Math. Proc. Camb. Phil. Soc. (1986), **100**, 237
Printed in Great Britain

Uniform bounds for the number of solutions to $Y^n = f(X)$

BY J.-H. EVERTSE
Centre of Mathematics and Computer Science, 1009 AB Amsterdam, The Netherlands

AND J. H. SILVERMAN
Massachusetts Institute of Technology, Cambridge, MA 02139, U.S.A.

(*Received* 3 *October* 1985; *revised* 11 *February* 1986)

0. *Introduction*

Let K be an algebraic number field and $f(X) \in K[X]$. The Diophantine problem of describing the solutions to equations of the form

$$y^n = f(x) \quad (n \geqslant 2) \tag{+}$$

has attracted considerable interest over the past 60 years. Siegel [12], [13] was the first to show that under suitable non-degeneracy conditions, the equation (+) has only finitely many integral solutions in K. LeVeque [7] proved the following, more explicit, result. Let

$$f(x) = a(x-\alpha_1)^{r_1} \dots (x-\alpha_k)^{r_k}, \quad n_i = n/\gcd(n, r_i) \quad \text{for} \quad i = 1, \dots, k,$$

where $a \in K^*$ and $\alpha_1, \dots, \alpha_k$ are distinct and algebraic over K. Then (+) has only finitely many integral solutions unless $(n_1, \dots, n_k)$ is a permutation of one of the n-tuples

$$(2, 2, 1, 1, \dots, 1) \quad \text{or} \quad (t, 1, 1, \dots, 1) \quad \text{with} \quad t \geqslant 1.$$

We mention that Leveque's theorem was ineffective. When $K = \mathbb{Q}$ and $f(x)$ has at least two simple zeros with $n \geqslant 3$ or three simple zeros with $n = 2$, Baker [1] has given an explicit upper bound for the solutions to (+) which depends on n and f. Under the same conditions for K and f, Schinzel and Tijdeman [9] derived an effective constant C, depending only on f, such that if $n > C$, then (+) has no solutions $x, y \in \mathbb{Z}$ with $y \neq \pm 1$. Effective upper bounds for solutions to (+) in S-integers of a number field have been given by Trelina [17] and Bindza [2]. Finally, Faltings [5] has shown that if K is an algebraic number field and (+) describes a curve of genus at least 2, then (+) has only finitely many solutions $x, y \in K$. Faltings' theorem is not effective.

The equation (+) has also been extensively studied in the case that K is a (one-dimensional) function field. In this case, if (+) gives a curve of genus at least 2, effective upper bounds for the heights of solutions in K have been given by Schmidt [10] and Mason [8]. However, in contrast to the number field case, a bound for the heights of solutions does not imply that there are only finitely many solutions. Mason [8] has given an effective procedure for finding all the solutions to (+).

It is our aim in this paper to give an explicit upper bound for the *number* of solutions to (+) when $f(x)$ has distinct roots (in an algebraic closure of K). We will do this for S-integral solutions when K is a number field, and for rational solutions (i.e. in K) when K is a function field. In both cases, we have attempted to give bounds which depend minimally on K, S, and f. For example, our bounds depend only on the number of primes dividing the discriminant of f, and not on which primes are in this set. We were not able to derive such attractive bounds under LeVeque's more general condition on f. Our result for number fields is as follows.

THEOREM 1. *Set the following notation*:

K	*an algebraic number field of degree* m.
S	*a finite set of places of* K, *containing the infinite places.*
s	$= \# S$.
R_S	*the ring of* S-*integers of* K.
$f(X)$	$\in R_S[X]$, *a polynomial of degree* d *with discriminant* $\operatorname{disc}(f) \in R_S^*$.
L/K	*an extension of degree* M.
$\kappa_n(L)$	*the* n-*rank of the ideal class group of* L.

For $n \geqslant 2$, *let*

$$V(R_S, f, n) = \{x \in R_S : f(x) \in K^{*n}\}.$$

(*a*) *Let* $n \geqslant 3$, $d \geqslant 2$, *and assume that* L *contains at least two zeros of* f. *Then*

$$\# V(R_S, f, n) \leqslant 17^{M(6m+s)} . n^{2Ms+\kappa_n(L)}.$$

(*b*) *Let* $d \geqslant 3$, *and assume that* L *contains at least three zeros of* f. *Then*

$$\# V(R_S, f, 2) \leqslant 7^{M(4m+9s)} . 4^{\kappa_2(L)}.$$

Remark 1. It is possible to choose L such that $M \leqslant d^2$ in (*a*), and $M \leqslant d^3$ in (*b*).

Remark 2. Sprindzuk [16] has given a proof of Theorem 1 (with constants left uncomputed) in the special case that $R_S = \mathbb{Z}$, $f(X) = X^2 - A$, and $n = 3$.

Remark 3. Let K, S, f be as in Theorem 1, and suppose that f has degree at least 2. One possible generalization of Theorem 1 would be to give an upper bound for the number of solutions $(x, y, n) \in R_S \times R_S \times \mathbb{Z}$ to the equation $y^n = f(x)$ satisfying $n \geqslant 3$, $y \neq 0$, and y not a root of unity. It is very likely that by applying Baker's method one can compute an explicit constant C such that there are no solutions with $n > C$. Shorey, van der Poorten, Tijdeman and Schinzel [11] proved this for $K = \mathbb{Q}$, although they did not give an actual value for C. Combined with Theorem 1, such a constant would immediately give an upper bound for the number of solutions. However, this bound would depend not only on the *number* of places in S, but also on the specific places in the set S.

When K is a (one-dimensional) function field, we can say considerably more about the number of solutions to (+). First, rather than restrict to integral solutions, we deal with arbitrary rational solutions. Second, as in [14], we also allow n to vary. Thus we count the number of $x \in K$ for which $f(x)$ is a perfect nth-power for any $n \geqslant 4$. The precise result is as follows.

THEOREM 2. *Set the following notation.*

k	*a field of characteristic* 0.
K/k	*a (one-dimensional) function field of genus* g *over* k.
S	*a finite set of valuations of* K *containing* $s \geqslant 1$ *elements.*
R_S	*the ring of* S-*integers of* K.
$f(X)$	$\in R_S[X]$, *a monic polynomial of degree* $d \geqslant 3$ *with* $\operatorname{disc}(f) \in R_S^*$.

We further assume that $f(X)$ is non-degenerate. (See section 2 for the precise definition. In essence, this means that f does not arise by change of variables from a polynomial in $k[X]$.) Then the set

$$\{x \in K : f(x) \in K^{*n} \quad \text{for some} \quad n \geqslant 4\}$$

contains at most

$$2^{2d^{18}(2g+s)^6}$$

elements.

1. *The equation $y^n = f(x)$ over algebraic number fields*

Let K be an algebraic number field of degree m, and let M_K denote the places of K. Let $S \subset M_K$ be a finite set of places, containing all infinite places and t finite places, corresponding to the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ respectively. Let R_S be the ring of S-integers of K, $I(K)$ the group of fractional ideals of K, $s = \# S$, and $\kappa_n(K)$ the n-rank of the ideal class group for K. For $\alpha_1, \ldots, \alpha_r \in K$, we let $\langle \alpha_1, \ldots, \alpha_r \rangle$ denote the fractional ideal of K generated by $\alpha_1, \ldots, \alpha_r$. Finally, if $\mathfrak{a}, \mathfrak{b} \in I(K)$ and $n \geqslant 2$ is a rational integer, then we write

$$\mathfrak{a} \equiv \mathfrak{b} \bmod S,$$

if $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_t^{k_t}$ for some $k_1, \ldots, k_t \in \mathbb{Z}$; and

$$\mathfrak{a} \equiv \mathfrak{b} \bmod (n, S),$$

if $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_t^{k_t} \mathfrak{c}^n$ for some $k_1, \ldots, k_t \in \mathbb{Z}$ and $\mathfrak{c} \in I(K)$.

Lemma 1. *Let $\mathfrak{a} \in I(K)$ and $n \geqslant 2$. Then*

$$\# \{z \in K^*/K^{*n} : \langle z \rangle \equiv \mathfrak{a} \bmod (n, S)\} \leqslant n^{s+\kappa_n(K)}.$$

Proof. Suppose that there exists a $z_0 \in K^*$ with $\langle z_0 \rangle \equiv \mathfrak{a} \bmod (n, S)$. Then for each $z \in K^*$, we have $\langle z \rangle \equiv \mathfrak{a} \bmod (n, S)$ if and only if $\langle z/z_0 \rangle \equiv \langle 1 \rangle \bmod (n, S)$. Hence it suffices to prove Lemma 1 in the case that $\mathfrak{a} = \langle 1 \rangle$.

Let $\mathscr{A}$ denote the group $\{z \in K^* : \langle z \rangle \equiv \langle 1 \rangle \bmod (n, S)\}$, let $\mathscr{C}$ denote the ideal class group of K, let $\mathscr{C}(S)$ denote the subgroup of $\mathscr{C}$ generated by the ideal classes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, and let $(\mathscr{C}/\mathscr{C}(S))[n]$ be the subgroup of $\mathscr{C}/\mathscr{C}(S)$ consisting of elements of order dividing n. There is a natural inclusion $i : R_S^*/R_S^{*n} \to \mathscr{A}/\mathscr{A}^n$; and we define a map $j : \mathscr{A}/\mathscr{A}^n \to (\mathscr{C}/\mathscr{C}(S))[n]$ as follows: if $\langle z \rangle = \mathfrak{a}\mathfrak{b}^n$ with $\mathfrak{a}, \mathfrak{b} \in I(K)$ and $\mathfrak{a} \equiv \langle 1 \rangle \bmod S$, then $j(z \bmod \mathscr{A}^n)$ is the coset in $\mathscr{C}/\mathscr{C}(S)$ of the ideal class of $\mathfrak{b}$. One easily checks that this gives an exact sequence

$$0 \to R_S^*/R_S^{*n} \xrightarrow{i} \mathscr{A}/\mathscr{A}^n \xrightarrow{j} (\mathscr{C}/\mathscr{C}(S))[n].$$

Now R_S^* is the direct product of s cyclic groups, so $\# (R_S^*/R_S^{*n}) \leqslant n^s$; while by definition of $\kappa_n(K)$, we have

$$\# (\mathscr{C}/\mathscr{C}(S))[n] \leqslant \# \mathscr{C}[n] \leqslant n^{\kappa_n(K)}.$$

Therefore $\# (\mathscr{A}/\mathscr{A}^n) \leqslant n^{s+\kappa_n(K)}$. This proves Lemma 1 for $\mathfrak{a} = \langle 1 \rangle$.

Lemma 2. *Let $w \in K^*$ and $n \geqslant 3$. Then the number of $\zeta \in K^*$ with*

$$\langle 1 - w\zeta^n \rangle \equiv \langle 1, w\zeta^n \rangle \bmod S \tag{1}$$

is at most

$$5(2.3^{3+30/n})^m + 2(nU(n))^s,$$

where

$$U(n) = \frac{16n-2}{8n-17}\left(\frac{16n-2}{8n+15}\right)^{(8n+15)/(8n-17)}.$$

Proof. Let $\bar{K}$ be an algebraic closure of K, and let $H: \bar{K} \to [1, \infty)$ be the absolute height on $\bar{K}$. In Evertse[3] (chap. 6, theorem 6.2) it was shown that (1) has at most $2(nU(n))^s$ solutions $\zeta \in K^*$ with $H(w\zeta^n) \geqslant 3^n 5^{10}$. In Evertse[4] (lemma 1) it was shown that for every $\theta \in \bar{K}$ and for every $C \geqslant 1$, the number of $z \in K^*$ with $H(\theta z) \leqslant C$ is at most $5(2C^3)^m$. Combining these results (with $\theta = w^{1/n}$ and $C = 3^{1+10/n}$) yields Lemma 2.

PROPOSITION 1. *Let $n \in \mathbb{Z}$ with $n \geqslant 3$, $\mathfrak{a} \in I(K)$, and put*

$$V_1 = \{z \in K^*: \langle z \rangle \equiv \mathfrak{a} \bmod (n, S) \quad \textit{and} \quad \langle 1-z \rangle \equiv \langle 1, z \rangle \bmod S\}.$$

Then

$$\# V_1 \leqslant 17^{6m+s} n^{2s+\kappa_n(K)}.$$

Proof. For $w \in K^*$, let $V_1(w) = \{z \in V_1: z/w \in K^{*n}\}$. By Lemma 1, V_1 is contained in at most $n^{s+\kappa_n(K)}$ sets of the form $V_1(w)$. Moreover, since $U(n) < 17$ for $n \geqslant 3$, and $s \geqslant \frac{1}{2}m$, we see that Lemma 2 implies that each set $V_1(w)$ has cardinality at most

$$5(2 \,.\, 3^{3+30/n})^m + 2(nU(n))^s \leqslant 17^{6m+s} \,.\, n^s.$$

This proves Proposition 1.

LEMMA 3. *Let $\mathfrak{a}, \mathfrak{b} \in I(K)$, and put*

$$W = \{z \in K^*: \langle z \rangle \equiv \mathfrak{a} \bmod S \quad \textit{and} \quad \langle 1-z \rangle \equiv \mathfrak{b} \bmod S\}.$$

Then

$$\# W \leqslant 3 \,.\, 7^{m+2s}.$$

Proof. Suppose that W is non-empty, and let λ be a fixed element of W. Put $\mu = 1-\lambda$. Then $z \in W$ if and only if $z = \lambda\xi$ and $1-z = \mu\eta$ for some $\xi, \eta \in R_S^*$. Now Lemma 3 follows immediately from Evertse[4] (theorem 1), which states that for fixed $\lambda, \mu \in K^*$, the equation $\lambda\xi + \mu\eta = 1$ has at most $3 \,.\, 7^{m+2s}$ solutions with $\xi, \eta \in R_S^*$.

PROPOSITION 2. *Let $\mathfrak{a}, \mathfrak{b} \in I(K)$, let $\gamma \in K^*$, $\gamma \neq 1$, and let V_2 be the set of pairs*

$$(z_1, z_2) \in K^* \times K^*$$

with the following properties:

$$\langle z_1 \rangle \equiv \mathfrak{a} \bmod (2, S) \quad \textit{and} \quad \langle z_2 \rangle \equiv \mathfrak{b} \bmod (2, S): \tag{2}$$

$$(1-z_1)/(1-z_2) = \gamma; \tag{3}$$

$$\langle 1-z_1 \rangle \equiv \langle 1, z_1 \rangle \bmod S, \quad \langle 1-z_2 \rangle \equiv \langle 1, z_2 \rangle \bmod S \quad \textit{and} \quad \langle z_1 - z_2 \rangle \equiv \langle z_1, z_2 \rangle \bmod S. \tag{4}$$

Then

$$\# V_2 \leqslant 7^{4m+9s} \,.\, 4^{\kappa_2(K)}.$$

Proof. For $w_1, w_2 \in K^*$, let

$$V_2(w_1, w_2) = \{(z_1, z_2) \in V_2: z_1/w_1 \in K^{*2} \quad \text{and} \quad z_2/w_2 \in K^{*2}\}$$

and

$$W_2(w_1, w_2) = \{(\zeta_1, \zeta_2) \in K^* \times K^*: (w_1\zeta_1^2, w_2\zeta_2^2) \in V_2(w_1, w_2)\}.$$

Then

$$\# V_2(w_1, w_2) \leqslant \tfrac{1}{4} \# W_2(w_1, w_2).$$

Furthermore, by Lemma 1, V_2 is contained in at most $4^{s+\kappa_2(K)}$ sets of the type $V_2(w_1, w_2)$. Hence it suffices to prove that

$$\# W_2(w_1, w_2) \leqslant 4^{1-s} \,.\, 7^{4m+9s} \quad \text{for} \quad (w_1, w_2) \in K^* \times K^*. \tag{5}$$

Let $w_1, w_2 \in K^*$, let $L = K(\sqrt{w_1}, \sqrt{w_2})$, and let T be the set of places of L lying above the places in S. We will use the symbol $\langle\ldots\rangle$ to denote a fractional ideal in L. For $(\zeta_1, \zeta_2) \in K^* \times K^*$, we put

$$\Lambda(\zeta_1, \zeta_2) = \frac{1-\sqrt{w_1}\,\zeta_1}{\sqrt{w_2}\,\zeta_2 - \sqrt{w_1}\,\zeta_1}.$$

Then $\Lambda(\zeta_1, \zeta_2) \in L^*$. Further, if $(\zeta_1, \zeta_2) \in W_2(w_1, w_2)$, then (3), (4), and the inclusions

$$\langle 1 \pm \sqrt{w_i}\,\zeta_i\rangle \subset \langle 1, \sqrt{w_i}\,\zeta_i\rangle\ (i = 1, 2) \quad\text{and}\quad \langle\sqrt{w_1}\,\zeta_1 \pm \sqrt{w_2}\,\zeta_2\rangle \subset \langle\sqrt{w_1}\,\zeta_1\, \sqrt{w_2}, \zeta_2\rangle,$$

imply that

$$\langle\Lambda(\zeta_1, \zeta_2)\rangle^2 \equiv \frac{\langle 1, \sqrt{w_1}\,\zeta_1\rangle^2}{\langle\sqrt{w_1}\,\zeta_1, \sqrt{w_2}\,\zeta_2\rangle^2} \equiv \frac{\langle 1, w_1\zeta_1^2\rangle}{\langle w_1\zeta_1^2, w_2\zeta_2^2\rangle}$$
$$\equiv \frac{\langle 1 - w_1\zeta_1^2\rangle}{\langle w_1\zeta_1^2 - w_2\zeta_2^2\rangle} \equiv \langle 1-\gamma^{-1}\rangle^{-1} \bmod T.$$

By a similar argument, we have

$$\langle 1-\Lambda(\zeta_1, \zeta_2)\rangle^2 = \left\langle\frac{1-\sqrt{w_2}\,\zeta_2}{\sqrt{w_1}\,\zeta_1 - \sqrt{w_2}\,\zeta_2}\right\rangle^2 \equiv \langle 1-\gamma\rangle^{-1} \bmod T.$$

Together with Lemma 3 and the fact that $[L\colon K] \leqslant 4$, this implies that

$$\# \{\Lambda \in L^*\colon \Lambda = \Lambda(\zeta_1, \zeta_2) \quad\text{for some}\quad (\zeta_1, \zeta_2) \in W_2(w_1, w_2)\} \leqslant 3\,.\,7^{4(m+2s)}. \tag{6}$$

Let $\Lambda \in L^*$, and suppose that $\Lambda = \Lambda(\zeta_1, \zeta_2)$ for some $(\zeta_1, \zeta_2) \in W_2(w_1, w_2)$. Then (3) and a straightforward computation yields

$$1 + 2(\Lambda-1)\sqrt{w_1}\,\zeta_1 + (\Lambda-1)^2 w_1\zeta_1^2 = \Lambda^2 w_2\zeta_2^2 = (\Lambda^2/\gamma)(w_1\zeta_1^2 + \gamma - 1).$$

Hence for each $\Lambda \in L^*$, there are at most two pairs $(\zeta_1, \zeta_2) \in W_2(w_1, w_2)$ with $\Lambda(\zeta_1, \zeta_2) = \Lambda$. By combining this with (6), we obtain

$$\# W_2(w_1, w_2) \leqslant 6\,.\,7^{4(m+2s)} \leqslant 4^{1-s}\,.\,7^{4m+9s}.$$

This completes the proof of (5) and of Proposition 2.

Lemma 4. *Let $\mathscr{K}$ be a field endowed with a valuation v satisfying $v(\mathscr{K}^*) = \mathbb{Z}$; and let $f(X) = a_d X^d + \ldots + a_0 \in \mathscr{K}[X]$ be a polynomial such that $v(a_i) \geqslant 0$ for all $0 \leqslant i \leqslant d$, $v(\operatorname{disc}(f)) = 0$, and f has d distinct roots $\alpha_1, \ldots, \alpha_d$ in $\mathscr{K}$.*

(*a*) *For all $1 \leqslant i < j \leqslant d$,*

$$v(\alpha_i - \alpha_j) = \min\{0, v(\alpha_i)\} + \min\{0, v(\alpha_j)\}.$$

(*b*) *For all $1 \leqslant i < j \leqslant d$ and all $x \in \mathscr{K}$ with $v(x) \geqslant 0$,*

$$\min\{v(x-\alpha_i), v(x-\alpha_j)\} = v(\alpha_i - \alpha_j).$$

(*c*) *Let $n \geqslant 2$, and suppose that $x \in \mathscr{K}$ satisfies $f(x) \in \mathscr{K}^{*n}$.*

(i) *If $v(x) \geqslant 0$, then for all $1 \leqslant i \leqslant d$,*

$$v(x-\alpha_i) \equiv \min\{0, v(\alpha_i)\} + \min\{0, v(x)\} \pmod n.$$

(ii) *If $v(x) < 0$, then there exists an l, $1 \leqslant l \leqslant d$, such that*

$$v(x-\alpha_l) \equiv \min\{0, v(\alpha_l)\} + \min\{0, v(x)\} - dv(x) \pmod n;$$
$$v(x-\alpha_i) \equiv \min\{0, v(\alpha_i)\} + \min\{0, v(x)\} \pmod n \quad \textit{for all}\quad i \neq l.$$

Proof. For each i, choose $\beta_i, \gamma_i \in \mathscr{K}$ satisfying $\alpha_i = \gamma_i/\beta_i$ and $\min\{v(\beta_i), v(\gamma_i)\} = 0$. Then $v(\beta_i) = -\min\{0, v(\alpha_i)\}$. Let $a = a_d/(\beta_1 \dots \beta_d)$. Then

$$f(X) = a \prod_{1 \leqslant i \leqslant d} (\beta_i X - \gamma_i) \quad \text{and} \quad \operatorname{disc}(f) = a^{2d-2} \prod_{1 \leqslant i < j \leqslant d} (\beta_i \gamma_j - \beta_j \gamma_i)^2.$$

By Gauss' lemma, $v(a) \geqslant 0$. Moreover, since $v(\operatorname{disc}(f)) = 0$, we see that

$$v(\beta_i \gamma_j - \beta_j \gamma_i) = 0 \quad \text{for all} \quad 1 \leqslant i < j \leqslant d; \tag{8}$$

and

$$v(a) = 0. \tag{9}$$

Lemma 4*a* follows immediately from (8). Further, in view of (9), we may henceforth assume that

$$f(X) = \prod (\beta_i X - \gamma_i) \quad \text{with} \quad \min\{v(\beta_i), v(\gamma_i)\} = 0 \quad \text{for all} \quad 1 \leqslant i \leqslant d. \tag{10}$$

Let $x \in \mathscr{K}$, and choose $\xi, \eta \in \mathscr{K}$ such that $x = \xi/\eta$ and $\min\{v(\xi), v(\eta)\} = 0$. Then $v(\eta) = -\min\{0, v(x)\}$. Using (8), a little bit of algebra yields

$$0 \leqslant \min\{v(\beta_i \xi - \gamma_i \eta), v(\beta_j \xi - \gamma_j \eta)\} \leqslant v(\beta_i \gamma_j - \beta_j \gamma_i) \min\{v(\xi), v(\eta)\} = 0;$$

whence

$$\min\{v(\beta_i \xi - \gamma_i \eta), v(\beta_j \xi - \gamma_j \eta)\} = 0 \quad \text{for all} \quad 1 \leqslant i < j \leqslant d. \tag{11}$$

Now Lemma 4*b* follows from (8), (11), and the fact that $v(x) \geqslant 0$ implies $v(\eta) = 0$.

It remains to prove Lemma 4*c*. Let x, ξ, η be as above, and suppose that $f(x) = y^n$ for some $y \in \mathscr{K}^*$ and some $n \geqslant 2$. Then, by (10),

$$y^n \eta^d = \prod (\beta_i \xi - \gamma_i \eta).$$

Combining this with (11) shows that there is an l such that

$$v(\beta_l \xi - \gamma_l \eta) \equiv d v(\eta) \pmod{n};$$

and

$$v(\beta_i \xi - \gamma_i \eta) \equiv 0 \pmod{n} \quad \text{for all} \quad i \neq l.$$

Since

$$v(\beta_i \xi - \gamma_i \eta) = v(x - \alpha_i) - \min\{0, v(x)\} - \min\{0, v(\alpha_i)\} \quad \text{for all} \quad 1 \leqslant i \leqslant d,$$

and since $v(\eta) = -\min\{0, v(x)\}$, we obtain Lemma 4*c*(i) and (ii) by taking $v(x) \geqslant 0$ and $v(x) < 0$ respectively.

Proof of Theorem 1. We use the notation as in the statement of Theorem 1. Factorize $f(X)$ as $f(X) = a(X - \alpha_1)\dots(X - \alpha_d)$ over an algebraic closure $\bar{K}$ of K. Relabelling the α_i's if necessary, we may assume that $\alpha_1, \alpha_2 \in L$ if $n \geqslant 3$, and $\alpha_1, \alpha_2, \alpha_3 \in L$ if $n = 2$. Let T be the set of places of L lying above the places in S. We will denote fractional ideals in L by $\langle \dots \rangle$.

For $i, j \in \{1, 2\}$ if $n \geqslant 3$, and $i, j \in \{1, 2, 3\}$ if $n = 2$, for each $x \in K$ we let

$$Z_{ij}(x) = \frac{x - \alpha_i}{x - \alpha_j}.$$

Then for $x \in V(R_S, f, n)$, the following relations hold:

$$\left.\begin{aligned} \langle Z_{ij}(x)\rangle &\equiv \frac{\langle 1, \alpha_i\rangle}{\langle 1, \alpha_j\rangle} \bmod (n, T) \\ \langle 1 - Z_{ij}(x)\rangle &\equiv \langle 1, Z_{ij}(x)\rangle \bmod T. \end{aligned}\right\} \quad (12)$$

These relations follow from Lemma 4c(i) and 4b respectively, in view of the facts that $f(X) \in R_T[X]$ and disc $(f) \in R_T^*$.

Let $n \geqslant 3$. From (12), Proposition 1, and the fact that $[L: K] = M$, we see that the set

$$\{Z_{12}(x) : x \in V(R_S, f, n)\}$$

has at most $17^{M(6m+s)} . n^{2Ms+\kappa_n(L)}$ elements. Since x is completely determined by $Z_{12}(x)$, this proves (*a*).

Now let $n = 2$. For $x \in V(R_S, f, 2)$, we have

$$\frac{1 - Z_{13}(x)}{1 - Z_{23}(x)} = \frac{\alpha_1 - \alpha_3}{\alpha_2 - \alpha_3} \neq 1;$$

and by (12),

$$\langle Z_{13}(x) - Z_{23}(x)\rangle \equiv \langle Z_{13}(x), Z_{23}(x)\rangle \bmod T.$$

Together with (12), Proposition 2, and the fact that $[L: K] = M$, this shows that the set

$$\{(Z_{13}(x), Z_{23}(x)) : x \in V(R_S, f, 2)\}$$

has cardinality at most $7^{M(4m+9s)} . 4^{\kappa_2(L)}$. Since x is completely determined by the pair $(Z_{13}(x), Z_{23}(x))$, this completes the proof of (*b*).

2. *The equation $y^n = f(x)$ over function fields*

The following notation will be used throughout this section.

k	an algebraically closed field of characteristic 0
K/k	a one-dimensional function field of genus g over k
M_K	a complete set of valuations on K, normalized so that $v(K^*) = \mathbb{Z}$
S	a finite subset of M_K containing $s \geqslant 1$ elements
R_S	the ring of S-integers of K
h_K	the (logarithmic) height on K relative to M_K: for $z \in K$, $z \neq 0$,

$$h_K(z) = \sum_{v \in M_K} \max\{0, v(z)\} = \tfrac{1}{2} \sum_{v \in M_K} |v(z)|.$$

Definition: An element $z \in K^*$ is an (*idelic*) nth-*power modulo* S, denoted

$$z \equiv 0 \mod (n, S),$$

if the ideal zR_S is the nth-power of a (fractional) ideal of R_S. (In terms of divisors, this means that

$$(z) = nD_1 + D_2$$

with Support$(D_2) \subset S$.)

LEMMA 5. (*a*) *The group*

$$\{z \in K^*/K^{*n} : z \equiv 0 \bmod (n, S)\}$$

contains at most n^{2g+s} elements.

(*b*) *The set*

$$\{z \in R_S^*/k^*: h_K(z) \leqslant H\}$$

contains at most 2^{2H+2s} *elements.*

(*c*) *Let* $z \in K$, $z \notin k$. *Then the set*

$$\{\alpha \in k: 1-\alpha z \in R_S^*\}$$

contains at most $s-1$ *elements.*

Proof. (*a*) Let $\mathrm{Pic}^0(K)[n]$ be the group of elements of order n in the divisor class group of K. Then there is an exact sequence

$$0 \to \mathrm{Pic}^0(K)[n] \xrightarrow{i} \{z \in K^*/K^{*n}: z \equiv 0 \bmod (n, S)\} \xrightarrow{j} (\mathbb{Z}/n\mathbb{Z})^s,$$

where i and j are defined by

$$i(\mathrm{class}\{D\}) = z \bmod K^{*n} \quad \text{for } (z) = nD;$$

and

$$j(z \bmod K^{*n}) = (v(z) \bmod n)_{v \in S}.$$

Now $\mathrm{Pic}^0(K)$ is isomorphic to an abelian variety (over k) of dimension g, so

$$\mathrm{Pic}^0(K)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

This and the exact sequence give the desired estimate.

(*b*) Let $z \in R_S^*$ with $h_K(z) \leqslant H$. Write the divisor of z as

$$(z) = \sum_{v \in S} n_v(v).$$

Then $h_K(z) = \frac{1}{2}\Sigma |n_v|$. Since (z) determines the class of z in R_S^*/k^*, it suffices to estimate the size of the set

$$\left\{(n_1, \ldots, n_s) \in \mathbb{Z}^s: \sum_{i=1}^{s} |n_i| \leqslant 2H\right\}.$$

This last set has exactly $\sum_{j=0}^{s} \binom{s}{j} 2^j \binom{2H}{j}$ elements, a quantity which is certainly less then 2^{2H+2s}.

(*c*) Let $v_1, \ldots, v_r \in S$ be the places of S for which z does not have a pole. (Note that $r \leqslant s-1$, since z is not constant.) Then the fact that $1-\alpha z \in R_S^*$ implies that all of the zeros of $1-\alpha z$ are in the set $\{v_1, \ldots, v_r\}$. Since $1-\alpha z$ has at least one zero, we see that $1/z$ takes the value α for at least one of the places $v_1, \ldots, v_r$. Hence the number of such α's is at most r.

PROPOSITION 3. *Let* $n \geqslant 4$, *and define*

$$V(K, n, S) = \{z \in K^*: z \notin k, z \equiv 0 \bmod (n, S), \quad \textit{and} \quad 1-z \equiv 0 \bmod (n, S)\}.$$

(*a*) *Let* $z \in V(K, n, S)$. *Then*

$$h_K(z) \leqslant (2g-2+s)(1-3/n)^{-1}.$$

(*b*) *The set* $V(K, n, S)$ *contains at most* $2^{n^4(2g+s)^2}$ *elements.*

Remark. For number fields, a bound for the height as in (*a*) immediately implies finiteness; but for function fields, this is certainly not the case. Here the finiteness statement in (*b*) lies deeper than the height bound in (*a*).

Proof of Proposition 3. (*a*) This can be proven either by using results of Mason[8] or by adapting the argument of Silverman[15]. We choose the latter course, since we will use similar methods to prove (*b*).

Let K'/K be the extension given by

$$K' = K(z^{1/n}, (1-z)^{1/n}),$$

and let g' be the genus of the function field K'. Since the ideals zR_S and $(1-z)R_S$ are nth-powers, it follows that the only ramification in K'/K occurs over the places of S. Hence the Hurwitz genus formula gives the estimate

$$2g'-2 \leqslant [K':K](2g-2+s). \tag{13}$$

On the other hand, letting $F = k(x,y)$ be the function field of the Fermat curve $x^n+y^n = 1$, we can embed $F \subset K'$ by setting $x = z^{1/n}$ and $y = (1-z)^{1/n}$. Let F' be the image of F in K'. Then another application of the Hurwitz genus formula and the fact that F has genus $\frac{1}{2}(n-1)(n-2)$ yields

$$2g'-2 \geqslant [K':F'](2\,\mathrm{genus}\,(F)-2) = [K':F'](n^2-3n). \tag{14}$$

Next, since $K' = KF'$, we can compute the degree $[K':k(z)]$ in two ways to obtain

$$[K':K][K:k(z)] = [K':F'][F':k(z)].$$

Since $$[K:k(z)] = h_K(z) \quad \text{and} \quad [F':k(z)] = n^2,$$

this yields $$[K':F']/[K':K] = h_K(z)/n^2. \tag{15}$$

Now combining equations (13), (14), and (15) gives the desired result

$$2g-2+s \geqslant ([K':F']/[K':K])(n^2-3n) = h_K(z)(1-3/n).$$

(*b*) For each $z \in V(K,n,S)$, let K_z/K be the field extension (as above)

$$K_z = K(z^{1/n}, (1-z)^{1/n}).$$

We ask first how many such fields K_z there are (up to k-isomorphism). Since

$$z \equiv 0 \bmod (n,S) \quad \text{and} \quad 1-z \equiv 0 \bmod (n,S),$$

the number of such fields is certainly at most the number of fields of the form

$$K(\xi_1^{1/n}, \xi_2^{1/n}) \quad \text{with} \quad \xi_1, \xi_2 \in \{\xi \in K^*: \xi \equiv 0 \bmod (n,S)\}/K^{*n}.$$

Hence, from Lemma 5(*a*), there are at most $(n^{2g+s})^2$ fields K_z as z ranges over $V(K,n,S)$. We now fix one such field K', and attempt to estimate the size of the set

$$V(K,n,S,K') = \{z \in V(K,n,S): K_z \cong K'\}.$$

We recall from the proof of (*a*) (equation (13)) that the genus g' of K' is bounded by

$$2g'-2 \leqslant [K':K](2g-2+s) \leqslant n^2(2g-2+s). \tag{16}$$

As above, let $F = k(x,y)$ be the function field of the Fermat curve $x^n+y^n = 1$. Then each element $z \in V(K,n,S,K')$ gives a distinct embedding $F \subset K'$ by setting $x = z^{1/n}$ and $y = (1-z)^{1/n}$. (Actually, there are n^2 embeddings corresponding to different choices of the nth roots; but we will just choose one such embedding.) We thus have an injection

$$V(K,n,S,K') \to \mathrm{Map}\,(F,K'). \tag{17}$$

We now use Kani's quantitative version of the De Franchis theorem ([6], theorem 1), which in our case gives the bound

$$\# \operatorname{Map}(F, K') \leqslant 2^{2g'^2-1}(2^{2g'^2-1}-1) < 2^{4g'^2-2}. \tag{18}$$

Now (16), (17), (18), and a little bit of algebra gives the estimate

$$\# V(K, n, S, K') \leqslant 2^{n^4(2g+s-1)^2}.$$

Since $V(K, n, S)$ is the union of $V(K, n, S, K')$ as K' ranges over at most n^{4g+2s} fields this completes the proof of (b).

We are now ready to state our main theorem, for which we need the following definition.

Definition. Let $f(X) \in K[X]$ be a polynomial of degree d. We say that f is *degenerate* if there are elements $A, B, C, D, E \in K$ with $AD - BC \in K^*$ and $E \in K^*$, and a polynomial $\phi(X) \in k[X]$, such that

$$f(X) = E(CX+D)^d \phi((AX+B)/(CX+D)).$$

(Thus f is degenerate if it arises by a fractional linear change of variables from a polynomial with constant coefficients.)

THEOREM 2. *Let $f(X) \in R_S[X]$ be a non-degenerate monic polynomial of degree $d \geqslant 3$ with* disc $(f) \in R_S^*$. *Then the set*

$$\{x \in K : f(x) \in K^{*n} \text{ for some } n \geqslant 4\}$$

contains at most $2^{2d^{18}(2g+s)^6}$ elements.

Proof. Factorize $f(X)$ (over a fixed algebraic closure $\bar{K}$ of K) as

$$f(X) = (X-\alpha_1) \dots (X-\alpha_d).$$

For each $1 \leqslant i, j \leqslant d$, let $K_{ij} = K(\alpha_1, \alpha_i, \alpha_j)$, let g_{ij} be the genus of K_{ij}, let S_{ij} be the set of places of K_{ij} lying above S, and let $s_{ij} = \# S_{ij}$. Since

$$f(X) \in R_S[X] \quad \text{and} \quad \operatorname{disc}(f) \in R_S^*,$$

the extension K_{ij}/K is ramified only over S; so by the Hurwitz genus formula we have

$$2g_{ij} - 2 + s_{ij} = [K_{ij}:K](2g-2+s) \leqslant d^3(2g-2+s). \tag{19}$$

(Note that $[K_{ij}:K] < d^3$.)

For each $1 \leqslant i, j \leqslant d$, $i \neq j$, and each x in the set

$$V(f) = \{x \in K^* : x \neq \alpha_1 \quad \text{and} \quad f(x) \in K^{*n} \text{ for some } n \geqslant 4\},$$

define $z_{ij} = z_{ij}(x) \in K$ by

$$z_{ij} = \frac{\alpha_1 - \alpha_j}{\alpha_i - \alpha_j} \frac{x - \alpha_i}{x - \alpha_1}.$$

Note that we have Siegel's identity

$$z_{ij} + z_{ji} = 1. \tag{20}$$

Let $x \in V(f)$. Since $f(X) \in R_{S_{ij}}[X]$, disc $(f) \in R_{S_{ij}}^*$, f is monic, and $f(x) \in (K_{ij}^*)^n$, we can make two deductions. First, $v(\alpha_i) \geqslant 0$ for all $1 \leqslant i \leqslant d$ and all valuations $v \notin S_{ij}$.

Second, if $v(x) < 0$ and $v \notin S_{ij}$, then $dv(x) \equiv 0 \pmod{n}$. Now, applying Lemma 4(*a*) and 4(*c*)(i) and (ii), we see that

$$z_{ij} \equiv 0 \bmod (n, S_{ij}).$$

Hence, using (19) and Proposition 3(*a*), we have

$$\begin{aligned} h_{K_{ij}}(z_{ij}) &\leqslant (2g_{ij} - 2 + s_{ij})(1 - 3/n)^{-1} \\ &\leqslant d^3(2g - 2 + s)(1 - 3/n)^{-1}. \end{aligned} \tag{21}$$

We break $V(f)$ into three pieces, and analyse each one separately:

$$V_1(f) = \{x \in V(f) : z_{ij} \notin R^*_{S_{ij}} \quad \text{for some} \quad i \neq j\}$$

$$V_2(f) = \{x \in V(f) : z_{ij} \in R^*_{S_{ij}} \quad \text{for all} \quad i \neq j, \quad \text{and} \quad z_{ij} \notin k \quad \text{for some} \quad i \neq j\}$$

$$V_3(f) = \{x \in V(f) : z_{ij} \in k \quad \text{for all} \quad i \neq j\}.$$

Let $x \in V_1(f)$, and choose $i \neq j$ such that $z_{ij} \notin R^*_{S_{ij}}$. Since $z_{ij} \equiv 0 \bmod (n, S_{ij})$, this implies that $h_{K_{ij}}(z_{ij}) \geqslant n$. Hence from (21), we obtain the bound

$$n \leqslant d^3(2g - 2 + s) + 3 < d^3(2g + s).$$

Further, for any particular $n \geqslant 4$, Proposition 3(*b*) says that the set

$$\{z \in K^*_{ij} : z \notin k,\ z \equiv 0 \bmod (n, S_{ij}), \quad \text{and} \quad 1 - z \equiv 0 \bmod (n, S_{ij})\}$$

contains at most

$$2^{n^4(2g_{ij}+s_{ij})^2} \leqslant 2^{n^4 d^6 (2g+s)^2}$$

elements. Summing over n and noting that there are $d(d-1)$ choices for (i,j) gives the estimate

$$\# V_1(f) \leqslant d(d-1) \sum_{n=4}^{d^3(2g+s)-1} 2^{n^4 d^6 (2g+s)^2} < 2^{d^{18}(2g+s)^6}. \tag{22}$$

Now let $x \in V_2(f)$, and let i, j be such that $z_{ij} \notin k$. Since $z_{ij} \equiv 0 \bmod (n, S_{ij})$ for every n, we can let $n \to \infty$ in (21) to obtain the bound

$$h_{K_{ij}}(z_{ij}) \leqslant d^3(2g - 2 + s).$$

Moreover, since $[K_{ij} : K] \leqslant d^3$, we have $s_{ij} \leqslant d^3 s$. Hence, applying Lemma 5(*b*, *c*) and noting that there are $d(d-1)$ choices for (i,j), we see that

$$\# V_2(f) \leqslant d(d-1)(d^3 s - 1)\, 2^{2d^3(2g-2+s)+2d^3 s} < 2^{5d^3(2g+s)}. \tag{23}$$

Finally, suppose that $\# V_3(f) \geqslant 3$. We will show that f is degenerate. Let $x_0 \in V_3(f)$, and let $l(X)$ be the linear polynomial defined by

$$l(X) = \sum_{1 \leqslant i \leqslant d} \frac{X - \alpha_i}{x_0 - \alpha_i}.$$

Then $l(X)$ has coefficients in K, and since $l(x_0) = d \neq 0$, l is not identically zero. (Note that since $f(x_0) \in K^{*n}$, we have $x_0 \neq \alpha_i$ for all $1 \leqslant i \leqslant d$.) By assumption, $\# V_3(f) \geqslant 3$; so the fact that $l(X)$ has only one root implies that there is an $x_1 \in V_3(f)$ such that $x_1 \neq x_0$ and $l(x_1) \neq 0$. Now combining the facts that $l(x_1) \in K^*$ and

$$\frac{x_1 - \alpha_i}{x_0 - \alpha_i} \Big/ \frac{x_1 - \alpha_j}{x_0 - \alpha_j} = \frac{z_{ij}(x_1)}{z_{ij}(x_0)} \in k \quad \text{for all} \quad 1 \leqslant i < j \leqslant d,$$

we see that

$$\frac{x_1 - \alpha_i}{x_0 - \alpha_i} \in K,$$

whence

$$\alpha_i \in K \quad \text{for all} \quad 1 \leqslant i \leqslant d. \tag{24}$$

Choose some $j > 1$, and define

$$A = \frac{x_0 - \alpha_1}{\alpha_1 - \alpha_j}, \quad B = (x_0 - \alpha_j) \prod_{\substack{i=1 \\ i \neq j}}^{d} (\alpha_j - \alpha_i).$$

Then using $f(X) = \prod (X - \alpha_i)$, a little bit of algebra yields

$$(AX+1)^d f\left(\frac{\alpha_j AX + x_0}{AX+1}\right) = A^{d-1} B \prod_{\substack{i=1 \\ i \neq j}}^{d} (X - z_{ij}).$$

Since by assumption each $z_{ij} \in k$, and since by (24), $\alpha_j, A, B \in K$, this proves that if $\# V_3(f) \geqslant 3$, then f is degenerate. But by assumption f is non-degenerate, so

$$\# V_3(f) \leqslant 2. \tag{25}$$

Now combining (22), (23), and (25) gives the desired estimate,

$$\begin{aligned} \# V(f) &\leqslant \# V_1(f) + \# V_2(f) + \# V_3(f) \\ &\leqslant 2^{d^{18}(2g+s)^6} + 2^{5d^3(2g+s)} + 2 \\ &< 2^{2d^{18}(2g+s)^6}. \end{aligned}$$

REFERENCES

[1] A. BAKER. *Transcendental Number Theory* (Cambridge University Press, 1975).

[2] B. BRINDZA. On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hung.* **44** (1984), 133–139.

[3] J.-H. EVERTSE. *Upper Bounds for the Number of Solutions of Diophantine Equations*. MC-tract 168, Centre of Math. and Comp. Sci. (Amsterdam, 1983).

[4] J.-H. EVERTSE. On equations in S-units and the Thue–Mahler equation. *Invent. Math.* **75** (1984), 561–584.

[5] G. FALTINGS. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), 349–366.

[6] E. KANI. Bounds on the number of non-rational subfields of a function field. Pre-print.

[7] W. J. LEVEQUE. On the equation $y^n = f(x)$. *Acta Arith.* **9** (1964), 209–219.

[8] R. C. MASON. *Diophantine Equations over Function Fields*. London Math. Soc. Lecture Note Series, vol. 96 (Cambridge University Press, 1984).

[9] A. SCHINZEL and R. TIJDEMAN. On the equation $y^m = P(x)$. *Acta Arith.* **31** (1976), 199–204.

[10] W. SCHMIDT. Thue's equation over function fields. *J. Austral. Math. Soc.* (A) **25** (1978), 385–422.

[11] T. N. SHOREY, A. J. VAN DER POORTEN, R. TIJDEMAN and A. SCHINZEL. Applications of the Gel'fond-Baker method to Diophantine equations. In *Transcendence Theory, Advances and Applications*, proc. conf. Cambridge 1976 (ed. A. Baker and D. W. Masser), pp. 59–77.

[12] C. L. SIEGEL (under the pseudonym X). The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + h$, *Gesammelte Abhandlungen*, vol. I (Springer-Verlag, 1966), 207–208.

[13] C. L. SIEGEL. Über einige Anwendungen diophantischer Approximationen (1929), *Gesammelte Abhandlungen*, vol. I (Springer-Verlag, 1966), 209–266.

[14] J. H. SILVERMAN. The Catalan equation over function fields. *Trans. Amer. Math. Soc.* **273** (1982), 201–205.

[15] J. H. SILVERMAN. The S-unit equation over function fields. *Math. Proc. Cambridge Philos. Soc.* **95** (1984), 3–4.

[16] V. G. SPRINDZUK. On the number of solutions of the Diophantine equation $x^3 = y^2 + A$ (in Russian). *Dokl. Akad. Nauk. BSSR* **7** (1963), 9–11.

[17] L. A. TRELINA. On S-integral solutions of the hyperelliptic equation (in Russian). *Dokl. Akad. Nauk. BSSR* (1978), 881–884.