UNDECIDABLE EXISTENTIAL PROBLEMS FOR ADDITION AND DIVISIBILITY IN ALGEBRAIC NUMBER RINGS. II

LEONARD LIPSHITZ¹

ABSTRACT. It is shown that for all algebraic number rings, except imaginary quadratic ones, the problem of deciding existential formulas involving only addition and the divisibility predicate is equivalent to the full diophantine problem for these rings.

In this paper we shall prove the following

THEOREM. *Let R be the ring of integers of any algebraic number ring other than imaginary quadratic. Then the problem of deciding formulas of the form*

$$\exists x_1 \cdots \exists x_n \in R \bigwedge_i f_i(x_1 \cdots x_n) | g_i(x_1 \cdots x_n),$$

where the f_i and g_i are linear polynomials with coefficients from $\mathbf{Z}$ and $a|b$ means “ a divides b ”, is equivalent to the full Diophantine Problem for R .

This is in contrast to the result of [3] where it was shown that the corresponding problems for $\mathbf{Z}$ and imaginary quadratic number rings are decidable. This theorem generalizes the result of [4] where the same theorem was proved in the special case that R is the ring of integers of a real quadratic extension of the rationals and a somewhat weaker result was proved for arbitrary extensions (not imaginary quadratic).

The theorem will be proved by giving an existential definition of multiplication from $+$, $-$, $|$, 1 using only the connectives $\wedge$, $\vee$. Since it is well known how to define multiplication from the squaring function and addition (viz. $ab = c \leftrightarrow (a + b)^2 = a^2 + b^2 + 2c$), it is sufficient to define squaring existentially from $+$, $|$. We shall show that we can define squaring for “large” units (see the definition of “large” below) in Lemma 3. Then we shall use this to define squaring in general in R . The idea is that if $\epsilon \gg a, b$ and $a \pm k\epsilon | b - k^2\epsilon^2$ for several values of $k \in \mathbf{N}$ then $b = a^2$. (That is Lemma 4.)

From now on let R be the ring of integers of an algebraic number ring of degree n which is not an imaginary quadratic extension of the rationals. Then from the Dirichlet Unit Theorem R has a fundamental unit ϵ_0 which is not a root of unity. Let R have integral basis $\alpha_1, \dots, \alpha_n$ and let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of R in $\mathbf{C}$. If $x = \sum x_i \alpha_i$ ($x_i \in \mathbf{Z}$) let $\|x\| = \max |\sigma_i(x)|$

Received by the editors August 9, 1976.

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

¹Supported in part by NSF grant MCS 76-06357.

© American Mathematical Society 1977

and let $|x| = \max |x_i| \in \mathbf{N}$. Then $|x|$ and $\|x\|$ are related as follows.

LEMMA 1. *There exist $B, C > 0$ ($B \geq 1, C \leq 1$) such that $C\|x\| \leq |x| \leq B\|x\|$.*

PROOF. The existence of C is clear since

$$|\sigma_i(x)| = \sum_j |x_j \sigma_i(\alpha_j)| \leq |x| \sum_j |\sigma_i(\alpha_j)|.$$

The existence of B is shown on p. 119 of [1].

We shall want to be able to say that $\varepsilon \gg a$ for unit ε (in either meaning of size). We must show that we can achieve this by writing down some divisibilities. Let ε be any unit of R (e.g. $\varepsilon = \varepsilon_0$) which is not a root of unity. Let $D_m = (\varepsilon^m - 1)/(\varepsilon - 1) \in R$.

LEMMA 2 (cf. [2]). (1) *If $m|n$ then $D_m | D_n$.*

(2) *If $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{p} \nmid \varepsilon - 1$ and $N(\mathfrak{p}) = p^k \in \mathbf{N}$ (N is the norm), then $\mathfrak{p} | D_{p^k-1}$.*

(3) *If $\mathfrak{p} | \varepsilon - 1$ then $\mathfrak{p} | D_p$ ($\mathfrak{p} | p \in \mathbf{N}$).*

(4) *If $\mathfrak{p}^\lambda | D_m, \lambda > 0$, then $\mathfrak{p}^{\lambda+1} | D_{mp}$.*

(5) *Given any $a \neq 0$ in R there exists $m \in \mathbf{N}$ such that $a | D_m$ and hence $a | \varepsilon^m - 1$. So there exists a unit $u \neq 1$ of R such that $a | u - 1$.*

PROOF. (1) is clear.

(2) Since ε is a unit, ε is prime to $\mathfrak{p}$. $(R/\mathfrak{p})^*$ is a group of order $N(\mathfrak{p}) - 1 = p^k - 1$ (cf. [5, Theorem IV 4D]). So $\varepsilon^{p^k-1} \equiv 1 \pmod{\mathfrak{p}}$ and $\mathfrak{p} | \varepsilon^{p^k-1} - 1$. Since $\mathfrak{p} \nmid \varepsilon - 1$, $\mathfrak{p} | D_{p^k-1}$.

(3) First suppose that $\mathfrak{p} | p \in \mathbf{N}$ (p an odd prime). Then $(\varepsilon - 1)^p = (\varepsilon^p - 1) - p\varepsilon(\varepsilon^{p-2} - 1) + \dots$. So $(\varepsilon - 1)^{p-1} = D_p + pI$ ($I \in R$ since $\varepsilon - 1 \equiv \varepsilon^I - 1$). Thus $D_p \equiv (\varepsilon - 1)^{p-1} \equiv 0 \pmod{\mathfrak{p}}$. Now suppose $\mathfrak{p} | 2$. $D_2 = (\varepsilon^2 - 1)/(\varepsilon - 1) = \varepsilon + 1 \equiv \varepsilon - 1 \equiv 0 \pmod{\mathfrak{p}}$.

(4) If $\mathfrak{p} | p$ (p odd) then

$$D_{mp} = (\varepsilon - 1)^{p-1} D_m^p + a_1(\varepsilon - 1)^{p-3} \varepsilon^m D_m^{p-2} + \dots + a_s \varepsilon^{sm} D_m$$

where $s = (p - 1)/2$. It is not hard to check that $a_s = p$ (see [2, p. 41]). So $D_{mp} \equiv p\varepsilon^{sm} D_m \pmod{\mathfrak{p}^{3\lambda}}$ and hence $D_{mp} \equiv 0 \pmod{\mathfrak{p}^{\lambda+1}}$.

If $\mathfrak{p} | 2$ then $D_{2m} = (\varepsilon^{2m} - 1)/(\varepsilon - 1) = (\varepsilon^m + 1)D_m$. Now $\varepsilon^m + 1 \equiv \varepsilon^m - 1 \equiv 0 \pmod{\mathfrak{p}}$ so $\mathfrak{p}^{\lambda+1} | D_{2m}$.

(5) Given any prime $\mathfrak{p}$ and integer k , using (2), (3) and (4) we see that there is an $m \in \mathbf{N}$ such that $\mathfrak{p}^k | D_m$. The required result now follows from this and part (1).

Let $N = 16(n + 1)^2$ and $K = \prod_{i < j \leq N} (j - i)^{2N}$ and let J be chosen so that

$$N^J \geq 6 \max \left(\left[C \frac{1}{K} \left(\frac{1}{2B} \right)^{(2N-2n)/n} \right]^{-1}, \left[\frac{C(4N/n) + n - 1}{(2B)^{2(N/n)-1}} \frac{1}{K} \right]^{-1} \right).$$

LEMMA 3. Let ϵ and δ be units and let N, K, J be as above. Suppose that $N^J|\epsilon - 1, N^J|\delta - 1$ and $N^J|\delta - \epsilon$. Then

$$\delta = \epsilon^2 \leftrightarrow \bigwedge_{k=1}^N (\epsilon \pm k|\delta - k^2 \text{ and } \delta \pm k\epsilon|\epsilon \pm k).$$

PROOF. One direction is trivial. For the other direction suppose that $N^J|\epsilon - 1, N^J|\delta - 1$ and $\bigwedge_{k=1}^N (\epsilon \pm k|\delta - k^2 \wedge \delta \pm k\epsilon|\epsilon \pm k)$. Notice that if $i \neq j$ and $y|\epsilon + i$ and $y|\epsilon + j$ then $y|i - j$, so if $\epsilon \pm k|x$ for $k = 1, \dots, N$ then $x = (\gamma/K)\prod_{k=-N}^N (\epsilon + k)$ where $\gamma \in R$ and K is as above. Hence from $\epsilon \pm k|\delta - k^2$ for $k = 1, \dots, N$ we have that $\delta = \epsilon^2 + (\gamma/K)\prod_{k=-N}^N (\epsilon + k)$. Suppose that $\delta \neq \epsilon^2$ so that $\gamma \neq 0$. Then

$$\delta - \epsilon^2 = \frac{\gamma}{K} \prod_{k=-N}^N (\epsilon + k)$$

and

$$|N(\delta - \epsilon^2)| = \left| \frac{N(\gamma)}{K^n} \prod_{k=-N}^N N(\epsilon + k) \right| \geq \frac{1}{K^n} \prod_{k=-N}^N |N(\epsilon + k)|$$

since $|N(\gamma)| \geq 1$. Now for fixed $i = 1, \dots, n$, $|\sigma_i(\epsilon + k)| < 1$ for at most two values of k . So except for at most $2n$ values of k , $|\sigma_i(\epsilon + k)| \geq 1$ for $i = 1, \dots, n$, and hence except for at most $2n$ values of k , $|N(\epsilon + k)| \geq \|\epsilon + k\| \geq B^{-1}|\epsilon + k|$. From $N^J|\epsilon - 1$ we have $N^{Jn}|N(\epsilon - 1)|$, so $|N(\epsilon - 1)| \geq N^{Jn}$ and, hence, $|\sigma_i(\epsilon - 1)| \geq N^J$ for some i and, hence, $\|\epsilon - 1\| \geq N^J$ and $|\epsilon - 1| \geq C^{-1}N^J$. Since $C^{-1}N^J > N^2$, $|\epsilon| \geq C^{-1}N^J - 1 \geq 2N$ and, hence, $|\epsilon \pm k| \geq |\epsilon| - k \geq \frac{1}{2}|\epsilon|$. For the exceptional values of k we certainly have $|N(\epsilon + k)| \geq 1$. Hence,

$$|N(\delta - \epsilon^2)| \geq K^{-n}(1/2B)^{2N-2n}|\epsilon|^{2N-2n}.$$

Hence,

$$\|\delta - \epsilon^2\|^n \geq K^{-n}(1/2B)^{2N-2n}|\epsilon|^{2N-2n},$$

$$\|\delta - \epsilon^2\| \geq K^{-1}(1/2B)^{2(N/n)-2}|\epsilon|^{2(N/n)-2}.$$

Now

$$|\delta| + |\epsilon^2| \geq C(\|\delta\| + \|\epsilon^2\|) \geq C\|\delta - \epsilon^2\|.$$

So

$$|\delta| \geq (C/K)(1/2B)^{2(N/n)-2}|\epsilon|^{2(N/n)-2} - |\epsilon^2|.$$

Above we had that

$$|\epsilon| \geq (2C)^{-1}N^J \geq 3[(C/K)(1/2B)^{2(N/n)-2}]^{-1}.$$

Also $|\epsilon^2| \leq (B/C^2)|\epsilon|^2$ and so

$$(*) \quad |\delta| \geq 3|\epsilon|^{2(N/n)-3} - |\epsilon^2| \geq |\epsilon|^{2(N/n)-3}.$$

Next we shall use the divisibilities $\delta \pm k\epsilon|\epsilon \pm k$ to derive an inequality in the opposite direction. As above, it follows from these divisibilities, supposing that $\delta \neq \epsilon^2$ that

$$\epsilon = \delta\epsilon^{-1} + \frac{\gamma'}{K} \prod_{k=-N}^N (\delta\epsilon^{-1} + k), \quad \gamma' \in R, \gamma' \neq 0$$

(since $\delta \pm k\epsilon|\epsilon \pm k \leftrightarrow \delta\epsilon^{-1} \pm k|\epsilon \pm k$). Thus

$$|N(\epsilon - \delta\epsilon^{-1})| \geq \frac{1}{K^n} \prod_{k=-N}^N |N(\delta\epsilon^{-1} + k)|.$$

From $N^J|\delta - \epsilon$ we have $N^J|\delta\epsilon^{-1} - 1$, and so, as above, $|\delta\epsilon^{-1} + k| \geq \frac{1}{2}|\delta\epsilon^{-1}|$. But

$$|\delta\epsilon^{-1}| \geq C\|\delta\epsilon^{-1}\| \geq C \frac{\|\delta\|}{\|\epsilon\|} \geq \frac{C^2}{B} \frac{|\delta|}{|\epsilon|}.$$

So $|\delta\epsilon^{-1} + k| \geq (C^2/2B)|\delta||\epsilon|^{-1}$. Again, as above, we get

$$|N(\epsilon - \delta\epsilon^{-1})| \geq K^{-n}((C^2/2B)|\delta||\epsilon|^{-1})^{2N-2n}$$

so

$$|\epsilon - \delta\epsilon^{-1}| \geq (C/K)((C^2/2B)|\delta||\epsilon|^{-1})^{2(N/n)-2}.$$

But

$$2|\delta\epsilon^{-1}||\epsilon| \geq |\delta\epsilon^{-1}| + |\epsilon| \geq |\delta\epsilon^{-1} \pm \epsilon|$$

so

$$2|\delta\epsilon^{-1}||\epsilon| \geq (C/K)((C^2/2B)|\delta||\epsilon|^{-1})^{2(N/n)-2n}.$$

But

$$|\delta\epsilon^{-1}| \leq B\|\delta\|\|\epsilon^{-1}\| \leq B\|\delta\|\|\epsilon\|^n \leq \frac{B}{C^{n+1}}|\delta||\epsilon|^n$$

(since $\epsilon^{-1} = N(\epsilon)/\epsilon$) and so

$$\frac{2B}{C^{n+1}}|\delta||\epsilon|^{n+1} \geq \frac{C}{K} \left(\frac{C^2}{2B}|\delta||\epsilon|^{-1} \right)^{2(N/n)-2}.$$

Hence

$$|\epsilon|^{2(N/n)+n-1} \geq \frac{C^{4(N/n)+n-2}}{(2B)^{2(N/n)-1}} K^{-1} |\delta|^{2(N/n)-3}.$$

Now, as above, $|\delta| \geq (2C)^{-1}N^J > [C^{4(N/n)+n-2}/(2B)^{2(N/n)-1}K]^{-1}$ and so

$$(**) \quad |\epsilon|^{2(N/n)+n-1} \geq |\delta|^{2(N/n)-4}.$$

Combining (*) and (**) we have

$$|\epsilon|^{2(N/n)+n-1} \geq |\epsilon|^{(2(N/n)-3)(2(N/n)-4)},$$

i.e.,

$$\begin{aligned} 1 &\geq |\epsilon|^{4(N^2/n^2)-16(N/n)+13-n} \\ &\geq |\epsilon| \quad \text{since } 4(N^2/n^2) - 16(N/n) + 13 - n > 1 \\ &\geq (2C)^{-1}N^J > 1. \end{aligned}$$

This contradiction shows that $\delta = \epsilon^2$.

REMARK. Lemma 2 shows that the condition $N^J|\epsilon - 1|$ can be satisfied for units $\epsilon \neq 1$. Hence, if we can exclude the case $\epsilon = 1$, Lemma 3 will enable us to pick out arbitrarily large pairs of units ϵ, ϵ^2 . Choose prime p large enough so that $2^n \not\equiv \pm 1 \pmod{p}$. Then it is easy to see that

$$\begin{aligned} y \neq 0 &\leftrightarrow \exists r, s, h[(ry) + s(ph + 2)) = 1] \\ &\leftrightarrow \exists A, B, h[y|A \wedge ph + 2|B \wedge A + B = 1]. \end{aligned}$$

This gives us an existential definition of $y \neq 0$.

LEMMA 4. Let N be as above and let $I \geq (4K^2/C^2)B^{2N/n}2^{4N/n}$. Then if ϵ is a unit and $\delta = \epsilon^2$ and $\epsilon - 1 \neq 0, \delta - 1 \neq 0$ and

$$\bigwedge_{k=0}^N [Ia \pm k|\epsilon - 1 \wedge Ib \pm k|\epsilon - 1],$$

then

$$a^2 = b \leftrightarrow \bigwedge_{k=0}^N [a \pm k\epsilon|b - k^2\delta].$$

PROOF. Again one direction is trivial. Conversely, suppose that a, b, ϵ, δ satisfy $Ia \pm k|\epsilon - 1, Ib \pm k|\epsilon - 1$ and $a \pm k\epsilon|b - k^2\delta$ for $k = 0, \dots, N$. From $Ia \pm k|\epsilon - 1, k = 0, \dots, N$, we have

$$\epsilon - 1 = (\gamma/K) \prod_{k=-N}^N (Ia + k)$$

and so

$$|N(\epsilon - 1)| \geq K^{-n} \prod |N(Ia + k)|.$$

As above this gives

$$|N(\epsilon - 1)| \geq K^{-n}((1/2B)I|a|)^{2N-2n}$$

and so

$$(1) \quad \begin{aligned} |\epsilon|^n &\geq (C^n/2^n K^n)((1/2B)I|a|)^{2N-2n}, \\ |\epsilon| &\geq \frac{C}{2K} \left(\frac{1}{2B} I|a| \right)^{2(N/n)-2} \geq \frac{2B}{C^2} |a|^2 \geq 2|a| \end{aligned}$$

(since $I \geq (4K^2/C^4)(2B)^{2N/n+1}$). Similarly

$$(2) \quad |\epsilon| \geq 2|b|.$$

Now if $b \neq a^2$, then from $a \pm k\epsilon|b - k^2\delta$, $k = 1, \dots, N$, we get

$$b - a^2 = \frac{\gamma''}{K} \prod_{k=-N}^N (a + k\epsilon).$$

So

$$|N(b - a^2)| \geq \frac{1}{K^n} \prod_{k=-N}^N |N(a + k\epsilon)|.$$

Now except for at most $2n$ values of k ,

$$|N(a + k\epsilon)| \geq \|a + k\epsilon\| \geq B^{-1}|a + k\epsilon| \geq (2B)^{-1}|\epsilon|$$

from (1). Hence,

$$|b| + |a^2| \geq (C/K)((1/2B)|\epsilon|)^{2(N/n)-2n}.$$

So

$$|b| \geq (C/K)((1/2B)|\epsilon|)^{2(N/n)-2} - |a^2|.$$

Now

$$|a^2| \leq B\|a^2\| = B\|a\|^2 \leq (B/C^2)|a|^2.$$

Hence

$$|b| \geq \left(\frac{C}{K} \frac{1}{2B} \right)^{2(N/n)-2} |\epsilon|^{2(N/n)-2} - \frac{B}{C^2} |a|^2.$$

From (1),

$$\left(\frac{C}{K} \frac{1}{2B} \right)^{2(N/n)-2} |\epsilon|^{2(N/n)-2} > \frac{2B}{C^2} |a|^2$$

and so

$$|b| \geq \frac{1}{2} \left(\frac{C}{K} \frac{1}{2B} \right)^{2(N/n)-2} |\epsilon|^{2(N/n)-2} > |\epsilon|$$

again from (1). This contradicts (2). Hence $b = a^2$.

PROOF OF THE THEOREM. Lemma 2 shows that we can find ϵ satisfying all the divisibilities in Lemmas 3 and 4, of the form $x|\epsilon - 1$. The additional divisibilities in Lemma 3 guarantee that $\delta = \epsilon^2$ and the other divisibilities in Lemma 4 guarantee that $b = a^2$.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1965.
2. R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$* , Ann. of Math. (2) **15** (1913).
3. L. Lipshitz, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. (to appear).
4. L. Lipshitz, *Undecidable existential problems for addition and divisibility in algebraic number rings*, Trans. Amer. Math. Soc. (to appear).
5. H. Weyl, *Algebraic theory of numbers*, Ann. of Math. Studies, Princeton Univ. Press, Princeton, N.J., 1940.

THE INSTITUTE FOR ADVANCED STUDY, SCHOOL OF MATHEMATICS, PRINCETON, NEW JERSEY
08540