PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 48, Number 1, March 1975

HILBERT'S TENTH PROBLEM FOR QUADRATIC RINGS

J. DENEF[1]

ABSTRACT. Let $\mathbf{A}(D)$ be any quadratic ring; in this paper we prove that Hilbert's tenth problem for $\mathbf{A}(D)$ is unsolvable, and we determine which relations are diophantine over $\mathbf{A}(D)$.

1. **Introduction.** A *quadratic ring* $\mathbf{A}(D)$ is the ring of algebraic integers of the quadratic field $\mathbf{Q}(\sqrt{D})$, with D a square-free rational integer. A polynomial is called *diophantine* if its coefficients are rational integers. A *diophantine equation* is an equation of the form $P(x_1, \cdots, x_n) = 0$, where $P(x_1, \cdots, x_n)$ is a diophantine polynomial. In this paper, a relation $R(x_1, \cdots, x_n)$ in $\mathbf{A}(D)$ is called *diophantine over* $\mathbf{A}(D)$ if there exists a diophantine polynomial $P(x_1, \cdots, x_n, y_1, \cdots, y_m)$ such that $R(x_1, \cdots, x_n)$ holds if and only if there exist $y_1, \cdots, y_m$ in $\mathbf{A}(D)$ such that $P(x_1, \cdots, x_n, y_1, \cdots, y_m) = 0$. By definition, a relation is *recursively enumerable* if there exists an algorithm to enumerate the n-tuples for which the relation holds. In this paper, a relation $R(x_1, \cdots, x_n)$ in $\mathbf{A}(D)$ is called *self-conjugate in* $\mathbf{A}(D)$ if $R(x_1, \cdots, x_n)$ holds if and only if $R(\overline{x}_1, \cdots, \overline{x}_n)$ holds, where $\overline{x}_i$ is the conjugate of x_i in $\mathbf{A}(D)$.

We use the following notations: $\mathbf{N}$ is the set of natural numbers 0, 1, 2, $\cdots$; $\mathbf{Z}$ is the set of rational integers; $\mathbf{Q}$ is the set of rational numbers. Where the contrary is not explicitly stated, capital Latin letters stand for rational integers, and lower case Latin letters, except n, k, m, j, stand for elements of $\mathbf{A}(D)$. n, k run over $\mathbf{N}$. m, j run over $\mathbf{Z}$. D always stands for a fixed square-free rational integer. By $N(x)$, we mean the norm of x in $\mathbf{A}(D)$: $N(x) = x\overline{x}$.

The main results of this paper are the following two theorems:

Received by the editors October 24, 1973.
AMS (MOS) subject classifications (1970). Primary 02F50, 10N05, 10B99, 12L05, 02E15.
Key words and phrases. Hilbert's tenth problem, unsolvable problems, diophantine equations, recursive functions.

[1]Yu. Matijasevič suggested my treating Hilbert's tenth problem for the Gaussian integers. I am also grateful to C. Smorynski and E. Vantieghem for giving me some useful advice.

Theorem 1. *Let* $\mathbf{A}(D)$ *be a quadratic ring. There cannot exist an algorithm to decide whether or not a given diophantine equation has a solution in* $\mathbf{A}(D)$; *i.e. Hilbert's tenth problem for the quadratic ring* $\mathbf{A}(D)$ *is unsolvable.*

Theorem 2. *A relation is diophantine*[2] *over* $\mathbf{A}(D)$ *if and only if the relation is recursively enumerable and self-conjugate in* $\mathbf{A}(D)$.

These theorems are analogues of the famous results of M. Davis, Yu. Matijasevič, H. Putnam and J. Robinson [2] concerning Hilbert's tenth problem for the rational integers. In view of their results we only have to prove that the relation $x \in \mathbf{N}$ is diophantine over $\mathbf{A}(D)$.

Let D' be a square-free rational integer, different from D, and let $x, y \in \mathbf{A}(D)$; then $x = 0$ and $y = 0$ if and only if $x^2 - D'y^2 = 0$. Moreover, by Lagrange's theorem, every natural number is the sum of four squares of natural numbers. By those two facts it is sufficient to prove the

Main lemma. *For every quadratic ring* $\mathbf{A}(D)$ *there exists a (finite) system* Σ *of diophantine equations in the unknowns* $t, x, \cdots, s$ *such that the following two conditions are satisfied*:

(1) *If* Σ *has a solution* $\langle t, x, \cdots, s \rangle$ *in* $\mathbf{A}(D)$, *then* $t \in \mathbf{Z}$.

(2) *If* $k \in \mathbf{N}$ *and* $k \neq 0$, *then* Σ *has a solution* $\langle t, x, \cdots, s \rangle$ *in* $\mathbf{A}(D)$ *with* $t = k^2$.

We construct such a system of diophantine equations in §2 for real quadratic rings and in §3 for imaginary quadratic rings; this will complete the proof of Theorems 1 and 2.

First we consider some lemmas concerning the solutions in $\mathbf{N}$ of the so-called Pell equation:

$$X^2 - PY^2 = 1. \tag{1}$$

The first two lemmas are standard results from number theory.

Lemma 1. *If* $P \in \mathbf{N}$, *and* P *is not a square, then there exist natural numbers* X *and* Y, *with* $Y \neq 0$, *satisfying* (1).

Definition. *For* $A \in \mathbf{N}$, $A > 1$, $n \in \mathbf{N}$, *we define* $X_n(A)$, $Y_n(A)$, *by setting*:

---

[2] If we change the definition of "diophantine relation" by permitting not only polynomials with rational integer coefficients, but also polynomials with arbitrary coefficients from the quadratic ring, then the analogue to Theorem 2 is obtained by simply omitting the words "and self-conjugate".

$$X_n(A) + (A^2 - 1)^{1/2} Y_n(A) = (A + (A^2 - 1)^{1/2})^n, \qquad X_n(A),\ Y_n(A) \in \mathbf{N}.$$

Where the context permits, the dependence on A is not explicitly shown, writing X_n, Y_n.

Lemma 2. *If $P = A^2 - 1$, $A \in \mathbf{N}$, and $A > 1$, then all solutions in $\mathbf{N}$ of the Pell equation (1) are given by $X = X_n(A)$, $Y = Y_n(A)$.*

Lemma 3. *If A, n, k are in $\mathbf{N}$, and $A > 1$, then*

$$(Y_{nk}(A))^2 \equiv (Y_n(A))^2 k^2 \pmod{(Y_n(A))^4}.$$

Proof. It is well known that

$$Y_{nk} = \sum_{j=1;\, j \text{ odd}}^{k} \binom{k}{j} (A^2 - 1)^{(j-1)/2} X_n^{k-j} Y_n^j.$$

So,

$$Y_{nk} \equiv k X_n^{k-1} Y_n \pmod{Y_n^3} \quad \text{and} \quad (Y_{nk}/Y_n) \equiv k X_n^{k-1} \pmod{Y_n^2}.$$

Squaring yields:

$$(Y_{nk}/Y_n)^2 \equiv k^2 (X_n^2)^{k-1} \pmod{Y_n^2}.$$

But in virtue of Lemma 2 we also have $X_n^2 \equiv 1 \pmod{Y_n^2}$.

2. The main lemma for real quadratic rings.

Lemma 4. *Let $\mathbf{A}(D)$ be a real quadratic ring, i.e. $D > 1$. Let $\langle A, B \rangle$ be one of the solutions in $\mathbf{N}$ of the Pell equation $A^2 - DB^2 = 1$, with $B \neq 0$ (cf. Lemma 1). Set $E = A^2 - 1$. If $x^2 - Ey^2 = 1$ and $x, y \in \mathbf{A}(D)$, then $y^2 \in \mathbf{N}$.*

Proof. Obviously $A > 1$ and $E = B^2 D$. We have $(x - B\sqrt{D}y)(x + B\sqrt{D}y) = 1$; thus $x + B\sqrt{D}y$ is a unit in $\mathbf{A}(D)$. Set $u = x + B\sqrt{D}y$; then $u^{-1} = x - B\sqrt{D}y$. Subtracting and squaring yield: $4B^2 D y^2 + 2 = u^2 + (u^{-1})^2$. Since u is a unit, $N(u) = \pm 1$, and $u^{-1} = \pm \bar{u}$. Hence, $4B^2 D y^2 + 2 = u^2 + \bar{u}^2$. Thus $4B^2 D y^2 + 2 \in \mathbf{Q}$, $y^2 \in \mathbf{Q}$. But $y^2 \in \mathbf{A}(D)$, so $y^2 \in \mathbf{Z}$; and since $D > 1$, $y^2 \in \mathbf{N}$.

Lemma 5. *Let $D > 1$, and $x, y, z \in \mathbf{A}(D)$. If $x \equiv y \pmod{z}$ and $0 \leq x < z$, $0 \leq \bar{x} < \bar{z}$, $0 \leq y < z$, $0 \leq \bar{y} < \bar{z}$, then $x = y$.*

Proof. Suppose $x \neq y$; then $x - y = zw$, with $w \neq 0$. So

$$|x - y||\bar{x} - \bar{y}| = |z\bar{z}||N(w)|.$$

Since $w \neq 0$, $|N(w)| \geq 1$, hence $|x - y||\bar{x} - \bar{y}| \geq |z\bar{z}|$. But this is in contradiction with the hypothesis of the lemma.

Lemma 6. *Let* $\mathbf{A}(D)$ *be a real quadratic ring, i.e.* $D > 1$. *Let* E *be as defined in the hypothesis of Lemma* 4, *and let* Σ *be the following system of diophantine equations* (1)–(5) *in the unknowns* $t, x, y, u, v, z, w, h, q, r, s$.

(1) $x^2 - Ey^2 = 1$,

(2) $u^2 - Ev^2 = 1$,

(3) $v^2 - y^2 t = zy^4$,

(4) $t = w^2$,

(5) $y^2 - t = 1 + h^2 + q^2 + r^2 + s^2$.

Then conditions (1) *and* (2) *of the main lemma are satisfied.*

Proof. (1) Suppose that $t, x, \cdots, s$ are in $\mathbf{A}(D)$, and satisfy (1)–(5). From (1), (2) and Lemma 4 we have: $y^2 \in \mathbf{N}$, $v^2 \in \mathbf{N}$. From (3) follows $(v^2/y^2) \equiv t \pmod{y^2}$, thus $(v^2/y^2) \equiv \bar{t} \pmod{y^2}$. Hence $t \equiv \bar{t} \pmod{y^2}$. By (4) and (5): $0 \leq t < y^2$, $0 \leq \bar{t} < y^2$. Using Lemma 5, we obtain $t = \bar{t}$. So $t \in \mathbf{N}$.

(2) Suppose $t = k^2$, $k \in \mathbf{N}$. Take n, such that $Y_n(A) > k$, where A is as in Lemma 4. Set $x = X_n$, $y = Y_n$, $u = X_{nk}$, $v = Y_{nk}$, $w = k$. By Lemma 2, (1) and (2) are satisfied. By Lemma 3, we can choose z such that (3) holds. Obviously (4) is satisfied. Finally, $y^2 - k^2 > 0$ and by Lagrange's theorem, (5) can also be satisfied. So we have proved the main lemma for real quadratic rings.

3. The main lemma for imaginary quadratic rings. In the following lemma we need some properties of totally imaginary biquadratic fields: $\mathbf{Q}(\sqrt{F}, \sqrt{D})$, where $D \leq -1$, $F > 1$, and D, F are square-free. The only possible[3] roots of unity in such fields are: ± 1, $\pm i$, $(\pm 1 \pm i\sqrt{3})/2$, $(\pm\sqrt{2} \pm i\sqrt{2})/2$, $(\pm i \pm \sqrt{3})/2$. By σ_1, σ_2 we mean the automorphisms defined by:

$$\sigma_1(\sqrt{F}) = -\sqrt{F}, \qquad \sigma_1(\sqrt{D}) = \sqrt{D},$$

$$\sigma_2(\sqrt{F}) = \sqrt{F}, \qquad \sigma_2(\sqrt{D}) = -\sqrt{D}.$$

[3]See e.g. Borevich and Shafarevich [1, p. 326], and notice that the primitive 5- and 10-roots of unity are excluded because their Galois group is cyclic.

If $q \in Q$, then $\sigma_1(q) = q$, $\sigma_2(q) = q$. By the Dirichlet-Minkowski Theorem on units there exists a fundamental unit η such that every unit u in $\mathbf{Q}(\sqrt{F}, \sqrt{D})$ can be uniquely written in the form $u = \rho\eta^m$, where $m \in \mathbf{Z}$ and ρ is a root of unity in $\mathbf{Q}(\sqrt{F}, \sqrt{D})$. By the same theorem, there exists a fundamental unit ϵ in $\mathbf{Q}(\sqrt{F})$ such that every unit e in $\mathbf{Q}(\sqrt{F})$ can be uniquely written in the form $e = \pm \epsilon^{m'}$, where $m' \in \mathbf{Z}$.

Now ϵ is also a unit in $\mathbf{Q}(\sqrt{F}, \sqrt{D})$, hence $\epsilon = \rho\eta^m$. So $\epsilon\sigma_2(\epsilon) = \rho\sigma_2(\rho)(\eta\sigma_2(\eta))^m$. Hence $\epsilon^2 = \rho' e^m$, where ρ' is a root of unity in $\mathbf{Q}(\sqrt{F})$, and e a unit in $\mathbf{Q}(\sqrt{F})$. Thus, $\epsilon^2 = (\pm 1)(\pm \epsilon^{m'})^m$, $|\epsilon|^2 = |\epsilon|^{m'm}$. Hence $|m| = 1$ or $|m| = 2$. From $\epsilon = \rho\eta^m$, we conclude:

$$\eta^2 = \rho_1 \epsilon^j, \qquad j = \pm 1 \text{ or } \pm 2, \qquad \rho_1 \text{ root of unity in } \mathbf{Q}(\sqrt{F}, \sqrt{D}).$$

Lemma 7. *Let* $\mathbf{A}(D)$ *be an imaginary quadratic ring, i.e.* $D \leq -1$. *Put* $A = 2$ *and* $F = A^2 - 1 = 3$, *if* $D \neq -1$ *and* $D \neq -3$; $A = 4$ *and* $F = A^2 - 1 = 15$, *if* $D = -1$ *or* $D = -3$. *If* $x^2 - Fy^2 = 1$ *and* $x, y \in \mathbf{A}(D)$, *then* $y^2 \in \mathbf{Z}$.

Proof. We have $(x - \sqrt{F}y)(x + \sqrt{F}y) = 1$, thus $x + \sqrt{F}y$ is a unit in $\mathbf{Q}(\sqrt{F}, \sqrt{D})$. Hence, $x + \sqrt{F}y = \rho\eta^m$, so $x - \sqrt{F}y = \rho^{-1}\eta^{-m}$. Subtracting and squaring yield $4Fy^2 + 2 = \rho^2(\eta^2)^m + \rho^{-2}(\eta^2)^{-m}$. But $\eta^2 = \rho_1 \epsilon^j$, hence

$$4Fy^2 + 2 = \rho^2\rho_1^m\epsilon^{jm} + (\rho^2\rho_1^m)^{-1}(\epsilon^{-1})^{jm}.$$

After some change of variables we have $4Fy^2 + 2 = \rho\epsilon^m + \rho^{-1}(\epsilon^{-1})^m$, where ρ is a root of unity in $\mathbf{Q}(\sqrt{F}, \sqrt{D})$. But for the defined values of F, $N(\epsilon) = +1$, thus $\epsilon^{-1} = \sigma_1(\epsilon)$. Hence $4Fy^2 + 2 = \rho\epsilon^m + \rho^{-1}\sigma_1(\epsilon^m)$.

Let us compute the imaginary part of both sides of this equation. Since $\mathrm{Im}(\epsilon) = 0$, and $\mathrm{Im}(\rho^{-1}) = -\mathrm{Im}(\rho)$, we have

$$\mathrm{Im}(4Fy^2 + 2) = (\epsilon^m - \sigma_1(\epsilon^m))\,\mathrm{Im}(\rho).$$

Since $y \in \mathbf{A}(D)$, and $\epsilon \in \mathbf{Q}(\sqrt{F})$, we have

$$\mathrm{Im}(4Fy^2 + 2) = q_1\sqrt{|D|}, \qquad (\epsilon^m - \sigma_1(\epsilon^m)) = q_2\sqrt{F},$$

where $q_1, q_2 \in \mathbf{Q}$. But $\mathrm{Im}(\rho) = q_3\sqrt{S}$, where $q_3 \in \mathbf{Q}$, and $S = 0$, 1, or 3. $S = 2$ is excluded since $F = 3$ or 15. So,

$$\mathrm{Im}(4Fy^2 + 2) = q_1\sqrt{|D|} = q_2q_3\sqrt{F}\sqrt{S}.$$

By our choice of F, we can conclude: $\mathrm{Im}(4Fy^2 + 2) = 0$. Hence, $4Fy^2 + 2 \in \mathbf{Q}$, and thus $y^2 \in \mathbf{Z}$.

Lemma 8. *Let* $D \leq -1$, $t \in \mathbf{A}(D)$, *and* W, $R \in \mathbf{Z}$. *If* $R \equiv t \pmod{W}$ *and* $N(t) < W^2/4$, *then* $t \in \mathbf{Z}$.

Proof. We have $t = R + (U + i\sqrt{|D|}V)W/2$, with U, $V \in \mathbf{Z}$. So, $N(t) = (R + UW/2)^2 + |D|V^2W^2/4$. If $V \neq 0$, then $N(t) \geq W^2/4$. From this contradiction we conclude $V = 0$, thus $t \in \mathbf{Z}$.

Lemma 9. *Let* $\mathbf{A}(D)$ *be an imaginary quadratic ring, i.e.,* $D \leq -1$. *Let* F *be as defined in the hypothesis of Lemma* 7, *and let* Σ *be the following system of diophantine equations* (1)–(5), *in the unknowns* t, x, y, u, v, z, w, h, r, s.

(1) $x^2 - Fy^2 = 1$,

(2) $u^2 - Fv^2 = 1$,

(3) $v^2 - y^2t = zy^4$,

(4) $ry + s(5h + 2) = 1$,

(5) $y = 2tw$.

Then conditions (1) *and* (2) *of the main lemma are satisfied.*

Proof. (1) Suppose that t, x, $\cdots$, s are in $\mathbf{A}(D)$, and satisfy (1)–(5). From (1), (2) and Lemma 7 follows $y^2 \in \mathbf{Z}$, $v^2 \in \mathbf{Z}$. From (3), we have:

$$(v^2/y^2) \equiv t \pmod{y^2}. \tag{6}$$

Suppose for a moment that $y = 0$; then (4) yields $s(5h + 2) = 1$. Thus in this supposition, $5h + 2$ should be a unit. But the only possible units in an imaginary quadratic ring are: ± 1, $\pm i$, $(\pm 1 \pm i\sqrt{3})/2$. Since $h \in \mathbf{A}(D)$, we have a contradiction, and we conclude $y \neq 0$. From (5) we have $N(y^2) = 16(N(t))^2(N(w))^2$. But $y \neq 0$, thus $N(y^2) \geq 16N(t)$. So,

$$N(t) < (y^2)^2/4. \tag{7}$$

Now, (v^2/y^2), $y^2 \in \mathbf{Z}$; thus by (6), (7) and Lemma 8, we conclude $t \in \mathbf{Z}$.

(2) Suppose $t = k^2$, $k \in \mathbf{N}$, and $k \neq 0$. By Lemma 1, there exist natural numbers X and Y, with $Y \neq 0$, satisfying $X^2 - F(2t)^2Y^2 = 1$. But $F = A^2 - 1$; thus, by Lemma 2, we have $X = X_n(A)$, $2tY = Y_n(A)$. Set $x = X_n$, $y = Y_n$, $u = X_{nk}$, $v = Y_{nk}$, $w = Y$. Obviously (5) is satisfied, and $y \neq 0$. By Lemma 2, (1) and (2) hold. By Lemma 3, (3) can be satisfied. Since $y \neq 0$, we can choose a natural number h, such that y and $5h + 2$ have no common divisors in $\mathbf{N}$. Hence, there exist rational integers r and s satisfying (4). So we have proved the main lemma for imaginary quadratic rings too.

REFERENCES

1. Z. I. Borevič and I. R. Šafarevič, *Number theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR 30 #1080; 33 #4001.

2. Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly, 80 (1973), 233–269.

3. Raphael M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. 70 (1951), 137–159. MR 12, 791.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LEUVEN, HEVERLEE, BELGIUM