Proceedings of the Edinburgh Mathematical Society (1999) **42**, 127–141 ©

BOUNDS FOR THE SIZE OF INTEGRAL SOLUTIONS TO $Y^m = f(X)$

by DIMITRIOS POULAKIS

(Received 20th February 1997)

Let K be an algebraic number field with ring of integers O_K and $f(X) \in O_K[X]$. In this paper we establish improved explicit upper bounds for the size of solutions in O_K, of diophantine equations $Y^2 = f(X)$, where $f(X)$ has at least three roots of odd order, and $Y^m = f(X)$, where m is an integer ≥ 3 and $f(X)$ has at least two roots of order prime to m.

1991 *Mathematics subject classification:* 11D41.

1. Introduction

Let K be an algebraic number field with ring of integers O_K, $f(X)$ a polynomial in $O_K[X]$ and m an integer ≥ 2. Consider the diophantine equation

$$Y^m = f(X) \qquad (*)$$

and assume that if $m \geq 3$, $f(X)$ has at least two roots of order prime to m and if $m = 2$, $f(X)$ has at least three roots of odd order. When $K = \mathbb{Q}$, Baker [**1**] obtained the first explicit upper bound for the size of integral solutions to the equation (*). This result has been extended to an arbitrary algebraic number field and has been improved by several authors. The best known results have been obtained by Voutier [**10**]. Moreover, a generalization of the equation (*) has been studied in [**5**].

Throughout this paper we denote by d, D_K and N_K the degree of K, the discriminant of K and the norm from K to $\mathbb{Q}$. Further, we denote by $\overline{K}$ an algebraic closure of K. By an *absolute value* we will always understand an absolute value that it extends either the standard absolute value of $\mathbb{Q}$ or a p-adic absolute value $|\,|_p$ of $\mathbb{Q}$. Let $M(K)$ be a set of symbols v such that with every $v \in M(K)$ an absolute value $|\,|_v$ is associated. We denote by d_v the local degree of $|\,|_v$. We define the *field height* of a point $\mathbf{x} = (x_0, \ldots, x_n)$ in the projective n-space $\mathbb{P}^n(K)$ by

$$H_K(\mathbf{x}) = \prod_{v \in M(K)} \max\{|x_0|_v, \ldots, |x_n|_v\}^{d_v},$$

and the *absolute height* by $H(\mathbf{x}) = H_K(\mathbf{x})^{1/d}$. For $x \in K$ we define $H_K(x) = H_K((1:x))$

and $H(x) = H((1:x))$. Let G be a polynomial in one or several variables and with coefficients in K. We define the *field height* $H_K(G)$ and the *absolute height* $H(G)$ of G, respectively, to be the field height and the absolute height of a point in a projective space having as coordinates the coefficients of G (in any order). For an account of the properties of heights see [**9**, Chapter VIII] and [**3**, Chapter 3]. Finally, for $z \in \mathbb{R}$, $z > 0$, we let $\log^* z = \max\{1, \log z\}$.

In [**6**] we have obtained the following improved upper bound on the size of integral solutions to the elliptic equation:

Theorem A. *Suppose $f(X) = X^3 + aX^2 + bX + c$ has coefficients in O_K and discriminant $\Delta(f) \neq 0$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^2 = f(X)$ satisfy*

$$\max\{H_K(x), H_K(y)\} < \exp\{\Omega(d)|D_K|^{25}|N_K(\Delta(f))|^{27} \log^* H_K(f)\},$$

where

$$\Omega(d) < 10^{740d+48} d^{312d+13}.$$

In this paper we generalize the above result and we obtain explicit upper bounds of the above type for the height of integral solutions to the equation $(*)$ over K, improving on the estimates obtained by Voutier.

Let $(x, y) \in O_K^2$ be a solution of $y^m = f(x)$. Since we have

$$H_K(y) \leq H_K(y)^m = H_K(y^m) \leq (\deg f + 1)^d H_K(f) H_K(x)^{\deg f},$$

it is sufficient to calculate an upper bound for $H_K(x)$. We obtain the following explicit estimates:

Theorem 1. *Let $f(X) = (X - \alpha_1)^{e_1} \dots (X - \alpha_r)^{e_r}$ be a polynomial of degree ≥ 3 in $O_K[X]$, where $\alpha_1, \dots, \alpha_r$ are pairwise distinct elements in $\overline{K}$. Assume that $\alpha_1, \alpha_2, \alpha_3 \in K$ and e_1, e_2, e_3 are odd. Put $g(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ and denote by $\Delta(g)$ the discriminant of $g(X)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^2 = f(X)$ satisfy*

$$H_K(x) < \exp\{\Phi_1(d)|D_K|^{50}|N_K(\Delta(g))|^{180} \log^* H_K(g)\},$$

where

$$\Phi_1(d) < 10^{1700d+53} d^{624d+13}.$$

Corollary 1. *Let $f(X) = a_0(X - \alpha_1)^{e_1} \dots (X - \alpha_r)^{e_r}$ be a polynomial of degree $n \geq 3$ in $O_K[X]$, where $\alpha_1, \dots, \alpha_r$ are pairwise distinct elements in $\overline{K}$ and e_1, e_2, e_3 are odd. Put $G(X) = a_0(X - \alpha_1) \dots (X - \alpha_r)$ and denote by $\Delta(G)$ the discriminant of $G(X)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^2 = f(X)$ satisfy*

$$H_K(x) < \exp\{\Phi_2(d, r)(|D_K|^{10}|N_K(\Delta(G))|^{36}|N_K(a_0)|^{36rn})^{10r^3} \log^*(H_K(a_0)H_K(G))\},$$

where

$$\Phi_2(d, r) < (10^{16}(dr^3)^5)^{250dr^3}.$$

Theorem 2. *Let p be a prime ≥ 3 and $f(X) = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$ a polynomial of degree ≥ 2 in $O_K[X]$, where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in $\overline{K}$ with $a_1, a_2 \in K$ and $(e_i, p) = 1$ $(i = 1, 2)$. Assume that K contains a primitive pth root of 1. Put $g(X) = (X - \alpha_1)(X - \alpha_2)$ and denote by $\Delta(g)$ the discriminant of $g(X)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^p = f(X)$ satisfy*

$$H_K(x) < \exp\{\Psi_1(d, p)|D_K|^{50p^2}|N_K(\Delta(g))|^{510p^2} \log^* H_K(g)\},$$

where

$$\Psi_1(d, p) < 10^{1700dp^2+53} d^{624dp^2+13} p^{1438dp^3+9}.$$

Corollary 2. *Let p be a prime ≥ 3 and $f(X) = a_0(X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$ a polynomial of degree $n \geq 2$ in $O_K[X]$, where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in $\overline{K}$ with $(e_i, p) = 1$ $(i = 1, 2)$. Put $G(X) = a_0(X - \alpha_1) \ldots (X - \alpha_r)$ and denote by $\Delta(G)$ the discriminant of $G(X)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^p = f(X)$ satisfy*

$$H_K(x) < \exp\{\Psi_2(d, r, p)(|D_K|^5|N_K(\Delta(G))|^{51}|N_K(a_0)|^{51nr})^{10r^2p^4} \log^*(H_K(a_0)H_K(G))\},$$

where

$$\Psi_2(d, r, p) < (10^3(dr^2)p^{3p})^{625dr^2p^4}.$$

Theorem 3. *Let $f(X) = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$ be a polynomial of degree ≥ 2 in $O_K[X]$, where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in $\overline{K}$ with $\alpha_1, \alpha_2 \in K$ and e_1, e_2 are odd. Assume that K contains a primitive 4th-root of 1. Denote by $\Delta(g)$ the discriminant of the polynomial $g(X) = (X - \alpha_1)(X - \alpha_2)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^4 = f(X)$ satisfy*

$$H_K(x) < \exp\{\Omega_1(d)|D_K|^{800}|N_K(\Delta(g))|^{4620} \log^* H_K(g)\},$$

where

$$\Omega_1(d) < 10^{50597d+73} d^{9984d+13}.$$

Corollary 3. *Let $f(X) = a_0(X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$ be a polynomial of degree $n \geq 2$ in $O_K^2[X]$, where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in $\overline{K}$ and e_1, e_2 are odd. Put $G(X) = a_0(X - \alpha_1) \ldots (X - \alpha_r)$ and denote by $\Delta(G)$ the discriminant of $G(X)$. Then, all solutions $(x, y) \in O_K^2$ to the equation $Y^4 = f(X)$ satisfy*

$$H_K(x) < \exp\{\Omega_2(d, r)(|D_K|^{64}|N_K(\Delta(G))|^{370}|N_K(a_0)|^{370nr})^{100r^2} \log^*(H_K(a)H_K(G))\},$$

where

$$\Omega_2(d, r) < ((10^{49}(dr^2)^8)^{10^4dr^2}).$$

Assume that m is an integer ≥ 4 and $f(X)$ a polynomial in $O_K[X]$ having at least two roots of order prime to m. Let $x, y \in O_K$ with $y^m = f(x)$. If m has a prime divisor $p \geq 3$, then $(x, y^{m/p})$ is an integral solution to the equation $Y^p = f(X)$. Hence Theorem 2 (or Corollary 2) implies an upper bound for $H_K(x)$. Similarly, if $m = 2^t, t \geq 2$, Theorem 3 (or Corollary 3) gives an upper bound for $H_K(x)$. Therefore, in all cases, Theorems 1, 2 and 3 (or Corollaries 1, 2 and 3) give a bound for the integral solutions to the equation $(*)$.

Following Kubert and Lang [**2**, §1], we reduce the proofs of Theorems 1, 2 and 3, to our Theorem A. This reduction relies on the following result:

Proposition 1. *Let $m = p^t$, where p is a prime and t is an integer ≥ 1. Let $f(X) = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$ be a polynomial in $O_K[X]$, where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in $\overline{K}$. Assume that K contains a primitive mth root of $1, \alpha_1, \ldots \alpha_s \in K$ $(s \leq r)$ and $(e_i, m) = 1$ $(i = 1, \ldots, s)$. Put $g(X) = (X - \alpha_1) \ldots (X - \alpha_r)$ and denote by $\Delta(g)$ the discriminant of $g(X)$. Let $x, y \in O_K$ with $y^m = f(x)$. Then the algebraic number field $L = K(w)$, where $w^m = (x - \alpha_1) \ldots (x - \alpha_s)$, has discriminant D_L satisfying*

$$|D_L| < p^{(2p-1)dtp^{t-1}} |D_K|^{pt} |N_K(\Delta(g))|^{(2p-1)tp^{t-1}}.$$

2. Auxiliary lemmas

For the proof of Proposition 1 and Theorems 1, 2 and 3 we shall need the following lemmas:

Lemma 1. *Let K be a field of characteristic p and m an integer ≥ 2 not divisible by p. Denote by C the algebraic curve defined by the equation*

$$Y^m = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r},$$

where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in an algebraic closure $\overline{K}$ of K and $(e_1, m) = 1$. Let V be a discrete valuation ring of $\overline{K}(C)$ above $X = \alpha_1$. Then, the function $t_V = (X - \alpha_1)^c Y^d$, where $c, d \in \mathbb{Z}$ with $mc + e_1 d = 1$, is a local parameter at V.

Proof. For $h \in \overline{K}(C)$ we denote by $\mathrm{ord}_V(h)$ the order of h at V. The equation

$$Y^m = (X - \alpha_1)^{e_1} \ldots (X - \alpha_r)^{e_r}$$

yields

$$m \, \mathrm{ord}_V(Y) = e_1 \, \mathrm{ord}_V(X - \alpha_1).$$

Since $(e_1, m) = 1$, we get

$$\mathrm{ord}_V(X - \alpha_1) = m \quad \text{and} \quad \mathrm{ord}_V(Y) = e_1.$$

Let $c, d \in \mathbb{Z}$ such that $mc + e_1 d = 1$. Then the function $t_V = (X - \alpha_1)^c Y^d$ has

$$\operatorname{ord}_V(t_V) = mc + e_1 d = 1.$$

Therefore t_V is a local parameter at V.

Lemma 2. *Let K be an algebraic number field with ring of integers O_K. Let L be a cyclic extension of K of degree ℓ, where ℓ is a prime, and T a finite set of prime ideals in O_K such that the extension L/K is unramified outside T. Then the discriminant D_L of L satisfies*

$$|D_L| < |D_K|^\ell \left| N_K \left(\prod_{P \in T} P \right) \right|^{2\ell - 1}.$$

Proof. Let $\mathcal{D}_{L/K}$ be the different of L over K. Then

$$\mathcal{D}_{L/K} = \mathcal{P}_1^{r_1} \dots \mathcal{P}_k^{r_k},$$

where $\mathcal{P}_1, \dots, \mathcal{P}_k$ are prime ideals in L such that $\mathcal{P}_j \cap O_K \in T$ $(j = 1, \dots, k)$. Let $\hat{L}_j$ and $\hat{K}_j$ be the completions of L and K with respect to the prime ideals $\mathcal{P}_j$ and $P_j = \mathcal{P}_j \cap O_K$ $(j = 1, \dots, k)$. Denote by $\mathcal{D}_{\hat{L}_j/\hat{K}_j}$ the different of $\hat{L}_j$ over $\hat{K}_j$ and by $\hat{\mathcal{P}}_j$ the prime ideal generated by $\mathcal{P}_j$ in the ring of $\mathcal{P}_j$-adic integers in $\hat{L}_j$. By [**8**, Proposition 10, page 61] we have $\mathcal{D}_{\hat{L}_j/\hat{K}_j} = \hat{\mathcal{P}}_j^{r_j}$. By [**8**, Corollary 4, page 41] $\hat{L}_j$ is a finite Galois extension of $\hat{K}_j$ and its Galois group is the group of decomposition of $\mathcal{P}_j$. Then [**8**, Lemma 3, page 91, and Exercise 3.c, page 79] give

$$r_j \leq 2\ell - 1 \quad (j = 1, \dots, k).$$

Denote by $N_{L/K}$ and $D_{L/K}$ respectively the norm and the discriminant ideal of L over K. The prime ideals P_i $(i = 1, \dots, k)$ are the only prime ideals in O_K that are ramified in L. Since ℓ is a prime number, it follows that the ramification index of P_i is ℓ. Then $N_{L/K}(\mathcal{P}_i) = P_i$ $(i = 1, \dots, k)$. Further, we have $N_{L/K}(\mathcal{D}_{L/K}) = D_{L/K}$. Thus

$$|N_K(D_{L/K})| \leq |N_K(P_1 \dots P_k)|^{2\ell - 1} \leq \left| N_K \left(\prod_{P \in T} P \right) \right|^{2\ell - 1}.$$

Therefore

$$|D_L| = |D_K|^\ell |N_K(D_{L/K})| \leq |D_K|^\ell \left| N_K \left(\prod_{P \in T} P \right) \right|^{2\ell - 1}.$$

Lemma 3. *Let K be an algebraic number field with ring of integers O_K. Let $g(X) = (X - \alpha_1) \dots (X - \alpha_r)$ be a polynomial in $O_K[X]$, where $\alpha_1, \dots, \alpha_r$ are pairwise*

https://doi.org/10.1017/S001309150002006X Published online by Cambridge University Press

distinct elements in $\overline{K}$. Set $K_i = K(\alpha_1, \ldots, \alpha_i)$ and denote by D_{K_i} the discriminant of K_i $(i = 1, \ldots, r)$. Then

$$|D_{K_i}| \leq |D_K|^{r(r-1)\ldots(r-i+1)} |N_K(\Delta(g))|^{ir^{i-1}},$$

where $\Delta(g)$ is the discriminant of $g(X)$.

Proof. Set $K_0 = K$ and denote by $D_{K_i/K_{i-1}}$ the discriminant ideal of the extension K_i/K_{i-1} $(i = 1, \ldots, r)$. By [**8**, Proposition 8, page 60] we get

$$|D_{K_1}| \leq |D_K|^r N_K(D_{K_1/K})|.$$

Let $G(X)$ be the irreducible polynomial of α_1 over K and $\deg G = \zeta$. Since α_1 is an algebraic integer, the discriminant $D_{K_1/K}$ divides the discriminant of elements $1, \alpha_1, \ldots, \alpha_1^{\zeta-1}$, which is equal to the discriminant $\Delta(G)$ of $G(X)$. The element α_1 is a root of $g(X)$. Thus $G(X)$ divides $g(X)$ and we deduce that $\Delta(G)$ divides $\Delta(g)$. It follows that $D_{K_1/K}$ divides $\Delta(g)$. Then

$$|D_{K_1}| \leq |D_K|^r |N_K(\Delta(g))|.$$

Assume that Lemma holds for $i - 1 \geq 1$. Thus

$$|D_{K_{i-1}}| \leq |D_K|^{r(r-1)\ldots(r-i+2)} |N_K(\Delta(g))|^{(i-1)r^{i-2}}.$$

By the reasoning above, we get

$$|D_{K_i}| \leq |D_{K_{i-1}}|^{(r-i+1)} |N_K(\Delta(g))|^{r(r-1)\ldots(r-i+2)}.$$

Applying the inductive hypothesis, we obtain

$$|D_{K_i}| \leq |D_K|^{r(r-1)\ldots(r-i+1)} |N_K(\Delta(g))|^{ir^{i-1}}.$$

Lemma 4. *Let f and g be two polynomials in one variable with coefficients in $\overline{K}$ and* $\deg f + \deg g < M$. *Then*

$$(1/4^M) H(fg) \leq H(f) H(g) \leq 4^M H(fg).$$

Proof. See [**3**, Proposition 2.4, page 57].

Lemma 5. *Let $G(X) = (X - \alpha_1) \ldots (X - \alpha_r)$ be a polynomial in $K[X]$ and $a \in K$. Then, the height of the polynomial $E_s(X) = (X - a\alpha_1) \ldots (X - a\alpha_s)$, $s \leq r$, satisfies*

$$H(E_s) < 2^{s-1}(s+1) 4^{r+1} H(a)^s H(G).$$

Proof. Set $G_s(X) = (X - \alpha_1)\dots(X - \alpha_s)$. By [9, Lemma 5.9, page 211] and [7, Lemma 3] we obtain

$$H(E_s) \le 2^{s-1} H(a)^s H(\alpha_1)\dots H(\alpha_s) \le 2^{s-1}(s+1)H(a)^s H(G_s).$$

On the other hand, Lemma 4 gives

$$H(G_s) \le 4^{r+1} H(G).$$

Hence

$$H(E_s) \le 2^{s-1}(s+1)4^{r+1} H(a)^s H(G).$$

3. Proof of Proposition 1

Denote by S the set of prime ideals in O_K dividing p or $\Delta(g)$. Let $(x, y) \in O_K^2$ such that $y^m = f(x)$ with $x \neq \alpha_i$ $(i = 1, \dots, s)$. Put $L = K(w)$, where w is an algebraic integer satisfying $w^m = (x - \alpha_1)\dots(x - \alpha_s)$. Let $\mathcal{P}$ be a prime ideal in O_K such that $\mathcal{P} \notin S$ and let $O_{K,\mathcal{P}}$ be the local ring of O_K at $\mathcal{P}$. Denote by $\bar{x}, \bar{y}, \bar{\alpha}_1, \dots, \bar{\alpha}_r$ respectively the reductions of $x, y, \alpha_1, \dots, \alpha_r \bmod \mathcal{P}$. Set $k = O_K/\mathcal{P}$ and denote by $\bar{k}$ an algebraic closure of k.

Let $\bar{C}$ be the curve over k defined by the equation

$$Y^m = (X - \bar{\alpha}_1)^{e_1}\dots(X - \bar{\alpha}_r)^{e_r}.$$

Since $\mathcal{P}$ does not divide $\Delta(g)$, the elements $\bar{\alpha}_1, \dots, \bar{\alpha}_r$ are pairwise distinct in $\bar{k}$. Put $[L:K] = \mu$. We have two cases:

First case $\bar{x} \neq \bar{\alpha}_i$ $(i = 1, \dots, s)$. Since w is an algebraic integer, the discriminant D_L of L divides the discriminant $D(1, w, \dots, w^{\mu-1})$ of the elements $1, w, \dots, w^{\mu-1}$. Further, $D(1, w, \dots, w^{\mu-1})$ divides the discriminant $\Delta(R)$ of the polynomial

$$R(T) = T^m - (x - \alpha_1)\dots(x - \alpha_s).$$

Then D_L divides $\Delta(R)$. We have

$$\Delta(R) = (-1)^{m-1} m^m [(x - \alpha_1)\dots(x - \alpha_s)]^{m-1}.$$

Since $\bar{x} \neq \bar{\alpha}_i$ $(i = 1, \dots, s)$, we deduce that $\Delta(R) \not\equiv 0 \bmod \mathcal{P}$. Thus $\mathcal{P}$ does not divide D_L. Therefore $\mathcal{P}$ is unramified in L.

Second case $\bar{x} = \bar{\alpha}_i$ $(1 \le i \le s)$. Let V be a discrete valuation ring of the function field $\bar{k}(\bar{C})$, above the local ring of $\bar{C}$ at $(\bar{x}, \bar{y})$. By Lemma 1, the function $t_V = (X - \bar{\alpha}_i)^c Y^d$, where $c, d \in \mathbb{Z}$ with $mc + e_i d = 1$, is a local parameter at V. Then the function

$$\tau = (X - \bar{\alpha}_1)\dots(X - \bar{\alpha}_s)/t_V^m$$

https://doi.org/10.1017/S001309150002006X Published online by Cambridge University Press

is a unit in V. Thus $\tau(\bar{x}, \bar{y}) \neq 0, \infty$. Consider the element

$$z = (x - \alpha_1)\dots(x - \alpha_s)/((x - \alpha_i)^c y^d)^m.$$

Since $x \neq \alpha_i$ $(i = 1, \dots, s)$, we deduce that $z \neq 0$. Further, we have $z \equiv \tau(\bar{x}, \bar{y}) \neq 0, \infty \bmod \mathcal{P}$. If z is not a unit in $O_{K,\mathcal{P}}$, then $z = 0$ or $\infty \bmod \mathcal{P}$ which is a contradiction. Thus z is a unit in $O_{K,\mathcal{P}}$. Put $\omega = w/(x - \alpha_i)^c y^d$. Since $\omega^m = z$, we deduce that ω is a unit in L. Then the discriminant $\mathbb{D}$ of the integral closure of $O_{K,\mathcal{P}}$ in L divides the discriminant $D(1, \omega, \dots, \omega^{\mu-1})$ of the elements $1, \omega, \dots, \omega^{\mu-1}$ in $O_{K,\mathcal{P}}$. Since ω is a root of the polynomial $Q(T) = T^m - z$, $D(1, \omega, \dots, \omega^{\mu-1})$ divides the discriminant

$$\Delta(Q) = (-1)^{m-1} m^m z^{m-1}$$

of $Q(T)$. It follows that $\mathbb{D}$ divides $\Delta(Q)$ in $O_{K,\mathcal{P}}$. The element z is a unit in $O_{K,\mathcal{P}}$ and $\mathcal{P}$ does not divide m. Thus $\Delta(Q)$ is a unit in $O_{K,\mathcal{P}}$. It follows that $\mathbb{D}$ is also a unit in $O_{K,\mathcal{P}}$. So we deduce that $\mathcal{P}$ is unramified in L. Therefore, the ideals of O_K which do not lie above the elements of S are unramified in L.

Put $K_i = K(w^{p^{t-i}})$ $(i = 0, \dots, t)$. Then $K_0 = K$ and $K_t = L$. Denote by S_i the set of prime ideals of K_i $(i = 1, \dots, t)$ lying above the elements of S and by D_{K_i} the discriminant of K_i. The extension K_{i+1}/K_i is unramified outside S_i. By Lemma 2,

$$|D_{K_{i+1}}| < |D_{K_i}|^p \left| N_{K_i}\left(\prod_{\mathcal{P} \in S_i} \mathcal{P}\right)\right|^{2p-1} \quad (i = 0, \dots, t-1).$$

Thus, we obtain by induction

$$|D_L| < |D_K|^{p^t} \left| N_K\left(\prod_{\mathcal{P} \in S} \mathcal{P}\right)\right|^{(2p-1)tp^{t-1}}.$$

Therefore

$$|D_L| < p^{(2p-1)dtp^{t-1}} |D_K|^{p^t} |N_K(\Delta(g))|^{(2p-1)tp^{t-1}}.$$

4. Proofs of Theorems 1, 2, 3 and Corollaries 1, 2, 3

Proof of Theorem 1. Let x, y be integers in K satisfying $y^2 = f(x)$. Set $g(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ and denote by $\Delta(g)$ the discriminant of $g(X)$. Let w be an algebraic integer such that $w^2 = g(x)$ and let $L = K(w)$. Theorem A gives

$$\max\{H_L(x), H_L(w)\} < \exp\{\Omega(2d)|D_L|^{25}|N_L(\Delta(g))|^{27} \log^* H_L(g)\}.$$

By Proposition 1, the discriminant D_L of the number field $L = K(w)$ satisfies

$$|D_L| < 8^d |D_K|^2 |N_K(\Delta(g))|^3.$$

Thus

$$\max\{H_L(x), H_L(w)\} < \exp\{\Phi_1(d)|D_K|^{50}|N_K(\Delta(g))|^{180} \log^* H_K(g)\},$$

where

$$\Phi_1(d) < 10^{1700d+53} d^{624d+13}.$$

Proof of Corollary 1. Let $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_n$ and $x, y \in O_K$ satisfying $y^2 = f(x)$. Then $(a_0x, a_0^{(n-1)/2}y)$ is an integral solution over $K(a_0^{(n-1)/2})$ to the equation $Y^2 = \tilde{f}(X)$, where

$$\tilde{f}(X) = X^n + a_1X^{n-1} + a_2a_0X^{n-1} + \ldots + a_na_0^{n-1} = (X - a_0\alpha_1)^{e_1} \ldots (X - a_0\alpha_r)^{e_r}.$$

Put $G(X) = a_0(X - \alpha_1)\ldots(X - \alpha_r)$, $G_1(X) = (X - a_0\alpha_1)\ldots(X - a_0\alpha_r)$ and denote by $\Delta(G)$, $\Delta(G_1)$ respectively their discriminants. By Lemma 5, the height of the polynomial $h(X) = (X - a_0\alpha_1)(X - a_0\alpha_2)(X - a_0\alpha_3)$ is

$$H(h) \leq 4^{r+3} H(a_0)^3 H(G).$$

Further, the discriminant $\Delta(h)$ of h satisfies

$$|N_M(\Delta(h))| \leq |N_M(\Delta(G_1))| \leq (|N_K(a_0)|^{(r-1)(r-2)} |N_K(\Delta(G))|)^{2r(r-1)(r-2)}.$$

By Lemma 3, the discriminant D_L of $L = K(\alpha_1, \alpha_2, \alpha_3)$ has

$$|D_L| \leq |D_K|^{r(r-1)(r-2)} |N_K(\Delta(G_1))|^{3r^2}.$$

Since $|N_K(\Delta(G_1))| \leq |N_K(a_0)|^{(r-1)(r-2)} |N_K(\Delta(G))|$, we get

$$|D_L| \leq (|D_K||N_K(a_0)|^{3r})^{r(r-1)(r-2)} |N_K(\Delta(G))|^{3r^2}.$$

On the other hand the discriminant D_M of $M = L(a_0^{(n-1)/2})$ satisfies

$$|D_M| \leq |D_L|^2 (4^d |N_K(a_0)|^{(n-1)})^{r(r-1)(r-2)}.$$

Thus

$$|D_M| \leq |N_K(\Delta(G))|^{6r^2} (4^d |D_K|^2 |N_K(a_0)|^{n+6r-1})^{r(r-1)(r-2)}.$$

Theorem 1 gives

$$H_M(a_0x) < \exp\{\Phi_1(2dr(r-1)(r-2))|D_M|^{50}|N_M(\Delta(h))|^{180}\log^* H_M(h)\}.$$

Since

$$H_M(x) \le H_M(a_0x)H_M(a_0^{-1}) = H_M(a_0x)H_M(a_0),$$

combining the above estimates, we get

$$H_M(x) < \exp\{\Phi_2(d,r)(|D_K|^{10}|N_K(\Delta(G))|^{36}|N_K(a_0)|^{36rn})^{10r^3}\log^*(H_K(a_0)H_K(G))\},$$

where

$$\Phi_2(d,r) < (10^{16}(dr^3)^5)^{250dr^3}.$$

Proof of Theorem 2. Let x, y be integers in K satisfying $y^p = f(x)$. Set $g(X) = (X-\alpha_1)(X-\alpha_2)$ and denote by $\Delta(g)$ the discriminant of $g(X)$. Let w be an algebraic integer such that $w^p = g(x)$. Thus

$$w^p - \alpha_1\alpha_2 = x^2 - (\alpha_1+\alpha_2)x.$$

Multiplying by 4^p and adding the term $(2^{p-1}(\alpha_1+\alpha_2))^2$ in the two members, we get

$$(4w)^p - 4^p(\alpha_1\alpha_2) + (2^{p-1}(\alpha_1+\alpha_2))^2 = (2^px)^2 - 2^p(\alpha_1+\alpha_2)(2^px) + (2^{p-1}(\alpha_1+\alpha_2))^2.$$

Setting

$$t = 2^{p-1}(2x-(\alpha_1+\alpha_2)) \quad \text{and} \quad u = 4w,$$

we obtain

$$t^2 = u^p + 4^{p-1}\Delta(g).$$

Put $L = K(w)$ and $R(X) = X^p + 4^{p-1}\Delta(g)$. Denote by D_L and $\Delta(R)$ respectively the discriminants of L and $R(X)$. Let $M = L(z)$, where z is a root of the polynomial $R(X)$. By Lemma 3,

$$|D_M| < |D_L|^p|N_L(\Delta(R))|.$$

It is well known that $\Delta(R) = p^p(4^{p-1}\Delta(g))^{p-1}$. Thus

$$|D_M| < (p4^p)^{dp^2}|D_L|^p|N_K(\Delta(g))|^{p(p-1)}.$$

By Proposition 1,

$$|D_L| < p^{(2p-1)d} |D_K|^p |N_K(\Delta(g))|^{2p-1}.$$

Therefore

$$|D_M| < (p^3 4^p)^{dp^2} |D_K|^{p^2} |N_K(\Delta(g))|^{3p^2}.$$

Let ω be a pth primitive root of 1. According to our assumptions $\omega \in K$. Put $h(X) = (X - z)(X - z\omega)(X - z\omega^2)$. Applying Theorem 1, we get

$$H_M(u) < \exp\{\Phi_1(dp^2)|D_M|^{50} |N_M(\Delta(h))|^{180} \log^* H_M(h)\}.$$

We have

$$|N_M(\Delta(h))| \le |N_M(z)|^6 p^{dp^3} \le |N_K(\Delta(g))|^{2p^2} p^{5dp^3}$$

and Lemma 4 gives

$$H_M(h) \le H_M(z)^3 4^{d(p+1)p^2} \le H_K(\Delta(g))^{p^2} 16^{dp^3} \le H_K(g)^{2p^2} 2^{5dp^3}.$$

Therefore

$$H_M(u) < \exp\{\Phi_1(dp^2) 4^{52dp^3} p^{950dp^3} |D_K|^{50p^2} |N_K(\Delta(g))|^{510p^2} \log^* H_K(g)\}.$$

We have

$$H(t) \le H(t)^2 = H(t^2) \le 2H(u^p)H(4^{p-1}\Delta(g)) \le 2^{2p-1} H(u^p)H(\Delta(g)) \le 2^{2p+2} H(u^p)H(g)^2.$$

Then

$$H(x) \le 2^{p+2} H(t)H(g) \le 2^{3p+4} H(u^p)H(g)^3.$$

Hence

$$H_M(x) < \exp\{\Psi_1(d, p)|D_K|^{50p^2} |N_K(\Delta(g))|^{510p^2} \log^* H_K(g)\},$$

where

$$\Psi_1(d, p) < 10^{1700dp^2+53} d^{624dp^2+13} p^{1438dp^3+9}.$$

Proof of Corollary 2. Let $x, y \in O_K$ be a solution of $y^p = f(x)$. Then $(a_0 x, a_0^{(n-1)/p} y)$ is an integral solution over $K(a_0^{(n-1)/p})$ to the equation $Y^p = \tilde{f}(X)$, where

$$\tilde{f}(X) = (X - a_0\alpha_1)^{e_1} \dots (X - a_0\alpha_r)^{e_r}.$$

Consider the polynomials $G(X) = a_0(X-\alpha_1)\dots(X-\alpha_r)$, $G_1(X) = (X-a_0\alpha_1)\dots(X-a_0\alpha_r)$ and denote by $\Delta(G), \Delta(G_1)$ respectively their discriminants. Let ω be a pth primitive root of 1. By Lemma 3, the discriminant D_L of $L = K(\alpha_1, \alpha_2, \omega)$ is

$$|D_L| \le p^{dpr^2}|D_K|^{r^2(p-1)}|N_K(\Delta(G_1))|^{2r(p-1)}.$$

Thus, we obtain

$$|D_L| \le p^{dpr^2}|D_K|^{r^2(p-1)}(|N_K(a_0)|^{(r-1)(r-2)}|N_K(\Delta(G))|)^{2r(p-1)}.$$

Put $M = L(a_0^{(n-1)/p})$ and denote by D_M the discriminant of M. Since the discriminant of the polynomial $X^p - a_0^{n-1}$ is $(-1)^{p(p-1)/2}p^p a_0^{(n-1)(p-1)}$, Lemma 3 gives

$$|D_M| \le |D_L|^p(p^{dp}|N_K(a_0)|^{(n-1)(p-1)})^{(p-1)r(r-1)}.$$

It follows that

$$|D_M| < p^{2dp^2r^2}|D_K|^{r^2(p-1)p}|N_K(\Delta(G))|^{2r(p-1)p}|N_K(a_0)|^{2r^2p^2(n-1)}.$$

By Lemma 5, the height of the polynomial $h(X) = (X - a_0\alpha_1)(X - a_0\alpha_2)$ satisfies

$$H(h) < 4^r 12 H(a_0)^2 H(G).$$

Furthermore, the discriminant $\Delta(h)$ of h satisfies

$$|N_M(\Delta(h))| \le |N_M(\Delta(G_1))| \le (|N_K(a_0)|^{(r-1)(r-2)}|N_K(\Delta(G))|)^{r(r-1)p(p-1)}.$$

Using Theorem 2 and the above estimates, we get

$$H_M(x) < \exp\{\Psi_2(d,r,p)(|D_K|^5|N_K(\Delta(G))|^{51}|N_K(a_0)|^{51rn})^{10r^2p^4}\log^*(H_K(a_0)H_K(G))\},$$

where

$$\Psi_2(d,r,p) < (10^3(dr^2)p^{3p})^{625dr^2p^4}.$$

Proof of Theorem 3. Let $x, y \in O_K$ be a solution of $y^4 = f(x)$. Consider the polynomial $g(X) = (X-\alpha_1)(X-\alpha_2)$ and denote by $\Delta(g)$ its discriminant. Let w be an algebraic integer such that $w^4 = g(x)$. Then

$$w^4 - \alpha_1\alpha_2 = x^2 - (\alpha_1 + \alpha_2)x.$$

Multiplying by 2^4 and adding the term $(2(\alpha_1+\alpha_2))^2$ in the two members, we obtain

$$(2w)^4 + 4\Delta(g) = [(4x) - 2(\alpha_1 + \alpha_2)]^2.$$

Setting $t = 2w$ and $z = (4x) - 2(\alpha_1 + \alpha_2)$, we get

$$z^2 = t^4 + 4\Delta(g).$$

Put $L = K(w)$ and $S(X) = X^4 + 4\Delta(g)$. Denote by D_L and $\Delta(S)$ respectively the discriminants of L and $S(X)$. Let $M = L(u)$, where u is a root of the polynomial $S(X)$. By Lemma 3,

$$|D_M| < |D_L|^4 |N_L(\Delta(S))|.$$

Since $\Delta(S) = 4^4(4\Delta(g))^3$, we have

$$|N_L(\Delta(S))| \le 4^{28d} |N_K(\Delta(g))|^{12}.$$

By Proposition 1,

$$|D_L| < 2^{12d} |D_K|^4 |N_K(\Delta(g))|^{12}.$$

Therefore

$$|D_M| < 4^{52d} |D_K|^{16} |N_K(\Delta(g))|^{60}.$$

Set $h(X) = (X - u)(X - u\omega)(X - u\omega^2)$, where ω is a 4th primitive root of 1. Then Theorem 1 gives

$$H_M(t) < \exp\{\Phi_1(16d) |D_M|^{50} |N_M(\Delta(h))|^{180} \log^* H_M(h)\}.$$

We deduce as in the proof of Theorem 2 that

$$|N_M(\Delta(h))| \le 4^{88d} |N_K(\Delta(g))|^{24} \quad \text{and} \quad H_M(h) < 4^{148d} H_K(g)^{32}.$$

Hence

$$H_M(t) < \exp\{\Phi_1(16d) 4^{18440d+4} |D_K|^{800} |N_K(\Delta(g))|^{4620} \log^* H_K(g)\}.$$

We have

$$H(z) \le H(z)^2 \le 8H(t)^4 H(\Delta(g)) \le 40H(t)^4 H(g)^2.$$

Hence

$$H(x) \le 8H(g)H(z) \le 320H(t)^4 H(g)^3.$$

Thus

$$H_M(x) < \exp\{\Omega_1(d) |D_K|^{800} |N_K(\Delta(g))|^{4620} \log^* H_K(g)\},$$

where

$$\Omega_1(d) < 10^{50597d+73} d^{9984d+13}.$$

Proof of Corollary 3. Consider the equation $Y^4 = \tilde{f}(X)$, where

$$\tilde{f}(X) = (X - a_0\alpha_1)^{e_1} \dots (X - a_0\alpha_r)^{e_r}.$$

If $x, y \in O_K$ is a solution of $y^4 = f(x)$, then $(a_0 x, a_0^{(n-1)/4} y)$ is an integral solution over $K(a_0^{(n-1)/p})$ to the equation $Y^2 = \tilde{f}(X)$. We set $G(X) = a_0(X - \alpha_1)\dots(X - \alpha_r)$, $G_1(X) = (X - a_0\alpha_1)\dots(X - a_0\alpha_r)$, $h(X) = (X - a_0\alpha_1)(X - a_0\alpha_2)$ and we denote by $\Delta(G)$, $\Delta(G_1)$, $\Delta(h)$ respectively their discriminants. By Lemma 3, the discriminant D_L of $L = K(\alpha_1, \alpha_2, \omega)$, where ω is a 4th primitive root of 1, satisfies

$$|D_L| \le 4^{dr^2} |D_K|^{2r^2} |N_K(\Delta(G_1))|^{4r} \le 4^{dr^2} |D_K|^{2r^2} (|N_K(a_0)|^{(r-1)(r-2)} |N_K(\Delta(G))|)^{4r}.$$

Put $M = L(a_0^{(n-1)/4})$ and denote by D_M the discriminant of M. Then, Lemma 3 gives

$$|D_M| \le 4^{32dr(r-1)} |D_L|^4 |N_K(a_0)|^{24(n-1)r(r-1)}.$$

Thus,

$$|D_M| \le 4^{36dr^2} |D_K|^{8r^2} |N_K(\Delta(G))|^{16r} |N_K(a_0)|^{40(n-1)r(r-1)}.$$

By Lemma 5, we get

$$H(h) < 4^r 12 H(a_0)^2 H(G).$$

Further, we deduce

$$|N_M(\Delta(h))| \le |N_M(\Delta(G_1))| \le (|N_K(a_0)|^{(r-1)(r-2)} |N_K(\Delta(G))|)^{8r(r-1)}.$$

Theorem 3 and the above estimates give

$$H_M(x) < \exp\{\Omega_2(d, r)(|D_K|^{64} |N_K(\Delta(G))|^{370} |N_K(a_0)|^{370nr})^{100r^2} \log^*(H_K(a) H_K(G))\},$$

where

$$\Omega_2(d, r) < ((10^{49}(dr^2)^8)^{10^4 dr^2}).$$

REFERENCES

1. A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambr. Philos. Soc.* **65** (1969), 439–444.

2. D. Kubert and A. Lang, Units in modular function field I, *Math. Ann.* (1975), 67–96.

3. S. Lang, *Fundamentals of Diophantine Geometry*, New York-Berlin-Heidelberg-Tokyo: Springer-Verlag, 1983.

4. S. Lang, *Introduction to algebraic and abelian Functions*, New York-Berlin-Heidelberg: Springer-Verlag, 1982.

5. D. Poulakis, Solutions entières de l'équation $f(X, Y)^2 = h(X)g(X, Y)$, *C.R. Acad. Sci. Paris* **315** (1992), 963–968.

6. D. Poulakis, Integer points on algebraic curves with exceptional units, *J. Austral. Math. Soc. (Series A)* **63** (1997), 145–164.

7. W. Schmidt, Eisenstein's theorem on power series expansions of algebraic functions, *Acta Arith.* **LVI** (1990), 161–179.

8. J. P. Serre, *Corps Locaux*, Hermann, Paris, 1962.

9. J. H. Silverman, *The Arithmetic of elliptic curves*, New York-Berlin-Heidelberg: Springer-Verlag, 1986.

10. P. Voutier, An Upper Bound for the Size of Integral Solutions to $Y^m = f(X)$, *J. Number Theory* **53** (1995), 247–271.

Aristotle University of Thessaloniki
Department of Mathematics
54006 Thessaloniki
GREECE
E-mail address: poulakis@ccf.auth.gr