# ON A THEOREM OF NIVEN

Kenneth S. Williams

(received October 27, 1966)

In 1940, I. Niven [2] proved that the gaussian integer $z = x + iy$ is the sum of two squares of gaussian integers if, and only if, $y$ is even and not both of $\frac{1}{2}x$ and $\frac{1}{2}y$ are rational odd integers. In this note we calculate the total number $g_2(z)$ of representations of $z$ in this form. Now

(1) $$z = (a+ib)^2 + (c+id)^2 ,$$

where $a, b, c, d$ are rational integers, if and only if

(2) $$z = \{(a-d) + i(b+c)\}\{(a+d) + i(b-c)\} .$$

Thus

$$g_2(z) = \sum_{\substack{z_1, z_2 \\ z_1 z_2 = z \\ (a-d)+i(b+c) = z_1 \\ (a+d)+i(b-c) = z_2 \\ a, b, c, d \text{ rat. ints}}} 1 = \sum_{\substack{z_1, z_2 \\ z_1 z_2 = z \\ \mathrm{Re}(z_1) + \mathrm{Re}(z_2) \equiv 0 \pmod 2 \\ \mathrm{Im}(z_1) + \mathrm{Im}(z_2) \equiv 0 \pmod 2}} 1$$

$$= \sum_{\substack{z_1 | z \\ \mathrm{Re}(z_1) + \mathrm{Re}(z/z_1) \equiv 0 \pmod 2 \\ \mathrm{Im}(z_1) + \mathrm{Im}(z/z_1) \equiv 0 \pmod 2}} 1$$

We can write z in the form

$$(3)\qquad z = \varepsilon(1+i)^{\alpha}\, \pi_1^{\alpha_1} \cdots \pi_k^{\alpha_k}\, q_1^{\beta_1} \cdots q_\ell^{\beta_\ell} ,$$

where $\varepsilon = \pm 1$, $\pm i$; $\alpha \geq 0$, $\alpha_j \geq 0$ $(j = 1, 2, \ldots, k)$, $\beta_j \geq 0$ $(j = 1, 2, \ldots, \ell)$, $\pi_j = u_j + iv_j$ $(j = 1, 2, \ldots, k)$ where $u_j \equiv 1 \pmod 2$, $v_j \equiv 0 \pmod 2$ and $u_j^2 + v_j^2$ = rational prime $\equiv 1 \pmod 4$ and $q_j$ $(j = 1, 2, \ldots, \ell)$ is a rational prime $\equiv 3 \pmod 4$. Now if $z_1 | z$ we can write $z_1$ in the form

$$(4)\qquad z_1 = \delta(1+i)^{\gamma}\, \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k}\, q_1^{\delta_1} \cdots q_\ell^{\delta_\ell} ,$$

where $\delta = \pm 1$, $\pm i$, $0 \leq \gamma \leq \alpha$, $0 \leq \gamma_j \leq \alpha_j$ $(j = 1, 2, \ldots, k)$ and $0 \leq \delta_j \leq \beta_j$ $(j = 1, 2, \ldots, \ell)$. Hence

$$(5)\qquad g_2(z) = \sum_{\delta} \sum_{\gamma=0}^{\alpha} \sum_{\gamma_1=0}^{\alpha_1} \cdots \sum_{\gamma_k=0}^{\alpha_k} \sum_{\delta_1=0}^{\beta_1} \cdots \sum_{\delta_\ell=0}^{\beta_\ell}{}' \; 1 ,$$

where the dash (') denotes that the summation is only taken over those $\delta, \gamma, \gamma_1, \ldots, \gamma_k, \delta_1, \ldots, \delta_\ell$ satisfying

$$(6)\qquad \begin{cases} \operatorname{Re}(\delta(1+i)^{\gamma}\, \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k}\, q_1^{\delta_1} \cdots q_\ell^{\delta_\ell}) \\ \quad + \operatorname{Re}(\varepsilon\delta^3 (1+i)^{\alpha-\gamma}\, \pi_1^{\alpha_1-\gamma_1} \cdots \pi_k^{\alpha_k-\gamma_k}\, q_1^{\beta_1-\delta_1} \cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv 0 \pmod 2 \\ \text{and} \\ \operatorname{Im}(\delta(1+i)^{\gamma}\, \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k}\, q_1^{\delta_1} \cdots q_\ell^{\delta_\ell}) \\ \quad + \operatorname{Im}(\varepsilon\delta^3 (1+i)^{\alpha-\gamma}\, \pi_1^{\alpha_1-\gamma_1} \cdots \pi_k^{\alpha_k-\gamma_k}\, q_1^{\beta_1-\delta_1} \cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv 0 \pmod 2. \end{cases}$$

Hence

$$(7) \qquad g_2(z) = 4 \sum_{\gamma=0}^{\alpha} \sum_{\gamma_1=0}^{\alpha_1} \cdots \sum_{\gamma_k=0}^{\alpha_k} \sum_{\delta_1=0}^{\beta_1} \cdots \sum_{\delta_\ell=0}^{\beta_\ell}{}'' \, 1 ,$$

where the double dash ('') denotes that the summation is now taken over those $\gamma, \gamma_1, \ldots, \gamma_k, \delta_1, \ldots, \delta_\ell$ satisfying

$$(8) \quad \begin{cases} \operatorname{Re}((1+i)^{\gamma} \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k} q_1^{\delta_1} \cdots q_\ell^{\delta_\ell}) \\ + \operatorname{Re}(\varepsilon(1+i)^{\alpha-\gamma} \pi_1^{\alpha_1-\gamma_1} \cdots \pi_k^{\alpha_k-\gamma_k} q_1^{\beta_1-\delta_1} \cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv 0 \pmod 2 \\ \text{and} \\ \operatorname{Im}((1+i)^{\gamma} \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k} q_1^{\delta_1} \cdots q_\ell^{\delta_\ell}) \\ + \operatorname{Im}(\varepsilon(1+i)^{\alpha-\gamma} \pi_1^{\alpha_1-\gamma_1} \cdots \pi_k^{\alpha_k-\gamma_k} q_1^{\beta_1-\delta_1} \cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv 0 \pmod 2 . \end{cases}$$

Now as each $\pi_j$ is of the form $u_j + iv_j$, where $u_j$ is <u>odd</u> and $v_j$ is <u>even</u>, the expression

$$(9) \qquad \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k}$$

is of the same form, and as each $q_j$ is odd, so also is

$$(10) \qquad \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k} q_1^{\delta_1} \cdots q_\ell^{\delta_\ell} .$$

Hence

$$(11) \quad \operatorname{Re}((1+i)^{\gamma} \pi_1^{\gamma_1} \cdots \pi_k^{\gamma_k} q_1^{\delta_1} \cdots q_\ell^{\delta_\ell}) \equiv \operatorname{Re}((1+i)^{\gamma}) \pmod 2$$

and

$$(12)\quad \mathrm{Im}((1+i)^{\gamma}\,\pi_1^{\gamma_1}\cdots\pi_k^{\gamma_k}\,q_1^{\delta_1}\cdots q_\ell^{\delta_\ell}) \equiv \mathrm{Im}((1+i)^{\gamma}) \pmod 2 .$$

Similarly

$$(13)\quad \mathrm{Re}(\varepsilon(1+i)^{\alpha-\gamma}\,\pi_1^{\alpha_1-\gamma_1}\cdots\pi_k^{\alpha_k-\gamma_k}\,q_1^{\beta_1-\delta_1}\cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv \mathrm{Re}(\varepsilon(1+i)^{\alpha-\gamma}) \pmod 2$$

and

$$(14)\quad \mathrm{Im}(\varepsilon(1+i)^{\alpha-\gamma}\,\pi_1^{\alpha_1-\gamma_1}\cdots\pi_k^{\alpha_k-\gamma_k}\,q_1^{\beta_1-\delta_1}\cdots q_\ell^{\beta_\ell-\delta_\ell}) \equiv \mathrm{Im}(\varepsilon(1+i)^{\alpha-\gamma}) \pmod 2 .$$

Thus

$$g_2(z) = 4 \sum_{\substack{\gamma=0 \\ \mathrm{Re}((1+i)^{\gamma}) + \mathrm{Re}(\varepsilon(1+i)^{\alpha-\gamma}) \equiv 0 \pmod 2 \\ \mathrm{Im}((1+i)^{\gamma}) + \mathrm{Im}(\varepsilon(1+i)^{\alpha-\gamma}) \equiv 0 \pmod 2}}^{\alpha} \sum_{\gamma_1=0}^{\alpha_1} \cdots \sum_{\gamma_k=0}^{\alpha_k} \sum_{\delta_1=0}^{\beta_1} \cdots \sum_{\delta_\ell=0}^{\beta_\ell} 1$$

and so

$$(15)\quad g_2(z) = 4(\alpha_1+1)\cdots(\alpha_k+1)(\beta_1+1)\cdots(\beta_\ell+1)\,h(\alpha,\varepsilon) ,$$

where

$$(16)\quad h(\alpha,\varepsilon) = \sum_{\substack{\gamma=0 \\ \mathrm{Re}((1+i)^{\gamma}) + \mathrm{Re}(\varepsilon(1+i)^{\alpha-\gamma}) \equiv 0 \pmod 2 \\ \mathrm{Im}((1+i)^{\gamma}) + \mathrm{Im}(\varepsilon(1+i)^{\alpha-\gamma}) \equiv 0 \pmod 2}}^{\alpha} 1$$

Now when $\theta \geq 2$ , $2 | (1+i)^{\theta}$ so

$$\mathrm{Re}((1+i)^{\theta}) \equiv \mathrm{Im}((1+i)^{\theta}) \equiv 0 \pmod 2 .$$

When $\theta = 1$

$$\mathrm{Re}((1+i)^{\theta}) \equiv \mathrm{Im}((1+i)^{\theta}) \equiv 1 \pmod 2$$

and when $\theta = 0$

$$\mathrm{Re}((1+i)^{\theta}) \equiv 1 \pmod 2 , \quad \mathrm{Im}((1+i)^{\theta}) \equiv 0 \pmod 2 .$$

Consequently the only terms which contribute to the sum in (16) are given by

(17) $$\alpha = \gamma = 0 ; \qquad \alpha = 2 , \ \gamma = 1 ; \qquad 2 \leq \gamma \leq \alpha - 2$$

when $\varepsilon = \pm 1$ , and by

(18) $$\alpha = 2 , \ \gamma = 1 ; \qquad 2 \leq \gamma \leq \alpha - 2$$

when $\varepsilon = \pm i$ . Hence finally we have

(19) $$g_2(z) = 4(\alpha_1 + 1) \ldots (\alpha_k + 1)(\beta_1 + 1) \ldots (\beta_\ell + 1) \, h(\alpha, \varepsilon) ,$$

where

$$h(0, \pm 1) = 1 , \qquad h(0, \pm i) = 0 ,$$

$$h(1, \varepsilon) = 0 ,$$

$$h(2, \varepsilon) = 1$$

and

$$h(\alpha, \varepsilon) = \alpha - 3 \qquad (\alpha \geq 3) .$$

It is easy to see that $g_2(z) = 0$ if and only if $h(\alpha, \varepsilon) = 0$ . From the list of values of $h(\alpha, \varepsilon)$ we can verify that this occurs if and only if $y$ is odd or $y$ is even and both $\frac{1}{2}x$ and $\frac{1}{2}y$ are odd integers. This provides an alternative proof of Niven's theorem. Another proof has been given recently by Leahey [1].

## REFERENCES

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

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

Carleton University, Ottawa