A Comment on Denef's Paper *Hilbert's Tenth Problem for Quadratic Rings*

Jaap van Oosten

November 7, 2013

We work in $A(D)$, the ring of integers of $\mathbb{Q}(\sqrt{D})$, where D is assumed to be a square-free integer > 1. We know that $A(D)$ is of the form $\mathbb{Z}[\omega]$ with either $\omega = \sqrt{D}$ (if $D = 2$ or $D \equiv 3 \bmod 4$) or $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{D}$ (if $D \equiv 1 \bmod 4$).

For an element $x = a + b\sqrt{D}$ of $A(D)$ we write $\bar{x} = a - b\sqrt{D}$ and $N(x) = a^2 - Db^2 = x\bar{x}$; $N(x)$ is called the *norm* of x.

Remark 1. Let D' be a square-free integer > 1, different from D. Then for $x, y \in A(D)$ we have: $x = 0$ and $y = 0$ if and only if $x^2 - D'y^2 = 0$.
Proof. The 'only if' part is trivial so assume $x^2 - D'y^2 = 0$. If $y = 0$ then clearly $x = 0$ so we're done; assume $y \neq 0$. Write the equation as $(x - y\sqrt{D'})(x + y\sqrt{D'}) = 0$. We see that $\frac{x}{y} = \pm\sqrt{D'}$ so $\frac{x\bar{y}}{N(y)} = \pm\sqrt{D'}$ from which we conclude that D' is a square in $\mathbb{Q}(\sqrt{D})$. Let $\alpha, \beta \in \mathbb{Q}$ be such that $(\alpha + \beta\sqrt{D})^2 = D'$. That means:

(1) $\alpha^2 + D\beta^2 = D'$

(2) $2\alpha\beta = 0$

If $\beta = 0$ then $\alpha^2 = D'$ but this is impossible because $\alpha \in \mathbb{Q}$ and D' is not a square. If $\alpha = 0$ then $D\beta^2 = D'$. Writing $\beta = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ coprime, we obtain $Dp^2 = D'q^2$. So $p^2 | D'q^2$ but p^2 and q^2 are coprime; hence $p^2 | D'$. If $p > 1$ this contradicts the assumption that D' is square-free; if $p = 1$ we have $D = D'q^2$ which contradicts the assumption that D is square-free unless $q = 1$; but clearly, $p = 1, q = 1$ is no solution since $D' > 1$.

The point of Remark 1 is that Diophantine relations over $A(D)$ are closed under $\wedge$ and $\vee$: if

$$\begin{array}{rcl} R & = & \{\vec{a} \in A(D) \,|\, \exists \vec{x} P(\vec{a}, \vec{x}) = 0\} \\ S & = & \{\vec{b} \in A(D) \,|\, \exists \vec{y} Q(\vec{b}, \vec{y}) = 0\} \end{array}$$

for diophantine polynomials P and Q, then

$$R \wedge S = \{(\vec{a}, \vec{b}) \in A(D) \,|\, \vec{a} \in R \text{ and } \vec{b} \in S\}$$

can be written as

$$\{(\vec{a}, \vec{b}) \in A(D) \,|\, \exists \vec{x}\vec{y}[(P(\vec{a}, \vec{x})^2 - D' Q(\vec{b}, \vec{y})^2 = 0]\}$$

and, as usual, $R \vee S$ can be written as

$$\{(\vec{a}, \vec{b}) \in A(D) \,|\, \exists \vec{x}\vec{y}[P(\vec{a}, \vec{x}) Q(\vec{b}, \vec{y}) = 0]\}$$

Knowing this, we can reformulate the 'main Lemma' as follows:

Main Lemma. *For every quadratic ring $A(D)$ there is a Diophantine relation $\Sigma(t, \vec{a})$ (writing $\vec{a}$ for $(a_1, \ldots, a_n)$) such that the following hold:*

1) *For all $n+1$-tuples $(t, \vec{a})$ of $A(D)$, if $(t, \vec{a}) \in \Sigma$ then $t \in \mathbb{Z}$*

2) *For every natural number $k > 0$, there is $\vec{a}$ in $A(D)$ such that $(k^2, \vec{a}) \in \Sigma$*

With Main Lemma we can prove that $\mathbb{N}$ is Diophantine over $A(D)$. First, we show that $\mathbb{Z}$ is Diophantine.

Indeed we have:

$$\begin{array}{rcl} x \in \mathbb{Z} & \Leftrightarrow & \exists t_1 \cdots t_4 \exists \vec{a_1} \cdots \vec{a}_4 \\ & & ((t_1, \vec{a}_1) \in \Sigma \text{ or } t_1 = 0) \text{ and} \\ & & \vdots \\ & & ((t_4, \vec{a}_4) \in \Sigma \text{ or } t_4 = 0) \text{ and} \\ & & x = t_1 + \cdots + t_4 \text{ or } x + t_1 + \cdots + t_4 = 0 \end{array}$$

Clearly, if RHS holds then $x = \pm(t_1 + \cdots + t_4)$ and $t_1, \ldots, t_4 \in \mathbb{Z}$ by a) of Main Lemma, so $x \in \mathbb{Z}$.
Conversely if $x \in \mathbb{Z}$, write $|x|$ as sum of four squares $k_1^2 + \cdots + k_4^2$, with $k_i \in \mathbb{N}$. Let $t_i = k_i^2$. If $t_i = 0$ let $\vec{a}_i$ be arbitrary; if $t_i > 0$ take $\vec{a}_i$ as in b) of Main Lemma. Then RHS is satisfied.

Finally

$$x \in \mathbb{N} \;\Leftrightarrow\; \exists y_1 \cdots y_4 \,(y_1, \ldots y_4 \in \mathbb{Z} \text{ and } x = y_1^2 + \cdots + y_4^2)$$

so N is Diophantine over $A(D)$, as required.