ANOTHER PROOF OF A THEOREM OF NIVEN

KENNETH S. WILLIAMS, Carleton University, Ottawa

Niven [3] has proved that the gaussian integer $a + 2bi$ (a, b integers) is the sum of two squares of gaussian integers if and only if $(1 + i)^3 \nparallel a + 2bi$. (If $w\ (\neq 0)$ and z are gaussian integers such that $w^k \mid z$, $w^{k+1} \nmid z$ for some integer $k \geq 1$ we write $w^k \parallel z$.) Simple proofs of this result have been given recently by Leahey [1] and Mordell [2]. Here is another simple proof.

We begin by showing that if $(1 + i)^3 \nparallel a + 2bi$ then $a + 2bi$ is the sum of two squares of gaussian integers. If a is odd, so that $1 + i \nmid a + 2bi$, we have

$$a + 2bi = \left(\frac{(a+1)}{2} + bi\right)^2 + \left(b - \frac{(a-1)}{2} i\right)^2.$$

If a is even we have $(1 + i)^2 \mid a + 2bi$. If $(1 + i)^2 \parallel a + 2bi$, say $a + 2bi = (1 + i)^2(c + di)$, where $c + d$ odd, then

$$a + 2bi = \left\{\left(\frac{c-d+1}{2}\right) + i\left(\frac{c+d+1}{2}\right)\right\}^2 + \left\{\left(\frac{c+d-1}{2}\right) + i\left(\frac{-c+d+1}{2}\right)\right\}^2.$$

If $(1 + i)^4 \mid a + 2bi$, say $a + 2bi = (1 + i)^4(e + fi)$, then we have

$$a + 2bi = ((e - 1) + fi)^2 + (f - (e + 1)i)^2.$$

Finally suppose $(1 + i)^3 \parallel a + 2bi$, say $a + 2bi = (1 + i)^3(g + hi)$, where $g + h$ is odd. We show that $a + 2bi$ is not the sum of two squares of gaussian integers, for if $a + 2bi = (a_1 + b_1 i)^2 + (a_2 + b_2 i)^2$ then

$$(1 + i)^3(g + hi) = \{(a_1 + b_2) - (a_2 - b_1)i\}\{(a_1 - b_2) + (a_2 + b_1)i\},$$

and so on multiplying both sides by their complex conjugates we obtain

$$2^3(g^2 + h^2) = \{(a_1 + b_2)^2 + (a_2 - b_1)^2\}\{(a_1 - b_2)^2 + (a_2 + b_1)^2\},$$

which a simple parity argument shows to be impossible as the left hand side is $\equiv 8 \pmod{16}$ yet the right hand side is $\equiv 0, 1, 4, 5, 9, 13 \pmod{16}$. This completes the proof.

References

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

2. L. J. Mordell, The representation of a gaussian integer as a sum of two squares, this MAGAZINE, 40 (1967) 209.

3. I. Niven, Integers of quadratic fields as sums of squares, Trans. Amer. Math. Soc., 48 (1940) 405–417.