JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Anton MOSUNOV

Absolute Bound On the Number of Solutions of Certain Diophantine Equations of Thue and Thue–Mahler Type

Tome 36, nº 3 (2024), p. 947-965.

https://doi.org/10.5802/jtnb.1301

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **36** (2024), 947–965

Absolute Bound On the Number of Solutions of Certain Diophantine Equations of Thue and Thue–Mahler Type

par Anton MOSUNOV

Résumé. Soit F une forme binaire irréductible de degré $d \geq 7$ à coefficients entiers dont le plus grand diviseur commun est égal à 1. Soit α une racine complexe de $F(x,1)$. Supposons que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne. Nous prouvons que, pour toute puissance p^k suffisamment grande d'un nombre premier p, le nombre de solutions de l'équation diophantienne de type Thue

$$|F(x,y)| = hp^k$$

en nombres entiers (x,y,h) tels que

$$\gcd(x,y) = 1 \quad \text{et} \quad 1 \leq h \leq (p^k)^\lambda$$

est borné par 24. Ici $\lambda = \lambda(d)$ est une fonction positive et monotone croissante qui s'approche de 1 lorsque d tend vers l'infini. Nous prouvons également que, pour tout nombre premier p suffisamment grand, le nombre de solutions de l'équation diophantienne de type Thue–Mahler

$$|F(x,y)| = hp^z$$

en entiers (x,y,z,h) tels que

$$\gcd(x,y) = 1, \quad z \geq 1 \quad \text{et} \quad 1 \leq h \leq (p^z)^{\frac{10d-61}{20d+40}}$$

ne dépasse pas 3984. Nos preuves découlent de la combinaison de deux principes d'approximation diophantienne, à savoir le principe d'écart non-archimédien généralisé et le principe de Thue–Siegel.

Abstract. Let $F \in \mathbb{Z}[x,y]$ be an irreducible binary form of degree $d \geq 7$ and content one. Let α be a complex root of $F(x,1)$ and assume that the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. We prove that, for every sufficiently large prime power p^k, the number of solutions to the Diophantine equation of Thue type

$$|F(x,y)| = hp^k$$

in integers (x,y,h) such that

$$\gcd(x,y) = 1 \quad \text{and} \quad 1 \leq h \leq (p^k)^\lambda$$

Manuscrit reçu le 31 mars 2023, révisé le 25 août 2023, accepté le 7 octobre 2023.

2020 *Mathematics Subject Classification.* 11D59.

Mots-clefs. Thue equation, Thue–Mahler equation, Diophantine approximation, binary form.

The author is grateful to Prof. Cameron L. Stewart for his wise supervision, as well as to the anonymous referees for their suggestions on how to improve the article.

does not exceed 24. Here $\lambda = \lambda(d)$ is a certain positive, monotonously increasing function that approaches one as d tends to infinity. We also prove that, for every sufficiently large prime number p, the number of solutions to the Diophantine equation of Thue–Mahler type

$$|F(x,y)| = hp^z$$

in integers (x, y, z, h) such that

$$\gcd(x,y) = 1, \quad z \geq 1 \quad \text{and} \quad 1 \leq h \leq (p^z)^{\frac{10d-61}{20d+40}}$$

does not exceed 3984. Our proofs follow from the combination of two principles of Diophantine approximation, namely the generalized non-Archimedean gap principle and the Thue–Siegel principle.

1. Introduction

In this article we analyze certain Diophantine equations of Thue and Thue–Mahler type. A *Thue equation* is a Diophantine equation of the form

$$F(x,y) = m, \tag{1.1}$$

where $F \in \mathbb{Z}[x,y]$ is a homogeneous polynomial of degree $d \geq 3$ with nonzero discriminant $D(F)$, m is a fixed positive integer, and x, y are integer variables. In 1909 Thue [17] proved that (1.1) has only finitely many solutions in integers x and y, provided that F is irreducible. In 1933, assuming that F is irreducible, Mahler established the existence of a number C_1, dependent only on F, such that the number of primitive solutions to (1.1) (that is, integer solutions with x and y coprime) does not exceed $C_1^{1+\omega(m)}$, where $\omega(m)$ denotes the number of distinct prime divisors of m [10]. In fact, his result was even stronger: if instead of (1.1) we consider the equation

$$F(x,y) = p_1^{z_1} \cdots p_\ell^{z_\ell}, \tag{1.2}$$

where $p_1, \ldots, p_\ell$ are distinct fixed prime numbers, then it follows from Mahler's argument that the number of integer solutions $(x, y, z_1, \ldots, z_\ell)$ to (1.2), with x, y coprime and z_i non-negative, does not exceed $C_1^{1+\ell}$. The Diophantine equation (1.2) is called a *Thue–Mahler equation*. Further improvements to Mahler's estimate have been made by Erdős and Mahler [5], and Lewis and Mahler [9].

It was conjectured by Siegel that the number of primitive solutions to (1.1) should not depend on the coefficients of F. The truth of Siegel's conjecture was established in 1984 by Evertse [7], who proved that the number of primitive solutions to (1.2) does not exceed

$$2 \cdot 7^{d^3(2\ell+3)}, \tag{1.3}$$

where a binary form F of degree d was assumed to be divisible by at least three pairwise linearly independent linear forms in some algebraic

number field. An estimate on the number of solutions to (1.1) thus follows by replacing the number ℓ in (1.3) with $\omega(m)$.

The number of integer solutions to (1.1), not necessarily primitive, can be large. For example, in 2008 Stewart [16] proved that when F is of degree 3 and $D(F) \neq 0$ then there is a positive number c, which depends only on F, such that the number of integer solutions to (1.1) is at least $c(\log m)^{1/2}$ for infinitely many positive integers m. If, however, we restrict our attention to primitive solutions only, then their number does not seem to increase as m grows. In 1987 it was conjectured by Erdős, Stewart and Tijdeman [6] that the number of primitive solutions to (1.1) does not exceed some constant, which depends only on d. In the same year Bombieri and Schmidt [3] proved that the number of primitive solutions to (1.1) does not exceed

$$C_2 d^{1+\omega(m)},$$

where the constant C_2 is absolute. In 1991 Stewart [15] replaced $\omega(m)$ in the above estimate with $\omega(g)$, where g is a divisor of m satisfying $g \gg_F m^{(4+d)/3d}$ (this is the statement of [15, Theorem 1] with $\varepsilon = 1/2$). In the same paper, Stewart conjectured the following.

Conjecture 1.1. (Stewart, [15, Section 6]) *There exists an absolute constant c_0 such that for every binary form $F \in \mathbb{Z}[x, y]$ with nonzero discriminant and degree at least three there exists a number C, which depends only on F, such that if m is an integer larger than C, then the Thue equation* (1.1) *has at most c_0 solutions in coprime integers x and y.*

The most notable step forward towards Conjecture 1.1 can be found in the work of Thunder [18, Theorems 3 and 5]. Based on [15] he gives a heuristic argument that supports the conjecture of Stewart when the degree of the form F is at least five. Roughly speaking, every primitive solution to (1.1) lies in a sublattice of $\mathbb{Z}^2$ of determinant m', where m' is a divisor of m. Furthermore, it corresponds to the first Minkowski minimum of this sublattice. One can then show that the first and second Minkowski minima must drastically differ in size, making this sublattice very skewed. As m grows unboundedly, the proportion of these skewed sublattices among all lattices of the same determinant tends to zero, and so we do not expect many of them to occur, unless primitive solutions that they contain are connected to each other algebraically (e.g., via a linear fractional transformation, as it is the case for the results stated below).

By using a generalization of the non-Archmiedean gap principle established in [12], we develop new methods for estimating the number of primitive solutions of (1.1) and (1.2) in the case $\ell = 1$, thus providing theoretical evidence in support of Stewart's conjecture. Instead of looking at (1.1) and (1.2) though, we study Diophantine equations of the form

$$|F(x, y)| = hp^z,$$

with p^z a prime power and h a positive integer variable, which is "small" in comparison to p^z. We demonstrate that it is possible to provide an absolute bound on their number of primitive solutions, provided that F is irreducible of degree $d \geq 7$ and the order of the Galois group of $F(x,1)$ over $\mathbb{Q}$ is equal to d.

In order to state the main results given in Theorems 1.2 and 1.3, we need to introduce the notion of an *enhanced automorphism group* of a binary form. For a 2×2 matrix $M = \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right)$, with complex entries, define the binary form F_M by

$$F_M(x,y) = F(sx+uy, tx+vy).$$

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of the rationals (embedded) in $\mathbb{C}$ and let K be a field containing $\mathbb{Q}$. We say that a matrix $M = \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right) \in \mathrm{M}_2(K)$ is a *K-automorphism of F* (resp., $|F|$) iff $F_M = F$ (resp., $F_M = \pm F$). The set of all K-automorphisms of F (resp., $|F|$) is denoted by $\mathrm{Aut}_K F$ (resp., $\mathrm{Aut}_K |F|$). We define

$$\mathrm{Aut}'\,|F| = \left\{ \frac{1}{\sqrt{|sv-tu|}} \begin{pmatrix} s & u \\ t & v \end{pmatrix} : s,t,u,v \in \mathbb{Z} \right\} \cap \mathrm{Aut}_{\overline{\mathbb{Q}}}\,|F| \tag{1.4}$$

and refer to it as the *enhanced automorphism group* of F. See [12, Lemma 7.2] for a proof that $\mathrm{Aut}'\,|F|$ contains at most 24 elements, provided that $d \geq 3$ and $D(F) \neq 0$.

For a nonzero polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$, we define the *content* of P to be the greatest common divisor of its coefficients. Let

$$f(d) = \frac{20d-41}{80}\left(\frac{\sqrt{d^2+16d}}{d} - 1\right) - 1 \tag{1.5}$$

and notice that $f(d)$ is a positive monotonously increasing function on the interval $[7,\infty)$, which approaches one as d tends to infinity (notice that $f(d)$ is negative for $d \in \{3,4,5,6\}$). For an arbitrary finite set X, let $\#X$ denote its cardinality. We prove the following.

Theorem 1.2. *Let $F \in \mathbb{Z}[x,y]$ be an irreducible binary form of degree $d \geq 7$ and content one. Let α be a complex root of $F(x,1)$ and assume that the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Let λ be such that $0 \leq \lambda < f(d)$, where $f(d)$ is defined in* (1.5)*. Let p be prime, k a positive integer, and consider the equation*

$$|F(x,y)| = hp^k, \tag{1.6}$$

where x, y and h are integer variables, with $h \geq 1$. There exists a positive number C, which depends only on F and λ, and that is explicitly computable when $\alpha \notin \mathbb{R}$, with the following property. For all $p^k \geq C$, the number of

solutions to (1.6) *in integers* (x, y, h) *such that*

$$\gcd(x, y) = 1 \quad \textit{and} \quad 1 \le h \le (p^k)^\lambda$$

is at most $\#\operatorname{Aut}'|F|$. *In particular, it does not exceed* 24. *More precisely, for every two solutions* (x_1, y_1, h_1) *and* (x_2, y_2, h_2) *there exists a matrix*

$$M = |sv - tu|^{-1/2} \cdot \begin{pmatrix} s & u \\ t & v \end{pmatrix}$$

in $\operatorname{Aut}'|F|$ *such that*

$$\frac{x_2}{y_2} = \frac{sx_1 + uy_1}{tx_1 + vy_1}.$$

Theorem 1.3. *Let* $F \in \mathbb{Z}[x, y]$ *be an irreducible binary form of degree* $d \ge 7$ *and content one. Let* α *be a complex root of* $F(x, 1)$ *and assume that the field extension* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *is Galois. Let* λ *be such that*

$$0 \le \lambda < 1 - 8.1/(d + 2).$$

Let p *be prime and consider the equation*

$$|F(x, y)| = hp^z, \tag{1.7}$$

where x, y, h *and* z *are integer variables, with* $h, z \ge 1$. *There exists a positive number* C, *which depends only on* F *and* λ, *and that is explicitly computable when* $\alpha \notin \mathbb{R}$, *with the following property. For all* $p \ge C$, *the number of solutions to* (1.7) *in integers* (x, y, z, h) *such that*

$$\gcd(x, y) = 1, \quad z \ge 1 \quad \textit{and} \quad 1 \le h \le (p^z)^\lambda$$

is at most

$$2\#\operatorname{Aut}'|F| \cdot \left\lfloor 1 + \frac{11.51 + 1.5 \log d + \log\left((d - 2.05)/(1 + \lambda)\right)}{\log((d - 2.05)/(1 + \lambda) - 0.5d)} \right\rfloor.$$

If we let $\lambda(d) = 0.5 - 4.05/(d + 2)$, then the function

$$g(d) = 1 + \frac{11.51 + 1.5 \log d + \log\left((d - 2.05)/(1 + \lambda(d))\right)}{\log((d - 2.05)/(1 + \lambda(d)) - 0.5d)}$$

is monotonously decreasing on the interval $[7, \infty)$. Since $g(7) \approx 83.3$, we can use the upper bound $\#\operatorname{Aut}'|F| \le 24$ as well as Theorem 1.3 to conclude that the number of solutions (x, y, z, h) to (1.7) satisfying the aforementioned conditions does not exceed $48 \cdot \lfloor g(7) \rfloor = 3984$ when $d \ge 7$. Furthermore, since $g(10^{15}) < 4$ and $\lim_{d\to\infty} g(d) = 3.5$, we can also conclude that it does not exceed $48 \cdot \lfloor g(10^{15}) \rfloor = 144$ when $d \ge 10^{15}$.

The proof of Theorem 1.2 follows from the generalized non-Archimedean gap principle, whose statement is given in Section 2, Lemma 2.3. The proof of Theorem 1.3 follows from Lemma 2.5, which, in turn, is a consequence of both the generalized non-Archimedean gap principle and the Thue–Siegel principle, as formulated by Bombieri [1] and Bombieri and Mueller [2]. The

condition that the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois is necessary so to ensure that all the conjugates of α lie in $\mathbb{Q}(\alpha)$, as this enables us to invoke both lemmas. The condition $d \geq 7$ arises naturally in both of our arguments and we emphasize its usage in our proofs. For example, in order to apply each lemma, it is important to ensure that the inequality $(d/2) + 1 < \mu$ is satisfied. In both of our arguments we have $\mu = (d - 2.05)/(1 + \lambda)$, so $(d/2) + 1 < \mu$ if and only if $\lambda < 1 - 8.1/(d + 2)$. Notice that this last inequality can be solved for non-negative λ if and only if $d \geq 7$.

Unfortunately, in the case when α is real, due to the application of Roth's Theorem [13] it is not yet possible to determine how large a prime power p^k in Theorem 1.2 or a prime p in Theorem 1.3 should be in order for the respective absolute bound to hold. We expect that it is possible to overcome this problem if one is able to generalize the non-Archimedean gap principle even further and extend the range of μ from $(d/2) + 1 < \mu < d$ to, say, $\sqrt{2d} < \mu < d$, as it was done by Siegel [14] and Dyson [4] in the context of (what was later called) the Thue–Siegel principle.

As a final remark, we point the reader's attention to the fact that in Theorems 1.2 and 1.3 we are considering only one large prime power p^k and one large prime p, respectively. Once again, this is because we would like to apply Lemmas 2.3 and 2.5. To achieve this, a power of a prime p has to be a large divisor of the right-hand side, and that is why we control the magnitude of h by imposing the condition $h \leq (p^k)^\lambda$ for some fixed non-negative λ. When λ is small, the quantity $\mu = (d - 2.05)/(1 + \lambda)$ exceeds $(d/2) + 1$, thus enabling us to invoke each lemma. We expect that it would be possible to establish similar absolute bounds for Diophantine equations $|F(x, y)| = hp_1^{z_1} \cdots p_\ell^{z_\ell}$, at least when ℓ is small relative to d, provided that the non-Archimedean gap principle is generalized in a way that μ can take values less than $(d/2) + 1$.

The article is structured as follows. In Section 2 we outline a number of auxiliary results, which are used in later sections. We recommend the reader to skip this section and use it as a reference when reading proofs of Theorems 1.2 and 1.3, which are outlined in Sections 3 and 4, respectively. We conclude the article with Section 5, where we demonstrate two applications of the aforementioned theorems in the cases when $F = \Phi_n$, the n-th cyclotomic binary form, and $F = \Psi_n$, the homogenization of the minimal polynomial of $2\cos\frac{2\pi}{n}$.

2. Auxiliary Results

This section contains several definitions and results, which we utilize in Sections 3 and 4. We recommend the reader to use it as a reference.

For an arbitrary polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$, let $H(P)$ denote the maximum of Archimedean absolute values of its coefficients, and refer to

this quantity as the *height* of P. For a point $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, define

$$H(x_1, \ldots, x_n) = \max_{i=1,2,\ldots,n} \{|x_i|\}$$

and refer to this quantity as the *height* of $(x_1, \ldots, x_n)$.

Let $P \in \mathbb{C}[x]$ be a polynomial that is not identically equal to zero, with leading coefficient c_P. The *Mahler measure* of P, denoted $M(P)$, is defined to be $M(P) = |c_P|$ if $P(x)$ is the constant polynomial and

$$M(P) = |c_P| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

otherwise, where $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the roots of P. For a binary form $Q \in \mathbb{C}[x, y]$, we define the Mahler measure of Q as $M(Q) = M(Q(x, 1))$. The following lemma is a consequence of a well-known result of Lewis and Mahler [9].

Lemma 2.1 (see [12, Lemma 2.6])**.** *Let*

$$F(x, y) = c_d x^d + c_{d-1} x^{d-1} y + \cdots + c_0 y^d$$

be a binary form of degree $d \geq 2$ with integer coefficients such that $c_0 c_d \neq 0$. Let x_0, y_0 be nonzero integers. There exists a root α of $F(x, 1)$ such that

$$\min\left\{\left|\alpha - \frac{x_0}{y_0}\right|, \left|\alpha^{-1} - \frac{y_0}{x_0}\right|\right\} \leq \frac{C|F(x_0, y_0)|}{H(x_0, y_0)^d},$$

where

$$C = \frac{2^{d-1} d^{(d-1)/2} M(F)^{d-2}}{|D(F)|^{1/2}}.$$

Lemma 2.2 (Thunder, [18, Lemma 2])**.** *Let p be a rational prime and let $\overline{\mathbb{Q}_p}$ denote the algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. Let $F \in \mathbb{Z}[x, y]$ be an irreducible homogeneous polynomial of degree $d \geq 2$ and content one, and denote the roots of $F(x, 1)$ by $\alpha_1, \ldots, \alpha_d \in \overline{\mathbb{Q}_p}$. Let x and y be coprime integers. If i_0 is an index with*

$$\frac{|x - \alpha_{i_0} y|_p}{\max\{1, |\alpha_{i_0}|_p\}} = \min_{1 \leq i \leq d} \left\{\frac{|x - \alpha_i y|_p}{\max\{1, |\alpha_i|_p\}}\right\},$$

then

$$\frac{|x - \alpha_{i_0} y|_p}{\max\{1, |\alpha_{i_0}|_p\}} \leq \frac{|F(x, y)|_p}{|D(F)|_p^{1/2}}.$$

Further, if $|F(x, y)|_p < |D(F)|_p^{1/2}$, then the index i_0 above is unique and $\alpha_{i_0} \in \mathbb{Q}_p$.

The following three results were established in [12]. Lemma 2.3 states the generalized non-Archimedean gap principle, which plays a crucial role in the proof of Theorem 1.2. In turn, Lemma 2.5 follows from the combination of the generalized gap principle and the Thue–Siegel principle, as formulated by Bombieri [1] and Bombieri and Mueller [2, Section II].

Lemma 2.3 (see [12, Theorem 1.2]). *Let p be a rational prime. Let $\alpha \in \mathbb{Q}_p$ be a p-adic algebraic number of degree $d \geq 3$ over $\mathbb{Q}$ and let β be irrational and in $\mathbb{Q}(\alpha)$. Let μ be a real number such that $(d/2) + 1 < \mu < d$ and let C_0 be a positive real number. There exist positive real numbers C_1 and C_2, that are explicitly computable in terms of α, β, μ and C_0, with the following property. If x_1/y_1 and x_2/y_2 are rational numbers in lowest terms such that $H(x_2, y_2) \geq H(x_1, y_1) \geq C_1$ and*

$$|y_1\alpha - x_1|_p < \frac{C_0}{H(x_1, y_1)^\mu}, \quad |y_2\beta - x_2|_p < \frac{C_0}{H(x_2, y_2)^\mu},$$

then at least one of the following holds:

- $H(x_2, y_2) > C_2^{-1} H(x_1, y_1)^{\mu - d/2}$;
- *There exist integers s, t, u, v, with $sv - tu \neq 0$, such that*

$$\beta = \frac{s\alpha + t}{u\alpha + v} \quad \text{and} \quad \frac{x_2}{y_2} = \frac{sx_1 + ty_1}{ux_1 + vy_1}.$$

Lemma 2.4 (see [12, Proposition 7.3]). *Let $F \in \mathbb{Z}[x, y]$ be an irreducible binary form of degree $d \geq 3$ and let c_d denote the coefficient of x^d in F. Let $\alpha_1, \ldots, \alpha_d$ be the roots of $F(x, 1)$. There exists an index $j \in \{1, \ldots, d\}$ such that*

$$\alpha_j = \frac{v\alpha_1 - u}{-t\alpha_1 + s}$$

for some integers s, t, u and v if and only if the matrix

$$M = \frac{1}{\sqrt{|sv - tu|}} \begin{pmatrix} s & u \\ t & v \end{pmatrix}$$

is in $\mathrm{Aut}'\,|F|$. Furthermore, if $M \in \mathrm{Aut}'\,|F|$, then $|sv - tu| = \left|\frac{F(s,t)}{c_d}\right|^{2/d}$.

For an irrational number α, the *orbit* of α is the set

$$\mathrm{orb}(\alpha) = \left\{ \frac{v\alpha - u}{-t\alpha + s} \ : \ s, t, u, v \in \mathbb{Z},\ sv - tu \neq 0 \right\}.$$

Lemma 2.5 (see [12, Theorem 8.1]). *Let $K = \mathbb{R}$ or $\mathbb{Q}_p$, where p is a rational prime, and denote the standard absolute value on K by $|\cdot|$ (in the case $K = \mathbb{Q}_p$, the absolute value is normalized so that $|p| = p^{-1}$). Let $\alpha_1 \in K$ be an algebraic number of degree $d \geq 3$ over $\mathbb{Q}$ and $\alpha_2, \alpha_3, \ldots, \alpha_n$ be distinct elements of $\mathbb{Q}(\alpha_1)$, different from α_1, each of* degree d. *Let*

μ be such that $(d/2)+1 < \mu < d$. Let C_0 be a real number such that $C_0 > (4e^A)^{-1}$, where

$$A = 500^2 \left(\log \max_{i=1,\dots,n} \{M(\alpha_i)\} + \frac{d}{2} \right). \tag{2.1}$$

There exists a positive real number C_3, which is explicitly computable in terms of $\alpha_1, \alpha_2, \dots, \alpha_n$, μ and C_0, with the following property. The total number of rationals x/y in lowest terms, which satisfy $H(x,y) \geq C_3$ and

$$\left| \alpha_j - \frac{x}{y} \right| < \frac{C_0}{H(x,y)^\mu} \tag{2.2}$$

for some $j \in \{1, 2, \dots, n\}$ is less than

$$\gamma \left\lfloor 1 + \frac{11.51 + 1.5 \log d + \log \mu}{\log(\mu - d/2)} \right\rfloor,$$

where

$$\gamma = \max\{\gamma_1, \dots, \gamma_n\}, \quad \gamma_i = \#\{j \colon \alpha_j \in \operatorname{orb}(\alpha_i)\}. \tag{2.3}$$

Notice that when degree d extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois and $\alpha = \alpha_1, \dots, \alpha_d$ are the algebraic conjugates of α, then for $d \geq 3$ it follows from Lemma 2.4 that $\alpha_j = (v\alpha - u)/(-t\alpha + s)$ if and only if $M = |sv - tu|^{-1/2} \cdot \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right)$ is an element of $\operatorname{Aut}'|F|$. Thus, in this case, the quantity γ in (2.3) does not exceed $\#\operatorname{Aut}'|F|$. This fact plays an important role in the proof of Theorem 1.3.

We conclude this section with the statement of a simple corollary to Roth's Theorem, which is used in the proofs of both Theorem 1.2 and Theorem 1.3.

Theorem 2.6 (corollary to Roth's Theorem [13])**.** *Let α be an irrational algebraic number in $\mathbb{C}$ and let ε be a positive real number. There exists a positive number C, which depends only on α and ε, such that the inequality*

$$\min\left\{ \left| \alpha - \frac{x}{y} \right|, \left| \alpha^{-1} - \frac{y}{x} \right| \right\} > \frac{1}{H(x,y)^{2+\varepsilon}}$$

is satisfied for all coprime integer pairs (x,y) satisfying $H(x,y) > C$. Furthermore, the number C is explicitly computable when $\alpha \notin \mathbb{R}$.

3. Proof of Theorem 1.2

Theorem 2.6 implies that for every complex root α of $F(x,1)$ there exists a positive number C_α, which depends only on α, such that for all coprime integer pairs (x,y) with $H(x,y) > C_\alpha$ the inequality

$$\min\left\{ |\alpha - \frac{x}{y}|, \left| \alpha^{-1} - \frac{y}{x} \right| \right\} > H(x,y)^{-2.05}$$

is satisfied. Furthermore, if $\alpha \notin \mathbb{R}$ and β is another complex root of $F(x,1)$, then $\beta \notin \mathbb{R}$ due to the fact that the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Consequently, the number C_α is explicitly computable in terms of α for every root α of $F(x,1)$, as long as at least one of these roots is non-real. Since

$$|F(x,y)| \leq (d+1)H(F)H(x,y)^d$$

and $|F(x,y)| = hp^k$, we have

$$\frac{hp^k}{(d+1)H(F)} \leq H(x,y)^d.$$

Therefore, by choosing p^k so that $p^k > C_\alpha^d(d+1)H(F)$ for every complex root α of $F(x,1)$, we can ensure that $\min\{|\alpha - x/y|, |\alpha^{-1} - y/x|\} > H(x,y)^{-2.05}$ for every complex root α of $F(x,1)$.

Define

$$C_0 = \frac{2^{d-1}d^{(d-1)/2}M(F)^{d-2}}{|D(F)|^{1/2}}.$$

Assume that there exists a solution (x,y,h) to (1.6). By Lemma 2.1,

$$\min\left\{\left|\alpha - \frac{x}{y}\right|, \left|\alpha^{-1} - \frac{y}{x}\right|\right\} \leq \frac{C_0 hp^k}{H(x,y)^d}.$$

From our choice of p^k and the above inequality it follows that

$$\frac{1}{H(x,y)^{2.05}} < \min\left\{\left|\alpha - \frac{x}{y}\right|, \left|\alpha^{-1} - \frac{y}{x}\right|\right\} \leq \frac{C_0 hp^k}{H(x,y)^d},$$

which is equivalent to

$$H(x,y) < (C_0 hp^k)^{1/(d-2.05)}. \tag{3.1}$$

Since $h \leq (p^k)^\lambda$,

$$hp^k \leq (p^k)^{1+\lambda} \leq |F(x,y)|_p^{-(1+\lambda)}.$$

Combining this inequality with (3.1), we get

$$H(x,y)^{d-2.05} < C_0 hp^k \leq C_0 |F(x,y)|_p^{-(1+\lambda)}.$$

We conclude that

$$|F(x,y)|_p < \frac{C_0^{1/(1+\lambda)}}{H(x,y)^\mu}, \tag{3.2}$$

where

$$\mu = \frac{d-2.05}{1+\lambda}.$$

Since we would like the conditions of Lemma 2.3 to be satisfied, we want to ensure that the inequality $(d/2)+1 < \mu$ holds. This inequality is satisfied if and only if $\lambda < 1 - 8.1/(d+2)$. Here we can observe the importance of the condition $d \geq 7$, as the inequality $\lambda < 1 - 8.1/(d+2)$ cannot be solved

for non-negative λ when $d < 7$. Since we chose $\lambda < f(d)$ for $f(d)$ defined in (1.5), and since $f(d) \leq 1 - 8.1/(d+2)$ for every $d \geq 7$, we conclude that the inequality $(d/2) + 1 < \mu$ holds.

Next, we take p^k sufficiently large that

$$p^k > |D(F)|.$$

Then

$$|F(x,y)|_p \leq p^{-k} < |D(F)|^{-1} \leq |D(F)|_p.$$

By Lemma 2.2 there exists a unique p-adic root $\alpha \in \mathbb{Q}_p$ of $F(x,1)$ such that

$$\frac{|y\alpha - x|_p}{\max\{1, |\alpha|_p\}} \leq \frac{|F(x,y)|_p}{|D(F)|_p^{1/2}}.$$

Let c_d denote the coefficient of x^d in F. Since $c_d\alpha$ is an algebraic integer, we see that $|c_d\alpha|_p \leq 1$, so $\max\{1, |\alpha|_p\} \leq |c_d|_p^{-1}$. Combining this inequality with (3.2), we obtain

$$\begin{aligned} |y\alpha - x|_p &< \frac{\max\{1, |\alpha|_p\}}{|D(F)|_p^{1/2}} |F(x,y)|_p \\ &\leq \frac{C_1}{H(x,y)^\mu}, \end{aligned}$$

where

$$C_1 = C_0^{1/(1+\lambda)} c_d |D(F)|^{1/2}.$$

Now, assume that there exist two solutions (x_1, y_1, h_1) and (x_2, y_2, h_2) to (1.6), ordered so that $H(x_2, y_2) \geq H(x_1, y_1)$. Then it follows from the discussion above that there exist p-adic roots $\alpha, \beta \in \mathbb{Q}_p$ of $F(x,1)$ such that

$$|y_1\alpha - x_1|_p < \frac{C_1}{H(x_1,y_1)^\mu}, \quad |y_2\beta - x_2|_p < \frac{C_1}{H(x_2,y_2)^\mu}.$$

Since $(d/2)+1 < \mu < d$, it follows from Lemma 2.3 that there exist positive numbers C_2 and C_3, each of which is explicitly computable in terms of C_1, μ and F, such that if $H(x_2,y_2) \geq H(x_1,y_1) \geq C_2$, then either $H(x_2,y_2) > C_3 H(x_1,y_1)^{\mu - d/2}$, or α, β and $x_1/y_1, x_2/y_2$ are connected by means of a linear fractional transformation, or both. By choosing p^k sufficiently large we can always ensure that $H(x_1,y_1) \geq C_2$. We obtain an upper bound on $H(x_2,y_2)$ by combining the inequality $|F(x_1,y_1)| \leq (d+1)H(F)H(x_1,y_1)^d$

with (3.1):

$$\begin{aligned} H(x_2,y_2) &< (C_0 h_2 p^k)^{1/(d-2.05)} \\ &\le \left(C_0 (p^k)^{1+\lambda}\right)^{1/(d-2.05)} \\ &\le \left(C_0 (h_1 p^k)^{1+\lambda}\right)^{1/(d-2.05)} \\ &= \left(C_0 |F(x_1,y_1)|^{1+\lambda}\right)^{1/(d-2.05)} \\ &\le \left(C_0 \left((d+1)H(F)H(x_1,y_1)^d\right)^{1+\lambda}\right)^{1/(d-2.05)}. \end{aligned}$$

Merging the above upper bound with the lower bound $H(x_2,y_2) > C_3 H(x_1,y_1)^{\mu-d/2}$ results in the inequality

$$C_3 H(x_1,y_1)^{\mu-d/2-d(1+\lambda)/(d-2.05)} < \left(C_0\left((d+1)H(F)\right)^{1+\lambda}\right)^{1/(d-2.05)},$$

where $\mu = (d-2.05)/(1+\lambda)$. Our goal is to ensure that the exponent of $H(x_1,y_1)$ on the left-hand side is positive, i.e.,

$$\frac{d-2.05}{1+\lambda} - \frac{d}{2} - \frac{d(1+\lambda)}{d-2.05} > 0.$$

Notice that this inequality cannot be solved for non-negative λ when $d < 7$. It does, however, admit a solution for $d \ge 7$, and in fact the above inequality is always satisfied due to our choice of λ (recall that $0 \le \lambda < f(d)$, where the function $f(d)$ is defined in (1.5)). Since the exponent of $H(x_1,y_1)$ is positive, we conclude that $H(x_1,y_1)$ is bounded. Thus, by making p^k (and therefore $H(x_1,y_1)$) sufficiently large we can always ensure that the inequality $H(x_2,y_2) > C_3 H(x_1,y_1)^{\mu-d/2}$ does not hold. Then α, β and $x_1/y_1, x_2/y_2$ are connected by means of a linear fractional transformation:

$$\beta = \frac{v\alpha - u}{-t\alpha + s} \quad \text{and} \quad \frac{x_2}{y_2} = \frac{vx_1 - uy_1}{-tx_1 + sy_1},$$

where $s,t,u,v \in \mathbb{Z}$ and $sv - tu \neq 0$. By Lemma 2.4, the matrix

$$M = \frac{1}{\sqrt{|sv-tu|}} \begin{pmatrix} s & u \\ t & v \end{pmatrix}$$

is an element of $\mathrm{Aut}'\,|F|$. Hence the number of solutions (x,y,h) to (1.6) is at most $\#\,\mathrm{Aut}'\,|F|$.

4. Proof of Theorem 1.3

The beginning of the proof is similar to the proof of Theorem 1.2. Theorem 2.6 implies that for every complex root α of $F(x,1)$ there exists a positive number C_α, which depends only on α, such that for all coprime integer pairs (x,y) with $H(x,y) > C_\alpha$ the inequality $\min\{|\alpha - x/y|, |\alpha^{-1} - y/x|\} >$

$H(x,y)^{-2.05}$ is satisfied. Furthermore, if $\alpha \notin \mathbb{R}$ and β is another complex root of $F(x,1)$, then $\beta \notin \mathbb{R}$ due to the fact that the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Consequently, the number C_α is explicitly computable in terms of α for every root α of $F(x,1)$, as long as at least one of these roots is non-real. Since

$$|F(x,y)| \leq (d+1)H(F)H(x,y)^d$$

and $|F(x,y)| = hp^z$, we have

$$\frac{p}{(d+1)H(F)} \leq \frac{hp^z}{(d+1)H(F)} = \frac{|F(x,y)|}{(d+1)H(F)} \leq H(x,y)^d.$$

Therefore, by choosing p so that $p > C_\alpha^d(d+1)H(F)$ for every complex root α of $F(x,1)$, we can ensure that $\min\{|\alpha - x/y|, |\alpha^{-1} - y/x|\} > H(x,y)^{-2.05}$ for every complex root α of $F(x,1)$.

Now, assume that there exists a solution (x,y,z,h) of (1.7). As in the proof of Theorem 1.2, for our choice of p the inequality

$$H(x,y) < (C_0 hp^z)^{1/(d-2.05)} \tag{4.1}$$

holds, where

$$C_0 = \frac{2^{d-1}d^{(d-1)/2}M(F)^{d-2}}{|D(F)|^{1/2}}.$$

Since

$$hp^z \leq (p^z)^{1+\lambda} \leq |F(x,y)|_p^{-(1+\lambda)},$$

it follows from (4.1) that

$$|F(x,y)|_p < \frac{C_0^{1/(1+\lambda)}}{H(x,y)^\mu},$$

where

$$\mu = \frac{d-2.05}{1+\lambda}.$$

Since we would like the conditions of Lemma 2.5 to be satisfied, we want to ensure that the inequality $(d/2)+1 < \mu$ holds. This inequality is satisfied if and only if $\lambda < 1 - 8.1/(d+2)$, which motivated our choice of λ in the first place. Here we can also observe the importance of the condition $d \geq 7$, as the inequality $\lambda < 1 - 8.1/(d+2)$ cannot be solved for non-negative λ when $d < 7$.

We take p sufficiently large that

$$p > |D(F)|.$$

Then

$$|F(x,y)|_p \leq p^{-1} < |D(F)|^{-1} \leq |D(F)|_p.$$

Let c_d denote the coefficient of x^d in F. By Lemma 2.2 there exists a unique p-adic root $\alpha \in \mathbb{Q}_p$ of $F(x,1)$ such that

$$|y\alpha - x|_p \leq \frac{\max\{1, |\alpha|_p\}}{|D(F)|_p^{1/2}} |F(x,y)|_p < \frac{C_1}{H(x,y)^\mu},$$

where

$$C_1 = C_0^{1/(1+\lambda)} c_d |D(F)|^{1/2}.$$

Note that C_1 is independent of p. Further, we can ensure that $p \nmid y$ by adjusting our choice of p as follows:

$$p > c_d.$$

Indeed, if $p \mid y$, then p does not divide x, because x and y are coprime. Since $z \geq 1$, it is evident from equation

$$c_d x^d + y(c_{d-1}x^{d-1} + \cdots + c_0 y^{d-1}) = \pm h p^z$$

that p divides c_d, in contradiction to our choice of p. Then $|y|_p = 1$, and so for every $\alpha \in \mathbb{Q}_p$ we have

$$\left|\alpha - \frac{x}{y}\right|_p = |y\alpha - x|_p.$$

Therefore

$$\left|\alpha - \frac{x}{y}\right|_p < \frac{C_1}{H(x,y)^\mu}.$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the roots of $F(x,1)$. Since $(d/2) + 1 < \mu < d$, we apply Lemma 2.5 and conclude that there exists a positive number C_2, which is explicitly computable in terms of $C_1, \mu, \alpha_1, \alpha_2, \ldots, \alpha_d$, such that the number of coprime integer pairs (x,y) satisfying $H(x,y) \geq C_2$ and

$$\left|\alpha_j - \frac{x}{y}\right|_p < \frac{C_1}{H(x,y)^\mu} \tag{4.2}$$

for some $j \in \{1, 2, \ldots, d\}$ is less than

$$2\#\operatorname{Aut}' |F| \cdot \left\lfloor 1 + \frac{11.51 + 1.5\log d + \log \mu}{\log(\mu - 0.5d)} \right\rfloor.$$

If we choose p so that $p \geq (d+1)H(F)C_2^d$, then

$$C_2^d \leq \frac{p}{(d+1)H(F)} \leq \frac{hp^z}{(d+1)H(F)} = \frac{|F(x,y)|}{(d+1)H(F)} \leq H(x,y)^d,$$

so the inequality $H(x,y) \geq C_2$ is satisfied. Since all solutions (x,y,z,h) to (1.7), including those that satisfy $H(x,y) \geq C_2$, also satisfy (4.2), the result follows.

5. Applications

In this section we demonstrate two applications of Theorems 1.2 and 1.3. For an integer $n > 1$, let ζ_n denote the primitive n-th root of unity, and let

$$\Phi_n(x, y) = \prod_{\substack{1 \le k < n \\ \gcd(k,n)=1}} \left(x - \zeta_n^k y\right)$$

be the n-th cyclotomic binary form. Then Φ_n has degree $d = \varphi(n)$, where $\varphi(n)$ is the Euler's totient function. Further, the Galois group of $\Phi_n(x, 1)$ has order d. Let

$$\mathbb{D}_2 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \quad \text{and} \quad \mathbb{D}_4 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Before we state our results, let us first compute the enhanced automorphism group of Φ_n.

Lemma 5.1. *Let n be a positive integer and assume that $d \ge 6$, where $d = \varphi(n)$. Then*

$$\operatorname{Aut}' |\Phi_n| = \begin{cases} \mathbb{D}_4 & \text{if } 4 \mid n, \\ \mathbb{D}_2 & \text{otherwise.} \end{cases}$$

Proof. It was proved by Fouvry and Waldschmidt [8] that

$$\operatorname{Aut} \Phi_n = \begin{cases} \mathbb{D}_4 & \text{if } 4 \mid n, \\ \mathbb{D}_2 & \text{otherwise.} \end{cases}$$

We will prove that $\operatorname{Aut}' |\Phi_n| = \operatorname{Aut} \Phi_n$. Let $M = |sv - tu|^{-1/2} \cdot \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right)$ be an element of $\operatorname{Aut}' |\Phi_n|$. Since $d \ge 6$, it follows from Lemma 2.4 that there exists a positive integer j coprime to n, with $1 \le j < n$, such that

$$\zeta_n^j = \frac{v\zeta_n - u}{-t\zeta_n + s}$$

for some $s, t, u, v \in \mathbb{Z}$ such that $sv - tu \ne 0$. At this point we consider three cases.

(1) Suppose that n is odd. Then there exists a field automorphism σ_2 in the Galois group of $\mathbb{Q}(\zeta_n)$ such that $\sigma_2(\zeta_n^\ell) = \zeta_n^{2\ell}$ for each ℓ coprime to n. Therefore,

$$\zeta_n^{2j} = \sigma_2(\zeta_n^j) = \sigma_2\left(\frac{v\zeta_n - u}{-t\zeta_n + s}\right) = \frac{v\sigma_2(\zeta_n) - u}{-t\sigma_2(\zeta_n) + s} = \frac{v\zeta_n^2 - u}{-t\zeta_n^2 + s},$$

which implies

$$\left(\frac{v\zeta_n - u}{-t\zeta_n + s}\right)^2 = \zeta_n^{2j} = \frac{v\zeta_n^2 - u}{-t\zeta_n^2 + s}.$$

We conclude that ζ_n is a root of the polynomial

$$\begin{aligned} f(x) &= (vx-u)^2(-tx^2+s) - (-tx+s)^2(vx^2-u) \\ &= (-tv^2-t^2v)x^4 + (2tu+2st)x^3 + (sv^2-s^2v-tu^2+t^2u)x^2 \\ &\quad + (-2suv-2stu)x + (su^2+s^2u), \end{aligned}$$

whose degree is at most 4. Since $d > 4$, it must be the case that $f(x)$ is identically equal to zero. Equating each of the coefficients of $f(x)$ to zero, we obtain a system of five equations in four unknowns. The only solutions to this system are $t = u = 0$, $v = s$, $s \neq 0$ and $s = v = 0$, $u = t$, $t \neq 0$. These solutions correspond to matrices $\frac{1}{|s|}\left(\begin{smallmatrix} s & 0 \\ 0 & s \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\frac{1}{|t|}\left(\begin{smallmatrix} 0 & t \\ t & 0 \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, respectively, which constitute $\mathbb{D}_2$. Hence $\mathrm{Aut}'\,|\Phi_n| = \mathbb{D}_2$.

(2) Suppose that $n \equiv 2 \pmod 4$. Then $\Phi_n(x,y) = \Phi_{n/2}(x,-y)$, meaning that $\Phi_n = (\Phi_{n/2})_S$ for $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. By the argument similar to [11, Lemma 3.3], we find that

$$\mathrm{Aut}'\,|\Phi_n| = S^{-1}(\mathrm{Aut}'\,|\Phi_{n/2}|)S = S^{-1}\mathbb{D}_2 S = \mathbb{D}_2.$$

(3) Suppose that $4 \mid n$, and assume for a contradiction that $\mathrm{Aut}'\,|\Phi_n| \neq \mathbb{D}_4$. Then it follows from [12, Lemma 7.2] that $\mathrm{Aut}'\,|\Phi_n|$ is a dihedral group of order 16 that properly contains $\mathbb{D}_4$. In particular, there must exist a matrix $M = |sv-tu|^{-1/2} \cdot \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right)$ in $\mathrm{Aut}'\,|\Phi_n|$ such that $M^2 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Solving this system of four equations for s, t, u and v, we find that $M = \pm\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. Since $(\Phi_n)_M = \pm\Phi_n$,

$$\Phi_n(x+y,-x+y) = 2^{\frac{\varphi(n)}{2}}\Phi_n(x,y)$$

for all x and y. Setting $x = 0$ and $y = 1$, we find that

$$\Phi_n(1) = \Phi_n(1,1) = 2^{\frac{\varphi(n)}{2}}\Phi_n(0,1) = 2^{\frac{\varphi(n)}{2}}.$$

However, it is well-known that $\Phi_n(1) = p$ if $n = p^k$ is a prime power with $k \geq 1$ and $\Phi_n(1) = 1$ otherwise. Since $\Phi_n(1)$ is even, we conclude that $n = 2^k$. But then $2 = \Phi_n(1) = 2^{\frac{\varphi(n)}{2}}$, meaning that $\varphi(n) = 2$. Since $d \geq 6$ and $d = \varphi(n)$, we reach a contradiction. Hence $\mathrm{Aut}'\,|\Phi_n| = \mathbb{D}_4$.

□

It follows from Lemma 5.1 that

$$\#\,\mathrm{Aut}'\,|\Phi_n| = \begin{cases} 8 & \text{if } 4 \mid n, \\ 4 & \text{otherwise.} \end{cases}$$

Combining this fact with Theorems 1.2 and 1.3 yields the following two results. Notice that in both cases the positive number C is explicitly computable in terms of Φ_n and a suitably chosen parameter λ.

Corollary 5.2. *Let n be a positive integer and assume that $d \geq 8$, where $d = \varphi(n)$. Let λ be such that $0 \leq \lambda < f(d)$, where $f(d)$ is defined in* (1.5). *Let p be prime, k a positive integer, and consider the equation*

$$\Phi_n(x, y) = hp^k, \tag{5.1}$$

where x, y and h are integer variables, with $h \geq 1$. There exists a positive number C, which is explicitly computable in terms of Φ_n and λ, such that for all $p^k > C$ the equation (5.1) *has either no solutions in integers (x, y, h) such that*

$$\gcd(x, y) = 1 \quad \textit{and} \quad 1 \leq h \leq (p^k)^\lambda,$$

or exactly eight solutions when $4 \mid n$, namely (x, y, h), $(-x, -y, h)$, (y, x, h), $(-y, -x, h)$, $(-x, y, h)$, $(x, -y, h)$, $(-y, x, h)$ and $(y, -x, h)$, or exactly four solutions otherwise, namely (x, y, h), $(-x, -y, h)$, (y, x, h) and $(-y, -x, h)$.

Corollary 5.3. *Let n be a positive integer and assume that $d \geq 8$, where $d = \varphi(n)$. Let λ be such that*

$$0 \leq \lambda < 1 - 8.1/(d + 2).$$

Let p be prime and consider the equation

$$\Phi_n(x, y) = hp^z, \tag{5.2}$$

where x, y, h and z are integer variables, with $h, z \geq 1$. There exists a positive number C, which is explicitly computable in terms of Φ_n and λ, such that for all $p > C$ the number of solutions to (5.2) *in integers (x, y, z, h) such that*

$$\gcd(x, y) = 1, \quad z \geq 1 \quad \textit{and} \quad 1 \leq h \leq (p^z)^\lambda$$

is at most

$$2a_n \left\lfloor 1 + \frac{11.51 + 1.5 \log d + \log\left((d - 2.05)/(1 + \lambda)\right)}{\log((d - 2.05)/(1 + \lambda) - 0.5d)} \right\rfloor.$$

Here $a_n = 8$ when $4 \mid n$ and $a_n = 4$ otherwise.

If we let $d = \varphi(n)$ and $\lambda(d) = 0.5 - 4.05/(d+2)$, then it is a consequence of Corollary 5.3 that the number of solutions in integers (x, y, z, h) to (5.2) does not exceed 1328 for all $d \geq 7$ and it does not exceed 48 for all $d \geq 10^{15}$.

For the next application of our results, let $n \geq 3$ be an integer, and let

$$\Psi_n(x, y) = \prod_{\substack{1 \leq k < \frac{n}{2} \\ \gcd(k,n)=1}} \left(x - 2\cos\left(\frac{2\pi k}{n}\right) y \right)$$

denote the homogenization of the minimal polynomial of $\zeta_n + \zeta_n^{-1} = 2\cos(\frac{2\pi}{n})$. Then Ψ_n has degree $d = \varphi(n)/2$. Further, the Galois group of $\Psi_n(x, 1)$ has order d [11, Lemma 3.1]. Before we state our results, let us first compute the enhanced automorphism group of Ψ_n.

Lemma 5.4. *Let n be a positive integer and assume that $d \geq 5$, where $d = \varphi(n)/2$. Then*

$$\operatorname{Aut}'|\Psi_n| = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Proof. Let $M = |sv-tu|^{-1/2} \cdot \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right)$ be an element of $\operatorname{Aut}'|\Psi_n|$. Since $d \geq 5$, it follows from Lemma 2.4 that there exists a positive integer j coprime to n, with $1 \leq j < n/2$, such that

$$2\cos\left(\frac{2\pi j}{n}\right) = \frac{2\cos\left(\frac{2\pi}{n}\right)v - u}{-2\cos\left(\frac{2\pi}{n}\right)t + s}.$$

By [11, Lemma 3.5], it must be the case that $t = u = 0$, $s = v$ and $s \neq 0$. Thus, $M = |sv - tu|^{-1/2} \cdot \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and so the result follows. □

It follows from Lemma 5.4 that $\#\operatorname{Aut}'|\Psi_n| = 2$ for every integer n such that $\varphi(n) \geq 10$. Combining this fact with Theorems 1.2 and 1.3 yields the following two results. Unlike in Corollaries 5.2 and 5.3, in both cases the number C is not explicitly computable due to the application of Roth's Theorem.

Corollary 5.5. *Let n be a positive integer and assume that $d \geq 7$, where $d = \varphi(n)/2$. Let λ be such that $0 \leq \lambda < f(d)$, where $f(d)$ is defined in* (1.5)*. Let p be prime, k a positive integer, and consider the equation*

$$|\Psi_n(x, y)| = hp^k, \tag{5.3}$$

where x, y and h are integer variables, with $h \geq 1$. There exists a positive number C, which depends only on F and λ, such that for all $p^k > C$ the equation (5.3) *has either no solutions in integers (x, y, h) such that*

$$\gcd(x, y) = 1 \quad \textit{and} \quad 1 \leq h \leq (p^k)^\lambda,$$

or exactly two solutions, namely (x, y, h) and $(-x, -y, h)$.

Corollary 5.6. *Let n be a positive integer and assume that $d \geq 7$, where $d = \varphi(n)/2$. Let λ be such that*

$$0 \leq \lambda < 1 - 8.1/(d + 2).$$

Let p be prime and consider the equation

$$|\Psi_n(x, y)| = hp^z, \tag{5.4}$$

where x, y, h and z are integer variables, with $h, z \geq 1$. There exists a positive number C, which depends only on F and λ, such that for all $p > C$ the number of solutions to (5.4) *in integers (x, y, z, h) such that*

$$\gcd(x, y) = 1, \quad z \geq 1 \quad \textit{and} \quad 1 \leq h \leq (p^z)^\lambda$$

is at most

$$4\left\lfloor 1+\frac{11.51+1.5\log d+\log\left((d-2.05)/(1+\lambda)\right)}{\log((d-2.05)/(1+\lambda)-0.5d)}\right\rfloor.$$

If we let $d=\varphi(n)/2$ and $\lambda(d)=0.5-4.05/(d+2)$, then it is a consequence of Corollary 5.6 that the number of solutions in integers (x,y,z,h) to (5.4) does not exceed 332 for all $d\geq 7$ and it does not exceed 12 for all $d\geq 10^{15}$.

References

[1] E. Bombieri, "On the Thue–Siegel–Dyson theorem", *Acta Math.* **148** (1982), p. 255-296.

[2] E. Bombieri & J. Mueller, "On effective measures of irrationality for $\sqrt[r]{a/b}$ and related numbers", *J. Reine Angew. Math.* **342** (1983), p. 173-196.

[3] E. Bombieri & W. M. Schmidt, "On Thue's equation", *Invent. Math.* **88** (1987), p. 69-81.

[4] F. Dyson, "The approximation of algebraic numbers by rationals", *Acta Math.* **79** (1947), p. 225-240.

[5] P. Erdős & K. Mahler, "On the number of integers which can be represented by a binary form", *J. Lond. Math. Soc.* **13** (1938), p. 134-139.

[6] P. Erdős, C. L. Stewart & R. Tijdeman, "Some Diophantine equations with many solutions", *Compos. Math.* **66** (1988), no. 1, p. 37-56.

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

[8] É. Fouvry & M. Waldschmidt, "Sur la représentation des entiers par les formes cyclotomiques de grand degré", *Bull. Soc. Math. Fr.* **148** (2020), no. 2, p. 253-282.

[9] D. Lewis & K. Mahler, "Representation of integers by binary forms", *Acta Arith.* **6** (1961), p. 333-363.

[10] K. Mahler, "Zur Approximation algebraischer Zahlen. II. Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen", *Math. Ann.* **108** (1933), p. 37-55.

[11] A. Mosunov, "On the automorphism group of a binary form associated with algebraic grigonometric quantities", *J. Number Theory* **240** (2022), p. 325-356.

[12] ———, "On the generalization of the gap principle", *Period. Math. Hung.* **87** (2023), no. 1, p. 119-151.

[13] K. Roth, "Rational approximations to algebraic numbers", *Mathematika* **2** (1955), no. 3, p. 1-20.

[14] C. L. Siegel, "Approximation algebraischer Zahlen", *Math. Z.* **10** (1921), p. 173-213.

[15] C. L. Stewart, "On the number of solutions of polynomial congruences and Thue equations", *J. Am. Math. Soc.* **4** (1991), p. 793-835.

[16] ———, "Cubic Thue equations with many solutions", *Int. Math. Res. Not.* **2008** (2008), article no. rnn040 (11 pages).

[17] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), p. 284-305.

[18] J. L. Thunder, "Thue equations and lattices", *Ill. J. Math.* **59** (2015), no. 4, p. 999-1023.

Anton Mosunov
Cornell University
212 Garden Avenue
Ithaca, NY 14853, USA
E-mail: am3435@cornell.edu
URL: https://math.cornell.edu/anton-mosunov