THE 3-SQUARES THEOREM

by S. CHOWLA, F.N.A. *and* P. HARTUNG, *Institute for Advanced Study, Princeton, N.J.*

(*Received* 16 *July* 1973)

This paper records recent new approaches to the "3-squares" theorem, a classical result of Gauss.

§1. One of the entries in Gauss's diary is the mysterious (?)

> Eureka! num $= \Delta + \Delta + \Delta$

i.e. for every n in Z^+ we have

$$n = \Delta_x + \Delta_y + \Delta_z$$

or

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

with x, y, z in Z. This is the same as

$$8n + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2.$$

This theorem is much deeper than Lagrange's theorem that every positive integer n can be expressed as a sum of 4 squares of integers.

We next prove (in order to give a new proof of Gauss's assertion) :

Lemma (*Cassell's*) — If the positive integer M can be expressed as a sum of 3 squares of rational numbers, then it can also be expressed as a sum of 3 squares of integers.

PROOF : From now on all letters denote integers. Suppose we have

$$x_1^2 + x_2^2 + x_3^2 = Ma^2$$

(i.e. M is a sum of 3 squares of rational numbers). We write this as

$$Q(x) = Ma^2. \qquad \ldots(1)$$

Set $x_j = ay_j + z_j$ $(j = 1, 2, 3,)$ $| z_j | \leqslant \frac{a}{2}$.

Briefly $x = ay + z$. Now (1) becomes

$$a^2Q(y) + 2aQ(y, z) + Q(z) = Ma^2 \qquad \ldots(2)$$

where

$$Q(y, z) = y_1z_1 + y_2z_2 + y_3z_3.$$

Clearly $Q(z) \equiv 0 \pmod{a}$. So write

$$Q(z) = -ab$$

where

$\left(\text{since } |z| \leqslant \frac{a}{2}\right)$, $|b| \leqslant \frac{3a}{4} < a$. Now (2) gives

$$2Q(y, z) - b = a(M - Q(y)). \qquad \ldots(3)$$

Next we shall choose an integer t such that

$$Q(by + tz) = Mb^2 \qquad \ldots(4)$$

or

$$b^2Q(y) + 2btQ(y, z) + t^2Q(z) = Mb^2. \qquad \ldots(5)$$

It is easy to see that (3) and (5) are compatible with

$$t = M - Q(y).$$

[We reject $t = \frac{b}{a}$ (since this is numerically less than 1) and $b = 0$ since this implies $z = 0$ and so $a \mid x$; the latter would make M a sum of 3 integral squares.]

Thus (1) leads to (4), with $|b| < a$. Continuing, we finally get

M = a sum of 3 squares of integers. q.e.d.

§2. We next use an argument suggested by A. Selberg to deduce from Cassell's Lemma that for $M \equiv 3(8)$, we have

$$M = u^2 + v^2 + w^2, \qquad (u, v, w \text{ in } Z).$$

By the Lemma it is enough to show the existence of x, y, z, f in Z, s.t.

$$x^2 + y^2 + z^2 = Mf^2 \qquad (f \text{ odd}) \qquad \ldots(6)$$

or

$$x^2 + y^2 = Mf^2 - z^2 \qquad \ldots(7)$$

From (6), x, y, z are odd.

Set $\hat{f} = \frac{p + q}{2}$, $z = \frac{p - q}{2}$, (7) becomes

$$x^2 + y^2 = 2\left\{\left(\frac{M-1}{2}\right)(p^2 + q^2) + (M+1)pq\right\} \qquad \ldots(8)$$

It now follows that p and q have opposite parity. $\ldots(9)$

Consider the primitive (i.e. the coefficients have no common factor 1) binary quadratic form

$$\left(\frac{M-1}{2}\right)(p^2 + q^2) + (M+1)pq. \qquad \ldots(10)$$

It represents (by a known but deep theorem of analytic number theory) infinitely many primes. Since $M \equiv 3(8)$, it follows that the expression (10) is a prime ρ requires that p and q have opposite parity. But then (10) is $\equiv 1(4)$. Hence $\rho = \alpha^2 + \beta^2$ (α, β in Z). So from (8)

$$x^2 + y^2 = 2\rho = (\alpha + \beta)^2 + (\alpha - \beta)^2.$$

Thus (2) and so (1) is satisfied with

$$x = \alpha + \beta, \qquad y = \alpha - \beta.$$

We have now proved G's assertion that

$$M \equiv 3(8) \Rightarrow M = \boxed{3} \qquad \ldots(11)$$

where $\boxed{g}$ stands for a sum of g squares of integers.

§3. There is still another proof of (11), suggested by A. Weil in his course "300 years of number theory" at the Institute for Advanced Study, Princeton. Apply the so-called "Hasse Principle" to the form

$$(x^2 + y^2 + z^2) - Mw^2$$

where $M > 0$, $M \equiv 3(8)$. Since this form represents 0 in every p-adic field (p, a prime), it represents 0, over Q (the rationals). Apply Cassell's Lemma. q.e.d.