Doktori (PhD) értekezés tézisei

Binomial Thue equations, ternary equations and their applications
Binom Thue-egyenletek, ternér egyenletek és alkalmazásaik

Bazsó András

Témavezető: Dr. Bérczes Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika és Számítástudományok Doktori Iskola
Debrecen, 2010.

Doktori (PhD) értekezés tézisei

Binomial Thue equations, ternary equations and their applications
Binom Thue-egyenletek, ternér egyenletek és alkalmazásaik

Bazsó András

Témavezető: Dr. Bérczes Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika és Számítástudományok Doktori Iskola
Debrecen, 2010.

Introduction

Our PhD dissertation consists of three chapters each containing new results. These results have been published in our papers [2], [4] and [3], respectively. Here we shall give an overview of the contents of the chapters, but before doing so we make some introductory notes on the subject of our thesis.

Each of the three chapters is devoted to the study of the solutions of various important classes of diophantine equations, namely Fermat-type ternary equations, binomial Thue equations and norm form equations, respectively. The proofs of the new results in Chapters 2 and 3 use the results and techniques presented in the first chapter. This is the reason for dealing first with ternary equations of the form

$$Ax^n + By^n = Cz^m \text{ with } m \in \{2, 3, n\}, \tag{1}$$

where A, B, C are given nonzero integers, $n \geq 3$ and x, y, z are unknown integers. Equation (1) has a famous special case, namely the Fermat-equation

$$x^n + y^n = z^n$$

which has been widely studied for centuries due to Fermat's Last Theorem (FLT) which was finally proved in 1995 by Wiles [53]. The so-called modular approach that arose from the proof of Wiles for FLT, has many applications in the theory of diophantine equations, since it can be used for proving the unsolvability of (1) for several concrete values of A, B, C, n and m. For the details of the modular approach we refer to the papers of Bennett [6], Siksek [47] and the book of Stein [49].

Further central objects of our thesis are binomial Thue equations, i.e. diophantine equations of the form

$$Ax^n - By^n = C, \tag{2}$$

where A, B, C, n are nonzero integers and $n \geq 3$ is either fixed or also unknown. Thue equations and among them binomial Thue equations have a rich literature. Thue's classical ineffective result [51] on diophantine approximation of algebraic numbers implied that Thue equations have only finitely many solutions. Baker [1] was the first who gave effective upper bounds for the size of the solutions of Thue equations. Both of these results imply that equation (2) has only finitely many solutions if n is fixed. Tijdeman [52] considered the case when, in (2), the exponent n is also unknown, and gave effective upper bounds for $\max\{|x|, |y|, n\}$, where (x, y, n) are integer solutions of (2) with $|xy| > 1$. For other related results on binomial Thue equations and their applications we refer to [39], [46], [5], [34], [7], [9], [28], [10], [15], [2], [31] and the references given there.

We note that an integer solution (x, y, n) to (2) induces a solution to (1) of the type $(x, y, 1, n, m)$. So if, for some values of A, B, C, n, m, the corresponding ternary equation (1) proves to be unsolvable in integers (x, y, z) with Ax, By and Cz pairwise coprime, $|xy| > 1$, then it follows that with those values of A, B, n (2) also has no solutions (x, y).

In what follows, we briefly summarize the main results of our thesis.

1 Ternary equations

In this chapter we consider ternary Diophantine eqiations of the form

$$Ax^n + By^n = Cz^m$$

where A, B, C are nonzero integers, $m \in \{2, 3, n\}$ and x, y, z are unknown integers. The triple of integers (n, n, m) is usually referred to as the *signature* of the equation. The investigation of such ternary equations gained a high level of interest since Wiles [53] published his proof of Fermat's Last Theorem.

In Sections 1.1 and 1.2, starting from Wiles' result, we survey results on the resolution of ternary equations. Then in the rest of this chapter we present our new results on ternary equations, which will be applied, in Section 2.4, to binomial Thue equations with S-unit coefficients.

1.1 On the modular approach to ternary equations

Frey [24] observed the connection between a putative nonzero integer solution x, y, z of the equation

$$x^n + y^n = z^n \tag{3}$$

and an elliptic equation of the form

$$X(X - x^n)(X + y^n) = Y^2 \quad \text{in unknown integers } X, Y. \tag{4}$$

The Taniyama-Weil conjecture (TW) states that every rational elliptic curve is modular. In other words, every rational elliptic curve can be associated to a special Fourier series, a modular form. Wiles proved the TW conjecture for semistable elliptic curves, which implied that if there exists a semistable elliptic curve of the form (4), then there exists a modular form with level 2. However, since such modular forms do not exist, this means that for all integer solutions of (3) we have $xyz = 0$.

Equation (3) is a special case of the equation

$$Ax^n + By^n = Cz^m \text{ with } m \in \{2, 3, n\}\,. \tag{1}$$

Approaches to solve such equations, analogous to that employed by Wiles [53], can be found in numerous papers. For a survey on this topic, see papers of Bennett [6], Siksek [47] or the book of Stein [49].

The so-called *modular approach* will be used in almost all of our proofs so in this section we give its outline in virtue of the paper of Bennett [6].

1.2 On the resolution of ternary equations

For our purposes, we restrict our attention to the equation

$$Ax^n - By^n = z^m \tag{5}$$

in the cases when $m = n$ and $m = 3$.

1.2.1 The case $m = n$

The resolution of equation (5) for $AB = p^\alpha$ with a prime

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$$

and nonnegative integer α follows from the papers of Serre [45], Wiles [53], Darmon and Merel [23], and Ribet [43].

The first results on the resolution of (5) when AB has two prime factors are due to Kraus [35]. Bennett, Győry, Mignotte and Pintér [10] considered the case when $AB = 2^\alpha q^\beta$ with primes $3 \le q \le 13$. Their result was recently extended by Győry and Pintér [31] who proved that if $AB = 2^\alpha q^\beta$ with primes $3 \le q \le 29$, $\alpha \notin \{1, 2, 3, 4\}$ and n is a prime, then for every integer solutions (x, y, z, A, B, n) of equation (5) with $|xy| > 1$ and Ax, By and z pairwise coprime we have $n \le 11$. Actually, they proved a more precise statement.

In [31], Győry and Pintér also considered the case when AB has two odd prime factors. They proved that if $AB = p^\alpha q^\beta$ with primes $5 \le p < q \le 29$ and n is a prime, then apart from 10 explicitly given possible exceptions (p, q), for every solution (x, y, z, A, B, n) of (5) with $|xy| > 1$ and Ax, By and z pairwise coprime we have $n \leq 11$.

1.2.2 The case $m = 3$

In this direction we first refer to the result of Bennett, Győry, Mignotte and Pintér [10]. They proved that if $AB = p^\alpha q^\beta$ with primes $3 \leq p, q \leq 13$ and $n > 7$ is a prime coprime to pq, then equation (5) has no solutions in integers (x, y, z) with $|xy| > 1$, xy even, and Ax, By and z pairwise coprime.

The above result was generalized by Győry and Pintér [31] to the situation when n is a prime and $AB = p^\alpha q^\beta$ with primes $3 \leq p < q \leq 29$ such that either $p \leq 7$ or

$$(p, q) \in \{(11, 13), (11, 17), (11, 19), (13, 17), (13, 19), (17, 23)\}.$$

Their result implies that in this case for every solution (x, y, z, A, B, n) of (5) with $|xy| > 1, xy$ even and Ax, By and z pairwise coprime we have $n \leq 29$.

1.3 New results on ternary equations

By means of the modular method we establish new results on the solutions of equation (5) both for $m = n$ and for $m = 3$. These results will be crucial in the proof of Theorem 2.7.

Theorem 1.1 (Bazsó, 201?). *Let* $AB = 2^\alpha q^\beta$ *with a prime* $3 \leq q \leq 151$, $q \neq 31, 127$ *and with nonnegative integers* α, β. *If* n *is a prime, then for every integer solution* (x, y, z, A, B, n) *of the equation*

$$Ax^n - By^n = z^n \tag{6}$$

with $|xy| > 1$ *and with* Ax, By *and* z *pairwise coprime we have* $n \leq 53$.

Moreover, apart from 31 possible exceptions (q, n, α) *given in Table 1.1 below, for every integer solution* (x, y, z, A, B, n) *of equation* (6) *with* $|xy| > 1$ *and* Ax, By *and* z *pairwise coprime we have* $n \leq 13$.

Table 1.1

(q,n,α)	(q,n,α)	(q,n,α)	(q,n,α)	(q,n,α)
$(3,n,1)$	$(17,n,4)$	$(73,17,1)$	$(109,29,1)$	$(149,37,4)$
$(3,n,2)$	$(37,19,\alpha)$	$(73,37,\alpha)$	$(113,19,\alpha)$	$(149,41,1)$
$(3,n,3)$	$(47,23,4)$	$(83,41,4)$	$(137,17,4)$	$(151,19,\alpha)$
$(5,n,2)$	$(53,17,1)$	$(97,29,1)$	$(137,23,\alpha)$	
$(5,n,3)$	$(59,29,4)$	$(101,17,\alpha)$	$(137,29,1)$	
$(7,n,2)$	$(61,31,\alpha)$	$(103,17,4)$	$(139,23,4)$	
$(7,n,3)$	$(67,17,\alpha)$	$(107,53,4)$	$(149,17,1)$	

For $q \leq 13$ and $n > 13$, this gives Theorem 2.2 of [10]; and for $q \leq 29,\ n > 13$, this implies Theorem 3 of [31]. Further, our Theorem 1.1 can be compared with the corresponding results of [45], [53], [43] and [7].

Theorem 1.2 (Bazsó, 201?). *Let $AB = p^\alpha q^\beta$ with primes $5 \leq p, q \leq 71$ and nonnegative integers α, β. If n is a prime, then apart from 28 possible exceptions (p, q, n) given in Table 1.2 below, for every integer solution (x, y, z, A, B, n) of (6) with $|xy| > 1$ and Ax, By and z pairwise coprime we have $n \leq 13$.*

Table 1.2

(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)
$(5,7,n)$	$(17,23,n)$	$(p,47,23)$	$(17,61,31)$	$(61,67,n)$
$(7,11,n)$	$(5,37,n)$	$(17,47,n)$	$(29,61,n)$	$(7,71,n)$
$(5,13,n)$	$(5,41,n)$	$(11,53,n)$	$(31,61,17)$	$(17,71,n)$
$(7,13,n)$	$(13,41,n)$	$(5,59,n)$	$(43,61,31)$	$(43,71,17)$
$(7,17,n)$	$(23,41,n)$	$(p,59,29)$	$(5,67,17)$	
$(13,19,n)$	$(11,43,n)$	$(5,61,n)$	$(53,67,17)$	

This is a generalization of Theorem 4 of [31]. For $\max\{p, q\} \leq 29,\ n > 13$ our result possesses two exceptions (p, q, n) fewer.

Theorem 1.3 (Bazsó, 201?). *Let $AB = p^\alpha q^\beta$ with nonnegative integers α, β and primes $3 \leq p < q \leq 71$ such that $pq \leq 583$. If n is a prime, then apart from 29 possible exceptions (p, q, n) given in Table 1.3 below, for every integer solution (x, y, z, A, B, n) of the equation*

$$Ax^n - By^n = z^3 \tag{7}$$

with $|xy| > 1$, xy even and Ax, By and z pairwise coprime we have $n \leq 13$.

Table 1.3

(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)
$(11,23,17)$	$(11,31,19)$	$(7,43,19)$	$(11,47,23)$	$(5,61,31)$
$(13,23,17)$	$(3,37,19)$	$(13,43,17)$	$(3,59,29)$	$(7,61,31)$
$(11,29,17)$	$(5,37,19)$	$(3,47,23)$	$(5,59,29)$	$(3,67,17)$
$(11,29,23)$	$(7,37,19)$	$(5,47,23)$	$(7,59,19)$	$(5,67,17)$
$(13,29,19)$	$(11,37,19)$	$(7,47,23)$	$(7,59,29)$	$(7,67,17)$
$(19,29,23)$	$(13,37,19)$	$(11,47,17)$	$(3,61,31)$	

For $q \leq 13$ and $n > 13$, this gives Theorem 2.1 of [10]. Further, Theorem 1.3 is a considerable extension of Theorem 5 of [31]. Under the assumptions of Theorem 5 of [31] on p, q our result implies that if $n > 13$ is a prime, then (7) has no solutions with xy even and $|xy| > 1$, without any exception (p, q, n).

The results of this chapter will be published in our paper [3].

2 Binomial Thue equations

In this chapter we deal with binomial Thue equations. We first summarize the corresponding ineffective and effective finiteness results then we turn our attention to results on the resolution of such equations. Finally, we present our new theorems.

2.1 Introduction and finiteness results

Let us consider the Diophantine equation

$$Ax^n - By^n = C, \tag{2}$$

where A, B, C, n are nonzero integers and $n \geq 3$ is either fixed or also unknown. Equation (2) with fixed n is called a *binomial Thue equation.* We use the same terminology also for the case of unknown n. We may assume that

$$1 \leq A < B \quad \text{and} \quad \gcd(A, B) = 1. \tag{8}$$

Thue equations and generalized Thue equations have many applications in number theory, see e.g. [39], [46], [5], [34], [7], [9], [28], [10], [15], [2], [31] and the references given there. By a classical theorem of Thue [51], for fixed n, equation (2) has at most finitely many solutions in integers x, y. This result is ineffective in the sense that it does not provide any algorithm for finding the solutions. The first effective upper bounds for the size of the solutions of (2) are due to Baker [1] for n fixed. For n also unknown, Tijdeman [52] proved that $\max\{|x|, |y|, n\}$ can be still effectively bounded for every integer solution (x, y, n) of (2) with $|xy| > 1$. This effective finiteness results is extended in [27] by Győry, Pink and Pintér to the case when the numbers A, B, C are taken to be unknown S-units (i.e. all their prime factors lie in S, where S is a finite set of primes).

Using Baker's theory of linear forms in logarithms, the results of [1] and [52] have been improved several times, but even the best known upper bounds are too large for finding the solutions of (2) in concrete cases.

2.2 The resolution of binomial Thue equations

The first results on the complete resolution of equation (2) with unknown $n \geq 3$ were obtained with $C = \pm 1$. In [5], Bennett showed by means of the hypergeometric method that for $B = A + 1$, the equation

$$Ax^n - By^n = \pm 1 \tag{9}$$

has no solutions with $|xy| > 1$. In [7], [9] and [42], (2) has been resolved for some choices of the coefficients (A, B). For certain sets S of primes all solutions of (9) with S-unit coefficients A, B have been determined by Bennett [7], Bennett, Győry, Mignotte and Pintér [10], Bugeaud, Mignotte and Siksek [21], and Győry and Pintér [31]. These results, together with our related result, will be discussed in detail in Section 2.4. Now we turn to the case when, in (2), the coefficients A, B and C are bounded positive integers. This situation was first considered by Győry and Pintér in [29]. They first derived for concrete values of A, B, C a relatively sharp upper bound for n, provided that (2) has no solutions with $|xy| \leq 1$. Then they explicitly solved equation (2) in integers x, y and n with $|xy| > 1,\ n \geq 3$ for a collection of coefficients A, B, C. Under the assumptions (8) and $\max\{A, B, |C|\} \leq 10$ they gave all integer solutions (x, y, n) to (2) with $|xy| > 1, n \geq 3$ and with

$$B \pm A \neq C \quad \text{if} \quad C \geq 2. \tag{10}$$

For $C = \pm 1$, assuming (8) and $\max\{A, B\} \leq 20$, they determined all solutions (x, y, n) to equation (9) with $|xy| > 1$ and $n \geq 3$. Finally, in the case $A = |C| = 1$,

$B \leq 70$, they gave all solutions to the equation

$$x^n - By^n = \pm 1 \tag{11}$$

in integers x, y, n with $|xy| > 1$ and $n \geq 3$. Their proofs require a wide variety of powerful techniques including local arguments, some classical results in cyclotomic fields, lower bounds for linear forms in logarithms of algebraic numbers, computational methods for finding the solutions of Thue equations of small degree, the hypergeometric method and results on ternary equations based on Galois representations and modular forms. We note that these statements of [29] cannot be deduced from the results of [5], [7], [10], [21] and [31].

2.3 New results

In this section, our purpose is to extend the above-mentioned results of [29] to much larger values of A, B, C. The main novelty in our proofs is a new result of ours (Theorem 2.6) concerning the solvability of binomial Thue equations of the form (11). The use of our Theorem 2.6 is crucial in proving Theorems 2.1 and 2.2. It is important to note that in our Theorems 2.1 to 2.5 we arrived at the limit of the applicability of the currently available methods. For equation (11) we prove the following results.

Theorem 2.1 (Bazsó, Bérczes, Győry and Pintér, 2010). *If* $1 < B \leq 400$, *then all integer solutions* (x, y, n) *of equation* (11) *with* $|xy| > 1, n \geq 3$ *and with* $(B, n) \notin \{(235, 23), (282, 23), (295, 29), (329, 23), (354, 29)\}$ *are given by*

$$\begin{aligned}
& n = 3,\ (B, x, y) = (7, \pm(2,1)), (9, \pm(2,1)), (17, \pm(18,7)), (19, \pm(8,3)), \\
& \quad (20, \pm(19,7)), (26, \pm(3,1)), (63, \pm(4,1)), (91, \pm(9,2)), (124, \pm(5,1)), \\
& \quad (126, \pm(5,1)), (182, \pm(17,3)), (215, \pm(6,1)), (217, \pm(6,1)), \\
& \quad (254, \pm(19,3)), (342, \pm(7,1)), (344, \pm(7,1)), \\
& n = 4,\ (B, x, y) = (5, \pm 3, \pm 2), (15, \pm 2, \pm 1), (17, \pm 2, \pm 1), (39, \pm 5, \pm 2), \\
& \quad (80, \pm 3, \pm 1), (150, \pm 7, \pm 2), (255, \pm 4, \pm 1), \\
& n = 5,\ (B, x, y) = (31, \pm(2,1)), (242, \pm(3,1)), (244, \pm(3,1)), \\
& n = 6,\ (B, x, y) = (63, \pm 2, \pm 1), \\
& n = 7,\ (B, x, y) = (127, \pm(2,1)), (129, \pm(2,1)), \\
& n = 8,\ (B, x, y) = (255, \pm 2, \pm 1).
\end{aligned}$$

This is a considerable extension of Theorem 4 of [29]. In the proofs of our Theorems 2.1 and 2.2 the method of modular forms and Theorem 2.6 play very important roles. In Theorem 2.1, and in Theorems 2.2 to 2.5 below, there are some exceptions (B, n) resp. (A, B, n) for which our methods do not work. This is partly due to the fact that the necessary data concerning the arising modular forms of too high levels are not at our disposal.

In the next theorem we restrict ourselves to the case when B is odd. Then xy is even, which fact considerably extends the applicability of our method of proof.

Theorem 2.2 (Bazsó, Bérczes, Győry and Pintér, 2010). *(i) If* $400 < B < 800$ *is odd, then all integer solutions* (x, y, n) *of equation* (11) *with* $|xy| > 1, n \geq 3$ *and apart from the possible exceptions* (B, n) *listed in Table 2.1 below are given by*

$$\begin{aligned}
&n = 3,\ (B, x, y) = (511, \pm(8,1)), (513, \pm(8,1)), (635, \pm(361,42)),\\
&\quad (651, \pm(26,3)),\\
&n = 9,\ (B, x, y) = (511, \pm(2,1)), (513, \pm(2,1)).
\end{aligned}$$

Table 2.1

(B,n)	(B,n)	(B,n)	(B,n)	(B,n)
$(413,29)$	$(519,43)$	$(649,29)$	$(695,23)$	$(757,379)$
$(415,41)$	$(535,53)$	$(669,37)$	$(699,29)$	$(767,29)$
$(417,23)$	$(537,89)$	$(681,113)$	$(717,17)$	$(789,131)$
$(447,37)$	$(573,19)$	$(683,31)$	$(721,17)$	$(799,23)$
$(501,83)$	$(581,41)$	$(685,17)$	$(745,37)$	
$(517,23)$	$(611,23)$	$(687,19)$	$(749,53)$	

(ii) Let $800 < B < 2000$ *be odd. If* $n < 13$*, then all integer solutions* (x, y, n) *of equation* (11) *with* $|xy| > 1, n \geq 3$ *are given by*

$$\begin{aligned}
&n = 3,\ (B, x, y) = (813, \pm(28,3)),\ (999, \pm(10,1)),\ (1001, \pm(10,1)),\\
&\quad (1521, \pm(23,2)), (1657, \pm(71,6)), (1727, \pm(12,1)), (1729, \pm(12,1)),\\
&\quad (1801, \pm(73,6)), (1953, \pm(25,2))\\
&n = 5,\ (B, x, y) = (1023, \pm(4,1)), (1025, \pm(4,1)),\\
&n = 10,\ (B, x, y) = (1023, \pm 2, \pm 1), (1025, \pm 2, \pm 1).
\end{aligned}$$

If $n > 100$ is a prime, then equation (11) has no solutions in integers (x, y, n) with $|xy| > 1, n \geq 3$ and apart from the possible exceptions (B, n) listed in Table 2.2 below.

Table 2.2

(B, n)	(B, n)	(B, n)
$(1041, 173)$	$(1509, 251)$	$(1795, 179)$
$(1077, 179)$	$(1527, 127)$	$(1821, 101)$
$(1135, 113)$	$(1589, 113)$	$(1841, 131)$
$(1149, 191)$	$(1671, 139)$	$(1857, 103)$
$(1315, 131)$	$(1689, 281)$	$(1915, 191)$
$(1401, 233)$	$(1735, 173)$	$(1929, 107)$
$(1437, 239)$	$(1761, 293)$	$(1959, 163)$

In case (ii), solving equation (11) with our present methods, for $13 \leq n \leq 100$ we obtained so many exceptions that we disregard that case.

For equation (9), we have the following.

Theorem 2.3 (Bazsó, Bérczes, Győry and Pintér, 2010). *Under the assumptions (8) and $\max\{A, B\} \leq 50$, all integer solutions (x, y, n) to equation (9) with $|xy| > 1$, $n \geq 3$ and with $(A, B, n) \notin \{(21, 38, 17), (26, 41, 17), (22, 43, 17), (17, 46, 17), (31, 46, 17), (21, 38, 19)\}$ are given by*

$$\begin{aligned}
n = 3,\ (A, B, x, y) = {} & (1, 7, \pm(2, 1)), (1, 9, \pm(2, 1)), (1, 17, \pm(18, 7)), \\
& (1, 19, \pm(8, 3)), (1, 20, \pm(19, 7)), (1, 26, \pm(3, 1)), (2, 15, \pm(2, 1)), \\
& (2, 17, \pm(2, 1)), (3, 10, \pm(3, 2)), (5, 13, \pm(11, 8)), (5, 17, \pm(3, 2)), \\
& (8, 17, \pm(9, 7)), (8, 19, \pm(4, 3)), (11, 19, \pm(6, 5)) \\
n = 4,\ (A, B, x, y) = {} & (1, 5, \pm 3, \pm 2), (1, 15, \pm 2, \pm 1), (1, 17, \pm 2, \pm 1), \\
& (1, 39, \pm 5, \pm 2).
\end{aligned}$$

The next theorem can be regarded as an extension of Theorem 2.3 to the case $\max\{A, B\} \leq 100$. For $n = 17$ and 19, there are, however, many exceptions (A, B, n) when none of our methods works. Hence we consider only the situation when n is a prime greater than 19.

Theorem 2.4 (Bazsó, Bérczes, Győry and Pintér, 2010). *Let* A, B *be integers with* (8) *and with* $\max\{A, B\} \le 100$*, and let* n *be a prime.*

(i) If $n > 41$*, then equation* (9) *has no integer solutions* (x, y, n) *with* $|xy| > 1$.

(ii) If $19 < n \le 41$*, then equation* (9) *has no integer solutions* (x, y, n) *with* $|xy| > 1$*, apart from the possible exceptions* $(A, B, n) = (35, 58, 29), (8, 75, 31), (11, 76, 31), (23, 78, 31), (31, 58, 31),$ $(39, 71, 31)$ *and* $(17, 82, 41)$.

We conjecture that for $\max\{A, B\} \le 100$, equation (9) possesses only the solutions listed in Theorem 2.3.

Finally, we consider the case when C is not necessarily ± 1.

Theorem 2.5 (Bazsó, Bérczes, Győry and Pintér, 2010). *Let* A, B, C *be integers with* (8) *and* (10)*, and with* $\max\{A, B, |C|\} \le 30$*, and let* n *be a prime.*

(i) If $n > 31$*, then equation* (2) *has no integer solutions* (x, y, n) *with* $|xy| > 1$.

(ii) If $19 < n \le 31$*, then equation* (2) *has no integer solutions* (x, y, n) *with* $|xy| > 1$*, apart from the possible exceptions* $(A, B, C, n) = (1, 19, 26, 31), (1, 26, 19, 31), (2, 15, 14, 31), (2, 23, 6, 31),$ $(6, 23, 2, 31)$ *and* $(13, 21, 30, 31)$.

In [9] and [29], some special cases of our Theorems 2.1 and 2.3 were used to solve, for certain values of k and D, the equations $1^k + 2^k + \ldots + x^k = y^n$ and $x(x + 1) = Dy^n$. Here x, y and n are unknown positive integers with $n \ge 2$.

The following result, which may have independent interest, will be crucial in solving equation (11) in many cases. Let $\phi(\ )$ denote Euler's function.

Theorem 2.6 (Bazsó, Bérczes, Győry and Pintér, 2010). *Suppose that in equation* (11) n *is a prime and that each of the following conditions holds:*

(i) $n \ge 17$,

(ii) $B \le \exp\{3000\}$,

(iii) $n \nmid B\phi(B)$,

(iv) $B^{n-1} \not\equiv 2^{n-1} \pmod{n^2}$*,*

(v) $r^{n-1} \not\equiv 1 \pmod{n^2}$ *for some divisor* r *of* B*.*

Then equation (11) *has no solutions in integers* (x, y, n) *with* $|xy| > 1$*.*

We remark that our results and their proofs provide the theoretical background of a possible implementation of a binomial Thue equation solver subroutine in certain computer algebraic systems like MAGMA [18] or SAGE [50].

2.4 The case of S-unit coefficients (A new result)

We end this chapter by considering binomial Thue equations of the form (9) in which the coefficients A, B are allowed to be arbitrary large but we specify the set of their prime divisors.

Let S be a finite set of primes. We recall that an integer with no prime factors outside S is an *S-unit*. As we mentioned in Section 2.1, binomial Thue equations have finitely many solutions which can be effectively bounded even in the case when the coefficients are unknown S-units. In the sequel we restrict our attention to the equation

$$Ax^n - By^n = \pm 1 \tag{12}$$

in unknown S-units $A, B \in \mathbb{Z}$, and unknown integers x, y, n with $|xy| \geq 1$ and $n \geq 3$. For $S = \{p\}$ with a prime $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$, it follows from the work of Wiles [53], Darmon and Merel [23] and Ribet [43] on Fermat-type equations that (12) has no solutions with $|xy| > 1$ and $n \geq 3$. For $S = \{2, 3\}$, (12) was solved by Bennett [7]. His result was extended by Bennett, Győry, Mignotte and Pintér [10] to the case when $S = \{p, q\}$ with primes $2 \leq p, q \leq 13$. Independently, Bugeaud, Mignotte and Siksek [21] solved (12) in the case when, in (12), $A = 2^\alpha, B = q^\beta$ with a prime $3 \leq q < 100$, or $A = p^\alpha, B = q^\beta$ with primes $3 \leq p < q \leq 31$, and in both cases α, β are nonnegative integers. Recently, Győry and Pintér [31] generalized the results of [10] to the case when $S = \{p, q\}$ with primes $2 \leq p, q \leq 29$.

As an application of our Theorems 1.1, 1.2, 1.3 and 2.6, combining them with some other techniques, we extend the above results by studying the solutions of equation (12) in the case when $S = \{p, q\}$ with primes $2 \leq p, q \leq 71$. Although our Theorem 2.7 does not give the resolution of equation (12), we give reasonable upper bounds for n which may be useful if someone needs to solve concrete binomial Thue equations of such type.

Our result is the following.

Theorem 2.7 (Bazsó, 201?). *Let $n \geq 3$ be a prime, $S = \{p, q\}$ with primes $2 \leq p, q \leq 71$ and let A, B be coprime integer S-units with $A < B$.*

If $(A, p, q) \neq (1, 2, 31)$ and

$$(p, q) \notin \{(23, 41), (17, 47), (29, 61), (61, 67), (17, 71)\},$$

then for every integer solution (x, y, A, B, n) of equation (12) with $|xy| > 1$ we have $n \leq 31$.

Moreover,
(i) if $A = 1$ and

$$(p, q, n) \notin \{(47, q, 23), (59, q, 29), (2, 61, 31), (17, 61, 31), (43, 61, 31), (53, 67, 17)\},$$

then for every integer solution (x, y, A, B, n) of equation (12) with $|xy| > 1$ we have $n \leq 13$;
(ii) if $A > 1$ and

$$(p, q, n) \notin \{(3, 37, 19), (5, 37, 19), (3, 61, 31), (17, 61, 31), (43, 61, 31)\},$$

then for every integer solution (x, y, A, B, n) of equation (12) with $|xy| > 1$ we have $n \leq 17$.

For the exceptional (p, q, n), the methods used in the proof of Theorem 2.7 proved to be inefficient to solve equation (12) for arbitrary nonnegative integer exponents of the primes p, q. However, they work for several particular exponents. We further note that binomial Thue equations with degree at most 17 can be solved in most cases by using a powerful computer and the program packages MAGMA [18], PARI [40] or SAGE [50].

The results presented in Section 2.3 have been obtained jointly with A. Bérczes, K. Győry and Á. Pintér, and have been published in [4]. The result concerning binomial Thue equations with S-unit coefficients will be published in [3].

3 An application of binomial Thue equations

As we have pointed out in the beginning of Chapter 2, many number theoretical problems lead to (generalized) binomial Thue equations. In this chapter we present an application to norm form equations, another important type of Diophantine equations. Under some conditions, such equations have infinitely many solutions. In this case we study those solutions whose coordinates form an arithmetic progression. For a certain family of norm form equations we determine all such solutions.

3.1 On norm form equations with solutions forming arithmetic progressions

Let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ be linearly independent algebraic numbers over $\mathbb{Q}$ and put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Denote by n the degree $[K : \mathbb{Q}]$ of the field K over the rationals. Let $\sigma_1, \ldots, \sigma_n$ be the $\mathbb{Q}$-isomorphisms of K into $\mathbb{C}$. For any $\alpha \in K$ put $\alpha^{(i)} = \sigma_i(\alpha)$. Consider the linear forms

$$l^{(i)}(\underline{X}) = X_1 + \alpha_2^{(i)} X_2 + \ldots + \alpha_n^{(i)} X_n\,, \quad i = 1, \ldots, n,\ \underline{X} = (X_1, \ldots, X_n)\,.$$

Then there exists a nonnegative integer a_0 such that the form

$$F(\underline{X}) := a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m) = a_0 \prod_{i=1}^{n} l^{(i)}(\underline{X})$$

has integer coefficients. Such a form is called a *norm form*, and the equation

$$a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m) = b \tag{13}$$

is called a *norm form equation.*

We call (13) *degenerate* if the $\mathbb{Q}$-vector space generated by $\alpha_1, \ldots, \alpha_m$ has a subspace, which is proportional to a full $\mathbb{Z}$-module of an algebraic number field, different from $\mathbb{Q}$ and the imaginary quadratic fields. In this case it is easy to see, that there exists $b \in \mathbb{Z}$, such that (13) has infinitely many solutions. For non-degenerate norm form equations Schmidt [44] proved in an ineffective way that the number of their solutions is finite. For a large class of norm form equations Győry and Papp [26] gained effective finiteness results and explicit bounds for the solutions. In the sequel, from the broad literature of norm form equations we mention only those results which motivated our investigations.

The study of searching for arithmetic progressions among the solutions of norm form equations has been initiated by Attila Pethő. The problem itself first raised when Buchmann and Pethő [19] found, as a byproduct of a search for independent units, that in the field $K := \mathbb{Q}(\alpha)$ with $\alpha^7 = 3$ the integer

$$10 + 9\alpha + 8\alpha^2 + 7\alpha^3 + 6\alpha^4 + 5\alpha^5 + 4\alpha^6$$

is a unit. This means that the equation

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_6\alpha^6\right) = 1$$

has a solution $(x_0, \ldots, x_6) \in \mathbb{Z}^7$ such that the coordinates form an arithmetic progression.

This led Bérczes and Pethő in [14] to investigate in more general context norm form equations with solutions whose coordinates form an arithmetic progression. They considered the equation

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = m. \tag{14}$$

where α is an algebraic number of degree n, $K = \mathbb{Q}(\alpha)$, $m \in \mathbb{Z}$ and $\{x_0, \ldots, x_{n-1}\} \in \mathbb{Z}^n$. Put $X = \max\{|x_0|, \ldots, |x_{n-1}|\}$. The sequence $\{x_0, \ldots, x_{n-1}\}$ is said to be *nearly an arithmetic progression* if there exists $d \in \mathbb{Z}$ and $0 < \delta \in \mathbb{R}$ such that

$$|(x_i - x_{i-1}) - d| < X^{1-\delta}, \quad i = 1, \ldots, n-1. \tag{15}$$

They proved an effective finiteness result on the solutions of (14) with property (15) provided that

$$\beta := \frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$$

is an algebraic number of degree at least 3, over $\mathbb{Q}$. In the special case when $\delta = 1$ they proved a nearly complete finiteness result.

Bérczes and Pethő also considered arithmetic progressions arising from the norm form equation

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = 1.$$

In [14], they determined all such solutions when α is a zero of either $x^n - 2$ or $x^n - 3$, both with $n \geq 3$. Further they proved in [15] that there are no such solutions at all when α is a zero of the polynomial $x^n - a$, with $n \geq 3$ and $4 \leq a \leq 100$.

In the case when α is a zero of the polynomial

$$f_a(x) = x^3 - (a-1)x^2 - (a+2)x - 1, \quad a \in \mathbb{Z},$$

Bérczes, Pethő and Ziegler [16] determined all primitive solutions of the norm form inequality

$$|N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2)| \leq |2a+1|$$

such that $x_0 < x_1 < x_2$ is an arithmetic progression.

We note that arithmetic progressions may occur not only in a solution but in the solution set of a norm form equation if we consider some fixed coordinate of the solutions. For results in this direction we refer to Bérczes, Hajdu and Pethő [13].

3.2 New results

In this section our aim is to extend the result of Bérczes and Pethő [15] on equation (16).

Let α be an algebraic integer of degree $n \geq 3$, $K = \mathbb{Q}(\alpha)$, and consider the equation

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = 1 \tag{16}$$

in $x_0, \ldots, x_{n-1} \in \mathbb{Z}$. Let α be a zero of the polynomial $x^n - a$, where a is an integer such that $x^n - a$ is irreducible. As was mentioned above, Bérczes and Pethő [15] proved that equation (16) has no solution in integers forming an arithmetic progression when $4 \leq a \leq 100$. In the following theorem, we extend their result to negative values of the parameter a. More precisely, for $-100 \leq a \leq -2$ we determine all such solutions of equation (16) for which $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ are consecutive terms of an arithmetic progression.

Theorem 3.1 (Bazsó, 2007)**.** *Let $n \geq 3$ be an integer, let α be a root of the polynomial $x^n - a \in \mathbb{Z}[x]$. Put $K = \mathbb{Q}(\alpha)$ and suppose that $-100 \leq a \leq -2$. Then the only solutions of equation (16) which form an arithmetic progression are $(2,1,0)$ when $(n,a) = (3,-7)$, and $(-2,-1,0)$ when $(n,a) = (3,-9)$. In the case when $(n,a) = (11,-67)$ our result is conditional and depends on the truth of the generalized Riemann Hypothesis (GRH).*

We will deduce Theorem 3.1 from the following result concerning a special family of generalized binomial Thue-equations.

Theorem 3.2 (Bazsó, 2007)**.** *The only solutions of the generalized binomial Thue-equation*

$$X^n - aY^n = (a-1)^2 \tag{17}$$

in (n, a, X, Y) *for* $-100 \leq a \leq -2$, *are those listed in Table 3.1 below. In the case when* $(n, a) = (11, -67)$ *our result depends on the truth of the GRH.*

Table 3.1

n	a	(X, Y)
3	-97	(35, -7)
3	-63	(4, 4), (16,0), (64, -16)
3	-62	(1, 4)
3	-61	(13, 3)
3	-39	(16, -4)
3	-35	(11, -1), (46, -14)
3	-27	(10, -2)
3	-26	(3, 3), (9, 0), (27, -9)
3	-25	(1, 3)
3	-18	(-5, 3), (7, 1)
3	-12	(-11, 5)
3	-9	(7, -3)
3	-7	(-5, 3), (2, 2), (4, 0), (8, -4)
3	-6	(1, 2)
3	-3	(-2, 2)
4	-99	(-10, 0), (10, 0)
4	-80	(-9, 0), (-3, -3), (-3, 3), (3, -3), (3, 3), (9, 0)
4	-79	(-1, -3), (-1, 3), (1, -3), (1, 3)
4	-63	(-8, 0), (8, 0)
4	-48	(-7, 0), (7, 0)
4	-35	(-6, 0), (6, 0)
4	-24	(-5, 0), (5, 0)
4	-15	(-4, 0), (-2, -2), (-2, 2), (2, -2), (2, 2), (4, 0)
4	-14	(-1, -2), (-1, 2), (1, -2), (1, 2)
4	-8	(-3, 0), (3, 0)
4	-3	(-2, 0), (2, 0)

Table 3.1 (Continued)

n	a	(X,Y)
5	-31	(2, 2), (4, 0), (8, -4)
5	-30	(1, 2)
6	-63	(2, 2), (-2, -2), (2, -2), (-2, 2), (4, 0), (-4, 0)
6	-26	(3, 0), (-3, 0)
6	-7	(2, 0), (-2, 0)
8	-80	(3, 0), (-3, 0)
8	-15	(2, 0), (-2, 0)
10	-31	(2, 0), (-2, 0)
12	-63	(2, 0), (-2, 0)

The results of the third chapter are published in [2].

Bevezetés

Értekezésem három fejezetből áll, melyekben a [2], [3] és [4] (részben társszerzős) cikkeimben közölt eredményeket ismertetem. A következőkben egy rövid bevezetőt követően összefoglalom az egyes fejezetekben szereplő eredményeket.

Mindhárom fejezetben nevezetes diofantikus egyenletek, nevezetesen Fermat-típusú ternér-, binom Thue- illetve norma forma egyenletek megoldásaival foglalkozunk. Az egyes fejezetek az egymásra épülés elve alapján követik egymást. Először az

$$Ax^n + By^n = Cz^m, \quad m \in \{2, 3, n\} \tag{1}$$

alakú ternér egyenletek megoldásaival foglalkozunk, ahol A, B és C nemnulla egészek, $n \geq 3$ és x, y, z pedig ismeretlen egészek. Az (1) egyenlet egy speciális esete az

$$x^n + y^n = z^n$$

ún. Fermat-egyenlet, amely a híres Fermat-sejtés miatt évszázadokon át vizsgálat tárgyát képezte. Fermat sejtése szerint ezen egyenletnek $n \geq 3$ esetén nincs nemnulla egészekből álló megoldása. E sejtést végül 1995-ben Wiles [53] igazolta. Bizonyításának módszere, az ún. moduláris módszer számos konkrét A, B, C, n és m esetén alkalmazható annak bizonyítására, hogy az (1) egyenletnek nincs olyan x, y, z egész megoldása, melyre $|xy| > 1$ teljesül. A módszer részletes leírása megtalálható Bennett [6] és Siksek [47] cikkeiben, illetve Stein [49] könyvében.

Dolgozatunkban központi szerepet játszanak a binom Thue-egyenletek, azaz az

$$Ax^n - By^n = C, \tag{2}$$

alakú diofantikus egyenletek, ahol A, B, C, n nemnulla egészek és $n \geq 3$ rögzített vagy ismeretlen egész. A Thue- illetve binom Thue-egyenletek irodalma meglehetősen gazdag. Thue [51] algebrai számok diofantikus approximációjára vonatkozó klasszikus ineffektív eredményéből következik, hogy Thue-egyenleteknek csak véges sok megoldása lehet. Baker [1] adott először effektív felső korlátot Thue-egyenletek megoldásainak a méretére. Mindkét eredményből következik, hogy a (2) egyenletnek is csak véges sok megoldása lehet rögzített n esetén. Tijdeman [52] ismeretlen n kitevő esetén effektív korlátot adott $\max\{|x|, |y|, n\}$ értékére, ahol (x, y, n) a (2) egy olyan megoldása, melyre $|xy| > 1$. További, binom Thue-egyenletekkel és alkalmazásaikkal kapcsolatos eredmények találhatók a [39], [46], [5], [34], [7], [9], [28], [10], [15], [2], [31] dolgozatokban és az ezekben hivatkozott munkákban.

Vegyük észre, hogy (2) egy (x, y, n) megoldásából az (1) egyenlet egy $(x, y, 1, n, m)$ alakú megoldását nyerjük. Így ha sikerül igazolnunk, hogy valamely A, B, C, n, m esetén a megfelelő (1) ternér egyenletnek nincs olyan (x, y, z) megoldása, melyre Ax, By és Cz páronként relatív prímek és $|xy| > 1$, akkor ugyanazon A, B, n esetén (2)-nek szintén nincs $|xy| > 1$ tulajdonságú megoldása.

A továbbiakban az egyes fejezetek főbb eredményeit ismertetjük.

1. Ternér egyenletek

Ebben a fejezetben

$$Ax^n + By^n = Cz^m$$

alakú ternér egyenletekkel foglalkozunk, ahol A, B, C nemnulla egészek, $m \in \{2, 3, n\}$ és x, y, z ismeretlen egészek. Az (n, n, m) számhármast a ternér egyenlet *szignatúrájának* nevezzük. Az ilyen egyenletek vizsgálata nagy lendületet kapott, mióta Wiles [53] publikálta a Fermat-sejtésre adott bizonyítását.

Az 1.1 és 1.2 szakaszokban áttekintjük a ternér egyenletek megoldásával kapcsolatos eredményeket. A fejezet további részében a ternér egyenletekre vonatkozó új eredményeinket tárgyaljuk, melyeket a 2.4 szakaszban S-egység együtthatós binom Thue-egyenletek megoldása során fogunk alkalmazni.

1.1. A moduláris módszer alkalmazása ternér egyenletekre

Frey [24] vette észre, hogy az

$$x^n + y^n = z^n \tag{3}$$

egyenlet egy feltételezett nullától különböző x, y, z megoldásához hozzárendelhető az

$$X(X - x^n)(X + y^n) = Y^2 \tag{4}$$

elliptikus egyenlet, ahol X, Y ismeretlen egészek. A Taniyama-Weil (TW) sejtés szerint minden racionális elliptikus görbe moduláris. Más szóval, minden racionális elliptikus görbéhez hozzárendelhető egy speciális Fourier sor: egy moduláris forma. Wiles belátta a TW-sejtést félig stabil elliptikus görbékre, amiből következik, hogy ha létezik (4) alakú félig stabil elliptikus görbe, akkor létezik 2 szintű moduláris forma. Azonban, mivel ilyen moduláris formák nincsenek, ez azt jelenti, hogy (3) bármely megoldására $xyz = 0$ teljesül.

A (3) egyenlet az

$$Ax^n + By^n = Cz^m, \quad m \in \{2, 3, n\} \tag{1}$$

egyenlet egy speciális esete. Ilyen egyenletek Wileséval [53] analóg módszerrel történő megoldásával számos cikkben találkozhatunk. E téma bővebb áttekintése található Bennett [6] illetve Siksek [47] dolgozatában és Stein [49] könyvében.

Mivel az ún. *moduláris technikát* majdnem minden bizonyításunkban alkalmazzuk, ebben a szakaszban Bennett [6] dolgozata alapján leírjuk a lényegét.

1.2. Ternér egyenletek megoldásáról

A fejezet további részében az

$$Ax^n - By^n = z^m \tag{5}$$

egyenlet megoldásaira koncentrálunk az $m = n$ ill. $m = 3$ esetekben.

1.2.1. Az $m = n$ eset

Serre [45], Wiles [53], Darmon és Merel [23], és Ribet [43] munkái alapján ismert az (5) egyenlet összes megoldása abban az esetben, ha $AB = p^\alpha$, ahol p egy prím, amelyre $p \leq 29$ vagy $p = 53, 59$.

Kraus [35] vizsgálta először azt az esetet, amikor (5)-ben AB-nek két prímosztója van. Bennett, Győry, Mignotte és Pintér [10] megoldották (5)-öt $n > 7$ prím és $AB = 2^\alpha q^\beta$ esetén, ha $3 \leq q \leq 13$ egy prím. Győry és Pintér [31] nemrég általánosították ezt az eredményt a $3 \leq q \leq 29$ esetre. Pontosabban belátták, hogy 8 kivételes (q, α)-tól eltekintve az (5) egyenlet minden olyan (x, y, z, A, B, n) megoldására, melyre $|xy| > 1$, és Ax, By, z páronként relatív prímek, teljesül, hogy $n \leq 11$.

[31]-ben Győry és Pintér foglalkozott azzal az esettel is, amikor AB két páratlan prímhatvány szorzata. Belátták, hogy ha $AB = p^\alpha q^\beta$, ahol $5 \leq p < q \leq 29$ prímek és ezenfelül n is prím, akkor 10 megadott (p, q) lehetséges kivételtől eltekintve az (5) egyenlet minden olyan (x, y, z, A, B, n) megoldására, ahol $|xy| > 1$, és Ax, By, z páronként relatív prímek, $n \leq 11$ teljesül.

1.2.2. Az $m = 3$ eset

Először Bennett, Győry, Mignotte és Pintér [10] eredményére hivatkozunk, akik belátták hogy ha $AB = p^\alpha q^\beta$, ahol $3 \leq p, q \leq 13$ prímek, továbbá $n > 7$ egy prím, amely nem osztja pq-t, akkor az (5) egyenletnek nincs olyan (x, y, z) egész megoldása, melyre $|xy| > 1$, xy páros, és Ax, By, z páronként relatív prímek.

Ezt az eredményt Győry és Pintér [31] kiterjesztette arra az esetre, amikor n prím és $AB = p^\alpha q^\beta$ ahol $3 \leq p < q \leq 29$ olyan prímek, melyekre vagy $p \leq 7$ vagy

$$(p, q) \in \{(11, 13), (11, 17), (11, 19), (13, 17), (13, 19), (17, 23)\}.$$

Tételükből következik, hogy ekkor az (5) bármely (x, y, z, A, B, n) megoldására, melyre $|xy| > 1$, xy páros, és Ax, By, z páronként relatív prímek, teljesül, hogy $n \leq 29$.

1.3. Ternér egyenletekre vonatkozó új eredmények

Ebben a szakaszban a moduláris módszer alkalmazásával új eredményeket bizonyítunk az (5) megoldásaira mind $m = n$, mind $m = 3$ esetén. Az alábbi tételeink meghatározóak lesznek a 2.7 Tétel bizonyításában.

1.1. Tétel. *[Bazsó, 201?] Legyen $AB = 2^\alpha q^\beta$, ahol q egy prím, melyre $3 \leq q \leq 151$, $q \neq 31, 127$, továbbá legyenek α, β nemnegatív egészek. Ha n prím, akkor a*

$$Ax^n - By^n = z^n \tag{6}$$

egyenlet minden olyan (x, y, z, A, B, n) megoldására, amelyre $|xy| > 1$, és Ax, By, z páronként relatív prímek, $n \leq 53$ teljesül. Továbbá, az alábbi 1.1 táblázatban szereplő 31 lehetséges (q, n, α) kivételtől eltekintve a (6) egyenlet minden olyan (x, y, z, A, B, n) megoldására, amelyre $|xy| > 1$, és Ax, By, z páronként relatív prímek, $n \leq 13$ teljesül.

1.1 táblázat

(q,n,α)	(q,n,α)	(q,n,α)	(q,n,α)	(q,n,α)
$(3,n,1)$	$(17,n,4)$	$(73,17,1)$	$(109,29,1)$	$(149,37,4)$
$(3,n,2)$	$(37,19,\alpha)$	$(73,37,\alpha)$	$(113,19,\alpha)$	$(149,41,1)$
$(3,n,3)$	$(47,23,4)$	$(83,41,4)$	$(137,17,4)$	$(151,19,\alpha)$
$(5,n,2)$	$(53,17,1)$	$(97,29,1)$	$(137,23,\alpha)$	
$(5,n,3)$	$(59,29,4)$	$(101,17,\alpha)$	$(137,29,1)$	
$(7,n,2)$	$(61,31,\alpha)$	$(103,17,4)$	$(139,23,4)$	
$(7,n,3)$	$(67,17,\alpha)$	$(107,53,4)$	$(149,17,1)$	

Megjegyezzük, hogy $q \leq 13,\ n > 13$ esetén, állításunk ekvivalens a [10]-beli Theorem 2.2-vel, illetve $q \leq 29,\ n > 13$ esetén, állításunkból következik a [31]-beli Theorem 3, továbbá az 1.1 Tételünk a [45], [53], [43] és [7]-beli megfelelő eredmények kiterjesztésének is tekinthető.

1.2. Tétel. *[Bazsó, 201?] Legyen* $AB = p^{\alpha}q^{\beta}$, *ahol* $5 \leq p, q \leq 71$ *prímek és* α, β *nemnegatív egészek. Ha* n *prím, akkor az alábbi 1.2 táblázatban szereplő 28 lehetséges* (p,q,n) *kivételtől eltekintve a (6) egyenlet minden olyan* (x,y,z,A,B,n) *megoldására, melyre* $|xy| > 1$, *és* Ax, By, z *páronként relatív prímek,* $n \leq 13$ *teljesül.*

1.2 táblázat

(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)
$(5,7,n)$	$(17,23,n)$	$(p,47,23)$	$(17,61,31)$	$(61,67,n)$
$(7,11,n)$	$(5,37,n)$	$(17,47,n)$	$(29,61,n)$	$(7,71,n)$
$(5,13,n)$	$(5,41,n)$	$(11,53,n)$	$(31,61,17)$	$(17,71,n)$
$(7,13,n)$	$(13,41,n)$	$(5,59,n)$	$(43,61,31)$	$(43,71,17)$
$(7,17,n)$	$(23,41,n)$	$(p,59,29)$	$(5,67,17)$	
$(13,19,n)$	$(11,43,n)$	$(5,61,n)$	$(53,67,17)$	

Ez a [31]-beli Theorem 4 kiterjesztése, ráadásul $\max\{p,q\} \leq 29,\ n > 13$ esetén állításunkban kettővel kevesebb (p,q,n) kivétel szerepel.

1.3. Tétel. *[Bazsó, 201?] Legyen* $AB = p^\alpha q^\beta$*, ahol* α, β *nemnegatív egészek és* $3 \le p < q \le 71$ *olyan prímek, melyekre* $pq \le 583$*. Ha* n *prím, akkor az alábbi 1.3 táblázatban szereplő 29 lehetséges* (p, q, n) *kivételtől eltekintve az*

$$Ax^n - By^n = z^3 \tag{7}$$

egyenlet minden olyan (x, y, z, A, B, n) *megoldására, melyre* $|xy| > 1$*,* xy *páros, és* Ax, By, z *páronként relatív prímek, teljesül, hogy* $n \le 13$*.*

1.3 táblázat

(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)	(p,q,n)
$(11,23,17)$	$(11,31,19)$	$(7,43,19)$	$(11,47,23)$	$(5,61,31)$
$(13,23,17)$	$(3,37,19)$	$(13,43,17)$	$(3,59,29)$	$(7,61,31)$
$(11,29,17)$	$(5,37,19)$	$(3,47,23)$	$(5,59,29)$	$(3,67,17)$
$(11,29,23)$	$(7,37,19)$	$(5,47,23)$	$(7,59,19)$	$(5,67,17)$
$(13,29,19)$	$(11,37,19)$	$(7,47,23)$	$(7,59,29)$	$(7,67,17)$
$(19,29,23)$	$(13,37,19)$	$(11,47,17)$	$(3,61,31)$	

Megjegyezzük, hogy $q \le 13$, $n > 13$ esetén állításunk ekvivalens a [10]-beli Theorem 2.1-gyel. Továbbá az 1.3 Tétel a [31]-beli Theorem 5 lényeges kiterjesztése, ugyanis az említett tétel p, q-ra vonatkozó feltételei mellett állításunkból következik, hogy ha $n > 13$ prím, akkor a (7) egyenletnek nincs olyan megoldása, melyre xy páros és $|xy| > 1$. Ekkor nincsenek kivételes (p, q, n)-ek.

Az első fejezetben szereplő eredményeink a [3] cikkünkben fognak megjelenni.

2. Binom Thue-egyenletek

Ebben a fejezetben binom Thue-egyenletek megoldásával foglalkozunk. A korábbi eredmények ismertetése után bemutatjuk saját eredményeinket.

2.1. Bevezetés és végességi eredmények

Tekintsük az

$$Ax^n - By^n = C, \tag{2}$$

diofantikus egyenletet, ahol A, B, C, n nemnulla egészek és $n \ge 3$ rögzített vagy ismeretlen. Rögzített n esetén (2) egy binom Thue-egyenlet. Ezt az elnevezést használjuk ismeretlen n esetére is. Az általánosság megszorítása nélkül feltehető, hogy

$$1 \leq A < B \quad \text{és} \quad \gcd(A, B) = 1. \tag{8}$$

A Thue-egyenleteknek és általánosított Thue-egyenleteknek számos számelméleti alkalmazása található pl. a [39], [46], [5], [34], [7], [9], [28], [10], [15], [2] és [31] dolgozatokban és az ezekben található hivatkozásokban. Mint említettük, Thue [51] híres eredményéből következik, hogy rögzített n-re (2)-nek csak véges sok x, y egész megoldása lehet. Ez az eredmény ineffektív abban az értelemben, hogy nem ad semmilyen algoritmust a megoldások megkeresésére. Az első effektív felső korlátok (2) megoldásainak a méretére Bakertől [1] származnak rögzített n esetén. Tijdeman [52] effektív korlátot nyert $\max\{|x|, |y|, n\}$ értékére, amikor n szintén ismeretlen, és (x, y, n) olyan megoldása (2)-nek, melyre $|xy| > 1$. Győry, Pink és Pintér [27] kiterjesztette ezt az effektív végességi eredményt arra az esetre, amikor az A, B, C együtthatók ismeretlen S-egységek. A Baker-módszer továbbfejlesztésével sokan javították [1] illetve [52] eredményeit, de konkrét esetben még a legélesebb korlátok is túl nagyok (2) teljes megoldásához.

2.2. Binom Thue-egyenletek megoldása

Ismeretlen $n \geq 3$ kitevővel a (2) egyenletet először $C = \pm 1$ esetén oldották meg. Bennett [5] a $B = A + 1$ esetben a hipergeometrikus módszer segítségével megmutatta, hogy az

$$Ax^n - By^n = \pm 1 \tag{9}$$

egyenletnek nincs $|xy| > 1$ tulajdonságú megoldása. A [7], [9] és [42] dolgozatokban megoldották (2)-t bizonyos (A, B) együtthatókkal. Prímszámok különböző S halmazai és S-egység A, B együtthatók esetén ismert (9) összes megoldása Bennett [7], Bennett, Győry, Mignotte és Pintér [10], Bugeaud, Mignotte és Siksek [21], és Győry és Pintér [31] munkái alapján. Ezeket az eredményeket a kapcsolódó új eredményünkkel együtt a 2.4 szakaszban fogjuk tárgyalni. Tekintsük most a (2) egyenletet korlátos egész A, B, C együtthatókkal. Ezt az esetet először Győry és Pintér [29] vizsgálta. Egy - a 2.4 szakaszban tárgyalt - lokális módszerrel sikerült konkrét A, B, C értékek mellett viszonylag éles felső korlátot adniuk n-re, feltéve, hogy a (2) egyenletnek nincs triviális, $|xy| \leq 1$ tulajdonságú megoldása. Továbbá, természetes feltételek mellett meghatározták a (2) összes $|xy| > 1$ tulajdonságú megoldását az együtthatókra vonatkozó különböző felső korátok esetén. A (8) ill.

$\max\{A, B, |C|\} \leq 10$ feltételek mellett megadták (2) összes (x, y, n) megoldását, melyre $|xy| > 1, n \geq 3$ és

$$B \pm A \neq C, \quad \text{ha} \quad C \geq 2. \tag{10}$$

A $C = \pm 1$, (8) és $\max\{A, B\} \leq 20$ feltételek mellett sikerült megoldaniuk a (9) egyenletet is, továbbá az $A = |C| = 1$, $B \leq 70$ esetben, meghatározták az

$$x^n - By^n = \pm 1 \tag{11}$$

egyenlet összes $|xy| > 1$, $n \geq 3$ tulajdonságú megoldását. Bizonyításaikban számos mély módszert használtak, pl. a lokális-, a hipergeometrikus- illetve a Baker-módszert, bizonyos körosztási testekkel kapcsolatos eredményeket, alacsony fokú Thue-egyenletekre vonatkozó számítógépes eljárásokat és a moduláris technikát. Megjegyezzük, hogy a [29]-beli tételek nem következnek az [5], [7], [10], [21] és [31]-beli eredményekből.

2.3. Új eredmények

Ebben a szakaszban jelentősen kiterjesztjük az említett [29]-beli eredményeket nagyobb A, B, C értékekre. Bizonyításaink újdonságát a 2.6 Tételünk adja, amely (11) alakú binom Thue-egyenletek megoldhatóságára vonatkozik, és amely nélkül a 2.1 és 2.2 Tételeinket nem tudnánk bizonyítani. Megjegyezzük, hogy a 2.1-2.5 Tételeinkben elértük a jelenlegi módszereink alkalmazhatóságának a határát. Először tekintsük a (11) egyenletet.

2.1. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] Ha* $1 < B \leq 400$, *akkor a* (11) *egyenlet összes* (x, y, n) *megoldásai, melyekre* $|xy| > 1, n \geq 3$ *és* $(B, n) \notin \{(235, 23), (282, 23), (295, 29), (329, 23), (354, 29)\}$ *a következők:*

$$\begin{aligned} n = 3,\ (B, x, y) = {} & (7, \pm(2, 1)), (9, \pm(2, 1)), (17, \pm(18, 7)), (19, \pm(8, 3)), \\ & (20, \pm(19, 7)), (26, \pm(3, 1)), (63, \pm(4, 1)), (91, \pm(9, 2)), (124, \pm(5, 1)), \\ & (126, \pm(5, 1)), (182, \pm(17, 3)), (215, \pm(6, 1)), (217, \pm(6, 1)), \\ & (254, \pm(19, 3)), (342, \pm(7, 1)), (344, \pm(7, 1)), \end{aligned}$$

$n = 4,\ (B,x,y) = (5,\pm3,\pm2),(15,\pm2,\pm1),(17,\pm2,\pm1),(39,\pm5,\pm2),$
$(80,\pm3,\pm1),(150,\pm7,\pm2),(255,\pm4,\pm1),$
$n = 5,\ (B,x,y) = (31,\pm(2,1)),(242,\pm(3,1)),(244,\pm(3,1)),$
$n = 6,\ (B,x,y) = (63,\pm2,\pm1),$
$n = 7,\ (B,x,y) = (127,\pm(2,1)),(129,\pm(2,1)),$
$n = 8,\ (B,x,y) = (255,\pm2,\pm1).$

E tételünk jelentős mértékben kiterjeszti a [29]-beli Theorem 4 állítását. A 2.1 ill. 2.2 Tételeink bizonyításában a moduláris technika és a 2.6 Tétel fontos szerepet játszik. Tételeinkben szerepelnek bizonyos (B,n) ill. (A,B,n) kivételek, amelyekre módszereink egyike sem működik. Ennek részben az az oka, hogy túl magas szintű moduláris formák együtthatóit nem tudjuk a jelenlegi számítógépes eljárásokkal kiszámolni.

A következő tételben csak páratlan B értékeket tekintünk. Ekkor xy szükségképpen páros, ami jelentősen megnöveli a bizonyítás módszerének alkalmazhatóságát.

2.2. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] (i) Ha* $400 < B < 800$ *páratlan, és* (B,n) *nem szerepel a 2.1 táblázatban, akkor a* (11) *egyenlet összes* $(x,y,n), |xy| > 1, n \geq 3$ *tulajdonságú megoldásai a következők:*

$n = 3,\ (B,x,y) = (511,\pm(8,1)),(513,\pm(8,1)),(635,\pm(361,42)),$
$(651,\pm(26,3)),$
$n = 9,\ (B,x,y) = (511,\pm(2,1)),(513,\pm(2,1)).$

2.1 táblázat

(B,n)	(B,n)	(B,n)	(B,n)	(B,n)
$(413,29)$	$(519,43)$	$(649,29)$	$(695,23)$	$(757,379)$
$(415,41)$	$(535,53)$	$(669,37)$	$(699,29)$	$(767,29)$
$(417,23)$	$(537,89)$	$(681,113)$	$(717,17)$	$(789,131)$
$(447,37)$	$(573,19)$	$(683,31)$	$(721,17)$	$(799,23)$
$(501,83)$	$(581,41)$	$(685,17)$	$(745,37)$	
$(517,23)$	$(611,23)$	$(687,19)$	$(749,53)$	

(ii) Legyen $800 < B < 2000$ *páratlan. Ha* $n < 13$*, akkor a* (11) *egyenlet összes* (x, y, n)*,* $|xy| > 1$*,* $n \geq 3$ *tulajdonságú megoldásai*

$$\begin{aligned}
&n = 3,\ (B, x, y) = (813, \pm(28, 3))\,,\ (999, \pm(10, 1))\,,\ (1001, \pm(10, 1))\ ,\\
&\quad (1521, \pm(23, 2))\,, (1657, \pm(71, 6))\,, (1727, \pm(12, 1))\,, (1729, \pm(12, 1)),\\
&\quad (1801, \pm(73, 6))\,, (1953, \pm(25, 2))\\
&n = 5,\ (B, x, y) = (1023, \pm(4, 1))\,, (1025, \pm(4, 1))\,,\\
&n = 10,\ (B, x, y) = (1023, \pm 2, \pm 1)\,, (1025, \pm 2, \pm 1)\,.
\end{aligned}$$

Ha $n > 100$ *egy prím, akkor eltekintve a 2.2 táblázatbeli lehetséges* (B, n) *kivételektől, a* (11) *egyenletnek nincs* $(x, y, n), |xy| > 1, n \geq 3$ *tulajdonságú megoldása.*

2.2 táblázat

(B, n)	(B, n)	(B, n)
$(1041, 173)$	$(1509, 251)$	$(1795, 179)$
$(1077, 179)$	$(1527, 127)$	$(1821, 101)$
$(1135, 113)$	$(1589, 113)$	$(1841, 131)$
$(1149, 191)$	$(1671, 139)$	$(1857, 103)$
$(1315, 131)$	$(1689, 281)$	$(1915, 191)$
$(1401, 233)$	$(1735, 173)$	$(1929, 107)$
$(1437, 239)$	$(1761, 293)$	$(1959, 163)$

A (ii) esetben, a $13 \leq n \leq 100$ kitevőjű (11) egyenletek megoldásától eltekintünk, mivel ekkor megnő a fellépő kivételek száma.

Tekintsük az (9) egyenletet.

2.3. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] Az* $1 \leq A < B \leq 50$ *és a* (8) *feltételek mellett, a* (9) *egyenlet összes olyan* $(x, y, n), |xy| > 1, n \geq 3$ *megoldásai, amelyekre* $(A, B, n) \notin \{(21, 38, 17)\,, (26, 41, 17)\,, (22, 43, 17)\,, (17, 46, 17)\,, (31, 46, 17), (21, 38, 19)$ *a következők:*

$$\begin{aligned}
&n = 3,\ (A, B, x, y) = (1, 7, \pm(2, 1))\,, (1, 9, \pm(2, 1))\,, (1, 17, \pm(18, 7))\,,\\
&\quad (1, 19, \pm(8, 3))\,, (1, 20, \pm(19, 7))\,, (1, 26, \pm(3, 1))\,, (2, 15, \pm(2, 1))\,,\\
&\quad (2, 17, \pm(2, 1))\,, (3, 10, \pm(3, 2))\,, (5, 13, \pm(11, 8))\,, (5, 17, \pm(3, 2))\,,\\
&\quad (8, 17, \pm(9, 7))\,, (8, 19, \pm(4, 3))\,, (11, 19, \pm(6, 5))
\end{aligned}$$

$n=4,\ (A,B,x,y)=(1,5,\pm 3,\pm 2),(1,15,\pm 2,\pm 1),(1,17,\pm 2,\pm 1),$
$(1,39,\pm 5,\pm 2).$

A következő tételünk a 2.3 Tétel kiterjesztésének tekinthető $\max\{A,B\}\le 100$ együtthatókra. Az $n=17,19$ kitevők esetén fellépő kivételek miatt azonban csak $n>19$ prím kitevőket vizsgálunk.

2.4. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] Legyenek A,B olyan egészek, melyekre* $\max\{A,B\}\le 100$ *és* (8) *teljesül, és legyen n prím. Ekkor*

(i) ha $n>41$, akkor a (9) *egyenletnek nincs olyan (x,y,n) megoldása, melyre $|xy|>1$.*

(ii) ha $19<n\le 41$, *akkor az* $(A,B,n)=(35,58,29),(8,75,31),(11,76,31),$ $(23,78,31),(31,58,31),(39,71,31)$ *és* $(17,82,41)$ *lehetséges kivételektől eltekintve a* (9) *egyenletnek nincs olyan (x,y,n) megoldása, melyre $|xy|>1$.*

Sejtésünk szerint $\max\{A,B\}\le 100$ esetén (9) összes megoldása a 2.3 Tételben felsorolt megoldások közül kerül ki.

Végül tekintsük azt az esetet, amikor C nem feltétlenül ± 1.

2.5. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] Legyenek A,B,C olyan egészek, melyekre* $\max\{A,B,|C|\}\le 30$, (8) *és* (10) *teljesül, továbbá legyen n prím. Ekkor*

(i) ha $n>31$, akkor a (2) *egyenletnek nincs olyan (x,y,n) megoldása, melyre $|xy|>1$.*

(ii) ha $19<n\le 31$, *akkor eltekintve az* $(A,B,C,n)=(1,19,26,31),(1,26,$ $19,31),(2,15,14,31),(2,23,6,31),(6,23,2,31)$ *és* $(13,21,30,31)$ *lehetséges kivételektől a* (2) *egyenletnek nincs olyan (x,y,n) megoldása, melyre $|xy|>1$.*

A [9] és [29] dolgozatokban a 2.1 ill. 2.3 Tételeink bizonyos speciális esetei segítségével különböző k és D értékekre megoldották az $1^k+2^k+\ldots+x^k=y^n$ és $x(x+1)=Dy^n$ egyenleteket, amelyben x,y és $n\ge 2$ ismeretlen pozitív egészek.

Az alábbi önmagában is érdekes eredményünk kulcsfontosságú a (11) alakú egyenletek megoldásában. Jelölje $\phi(\ )$ az Euler-féle függvényt.

2.6. Tétel. *[Bazsó, Bérczes, Győry és Pintér, 2010] Tegyük fel, hogy a* (11) *egyenletben n prím és hogy az alábbi feltételek mindegyike teljesül:*

(i) $n \geq 17$,

(ii) $B \leq \exp\{3000\}$,

(iii) $n \nmid B\phi(B)$,

(iv) $B^{n-1} \not\equiv 2^{n-1} \pmod{n^2}$,

(v) $r^{n-1} \not\equiv 1 \pmod{n^2}$ *valamely $r|B$ esetén.*

Ekkor (11)*-nek nincs olyan (x, y, n) megoldása, melyre $|xy| > 1$.*

Megjegyezzük, hogy a fent említett eredményeink és bizonyításaik elméleti hátteret szolgáltatnak egy lehetséges binom Thue-egyenlet megoldó rutin megírásához egy olyan komputeralgebrai programcsomagban, mint a MAGMA [18] vagy a SAGE [50].

2.4. S-egység együtthatós binom Thue-egyenletek

Tekintsük most azt az esetet, amikor a (9) egyenletben az A, B együtthatóknak csak a prímosztóit rögzítjük.

Legyen S prímszámok egy véges halmaza. Egy egész szám S-egység, ha nincs S-en kívüli prímosztója. Ahogy a 2.1 szakaszban említettük, binom Thue-egyenleteknek csak véges sok megoldásuk van és ezekre effektív felső korlát adható akkor is, ha az együtthatók ismeretlen S-egységek. A továbbiakban

$$Ax^n - By^n = \pm 1 \tag{12}$$

alakú egyenletekkel foglalkozunk, melyben $A, B \in \mathbb{Z}$ ismeretlen S-egységek, és x, y, n ismeretlen egészek, melyekre $|xy| \geq 1$ és $n \geq 3$ teljesül. Ha $S = \{p\}$ és $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$, a (12) egyenletnek nincs $|xy| > 1, n \geq 3$ tulajdonságú megoldása Wiles [53], Darmon és Merel [23] és Ribet [43] ternér egyenletekre vonatkozó eredményei alapján. Bennett [7] megoldotta (12)-et az $S = \{2, 3\}$ esetben, amit Bennett, Győry, Mignotte és Pintér [10] kiterjesztett az $S = \{p, q\}, 2 \leq p, q \leq 13$ esetre. Bugeaud, Mignotte és Siksek [21] más módszerrel megoldotta (12)-t, ha $A = 2^\alpha, B = q^\beta$ ahol $3 \leq q < 100$ egy prím, vagy $A = p^\alpha, B = q^\beta$, ahol $3 \leq p < q \leq 31$ prímek. Győry és Pintér [31]-ben kiterjesztete a [10]-beli eredményeket az $S = \{p, q\}, 2 \leq p, q \leq 29$ esetre.

Többek között az 1.1, 1.2, 1.3 és a 2.6 Tételeink alkalmazásával kiterjesztjük a fenti eredményeket arra az esetre, amikor $S = \{p, q\}$ és $2 \leq p, q \leq 71$. Az alábbi tételünkben olyan felső korlátot adunk n-re, amely hasznos eszköz lehet konkrét S-egység együtthatós binom Thue-egyenletek megoldása során.

2.7. Tétel. *[Bazsó, 201?] Legyen $n \geq 3$ prím, $S = \{p, q\}$, ahol $2 \leq p, q \leq 71$, legyenek $A, B \in \mathbb{Z}$ relatív prím S-egységek, továbbá $A < B$. Ekkor ha $(A, p, q) \neq (1, 2, 31)$ és $(p, q) \notin \{(23, 41), (17, 47), (29, 61), (61, 67), (17, 71)\}$, akkor a (12) egyenlet bármely (x, y, z, A, B, n), $|xy| > 1$ tulajdonságú megoldására $n \leq 31$ teljesül.*

Továbbá,
(i) ha $A = 1$ és

$$(p, q, n) \notin \{(47, q, 23), (59, q, 29), (2, 61, 31), (17, 61, 31), (43, 61, 31), (53, 67, 17)\},$$

akkor a (12) egyenlet bármely (x, y, z, A, B, n), $|xy| > 1$ tulajdonságú megoldására $n \leq 13$ teljesül.
(ii) ha $A > 1$ és

$$(p, q, n) \notin \{(3, 37, 19), (5, 37, 19), (3, 61, 31), (17, 61, 31), (43, 61, 31)\},$$

akkor a (12) egyenlet bármely (x, y, z, A, B, n), $|xy| > 1$ tulajdonságú megoldására $n \leq 17$ teljesül.

A kivételes (p, q, n) esetekben a jelenlegi módszereinkkel nem sikerült megoldanunk a (12) egyenletet az adott korlát fölötti n kitevő és a p, q prímek tetszőleges nemnegatív hatványai esetén, ám ezekben az esetekben is számos konkrét α, β kitevő esetén megoldottuk az egyenletet. Megjegyezzük továbbá, hogy legfeljebb 17-edfokú binom Thue-egyenleteket általában megoldhatunk a MAGMA [18], PARI [40] ill. SAGE [50] programcsomagok segítségével.

A 2.3 szakaszban közölt eredményeink a Bérczes Attilával, Győry Kálmánnal és Pintér Ákossal közös [4] cikkünkben jelentek meg, míg az S-egység együtthatójú binom Thue-egyenletekre vonatkozó 2.7 Tétel a [3] dolgozatban fog megjelenni.

3. Binom Thue-egyenletek egy alkalmazásáról

A 2. fejezet elején említettük, hogy számos számelméleti probléma visszavezethető binom Thue-egyenletek megoldására. Ebben a fejezetben egy norma forma egyenletekkel kapcsolatos alkalmazást mutatunk be. Ismert, hogy bizonyos feltételek mellett a norma forma egyenleteknek végtelen sok megoldása lehet. Ebben az esetben tanulmányozzuk azokat a megoldásokat, amelyekben a koordináták számtani sorozatot alkotnak. Norma forma egyenletek egy adott családjára meghatározzuk az összes ilyen megoldást.

3.1. Norma forma egyenletek számtani sorozatot alkotó megoldásairól

Legyenek $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ $\mathbb{Q}$ fölött lineárisan független algebrai számok, $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ egy n-edfokú algebrai számtest, legyenek $\sigma_1, \ldots, \sigma_n$ a K számtest $\mathbb{Q}$-t fixen hagyó beágyazásai $\mathbb{C}$-be, és $\alpha^{(i)} = \sigma_i(\alpha)$ $(\alpha \in K)$. Tekintsük az

$$l^{(i)}(\underline{X}) = X_1 + \alpha_2^{(i)} X_2 + \ldots + \alpha_n^{(i)} X_n\,, \quad i = 1, \ldots, n,\ \underline{X} = (X_1, \ldots, X_n)\,.$$

lineáris formákat. Ekkor létezik olyan a_0 nemnegatív egész, amelyre az

$$F(\underline{X}) := a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m) = a_0 \prod_{i=1}^{n} l^{(i)}(\underline{X})$$

forma együtthatói egészek. Az ilyen formákat norma formáknak, az

$$a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m) = b \tag{13}$$

alakú egyenleteket norma forma egyenleteknek nevezzük.

A (13) egyenletet degeneráltnak nevezzük, ha az $\alpha_1, \ldots, \alpha_m$ által generált $\mathbb{Q}$-fölötti vektortér egy altere arányos egy $\mathbb{Q}$-tól és az imaginárius másodfokú számtestektől különböző algebrai számtest teljes $\mathbb{Z}$-modulusával. Ekkor belátható, hogy létezik olyan $b \in \mathbb{Z}$, melyre (13)-nak végtelen sok megoldása van. Schmidt [44] nevezetes ineffektív tétele szerint nem-degenerált norma forma egyenleteknek csak véges sok megoldása lehet. Győry és Papp [26] effektív végességi eredményeket és explicit felső korlátokat nyertek norma forma egyenletek széles osztályainak megoldásaira. A norma forma egyenletek gazdag irodalmából azon eredményekkel folytatjuk, amelyek vizsgálataink előzményét képezték.

A norma forma egyenletek megoldásai közötti számtani sorozatok vizsgálatának ötletét Pethő Attila vetette fel. A probléma akkor merült fel, amikor Buchmann és Pethő [19] észrevette, hogy $\alpha^7 = 3$ esetén a $K := \mathbb{Q}(\alpha)$ számtestben a

$$10 + 9\alpha + 8\alpha^2 + 7\alpha^3 + 6\alpha^4 + 5\alpha^5 + 4\alpha^6$$

algebrai egész egység. Ez azt jelenti, hogy az

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_6\alpha^6\right) = 1$$

egyenletnek van olyan $(x_0, \ldots, x_6) \in \mathbb{Z}^7$ megoldása, melyben a koordináták egy számtani sorozat egymást követő elemei.

Ez megfigyelés az alapja Bérczes és Pethő [14] cikkének, amelyben általánosan vizsgálják

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = m. \tag{14}$$

norma forma egyenletek számtani sorozatot alkotó megoldásait, amelyben α egy n-edfokú algebrai szám, $K = \mathbb{Q}(\alpha)$, $m \in \mathbb{Z}$ és $\{x_0, \ldots, x_{n-1}\} \in \mathbb{Z}^n$. Legyen $X = \max\{|x_0|, \ldots, |x_{n-1}|\}$. Az $\{x_0, \ldots, x_{n-1}\}$ sorozatot majdnem számtani sorozatnak nevezzük, ha létezik olyan $d \in \mathbb{Z}$ és $0 < \delta \in \mathbb{R}$, amelyre

$$|(x_i - x_{i-1}) - d| < X^{1-\delta}, \quad i = 1, \ldots, n-1. \tag{15}$$

Bérczes és Pethő [14]-ben effektív végességi eredményt bizonyított a (14) egyenlet (15) tulajdonságú, azaz majdnem számtani sorozatot alkotó megoldásaira amikor a

$$\beta := \frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$$

egy legalább harmadfokú algebrai szám. A $\delta = 1$ speciális esetben majdnem teljes végességi eredményt nyertek.

Bérczes és Pethő [14] meghatározták továbbá a

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = 1.$$

norma forma egyenlet összes számtani sorozatot alkotó megoldását, amikor α az $x^n - 2$ vagy $x^n - 3$ $(n \geq 3)$ polinom egyik gyöke. Ezenkívül [15]-ben belátták, hogy az egyenletnek nincs számtani sorozatot alkotó megoldása, amikor α az $x^n - a$ $(n \geq 3)$ polinom egyik gyöke és $4 \leq a \leq 100$.

Bérczes, Pethő és Ziegler [16] megadták az

$$|N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2)| \leq |2a + 1|$$

norma forma egyenlőtlenség összes olyan primitív megoldását, melyre $x_0 < x_1 < x_2$ egy számtani sorozat, ahol α az

$$f_a(x) = x^3 - (a-1)x^2 - (a+2)x - 1, \quad a \in \mathbb{Z},$$

polinom egyik gyöke.

Megjegyezzük, hogy számtani sorozatok nem csak egy-egy megoldáson belül fordulhatnak elő, hanem a norma forma egyenlet megoldáshalmazában is, ha a megoldások egy rögzített koordinátáját tekintjük. Ebben az irányban Bérczes, Hajdu és Pethő [13] nyertek eredményeket.

3.2. Saját eredmények

Az alábbiakban kiterjesztjük Bérczes és Pethő [15] eredményét a (16) egyenlettel kapcsolatban.

Legyen α egy $n \geq 3$ fokú algebrai egész, $K = \mathbb{Q}(\alpha)$, és tekintsük az

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}\right) = 1 \tag{16}$$

egyenletet, melyben $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ ismeretlenek. Legyen α az $x^n - a$ polinom egy gyöke, melyben a egy olyan egész, amelyre $x^n - a$ irreducibilis. Amint említettük, Bérczes és Pethő [15] belátták, hogy (16)-nak nincs számtani sorozatot alkotó megoldása, amikor $4 \leq a \leq 100$. Az alábbi tételben kiterjesztjük ezt az eredményt az a paraméter negatív értékeire, azaz $-100 \leq a \leq -2$ esetén meghatározzuk a (16) összes olyan megoldását, amelyre $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ egy számtani sorozat egymást követő elemei.

3.1. Tétel. *[Bazsó, 2007] Legyen $n \geq 3$, $-100 \leq a \leq -2$, α az $x^n - a \in \mathbb{Z}[x]$ irreducibilis polinom gyöke és $K = \mathbb{Q}(\alpha)$. Ekkor a (16) egyenlet összes számtani sorozatot alkotó megoldásai $(n, a) = (3, -7)$ esetén a $(2, 1, 0)$, és $(n, a) = (3, -9)$ esetén a $(-2, -1, 0)$. Ha $(n, a) = (11, -67)$, az állításunk az általánosított Riemann Hipotézis (GRH) feltevése mellett igazolható.*

A 3.1 Tételt a következő tétel segítségével bizonyítjuk, amely általánosított binom Thue-egyenletek egy családjának a teljes megoldását tartalmazza.

3.2. Tétel. *[Bazsó, 2007] Legyen* $-100 \le a \le -2$*. Ekkor az*

$$X^n - aY^n = (a-1)^2 \tag{17}$$

egyenlet összes (n, a, X, Y) *megoldása szerepel az alábbi 3.1 táblázatban. Ha* $(n, a) = (11, -67)$*, az állításunk a GRH feltevése mellett igazolható.*

3.1 táblázat

n	a	(X, Y)
3	-97	(35, -7)
3	-63	(4, 4), (16,0), (64, -16)
3	-62	(1, 4)
3	-61	(13, 3)
3	-39	(16, -4)
3	-35	(11, -1), (46, -14)
3	-27	(10, -2)
3	-26	(3, 3), (9, 0), (27, -9)
3	-25	(1, 3)
3	-18	(-5, 3), (7, 1)
3	-12	(-11, 5)
3	-9	(7, -3)
3	-7	(-5, 3), (2, 2), (4, 0), (8, -4)
3	-6	(1, 2)
3	-3	(-2, 2)
4	-99	(-10, 0), (10, 0)
4	-80	(-9, 0), (-3, -3), (-3, 3), (3, -3), (3, 3), (9, 0)
4	-79	(-1, -3), (-1, 3), (1, -3), (1, 3)
4	-63	(-8, 0), (8, 0)
4	-48	(-7, 0), (7, 0)
4	-35	(-6, 0), (6, 0)
4	-24	(-5, 0), (5, 0)
4	-15	(-4, 0), (-2, -2), (-2, 2), (2, -2), (2, 2), (4, 0)
4	-14	(-1, -2), (-1, 2), (1, -2), (1, 2)
4	-8	(-3, 0), (3, 0)
4	-3	(-2, 0), (2, 0)

3.1 táblázat (folytatás)

n	a	(X, Y)
5	-31	(2, 2), (4, 0), (8, -4)
5	-30	(1, 2)
6	-63	(2, 2), (-2, -2), (2, -2), (-2, 2), (4, 0), (-4, 0)
6	-26	(3, 0), (-3, 0)
6	-7	(2, 0), (-2, 0)
8	-80	(3, 0), (-3, 0)
8	-15	(2, 0), (-2, 0)
10	-31	(2, 0), (-2, 0)
12	-63	(2, 0), (-2, 0)

A harmadik fejezet eredményei [2]-ben jelentek meg.

References/Irodalomjegyzék

[1] A. Baker, Contributions to the theory of Diophantine equations, *Phil. Trans. Roy. Soc. London*, **263** (1968), 173–208.

[2] A. Bazsó, Further computational experiences on norm form equations with solutions forming arithmetic progressions, *Publ. Math. Debrecen*, **71** (2007), 489–497.

[3] A. Bazsó, On binomial Thue equations and ternary equations with S-unit coefficients, *Publ. Math. Debrecen*, accepted for publication.

[4] A. Bazsó, A. Bérczes, K. Győry and Á. Pintér, On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$, II, *Publ. Math. Debrecen*, **76** (2010), 227–250.

[5] M. A. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, *J. Reine Angew. Math.*, **535** (2001), 1–49.

[6] M. A. Bennett, Recipes for ternary Diophantine equations of signature (p, p, k), *RIMS Kokyuroku (Kyoto)*, **1319** (2003), 51–55.

[7] M. A. Bennett, Products of consecutive integers, *Bull. London Math. Soc.*, **36** (2004), 683–694.

[8] M. A. Bennett, The Diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)^t$, *Indag. Math. (N.S.)*, **18** (2007), no. 4, 507–525.

[9] M. A. Bennett, K. Győry, and Á. Pintér, On the Diophantine equation $1^k + 2^k + \cdots + x^k = y^n$, *Compos. Math.* **140** (2004), 1417–1431.

[10] M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér, Binomial Thue equations and polynomial powers, *Compos. Math.*, **142** (2006), no. 5, 1103–1121.

[11] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, **56** (2004), 23–54.

[12] M. A. Bennett, V. Vatsal and S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, *Compos. Math.*, **140** (2004), 1399–1416.

[13] A. Bérczes, L. Hajdu and A. Pethő, Arithmetic progressions in the solution sets of norm form equations, *Rocky Mountain J. Math.*, **40** (2010), 383–395.

[14] A. Bérczes and A. Pethő, On norm form equations with solutions forming arithmetic progressions, *Publ. Math. Debrecen*, **65** (2004), 281–290.

[15] A. Bérczes and A. Pethő, Computational experiences on norm form equations with solutions from an arithmetic progression, *Glasnik Matematički. Serija III*, **41(61)** (2006), 1–8.

[16] A. Bérczes, A. Pethő and V. Ziegler, Parametrized norm form equations with arithmetic progressions, *J. Symbolic Comput.*, **41** (2006), 790–810.

[17] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539** (2001), 75–122.

[18] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[19] J. Buchmann and A. Pethő, Computation of independent units in number fields by Dirichlet's method, *Math. Comp.*, **52** (1989), 149–159, S1–S14.

[20] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations II: The Legesgue-Nagell equation, *Compos. Math.*, **142** (2006), 31–62.

[21] Y. Bugeaud, M. Mignotte and S. Siksek, A multi-frey approach to some multi-parameter families of Diophantine equations, *Canad. J. Math.*, **60** (2008), 491–519.

[22] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä and M. A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comput.*, **31** (2001), 89–96.

[23] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem, *J. Reine Angew. Math.*, **490** (1997), 81–100.

[24] G. Frey, Links between stable elliptic curves and certain diophantine equations, *Ann. Univ. Sarav., Ser. Math.*, **1** (1986), 1–40.

[25] K. Győry, Über die diophantische gleichung $x^p + y^p = cz^p$, *Publ. Math. Debrecen*, **13** (1966), 301–305.

[26] K. Győry and Z.Z. Papp, Effective estimates for the integer solutions of norm form and discriminant form equations, *Publ. Math. Debrecen*, **25** (1978), 311–325.

[27] K. Győry, I. Pink and Á. Pintér, Power values of polynomials and binomial Thue-Mahler equations, *Publ. Math. Debrecen*, **65** (2004), 341–362.

[28] K. Győry and Á. Pintér, Almost perfect powers in products of consecutive integers, *Monatsh. Math.*, **145** (2005), 19–33.

[29] K. Győry and Á. Pintér, On the resolution of equations $\mathrm{A}x^n - \mathrm{B}y^n = \mathrm{C}$ in integers x, y and $n \geq 3$, I, *Publ. Math. Debrecen*, **70** (2007), 483–501.

[30] K. Győry and Á. Pintér, *Polynomial powers and a common generalization of binomial Thue-Mahler equations and S-unit equations*, Diophantine Equations, Narosa Publ. House, India, 2008, pp. 103–119.

[31] K. Győry and Á. Pintér, Binomial Thue equations, ternary equations and power values of polynomials, *Fundamental and Applied Mathematics* (to appear).

[32] E. Halberstadt and A. Kraus, Courbes de Fermat: résultats et problèmes, *J. Reine Angew. Math.*, **548** (2002), 167–234.

[33] G. Hanrot, Solving Thue equations without the full unit group, *Math. Comp.*, **69** (2000), no. 229, 395–405.

[34] G. Hanrot, N. Saradha and T. N. Shorey, Almost perfect powers in consecutive integers, *Acta Arith.*, **99** (2001), 13–25.

[35] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.*, **49** (1997), 1139–1161.

[36] E. MAILLET, Sur les équations indéterminés de la forme $x^\lambda + y^\lambda = cz^\lambda$, *Acta Math.*, **21** (1901), 247–256.

[37] M. MIGNOTTE, A note on the equation $ax^n - by^n = c$, *Acta Arith.*, **75** (1996), 287–295.

[38] P. MIHĂILESCU, *Class number conditions for the diagonal case of the equation of Nagell and Ljunggren*, Diophantine Approximation, Springer-Verlag, 2008, pp. 245–273.

[39] L. J. MORDELL, *Diophantine equations*, Academic Press, London, 1969.

[40] The PARI Group, Bordeaux, *PARI/GP, version* `2.1.5`, 2004, available from `http://pari.math.u-bordeaux.fr/`.

[41] A. PETHŐ, On the resolution of Thue inequalities, *J. Symbolic Comput.*, **4** (1987), 103–109.

[42] Á. PINTÉR, On the power values of power sums, *J. Number Theory*, **125** (2007), 412–423.

[43] K. A. RIBET, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.*, **79** (1997), 7–16.

[44] W. M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II., *Math. Ann.*, **191** (1971), 1–20.

[45] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$), *Duke Math. J.*, **54** (1987), 179–230.

[46] T. N. SHOREY and R. TIJDEMAN, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge–New York, 1986.

[47] S. SIKSEK, The modular approach to Diophantine equations, in: *H. Cohen: Number Theory*, Springler-Verlag, Berlin, 2007, pp. 1107–1138.

[48] S. SIKSEK and J. E. CREMONA, On the Diophantine equation $x^2+7 = y^m$, *Acta Arith.*, **109** (2003), 143–149.

[49] W. Stein, *Modular forms, a computational approach*, vol. 79 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 2007, with an appendix by Paul E. Gunnells.

[50] W. Stein et al., The Sage Development Team, *Sage Mathematics Software (Version 3.4)*, 2009, available from http://www.sagemath.org/.

[51] A. Thue, Über Annäherungenswerte algebraischer Zahlen, *J. Reine Angew. Math.*, **135** (1909), 289–305.

[52] R. Tijdeman, Some applications of Baker's sharpened bounds to Diophantine equations, in: *Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 2, Exp. No. 24*, Secrétariat Mathématique, Paris, 1975, p. 7.

[53] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)*, **141** (1995), 443–551.

Publications of the author/A szerző publikációi

1. A. Bazsó, *Further computational experiences on norm form equations with solutions forming arithmetic progressions*, Publ. Math. Debrecen 71(3-4) (2007), 489-497.

2. A. Bazsó, A. Bérczes, K. Győry and Á. Pintér, *On the resolution of equations* $Ax^n - By^n = C$ *in integers* x, y *and* $n \geq 3$*, II*, Publ. Math. Debrecen 76(1-2) (2010), 227-250.

3. A. Bazsó, *On binomial Thue equations and ternary equations with* S*-unit coefficients*, Publ. Math. Debrecen, accepted for publication.

Talks of the author/A szerző konferencia-előadásai

1. *Norm form equations with solutions forming arithmetic progressions*, The 18th Czech and Slovak International Conference on Number Theory, 27-31 August 2007, Smolenice (Slovakia).

2. *Norma forma egyenletek számtani sorozatot alkotó megoldásairól*, Egri Számelméleti és Kriptográfiai Napok, 6 October 2007, Eger.

3. *On the resolution of equations of the form $Ax^n - By^n = C$ in integers x, y and $n \geq 3$*, The 7th Polish, Slovak and Czech Conference on Number Theory, 10-12 June 2008, Ostravice (Czech Republic).

4. *Binom Thue-egyenletek megoldásáról*, II. Soproni Diofantikus és Kriptográfiai Napok, 10-12 October 2008, Sopron.

5. *Solving binomial Thue equations*, Winter School on Explicit Methods in Number Theory, 26-30 January 2009, Debrecen.

6. *On the resolution of binomial Thue equations*, 26th Journées Arithmétiques, 6-10 July 2009, Saint-Étienne (France).

7. *On ternary and binomial Thue equations with S-unit coefficients*, The 19th Czech and Slovak International Conference on Number Theory, 31 August - 4 September 2009, Hradec nad Moravicí (Czech Republic).

8. *On ternary and binomial Thue equations with S-unit coefficients*, Debreceni Diofantikus és Kriptográfiai Napok, 7 November 2009, Debrecen.

9. *On ternary equations and binomial Thue equations*, The 8th Czech, Polish and Slovak Conference on Number Theory, 21-24 June 2010, Bukowina Tatrzańska (Poland).