REKURENT DİZİLERİN ARİTMETİK ÖZELLİKLERİ

İpek ÇOLAK

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

REKURENT DİZİLERİN ARİTMETİK ÖZELLİKLERİ

İpek ÇOLAK
0000-0002-6502-0251

Prof. Dr. Betül GEZER
(Danışman)

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2023

TEZ ONAYI

İpek ÇOLAK tarafından hazırlanan "REKURENT DİZİLERİN ARİTMETİK ÖZELLİKLERİ" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Bursa Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman: Prof. Dr. Betül GEZER

Başkan	**:**	Prof. Dr. Osman BİZİM 0000-0001-5236-4023 Bursa Uludağ Üniversitesi, Fen Edebiyat Fakültesi, Matematik Anabilim Dalı	İmza
Üye	**:**	Prof. Dr. Betül GEZER 0000-0001-9133-1734 Bursa Uludağ Üniversitesi, Fen Edebiyat Fakültesi, Matematik Anabilim Dalı	İmza
Üye	**:**	Doç. Dr. İrem KÜPELİ ERKEN 0000-0003-4471-3291 Bursa Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Matematik Anabilim Dalı	İmza

Yukarıdaki sonucu onaylarım

Prof. Dr. Hüseyin Aksel EREN
Enstitü Müdürü
../../….

B.U.Ü. Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

04/05/2023

İpek ÇOLAK

TEZ YAYINLANMA
FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezin/raporun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma izni Bursa Uludağ Üniversitesi'ne aittir. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet hakları ile tezin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları tarafımıza ait olacaktır. Tezde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığını ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederiz.

Yükseköğretim Kurulu tarafından yayınlanan "**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge**" kapsamında, yönerge tarafından belirtilen kısıtlamalar olmadığı takdirde tezin YÖK Ulusal Tez Merkezi / B.U.Ü. Kütüphanesi Açık Erişim Sistemi ve üye olunan diğer veri tabanlarının (Proquest veri tabanı gibi) erişimine açılması uygundur.

Danışman Adı-Soyadı Tarih	Öğrencinin Adı-Soyadı Tarih
Prof. Dr. Betül GEZER 09.05.2023	İpek ÇOLAK 09.05.2023

ÖZET

Yüksek Lisans Tezi

REKURENT DİZİLERİN ARİTMETİK ÖZELLİKLERİ

İpek ÇOLAK

Bursa Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Betül GEZER

Bu çalışmada Zsigmondy teoremi ve bu teoremin uygulamaları ele alınmıştır. İlk olarak klasik Zsigmondy teoremi verilmiş ve daha sonra lineer diziler için Zsigmondy teoremi ele alınmıştır. Daha sonra çalışılan ilk lineer olmayan dizilerden eliptik bölünebilir dizilerdeki ilkel asal bölen kavramı üzerinde durulmuş ve belli eliptik eğrilerle eşleşen eliptik bölünebilir diziler için Zsigmondy sınırı verilmiştir.

Birinci bölümünde bazı aritmetik fonksiyonlar ile ilgili temel kavramlar ele alınmış ve daha sonra döngüsel polinomlar ve özellikleri üzerinde durulmuştur.

İkinci bölümde ilk olarak ilkel asal bölen tanımı verilerek klasik Zsigmondy teoremi ele alınmıştır. Daha sonra bu teoremin bir elementer ispatı verilerek Zsigmondy teoreminin uygulamaları üzerinde durulmuştur. Son olarak büyük Zsigmondy asal sayısı kavramı verilerek Lucas ve Lehmer dizilerinin ilkel asal bölene sahip oldukları gösterilmiştir.

Üçüncü bölümde eliptik dizi kavramı tanımlanarak bu dizilerin özellikleri üzerinde durulmuştur. Daha sonra bu dizilerin eliptik eğrilerle olan ilişkisi kullanılarak bu dizilerde ortaya çıkan ilkel asal bölenler belirlenmiş ve Zsigmondy sınırları verilmiştir.

Anahtar Kelimeler: İlkel asal bölen, Zsigmondy teoremi, Zsigmondy asalları, eliptik bölünebilir diziler, eliptik eğriler.
2023, vi + 61 sayfa.

ABSTRACT

MSc Thesis

THE ARITHMETIC PROPERTIES OF RECURRENCE SEQUENCES

İpek ÇOLAK

Bursa Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Prof. Dr. Betül GEZER

In this work, the Zsigmondy's theorem and its applications have been discussed. First, the classical Zsigmondy's theorem was given and then the Zsigmondy's theorem for linear sequences was discussed. Later, the concept of primitive prime divisors in elliptic divisible sequences, which are one of the first studied non-linear sequences, was discussed and the Zsigmondy bound was given for the elliptic divisibility sequences associated to certain elliptic curves.

In the first section, fundamental concepts related to arithmetic functions were discussed, and later on the fundamental concepts of cyclic polynomials and their properties were emphasized.

In the second chapter, first the definition of primitive prime divisor was given, and the classical Zsigmondy's theorem was discussed. Then an elementary proof of the Zsigmondy theorem was given, and applications of the theorem were discussed. Finally, the concept of the large Zsigmondy prime was introduced, and it was shown that Lucas and Lehmer sequences have primitive prime divisors.

In the third chapter, the definition of elliptic sequences and their properties were given. Then the relation between these sequences and elliptic curves were used to determine the primitive divisors and Zsigmondy bound for these sequences.

Key words: Primitive divisor, Zsigmondy's theorem, Zsigmondy primes, elliptic divisibility sequences, elliptic curves.
2023, vi + 61 pages.

TEŞEKKÜR

Yüksek Lisans çalışmamın her aşamasında yakın ilgi ve desteğini gördüğüm, bana yön gösteren, tecrübelerini ve emeklerini esirgemeyerek gelişimime katkıda bulunan, öğrencisi olmaktan her zaman gurur duyacağım saygıdeğer hocam Prof. Dr. Betül GEZER'e teşekkür ederim.

Ayrıca bu tez çalışması boyunca bana her türlü manevi desteği veren anneme ve çalışmalarım sırasında maddi desteklerini esirgemeyen TÜBİTAK'a teşekkürü bir borç bilirim.

İpek ÇOLAK
03/05/2023

İÇİNDEKİLER

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	**Açıklama**
$Z(A_n)$	(A_n) tamsayılar dizisinin Zsigmondy kümesi
$E(K)$	bir K cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar grubu
$\boldsymbol{O}$	bir eliptik eğri üzerindeki sonsuzdaki nokta
μ	Möbius fonksiyonu
ϕ_n	n. döngüsel polinom
$\mathrm{ord}_p(n)$	n tamsayısının p-adik valüasyonu

Kısaltmalar	**Açıklama**
EBD	Eliptik Bölünebilir Diziler

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bu kısımda ilk olarak bazı aritmetik fonksiyonlar ele alınacak ve daha sonra döngüsel polinomlar ve özellikleri üzerinde durulacaktır.

1.1. Aritmetik Fonksiyonlar

Bu kısımda çalışmada kullanılacak olan bazı aritmetik fonksiyonlar ve bunların özellikleri üzerinde durulacaktır. İlk olarak Möbius fonksiyonu ve özellikleri ele alınacaktır.

1.1.1. Tanım. $\mu : \mathbb{N} \to \{-1, 0, 1\}$, her $n \in \mathbb{N}$ için

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k & n \text{ karesiz bir sayı ve } k, n \text{ nin} \\ & \text{farklı asal bölenlerinin sayisi} \\ 0, & \text{diger hallerde} \end{cases}$$

biçiminde tanımlanan μ fonksiyonuna *Möbius fonsiyonu* denir.

1.1.2. Örnek. Aşağıda bazı $\mu(n)$ değerleri verilmiştir.

n :	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	–1	–1	0	–1	1	–1	0	0	1

Aşağıda μ fonksiyonun özellikleri ile ilgili oldukça önemli bir teorem verilmiştir.

1.1.3. Teorem. *n* bir pozitif tamsayı olmak üzere

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & n=1 \\ 0, & n \geq 2 \end{cases}$$

dir (Apostol, 1998).

Bu teorem kullanılarak

$$\sum_{d|2}\mu(d) = \mu(1) + \mu(2) = 0$$

ve

$$\sum_{d|4}\mu(d) = \mu(1) + \mu(2) + \mu(4) = 0$$

olduğu kolayca görülebilir.

1.1.4. Uyarı. Möbius fonksiyonu çarpımsal bir fonksiyondur, yani aralarında asal her *m* ve *n* pozitif tamsayıları için

$$\mu(m, n) = \mu(m) \cdot \mu(n)$$

dir.

1.1.5 Teorem (Möbius İnversiyon Teoremi). *f*, *g* ve *h*, her $n \geq 1$ tamsayısı için

$$f(n) = \sum_{d|n} g(d) \quad \text{ve} \quad h(n) = \prod_{d|n} g(d)$$

özelliğinde aritmetik fonksiyonlar ve μ, Möbius fonksiyonu olmak üzere

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \prod_{d|n} h(\frac{n}{d})^{\mu(d)}$$

dir (Apostol, 1998).

1.1.6 Tanım. $n \geq 1$ bir tamsayı olmak üzere n ile aralarında asal ve n sayısından küçük olan pozitif tamsayıların sayısını belirten fonksiyona *Euler fonksiyonu* denir ve $\varphi(n)$ ile gösterilir.

Diğer bir ifade ile

$$\varphi(n) = \#\{k \in \mathbb{N} \mid (k, n) = 1, 0 < k < n\}$$

dir. Özel olarak p asal ise $\varphi(p) = p - 1$ dir. Tanımdan faydalanılarak $\varphi(6) = 2$, $\varphi(8) = 4$ olduğu kolayca görülebilir.

1.2. Döngüsel Polinomlar

Bu kısımda klasik Zsigmondy teoreminin ispatında kullanılacak olan döngüsel polinomlar ve bu polinomların özellikleri ele alınacaktır. İlk olarak döngüsel polinom tanımı verilecektir.

1.2.1 Tanım. n bir pozitif tamsayı ve ζ, birimin n. ilkel kökü olmak üzere

$$\phi_n(x) = \prod_{k=1}^{\varphi(n)} (x - \zeta^k)$$

polinomuna *n. döngüsel polinom* adı verilir.

Aşağıdaki teoremde $\phi_n(x)$ *n.* döngüsel polinomunun bazı özellikleri verilmiştir.

1.2.2. Teorem. *n* bir pozitif tamsayı olmak üzere

i. $x^n - 1 = \prod_{d|n} \phi_d(x)$, (1. 1)

ii. $\phi_n(x) \in \mathbb{Z}[x]$

dir (Gezer, Bizim 2017).

Bu teoreme göre $x^n - 1 = \prod_{d|n} \phi_d(x)$ olduğundan $h(n) = x^n - 1$ ve $g(d) = \phi_d(x)$ alınarak Möbius İnversiyon Teoremi uygulanırsa $\phi_n(x)$ döngüsel polinomunun

$$\phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

olarak ifade edilebileceği sonucu elde edilir. Böylece aşağıdaki sonuç elde edilmiş olur.

1.2.3. Teorem. $n \geq 1$ bir tamsayı ve μ, Möbius fonksiyonu olmak üzere

$$\phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \quad (1.\ 2)$$

dir (Cox, 2012).

Bu teorem kullanılarak 2., 3. ve 4. döngüsel polinomları sırasıyla

$$\phi_2(x) = \prod_{d|2} (x^{\frac{2}{d}} - 1)^{\mu(d)} = (x^2 - 1)^{\mu(1)} \cdot (x - 1)^{\mu(2)} = \frac{x^2 - 1}{x - 1} = x + 1$$

$$\phi_3(x) = \prod_{d|3}(x^{\frac{3}{d}} - 1)^{\mu(d)} = (x^3 - 1)^{\mu(1)} \cdot (x - 1)^{\mu(3)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

$$\phi_4(x) = \prod_{d|4}(x^{\frac{4}{d}} - 1)^{\mu(d)} = (x^4 - 1)^{\mu(1)} \cdot (x^2 - 1)^{\mu(2)} \cdot (x - 1)^{\mu(4)} = x^2 + 1$$

olarak bulunur.

Aşağıda döngüsel polinomların klasik Zsigmondy teoreminin ispatında kullanılacak olan önemli bir lemma ele alınmıştır.

1.2.4. Lemma. *p* bir asal sayı ve *n* bir pozitif tamsayı olmak üzere

$$\phi_{pn}(x) = \begin{cases} \phi_n(x^p), & p \mid n \, ise \\ \dfrac{\phi_n(x^p)}{\phi_n(x)}, & p \nmid n \ ise \end{cases}$$

dir (Ge, 2023).

Lemma 1.2.4 kullanılarak aşağıdaki sonuç elde edilebilir.

1.2.5. Sonuç. *p* bir asal sayı ve *n* ve *k* pozitif tamsayılar olmak üzere

$$\phi_{p^k n}(x) = \begin{cases} \phi_n(x^{p^k}), & p \mid n \ \text{ise} \\ \dfrac{\phi_n(x^{p^k})}{\phi_n(xp^{k-1})}, & p \nmid n \ \text{ise} \end{cases}$$

dir (Ge, 2023).

Aşağıdaki teoremde $\phi_n(x)$'in asal bölenlerinin özellikleri belirtilmiştir.

1.2.6. Teorem. n bir pozitif tamsayı ve x herhangi bir tamsayı olmak üzere $\phi_n(x)$ in her p asal böleni ya n tamsayısını böler ya da n modülüne göre 1'e denktir (Ge, 2023).

Aşağıda $x > 1$ bir gerçel sayı olmak üzere $\phi_n(x)$ için bir alt sınır ve bir üst sınır verilmiştir.

1.2.7. Teorem. n bir pozitif tamsayı $x > 1$ bir gerçel sayı olmak üzere

$$(x-1)^{\varphi(n)} \leq \phi_n(x) < (x+1)^{\varphi(n)}$$

dir, burada $\varphi(n)$ Euler fonksiyonunu belirtmektedir (Sheng, 2023).

İspat. ζ, birimin n. ilkel kökü olduğundan $|\zeta| = 1$ ve üçgen eşitsizliğinden

$$x - 1 \leq |x - \zeta| \leq x + 1$$

eşitsizliği elde edilir. Böylece tüm ζ lar üzerinden çarpım alınırsa istenilen elde edilir.

1.2.8. Uyarı. $n = 2$ olması halinde ilk eşitsizliğin eşitlik haline geldiği kolayca görülebilir.

$a > 1$ bir tamsayı olmak üzere

$$a^n - 1 = \prod_{d|n} \phi_d(a)$$

olduğu dikkate alınırsa döngüsel polinomlar, Zsigmondy teoreminin ispatında kullanılabilir. Bunun için bu polinomlar $a^n - b^n$ ifadesi ile eşleştirilebilir. Böylece aşağıdaki tanım verilebilir.

1.2.9. Tanım. n bir pozitif tamsayı ve μ, Möbius fonksiyonu olmak üzere

$$\phi_n(a, b) = \prod_{d|n} (a^{\frac{n}{d}} - b^{\frac{n}{d}})^{\mu(d)}$$

polinomuna *homojenize döngüsel polinom* adı verilir.

Dikkat edilirse

$$a^n - b^n = b^n((\frac{a}{b})^n - 1)$$

olarak yazılabileceğinden (1.1) ve (1.2) gereği, $\phi_n(a, b)$ fonksiyonu

$$\phi_n(a, b) = b^{\varphi(n)}\, \phi_n(\frac{a}{b}) \qquad (1.\ 3)$$

biçiminde ifade edilebilir. Diğer yandan

$$a^n - b^n = \prod_{d|n} \phi_d(a, b) \qquad (1.\ 4)$$

olduğu (1. 3) eşitliği kullanılarak kolayca elde edilir.

1.2.10. Örnek. (1.4) eşitliği kullanılarak ϕ_1, ϕ_2, ϕ_3, ϕ_4, ϕ_5 ve ϕ_6 homojenize polinomlarının

$\phi_1(a, b) = a - b$,

$\phi_2(a, b) = a + b$,

$\phi_3(a, b) = a^2 + ab + b^2$,

$\phi_4(a, b) = a^2 + b^2$,

$\phi_5(a, b) = a^4 + a^3b + a^2b^2 + ab^3 + b^4$,

$\phi_6(a, b) = a^2 - ab + b^2$

biçiminde olduğu görülebilir.

Aşağıda Lemma 1.2.4 ve Teorem 1.2.7'de verilen sonuçlara benzer sonuçlar homojenize döngüsel polinomlar için verilmiştir.

1.2.11. Teorem. p bir asal sayı ve n bir pozitif tamsayı olmak üzere

$$\phi_{pn}(a, b) = \begin{cases} \phi_n(a^p, b^p), & p \mid n \text{ ise} \\ \dfrac{\phi_n(a^p, b^p)}{\phi_n(a, b)}, & p \nmid n \text{ ise} \end{cases}$$

dir (Ge, 2023).

1.2.12. Teorem. $n \geq 3$ bir tamsayı ve a ve b pozitif tamsayılar olmak üzere

$$(a - b)^{\varphi(n)} < \phi_n(a, b) < (a + b)^{\varphi(n)}$$

dir (Sheng, 2023).

1.3. *p*-sel Değerleme (*p*-adik Valüasyon)

$n \in \mathbb{Z}$ ve p bir asal sayı olsun. Eğer n sayısı sıfırdan farklı ise $p^k \mid n$ ancak $p^{k+1} \nmid n$ olacak biçimde negatif olmayan bir k tamsayısı vardır. Bu k tamsayısı, p asal sayısının n tamsayısını bölme sayısıdır ve bu sayı $\text{ord}_p(n)$ ile gösterilir.

Örneğin $p = 3$ ve $n = 18$ olarak alınırsa, 18 sayısı 3, $3^2 = 9$ sayılarına bölünebilir ancak 18 sayısı $3^3 = 27$ sayısına bölünmez.

1.3.1. Tanım. p bir asal sayı olmak üzere

$\text{ord}_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$, sıfırdan faklı her $n \in \mathbb{Z}$ için $\text{ord}_p(n) = \text{maks}\{k \in \mathbb{N} \mid p^k \mid n\}$

olarak tanımlanan ord_p fonksiyonuna n tamsayısının *p-adik valüasyonu* denir. Özel olarak $\text{ord}_p(0) = \infty$ olarak alınır.

Örneğin

$$\text{ord}_2(18) = 1,\ \text{ord}_3(18) = 2,\ \text{ord}_5(18) = \text{ord}_7(18) = \text{ord}_{11}(18) = 0$$

dır.

p-adik valüasyon fonksiyonu rasyonel sayılar kümesine de genelleştirilebilir. Buna göre

$$\text{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\},\ \text{her } \frac{a}{b} \in \mathbb{Q} \text{ için } \text{ord}_p(\frac{a}{b}) = \text{ord}_p(a) - \text{ord}_p(b)$$

olarak tanımlanır. Örneğin,

$$\text{ord}_2(\frac{8}{9}) = \text{ord}_2(8) - \text{ord}_2(9) = 3,\ \text{ord}_3(\frac{8}{9}) = -2 \text{ ve } \text{ord}_5(\frac{8}{9}) = 0$$

dır.

1.3.2. Uyarı. p-adik valüasyon fonksiyonunun bazı özellikleri aşağıda verilmiştir.

1) Her $a, b \in \mathbb{Z}$ için $\text{ord}_p(a \cdot b) = \text{ord}_p(a) + \text{ord}_p(b)$,

2) Her $a, b \in \mathbb{Z}$ için

$$\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}$$

dır ve üstelik $\text{ord}_p(a) \neq \text{ord}_p(b)$ ise $\text{ord}_p(a + b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ dir.

1.3.3. Lemma. a ve b tamsayılar, n bir pozitif tamsayı, p bir asal sayı olmak üzere $(n, p) = 1$ ve $p \mid a - b, p \nmid a,\ p \nmid b$ olsun. Bu durumda

$$\text{ord}_p(a^n - b^n) = \text{ord}_p(a - b)$$

dir (Parvardi, 2022).

Örneğin, $a = 27$, $b = 2$, $p = 5$, $n = 4$ olarak alınırsa

$$\text{ord}_5(27^4 - 2^4) = \text{ord}_5(3^{12} - 2^4) = \text{ord}_5(5^2 \cdot 29 \cdot 733) = 2$$

ve diğer yandan

$$\text{ord}_5(27 - 2) = \text{ord}_5(5^2) = 2$$

dir.

1.3.4. Lemma. a ve b tamsayılar, n bir tek pozitif tamsayı ve p bir asal sayı olmak üzere $(n, p) = 1$, $p \mid a + b$, $p \nmid a$ ve $p \nmid b$ olsun. Bu durumda

$$\text{ord}_p(a^n + b^n) = \text{ord}_p(a + b)$$

dir (Parvardi, 2022).

a ve b tamsayılar, n bir tek pozitif tamsayı ve p bir asal sayı olmak üzere $(n, p) \neq 1$ olması halinde Lemma 1.3.3 ve Lemma 1.3.4 kullanılarak aşağıdaki teoremler verilebilir.

1.3.5. Teorem (Kuvvet Yükseltme Lemması). a ve b tamsayılar, n bir pozitif tamsayı ve p bir tek asal sayı olmak üzere $p \mid a - b$, $p \nmid a$ ve $p \nmid b$ olsun. Bu durumda

$$\text{ord}_p(a^n - b^n) = \text{ord}_p(a - b) + \text{ord}_p(n)$$

dir (Parvardi, 2022).

İspat. $\text{ord}_p(n)$ fonksiyonu üzerine tümevarım uygulanarak görülebilir.

Kuvvet yükseltme lemması aşağıdaki şekilde de ifade edilebilir.

1.3.6. Teorem (Kuvvet Yükseltme Lemması). a ve b tamsayılar, n bir tek pozitif tamsayı ve p bir tek asal sayı olmak üzere $p \mid a+b,\ p \nmid a$ ve $p \nmid b$ olsun. Bu durumda

$$\text{ord}_p(a^n + b^n) = \text{ord}_p(a+b) + \text{ord}_p(n)$$

dir (Parvardi, 2022).

Aşağıda $p = 2$ için kuvvet yükseltme lemması ele alınmıştır.

1.3.7. Teorem ($p = 2$ için Kuvvet Yükseltme Lemması). a ve b iki tek tamsayı ve $4 \mid a - b$ olsun.

$$\text{ord}_2(a^n - b^n) = \text{ord}_2(a-b) + \text{ord}_2(n)$$

dir (Parvardi, 2022).

Aşağıdaki teoremde döngüsel polinomlar için kuvvet yükseltme lemması verilmiştir.

1.3.8. Teorem (Döngüsel Polinomlar için Kuvvet Yükseltme Lemması). $p \geq 3$ bir asal sayı $p \nmid a,\ p \nmid b,\ n \geq 1$ ve $k \geq 1$ sayısı $p \mid a^k - b^k$ özelliğindeki en küçük tamsayı olsun. Bu durumda

$$\text{ord}_p(\phi_n(a,b)) = \begin{cases} \text{ord}_p(a^k - b^k), & n = k \\ 1, & n = p^\alpha k, \alpha \geq 1 \\ 0, & \text{diger durumlarda} \end{cases}$$

dir (Sheng, 2023).

Aşağıdaki teoremde $p = 2$ halinde döngüsel polinomlar için kuvvet yükseltme lemması ele alınmıştır.

1.3.9. Teorem. a ve b tek tamsayılar ve $n \geq 1$ olsun. Bu durumda

$$\mathrm{ord}_2(\phi_n(a, b)) = \begin{cases} \mathrm{ord}_2(a-b), & n = 1 \\ \mathrm{ord}_2(a+b), & n = 2 \\ 1, & n = 2^m, m \geq 2 \\ 0, & \text{diger durumlarda} \end{cases}$$

dir (Sheng, 2023).

1.4. Eliptik Eğriler.

Çalışmada eliptik eğrilerle eşleşen dizilerin bazı özellikleri ele alınacağından bu kısımda eliptik eğri kavramı üzerinde durularak bunların özellikleri ele alınacaktır.

1.4.1. Tanım. K bir cisim ve $a_1, a_2, a_3, a_4, a_6 \in K$ olmak üzere

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

biçimindeki denklemin tüm çözümlerinin oluşturduğu (x, y) sıralı ikililerinin kümesine $\boldsymbol{O}$ noktası ile birlikte bir *eliptik eğri* denir ve bu denklem E eliptik eğrisinin *genelleştirilmiş Weierstrass denklemi*dir.

K bir cisim ve $\mathrm{kar}(K) \neq 2, 3$ olsun. $p, q \in K$ olmak üzere $4p^3 + 27q^2 \neq 0$ ise

$$E : y^2 = x^3 + px + q$$

şeklindeki bir denklem E eliptik eğrisinin *Weierstrass denklemi* olarak adlandırılır.

Eğer E, K cismi üzerinde tanımlı bir eliptik eğri ise bu eğri üzerindeki noktaların kümesi $E(K)$ ile belirtilir. Diğer bir ifade ile

$$E(K) = \{(x, y) \mid x, y \in K \times K \mid \ y^2 = x^3 + px + q\} \cup \{\boldsymbol{O}\}$$

dir. Ayrıca $E(K)$, E eliptik eğrisinin üzerindeki noktaların özel bir toplama işlemi ile bir gruptur ve bu grubun etkisiz elemanı ise $\boldsymbol{O}$ noktası, yani sonsuzdaki noktadır. Bu noktanın x-eksenine dik olan tüm doğruların üzerinde olduğu varsayılır.

Bir E eliptik eğrisi üzerindeki iki noktanın toplamı şu şekilde tanımlanır: Eğer M ve N bir E eliptik eğrisi üzerinde iki farklı nokta ise bu noktalardan geçen d doğrusu alınır. Diğer yandan d doğrusu E eliptik eğrisini bir başka $M \clubsuit N$ noktasında keser, $M \clubsuit N$ noktasının x-eksenine göre simetriği olan nokta $M + N$ olarak tanımlanır. M noktasını kendisi ile toplamak için M noktasından geçen teğet doğru denklemi bulunur. M noktasının x-eksenine göre simetriği olan M' noktası ile toplamı ise

$$M + M' = \boldsymbol{O}$$

dur. Son olarak E eliptik eğrisi üzerindeki her bir M noktasının için

$$M + \boldsymbol{O} = M$$

dir.

Aşağıda ifade edilen kuralla tanımlanan bu toplama işlemi için bir algoritma verilmiştir.

1.4.2 Algoritma (Grup Kuralı). E, Weierstrass denklemi ile verilen bir eliptik eğri olmak üzere bu eğri üzerinde $M = (x_1, y_1)$ ve $N = (x_2, y_2)$ noktalarını alalım.

1. Eğer her $M \in E(K)$ için $M + \boldsymbol{O} = M$ dir.

2. $x_1 = x_2$ ve $y_1 + y_2 = 0$ ise $M + N = \boldsymbol{O}$ dur.

3. $M \neq N$ ve $x_1 \neq x_2$ ise

$$e = \frac{y_2 - y_1}{x_2 - x_1}$$

ve $M = N$ ve $y_1 \neq 0$ ise

$$e = \frac{3x_1^{\,2} + a}{2y_1}$$

olmak üzere

$$x_3 = e^2 - x_1 - x_2 \text{ ve } y_3 = e(x_1 - x_3) - y_1$$

ve böylece $M + N = (x_3, y_3)$ tür.

Böylece aşağıdaki teorem verilebilir.

1.4.3. Teorem. E, bir K cismi üzerinde tanımlı bir eliptik eğri ise $E(K)$ eliptik eğrilerin üzerinde tanımlanan toplama işlemine göre bir değişmeli gruptur (Silverman 2009).

1.4.4. Uyarı. E, $y^2 = x^3 + px + q$ denklemi ile verilmiş bir eğri ve $M = (x, y)$, E eğrisi üzerinde bir nokta ise $-M = (x, -y)$ dir. Ayrıca $M \in E$ ve $k \in \mathbb{Z}$ olmak üzere $k > 0$ ise

$$kM = \underbrace{M + \ldots + M}_{k \tan e}$$

ve $k < 0$ ise

$$kM = (-k)(-M)$$

dir ve $0M = \boldsymbol{O}$ olarak tanımlanır.

2. KURAMSAL TEMELLER VE KAYNAK ARAŞTIRMASI

Bu kısımda ilk olarak Bang (1886) tarafından ele alınmış, 1892'de Zsigmondy tarafından genelleştirilmiş ve 1904'de Birkoff ve Vandiver tarafından yeniden keşfedilmiş olan sayılar teorisinin klasik teoremlerinden Zsigmondy teoremi ele alınacak ve bu teoremin bir elementer ispatı verilecektir.

2.1. Zsigmondy Teoremi.

Zsigmondy teoremini ifade etmeden önce bir tamsayı dizisindeki ilkel asal bölen tanımına ihtiyaç vardır.

2.1.1. Tanım. (A_n) tamsayıların bir dizisi ve n bir doğal sayı olmak üzere $A_n \neq 0$ terimini bölen bir p asal sayısı her $m < n$ için A_m terimlerini bölmüyorsa p asal sayısı A_n teriminin bir *ilkel asal böleni*dir denir.

(A_n) tamsayılar dizisinin *Zsigmondy kümesi* $Z(A_n)$ ile gösterilir ve

$$Z(A_n) = \{n \mid A_n \text{ teriminin bir ilkel asal böleni yoktur.}\}$$

biçiminde tanımlanır. Bu kümenin supremumu, yani $\sup(Z(A_n))$ sayısına ise (A_n) tamsayılar dizisinin *Zsigmony sınırı* denir.

2.1.2. Örnek 1. $F_n = F_{n-2} + F_{n-1}$ eşitliği ile verilen Fibonacci dizisi için Zsigmody kümesi $Z(F_n) = \{1, 2, 6, 12\}$ dir. Diğer bir ifade ile Fibonacci dizisinin birinci, ikinci,

altıncı ve on ikinci terimleri dışındaki tüm terimleri birer ilkel asal bölene sahiptir. Dolayısıyla, (F_n) dizisinin Zsigmondy sınırı $\sup(Z(F_n)) = 12$ dir.

2. Zsigmondy (1892), $M_n = 2^n - 1$ eşitliği ile verilen

$$1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, ...$$

Mersenne dizisinin birinci ve altıncı terimleri dışındaki tüm terimlerinin birer ilkel asal bölen bulundurduğunu göstermiştir. Diğer bir ifade ile $\sup(Z(M_n)) = 6$ olduğunu ispat etmiştir. Aşağıdaki çizelgede bu dizinin ilk on terimi çarpanlarına ayrılarak ilkel asal bölenleri koyu olarak belirtilmiştir.

Çizelge 2.1. (M_n) dizisinin ilkel asal bölenleri

n	M_n	Çarpanlar
2	3	**3**
3	7	**7**
4	15	$3 \cdot$ **5**
5	31	**31**
6	63	$3^2 \cdot 7$
7	127	**127**
8	255	$3 \cdot 5 \cdot$ **17**
9	511	$7 \cdot$ **73**
10	1023	$3 \cdot$ **11** $\cdot 31$
11	2047	**23** $\cdot$ **89**
12	4095	$3^2 \cdot 5 \cdot 7 \cdot$ **13**
13	8191	**8191**
14	16383	$3 \cdot$ **43** $\cdot 127$

3. $C_n = 7^n - 2^n$ eşitliği ile verilen $(C_n)_{n \geq 1}$ dizisinin terimleri

$$5, 45, 335, 2385, 16775, 117585, 823415, 5764545, ...$$

biçimindedir ve bu dizinin tüm terimleri bir ilkel asal bölen bulundurur.

Zsigmondy, daha genel olarak a ve b aralarında asal pozitif tamsayılar ve $a > b$ olmak üzere $(a^n - b^n)_{n \geq 1}$ dizisinin, $n = 6$, $a = 2$ ve $b = 1$ olması veya $n = 2$ ve $a + b$ sayısı 2 nin bir kuvveti olmaması halinde bir ilkel asal bölene sahip olduğunu göstermiştir. Diğer bir ifade ile $\sup(Z(a^n - b^n)) \leq 6$ dır.

2.1.3. Teorem (Zsigmondy Teoremi). a ve b aralarında asal pozitif tamsayılar, $a > b$ olmak üzere $(a^n - b^n)_{n \geq 1}$ dizisi verilsin. Bu durumda $n = 6$, $a = 2$ ve $b = 1$ veya $n = 2$ ve $a + b$ sayısı 2 nin bir kuvveti değilse $a^n - b^n$ terimini bölen ve her $k < n$ tamsayısı için $a^k - b^k$ terimini bölmeyen $a^n - b^n$ teriminin bir ilkel asal böleni vardır (Zsigmondy, 1892).

2.1.4 Uyarı 1. $n = 1$, $a - b = 1$ ise $a^n - b^n = 1$ dir ve bu ifadenin ilkel asal böleninin olmadığı açıktır.

2. $n = 2$ halini dikkate alınırsa $a^2 - b^2$ teriminin bir ilkel asal böleni yoksa $a + b$ yi bölen her p asalı $a^2 - b^2$ terimini de böler ve dolayısıyla $a - b$ yi de böler. Böylece ortak çarpan olan bu p asalı $a^2 - b^2$ nin çarpanlarının toplamı olan $(a + b) + (a - b) = 2a$ sayısını ve farkı olan $(a + b) - (a - b) = 2b$ sayısını da böler. Diğer bir ifade ile

$$p \mid 2a \quad \text{ve} \quad p \mid 2b$$

dir. Diğer yandan a ve b tamsayıları aralarında asal olduğundan $p = 2$ dir. O halde $a + b$, 2 nin bir kuvvetidir. Dolayısıyla Zsigmondy teoreminin ispatı verilirken $n > 2$ olarak alınacaktır.

3. $a - b = 1$ hali dışında $a^n - b^n$ terimi

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$$

biçiminde ifade edilebildiğinden $a^n - b^n$ terimi $a - b$ ile bölünebilir. Bununla birlikte a ve b aralarında asal pozitif tamsayılar olmak üzere $((a^n - b^n)/(a - b))$ dizisinin sonsuz çoklukta asal terime sahip olduğu bilinmektedir.

4. Daha sonra Zsigmondy teoremi daha genel lineer dizilere, sayı cisimlerine ve eliptik dizilere genelleştirilmiştir. Zsigmondy teoreminin Diophantine denklemlerinin çözümünde ve sonlu gruplar teorisinde uygulamaları bulunmaktadır.

2.2. Zsigmondy Teoreminin İspatı.

Bu kısımda a ve b aralarında asal pozitif tamsayılar, $a > b$ olmak üzere $(a^n - b^n)_{n \geq 1}$ dizisi için Zsigmondy teoreminin ispatı verilecek ve bunun için $\phi_n(a, b)$, n. homojenize döngüsel polinomunun özellikleri kullanılacaktır. Hatırlanacağı gibi n. homojenize döngüsel polinom için

$$a^n - b^n = \prod_{d|n} \phi_d(a,b)$$

dir.

İlk olarak $a^n - b^n$ teriminin bir ilkel asal böleninin olmadığını varsayalım. Eğer $\phi_n(a, b)$ nin bir asal çarpanı yoksa $\phi_n(a, b) = 1$ dir, aksi halde $\phi_n(a, b)$ nin bir p asal çarpanı vardır, yani $p \mid a^n - b^n$ dir. Dolayısıyla varsayım gereği $p \mid a^k - b^k$ olacak biçimde bir en küçük $1 \leq k < n$ sayısı vardır.

Diğer yandan $\text{ord}_p(\phi_n(a, b)) \geq 1$ olduğundan belli bir $m \geq 1$ tamsayısı için $n = p^m k$ olarak yazılabilir. Burada k, a/b nin $\mathbb{Z}_p^*$ daki mertebesi olduğundan $k \mid p - 1$, yani $k < p$ dir. Bu ise p asalının n tamsayısının en büyük asal böleni olduğunu gösterir. Aksi halde n tamsayısının en büyük asal böleni p asalından büyüktür ve k sayısını böler ki bu $k < p$

olması ile çelişkidir. Eğer p bir tek asal sayı ise $\text{ord}_p(\phi_n(a, b)) = 1$ dir. Eğer $p = 2$ ise $n \geq 3$ sayısı 2 nin bir kuvveti ve dolayısıyla $4 \mid n$ olması

$$\phi_n(a, b) = a^{n/2} + b^{n/2} \equiv 2 \pmod 4$$

olmasını gerektirir. Bu ise bu halde de $\text{ord}_p(\phi_n(a, b)) = 1$ olduğunu göster. Dolayısıyla $\phi_n(a, b) = 1$ dir veya p asalı n tamsayısının en büyük asal çarpanıdır. Diğer yandan $\phi_n(a, b)$ nin alt sınırı p olduğundan döngüsel polinomlar için verilen sınır teoremi kullanılarak

$$p \geq \phi_n(a, b) \geq (a - b)^{\varphi(n)} \geq (a - b)^{p-1}$$

olduğu elde edilir. Eğer $a - b \geq 2$ ise eşitlik sadece $p = 2$ ve $n = 2$ olması durumda doğru olur ki bu $n > 2$ olması ile çelişkidir.

Eğer $a - b = 1$ ise $m \geq 1$ bir tamsayı olmak üzere $n = p^m k$ olarak yazılabilir. Eğer $m \geq 2$ ise

$$p \geq \phi_n(a, b) = \phi_{p^m k}(a, b) = \phi_{pk}(a^{p^{m-1}}, b^{p^{m-1}})$$

$$\geq (a^{p^{m-1}} - b^{p^{m-1}})^{\varphi(pk)}$$

$$\geq a^p - b^p = pb^{p-1} + pb^{p-2} + \ldots + 1 \qquad (a = b + 1 \text{ olduğundan})$$

olur ki bu $p > 2$ olduğundan bir çelişkidir. O halde $m = 1$ olmalıdır. Bu ise $n = pk$ olduğunu gösterir. Dolayısıyla

$$p \geq \phi_n(a, b) = \frac{\phi_k(a^p, b^p)}{\phi_k(a, b)} \geq \frac{(a^p - b^p)^{\varphi(k)}}{(a + b)^{\varphi(k)}}$$

$$\geq \frac{(a^p - b^p)}{a + b} \geq \frac{(2^p - 1)b}{2b + 1} \geq \frac{2^p - 1}{3}$$

olduğu elde edilir. Bu ise $p > 3$ olması halinde mümkün değildir, o halde $p = 3$ olmalıdır. Üstelik bu halde $p = \phi_n(a, b)$ olduğu kolayca görülebilir. Diğer yandan $k < p$ olduğundan $k = 1$ veya 2 ve dolayısıyla $n = 3$ veya 6 dır.

Eğer $n = 3$ ise $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$ ve $a - b = 1$ olduğundan $a^2 + ab + b^2$ bir ilkel bölendir, yani teorem $n = 3$ için doğrudur. Bununla birlikte

$$3 = \phi_6(a, b) = a^2 - ab + b^2$$

olduğundan $a = 2$ ve $b = a - 1 = 1$ dir, yani $n = 6$ için Zsigmondy teoremi geçerli değildir. Bu ise Zsigmondy teoreminin ispatını tamamlar.

2.3. Zsigmondy Teoreminin Uygulamaları.

Bu kısımda yukarıda ele alınmış olan Zsigmondy teoreminin uygulamaları olarak bazı matematik olimpiyatlarının soruları ele alınacaktır. Bu örneklere (Loo, 2012)'den ulaşılabilir.

2.3.1. Örnek (Japanese MO 2011). $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$ eşitliğini gerçekleyen tüm (a, n, p, q, r) pozitif tam sayı beşlilerini bulunuz.

Çözüm. Problemin çözümü için Zsigmondy teoremini kullanalım. Buna göre $a \geq 3$ ve $n \geq 3$ ise $n > p, q, r$ olduğundan $a^n - 1$ sayısının $a^p - 1$, $a^q - 1$ ve $a^r - 1$ sayılarını bölmeyen bir asal çarpanı vardır. Dolayısıyla $a \geq 3$ ve $n \geq 3$ için çözüm yoktur. O zaman $a < 3$ veya $n < 3$ olması durumlarını inceleyelim.

İlk olarak $a = 1$ ise

$$1^n - 1 = (1^p - 1)(1^q - 1)(1^r - 1)$$

olduğundan $n = 1, 2$ için $1^n - 1 = 0$ dır. Dolayısıyla her p, q, r pozitif tam sayıları için eşitlik gerçeklenir.

$a = 2$ ise

$$2^n - 1 = (2^p - 1)(2^q - 1)(2^r - 1)$$

dir. $n = 1$ için yukarıdaki eşitliğin sol tarafı 1'e eşit olduğundan p, q, r değerleri de 1'e eşit olmalıdır. Böylece $(a, n, p, q, r) = (2, 1, 1, 1, 1)$ pozitif tam sayı beşlisi elde edilir. Diğer yandan $n = 2$ ise

$$3 = (2^p - 1)(2^q - 1)(2^r - 1)$$

dir. Bu halde eşitliğin sol tarafı 3 olduğundan sağ taraftaki çarpanlardan birisi 3 diğerleri 1'dir. Dikkat edilirse bu çarpanlar negatif olamazlar. O halde üç hal söz konusudur:

i) $2^p - 1 = 3$, $2^q - 1 = 2^r - 1 = 1$ ise $p = 2$, $q = r = 1$ olduğundan

$$(a, n, p, q, r) = (2, 2, 2, 1, 1)$$

ii) $2^q - 1 = 3$, $2^p - 1 = 2^r - 1 = 1$ ise $q = 2$, $p = r = 1$ olduğundan

$$(a, n, p, q, r) = (2, 2, 1, 2, 1)$$

iii) $2^r - 1 = 3$, $2^q - 1 = 2^p - 1 = 1$ ise $r = 2$, $q = p = 1$ olduğundan

$$(a, n, p, q, r) = (2, 2, 1, 1, 2)$$

olarak bulunur.

2.3.2. Örnek (IMO Shortlist 2000). $a^m + 1 \mid (a + 1)^n$ olacak biçimindeki tüm (a, m, n) pozitif tam sayı üçlülerini bulunuz.

Çözüm. İlk olarak $a = 1$ için $1^m + 1 \mid 2^n$ olur ki bu önerme her m, n pozitif tam sayıları için doğrudur. Diğer yandan $a = 2$, $m = 3$ için $2^3 + 1 \mid (2 + 1)^n$ yani $9 \mid 3^n$ olduğundan bu önerme her $n \geq 2$ tamsayısı için doğrudur.

Şimdi $a > 1$, $m \geq 2$ ve $(a, m) \neq (2, 3)$ olsun. Bu durumda Zsigmondy teoremi gereği, $a^m + 1$ değerinin $a + 1$ değerini ve dolayısıyla $(a + 1)^m$ değerini bölmeyen bir asal çarpanı olduğundan diğer durumlar için (a, m, n) üçlüleri yoktur.

2.3.3. Örnek (MOSP 2001). p bir asal sayı, n, $r > 1$ ve $x^r - 1 = p^n$ olacak şekildeki tüm (x, r, p, n) pozitif tam sayı dörtlülerini bulunuz.

Çözüm. $x^r - 1$ sayısının $x - 1$ değerini bölmeyen bir asal çarpanı varsa $x^r - 1$, $x - 1$ ile bölündüğünden $x^r - 1$'in iki farklı asal çarpanı vardır. Bu ise $x = 2$, $r = 6$ olması ve $r = 2$ ve $x + 1$ değerinin 2 nin bir kuvvetidir istisnai durumları dışında Zsigmondy teoremi ile çelişir. Eğer $x = 2$ ve $r = 6$ ise $2^6 - 1 = 63$ bir p asalının kuvveti şeklinde yazılamaz, yani bu halde bir çözüm yoktur. Diğer yandan $r = 2$ ve $x + 1$, 2 nin bir kuvveti ise $x = 2^k - 1$, $k \geq 1$ biçiminde yazılabilir. Bu ise $x^r - 1$ sayısının çift ve dolayısıyla $p = 2$ olmasını gerektirir. O halde

$$2^n = x^2 - 1 = (x - 1)(x + 1) = 2^k (2^k - 2)$$

olduğundan $k > 2$ için eşitliğin sağ tarafı 2 den farklı bir çarpan bulunduracağından $k = 2$ ve böylece $x = 3$ ve $n = 3$ olarak bulunur.

2.3.4. Örnek (Balkan MO 2009). $5^x - 3^y = z^2$ eşitliğini sağlayan tüm pozitif tam sayı çözümlerini belirleyiniz.

Çözüm. Bu eşitlik 3 modülüne göre düşünülürse $z^2 \equiv 2^x \pmod 3$ olduğundan x bir çift sayı olmalıdır. O halde $k \geq 1$ bir tamsayı olmak üzere $x = 2k$ olarak yazılabilir ve böylece $5^x - 3^y = z^2$ eşitliği

$$3^y = 5^{2k} - z^2 = (5^k - z)(5^k + z)$$

olarak ifade edilebilir. Üstelik $5^k - z$ ve $5^k + z$ değerlerinin ortak çarpanı yoktur. Gerçekten de $p \mid 5^k - z$ ve $p \mid 5^k + z$ ise p asal sayısı bunların toplamlarını ve farklarını bölmelidir, yani

$$p \mid 5^{2k} \text{ ve } p \mid -2z$$

dir. Ancak bu halde z sayısı 5 sayısı bir katı olmalıdır ki bu $3^y = 5^{2k} - z^2$ olduğundan mümkün değildir. O halde $(5^k - z, 5^k + z) = 1$ ve dolayısıyla $5^k - z = 1$ ve $m \geq 2$ için $5^k + z = 3^m$ dir. Diğer yandan $5^k + z = 3^m$ ifadesinin her iki tarafına 1 eklenirse $5^k + z + 1 = 3^m + 1$ ve üstelik $5^k = z + 1$ olduğundan

$$2 \cdot 5^k = 3^m + 1$$

olduğu elde edilir. Eğer $m = 2$ ise $k = 1$ ve böylece $x = 2$, $y = 2$ ve $z = 4$ dir. Diğer yandan $m \geq 3$ için Zsigmondy teoremi gereği, $3^m + 1$ sayısının $3^2 + 1 = 10$ sayısını bölmeyen 2 ve 5 asallarından farklı bir asal çarpanı vardır ki bu bir çelişkidir. O halde bu eşitliğin $m \geq 3$ için bir çözümü yoktur.

2.3.5. Örnek. p bir asal sayı olmak üzere $p^k - 1 = 2^n(p - 1)$ eşitliğini sağlayan tüm pozitif tamsayı çözümlerini bulunuz (Loo, 2012).

Çözüm. İlk olarak $p = 2$ alınırsa $2^k - 1 = 2^n(2 - 1)$ ve dolayısıyla $2^k - 1 = 2^n$ olur ki bu durumda bu eşitliğin bir çözümü yoktur.

O halde $p > 2$ olarak alalım ve k sayısının asal olmadığını varsayalım. Böylece $k = x \cdot y$ olacak biçimde x ve y tamsayıları vardır ve dolayısıyla sorudaki eşitlik

$$p^{xy} - 1 = 2^n(p - 1)$$

biçiminde ifade edilebilir. O halde $p^{xy} - 1$ sayısının $p - 1$ sayısını bölmeyen bir asal çarpanı vardır. Diğer yandan $p^{xy} - 1$ sayısı $2^n(p - 1)$ sayısını da böldüğünden $p^{xy} - 1$ sayısının bu asal çarpanı 2 olmalıdır. Ancak Zsigmondy teoremine göre, $p^{xy} - 1$ sayısının $p - 1$ sayısını bölmeyen bir asal çarpanı olmalıdır ki bu bir çelişkidir. O halde $k = x \cdot y$ olarak yazılamaz yani k sayısı bir asal sayıdır.

Eğer $k = 2$ ise $p^2 - 1 = 2^n (p - 1)$ olduğundan

$$p = 2^n - 1$$

dir, yani p bir Mersenne asalıdır. Bu halde pozitif çözümler

$$(k, n, p) = (2, 2, 3), (2, 3, 7), (2, 5, 31), (2, 7, 127), \ldots$$

biçimindedir. Şimdi de k sayısının bir tek asal olduğunu varsayalım. Zsigmondy teoremine göre, $p^k - 1 = 2^n (p - 1)$ sayısının $p - 1$ sayısını bölmeyen bir asal çarpanı

vardır ve bu asal çarpan 2 olmalıdır ancak 2, $p - 1$ sayısını böler ki bu bir çelişkidir. O halde k sayısının bir tek asal olması durumunda bir çözüm yoktur.

2.4. Büyük Zsigmondy Asalları.

Tanım 2.1.1'de geçen p ilkel asal böleni $(a^n - 1)_{n \geq 1}$ dizisi için W. Feit (Feit, 1988) tarafından bir *Zsigmondy asalı* olarak da isimlendirilmiştir. Bu kısımda aşağıda tanımlanacak olan büyük Zsigmondy asalları ile ilgilenilecektir.

a bir pozitif tamsayı olmak üzere p asal sayısı $(a^n - 1)_{n \geq 1}$ dizisi için bir Zsigmondy asalı ise a sayısının p modülüne göre mertebesi n dir. Dolayısıyla Fermat'nın küçük teoremi gereği, $n \mid p - 1$ ve böylece $p \equiv 1 \pmod{n}$ dir. Diğer bir ifade ile $p \geq n + 1$ dir. O halde aşağıdaki tanım verilebilir.

2.4.1 Tanım. a bir pozitif tamsayı ve p asal sayısı $(a^n - 1)_{n \geq 1}$ dizisi için bir Zsigmondy asal sayısı olmak üzere ya $p > n + 1$ veya $p^2 \mid a^n - 1$ oluyorsa p Zsigmondy asal sayısına bir *büyük Zsigmondy asal sayısı* denir.

2.4.2. Örnek. Hatırlanacağı gibi $M_n = 2^n - 1$ eşitliği ile verilen Mersenne dizisinin terimleri

1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, …

biçimindedir ve Çizelge 2.1'de $n \geq 2$ için bu dizideki Zsigmondy asalları koyu olarak belirtilmiştir. Buna göre $n = 2$ için 3 asalı bir Zsigmondy asalı olduğu halde bir büyük Zsigmondy asalı değildir. Benzer biçimde $n = 4$, 10, 12 ve 18 için dizinin terimleri birer Zsigmondy asalı bulundurduğu halde bu asallar bir büyük Zsigmondy asalı değildir. Bu hallerde p^2 sayısı $2^n - 1$ sayısını bölmediği gibi $p = n + 1$ dir. Bundan başka bu dizinin $n = 6$ için bir Zsigmondy asalı olmadığından bir büyük Zsigmondy asalı da yoktur.

Üstelik aşağıda verilecek olan teoreme göre bu haller dışında Mersenne dizisinin tüm terimleri bir büyük Zsigmondy asalı bulundurur.

Feit (Feit, 1988) "*On Large Zsigmondy Primes*" adlı makalesinde büyük Zsigmondy asallarının ne zaman ortaya çıktığını belirlemiştir.

2.4.3. Teorem. a bir pozitif tamsayı olmak üzere p sayısı $(a^n - 1)_{n \geq 1}$ dizisi için bir Zsigmondy asalı olsun. Bu durumda aşağıdaki durumlar dışında (a, n) ikilisi için bir büyük Zsigmondy asalı vardır.

i) Belli bir $s \in \mathbb{N}$ sayısı ve $t = 0$ veya 1 için $n = 2$ ve $a = 2^s 3^t - 1$.

ii) $a = 2$ ve $n = 4$, 6, 10, 12 veya 18.

iii) $a = 3$ ve $n = 4$ veya 6.

iv) $a = 5$ ve $n = 6$ (Feit, 1988).

2.4.4. Örnek. $A_n = 7^n - 1$ eşitliği ile verilen $(A_n)_{n \geq 1}$ dizisinin terimleri

6, 48, 342, 2400, 16806, 117648, 823542, 5764800, 40353606, 282475248, …

biçimindedir. Aşağıdaki çizelgede $(7^n - 1)_{n \geq 1}$ dizisi için Zsigmondy asalları koyu olarak belirtilmiştir ve bunlardan büyük Zsigmondy asalı olanları belirtilmiştir.

Aşağıdaki çizelge dikkate alındığında $n = 2$ hali için bir Zsigmondy asalının ve dolayısıyla bir büyük Zsigmondy asalının olmadığı görülür. Bundan başka $n = 1$ için 2 ve 3 asalları birer Zsigmondy asalı olduğu halde sadece 3 asalı bir büyük Zsigmondy asalıdır. Üstelik $n = 2, 3, \ldots, 9$ için Zsigmondy asalları aynı zamanda birer büyük Zsigmondy asalıdır. Bununla birlikte $n = 10$ için 11 ve 191 asalları birer Zsigmondy asalı olduğu halde sadece 191 asalı bir büyük Zsigmony asalıdır.

Çizelge 2.2. $(7^n - 1)_{n \geq 1}$ dizisindeki büyük Zsigmondy asalları

n	$7^n - 1$	Çarpanlar	Büyük Zsigmondy Asalları
1	6	$\mathbf{2 \cdot 3}$	3
2	48	$2^4 \cdot 3$	–
3	342	$2 \cdot 3^2 \cdot \mathbf{19}$	19
4	2400	$2^5 \cdot 3 \cdot \mathbf{5^2}$	5
5	16806	$2 \cdot 3 \cdot \mathbf{2801}$	2801
6	117648	$2^4 \cdot 3^2 \cdot 19 \cdot \mathbf{43}$	43
7	823542	$2 \cdot 3 \cdot \mathbf{29} \cdot \mathbf{4733}$	29, 4733
8	5764800	$2^6 \cdot 3 \cdot 5^2 \cdot \mathbf{1201}$	1201
9	40353606	$2 \cdot 3^3 \cdot 19 \cdot \mathbf{37} \cdot \mathbf{1063}$	37, 1063
10	282475248	$2^4 \cdot 3 \cdot \mathbf{11} \cdot \mathbf{191} \cdot 2801$	191

2.5. Lineer Dizilerdeki İlkel Asal Bölenler.

Mersenne dizisi ve daha genel olarak Zsigmondy tarafından ele alınan $C_n = a^n - b^n$ dizileri her $n \geq 1$ için

$$C_{n+2} = (a+b)C_{n+1} - abC_n$$

bağıntısını gerçekleyen birer lineer dizidir. Daha genel olarak d ve e tamsayı katsayılı ikinci dereceden monik indirgenemez bir polinomun kökü (karakteristik polinom) olmak üzere

$$D_n = (d^n - e^n)/(d - e)$$

eşitliği ile verilen Lucas dizisi her $n \geq 1$ için

$$D_{n+2} = (d+e)D_{n+1} - deD_n$$

lineer indirgeme bağıntısını gerçekler. Bu eşitlikleri gerçekleyen (d, e) ikilisine bir *Lucas ikilisi* adı verilir. Bundan başka

$$E_n = d^n + e^n$$

eşitliği ile verilen eş-Lucas dizisinin de benzer bir indirgeme bağıntısını gerçeklediği görülebilir.

Benzer biçimde, r ve s sıfırdan farklı tamsayılar, d ve e sayıları $x^2 - \sqrt{r}\,x + s$ polinomun kökü olmak üzere her $n \geq 0$ için

$$G_n = \begin{cases} \dfrac{d^n - e^n}{d - e} & n \text{ tek} \\ \dfrac{d^n - e^n}{d^2 - e^2} & n \text{ çift} \end{cases}$$

eşitliği ile verilen G_n dizisine bir *Lehmer dizisi* adı verilir.

Carcmichael 1913'te yayınlanan makalesinde $n > 12$ için $(D_n)_{n \geq 1}$ Lucas dizisinin bir ilkel böleninin olduğunu ispat etmiştir. Gerçektende Fibonacci dizisinin 12. teriminin bir asal böleni olmadığından bu en iyi ihtimal olarak düşünülebilir. Bu sonuç Ward (1955) ve daha sonra Stewart (1977) tarafından Lehmer dizilerine genelleştirilmiştir.

2.5.1 Teorem. $n > 12$ için Lucas ve ve Lehmer dizilerin bir ilkel asal bölene sahiptir (Carcmichael 1913, Ward, 1955).

Daha sonra 2001 yılında Bilu ve ark., bu sonucu geliştirerek daha keskin bir sınır vermişlerdir. Buna göre, her $n > 30$ için n. Lucas ve Lehmer sayıları bir ilkel asal bölene

sahiptir. Böylece Bilu ve ark. (2001)'da bir ilkel asal bölene sahip olmayan tüm Lucas ve Lehmer dizilerini listelemişlerdir.

2.5.2 Teorem. $n > 30$ için n. Lucas ve Lehmer sayıları birer ilkel asal bölene sahiptir (Bilu ve ark., 2001).

Aşağıdaki örnekte verilen Lucas dizisinin 30. teriminin bir ilkel asal bölene sahip olmadığı görülmektedir.

2.5.3 Örnek 1. $(\frac{1+\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2})$ Lucas ikilisi ile elde edilen $(D_n)_{n \geq 1}$ Lucas dizisinin terimleri

1, –1, –3, –1, 5, 7, –3, –17, –11, 23, 45, –1, –91, –89, 93, 271, 85, –457, –627,

287, 1541, 967, –2115, –4049, 181, 8279, 7917, –8641,–24475, –7193, 41757, …

biçimindedir. Dikkat edilirse bu dizinin terimleri

$$D_{n+2} = D_{n+1} - 2D_n$$

indirgeme bağıntısını gerçeklerler. Üstelik dizinin 6. terimi 5, 10. terimi –11, 15. terimi –89 ve 30. terimi $-24475 = -5^2 \cdot 11 \cdot 89$ olduğundan bu dizinin 30. terimi bir ilkel asal bölene sahip değildir.

2. Benzer biçimde $(\frac{1+\sqrt{-15}}{2}, \frac{1-\sqrt{-15}}{2})$ Lucas ikilisi ile elde edilen $(D_n)_{n \geq 1}$ Lucas dizisinin terimleri

1, 1, –3, –7, 5, 33, 13, –119, –171, 305, 989, –231, –40187, –3263, 13485, 26537, –27403, –133551, –23939, 510265, …

biçimindedir. Dikkat edilirse bu dizinin terimleri de

$$D_{n+2} = D_{n+1} - 4D_n$$

indirgeme bağıntısını gerçeklerler. Üstelik dizinin 3. terimi –3, 4. terimi –7, 6. terimi 33 ve 15. terimi –231 = 3·7·11 olduğundan bu dizinin 15. terimi bir ilkel asal bölene sahip değildir.

3. MATERYAL VE YÖNTEM

Daha önceki kısımlarda ele alınan bir lineer dizideki asal ilkel bölenlerin bulunması problemi lineer olmayan dizilere de genelleştirilebilir. Bu kısımda ilk olarak iki farklı biçimde lineer olmayan eliptik dizi kavramı tanımlanacak ve daha sonra bu dizilerin eliptik eğrilerle olan ilişkisi kullanılarak bu dizilerde ortaya çıkan ilkel asal bölenler belirlenecektir.

3.1. Eliptik Diziler.

Bu kısımda eliptik bölünebilir diziler tanıtılacak, bu dizilerle ilgili örnekler verilecek ve bu dizilerin temel özellikleri ele alınacaktır. Daha sonraki kısımlarda ise bu dizilerin klasik tanımından (Ward (1948) tanımından) farklı bir biçimde tanımı verilerek özellikleri üzerinde durulacaktır.

3.1.1. Tanım. Başlangıç terimleri d_0, d_1, d_2, d_3 tam sayıları olan ve her $m \geq n \geq 1$ için lineer olmayan

$$d_{m+n}\, d_{m-n} = d_{m+1}\, d_{m-1} d_n^{\,2} - d_{n+1} d_{n-1} d_m^{\,2} \tag{3.1}$$

indirgeme bağıntısını gerçekleyen (d_n) dizisine bir *eliptik dizi* denir ve üstelik $n \mid m$ iken $d_n \mid d_m$ ise (d_n) dizisine bir *eliptik bölünebilir dizi* (*EBD*) adı verilir. Eğer

$$d_0 = 0,\ d_1 = 1 \text{ ve } d_2 d_3 \neq 0$$

ise (d_n) dizisine bir *has eliptik bölünebilir dizi* denir.

3.1.2. Uyarı 1. (3.1) eşitliği kullanılarak bir EBDnin çift ve tek indisli terimlerinin hesaplanması için daha kullanışlı formüller elde edilebilir. Buna göre (3.1) eşitliğinde $n = 2$ olarak alınırsa

$$d_{m+2}\, d_{m-2} = d_{m+1}\, d_{m-1}\, d_2^{\,2} - d_3\, d_1\, d_m^{\,2} \tag{3.2}$$

eşitliği elde edilir. Ayrıca (3.1) eşitliğinde, öncelikle $m = n + 1$, $n = n$ ve daha sonra ise $m = n + 1$, $n = n - 1$ yazılırsa, sırasıyla,

$$d_{2n+1} = d_{n+2}\, d_n^{\,3} - d_{n-1}\, d_{n+1}^{\,3} \tag{3.3}$$

$$d_{2n}\, d_2 = d_n\,(d_{n+2}\, d_{n-1}^{\,2} - d_{n-2}\, d_{n+1}^{\,2}) \tag{3.4}$$

eşitlikleri elde edilir. Bu eşitliklerdeki formüllere *duplikasyon formülleri* denir. Bu eşitliklere n üzerine tümevarım uygulanarak bir EBDnin 4. teriminden sonraki her bir teriminin d_1, d_2, d_3 ve d_4 başlangıç terimleri ile elde edilebileceği görülebilir.

2. (d_n) bir has eliptik bölünebilir dizi ise her $n \in \mathbb{N}$ için

$$d_{-n} = -d_n$$

dir. Gerçektende $d_{n+2} \neq 0$ olduğu varsayılır ve (3.1) eşitliğinde $m = 1$, $n = n + 1$ yazılırsa

$$d_{n+2}\, d_{-n} = -d_{n+2}\, d_n$$

eşitliği elde edilir. Böylece $d_{n+2} \neq 0$ olduğundan $d_{-n} = -d_n$ olduğu elde edilir.

3. $d_{-n} = -d_n$ eşitliği kullanılarak (d_n) dizisinin tüm negatif indisli terimlerin de d_1, d_2, d_3 ve d_4 başlangıç terimleri ile belirlenebileceği sonucu elde edilir.

4. Eğer (3.3) eşitliğinde $n = 2$ yazılırsa

$$d_5 = d_4\, d_2^{\,3} - d_1\, d_3^{\,3}$$

olarak bulunur, yani d_1, d_2, d_3 ve d_4 başlangıç terimleri kullanılarak d_5 terimi elde edilir. Şimdi d_5 terimi bilindiğinden benzer biçimde bu kez (3.4) eşitliğinde $n = 3$ yazılırsa d_6 terimi elde edilir. Bu şekilde devam edilerek dizinin tek ve çift indisli diğer tüm terimleri ikiye katlama (duplikasyon) formülleri yardımıyla elde edilmiş olur. O halde bir eliptik bölünebilir dizinin ilk beş terimi biliniyorsa (d_n) dizisinin tüm terimleri belirlenebilir, yani (d_n) dizisi iyi tanımlıdır.

5. Eğer (d_n'), başlangıç terimleri d_0', d_1', d_2', d_3' ve d_4' olan bir eliptik bölünebilir dizi olmak üzere

$$d_0 = d_0',\ d_1 = d_1',\ d_2 = d_2',\ d_3 = d_3',\ d_4 = d_4'$$

ise (d_n) ve (d_n') dizileri *özdeş dizi*lerdir. Bu nedenle bir eliptik bölünebilir dizi ilk beş terimi ile bir tek şekilde ifade edilebilir. Bundan başka bir has eliptik bölünebilir dizi için $d_0 = 0$ ve $d_1 = 1$ olduğundan bir has eliptik bölünebilir dizinin tüm terimleri ise sadece d_2, d_3 ve d_4 terimleri ile belirlenir. Bu sonuç Teorem 3.1.5'te ifade edilecektir.

3.1.3. Örnek 1. $d_n = n$ eşitliği ile verilen

$$\ldots,-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots$$

tamsayılar dizisi en iyi bilinen eliptik bölünebilir dizi örneğidir. Gerçektende

$$d_0 = 0,\ d_1 = 1 \text{ ve } d_2 \mid d_4$$

ve bu dizinin tüm terimlerinin tamsayı olduğu açıktır. Bundan başka

$$d_{m+n}\, d_{m-n} = (m+n)(m-n) = m^2 - n^2$$

ve

$$\begin{aligned} d_{m+1}\, d_{m-1}\, d_n^2 - d_{n+1}\, d_{n-1}\, d_m^2 &= (m^2-1)n^2 - (n^2-1)m^2 \\ &= m^2n^2 - n^2 - n^2m^2 + m^2 \\ &= m^2 - n^2 \end{aligned}$$

olduğundan (d_n) dizisi (3.1) eşitliğini gerçekler ve dolayısıyla bir has eliptik bölünebilir dizidir.

2. Başlangıç terimleri

$$e_0 = 0, e_1 = 1, e_2 = -1, e_3 = 2, e_4 = 1$$

olan ve terimleri

$$-9, 20, -71, -161, 1478, -7839, 43759, 361640, -4509199, 58538719,$$
$$-445526838, -13396178719, 26194973151, -8124893273540,$$
$$63728599810409, 8609476941663039, -298048597483659122, \ldots$$

biçiminde devam eden (e_n) dizisi de bir has eliptik bölünebilir dizidir ve bu dizi

$$e_{m+2}\, e_{m-2} = e_{m+1}\, e_{m-1} - 2e_m^{\,2}$$

indirgeme bağıntısını gerçekler.

3. Başlangıç terimleri

$$f_0 = 0, f_1 = 1, f_2 = 3, f_3 = -1, f_4 = 5$$

olan ve terimleri

$$136, -\frac{1199}{3}, -511, -\frac{838315}{9}, \frac{7396493}{3}, \frac{179877136}{27}, -\frac{26087328437}{27}, \ldots.$$

biçiminde devam eden (f_n) dizisi de bir eliptik dizidir ancak bu dizi bir bölünebilir dizi değildir. Dikkat edilirse dizininin başlangıç terimleri birer tamsayı olduğu halde f_2 terimi f_4 terimini bölmez. Bu ise $n \mid m$ olduğu halde f_n teriminin f_m terimini bölmediğini gösterir.

Ward, bir has EBDnin ardışık iki terimi sıfır ise dizinin diğer tüm terimlerinin de sıfır olduğunu göstermiştir.

3.1.4 Lemma. Bir (d_n) has eliptik bölünebilir dizinin ardışık iki terimi sıfır ise $n \geq 4$ için $d_n = 0$ dır (Ward 1948).

3.1.5. Uyarı 1. Bununla birlikte dizinin başlangıç terimleri sıfır olmadığı halde bazı terimleri sıfır olabilir. Bu durum Kısım 3.2'de ele alınan bir eliptik eğri ile eşleşen EBD kavramı ve dolayısıyla $\mathbb{Q}$ üzerinde tanımlı eliptik eğrilerin üzerindeki büküm noktalarının oluşturduğu grubun grup yapısı ile ilgilidir. Buna göre, bir EBDnin 7. terimi sıfır olabileceği halde 11. terimi sıfır olamaz. Diğer yandan bir EBDnin 7. terimi sıfır ise her k doğal sayısı için $7k$. terimlerinin de sıfır olacağı açıktır.

2. Bir EBDnin başlangıç terimlerinden ikinci, üçüncü veya dördüncü terimlerinden birisinin sıfır olması halinde, sırasıyla her k doğal sayısı için $2k$., $3k$. veya $4k$. terimlerinin de sıfır olacağı açıktır.

Aşağıdaki örnekte 7. terimi sıfır olan bir EBD verilmiştir. Dikkat edilirse bu dizinin 7. terimi sıfır olduğundan her k doğal sayısı için $7k$. terimi de sıfırdır.

3.1.6. Örnek. İlk 7 terimi

$$d_0 = 0,\ d_1 = 1,\ d_2 = -18,\ d_3 = -5832,\ d_4 = 11337408$$

$$d_5 = 132239526912,\ d_6 = -27763953154228224,\ d_7 = 0$$

ve dizinin daha sonraki diğer 7 terimi

d_8 =396521139274783615537700143104,

d_9 = –269731316194982757663962754241706065 92,

d_{10} = –330269830064458892427295904529733084682427301888,

d_{11} = 24263736711693263194228387613594560866881223119454024 4992,

d_{12} = 106954168795721455442075464896743512960425385140417235450288857415 68,

d_{13} = –8486141209687438822432888378408699504997495610554650194374226827 9036727678468096,

d_{14} = 0

biçimindedir.

Aşağıdaki teoremde, Ward başlangıç terimleri tamsayılar olan bir has eliptik bölünebilir dizinin tüm terimlerinin birer tamsayı olduğunu ve bu dizinin bölünebilir olduğunu göstermiştir.

3.1.7. Teorem. (d_n) bir has EBD ve d_2, d_3 ve d_4 terimleri birer tamsayı olmak üzere $d_2 \mid d_4$ olsun. Bu durumda (d_n) dizisinin tüm terimleri birer tamsayıdır ve üstelik her m, $n \in \mathbb{N}$ için

$$n \mid m \;\Rightarrow\; d_n \mid d_m$$

dir. Bundan başka (d_n) dizisi d_2, d_3 ve d_4 terimleri ile bir tek şekilde belirlenir (Ward, 1948).

İspatın taslağı. Teoremin ispatı için $d_2 \neq 0$ olduğu varsayılarak tümevarım kullanılabilir ve böylece aşağıdaki üç iddia ispat edilebilir.

(*i*) (d_n) dizisinin tüm terimleri tamsayıdır ve her n için d_2 terimi d_{2n} terimini böler.

(*ii*) (d_n) bir bölünebilir dizidir.

(*iii*) $n > 4$ için $d_0, d_1, \ldots, d_{n-1}$ terimleri bir tek şekilde belirlenirse d_n terimi de bir tek şekilde belirlenir.

3.1.8. Uyarı. Bir EBDnin başlangıç terimlerinin tamsayı olması dizinin diğer tüm terimlerinin tamsayı olmasını gerektirmediği Örnek 3.1.3 (3)'te görülmüştü. Bununla birlikte Ward'ın bu teoremi bir EBDnin başlangıç terimlerinin tamsayı olması ve üstelik

dizinin ikinci teriminin dördüncü terimini bölmesi halinde dizinin tüm terimlerinin birer tamsayı olduğunu gösterir.

3.2. Eliptik Bölünebilir Diziler ve Eliptik Eğriler

Bu kısımda eliptik eğriler ve eliptik fonksiyonlar arasındaki ilişkiler kullanılarak bunların eliptik bölünebilir dizilerle olan ilişkisi verilecektir. Bunun için öncelikle bir E eliptik eğrisinin bölüm polinomu kavramı üzerinde durulacaktır.

3.2.1. Tanım. E, bir F cismi üzerinde tanımlı ve

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Weierstrass denklemi ile verilen eliptik eğri olmak üzere E eğrisinin p_n *bölüm polinomları* başlangıç terimleri

$p_1 = 1$

$p_2 = 2y + a_1x + a_3$

$p_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6 x + b_8$

$p_4 = p_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2))$

olmak üzere diğer terimleri $n \geq 2$ için

$p_{2n+1} = p_{n+2}p_n^3 - p_{n-1}p_{n+1}^3$

ve $n \geq 3$ için

$p_{2n}p_2 = p_{n-1}^2 p_n p_{n+2} - p_{n-2}p_n p_{n+1}^3,$

bağıntıları ile tanımlanır.

3.2.2. Uyarı. Yukarıdaki tanımda ilk dört terimi ifade ederken kullanılan b_i değerleri E eliptik eğrisinin Tate değerleridir (Silverman 2009, Bölüm III.1).

2. Dikkat edilirse bir eliptik eğrinin bölüm polinomları da (3.3) ve (3.4)'te verilen bağıntıları gerçeklerler.

3. Üstelik bir E eliptik eğrisinin P noktasındaki bölüm polinomları yardımıyla P noktasının n katı yani nP noktasının koordinatları da ifade edilebilir. Buna göre, $r_n(P)$ ve $s_n(P)$ polinomları $p_n(P)$ bölüm polinomu yardımıyla verilen polinomlar, $r_n(P)$ ve $p_n(P)^2$ aralarında asal olmak üzere her $n \geq 1$ için

$$nP = \left(\frac{r_n(P)}{p_n(P)^2}, \frac{s_n(P)}{p_n(P)^3} \right)$$

dir (Silverman, 2009).

3.2.3. Örnek. $y^2 = x^3 - 36x$ eliptik eğrisi üzerindeki $(-2, 8)$ noktası ile elde edilen $n = 1, 2, \ldots, 7$ için $r_n(P)$, $s_n(P)$ ve $p_n(P)$ terimleri aşağıdaki çizelgede verilmiştir.

Çizelge 3.1. E üzerindeki $(-2, 8)$ noktası ile elde edilen $r_n(P)$, $s_n(P)$ ve $p_n(P)$ terimleri

n	$r_n(P)$	$s_n(P)$	$p_n(P)$
1	−2	8	1
2	25	35	2
3	−4418	−319976	33
4	1442401	−1726556399	140
5	−1074902978	394955797978664	44897
6	60473718955225	339760634079313268605	2639802
7	−15703132146020645762	−19830090239372020077660464072	1657367489

Ward (1948) eliptik fonksiyonları kullanarak bölüm polinomlarını $\mathbb{C}$ karmaşık sayılar cismi üzerinde tanımlamış ve eliptik fonksiyonlar ile eliptik bölünebilir diziler arasındaki ilişkiyi aşağıdaki teoremde ortaya koymuştur.

3.2.4. Teorem. (d_n) bir has eliptik bölünebilir dizi ve d_2, d_3, d_4 birer tamsayı olmak üzere $d_2|d_4$ olsun. Bu durumda $p_n(z, L)$ klasik n-bölüm fonksiyonu ve $\sigma(z, L)$ Weierstrass σ-fonksiyonu olmak üzere her $n \geq 1$ için

$$d_n = p_n(z, L) = \frac{\sigma(nz, L)}{\sigma(z, L)^{n^2}}$$

olacak biçimde bir $L \subset \mathbb{C}$ kafesi ve bir $z \in \mathbb{C}$ karmaşık sayısı vardır (Ward, 1948).

Ward'ın bu teoremi herhangi bir cisim üzerinde yeniden ifade edilebilir.

3.2.5. Teorem. E, bir F cismi üzerinde tanımlı bir eliptik eğri ve P, E eğrisi üzerinde bir nokta, $p_n(P)$ ise E eğrisinin P noktasındaki n. bölüm polinomu olmak üzere her $n \geq 1$ için

$$d_n = p_n(P)$$

olarak tanımlanan (d_n) dizisi bir EBDdir (Silverman, 2005).

Yukarıdaki teoremde olduğu gibi tanımlanan (d_n) dizisine *E eliptik eğrisi ve P noktası ile eşleşen bir EBD*dir denir.

3.3. Eliptik Bölünebilir Dizilerdeki İlkel Asal Bölenler.

Eliptik bölünebilir diziler Ward (1948)' de ele alınmış olan tanımdan (Tanım 3.1) farklı olarak da ifade edilebilirler. Buna göre bir eliptik eğri ve üzerinde bir büküm olmayan noktanın katlarının x-koordinatlarının paydaları yardımıyla tanımlanabilir. Diğer bir ifade ile P, bir K cismi üzerinde tanımlı bir E eliptik eğrisi üzerinde büküm olmayan bir nokta ve $x(nP)$,

$$nP = \left(\frac{r_n(P)}{p_n(P)^2}, \frac{s_n(P)}{p_n(P)^3} \right)$$

noktasının x-koordinatı olmak üzere $(p_n(P))$ dizisinin terimlerinin (3.1) bağıntısını gerçeklediği görülebilir ve üstelik $(p_n(P))$ bir bölünebilir dizidir. Bu gerçekten hareket ile Silverman (1988), Everest ve ark. (2006)'nın çalışmaları ile bir EBD aşağıdaki şekilde tanımlanabilir.

3.3.1. Tanım. P, bir K cismi üzerinde tanımlı bir E eliptik eğrisi üzerinde bir büküm olmayan nokta, $r_n(P)$ ve $p_n(P)^2$ aralarında asal olmak üzere her $n \geq 1$ için

$$x(nP) = \frac{r_n(P)}{p_n(P)^2}$$

olarak yazılsın. Bu durumda $(p_n(P))$ dizisine bir *eliptik bölünebilir dizi* denir.

3.3.2. Örnek 1. E: $y^2 + y = x^3 - 2x$ eliptik eğrisi üzerindeki $P = (0, -1)$ noktası ile elde edilen dizinin terimleri

$$1, 1, 4, 25, 79, 584, 8431, 46545, 3943156, 42087329, \ldots$$

biçimindedir. Eğri üzerindeki P noktasının n katının x-koordinatı ve bu noktanın x-koordinatının paydaları ile elde edilen $(p_n(P))$ dizisinin ilk 10 terimi aşağıdaki çizelgede verilmiştir.

Çizelge 3.2. E eğrisi üzerindeki P noktasının n katının x-koordinatı ve bu noktaların paydaları ile elde edilen $(p_n(P))$ dizisinin terimleri

n	$x(nP)$	$(p_n(P))$
1	0	1
2	4	1
3	$-\frac{15}{16}$	4
4	$\frac{316}{225}$	25
5	$-\frac{870}{6241}$	79
6	$\frac{666049}{341056}$	584
7	$-\frac{27182280}{71081761}$	8431
8	$\frac{33244748236}{2166437025}$	46545
9	$\frac{195895478305}{15548479240336}$	3943156
10	$\frac{28171729657096564}{1771343262354241}$	42087329

2. $E : y^2 = x^3 + 17$ eliptik eğrisi üzerindeki $P = (-2, 3)$ noktası ile elde edilen dizinin terimleri

1, 1, 5, 23, 181, 1740, 8749, 1247497, 33863035, 4642247999, …

biçimindedir.

Bu eğri üzerindeki P noktasının n katının x-koordinatı ve bu noktanın x-koordinatının paydası ile elde edilen $(p_n(P))$ dizisinin ilk 8 terimi de aşağıda verilmiştir.

Çizelge 3.3. E eğrisi üzerindeki P noktasının n katının x-koordinatı ve bu noktaların paydaları ile elde edilen $(p_n(P))$ dizisinin terimleri

n	$x(nP)$	$(p_n(P))$
1	-2	1
2	8	1
3	$\frac{19}{25}$	5
4	$\frac{752}{529}$	23
5	$\frac{174598}{32761}$	181
6	$-\frac{4471631}{3027600}$	1740
7	$\frac{1287077867\ 8}{76545001}$	8749
8	$-\frac{3705032916\ 448}{1556248765\ 009}$	1247497

3.3.3 Uyarı 1. Silverman (1988), E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve P noktası E eğrisi üzerinde bir büküm olmayan nokta ise $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimlerinin bir ilkel asal bölene sahip olduğunu göstermiştir. Diğer bir ifade ile E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve $P \in E(\mathbb{Q})$ bir büküm olmayan nokta olmak üzere yeterince büyük n doğal sayıları için

$$nP \equiv \boldsymbol{O} \pmod{p} \text{ ve her } k < n \text{ için } kP \not\equiv \boldsymbol{O} \pmod{p}$$

olacak biçimde bir p asal sayısı vardır.

2. Bununla birlikte P noktası bir büküm nokta ise $(p_n(P))$ dizisinin sadece sonlu çokluktaki terimi bir ilkel asal bölen bulundurur.

Aşağıda Silverman'nın bu teoremi ifade edilmiştir.

3.3.4 Teorem. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ve $P \in E(\mathbb{Q})$ bir büküm olmayan nokta olmak üzere $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimleri bir ilkel asal bölene sahiptir (Silverman, 1988).

Silverman'nın bu sonucu herhangi bir sayı cismine genişletilebilir.

3.3.5 Teorem. E, bir K sayı cismi üzerinde tanımlı bir eliptik eğri ve $P \in E(K)$ bir büküm olmayan nokta olmak üzere $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimleri bir ilkel asal bölene sahiptir (Cheon ve Hahn, 1999).

Teorem 3.3.4 ve Teorem 3.3.5'teki sonuçlarda $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimleri bir ilkel asal bölene sahip olduğu belirtilmiş ancak açık bir sınır ortaya konulmamıştır. Bununla birlikte bazı özel dizi aileleri için (Everest ve ark., 2006) de olduğu gibi daha açık formüller verilebilir.

3.3.6 Teorem. $t > 0$ bir kare olmayan sayı olmak üzere E, $y^2 = x^3 - t^2x$ denklemi ile verilen $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri $P = (x(P), y(P))$, E eğrisi üzerinde bir büküm olmayan nokta olsun. Bu durumda $p_n(P)$ terimi bir ilkel asal bölene sahip değilse

i) n çift ise $n \leq 10$,

ii) n tek ise $n \leq 3$ ve $x(P) < 0$,

iii) n tek ise $n \leq 21$ ve $x(P)$ bir kare

dir (Everest ve ark., 2006).

3.3.7. Örnek. E: $y^2 = x^3 - 25x$ eliptik eğrisi üzerindeki $P = (-4, 6)$ noktası ile elde edilen dizinin terimleri

1, 12, 2257, 1494696, 8914433905, 178761481355556, 62419747600438859233, …

biçimindedir. Eğri üzerindeki P noktasının n. katının x-koordinatı ve P noktasının x-koordinatının paydaları ile elde edilen $(p_n(P))$ dizisinin ilk 6 terimi aşağıdaki çizelgede verilmiştir.

Çizelge 3.4. E eğrisi üzerindeki P noktası ile elde edilen $(p_n(P))$ dizisinin terimleri ve bu dizideki ilkel asal bölenler

n	$(p_n(P))$	Çarpanlar
1	1	1
2	12	$\mathbf{2^2 \cdot 3}$
3	2257	$\mathbf{37 \cdot 61}$
4	1494696	$2^3 \cdot 3 \cdot \mathbf{7^2} \cdot \mathbf{31} \cdot \mathbf{41}$
5	8914433905	$\mathbf{5} \cdot \mathbf{13} \cdot \mathbf{17} \cdot \mathbf{761} \cdot \mathbf{10601}$
6	178761481355556	$2^2 \cdot 3^2 \cdot \mathbf{11} \cdot 37 \cdot 61 \cdot \mathbf{71} \cdot \mathbf{587} \cdot \mathbf{4799}$

Çizelgeye dikkat edilirse $(p_n(P))$ dizisinin her terimi $n \geq 2$ için bir ilkel asal bölene sahiptir. Bu asal bölenler çizelgede koyu olarak belirtilmiştir.

Yabuta (2009), bu çalışmalardan esinlenerek bazı özel eliptik eğri aileleri üzerindeki büküm olmayan noktalardan elde edilen dizilerin alt dizilerindeki ilkel asal bölenlerle ilgilenmiştir.

3.3.8. Teorem. (*a*). D, 6 | $\mathrm{ord}_p D$ özelliğinde bir p asal böleni olmayan bir tam sayı olmak üzere E, $y^2 = x^3 + D$ denklemi ile verilen bir eliptik eğri olsun. $P \in E(\mathbb{Q})$ bir büküm olmayan nokta olmak üzere $(p_{2^n}(P))_{n\geq 0}$ eliptik bölünebilir dizisinin $p_{2^n}(P)$ terimi her $n \geq 3$ için bir ilkel asal bölene sahiptir.

(*b*). D, 4 | $\mathrm{ord}_p D$ özelliğinde bir p asal böleni olmayan bir tam sayı olmak üzere E, $y^2 = x^3 + Dx$ denklemi ile verilen bir eliptik eğri olsun. $P \in E(\mathbb{Q})$ bir büküm olmayan nokta olmak üzere $(p_{2^n}(P))_{n\geq 0}$ eliptik bölünebilir dizisinin $p_{2^n}(P)$ terimi her $n \geq 3$ için bir ilkel asal bölene sahiptir Yabuta (2009).

Yukarıdaki teoreme bir örnek olarak, E: $y^2 = x^3 + 26$ eliptik eğrisi üzerindeki $P = (-1, 5)$ noktasını ele alalım.

Çizelge 3.5. $y^2 = x^3 + 26$ eğrisi üzerindeki $P = (-1, 5)$ noktası ile elde edilen $(p_n(P))$ dizisinin terimleri ve terimlerdeki ilkel asal bölenler.

n	$(p_n(P))$	Çarpanlar
1	1	1
2	10	**2** · **5**
3	309	**3** · **103**
4	118540	2^2 · 5 · **5927**
5	89036371	**31**· **2872141**
6	709320892930	2 · 3 · 5 · **11** · **19** · **47**· 103 · **23369**
7	19283818696130359	$\mathbf{7}^3$ · **223** · **252112312831**
8	136891004808073663720	2^3 · 5 · 5927 · **11593** · **49806285863**
9	139961291771652438668459 8599	3^2 · **53** · 103 · **10151** · **27271** · **1089919** · **94416571**
10	37968679701109967700670252380 95950	2 · 5^2 · 31 · 2872141 · **5724028300720491**

Bu nokta ile elde edilen $(p_n(P))_{n\geq 0}$ dizisinin terimleri

1, 10, 309, 118540, 89036371, 709320892930, 19283818696130359,

136891004808073663720, 139961291771652438668459859 9,

37968679701109967700670252380959 50, …

biçimindedir. Eğri üzerindeki P noktasının x-koordinatının paydaları ile elde edilen $(p_n(P))$ dizisinin ilk 10 terimi ve bu terimlerdeki ilkel asal bölenler yukarıdaki çizelgede verilmiştir. Bu çizelgeye göre her $n = 2, \ldots, 10$ için $(p_n(P))$ dizisinin bir ilkel asal böleni vardır. Üstelik Teorem 3.3.8 (a)'ya göre her $n \geq 3$ için $(p_2^n(P))$ alt dizisinin tüm terimleri bir ilkel asal bölene sahiptir.

Bu kısımda Yabuta (2009)'da verilmiş olan Teorem 3.3.8'in (*a*) şıkkının ispatı ele alınacaktır. Teorem 3.3.8'in (*b*) şıkkının ispatı da benzer biçimde yapılabilir. Bunun için ikiye katlama formülünü kullanarak $y^2 = x^3 + D$ eğrisi üzerinde verilen bir $P \in E(\mathbb{Q})$ noktası için $x(2P)$ ve $y(2P)$ için formüller elde edelim.

$E : y^2 = x^3 + D$ ve $P = (u/e^2, v/e^3) \in E(\mathbb{Q})$ olmak üzere $2y_1y' = 3x_1^2$ olduğundan $m = 3u^2/2ve$ dir. Böylece $x(2P) = m^2 - 2x_1$ ikiye katlama formülünde $x_1 = u/e^2$ yazılırsa

$$x(2P) = u(9u^3 - 8v^2)/4v^2e^2 \tag{3.5}$$

eşitliği elde edilir. Benzer biçimde $y(2P) = -mx(2P) - (y_1 - mx_1)$ ikiye katlama formülünde $x_1 = u/e^2$ ve $y_1 = v/e^3$ yazılırsa

$$y(2P) = (-27u^6 + 36u^3v^2 - 8v^4) / 8v^3e^3 \tag{3.6}$$

olarak bulunur.

$p^k \parallel m$ gösterimi ile m sayısını bölen p asalının en büyük kuvvetinin k sayısı olduğu belirtilmektedir. Teorem 3.3.8'in (*a*) şıkkının ispatı için aşağıda bazı lemmalar verilmiştir.

3.3.9. Lemma. $P \in E(\mathbb{Q})$ olmak üzere $P = (u/e^2, v/e^3)$ ve en küçük terimlerle $2^nP = (u_n/e_n^2, v_n/e_n^3)$ olsun. Eğer u ve v aralarında asal ise v_n tektir ve 3 ile bölünemez, üstelik her $n \geq 1$ için u_n ve v_n aralarında asaldır (Yabuta, 2009).

İspat. İlk olarak

$$U = u(9u^3 - 8v^2) \text{ ve } V = -27u^6 + 36u^3v^2 - 8v^4$$

olsun. Eğer u çift ise $(u, v) = 1$ olduğundan v tektir ve $2^3 \parallel V$ dir. Ancak bu halde $y(2P)$ nin paydası 8 ile bölündüğünden v_1 ile e_1^3 aralarında asal olamaz. u tek ise V sayısı da tektir. Diğer yandan v sayısı 3 ile bölünebilirse $3^3 \parallel V$ dir. Bu halde de $y(2P)$ nin paydası da 27 ile bölünür ki bu v_1 ile e_1^3 nün aralarında asal olması ile çelişkidir. Eğer v sayısı 3 ile bölünmüyorsa V sayısı da 3 ile bölünmez. O halde v_1 tektir ve 3 ile bölünemez. Şimdi $(u_n, v_n) = 1$ olduğunu gösterelim. Bir p asal sayısı için $u_1 \equiv v_1 \equiv 0 \pmod{p}$ olsun. v_1 tek ve 3 ile bölünmediğinden $p \geq 5$ olarak alabiliriz. Böylece

$$u(9u^3 - 8v^2) \equiv 0 \pmod{p} \tag{3.7}$$

$$-27u^6 + 36u^3v^2 - 8v^4 \equiv 0 \pmod{p} \tag{3.8}$$

dir. Eğer $u \equiv 0 \pmod{p}$ ise (3.8) denkliğinden $v \equiv 0 \pmod{p}$ dir. Eğer $9u^3 - 8v^2 \equiv 0 \pmod{p}$ ve $v^2 = 9u^3/8$ değerleri (3.8) denkliğinde yerine yazılırsa $u \equiv v \equiv 0 \pmod{p}$ olur ki bu da u ile v sayılarının aralarında asal olması ile çelişir. Dolayısıyla u_1 ile v_1 sayıları aralarında asaldır. Diğer yandan n için tümevarım kullanılarak her $n > 1$ için u_n ve v_n sayılarının da aralarında asal olduğu sonucu elde edilir.

3.3.10. Lemma. $k, l > 0$, p bir asal sayı, s ve t sayıları p ile aralarında asal sayılar olmak üzere en küçük terimlerle $P = (p^k s/e^2, p^l t/e^3) \in E(\mathbb{Q})$ olarak yazılsın. Bundan başka s_n ve t_n sayıları p ile aralarında asal sayılar olmak üzere en küçük terimlerle

$$2^nP = \left(\frac{p^{k_n}s_n}{e_n^2}, \frac{p^{l_n}t_n}{e_n^3}\right)$$

olarak yazılsın. Ayrıca $v_n = 3k_n - 2l_n$ ve

$$T_{n+1} = -27p^{2v_n}s_n^{\,6} + 36p^{v_n}s_n^{\,3}t_n^{\,2} - 8t_n^{\,4}$$

olmak üzere s ve t sayıları aralarında asal olsun. Bu durumda her $n \geq 1$ tamsayısı için

(1) t_n tektir, 3 ile bölünemez ve s_n ile aralarında asaldır.

(2) $3p^{v_n}$ bir tam sayıdır ve $t_{n+1} = T_{n+1}$ veya $t_{n+1} = 2^{-3}\ T_{n+1}$ dir (Yabuta, 2009).

İspat. Teoremin ispatı için $x(2P)$ ve $y(2P)$ için verilmiş olan formülleri yeniden düzenleyelim. Eğer (3.5) ve (3.6) eşitliklerinde $u = p^k s$ ve $v = p^l t$ yazılır ve $v = 3k - 2l$ denirse

$$x(2P) = \frac{p^k s(9s^3 - 8t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2} \tag{3.9}$$

ve

$$y(2P) = \frac{p^l(-27p^{2v}s^6 + 36p^v s^3 t^2 - 8t^4)}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3} \tag{3.10}$$

olarak bulunur. $S_{n+1} = s_n(9p^{v_n}s_n^{\,3} - 8t_n^{\,2})$ olsun.

(1) Lemmanın bu şıkkının ispatı için Lemma 3.3.9' a benzer şekilde hareket edilir ve t_n sayısının tek, 3 ile bölünemez ve s_n ile aralarında asal olduğu görülebilir.

(2) Lemmanın bu şıkkını 3 durumda inceleyeceğiz.

1. Durum. İlk olarak $p \geq 5$ halini dikkate alalım.

i) $v > 0$ olsun. $(t, p) = (s, p) = 1$ ve $p \neq 2$ olduğundan $(s(9p^v s^3 - 8t^2), p) = 1$ dir ve böylece (3.9) eşitliği dikkate alınırsa

$$s_1 = s(9p^v s^3 - 8t^2)$$

dir. O halde v pozitif olduğundan $k_1 = k$ dır. Benzer şekilde $p \neq 2$ ve $(s, p) = 1$ olduğundan $(-27p^{2v}s^6 + 36p^v s^3 t^2 - 8t^4, p) = 1$ dir. (3.10) eşitliği dikkate alınırsa

$$t_1 = -27p^{2v}s^6 + 36p^v s^3 t^2 - 8t^4$$

ve $l_1 = l$ dir. Diğer bir ifade ile v pozitif ise $k_1 = k$, $l_1 = l$ ve $v_1 = 3k_1 - 2l_1 = 3k - 2l > 0$, yani v_1 değeri de pozitiftir.

ii) $v < 0$ olsun. Bu durumda

$$x(2P) = \frac{p^{k+v}s(9s^3 - 8p^{-v}t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

ve

$$y(2P) = \frac{p^{l+2v}(-27s^6 + 36p^{-v}s^3t^2 - 8t^4p^{-2v})}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3}$$

olarak yazılabilir. $v < 0$ ise $-v > 0$ ve böylece $(s(9s^3 - 8p^{-v}t^2), p) = 1$ yani

$$s_1 = s(9s^3 - 8p^{-v}t^2)$$

dir. Dolayısıyla $k + v = k_1$ dir. Benzer biçimde $(s, p) = 1$ olduğundan $(-27s^6 + 36p^{-v}s^3t^2 - 8t^4p^{-2v}, p) = 1$ yani

$$t_1 = -27s^6 + 36p^{-v}s^3t^2 - 8t^4p^{-2v}$$

dir. O halde $l_1 = l + 2v$ dir. Diğer yandan, $v_1 = 3k_1 - 2l_1$ olduğundan

$$v_1 = 3(k + v) - 2(l + 2v) = 3k + 3v - 2l - 4v = 3k - 2l - v$$

ve $3k - 2l = v$ olduğundan

$$v_1 = 3k - 2l - v = v - v = 0$$

olduğu sonucuna ulaşılır. Dolayısıyla $v < 0$ ise $v_1 = 0$ olur.

iii) $v = 0$ ise $v = 3k - 2l = 0$ olduğundan $3k = 2l$ dir, böylece belli bir m pozitif tam sayısı için $k = 2m$ ve $l = 3m$ olarak yazılabilir. Diğer yandan $P = (p^k s/e^2, p^l t/e^3)$ ifadesinde $k = 2m$ ve $l = 3m$ olarak yazılırsa

$$x = \frac{p^{2m}s}{e^2}, y = \frac{p^{3m}t}{e^3}$$

olur. Şimdi bu değerler $y^2 = x^3 + D$ eliptik denkleminde yazılırsa

$$p^{6m}(t^2 - s^3) = De^6$$

olduğu görülür. Varsayım gereği $6 \nmid \text{ord}_p D$ olduğundan $t^2 - s^3 \equiv 0 \pmod{p}$ olmalıdır. Bu durumda $v = 0$ olduğundan

$$S_1 = s_0(9p^{v_0}s_0{}^3 - 8t_0{}^2) = s(9p^v s^3 - 8t^2) = s(9s^3 - 8t^2)$$

ve $t^2 \equiv s^3$ olduğundan

$$S_1 = s^4 \not\equiv 0 \pmod{p}$$

dir. Benzer biçimde

$$T_1 = -27p^{2v_0}s_0{}^6 + 36p^{v_0}s_0{}^3t_0{}^2 - 8t_0{}^4 = s^6 \not\equiv 0 \pmod{p}$$

olduğu da görülebilir. Dolayısıyla $k_1 = 2m$ ve $l_1 = 3m$ ise $v_1 = 0$ dır.

2. Durum. $p = 2$ olsun. Bu durumda

$$x(2P) = \frac{2^k s(9 \cdot 2^{v-2}s^3 - 2t^2)}{(te)^2} = \frac{2^{k_1}s_1}{e_1^2} \tag{3.11}$$

ve

$$y(2P) = \frac{2^l(-27 \cdot 2^{2v-3}s^6 + 9 \cdot 2^{v-1}s^3t^2 - t^4)}{(te)^3} = \frac{2^{l_1}t_1}{e_1^3} \tag{3.12}$$

olarak yazılabilir.

i) $v - 2 > 0$ ise

$$x(2P) = \frac{2^k s(9 \cdot 2^{v-2}s^3 - 2t^2)}{(te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

ve üstelik $(t, 2) = 1$ olduğundan

$$s_1 = s(9 \cdot 2^{v-3}s^3 - t^2)$$

dir. O halde $k_1 = k + 1$ dir. Diğer yandan $(t, p) = 1$ olduğundan

$$t_1 = -27 \cdot 2^{2v-3}s^6 + 9 \cdot 2^{v-1}s^3t^2 - t^4$$

yani $l_1 = l$ dir. Böylece $v_1 \geq 2$ dir.

ii) $v = 2$ olsun. $(s, 2) = 1$ olduğundan (3.11) eşitliğinde $v = 2$ yazılırsa

$$s_1 = s(9s^3 - 2t^2)$$

dir. O halde $k_1 = k$ ve benzer biçimde $(t, 2) = 1$ olduğundan

$$t_1 = -54s^6 + 18s^3t^2 - t^4$$

olarak bulunur yani $l_1 = l$ dir. Böylece

$$v_1 = 3k_1 - 2l_1 = 3k - 2l = v = 2$$

olduğundan $v_1 = 2$ olduğu sonucuna ulaşılır.

iii) $v - 2 < 0$ ise

$$x(2P) = \frac{p^{k+v-2}s(9s^3 - 2^{3-v}t^2)}{(te)^2}$$

olarak yazılabilir. Böylece $k_1 = k + v - 2$ ve $l_1 = l + 2v - 3$ dir. O halde

$$v_1 = 3k_1 - 2l_1 = 3(k + v - 2) - 2(l + 2v - 3) = 0$$

olarak bulunur. Diğer bir ifade ile $v - 2 < 0$ ise $v_1 = 0$ dır.

3. Durum. $p = 3$ olsun. Bu durumda

$$x(2P) = \frac{p^k s(9p^v s^3 - 8t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

ve

$$y(2P) = \frac{p^l(-27p^{2v}s^6 + 36p^v s^3 t^2 - 8t^4)}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3}$$

olarak yazılabilir.

i) Şimdi $v \geq 0$ ise $(t, 3) = 1$ ve $(s, 3) = 1$ olduğundan

$$s_1 = s(9 \cdot 3^v s^3 - 8t^2)$$

dir. O halde $k_1 = k$ dır. Benzer biçimde $(t, 3) = 1$ olduğundan

$$t_1 = -27\cdot 3^{2v}s^6 + 36\cdot 3^v s^3 t^2 - 8t^4$$

elde edilir. Yani $l_1 = l$ dir. Dolayısıyla $v_1 = v \geq 0$ dır.

ii) $v = 0$ ise

$$x(2P) = \frac{3^k s(9s^3 - 8t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

ve

$$y(2P) = \frac{3^l(-27s^6 + 36s^3t^2 - 8t^4)}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3}$$

olarak yazılabilir. Böylece $(t, 3) = 1$ olduğundan (*i*) haline benzer biçimde $k_1 = k$ ve $l_1 = l$ ve dolayısıyla $v_1 = 0$ dır.

iii) $v < 0$ olsun. İlk olarak $v \leq -2$ olsun. Bu durumda

$$x(2P) = \frac{p^{k+v+2}s(s^3 - 8\cdot 3^{-v-2}t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

ve

$$y(2P) = \frac{p^{l+2v+3}(-s^6 + 4\cdot 3^{-v-1}s^3t^2 - 8t^4 3^{-2v-3})}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3}$$

olarak yazılabilir ve böylece $k_1 = k + v + 2$ ve $l_1 = l + 2v + 3$ olduğu elde edilir. Dolayısıyla

$$v_1 = 3k_1 - 2l_1 = 3(k + v + 2) - 2(l + 2v + 3) = 0,$$

yani $v_1 = 0$ dır. Şimdi de $v = -1$ olduğu durumu ele alalım. Bu durumda

$$x(2P) = \frac{3^k s(3s^3 - 8t^2)}{(2te)^2} = \frac{p^{k_1}s_1}{e_1^2}$$

olarak yazılabilir. Diğer yandan $s(3s^3 - 8t^2, 3) = 1$ olduğundan

$$s_1 = 3s^3 - 8t^2$$

dir, yani $k_1 = k$ dır. Benzer biçimde

$$y(2P) = \frac{3^l(-3s^6 + 12s^3t^2 - 8t^4)}{(2te)^3} = \frac{p^{l_1}t_1}{e_1^3}$$

olarak yazılabilir. Diğer yandan $(-3s^6 + 12s^3t^2 - 8t^4, 3) = 1$ olduğundan

$$t_1 = -3s^6 + 12s^3t^2 - 8t^4$$

dir, yani $l_1 = l$ dir.

Böylece her halde de $3p^{v_1}$ sayısının bir tam sayı olduğu sonucuna ulaşılır. Şimdi $t_2 = T_2$ veya $2^{-3}T_2$ olduğunu gösterelim. Lemma'nın (1) şıkkı gereği, t_1, 3 ile bölünmeyen ve s_1 ile aralarında asal olan bir tek tam sayıdır. Eğer $p \geq 3$ ve $2 \mid s_1$ veya $p = 2$ ve $v_1 \geq 2$ ise $8 \parallel T_2$ dir. Aksi halde T_2 tektir. O halde Lemma 3.3.9'a benzer bir biçimde hareket edilirse s_2 ve T_2 nin 2'den farklı bir asal çarpanının olmadığı görülebilir. O halde $t_2 = T_2$ veya $t_2 = 2^{-3}T_2$ dir. Diğer yandan n için tümevarım uygulanarak Lemmanın (2) şıkkındaki önermenin doğru olduğu da görülür.

Teorem 3.3.8'in İspatı (a). P, E eğrisi üzerinde bir büküm olmayan nokta olmak üzere $n \geq 1$ bir tamsayı olsun. $e_n > 0$, $(s_n, t_n) = (s_n, a_n) = (t_n, b_n) = 1$ ve

$$a_n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \qquad b_n = p_1^{\beta_1} \cdots p_n^{\beta_n}$$

olmak üzere P noktasının 2^n. katı en küçük terimlerle

$$2^nP = \left(\frac{a_n s_n}{e_n^2}, \frac{b_n t_n}{e_n^3}\right)$$

olarak yazılsın. Eğer $c_n = a_n^3 b_n^{-2}$ denirse $v_i = 3\alpha_i - 2\beta_i$ olmak üzere

$$c_n = p_1^{v_1} \cdots p_n^{v_n}$$

olarak yazılabilir. Üstelik Lemma 3.3.10 gereği, $3c_n$ bir tam sayıdır. Lemma 3.3.10'nun ispatında da belirtildiği gibi $p_i \geq 5$ ve $6 \mid \mathrm{ord}_p D$ özelliğinde bir asal olmaması halinde $v_i \geq 0$ dır. Diğer yandan ikiye katlama formülleri yardımıyla

$$x(2^{n+1}P) = \frac{a_n s_n (9c_n s_n^3 - 8t_n^2)}{(2c_n t_n)^2}$$

ve

$$y(2^{n+1}P) = \frac{b_n (-27c_n^2 s_n^6 + 36c_n s_n^3 c_n^2 t_n^2 - 8t_n^4)}{(2c_n t_n)^3}$$

eşitlikleri elde edilir. Lemma 3.3.10 gereği, t_n tek, 3 ile bölünemez ve her $n \geq 1$ için s_n ile aralarında asaldır. O halde $x(2^{n+2}P)$ nin bir ilkel asal bölene sahip olduğunu görebilmek için $t_{n+1} \neq \pm 1$ olduğunu göstermeliyiz. Bunun için

$$T_{n+1} = -27c_n^2 s_n^6 + 36c_n s_n^3 t_n^2 - 8t_n^4 \tag{3.13}$$

denirse Lemma 3.3.10 gereği, $t_{n+1} = T_{n+1}$ veya $2^{-3}T_{n+1}$ dir. Şimdi $T_{n+1} \neq \pm 1, \pm 2^3$ olduğunu göstereceğiz. (3.13) eşitliği düzenlenirse

$$27c_n^2 s_n^6 - 36c_n s_n^3 t_n^2 + 8t_n^4 + T_{n+1} = 0$$

eşitliği elde edilir. Böylece bu son eşitlikte $3c_n s_n^3$ değerine x denirse

$$3x^2 - 12t_n^2 x + 8t_n^4 + T_{n+1} = 0$$

denklemi elde edilir. Bu denklemin diskriminantı

$$\Delta = 48t_n^4 - 12T_{n+1}$$

olduğundan bu denklemin kökleri

$$3c_n s_n^3 = 2t_n^2 \pm \frac{\sqrt{12t_n^4 - 3T_{n+1}}}{3} \tag{3.14}$$

olarak bulunur. Diğer yandan $3c_n$ bir tam sayı olduğundan

$$12t_n^4 - 3T_{n+1} = u_n^2$$

dir. O halde yukarıdaki eşitliğin sol tarafının bir tam kare olması için gerek ve yeter koşul belli bir w_n pozitif tamsayısı için

$$4t_n^4 - T_{n+1} = 3w_n^2 \tag{3.15}$$

olmasıdır. Şimdi T_{n+1} için 4 hal söz konusu olduğundan bu 4 hal için tüm durumları inceleyelim.

1. Hal. $T_{n+1} = -1$ olsun. Bu durumda (3.15) eşitliği

$$4t_n^4 + 1 = 3w_n^2$$

eşitliğine dönüşür. Bu eşitlik 3 modülüne göre indirgenirse $4t_n^4 + 1 \equiv 0 \pmod 3$ denkliği elde edilir. Ancak bu denkliğin bir çözümü yoktur. O halde $T_{n+1} \neq -1$ dir.

2. Hal. $T_{n+1} = 1$ olsun. Bu durumda (3.15) eşitliği

$$4t_n^4 - 1 = 3w_n^2$$

eşitliğine dönüşür. Bu eşitliğin her iki tarafı $432t_n^2$ ile çarpılırsa

$$1728\, t_n^4 - 432t_n^2 = 36t_n^2w_n^2$$

eşitliği elde edilir. Bu eşitlikte $x = 12t_n^2$ ve $y = 36t_nw_n$ denirse

$$y^2 = x^3 - 36x$$

eliptik denklemi elde edilir. Magma-Cebir programında *Ellog*[1] komutu kullanılarak bu eğri üzerindeki tüm tam sayı koordinatlı noktaların

$$(x, y) = (\pm 6, 0), (-3, \pm 9), (-2, \pm 8), (0, 0), (12, \pm 36), (18, \pm 72), (294, \pm 5040)$$

biçiminde olduğu görülebilir. Dolayısıyla

$$(12t_n^2, 36t_nw_n) = (12, \pm 36)$$

---

[1] *Elliptic Logarithm Method* uygulanmıştır. Bu yöntem (Stroeker ve Tzanakis, 1994) ve (Gebel ve ark., 1994) tarafından bağımsız olarak geliştirilmiş ve MAGMA (Bosma ve ark., 1997) programına (http://magma.maths.usyd.edu.au/calc/.) eklenmiştir.

dır ve böylece $t_n = \pm 1$ dir. (3.14) eşitliğinde $t_n = \pm 1$ ve $T_{n+1} = 1$ değerleri yerine yazılırsa $c_n s_n^3 = 1$ ve böylece $c_n = 1$ ve $s_n = 1$ dir. O halde

$$2^n P = (\frac{a_n}{e_n^2}, \pm \frac{b_n}{e_n^3})$$

ve

$$2^{n+1} P = (\frac{a_n}{4e_n^2}, \pm \frac{b_n}{8e_n^3})$$

dir. Diğer yandan $2^n P$ ve $2^{n+1} P$ noktaları $y^2 = x^3 + D$ eğrisi üzerinde olduğundan

$$b_n^2 = a_n^3 + De_n^6$$

ve

$$b_n^2 = a_n^3 + 64De_n^6$$

olur ki bu imkansızdır. Dolayısıyla $T_{n+1} \neq 1$ dir.

3. Hal. $T_{n+1} = 2^3$ olsun. Bu durumda (3.15) eşitliği

$$4t_n^4 - 2^3 = 3w_n^2$$

eşitliğine dönüşür. Bu eşitlik 3 modülüne göre indirgenirse $4t_n^4 - 2^3 \equiv 0 \pmod 3$ olur ki bu denkliğin de bir çözümü yoktur. Dolayısıyla $T_{n+1} \neq 2^3$ dir.

4. Hal. $T_{n+1} = -2^3$ ise (3.15) eşitliği

$$4t_n^4 + 2^3 = 3w_n^2$$

eşitliğine dönüşür. Bu eşitliğin her iki tarafı $432t_n^2$ ile çarpılırsa

$$1728t_n^6 + 3456t_n^6 = 36t_n^2 w_n^2$$

eşitliği elde edilir. Bu eşitlikte $x = 12t_n^2$ ve $y = 36t_n w_n$ denirse

$$y^2 = x^3 + 288x$$

eliptik denklemi elde edilir. Magma-Cebir programında *Ellog* komutu kullanılarak bu eğri üzerindeki tüm tam sayı koordinatlı noktaların

$$(x, y) = (0, 0), (1, \pm 17), (12, \pm 72), (24, \pm 144), (288, \pm 4896)$$

olduğu görülür. Dolayısıyla $(12t_n^2, 36t_nw_n) = (0,0), (12, \pm 72)$ dir. Böylece $t_n = 0$ veya ± 1 dir. O halde (3.14) eşitliğinden $t_n = 0$ ise $3c_ns_n^3 = \sqrt{24}$ olur ki bu da imkansızdır. Eğer $t_n = \pm 1$ ise $3c_ns_n^3 = 0$ veya 12 dir. O halde $c_ns_n^3 = 4$ ve böylece $s_n = \pm 1$ ve $c_n = \pm 4$ tür. Dolayısıyla 2. hale benzer biçimde

$$2^nP = (\pm\frac{a_n}{e_n^2}, \pm\frac{b_n}{e_n^3})$$

ve

$$2^{n+1}P = (\pm\frac{a_n}{4e_n^2}, \pm\frac{b_n}{8e_n^3})$$

biçimindedir ve üstelik 2^nP, $2^{n+1}P$ noktaları $y^2 = x^3 + D$ eğrisi üzerinde olduğundan

$$b_n^2 = \pm a_n^3 + De_n^6$$

ve

$$b_n^2 = \pm a_n^3 + 64De_n^6$$

olur ki bu imkansızdır. Dolayısıyla $T_{n+1} \neq -2^3$ dir. Böylece ispat tamamlanmış olur.

4. BULGULAR ve TARTIŞMA

Bu çalışmada rekurent dizilerdeki ilkel asal bölenler ele alınmıştır. Bunun için öncelikle lineer dizilerdeki ilkel asal bölenler üzerinde durulmuştur. İlk olarak Bang (1886) tarafından ele alınmış, 1892'de Zsigmondy tarafından genelleştirilmiş ve 1904'de Birkoff ve Vandiver tarafından yeniden keşfedilmiş olan sayılar teorisinin klasik teoremlerinden Zsigmondy teoremi verilmiş ve bu teoremin ispatı için gerekli hazırlıklar yapılmıştır. Klasik Zsigmondy teoreminin ispatı, döngüsel polinomlar ve özellikle bu polinomların özellikleri ile ilgilidir. Bu nedenle özellikle homojenize döngüsel polinomlar çalışmada önemli bir yer tutmaktadır. Daha sonra klasik Zsigmondy teoreminin bazı uygulamaları üzerinde durularak bu teoremin bazı matematik olimpiyat problemlerinin çözümünde nasıl kullanıldığına yer verilmiştir.

Çalışmada ikinci olarak ilk olarak 1948 yılında Ward (1948) tarafından çalışılmış eliptik bölünebilir dizilerdeki ilkel asal bölen kavramı ele alınmıştır. Eliptik bölünebilir diziler Ward'ın tanımından farklı olarak da ifade edilebilirler. Buna göre E bir K cismi üzerinde tanımlanmış bir eliptik eğri P, E eliptik eğrisi üzerinde bir büküm olmayan nokta, $x(nP)$, nP noktasının x-koordinatı olmak üzere $x(nP)$ noktasının paydası $p_n(P)$ ile gösterilirse her $n \in \mathbb{N}$ için $(p_n(P))$ dizisi bir eliptik bölünebilir dizidir. $(p_n(P))$ dizisindeki ilkel asal bölenleri bulma problemi ilk olarak 1988 yılında Silverman (1988) tarafından ele alınmıştır. Silverman (1988), P noktası E eğrisi üzerinde bir büküm olmayan nokta ise $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimlerinin bir ilkel asal bölene sahip olduğunu göstermiştir. Daha sonra bu sonuç Cheon ve Hahn (1999) tarafından herhangi bir sayı cismine genişletilmiştir. Diğer bir ifade iler E, bir K sayı cismi üzerinde tanımlı bir eliptik eğri ve $P \in E(K)$ bir büküm olmayan nokta olmak üzere $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimleri bir ilkel asal bölene sahiptir (Cheon ve Hahn, 1999).

5. SONUÇ

Bu çalışmada ilk olarak klasik Zsigmondy teoremi ele alınmıştır. Zsigmody (1892), a ve b aralarında asal pozitif tamsayılar ve $a > b$ olmak üzere $(a^n - b^n)_{n \geq 1}$ dizisinin, $n = 6$, $a = 2$ ve $b = 1$ olması veya $n = 2$ ve $a + b$ sayısı 2 nin bir kuvveti olmaması halinde bir ilkel asal bölene sahip olduğunu göstermiştir. Diğer bir ifade ile $\sup(Z(a^n - b^n)) \leq 6$ dır. Daha sonra Feit (1988), bu dizilerde büyük ilkel asal bölen kavramını tanımlayarak $(a^n - b^n)_{n \geq 1}$ dizisindeki büyük ilkel asal bölenleri belirlemiştir. Carcmichael 1913'te yayınlanan makalesinde $n > 12$ için $(D_n)_{n \geq 1}$ Lucas dizisinin bir ilkel böleninin olduğunu ispat etmiştir. Gerçektende Fibonacci dizisinin 12. teriminin bir asal böleni olmadığından bu en iyi ihtimal olarak düşünülebilir. Bu sonuç Ward (1955) ve daha sonra Stewart (1977) tarafından Lehmer dizilerine genelleştirilmiştir. Daha sonra 2001 yılında Bilu ve ark., bu sonucu geliştirerek daha keskin bir sınır vermişlerdir. Buna göre, her $n > 30$ için n. Lucas ve Lehmer sayıları bir ilkel asal bölene sahiptir. Böylece Bilu ve ark. (2001)'da bir ilkel asal bölene sahip olmayan tüm Lucas ve Lehmer dizilerini listelemişlerdir.

Çalışmada daha sonra ilk çalışılan lineer olmayan dizilerden eliptik bölünebilir dizilerdeki ilkel asal bölen kavramı üzerinde durulmuştur. Buna göre E bir $\mathbb{Q}$ cismi üzerinde tanımlanmış bir eliptik eğri P, E eliptik eğrisi üzerinde bir büküm olmayan nokta, $x(nP)$, nP noktasının x-koordinatı olmak üzere $x(nP)$ noktasının paydası $p_n(P)$ olsun. Silverman (1988), P noktası E eğrisi üzerinde bir büküm olmayan nokta ise $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimlerinin bir ilkel asal bölene sahip olduğunu göstermiştir. Bu teoreme göre, $(p_n(P))$ dizisinin sonlu sayıdaki terimleri hariç diğer tüm terimleri bir ilkel asal bölene sahip olduğu belirtilmiş ancak açık bir sınır ortaya konulmamıştır. Bununla birlikte bazı özel dizi aileleri için (Everest ve ark., 2006) de olduğu gibi daha açık formüller verilmiştir. Literatürde belli eliptik eğriler ile elde edilen $(p_n(P))$ dizileri için Zsigmondy sınırı verilmiştir.

KAYNAKLAR

Apostol, T. M. (1998). *Introduction to analytic number theory*. Springer, New York, 338 pp.

Bang, A. S. (1886). Taltheoretiske undersogelser. *Tidsskrift for Mathematik*, 4: 70-80.

Bilu, Y., Hanrot, G., Voutier, P. M. (2001). Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte. *J. Reine Agnew. Math*., 539: 75-122.

Birkhoff, G. D., Vandiver, H. S. (1904). On the integral divisors of $a^n - b^n$. *Annals of Mathematics*, 5 (4): 173-180.

Bosma, W., Cannon, J., Playoust, C. (1997). The Magma Algebra System I. the user language, *J. Symbolic Computation*, 24: 235-265.

Carcmichael, P. D. (1913). On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math*., 15 (2): 30-70.

Cheon, J., Hahn, S. (1999). The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve. *Acta Arith*. 88 (3): 219-222.

Cox, D. A. (2012). *Galois theory* (2nd ed.). John Wiley & Sons, New Jersey, USA, 559 pp.

Everest, G., Mclaren, G., Ward, T. (2006). Primitive divisorsof elliptic divisibility sequences. *Journal of Number Theory*, 118: 71-89.

Feit, W. (1988). On large Zsigmondy primes. *Proceedings of the American Mathematical Society*, 102 (1): 29-36.

Ge, Y. (2023, 3 Mart) Elementary Properties of Cyclotomic Polynomials, Erişim adresi: https://cdn.bcpf.org/resources/math/number_theory/exponents/cyclotomic_polynomials/Yimin_Ge-Elementary_Properties_of_Cyclotomic_Polynomials.pdf.

Gebel, J., Pethö, A., Zimmer, H. G. (1994). Computing integral points on elliptic curves. *Acta Arith.*, 68: 171-192.

Gezer, B., Bizim O. (2017). *Soyut cebir*. Dora Yayıncılık, Bursa, Türkiye, 662 pp.

Loo, A. (2012). Zsigmondy's Theorem. *Mathematical Excalibur*, 16(4): 1-4.

Parvardi, A. H. (2022, 12 Mart) Lifting the exponent lemma (LTE), Erişim adresi: http://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/lifting-the-exponent.pdf.

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.*, 44 (170): 483-494.

Silverman, J. H. (2005). *p*-adic properties of division polynomials and elliptic divisibility sequences, *Math. Ann*., 332: 443-471, addendum 473-474.

Silverman, J. H. (2009). *The arithmetic of elliptic curves*. Springer, New York, USA, 513 pp.

Silverman, J. H. (1988). Wieferich's criterion and the abc-conjecture. *Journal of Number Theory*, 30 (2): 226-237.

Sheng, Y. (2023, 25 Nisan). An elementary proof of Zsigmondy's theorem. Erişim adresi:https://angyansheng.github.io/blog/an-elementary-proof-of-zsigmondys-theorem.

Stewart, C. (1977). On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. *Proc. London Math*. Soc., 35 (3): 425-447.

Stroeker, R. J., Tzanakis, N. (1994). Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith*. 67: 177-196.

Ward, M. (1948). Memoir on elliptic divisibility sequences. *Amer. J. Math*., 70: 31-74.

Ward, M. (1955). The intrinsic divisors of Lehmer number. *Ann. of Math*., 62 (2): 230-236.

Yabuta, M. (2009). Primitive Divisors of Certain Elliptic Divisibility Sequences. *Experimental Mathematics*, 18(3): 303-310.

Zsigmondy, K. (1892). Zur theorie der potenzreste. *Journal Monatshefte für Mathematik*, 3 (1): 265-284.

ÖZGEÇMİŞ

Adı Soyadı	: İpek ÇOLAK
Doğum Yeri ve Tarihi	: BURSA – 03.03.1999
Yabancı Dili	: İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise	: Özel Bursa Sınav Koleji Anadolu Lisesi - 2017
Lisans	: Bursa Uludağ Üniversitesi - 2021
Yüksek Lisans	: Bursa Uludağ Üniversitesi Fen Bilimleri Enstitüsü-2023

Çalıştığı Kurum/Kurumlar ve Yıl	:
İletişim (e-posta)	: ipekk3353@gmail.com

Yayınlar : Çolak, İ. 2022. Eliptik Bölünebilir Diziler, 4th International Eurasian Conference on Science, Engineering and Technology (EurasianSciEnTech 2022), 14-16 Aralık 2022, Ankara, Türkiye.