TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 241, July 1978

UNDECIDABLE EXISTENTIAL PROBLEMS FOR ADDITION AND DIVISIBILITY IN ALGEBRAIC NUMBER RINGS

BY

L. LIPSHITZ[1]

ABSTRACT. Existential formulas involving addition and divisibility are shown to be undecidable in the ring of integers of a real quadratic extension of the rationals. A weaker result is proved for extensions of higher degree.

In [5] it was shown that there is an algorithm for deciding formulas of the form

$$\exists x_1 \cdots \exists x_{n_{\in \mathbf{N}}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x}), \tag{1}$$

where $\bar{x} = (x_1, \ldots, x_n)$, $a|b$ means "a divides b" and the f_i and g_i are linear polynomials with coefficients from the integers $\mathbf{Z}$ or from the ring R of integers of an imaginary quadratic extension of the rationals.

In this paper we shall show that the corresponding problem, where R is the ring of integers of any other algebraic number field (in particular, a real quadratic extension of the rationals) is undecidable. We shall also show that when R is the ring of integers of a real quadratic extension of the rationals, then the (apparently) weaker problem of deciding formulas of the form

$$\exists x_1 \cdots \exists x_{n_{\in R}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x}) \tag{2}$$

is also undecidable.

I would like to thank Julia Robinson for making some unpublished notes available to me, and the referee for helpful criticisms and suggestions.

1. The real quadratic case. In this section we shall show that formulas of the form (2) are undecidable in the real quadratic case. The undecidability of formulas of the form (1) then follows immediately.

Let $a \in \mathbf{N}$ be square free and > 1 and let $\alpha^2 = a$. R is the ring of integers in $\mathbf{Q}(\alpha)$.

Let $\omega = (1 + \alpha)/2$ if $a \equiv 1 \bmod 4$ and let $\omega = \alpha$ otherwise. Then $R = \mathbf{Z}[\omega]$ (see [2, p. 132]). Since $2R \subset \mathbf{Z}[\alpha]$ it is clear that the problem of deciding formulas of the form

Received by the editors April 1, 1976 and, in revised form, October 1, 1976 and January 24, 1977.

AMS (MOS) subject classifications (1970). Primary 02E10, 10N10.

[1] This research supported in part by the Purdue Research Foundation.

$$\exists x_1 \cdots \exists x_{n_{\in \mathbf{Z}[\alpha]}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x}) \tag{2'}$$

with the f_i and g_i having coefficients from $\mathbf{Z}[\alpha]$ is equivalent to the problem of deciding formulas of the form (2).

By the results of Denef [4] that Hilbert's 10th problem is unsolvable for the ring R (or equivalently for the ring $\mathbf{Z}[\alpha]$), it is sufficient to give an existential definition of multiplication in $\mathbf{Z}[\alpha]$ in terms of addition, subtraction and divisibility using only the logical connectives $\bigwedge$ (and) and $\bigvee$ (or). Then putting the formula in disjunctive normal form we would have the undecidability of formulas of the form $\exists \bar{x}_{\in \mathbf{Z}[\alpha]} \bigvee_j \bigwedge_i f_{ij}(\bar{x}) | g_{ij}(\bar{x})$, which is equivalent to $\bigvee_j \exists \bar{x}_{\in \mathbf{Z}[\alpha]} \bigwedge_i f_{ij}(\bar{x}) | g_{ij}(\bar{x})$ and, hence, we would have the undecidability of formulas of the form $\exists \bar{x}_{\in \mathbf{Z}[\alpha]} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x})$. We shall also use equality ($=$) in giving this definition. Using equality we would get the undecidability of formulas of the form $\exists \bar{x}[(\bigwedge_i f_i(\bar{x}) | g_i(\bar{x})) \wedge (\bigwedge_j h_j(\bar{x}) = k_j(\bar{x}))]$. We could then use the linear equations $h_j(\bar{x}) = k_j(\bar{x})$ to eliminate some of the variables, leading to an equivalent formula $\exists \bar{y} \bigwedge_i f_i(\bar{y}) | g_i(\bar{y})$. We shall follow the usual convention (cf. Hardy and Wright, *An introduction to the theory of numbers*, Oxford, 1938, p. 1) that $a|b \leftrightarrow a \neq 0 \wedge \exists c(ac = b)$. From this it follows that $x \neq 0 \leftrightarrow \exists y(x|y)$ and, hence, that inequality is existentially definable by formulas of the type we are considering. In the sequel we shall use the inequality symbol with the understanding that it can be eliminated in this way. Alternatively, if we wanted to allow $0|0$ we could define $y \neq 0$ as follows (cf. [4]). Choose prime $p \neq 2$ such that $4 \not\equiv \pm 1 \bmod p$. Then

$$y \neq 0 \leftrightarrow \exists r, s, h\left[(ry + s(ph + 2)) = 1\right]$$
$$\leftrightarrow \exists A, B, h(y|A \wedge ph + 2|B \wedge A + B = 1).$$

Here we use the fact that $N(ph + 2) \equiv 4 \pmod p$ and, hence, that $ph + 2 \nmid 1$ and so $y \neq 0$.

It is well known how to define multiplication existentially from addition and squaring, viz. $b \cdot c = d \leftrightarrow (b + c)^2 = b^2 + c^2 + 2d$. Consequently, it is sufficient to define the squaring function existentially from $+$, $-$, $|$, $=$, $\neq$, 0, 1 using only the logical connectives $\bigwedge$, $\bigvee$ in the ring $\mathbf{Z}[\alpha]$.

Let a and α be as above. N: $\mathbf{Z}[\alpha] \to \mathbf{Z}$ will denote the norm. In this paragraph x, y, x_i, y_i will denote elements of $\mathbf{Z}$. In the rest of this section they will denote elements of $\mathbf{Z}[\alpha]$ unless it is specified otherwise. We shall use some elementary facts about the Pell equation $x^2 - ay^2 = \pm 1$ (i.e. $x + \alpha y | 1$). $\varepsilon = x_1 + \alpha y_1$ will denote the fundamental unit in $\mathbf{Z}[\alpha]$ with $\varepsilon > 1$ (cf. [2]). Then the general solution is given by $x + \alpha y = \pm \varepsilon^i$ $(i \in \mathbf{Z})$. We shall use the notation $x_i + \alpha y_i = \varepsilon^i$ $(i \in \mathbf{Z})$. There are two cases to consider, viz. $N(\varepsilon) = 1$ and $N(\varepsilon) = -1$. All the lemmas and theorems are true in both cases. We shall, however, only give the proofs in the case $N(\varepsilon) = 1$. The proofs of Lemmas 1 and 2 require some small modifications in the case

$N(\varepsilon) = -1$, which we shall leave to the reader. The other proofs work in both cases. From now on assume $N(\varepsilon) = 1$. If $\varepsilon^i = x + \alpha y$ then $\varepsilon^{-i} = x - \alpha y$, $x = (\varepsilon^i + \varepsilon^{-i})/2 \in \mathbf{Z}$ and $y = (\varepsilon^i - \varepsilon^{-i})/2\alpha \in \mathbf{Z}$. Thus $x_i = |x| \sim \frac{1}{2}\varepsilon^{|i|}$ with error $< \frac{1}{2}$ and $y_i = |y| \sim \varepsilon^{|i|}/2\alpha$ with error $< \frac{1}{2}$. Hence $x_i \to \infty$ and $x_{i+1} - x_i \to \infty$ as $i \to \infty$, and similarly for the y_i.

Define

$$PI(x, y) \leftrightarrow x + \alpha y | 1 \wedge x - \alpha y | 1 \wedge x + 1 + \alpha y | x + 1 - \alpha y$$
$$\wedge x + 1 - \alpha y | x + 1 + \alpha y \wedge y \neq 0.$$

(Recall $y \neq 0 \leftrightarrow \exists z (y | z)$.)

Lemma 1. *There is a positive integer k $(= k(a))$ such that if $k | y$ then*

$$PI(x, y) \leftrightarrow x, y \in \mathbf{Z} \wedge x^2 - ay^2 = 1 \wedge y \neq 0.$$

Proof. Suppose that $PI(x, y)$. Since $y \neq 0$ and $\alpha \nmid 1$, we see that $x \neq 0$ and so $x + \alpha y = \pm \varepsilon^i$, $x - \alpha y = \pm \varepsilon^j$ for some $i \neq j$ (both $\in \mathbf{Z}$). We shall use σ_i to denote fixed but unknown signs, i.e., $\sigma_i = \pm 1$. Then we have $x + \alpha y = \sigma_1 \varepsilon^i$, $x - \alpha y = \sigma_2 \varepsilon^j$. From $x + 1 \pm \alpha y | x + 1 \mp \alpha y$ we have $N(x + 1 + \alpha y) = \pm N(x + 1 - \alpha y) = \sigma_3 N(x + 1 - \alpha y)$, say. Hence $N(1 + \sigma_1 \varepsilon^i) = \sigma_3 N(1 + \sigma_2 \varepsilon^j)$. But

$$N(1 + \sigma_1 \varepsilon^i) = (1 + \sigma_1 \varepsilon^i)(1 + \sigma_1 \varepsilon^{-i}) = 2 + \sigma_1(\varepsilon^i + \varepsilon^{-i}) = 2 + 2\sigma_1 x_i.$$

Similarly $N(1 + \sigma_2 \varepsilon^j) = 2 + 2\sigma_2 x_j$. (Recall that we are only considering the case $N(\varepsilon) = 1$.) So we have $2 + 2\sigma_1 x_i = \sigma_3(2 + 2\sigma_2 x_j)$. Since x_i and $x_{i+1} - x_i \to \infty$ as $i \to \infty$, this implies that for $|i|$ large enough (i.e. excluding a finite number of cases) we have $j = -i$ and $\sigma_1 = \sigma_2$. Then $x = \sigma_1 x_i$ and $y = \sigma_1 y_i$ are both in $\mathbf{Z}$. We need only choose $k > |y_i|$ for all the values of i that we want excluded so that $k | y$ excludes all these exceptional cases. Conversely, if x, y $(\in \mathbf{Z})$ is a solution of the Pell equation, then $x + \alpha y = \sigma_1 \varepsilon^i$ and $x - \alpha y = \sigma_1 \varepsilon^{-i}$. Since $(1 + \sigma_1 \varepsilon^i)\sigma_1 \varepsilon^{-i} = 1 + \sigma_1 \varepsilon^{-i}$, it is clear that $PI(x, y)$.

Remark. It follows directly from Lemma 1 that if $PI(u, v)$ and $ka | u - 1$ then $u, v \in \mathbf{Z}$.

Define

$$S(y, u) \leftrightarrow \exists x \exists v \big[PI(x, y) \wedge PI(u, v) \wedge k | y$$
$$\wedge x | (u + 1)/2 \wedge x \pm 1 | (u - 1)/2 \wedge x \pm 2 | (u + 1)/2 - 4$$
$$\wedge y | (u - 1)/2a \wedge y \pm 1 | (u - 1)/2a - 1$$
$$\wedge x + \alpha y + u + \alpha v | 2 + 2x \big].$$

Lemma 2. *There is an $l = l(a) \in \mathbf{N}$ such that if $l | y$ then*

$$S(y, u) \leftrightarrow \exists x \exists v \big(x, y \in \mathbf{Z} \wedge x^2 - ay^2 = 1 \wedge y \neq 0 \wedge u, v \in \mathbf{Z}$$
$$\wedge u^2 - av^2 = 1 \wedge v \neq 0 \wedge y^2 = (u - 1)/2a \big).$$

PROOF. Suppose that $S(y, u)$. From $PI(x, y)$ we see that $y \neq 0$. Then from $k|y$ and Lemma 1 we have that $x, y \in \mathbf{Z}$ and $x + \alpha y = \sigma_1 \varepsilon^i$ $(i \neq 0)$.

From $PI(u, v)$ we have $v \neq 0$. Then from $k|y$, $y|(u - 1)/2a$ and the remark following Lemma 1, we have $u + \alpha v = \sigma_2 \varepsilon^j$ $(j \neq 0)$ and $u \in \mathbf{Z}$. From $x + \alpha y + u + \alpha v | 2 + 2x$ we have $N(\varepsilon^j + \sigma_3 \varepsilon^i) | (2 + 2x)^2$, where $\sigma_3 = \sigma_1 \sigma_2$, so $N(1 + \sigma_3 \varepsilon^{j-i}) | (2 + 2x)^2$, i.e., $2 + \sigma_3(\varepsilon^{j-i} + \varepsilon^{i-j}) | (2 + \sigma_1(\varepsilon^i + \varepsilon^{-i}))^2$. From this it follows that for i large enough (i.e. except for finitely many cases) $|j| < 3|i|$ (because $\varepsilon > 1$). From

$$x|(u + 1)/2 \wedge x \pm 1|(u - 1)/2 \wedge x \pm 2|(u + 1)/2 - 4$$

we have

$$(u + 1)/2 = x^2 + (m/24)x(x^2 - 1)(x^2 - 4) \quad \text{for some } m \in \mathbf{Z}.$$

So again excluding finitely many cases we have either that $(u + 1)/2 = x^2$ (i.e. $m = 0$) or $|(u + 1)/2| > K\varepsilon^{5i}$ for some fixed $K > 0$ (e.g. $K = 3^{-2}2^{-8}$). But from $|j| < 3|i|$ we have $|(u + 1)/2| < (\varepsilon^{3|i|} + 1)/2$. Hence, excluding finitely many cases (i.e. for $|i|$ large enough) we have $(u + 1)/2 = x^2$. It follows by direct computation that $|j| = 2|i|$ and hence that $y^2 = (u - 1)/2a$. We need only choose l large enough so that $l|y$, $y \neq 0$, excludes all the exceptional cases.

Conversely, if $x, y, u, v \in \mathbf{Z}$ satisfy $x^2 - ay^2 = 1, y \neq 0$ and $u^2 - av^2 = 1$, $v \neq 0$, and $y^2 = (u - 1)/2a$, it follows by direct computation that $x + \alpha y = \pm\, \varepsilon^{\pm i}$ $(i \in \mathbf{N})$, and that $u + \alpha v = \varepsilon^{\pm 2i}$, and that $S(y, u)$ is satisfied.

Now define

$$\mathrm{Sq}_1(y, z) \leftrightarrow \exists u [S(y, u) \wedge l|y \wedge z = (u - 1)/2a].$$

LEMMA 3. (i) $\mathrm{Sq}_1(y, z) \rightarrow y, z \in \mathbf{Z}, z = y^2$ *and* $y \neq 0$; (ii) *for any* $n \in \mathbf{N}$ *there exist* $y, z \in \mathbf{Z}$ *such that* $\mathrm{Sq}_1(y, z) \wedge n|y \wedge y \neq 0$.

PROOF. (i) is immediate from Lemma 2. For (ii) notice that if $x + \alpha y = \varepsilon^i$ and $u + \alpha v = \varepsilon^{2i}$ $(x, y, u, v \in \mathbf{Z})$, then by direct calculation one sees that $x^2 = (u + 1)/2$ and $y^2 = (u - 1)/2a$ and, hence, that, except for $k|y$, $l|y$, all of $\mathrm{Sq}_1(y, z)$ is satisfied. The existence of solutions x, y of the Pell equation with y divisible by l or n follows from a theorem of Lucas that for any $n \in \mathbf{N}$ there is a solution of $x^2 - ay^2 = +1$ with $n|y, y \neq 0$ (see [3, Theorem XIII]). The lemma now follows immediately.

Lemma 3 allows us to find pairs y, y^2 with $y \in \mathbf{Z}$ as large as we please. Next we shall use this to define squaring in $\mathbf{Z}[\alpha]$. The idea is that if x, $z \in \mathbf{Z}[\alpha]$, say $x = x_1 + \alpha x_2$, $y = y_1 + \alpha y_2$ with the $x_i, y_i \in \mathbf{Z}$ and $c \in \mathbf{Z}$ is very much larger than the $|x_i|$ and $|y_i|$ (denoted by $c \gg x, z$), and if $x|z$, $x \pm 1|z - 1$ and $x \pm c|z - c^2$, then $z = x^2$. The previous lemma allows us to pick out the pairs c, c^2.

Define

$$\begin{aligned}\mathrm{Sq}(x,z) \leftrightarrow \exists c_1, c_1', c_2, c_2', c_3, c_3', c_4, c, d\\ &\big[x|c_1 \wedge x \pm 1|c_1 \wedge z|c_1 \wedge z \pm 1|c_1 \wedge 2ac_1|c_1'\\ &\wedge \mathrm{Sq}_1(c_1', c_2) \wedge c_2|c_2' \wedge \mathrm{Sq}_1(c_2', c_3) \wedge c_3|c_3'\\ &\quad\wedge \mathrm{Sq}_1(c_3', c_4) \wedge c_4|c \wedge \mathrm{Sq}_1(c, d) \wedge c \pm x|d - z\big]\\ &\vee[x = 0 \wedge z = 0].\end{aligned}$$

LEMMA 4. $\mathrm{Sq}(x, z) \leftrightarrow x^2 = z$ *for all* $x, z \in \mathbf{Z}[\alpha]$.

PROOF. If $x^2 = z$ it is easy to use Lemma 3 to obtain the required c_i, c_i', c, d. Conversely, suppose $\mathrm{Sq}(x,y)$ and $x \neq 0$. Then $d = c^2$ and $c \neq 0$ since $\mathrm{Sq}_1(c, d)$, and so from $c \pm x|d - z$ we have $(c^2 - x^2)/\text{g.c.d.}(c + x, c - x)|c^2 - z$. Hence, since $\text{g.c.d.}(c + x, c - x)|2x$, we have $\gamma(c^2 - x^2) = 2x(c^2 - z)$ for some $\gamma \in \mathbf{Z}[\alpha]$. Next we shall use the fact that $c \gg x, z$ to show that $\gamma = 2x$ and, hence, that $z = x^2$. Let $x = x_1 + \alpha x_2$, $z = z_1 + \alpha z_2$, $x^2 = x_3 + \alpha x_4$ with the $x_i, z_i \in \mathbf{Z}$, and let

$$m = \max(|x_1|, |x_3|, |z_1|, a|x_2|, a|x_4|, a|z_2|) \geqslant 1.$$

From the divisibilities $x|c_1$, $x \pm 1|c_1$, $z|c_1$ and $z \pm 1|c_1$, it follows by taking the norms and simple manipulations that $m \leqslant 4aN(c_1)^2$. From the other conditions we see that $c_1', c_2, c_2', c_3, c_3', c_4, c, d \in \mathbf{Z}$ and that

$$|c| \geqslant |c_4| = c_3'^2 \geqslant c_3^2 = c_2'^4 \geqslant c_2^4 = c_1'^8 \geqslant (2a)^8|N(c_1)|^4.$$

Hence, $16m^2 \leqslant |c|$ and thus $(2m + 1)^2 < |c|$, since $m \geqslant 1$. Let $\gamma = y_1 + \alpha y_2$ $(y_1, y_2 \in \mathbf{Z})$. Then we have

$$(y_1 + \alpha y_2)(c^2 - x_3 - \alpha x_4) = 2(x_1 + \alpha x_2)(c^2 - z_1 - \alpha z_2).$$

So

$$y_1(c^2 - x_3) - ay_2x_4 = 2x_1(c^2 - z_1) - 2ax_2z_2$$

and

$$y_2(c^2 - x_3) - y_1x_4 = 2x_2(c^2 - z_1) - 2x_1z_2.$$

(All the letters stand for integers.) Divide both equations by $c^2 - x_3$ to get

$$y_1 - A_1y_2 = 2x_1B_1 + D_1, \quad y_2 - A_2y_1 = 2x_2B_2 + D_2$$

with $|A_i|, |D_i| < (2m + 1)^{-3}$ for $i = 1, 2$ and

$$1 - (2m + 1)^{-3} < B_i < 1 + (2m + 1)^{-3} \quad \text{and} \quad |x_i| \leqslant m.$$

Eliminating y_2 and dividing through by $1 - A_1A_2$ we get that

$$y_1 = (2x_1B_1 + 2x_2B_2A_1 + D_1 + A_1D_2)/(1 - A_1A_2).$$

The right-hand side $\sim 2x_1$ with error $< 1/2m$. So since x_1 and $y_1 \in \mathbf{Z}$ we must have $y_1 = 2x_1$. Similarly $y_2 = 2x_2$. Hence $z = x^2$. We now have

THEOREM 1. *If $a \in \mathbf{N}$ is square free, $a > 1$, $\alpha^2 = a$ and R is the ring of integers in $\mathbf{Q}(\alpha)$, then multiplication is existentially definable from $+$, $-$, $|$, 0, 1, α (using only $\wedge$, $\vee$), and, hence, formulas of the form*

$$\exists x_1 \cdots \exists x_{n_{\in R}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x}), \tag{2}$$

with the f_i and g_i linear polynomials with coefficients from R, are undecidable.

COROLLARY. *With f_i, g_i, R as above formulas of the form*

$$\exists x_1 \cdots \exists x_{n_{\in \mathrm{N}}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x}) \tag{1}$$

are undecidable.

We can strengthen Theorem 1 to obtain

THEOREM 2. *There is no algorithm for deciding formulas of the form* (2) *where the f_i and g_i have coefficients from* $\mathbf{Z}$.

PROOF. We cannot define $y = \alpha x$ from 0, 1, $+$, $|$ since there is an automorphism of $\mathbf{Q}(\alpha)$ interchanging α and $-\alpha$. To establish the theorem, however, it is sufficient to show how to define $z = \pm\,\alpha$ and $y = zx$ by existential formula of the language $+$, $-$, $|$, 0, 1, $=$ using only the connectives $\wedge$, $\vee$. Let ε be a unit with $\varepsilon = c + \alpha d$, $|c| > 1$ $(c, d \in \mathbf{Z})$. Then $z = \pm\,\alpha \leftrightarrow c \pm dz | 1$. This is clear. Let $A(x,y) \leftrightarrow [x|y \wedge cx \pm dy|x] \vee [x = 0 \wedge y = 0]$. Then $A(x,y) \leftrightarrow y = \pm\,\alpha x$. If $x \neq 0$ then from $x|y$ we have $y = ux$ for some u. Let $u = A + \alpha B$ $(A, B \in \mathbf{Z})$. From $cx \pm dy|x$ we have immediately that $c + dA + \alpha dB | 1$ and $c - dA - \alpha dB | 1$. Hence $c + dA + \alpha dB = \sigma_1 \varepsilon^{i_1}$ and $c - dA - \alpha dB = \sigma_2 \varepsilon^{i_2}$. Since $c \neq 0$ the only possibility is $A = 0$ and, hence, $B = \pm 1$ and $u = \pm\,\alpha$. Let $z = \pm\,\alpha$ be fixed. We shall show finally that $y = zx \leftrightarrow A(x,y) \wedge A(x + 1, y + z)$. One direction is trivial. For the converse assume $A(x,y) \wedge A(x + 1, y + z)$. Then, by the above, $y = \sigma_1 zx$, $y + z = \sigma_2 z(x + 1)$ (for some $\sigma_i = \pm 1$). Hence $\sigma_1 zx + z = \sigma_2 z(x + 1)$. So $\sigma_1 x + 1 = \sigma_2(x + 1)$, i.e. $(\sigma_1 - \sigma_2)x = \sigma_2 - 1$. We need only consider the case $x \neq 0$. In this case if $\sigma_2 = 1$ then $\sigma_1 = \sigma_2 = 1$ and $y = zx$. If $\sigma_2 = -1$ then $(\sigma_1 + 1)x = -2$, and we must have $\sigma_1 = 1$ (for otherwise we get $0 = -2$) and, hence, $y = zx$.

2. Arbitrary algebraic extensions. In this section we shall prove

THEOREM 3. *If R is the ring of integers in any proper algebraic extension of the rationals, other than imaginary quadratic, then formulas of the form $\exists x_1 \cdots \exists x_{n_{\in \mathrm{N}}} \bigwedge_i f_i(\bar{x}) | g_i(\bar{x})$, where the f_i and g_i are linear polynomials with coefficients from R, are undecidable.*

PROOF. Let the degree of the extension be n and let $\alpha_1, \ldots, \alpha_n$ be an integral basis for R. If $x \in R$, say $x = \Sigma_i x_i \alpha_i$, then let $\|x\| = \max_i |x_i|$. Let the distinct embeddings of $R \to \mathbf{C}$ (the complex numbers) be $\sigma_1, \ldots, \sigma_n$ and let $K(x) = \max_i |\sigma_i(x)|$. It follows from [2, Lemma 1, p. 119] that there exist $B, C > 0$ such that for all $x \in R$,

$$CK(x) \leqslant \|x\| \leqslant BK(x).$$

From the Dirichlet Theorem on Units (cf. [2, Theorem 5, p. 112]) it follows that R has at least one fundamental unit. (The only proper algebraic extensions which do not are the imaginary quadratic ones, which we have excluded.) Hence there are infinitely many solutions to $x|1$.

We shall use the following

THEOREM 4. *Let* $k \geqslant 2$, $L \in \mathbf{N}$ *and let* $\phi(x, y)$ *satisfy*

(i) $\forall m \exists x, y (\phi(x, y) \wedge y > mx)$,

(ii) $\forall x, y (\phi(x, y) \to y < Lx^k)$.

(*The variables range over* $\mathbf{N}$.) *Then multiplication can be existentially defined in terms of* $+$, $|$, 0, 1 *and* ϕ.

This theorem has recently been published by A. Bel'tyukov [1].

Define

$$\phi(x, y) \leftrightarrow \exists x_1, \ldots, x_n, y_1, \ldots, y_{n \in \mathbf{Z}}$$

$$\left(\underline{x} = \sum x_i \alpha_i | 1 \wedge \underline{y} = \sum y_i \alpha_i | 1 \wedge x = \max_i |x_i| \wedge y = \max_i |y_i| \right.$$

$$\left. \wedge \exists z_{\in \mathbf{N}} \left(\bigwedge_{k=1}^{n+1} (\underline{y} + k\underline{x} | z \wedge z \leqslant x) \right) \right).$$

We shall show that ϕ has the above properties (i) and (ii) (with $k = n + 1$).

(i) Let ε be a fundamental unit of R and let m be given. We shall show that we can choose l and p so that if $\underline{x} = \Sigma x_i \alpha_i = \varepsilon^l$ and $\underline{y} = \Sigma y_i \alpha_i = \varepsilon^{l+p}$, then $y > mx$, where $x = \|\underline{x}\|$ and $y = \|\underline{y}\|$. Now $\underline{y} + k\underline{x} = \varepsilon^l(\varepsilon^p + k)$, so $N(\underline{y} + k\underline{x}) = \pm N(\varepsilon^p + k)$, where $N(w)$ is the norm of w, $N(w) = \Pi_i \sigma_i(w)$. $M = \max|\sigma_i(\varepsilon)| > 1$, since $\Pi_i \sigma_i(\varepsilon) = 1$, and if $|\sigma_i(w)| = 1$ for all i, then w is a root of unity. Then

$$|N(\varepsilon^p + k)| \leqslant (M^p + k)^n \leqslant (M^p + n + 1)^n \quad \text{for } k \leqslant n + 1.$$

Hence $\phi(x, y)$ will be satisfied with $z = |\Pi_{k=1}^{n+1} N(\varepsilon^p + k)|$ if

$$(M^p + n + 1)^{n(n+1)} \leqslant x.$$

Since $M^p + n + 1 \leqslant (M + n + 1)^p$ and $x \geqslant CK(\underline{x})$, it is sufficient that

$$(M + n + 1)^{n(n+1)p} \leqslant CK(\underline{x}).$$

But $K(\underline{x}) = \max|\sigma_i(\varepsilon^l)| = (\max|\sigma_i(\varepsilon)|)^l = M^l$, so it is sufficient that

$$(M+n+1)^{n(n+1)p} \leqslant CM^l,$$

i.e., $n(n+1)p \log_M(M+n+1) \leqslant \log_M(C) + l$. So if

$$p \leqslant (l + \log_M(C))/n(n+1)\log_M(M+n+1), \tag{3}$$

then $\phi(x, y)$ is satisfied. We also want $y > mx$. Now $y \geqslant CK(\underline{y}) = CM^{l+p}$ and $x \leqslant BK(\underline{x}) = BM^l$, so we also want $CM^{l+p} > BM^l m$, i.e.

$$CM^p > Bm \quad \text{or} \quad p > \log_M(Bm/C). \tag{4}$$

It is clear that we can choose p so that (4) is satisfied and then choose l so that (3) is satisfied.

(ii) We shall show that there is an $L \in \mathbf{N}$ so that $\phi(x, y) \to y < Lx^{n+1}$. Suppose that $\phi(x, y)$. Then $\underline{y} = \delta\underline{x}$ where δ is a unit of R, and $\underline{y} + k\underline{x} = \underline{x}(\delta + k)$, and since $\phi(x, y)$ is true we have $|N(\underline{y} + k\underline{x})| = |N(\delta + k)| \leqslant x^n$ for $k = 1, \ldots, n+1$. By the pigeonhole principle for some k $(1 \leqslant k \leqslant n+1)$, we have $|\sigma_i(\delta) + k| \geqslant \frac{1}{2}$ for $i = 1, \ldots, n$. For this k we have

$$|N(\delta + k)| \geqslant \frac{1}{2^{n-1}} \max_i |\sigma_i(\delta + k)| \geqslant \frac{1}{2^{n-1}} \left[\max|\sigma_i(\delta)| - k\right].$$

Hence

$$|N(\delta + k)| + \frac{k}{2^{n-1}} \geqslant \frac{1}{2^{n-1}} \max_i |\sigma_i(\delta)|$$

and so

$$|N(\delta + k)| \geqslant \frac{1}{2^{n+1}} \max_i |\sigma_i(\delta)| = \frac{1}{2^{n+1}} K(\delta),$$

since $k/2^{n-1} < 2$ and $|N(\delta + k)| \geqslant 1$. Hence

$$K(\delta) \leqslant 2^{n+1} \max_k |N(\delta + k)| \leqslant 2^{n+1} x^n;$$

and

$$y = \|\underline{y}\| \leqslant BK(\underline{y}) \leqslant BK(\delta)K(\underline{x}) \leqslant B2^{n+1}x^n \frac{x}{C} = \frac{B}{C} 2^{n+1} x^{n+1}.$$

Thus we can take $L \geqslant (B/C)2^{n+1} + 1$ and (ii) is satisfied. This completes the proof of Theorem 3.

References

1. A. P. Bel'tyukov, Abstracts: Students' Scientific Conference, Leningrad University, 1975.

2. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966. MR 33 #4001.

3. R. D. Carmichael, *On the numerical factors of the arithmetical forms $\alpha^n + \beta^n$*, Ann. of Math. (2) 15 (1913), 30–70.

4. J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. 48 (1975), 214–220.

5. L. Lipshitz, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. (to appear).

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540