ACTA ARITHMETICA
IX (1964)

On the equation $y^m = f(x)$

by

W. J. LeVeque (Ann Arbor, Michigan and Boulder, Colo.)*

1. Introduction. Let k be an algebraic number field, with O_k its ring of integers, and suppose that $f(x) \in O_k[x]$. The relationship between the set of solutions of the diophantine equation

$$y^m = f(x), \qquad x, y \in O_k \tag{1}$$

and the nature of the polynomial $f(x)$ has been studied by many authors; we cite a few of the results.

(i) When $k = \boldsymbol{Q}$, the field of rational numbers, the solvability in $\boldsymbol{Z} = O_{\boldsymbol{Q}}$ of $y^m = f(x)$, for every $x \in \boldsymbol{Z}$, implies that $f(x) = \big(g(x)\big)^m$ for some polynomial g. This result has been published as a problem at least three times, and several quite different solutions have been given (see [2], [3] and [4] for literature). The proofs are all fairly elementary, and led the authors to statements of varying degrees of precision and generality.

(ii) C. L. Siegel [7] showed by very deep methods that (1), and indeed any polynomial equation $f(x, y) = 0$ over k, has infinitely many integral solutions in k only if the curve represented by the equation is a special type of curve of genus 0. He had earlier [6] given a much simpler proof of the following special case: if $m = 2$ and $f(x)$ has at least three distinct zeros, then (1) has only finitely many solutions. This latter proof used the Thue-Siegel theorem, as well as the finiteness of the class number and the rank of the group of units in k.

(iii) H. Davenport, D. J. Lewis and A. Schinzel [1] showed, among other things, that if $k = \boldsymbol{Q}$ and if in every arithmetic progression there is an x satisfying (1), then $f = g^m$ for some $g \in \boldsymbol{Z}[x]$. Their proof depended on a density theorem from the theory of algebraic numbers.

Thus it is apparent that the simplicity of proof of results concerning (1) depends rather strongly on the kind of assumption made about the set of solutions. It is the object of the present note to apply Siegel's

* Work supported in part by a National Science Foundation Grant.

(1926) method to give a complete description of the circumstances under which (1) has infinitely many solutions, and, under those circumstances, an asymptotic estimate for the frequency of solutions.

We suppose throughout that $f(x)$ has the representations

$$f(x) = a_0x^N + \ldots + a_N = a_0\prod_{i=1}^{n}(x-a_i)^{r_i},$$

with $a_0 \neq 0$, and $a_i \neq a_j$ for $i \neq j$. Let $K_0 = k(a_1, \ldots, a_n)$, and let K be any finite extension of k.

2. Necessary conditions for solvability. Siegel has pointed out that while the determination of the circumstances under which a diophantine equation $f(x, y) = 0$ has infinitely many integral solutions in a fixed algebraic number field K is a very delicate problem, much of the delicacy disappears if one requires only that there be infinitely many solutions $x, y \epsilon K$ such that all the numbers ηx, ηy be integers, for some fixed integer $\eta \neq 0$ of K. In light of this observation, we introduce (as Siegel did) the notion of a *quasi-integral set* $G = G_K \subset K$, this being any infinite set such that ηG is a set of integers in K for some fixed integer $\eta \neq 0$ in K. (For finite sets this notion would be trivial, since there is then always such an η.)

We first show that unless $f(x)$ is of very special form, there is no infinite set of solutions in any fixed algebraic number field for which the x-components form a quasi-integral set.

THEOREM 1. *In the notation introduced earlier, put*

$$s_i = \frac{m}{(m, r_i)}, \qquad i = 1, 2, \ldots, n.$$

Then the equation (1) *has no infinite set of solutions in any algebraic number field for which X, the set of x-values, is quasi-integral, unless* $\{s_1, \ldots, s_n\}$ *is a permutation of one of the n-tuples*

(a) $\{s, 1, 1, \ldots, 1\}$, $s \geqslant 1$,

(b) $\{2, 2, 1, \ldots, 1\}$.

Suppose that there is a set of solutions in some algebraic number field K with X quasi-integral; with no loss in generality we may suppose that $K_0 \subset K$. In this section we abbreviate O_K to O. Choose $b \epsilon O$ in such fashion that $ba_1, \ldots, ba_n$, b^N/a_0 and all the numbers bx, for $x \epsilon X$, belong to O. Put $b^N/a_0 = a$ and $ba_i = \beta_i$ for $i = 1, \ldots, n$. Then (1) can be written in the form

$$ay^m = \prod_{i=1}^{n}(bx-\beta_i)^{r_i}. \tag{2}$$

From this it is seen that for all $x \epsilon X$, the number ay is an integer, so that, by increasing b if necessary, it can be supposed that $y \epsilon O$. Using brackets to indicate integral principal ideals in O, we have

$$[a][y]^m = \prod_{i=1}^{n}[bx-\beta_i]^{r_i}. \tag{3}$$

Now for $i \neq j$ and $bx \epsilon O$,

$$[bx-\beta_i, bx-\beta_j] \mid [\beta_i-\beta_j],$$

so that the g. c. d. of any two factors on the right hand side of (3) is a divisor of the fixed ideal

$$\prod_{1\leqslant i<j\leqslant n}[\beta_i-\beta_j]^N.$$

Thus there is a finite set $\mathscr{F}_1$ of ideals in O such that for every pair $x, y \epsilon O$ satisfying (3), and for every i, with $1 \leqslant i \leqslant n$, there is a $\mathfrak{d} \epsilon \mathscr{F}_1$ such that

$$[bx-\beta_i]^{r_i} = \mathfrak{d}\mathfrak{c}^m \tag{4}$$

for some ideal $\mathfrak{c}$ in O depending on x and i. Let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{c}$ and such that $N\mathfrak{p} > \max_{\mathfrak{d}\epsilon\mathscr{F}_1} N\mathfrak{d}$. Then if $\mathfrak{p}^t \parallel \mathfrak{c}^m$, t must be a multiple of m and of r_i, and hence of their l.c.m. r_is_i, so that we can write

$$\mathfrak{c}^m = \mathfrak{c}_1^{r_is_i}\cdot\mathfrak{c}_2, \tag{5}$$

where $\mathfrak{c}_2$ is divisible only by powers of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} \leqslant \max_{\mathfrak{d}\epsilon\mathscr{F}_1} N\mathfrak{d}$. The ideal $\mathfrak{c}_2$, in turn, can be written as a product $\mathfrak{c}_3^{r_is_i}\cdot\mathfrak{c}_4$, where $\mathfrak{c}_4$ is such that every prime power factor has exponent less than r_is_i; there are only finitely many such ideals $\mathfrak{c}_4$. Hence we have from (4),

$$[bx-\beta_i]^{r_i} = \mathfrak{d}(\mathfrak{c}_1\mathfrak{c}_3)^{r_is_i}\mathfrak{c}_4$$

or

$$[bx-\beta_i]^{r_i} = \mathfrak{c}_5^{r_is_i}\mathfrak{c}_6, \tag{6}$$

where $\mathfrak{c}_6$ is one of a finite set $\mathscr{F}_2$ of ideals in O. It follows from (6) that $\mathfrak{c}_6$ is an r_i-th power, so that

$$[bx-\beta_i] = \mathfrak{c}_5^{s_i}\mathfrak{c}_7 \tag{7}$$

where $\mathfrak{c}_7$ is a finitely many valued function of x and i.

Now let $\mathfrak{q}$ run over a fixed system of representatives of the various ideal classes in O; the number of $\mathfrak{q}$'s is finite. Each $\mathfrak{c}_5$ occurring in (7) is equivalent to some $\mathfrak{q}$, so that there are γ and δ in O such that

$$[\gamma]\mathfrak{c}_5 = [\delta]\mathfrak{q}; \tag{8}$$

we shall show that γ can be chosen from a finite subset of O.

Let $[\gamma, \delta] = \mathfrak{n}$, $[\gamma] = \mathfrak{n}\mathfrak{f}$, $[\delta] = \mathfrak{n}\mathfrak{g}$. Then from (8),

$$\mathfrak{n}\mathfrak{f}\mathfrak{c}_5 = \mathfrak{n}\mathfrak{g}\mathfrak{q}, \tag{9}$$

whence $\mathfrak{f} \mid \mathfrak{q}$, so that $\mathfrak{f}$ is one of a finite set $\mathscr{F}_3$ of ideals of O. As is wele known, there is a positive constant c_1, depending only on K, such thal there is an $\mathfrak{h}$ in O with $N\mathfrak{h} < c_1$ for which $\mathfrak{f}\mathfrak{h} = [\zeta]$ is principal. Henct from (9),

$$\mathfrak{h}\mathfrak{f}\mathfrak{c}_5 = \mathfrak{h}\mathfrak{g}\mathfrak{q}, \quad [\zeta]\mathfrak{c}_5 = (\mathfrak{h}\mathfrak{g})\mathfrak{q}.$$

Since $\mathfrak{c}_5 \sim \mathfrak{q}$, it follows from this that $[\zeta] \sim \mathfrak{h}\mathfrak{g}$, so for suitable $\xi \in O$, $\mathfrak{h}\mathfrak{g} = [\xi]$ and $[\zeta]\mathfrak{c}_5 = [\xi]\mathfrak{q}$. This shows that γ in equation (8) can be chosen to be one of the finitely many different integers ζ required to generate the various ideals $\mathfrak{f}\mathfrak{h}$.

Returning to (7), we obtain from (8) the relation

$$[bx-\beta_i][\gamma]^{s_i} = \mathfrak{c}_7[\gamma]^{s_i}\mathfrak{c}_5^{s_i} = \mathfrak{c}_7[\delta]^{s_i}\mathfrak{q}^{s_i},$$

so that $\mathfrak{c}_7\mathfrak{q}^{s_i}$ is a principal ideal, say $\mathfrak{c}_7\mathfrak{q}^{s_i} = [\theta]$. Thus for some unit $\varepsilon \in O$,

$$\gamma^{s_i}(bx-\beta_i) = \varepsilon\theta\delta^{s_i},$$

and θ is an element of a fixed finite set $\mathscr{F}_4 \subset O$. By Dirichlet's theorem on units, ε can be written in the form

$$\varepsilon = \varepsilon'\varepsilon''^{s_i},$$

in which ε' is one of a fixed finite set $\mathscr{F}_5$ of units in O. Thus finally we see that for every x, y in K satisfying (1) and such that $bx \in O$,

$$bx-\beta_i = \varkappa_i(x)\,\delta_i^{s_i}(x), \tag{10}$$

where $\varkappa_i$ is an element of a finite set $\mathscr{F}_6$ in K.

Now since there are infinitely many x of the required sort, there is a particular set of values of $\varkappa_1(x), \ldots, \varkappa_n(x)$, say $\lambda_1, \ldots, \lambda_n$, which is associated with infinitely many distinct solutions x, y, and it is obvious from the equation

$$bx-\beta_i = \lambda_i\,\delta_i^{s_i}(x) \tag{11}$$

that λ_i is not zero and that distinct values of x determine distinct values of $\delta_i(x)$.

If $\{s_1, \ldots, s_n\}$ is of neither of the forms (a) and (b) of the theorem, it must be that with suitable ordering either $s_1 = s_2 = s_3 = 2$ or $s_1 \geqslant 3$ and $s_2 \geqslant 2$. In the first case, m must be a multiple of 2 and $f(x)$ must have at least three distinct zeros; this case is covered by Siegel's theorem ([6]; or see [5], p. 155). On the other hand, if $s_1 \geqslant 3$ and $s_2 \geqslant 2$,

we see from (11) that the equation

$$\lambda_1 z^{s_1} = \lambda_2 w^{s_2} + (\beta_2-\beta_1) \tag{12}$$

must have a quasi-integral set of solutions $z = \delta_1(x)$, $w = \delta_2(x)$ in K; moreover, the polynomial $g(w) = \lambda_2 w^{s_2} + (\beta_2-\beta_1)$ has distinct zeros. In other words, (12) is the special case of (1) in which $m = s_1 \geqslant 3$, $n = N = s_2$, and $r_i = 1$ for $i = 1, \ldots, n$. Repeating the entire argument in this special case, we arrive at the following analogue of (12):

$$\mu_1 x^{s_1} - \mu_2 y^{s_1} = d. \tag{13}$$

More explicitly, there are nonzero numbers d (the difference between some two zeros of $g(w)$), μ_1 and μ_2 in K such that (13) has a quasi-integral solution set X, Y in O. But it is well known that this is impossible.

3. Case (a) of Theorem 1. We now investigate the nature of the solutions of (1) in case (a). If $m/(m, r_1) = s$, then $(m, r_1) = m/s$ and hence $r_1 = mt/s$, where $(t, s) = 1$. Thus $f(x)$ factors in K as

$$a_0(x-a_1)^{mt/s}\prod_{i=2}^{n}(x-a_i)^{mr_i'},$$

where $r_2', \ldots, r_n'$ are positive integers. If a_1 is of degree $\geqslant 2$ over k, then mt/s must be a multiple of m, which is the case if and only if $s = 1$. In this case, (1) can be written in the form

$$y^m = \varkappa f_1^m(x), \quad f_1 \in O_k[x], \ \varkappa \in k.$$

Clearly this equation has solutions in a number field $K \supset k$ if and only if $\varkappa$ is an mth power in K. If we suppose this, then we have the parametric solution

$$x = u, \quad y = \varkappa^{1/m} f_1(u). \tag{14}$$

Allowing u to range over a quasi-integral set G_K, we get quasi-integral sets X and Y, and it is clear that u must be restricted to such a set.

Now consider the case $s > 1$. Equation (1) can then be written in the form

$$y^m = \varkappa(x-a_1)^{mt/s} f_2^m(x), \quad \varkappa \in k, \ a_1 \in k, \ f_2 \in O_k[x]. \tag{15}$$

In order that this equation be solvable in K, it is clearly necessary that $\varkappa = \lambda^{m/s}$ for some $\lambda \in K$. If this is the case, x must then be chosen so that $\lambda(x-a_1)^t = u^s$, $u \in G_K$. To see that this is possible, we shall use the following

LEMMA. *If s and t are coprime rational integers and λ is an element of an algebraic number field K, then there are $\mu_1, \mu_2 \in K$ such that*

$$\lambda = \mu_1^s/\mu_2^t.$$

To prove this lemma, suppose that in K,

$$[\lambda] = \prod \mathfrak{p}_i^{a_i}, \qquad a_i \in \mathbf{Z}.$$

For each i, there are p_i and q_i such that $a_i = sp_i - tq_i$, so we can write

$$[\lambda] = \frac{\left(\prod \mathfrak{p}_i^{p_i}\right)^s}{\left(\prod \mathfrak{p}_i^{q_i}\right)^t} = \frac{\mathfrak{a}^s}{\mathfrak{b}^t}, \tag{16}$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of K. Now find $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} \sim 1$, say $\mathfrak{a}\mathfrak{c} = [\theta]$. By (16),

$$\mathfrak{b}^t\mathfrak{c}^s \sim 1. \tag{17}$$

Then if j and k are rational integers satisfying the equation $sj + tk = 1$, we have

$$\mathfrak{c}^{sj} \sim \mathfrak{b}^{-tj} \quad \text{and} \quad \mathfrak{c}^{sj} = \mathfrak{c}^{1-tk},$$

so that $\mathfrak{c} \sim (\mathfrak{b}^{-j}\mathfrak{c}^{-k})^t$, or $\mathfrak{c} \sim \mathfrak{d}^t$ for suitable $\mathfrak{d}$. Thus

$$\mathfrak{b}^t\mathfrak{c}^s \sim (\mathfrak{b}\mathfrak{d}^s)^t,$$

and hence

$$[\lambda] = \frac{[\theta]^s}{(\mathfrak{b}\mathfrak{d}^s)^t}.$$

Now by (17),

$$\mathfrak{b}\mathfrak{d}^s = \mathfrak{b}(\mathfrak{b}^{-j}\mathfrak{c}^{-k})^s = \mathfrak{b}^{1-js}\mathfrak{c}^{ks} = \mathfrak{b}^{tk}\mathfrak{c}^{ks} = (\mathfrak{b}^t\mathfrak{c}^s)^k \sim 1,$$

so that $\lambda = \varepsilon\theta^s/\xi^t$, where ε is a unit and $\varepsilon, \theta, \xi \in K$. Finally, ε can be written in the form $\varepsilon_1^s/\varepsilon_2^t$, by Dirichlet's units theorem and the argument used to obtain (16). We can then choose $\mu_1 = \varepsilon_1\theta$, $\mu_2 = \varepsilon_2\xi$.

Thus if K is a field in which $\varkappa = \lambda^{m/s}$, equation (15) can be written in the form

$$y^m = \mu_1^m\left(\frac{x-\alpha_1}{\mu_2}\right)^{mt/s} f_2^m(s); \qquad \mu_1, \mu_2, \alpha_1 \in K;\ f_2 \in O_k[x].$$

In order that the values of y constitute a quasi-integral set in K, it is clearly necessary and sufficient that

$$\left(\frac{x-\alpha_1}{\mu_2}\right)^{mt/s} = v^m, \qquad v \in G_K,$$

hence that

$$x = \alpha_1 + \mu_2 v^{s/t}.$$

But then x ranges over a G_K if and only if $v = u^t$, where u ranges over a G_K, so that in this case the general quasi-integral set of solutions of (1) in K is given by

$$x = \alpha_1 + \mu_2 u^s, \qquad y = \mu_1 u^t f_2(x), \qquad u \in G_K. \tag{18}$$

While the numbers μ_1 and μ_2 in the representation $\varkappa = \mu_1^m/\mu_2^{mt/s}$ are not unique, it is easily seen that the ratio μ_2/μ_2' corresponding to two such representations is an sth power in K, so that all quasi-integral sets X, Y are given by (18) with fixed μ_1, μ_2, if G_K ranges over all quasi-integral sets in K.

We now examine the frequency of solutions of (1) in case (a).

As usual, we shall mean by $\overline{|\alpha}$ the maximum of the absolute values of the conjugates of the algebraic number α. We designate by $\nu(T, K)$ the number of integers α of K with $\overline{|\alpha|} < T$; $\nu(T, K)$ is finite for every T and K. If G_K is any quasi-integral set, we designate by $\nu_{G_K}(T, K)$ the number of elements $\alpha \in G_K$ for which $\overline{|\alpha|} < T$. It is easy to see that for arbitrary G_K,

$$\nu_{G_K}(T, K) < c_2\nu(T, K)$$

for a suitable constant c_2, and that if G_K consists of a constant multiple of all the integers of K, then

$$\nu_{G_K}(T, K) \sim c_3\nu(T, K)$$

for suitable c_3. In view of these remarks, we can formulate the following theorem to summarize the results of the present section:

THEOREM 2. *Let $f(x)$ be as in Theorem 1, and suppose that $s_1 = s$, $s_2 = \ldots = s_n = 1$, so that*

$$f(x) = \begin{cases} \varkappa f_1^m(x), & \textit{in case } s = 1, \\ \varkappa(x-\alpha_1)^{mt/s} f_2^m(x) \textit{ with } (t, s) = 1, & \textit{in case } s > 1, \end{cases}$$

where $f_1, f_2 \in O_k[x]$ and $\varkappa$, $\alpha_1 \in k$. Then (1) is solvable in K if and only if $\varkappa = \lambda^{m/s}$ for some $\lambda \in K$. If this condition is satisfied there are $\mu_1, \mu_2 \in K$ such that $\varkappa = \mu_1^m/\mu_2^{mt/s}$, and every quasi-integral set of solutions of (1) is given by (14) in case $s = 1$, and by (18) in case $s > 1$, where in each case the range of u is an arbitrary quasi-integral set G_K. It follows that if X is the set of x corresponding to G_K, then always

$$\nu_X(T, K) < c_4\nu(T, K)^{1/s},$$

and that if G_K is suitably chosen,

$$\nu_X(T, K) > c_5\nu(T, K)^{1/s}.$$

Here c_4 and c_5 are suitably chosen positive constants. In particular, if there are infinitely many integral solutions of (1) in K, and X yields the full set of such solutions, then

$$\nu_X(T, K) \sim c_6\nu(T, K)^{1/s}.$$

By the *density* of a quasi-integral set $S \subset K$, we shall mean the limit

$$\lim_{T\to\infty} \frac{\nu_S(T, K)}{\nu(T, K)},$$

if this limit exists.

COROLLARY. *In case* (a) *of Theorem* 1, *the equation* $y^m = f(x)$ *has a quasi-integral set of solutions* $x, y \in K$ *for which* X *has positive density if and only if* $f(x) = f_1^m(x)$, *where* $f_1 \in O_K[x]$.

4. Case (b) **of Theorem 1.** Now suppose that $s_1 = s_2 = 2$, $s_3 = \ldots = s_n = 1$. It is easily seen that then

$$Q(x) = (x - a_1)(x - a_2) \in k[x],$$

and hence that (1) can be written in the form

$$(19) \qquad y^m = \varkappa Q^{mt/2}(x) f_3^m(x); \qquad t \text{ odd}, \ \varkappa \in k; \ Q, f_3 \in O_k[x].$$

This equation is clearly unsolvable (even if x and y are not required to be integers) in an extension K of k unless $\varkappa = \lambda^{m/2}$ for some $\lambda \in K$, so we shall suppose this. Then by the lemma, $\lambda = \mu_1^s/\mu_2^t$ for some $\mu_1, \mu_2 \in K$, and we can write (19) in the form

$$(20) \qquad y^m = \mu_1^m \left(\frac{Ax^2+Bx+C}{D}\right)^{mt/2} f_3(x), \qquad A, B, C, D \in O_K.$$

In order that the set Y of values of y, corresponding to x in a quasi-integral set $X \subset K$, be quasi-integral in K, it is clearly necessary and sufficient that for some G_K, and all $x \in X$,

$$Ax^2+Bx+C = Dw^2, \qquad w \in G_K.$$

This equation can also be written in the form

$$(2Ax+B)^2 - 4ADw^2 = B^2 - 4AC = \Delta.$$

If we put $2Ax+B = u$ and $v = 2w$, then as x (or w) runs through a quasi-integral set, so also does u (or v), and conversely. The Pell equation

$$(21) \qquad u^2 - Ev^2 = \Delta,$$

where we have put $E = AD$, may or may not be solvable in K. Suppose that it is so solvable. Then we have

$$(u - \sqrt{E}v)(u + \sqrt{E}v) = \Delta,$$

so that the solution in K corresponds to a factorization of Δ in $L = K(\sqrt{E})$ into factors conjugate over K. Conversely, every such factorization of Δ in L corresponds to a solution of (21). Moreover, if there is a quasi-integral set of solutions of (21) in K, there is an $\eta \in O_K$ such that ηu and ηv are integers in K, and to each such pair u, v corresponds biuniquely a factorization $\Delta = \Delta_1 \Delta_2$ such that Δ_1 and Δ_2 are conjugate over K and $\eta\Delta_1, \eta\Delta_2 \in O_L$. If we call such factorizations "appropriate", we see that we can count the solutions of (21) in K by counting the corresponding appropriate factorizations of Δ in L.

For fixed η there are only finitely many appropriate factorizations $\Delta = \Delta_1\Delta_2$ in which no two of the factors Δ_1 are associates in L. On the other hand, each of these nonassociated factorizations leads to the further factorizations $\varepsilon\Delta_1 \cdot \varepsilon^{-1}\Delta_2$, where ε ranges over the units of L, and these factorizations are appropriate if and only if ε and ε^{-1} are conjugate with respect to K. By Dirichlet's theorem on units, the group $\mathscr{E}_L$ of units in L is finitely generated, and since it is easily verified that the set of units ε for which $\bar{\varepsilon} = \varepsilon^{-1}$ is a subgroup $\mathscr{H}$ of $\mathscr{E}_L$, also $\mathscr{H}$ is finitely generated. Let $\varepsilon_1, \ldots, \varepsilon_\varrho$ be a basis for $\mathscr{H}$. Then all the appropriate factorizations of Δ are given by $\Delta_1\Delta_2$, in which $\Delta_1 = \Delta_1'\varepsilon$, Δ_1' is one of a finite set of elements of L, and $\varepsilon \in \mathscr{H}$. Moreover, if $\Delta_1 = u + \sqrt{E}v$, then

$$c_7 \, \overline{|\Delta_1|} < \overline{|u|} < c_8 \, \overline{|\Delta_1|},$$

so to within a bounded factor we can count the solutions of (20) with $\overline{|u|} \leqslant T$ by counting the Δ_1's with $\overline{|\Delta_1|} \leqslant T$. Since Δ_1' has finite range, it suffices to count the $\varepsilon \in \mathscr{H}$ for which $\overline{|\varepsilon|} \leqslant T$.

We have

$$\varepsilon = \varepsilon_1^{b_1} \ldots \varepsilon_\varrho^{b_\varrho}$$

for suitable exponents $b_1, \ldots, b_\varrho$, so that, using superscripts to denote conjugates,

$$(22) \qquad \log|\varepsilon^{(i)}| = b_1 \log|\varepsilon_1^{(i)}| + \ldots + b_\varrho \log|\varepsilon_\varrho^{(i)}|,$$

and $\overline{|\varepsilon|} \leqslant T$ $(T > 1)$ if and only if

$$(23) \qquad |\log|\varepsilon^{(i)}|| < \log T, \qquad i = 1, \ldots, l,$$

where $l = [L : Q]$. In view of (22), the solutions of (23) are those points of a certain lattice in ϱ-dimensional space which lie in a hypercube of side $2\log T$; evidently the number of such lattice points is asymptotic to $c_9 \log^\varrho T$ as $T \to \infty$, for suitable $c_9 > 0$. Hence for the corresponding solutions $x \in X$ of (18) we have

$$\nu_X(T, L) = M_1 \log^\varrho T,$$

where M_1 (and M_2 below) is a quantity depending on $L, \gamma, Q(x)$ and T, such that if L, γ and Q are fixed, M_1 remains bounded away from 0 and ∞ as $T \to \infty$.

Using an integral basis for L, we see by the same reasoning that

$$\nu(T, L) \sim c_{10} T^{l}, \qquad c_{10} > 0,$$

and hence that

$$\nu_X(T, L) = M_2 \log^{\varrho} \nu(T, L).$$

There remains the question of when ϱ is positive. Obviously $\varrho = 0$ if $L = K$, so suppose that $[L:K] = 2$. Suppose further that K has r_1 real and $2r_2$ nonreal conjugate fields over $\boldsymbol{Q}$, the corresponding numbers for L being r_1' and $2r_2'$. If $[K:\boldsymbol{Q}] = n$, then

$$n = r_1 + 2r_2,$$
$$2n = r_1' + 2r_2',$$

and the numbers of generators of infinite order of $\mathscr{E}_K$ and $\mathscr{E}_L$ are

$$r = r_1 + r_2 - 1,$$
$$r' = r_1' + r_2' - 1,$$

respectively. Now the relative norm mapping $\boldsymbol{N}_{L/K}$ is a homomorphism from $\mathscr{E}_L$ to $\mathscr{E}_K$ with kernel $\mathscr{H}$, and the kernel contains at least $r' - r$ infinite generators.

If $r_2 > 0$, then since $r_2' \leqslant r' + 1$,

$$r' = r_1' + r_2' - 1 = 2n - r_2' - 1 \geqslant 2n - r' - 2$$

so that $r' \geqslant n - 1 = r + r_2 > r$ and $r' - r > 0$.

If $r_2 = 0$ and also $r_2' = 0$, then $r' - r = r_1' - r_1 = n > 0$.

If on the other hand $r_2 = 0$ and $r_2' > 0$, so that K is totally real and L is a nonreal quadratic extension of K, then the equation $u^2 - Ev^2 = 1$ has only finitely many solutions in $\eta^{-1} O_K$, for each η. For let $K_1 = K$, $K_2, \ldots, K_n$ be the fields conjugate to K, and let subscripts denote conjugates. Then $u_j^2 - E_j v_j^2 = 1$ for $j = 1, \ldots, n$, and since the u_j and v_j are all real, while $\sqrt{E}$ is pure imaginary, the numbers $u_j \pm \sqrt{E} v_j$ are complex-conjugate for each j, and therefore $|u_j + \sqrt{E} v_j| = |u_j - \sqrt{E} v_j| = 1$ for $j = 1, \ldots, n$. Hence if u and v could range over quasi-integral sequences in K and retain the property $u^2 - Ev^2 = 1$, we should have a quasi-integral sequence $\{u + \sqrt{E} v\}$ in L such that $\overline{|u + \sqrt{E} v|} = 1$, and this is clearly impossible.

Collecting the results of this section, we have the following theorem:

THEOREM 3. *In case* (b) *of Theorem* 1, *the equation* (19) *is solvable in* $K \supset k$ *only if* $\varkappa = \lambda^{m/2}$, $\lambda \in K$. *If this condition is satisfied, then* (19) *can be written in the form* (20), *and it is solvable in* K *if and only if the relative Pell equation* $u^2 - ADv^2 = B^2 - 4AC$ *is solvable in* K. *If* (19) *is solvable in* K, *it has a quasi-integral set of solutions in* K *if and only if the group* $\mathscr{H}$ *of units* ε *of* $L = K(\sqrt{AD})$ *for which* $\boldsymbol{N}_{L/K}\varepsilon = 1$ *is infinite. If* $K = L$, *or if* K *is totally real and* $AD < 0$, *then* $\mathscr{H}$ *is finite; in all other cases* $\mathscr{H}$ *is infinite.*

When $\mathscr{H}$ *is infinite, let* ϱ *be the number of generators of* $\mathscr{H}$ *which are of infinite order. Then if* (19) *is solvable in* K, *there is a quasi-integral set of solutions* $x, y \in K$ *for which*

$$c_{11} \log^{\varrho} \nu(T, K) < \nu_X(T, K) < c_{12} \log^{\varrho} \nu(T, K) \tag{24}$$

for some positive constants c_{11} *and* c_{12}. *For every quasi-integral set* X, *the second inequality of* (24) *holds for suitable* c_{12}.

References

[1] H. Davenport, D. J. Lewis and A. Schinzel, *On polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107-116.

[2] E. Fried and J. Surányi, *New proof of a number theoretic theorem on polynomials*, Matematikai Lapok 11 (1960), pp. 75-84. (Hungarian).

[3] W. H. J. Fuchs, *A polynomial the square of another polynomial*, Amer. Math. Monthly 57 (1950), pp. 114-115.

[4] T. Kojima, *Note on number-theoretical properties of algebraic functions*, Tohôku Math. Journal 8 (1915), pp. 24-37.

[5] W. J. LeVeque, *Topics in number theory*, vol. 2, Reading, Mass. 1956.

[6] C. L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, Journ. London Math. Soc. 1 (1926), pp. 66-68.

[7] — *Über einige Anwendungen Diophantischer Approximationen*, Abh. preuss. Akad. Wiss. 1929, No. 1.

Reçu par la Rédaction le 31. 10. 1963