T. Ono
Nagoya Math. J.
Vol. 56 (1974) 201-207

ON THE HOPF FIBRATION OVER Z

TAKASHI ONO

§ 1. Statement of the result

Let $h: \boldsymbol{R}^4 \to \boldsymbol{R}^3$ be a quadratic map defined by

$$h(x) = (x_1^2 + x_2^2 - x_3^2 - x_4^2, 2(x_2x_3 - x_1x_4), 2(x_1x_3 + x_2x_4)) .$$

For a natural number t, put

$$S^3(t) = \{x \in \boldsymbol{R}^4, x_1^2 + x_2^2 + x_3^2 + x_4^2 = t\} ,$$
$$S^2(t) = \{y \in \boldsymbol{R}^3, y_1^2 + y_2^2 + y_3^2 = t\} .$$

Then h induces a map

$$h_t: S^3(t) \to S^2(t^2) .$$

Since everything is defined over $\boldsymbol{Z}, h_t$ induces the map

$$h_{t,\boldsymbol{Z}}: S^3(t)_{\boldsymbol{Z}} \to S^2(t^2)_{\boldsymbol{Z}} .$$

Because of the presence of 2 in the last two coordinates of $h(x), h_{t,\boldsymbol{Z}}$ is actually a map

$$h_{t,\boldsymbol{Z}}: S^3(t)_{\boldsymbol{Z}} \to S^2(t^2)_{\boldsymbol{Z}}^{\text{even}} ,$$

where

$$S^2(t^2)_{\boldsymbol{Z}}^{\text{even}} = \{y \in S^2(t^2)_{\boldsymbol{Z}}, y_2, y_3 \text{ are even}\} .$$

To each $y \in S^2(t^2)_{\boldsymbol{Z}}^{\text{even}}$ we shall associate two numbers as follows. First, we denote by $a(y)$ the number of $x \in S^3(t)_{\boldsymbol{Z}}$ such that $h_{t,\boldsymbol{Z}}(x) = y$. Next, we denote by Δ_y the greatest common divisor of the four integers $\frac{1}{2}(t + y_1), \frac{1}{2}(t - y_1), \frac{1}{2}y_2, \frac{1}{2}y_3$. On the other hand, for a natural number n, denote by $r(n)$ the number of integral solutions (X, Y) of the equation $X^2 + Y^2 = n$. It is well known that

$$r(n) = 4(d_1(n) - d_3(n))$$

Received June 11, 1974.

where $d_1(n)$ and $d_3(n)$ are the numbers of divisors of n of the form $4m+1$ and $4m+3$ respectively.

The purpose of the present paper is to prove the relation:

$$a(y) = r(\Delta_y)\ , \qquad y \in S^2(t^2)_{\boldsymbol{Z}}^{\text{even}}\ . \tag{1.1}$$

As the readers notice, (1.1) reflects the fact that each fibre of h_t is a circle.

§ 2. Change of the fibration

Let $\boldsymbol{H}$ be the classical quaternion algebra over $\boldsymbol{R}$ with the quaternion units $1, i, j, k$, with the relations $i^2 = j^2 = -1, k = ij = -ji$. We shall make the following natural identifications:

$$\boldsymbol{C} = \boldsymbol{R} + \boldsymbol{R}i = \boldsymbol{R}^2\ , \qquad \boldsymbol{H} = \boldsymbol{C} + \boldsymbol{C}j = \boldsymbol{C}^2 = \boldsymbol{R}^4\ ,$$
$$\boldsymbol{Z}[i] = \boldsymbol{Z} + \boldsymbol{Z}i = \boldsymbol{Z}^2\ , \qquad \boldsymbol{H}_{\boldsymbol{Z}} = \boldsymbol{Z}[i] + \boldsymbol{Z}[i]j = \boldsymbol{Z}[i]^2 = \boldsymbol{Z}^4\ .$$

As usual, for each $z = x + yj \in \boldsymbol{H}, x, y \in \boldsymbol{C}$, we write its conjugate, trace and norm by $\bar{z} = \bar{x} - yj, \operatorname{Tr} z = \bar{z} + z$ and $Nz = \bar{z}z$, respectively. In working with $\boldsymbol{H}$, we shall mean by $\boldsymbol{R}^3$ the subspace $\boldsymbol{R}i + \boldsymbol{R}j + \boldsymbol{R}k = \boldsymbol{R}i + \boldsymbol{C}j$. This space is known as the space of pure quaternions and is characterized as the set of all $z \in \boldsymbol{H}$ such that $\operatorname{Tr} z = 0$.

For $z \in \boldsymbol{H}$, put

$$h(z) = \bar{z}iz\ . \tag{2.1}$$

Since $\operatorname{Tr}(h(z)) = 0$, h is a map: $\boldsymbol{R}^4 \to \boldsymbol{R}^3$. A simple calculation shows that

$$\begin{aligned} h(z) &= (Nx - Ny)i + 2\bar{x}yk \\ &= (x_0^2 + x_1^2 - y_0^2 - y_1^2)i + 2(x_1y_0 - x_0y_1)j + 2(x_0y_0 + x_1y_1)k\ , \end{aligned} \tag{2.2}$$

where $z = x + yj$, $x = x_0 + x_1i$, $y = y_0 + y_1i$, $x_0, x_1, y_0, y_1 \in \boldsymbol{R}$. Hence the map (2.1) coincides with the map h introduced in § 1.

For $t > 0$, put

$$S^3(t) = \{z \in \boldsymbol{R}^4, Nz = t\}\ , \qquad S^2(t) = \{w \in \boldsymbol{R}^3, Nw = t\}\ .$$

Since $N(h(z)) = (Nz)^2$ by (2.1), h induces a map

$$h_t : S^3(t) \to S^2(t^2)\ .$$

When t is a natural number, put

$$S^3(t)_Z = S^3(t) \cap Z^4 , \qquad S^2(t)_Z = S^2(t) \cap Z^3 .$$

Then, h_t induces a map

$$h_{t,Z} \colon S^3(t)_Z \to S^2(t^2)_Z .$$

Our problem is to determine the image and the fibres of the map $h_{t,Z}$. To do this, it is convenient to replace the map h_t by a map f_t in the following way. Namely, put

$$\sum(t) = \{\sigma = (\alpha, \beta, \gamma), \alpha, \beta \in \boldsymbol{R}, \gamma \in \boldsymbol{C}, \alpha + \beta = t, N\gamma = \alpha\beta\} ,$$

and $f_t(z) = (Nx, Ny, i\bar{x}y)$ for $z = x + yj \in S^3(t)$.

$$\begin{array}{ccc} & S^3(t) & \\ {}^{h_t}\swarrow & & \searrow^{f_t} \\ S^2(t^2) & \underset{g_t}{\longleftarrow} & \Sigma(t) \end{array}$$

Since $Nx + Ny = Nz = t$ and $N(i\bar{x}y) = (Nx)(Ny)$, f_t is a map $S^3(t) \to \Sigma(t)$. Next, put

$$g_t(\sigma) = (\alpha - \beta)i + 2\gamma j , \qquad \text{for } \sigma = (\alpha, \beta, \gamma) \in \Sigma(t) .$$

Since $N(g_t(\sigma)) = (\alpha - \beta)^2 + N(2\gamma) = (\alpha - \beta)^2 + 4\alpha\beta = (\alpha + \beta)^2 = t^2$, g_t is a map $\Sigma(t) \to S^2(t^2)$. If $g_t(\sigma) = g_t(\sigma')$ with $\sigma' = (\alpha', \beta', \gamma')$, then $\alpha - \beta = \alpha' - \beta'$ and $\gamma = \gamma'$. Since $\alpha + \beta = \alpha' + \beta' = t$, we see that g_t is injective. For any $w = ui + vj \in S^2(t^2)$, we have $w = g_t(\sigma)$ with

$$\sigma = (\tfrac{1}{2}(t + u), \tfrac{1}{2}(t - u), \tfrac{1}{2}v) . \tag{2.3}$$

Hence g_t is surjective, and so bijective. Finally, it follows from (2.2) that $g_t(f_t(z)) = g_t(Nx, Ny, i\bar{x}y) = (Nx - Ny)i + 2i\bar{x}yj = (Nx - Ny)i + 2\bar{x}yk = h_t(z)$, the commutativity of the diagram.

Now, for a natural number t, put

$$\Sigma(t)_Z = \Sigma(t) \cap (Z^2 + Z[i]) .$$

Then, f_t, g_t induce maps

$$f_{t,Z} \colon S^3(t)_Z \to \Sigma(t)_Z , \qquad g_{t,Z} \colon \Sigma(t)_Z \to S^2(t^2)_Z ,$$

respectively such that $g_{t,Z} f_{t,Z} = h_{t,Z}$. If $w = ui + vj \in S^2(t^2)_Z$ is in the image of $g_{t,Z}, v$ must be a multiple of 2 in $\boldsymbol{Z}[i]$ and, since $Nw = u^2 + Nv$

$= t^2$, both $t + u$ and $t - u$ must be even. In view of (2.3), we see that $g_{t,Z}$ is a bijection between $\Sigma(t)_Z$ and the set $S^2(t^2)_Z^{\text{even}} = \{w = ui + vj \in S^2(t^2)_Z, 2|v\}$. Hence, to study the map $h_{t,Z}$ is equivalent to study the map $f_{t,Z}$.

$$\begin{array}{ccc} & S^3(t)_Z & \\ {}^{h_{t,Z}}\swarrow & & \searrow^{f_{t,Z}} \\ S^2(t^2)_Z^{\text{even}} & \underset{g_{t,Z}}{\longleftarrow} & \Sigma(t)_Z \end{array}$$

§ 3. Existence of solutions

Notation being as in § 2, we shall determine for what $\sigma \in \Sigma(t)_Z$ the equation $f_{t,Z}(z) = \sigma$ has a solution $z \in S^3(t)_Z$. In the following, we shall put $\sigma = (\alpha, \beta, \gamma)$, $\alpha, \beta \in \boldsymbol{Z}$, $\gamma = \gamma_0 + \gamma_1 i \in \boldsymbol{Z}[i]$, $\gamma_0, \gamma_1 \in \boldsymbol{Z}$. We shall first examine some special cases.

Case 1. $\gamma = 0$.

In this case, the relations $\alpha + \beta = t$ and $0 = N\gamma = \alpha\beta$ imply that either $\alpha = 0$, $\beta = t$ or $\alpha = t$, $\beta = 0$, i.e. $\sigma = (0, t, 0)$ or $(t, 0, 0)$. Hence $z = x + yj$ is a solution of $f_{t,Z}(z) = \sigma$ if and only if either $z = yj$, $Ny = t$ or $z = x$, $Nx = t$. Therefore it follows that

$$f_{t,Z}^{-1}(\sigma) \neq \emptyset \Leftrightarrow t \in N(\boldsymbol{Z}[i]) \,. \tag{3.1}$$

Case 2. $\gamma \neq 0$ and $(\gamma_0, \gamma_1) = 1$.

Assumptions imply that $\alpha, \beta \geqq 1$. Since $\alpha\beta = N\gamma = \gamma_0^2 + \gamma_1^2$, we have $(\gamma_1, \alpha) = 1$. Therefore, there are two integers r, s such that $\gamma_0 = r\gamma_1 + s\alpha$. Put $I = \boldsymbol{Z}\alpha + \boldsymbol{Z}(r + i)$. We claim that I is an ideal. It is enough to show that $i\alpha, i(r + i) \in I$. Firstly, $i\alpha = -r\alpha + (r + i)\alpha \in I$. Secondly, we have

$$\alpha\beta = N\gamma = \gamma_0^2 + \gamma_1^2 = (r\gamma_1 + s\alpha)^2 + \gamma_1^2 = (1 + r^2)\gamma_1 + 2rs\gamma_1\alpha + s^2\alpha^2 \,,$$

and so $(1 + r^2)\gamma_1 = \alpha(\beta - 2rs\gamma_1 - s^2\alpha)$. Since $(\gamma_1, \alpha) = 1$, α must divide $1 + r^2$: write $1 + r^2 = \alpha\alpha'$. Then, we have

$$i(r + i) = ir - 1 = r(r + i) - \alpha\alpha' \in I \,,$$

which shows that I is an ideal. Since $\boldsymbol{Z}[i]$ is a principal ideal ring, there is an $x \in \boldsymbol{Z}[i]$ such that $I = (\bar{x})$. Hence $Nx = N\bar{x} = NI = \alpha$. Since $\gamma = \gamma_0 + \gamma_1 i = (r\gamma_1 + s\alpha) + \gamma_1 i = (r + i)\gamma_1 + si\alpha \in I$, we can find $y \in \boldsymbol{Z}[i]$ such that $\gamma = i\bar{x}y$. Then the relation $N\gamma = \alpha\beta$ implies that $Ny = \beta$. If we put $z = x + yj$, then we have $f_{t,Z}(z) = (Nx, Ny, i\bar{x}y) = (\alpha, \beta, \gamma) = \sigma$. Hence $f_{t,Z}^{-1}(\sigma) \neq \emptyset$ in this case.

Case 3. $\gamma \neq 0$ and $(\alpha, \beta, \gamma_0, \gamma_1) = 1$.

Put $(\gamma_0, \gamma_1) = d_0, (d_0, \alpha) = d_1$. Hence we have $\gamma_0 = d_0\gamma_0', \gamma_1 = d_0\gamma_1'$ with $(\gamma_0', \gamma_1') = 1$ and $d_0 = d_1 d_0^*, \alpha = d_1\alpha^*$ with $(\alpha^*, d_0^*) = 1$. From

$$d_1\alpha^*\beta = \alpha\beta = N\gamma = \gamma_0^2 + \gamma_1^2 = d_1^2 d_0^{*2}(\gamma_0'^2 + \gamma_1'^2)$$

we get

$$\alpha^*\beta = d_1 d_0^{*2}(\gamma_0'^2 + \gamma_1'^2) . \tag{3.2}$$

Since d_1 divides $\alpha, \gamma_0, \gamma_1$ and $(\alpha, \beta, \gamma_0, \gamma_1) = 1$, we have $(d_1, \beta) = 1$ and hence d_1 divides $\alpha^* : \alpha^* = d_1\alpha'$. On the other hand, since $(\alpha^*, d_0^*) = 1, d_0^{*2}$ divides $\beta : \beta = d_0^{*2}\beta'$. Then (3.2) implies that

$$\alpha'\beta' = N\gamma' , \quad \gamma' = \gamma_0' + \gamma_1' i , \quad (\gamma_0', \gamma_1') = 1 .$$

Hence, by the argument in Case 2 one can find $x', y' \in \boldsymbol{Z}[i]$ such that $Nx' = \alpha', Ny' = \beta', \gamma' = i\bar{x}'y'$. Put $x = d_1 x', y = d_0^* y'$. Then, we have $Nx = d_1^2 Nx' = d_1^2\alpha' = d_1(d_1\alpha') = d_1\alpha^* = \alpha$, $Ny = d_0^{*2}Ny' = d_0^{*2}\beta' = \beta$, $i\bar{x}y = id_1 d_0^* \bar{x}'y' = d_1 d_0^*\gamma' = d_0\gamma' = \gamma$. Hence we still have $f_{t,Z}^{-1}(\sigma) \neq \emptyset$ in this case.

We are now ready to prove the following criterion for the existence of solutions. For $\sigma = (\alpha, \beta, \gamma) \in \Sigma(t)_Z$, put $\Delta_\sigma = (\alpha, \beta, \gamma_0, \gamma_1)$ where $\gamma = \gamma_0 + \gamma_1 i$. Then we have

$$f_{t,Z}^{-1}(\sigma) \neq \emptyset \Leftrightarrow \Delta_\sigma \in N(\boldsymbol{Z}[i]) . \tag{3.3}$$

Proof. When $\gamma = 0$, we have $\Delta_\sigma = (\alpha, \beta) = t$ and the assertion is nothing but (3.1). Hence, from now on, we shall assume that $\gamma \neq 0$. ($\Rightarrow$) Take $z = x + yj \in S^3(t)_Z$ such that $f_t(z) = \sigma$. Thus we have $\alpha = Nx$, $\beta = Ny, \gamma = i\bar{x}y$. Put $\alpha = \Delta_\sigma\alpha', \beta = \Delta_\sigma\beta', \gamma_0 = \Delta_\sigma\gamma_0', \gamma_1 = \Delta_\sigma\gamma_1'$. Then, by the argument in Case 3, there are $x', y' \in \boldsymbol{Z}[i]$ such that $Nx' = \alpha'$, $Ny' = \beta'$, $\gamma' = i\bar{x}'y'$, where $\gamma' = \gamma_0' + \gamma_1' i$. Since $\alpha = \Delta_\sigma\alpha'$, we have $Nx = \Delta_\sigma Nx'$, i.e. $\Delta_\sigma = N(x/x')$. Then we have $\Delta_\sigma = N\delta, \delta \in \boldsymbol{Z}[i]$, e.g. by the lemma of Davenport-Cassels applied to the binary form $X^2 + Y^2$.*)

($\Leftarrow$) Let x', y' be as in the proof of ($\Rightarrow$). By the assumption, there is a number $\delta \in \boldsymbol{Z}[i]$ such that $\Delta_\sigma = N\delta$. Put $x = \delta x', y = \delta y'$. Then, $Nx = \Delta_\sigma Nx' = \Delta_\sigma\alpha' = \alpha, Ny = \Delta_\sigma Ny' = \Delta_\sigma\beta' = \beta, i\bar{x}y = i\bar{\delta}\bar{x}'\delta y' = \Delta_\sigma\gamma' = \gamma$. Hence, we have $f_{t,Z}(z) = \sigma$ with $z = x + yj$, q.e.d.

Translating (3.3) in terms of $h_{t,Z}$, we obtain the following criterion.

*) See, e. g. J-P. Serre, Cours d'arithmétique, Paris, 1970, p. 80.

Notation being as in § 2, for $w = ui + vj \in S^2(t^2)_Z$, $u \in Z$, $v = v_0 + v_1 i \in Z[i]$, we have

(3.4) $$h_{t,Z}^{-1}(w) \neq \emptyset \Leftrightarrow 2|v \quad \text{and} \quad \Delta_w \in N(Z[i]) ,$$

where $\Delta_w = (\frac{1}{2}(t+u), \frac{1}{2}(t-u), \frac{1}{2}v_0, \frac{1}{2}v_1)$.

§ 4. Number of solutions

For a finite set F, we denote by Card F the number of elements in it. Thus $r(n) = \mathrm{Card}\,\{(x, y) \in Z^2, x^2 + y^2 = n\}$. Using notations in § 2, § 3, one restates the proposition (1.1) as

(4.1) $$\mathrm{Card}\,(h_{t,Z}^{-1}(w)) = r(\Delta_w) \qquad \text{for any } w \in S^2(t^2)_Z^{\text{even}} .$$

Translating (4.1) in terms of $f_{t,Z}$, we are reduced to prove that

(4.2) $$\mathrm{Card}\,(f_{t,Z}^{-1}(\sigma)) = r(\Delta_\sigma) \qquad \text{for any } \sigma \in \Sigma(t)_Z .$$

Proof. Put, as before, $\sigma = (\alpha, \beta, \gamma)$. In case $\gamma = 0$, since $\Delta_\sigma = t$, (4.2) follows from the argument in § 3, Case 1. Hence, from now on, we shall assume that $\gamma \neq 0$. Since we already have the criterion (3.3), it is enough to consider the case where $f_{t,Z}^{-1}(\sigma) \neq \emptyset$. So, take a point $z = x + yj \in f_{t,Z}^{-1}(\sigma)$ and call I_z the ideal in $Z[i]$ generated by x and y: $I_z = Z[i]x + Z[i]y$. Let $z' = x' + y'j$ be another point in the same fibre as z. We want to compare I_z and $I_{z'}$. Since $f_{t,Z}(z) = f_{t,Z}(z')$, we have $Nx = Nx'$, $Ny = Ny'$, $\bar{x}y = \bar{x}'y'$. From these relations, we see that there is an element $\rho \in Q(i)$ with $N\rho = 1$ such that $x' = \rho x$, $y' = \rho y$. It then follows that $I_{z'} = \rho I_z$ and so $NI_{z'} = NI_z = n_\sigma$, a natural number depending only on $\sigma \in \Sigma(t)_Z$. For a natural number n, Put:

$$\Theta(n) = \{\theta \in Z[i], N\theta = n\} .$$

Hence we have $\mathrm{Card}\,(\Theta(n_\sigma)) = r(n_\sigma)$. We shall show that there is a bijection between $f_{t,Z}^{-1}(\sigma)$ and $\Theta(n_\sigma)$. To do this, fix a point $\zeta = \xi + \eta j \in f_{t,Z}^{-1}(\sigma)$ and, for any $z = x + yj \in f_{t,Z}^{-1}(\sigma)$, denote by ρ_z the element in $Q(i)$ with $N\rho_z = 1$ such that $x = \rho_z \xi$, $y = \rho_z \eta$. Since $Z[i]$ is a principal ideal ring, there is an element $\omega \in Z[i]$ such that $I_\zeta = (\omega)$. Put

$$T(z) = \omega\rho_z , \qquad z \in f_{t,Z}^{-1}(\sigma) .$$

We claim that T is the bijection we are looking for. First of all, write $\omega = \lambda\xi + \mu\eta$, $\lambda, \mu \in Z[i]$. Then, $T(z) = \omega\rho_z = \lambda\xi\rho_z + \mu\eta\rho_z = \lambda x + \mu y \in Z[i]$

and $N(T(z)) = N\omega = NI_\zeta = n_\sigma$, which shows that T maps $f_{t,Z}^{-1}(\sigma)$ into $\Theta(n_\sigma)$. Next, assume that $T(z) = T(z')$. Then, we have $\rho_z = \rho_{z'}$ and hence $x = x'$, $y = y'$, i.e. $z = z'$. To see that T is surjective, take any $\theta \in \Theta(n_\sigma)$ and put $x = \theta\omega^{-1}\xi$, $y = \theta\omega^{-1}\eta$, $z = x + jy$. Since $I_\zeta = (\omega)$, we have $\xi = a\omega$, $\eta = b\omega$ with $a, b \in \boldsymbol{Z}[i]$. It follows that $x = \theta a$ and $y = \theta b$ both belong to $\boldsymbol{Z}[i]$. Now, since $Nx = N(\theta)n_\sigma^{-1}N\xi = N\xi = \alpha$, $Ny = N(\theta)n_\sigma^{-1}N\eta = N\eta = \beta$, we have $Nz = Nx + Ny = \alpha + \beta = t$, i.e. $z \in S^3(t)_{\boldsymbol{Z}}$. Furthermore, we have $i\bar{x}y = i\bar{\theta}\bar{\omega}^{-1}\bar{\xi}\theta\omega^{-1} = iN(\theta)n_\sigma^{-1}\bar{\xi}\eta = i\bar{\xi}\eta = \gamma$, which shows that $z \in f_{t,Z}^{-1}(\sigma)$. Finally, since $x = \theta\omega^{-1}\xi$, $y = \theta\omega^{-1}\eta$, we have $\rho_z = \theta\omega^{-1}$ and so $T(z) = \rho_z\omega = \theta$, which completes the proof of the surjectivity of T. In order to complete the proof of (4.2), we must show that

$$n_\sigma = \Delta_\sigma \qquad \text{whenever } f_{t,Z}^{-1}(\sigma) \neq \emptyset \ . \tag{4.3}$$

First, observe that $I_\zeta \bar{I}_\zeta = (n_\sigma)$ and so $n_\sigma = (\xi\bar{\xi}, \eta\bar{\eta}, \xi\bar{\eta} + \bar{\xi}\eta) = (\alpha, \beta, 2\gamma_1)$. From the relation $\alpha\beta = \gamma_0^2 + \gamma_1^2$, one sees easily that n_σ and Δ_σ contain each odd prime p with the same exponent. Hence, it remains to examine the exponent of 2. Denote by $\nu_2(a)$ the exponent of 2 in an integer a. Since we obviously have $\nu_2(\Delta_\sigma) \leqq \nu_2(n_\sigma)$, it is enough to show that $\nu_2(n_\sigma) \leqq \nu_2(\Delta_\sigma)$. Hence, we may assume that $\nu_2(n_\sigma) \geqq 1$. Put $e = \nu_2(n_\sigma)$ and write $\alpha = 2^e\alpha^*$, $\beta = 2^e\beta^*$, $\gamma_1 = 2^{e-1}\gamma_1^*$ and $\gamma_0 = 2^f\gamma_0^*$ with $(2, \gamma_0^*) = 1$. We have then $2^{2e}\alpha^*\beta^* = 2^{2f}\gamma_0^{*2} + 2^{2(e-1)}\gamma_1^{*2}$, or $2^{2f}\gamma_0^{*2} = 2^{2(e-1)}(4\alpha^*\beta^* - \gamma_1^{*2})$. If γ_1^* were odd, we must have $f = e - 1$, and then $4\alpha^*\beta^* = \gamma_0^{*2} + \gamma_1^{*2}$, which is impossible because both of γ_0^*, γ_1^* are odd. Therefore, γ_1^* must be even and so we have $e \leqq \inf(\nu_2(\gamma_1), \ \nu_2(\gamma_0))$, which implies that $\nu_2(n_\sigma) \leqq \nu_2(\Delta_\sigma)$, q.e.d.

The Johns Hopkins University