PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, No. 1, April 1971

NOTE ON A THEOREM OF PALL

KENNETH S. WILLIAMS

ABSTRACT. A simple proof is given of Pall's formula for the number of representations of a gaussian integer as the sum of two squares of gaussian integers.

Pall [2] has calculated the number $g_2(z)$ of representations of the nonzero gaussian integer $z=x+2iy$ as the sum of two squares of gaussian integers. This result was rediscovered (using a different method) by the author [3]. Using ideas from [2], [3] we give a very simple proof of Pall's theorem.

THEOREM. *If* $z=x+2iy=\epsilon(1+i)^a w$, *where* $\epsilon=1$ *or* i, $a\geqq 0$ *and* $\mathrm{Re}(w)\equiv 1 \pmod 2$, $\mathrm{Im}(w)\equiv 0 \pmod 2$, *then*

$$g_2(z) = h(a,\epsilon)\tau(w), \tag{1}$$

where $\tau(w)$ *is the number of divisors of* w *and*

$$\begin{aligned} h(a,\epsilon) &= 1, \qquad \text{if } a=0,\ \epsilon=1, \\ &= |a-3|, \quad \text{if } a \geqq 2. \end{aligned} \tag{2}$$

($a=1$ *and* $a=0$, $\epsilon=i$ *are excluded as* $\mathrm{Re}\, z$ ($=2y$) *is even.*)

PROOF. We let

$$D(z) = \{z_1 : z_1 \mid z,\ 2 \mid z_1 + z/z_1\},$$
$$R(z) = \{(a,b,c,d) : z = (a+ib)^2 + (c+id)^2\},$$

and define $\lambda : D(z) \to R(z)$ by

$$\lambda(z_1) = \left(\mathrm{Re}\left(\tfrac{1}{2}\left(z_1+\frac{z}{z_1}\right)\right), \mathrm{Im}\left(\tfrac{1}{2}\left(z_1+\frac{z}{z_1}\right)\right),\right.$$
$$\left.\mathrm{Im}\left(\tfrac{1}{2}\left(z_1-\frac{z}{z_1}\right)\right), -\mathrm{Re}\left(\tfrac{1}{2}\left(z_1-\frac{z}{z_1}\right)\right)\right).$$

λ is one-to-one and onto so that $|D(z)| = |R(z)|$, that is,

$$g_2(z) = \sum_{z_1 \mid z;\ 2 \mid z_1 + z/z_1} 1.$$

If $z_1 \mid z$ we have $z_1 = (1+i)^{a_1} w_1$, where $0 \leqq a_1 \leqq a$, $w_1 \mid w$. Since either

Received by the editors October 20, 1970.
AMS 1969 *subject classifications*. Primary 1043, 1046; Secondary 1066.
Key words and phrases. Gaussian integer, sum of two squares, Pall's theorem.

$w_1 \equiv w/w_1 \equiv 1 \pmod 2$ or $w_1 \equiv w/w_1 \equiv i \pmod 2$, we have $2 \mid z_1 + z/z_1$ if and only if $2 \mid (1+i)^{a_1} + \epsilon(1+i)^{a-a_1}$. Thus we obtain

$$g_2(z) = \sum_{\substack{a_1=0 \\ 2 \mid (1+i)^{a_1}+\epsilon(1+i)^{a-a_1}}}^{a} 1 \cdot \sum_{w_1 \mid w} 1. \tag{3}$$

For $a=0$, $\epsilon=1$ or $a=2$ the first sum of the product in (3) is 1, and for $a=3$ it is zero. For $a \geqq 4$ the only terms which contribute anything are $a_1 = 2, \cdots, a-2$ so that the sum is $a-3$. The first sum therefore is just (2). The second sum is just the number of divisors of w, that is $\tau(w)$. This proves (1).

In particular $z = x+2iy$ is the sum of two squares of gaussian integers if and only if $(1+i)^3 z$ (see for example [1]).

References

1. W. J. Leahey, *A note on a theorem of I. Niven*, Proc. Amer. Math. Soc. **16** (1965), 1130–1131. MR **31** #5860.

2. G. Pall, *Sums of two squares in a quadratic field*, Duke Math. J. **18** (1951), 399–409. MR **12**, 676.

3. K. S. Williams, *On a theorem of Niven*, Canad. Math. Bull. **10** (1967), 573–578; Addendum, Canad. Math. Bull. **11** (1968), 145. MR **37** #138; MR **37** #5152.

Carleton University, Ottawa, Canada