\right)^a \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_r}\right) = \left(\frac{2}{q}\right)^a \left(\frac{-2^\beta}{p_1}\right) \cdots \left(\frac{-2^\beta}{p_r}\right) = \left(\frac{2}{q}\right)^a \left(\frac{-2^\beta}{m_1}\right) = 1.$$

This implies solvability of the congruences $x^2 \equiv -2^\beta q \bmod p_i$, $x^2 \equiv m \bmod q$ and consequently also of the congruences $x^2 \equiv -2^\beta q \bmod m$, $x^2 \equiv m \bmod 2^\beta q$. In virtue of a theorem of Legendre it follows that the equation $mt^2-z^2-2^\beta qu^2 = 0$ is solvable in integers t, z, u, where $t \neq 0$ (see [3], p. 157-158). On the other hand, since $q \equiv 1 \bmod 4$, $2^\beta qu^2$ is the sum of two squares of integers. Hence $mt^2-z^2 = 2^\beta qu^2 = x^2+y^2$, $m = (x/t)^2+(y/t)^2+(z/t)^2$. The proof is complete.

REFERENCES

[1] N. C. Ankeny, *Sums of three squares*, Proceedings of the American Mathematical Society 8 (1957), p. 316-319.

[2] J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin-Göttingen-Heidelberg 1959.

[3] H. Davenport, *The higher arithmetic, an introduction to the theory of numbers*, New York-Melbourne-Sydney-Cape Town 1952.

[4] L. J. Mordell, *On the representation of a number as a sum of three squares*, Revue Roumaine de Mathématiques Pures et Appliquées 3 (1958), p. 25-27.

[5] W. Sierpiński, *Elementary theory of numbers*, Warszawa 1964.

Reçu par la Rédaction le 27. 6. 1970