T. C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

REKURRENT DİZİLER VE UYGULAMALARI

Buse UZATICI

Prof. Dr. Osman BİZİM

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2015

ÖZET

Doktora Tezi

REKURRENT DİZİLER ve UYGULAMALARI

Buse UZATICI

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Osman BİZİM

Bu çalışmada özel bir eğri ailesi olan Tate normal formdaki eliptik eğriler ile eşleşen rekurrent Somos 4 dizileri ele alınmış ve bu dizilerin $h_{-1} = \pm 1$ olmak üzere $n \geq 0$ için tüm h_n terimlerinin birer tamsayı oldukları gösterilmiştir. Bir uygulama olarak, bu dizilerdeki kare ve küp terimlerin sonsuz çoklukta bulunduğu belirlenmiştir.

Çalışmanın birinci bölümünde, ikinci ve üçüncü bölümlere temel oluşturacak kavramlar verilmiştir. Genel olarak lineer ve bilineer rekurrent diziler incelenerek bu dizilerin temel özellikleri üzerinde durulmuştur. Bu bölümün son kısmında eliptik eğriler ele alınmış ve temel özellikleri belirtilmiştir.

Çalışmanın ikinci bölümünde, rekurrent eliptik bölünebilir diziler ile ilgili temel kavramlar ve teoremler ifade edilmiştir.

Üçüncü bölüm ise çalışmanın ana kısmını oluşturmaktadır. Bu bölümde, öncelikle, genel olarak rekurrent Somos dizileri tanımlanmış ve bu dizilerin genel özellikleri üzerinde durulmuştur. Daha sonra Tate normal formdaki eliptik eğriler ile eşleşen Somos 4 dizilerinin tüm terimlerinin birer tamsayı oldukları gösterilmiştir. Uygulama olarak, bu dizilerdeki kare ve küp terimlerin neler oldukları belirlenmiştir.

Anahtar Kelimeler: Somos dizileri, Somos 4 dizileri, Eliptik bölünebilir diziler, Tate normal form, Eliptik eğriler.

2015, vii + 97 sayfa.

ABSTRACT

PhD Thesis

RECURRENCE SEQUENCES AND APPLICATIONS

Buse UZATICI

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

Supervisor: Prof. Dr. Osman BİZİM

In this work, a family of Somos 4 sequences is given and it is proved that all Somos 4 sequences associated to Tate normal forms with $h_{-1} = \pm 1$ consist entirely of integers for $n \geq 0$. As an application, it is shown that there are infinitely many squares and infinitely many cubes in Somos 4 sequences associated to Tate normal forms.

First chapter is the basis for the second chapter and the third chapter. Linear and bilinear recurrence sequences are discussed in this chapter. Also elliptic curves are considered in this chapter.

In the second chapter, elliptic divisibility sequences are examined.

Third chapter is the main part of the work. First, Somos sequences are defined. Then by obtaining the general terms of Somos 4 sequences associated to Tate normal forms, it is proved that these sequences with $h_{-1} = \pm 1$ consist entirely of integers for $n \geq 0$. Finally, as an application, square terms and cube terms of these sequences are determined by using general terms.

Key words: Somos sequences, Somos 4 sequences, Elliptic divisibility sequences, Tate normal form, Elliptic curves.

2015, vii + 97 pages.

TEŞEKKÜR

Yüksek lisans ve doktora çalışmam esnasında her soruma ve sorunuma hemen cevap ve çözüm üreten çok kıymetli danışman hocam Prof. Dr. Osman BİZİM' e en içten teşekkürlerimi sunarım. Kendisinin bu çalışma sürecinde bana kattıkları hayatım boyunca yoluma ışık tutacaktır. Sayın hocamın öğrencisi olmak benim için bir onurdur. 6 yıl süren bu lisansüstü çalışma dönemimde her türlü bilgisini, deneyimini ve yardımını benden esirgemeyen değerli hocam Doç. Dr. Betül GEZER' e sonsuz teşekkür ederim.

Buse UZATICI
11/11/2015

İÇİNDEKİLER

Sayfa

SİMGELER DİZİNİ

Simgeler	Açıklama
$\left(\frac{a}{p}\right)$	a tamsayısının modülo p deki Legendre sembolü ($p > 2$)
$\mathbb{F}$	Cisim
$\mathbb{F}^*$	$\mathbb{F}$ cisminin sıfırdan farklı elemanlarının oluşturduğu çarpımsal grup
$\overline{\mathbb{F}}$	$\mathbb{F}$ cisminin cebirsel kapanışı
R	Halka
$\mathbb{Z}_n$	Modülo n de tamsayıların halkası
$\mathbb{F}_p$	p elemanlı sonlu cisim
$\mathbb{F}_p^*$	p elemanlı sonlu cismin çarpımsal grubu
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{N}$	Doğal sayılar kümesi
$j(E)$	E eliptik eğrisinin j-değişmezi
$\Delta(E)$	E eliptik eğrisinin diskriminantı
$E[n]$	E eliptik eğrisi üzerindeki n-büküm (n-torsiyon) noktalarının kümesi
$E(\mathbb{F})$	$\mathbb{F}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktaların kümesi
$E_{\text{tors}}(\mathbb{Q})$	$\mathbb{Q}$ cismi üzerinde tanımlı E eliptik eğrisinin torsiyon alt grubu
$(a(x))$	Rekurrent dizinin genel terimi
$L(f)$	Lineer rekurrent dizilerin kümesi
δ_{ij}	Kronecker delta sembolü
$\lfloor x \rfloor$	x sayısının tam değeri
σ	Weierstrass σ - fonksiyonu
per(f)	f polinomunun periyodu
$\mathbb{P}$	Asal sayıların kümesi
$P_a(N)$	Dizideki asal terimlerin sayısı

ψ_n	Eliptik eğrinin bölüm polinomları
$\Delta(h_2, h_3, h_4)$	Eliptik bölünebilir dizinin diskriminantı
N_r	p^r sayısının dizideki rankı
π	Dizinin periyodu
□	Dizinin kare terimleri
C	Dizinin küp terimleri
$\{U_n(P, Q)\}$	Lucas dizisi

ŞEKİLLER DİZİNİ

Sayfa

REKURRENT DİZİLER VE UYGULAMALARI

1. BÖLÜM

ÖN BİLGİLER

Bu bölümde çalışmada kullanılacak olan bazı temel kavramlar tanımlanacak ve bazı temel teoremler verilecektir. Kısım 1.1 de genel olarak rekurrent diziler ve bu dizilerin temel özellikleri üzerinde durulacaktır. Kısım 1.2 de bilineer rekurrent diziler ile ilgili bazı kavram ve özellikler verilecektir. Kısım 1.3 de dizilerde periyodiklik kavramı ele alınacaktır. Kısım 1.4 de lineer rekurrent dizilerde asal terimler ile ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir. Kısım 1.5 de ise bilineer dizilerle yakından ilgileri olan eliptik eğriler ele alınacak ve bu eğrilerin genel özellikleri üzerinde durulacaktır.

1.1 Rekurrent Diziler

İlk olarak, birimi 1 olan değişmeli bir R halkası üzerinde tanımlanmış bir indirgeme bağıntısına sahip olan lineer diziler ele alınacak ve daha sonra kullanılacak kavramlar hakkında genel bilgiler verilecektir.

$x \in \mathbb{N}$ olmak üzere

$$a(x+n) = s_1 a(x+n-1) + \ldots + s_{n-1} a(x+1) + s_n a(x) \qquad (1.1)$$

homojen bağıntısını gerçekleyen $a(x) \in R$ terimlerinin oluşturduğu $a = (a(x))$ dizisi dikkate alınacaktır. Bu eşitlikteki s_j sabit katsayıları, *katsayı halkası* olarak adlandırılan R halkasının sıfır böleni olmayan elemanlarıdır.

Yukarıda verilen (1.1) bağıntısı ile ilişkili olan

$$f(X) = X^n - s_1 X^{n-1} - \ldots - s_{n-1} X - s_n$$

polinomu, $a = (a(x))$ dizisinin *karakteristik polinomu* olarak adlandırılır ve bu durumda (1.1) *indirgeme bağıntısının mertebesi n* dir denir.

R halkası sıfır bölensiz ise herhangi lineer rekurrent a dizisi minimum uzunluktaki bir indirgeme bağıntısı gerçekler, bu minimum uzunluktaki indirgeme bağıntısının karakteristik polinomu a dizisinin minimum polinomu olarak adlandırılır. Bu durumda minimum polinomun derecesi lineer rekurrent a dizisinin mertebesi olur ve dizinin minimum polinomu karakteristik polinomu böler.

Mertebesi 2 ve 3 olan lineer rekurrent diziler sırasıyla *ikili* ve *üçlü rekurrent dizi* olarak adlandırılır. Özel olarak $\mathbb{Z}$, $\mathbb{Q}$, $\overline{\mathbb{Q}}$, $\mathbb{R}$, $\mathbb{C}$ ve $\mathbb{Q}_p$ halkaları üzerinde tanımlı lineer diziler sırasıyla *tamsayı*, *rasyonel*, *cebirsel*, *reel*, *karmaşık* ve *p-adic* lineer rekurrent diziler olarak adlandırılır.

Homojen olmayan lineer bağıntılar, $x \in \mathbb{N}$ olmak üzere

$$a(x+n) = s_1 a(x+n-1) + \ldots + s_{n-1} a(x+1) + s_n a(x) + s_{n+1}$$

formundaki bağıntılardır. Bu formdaki bir a dizisi de mertebesi $n + 1$ olan homojen

$$a(x+n+1) = (s_1+1)a(x+n) + \sum_{i=1}^{n-1} (s_{i+1} - f_i) a(x+n-i) - s_n a(x)$$

bağıntısını gerçekler. Bu diziye karşılık gelen karakteristik polinom ise

$$F(X) = (X^n - s_1 X^{n-1} - \ldots - s_{n-1} X - s_n)(X-1)$$

şeklindedir.

(1.1) bağıntısını gerçekleyen n mertebeli lineer rekurrent dizinin $a(1)$, …, $a(n)$ terimleri dizinin *başlangıç terimleri* olarak adlandırılır ve bu başlangıç terimleri (1.1) bağıntısı yardımıyla dizinin diğer terimlerini tanımlar. Eğer s_n elemanının R halkasında tersi var ise dizi ters yönde,

$$a(0), a(-1), a(-2), \ldots$$

şeklinde devam eder.

Ele alınan diziler halka yerine bir cisim üzerinde de tanımlanabilir. f, bir cisim üzerinde tanımlı bir polinom olmak üzere (1.1) bağıntısını gerçekleyen lineer rekurrent dizilerin

kümesi $L(f)$, karakteristik polinomu f olan lineer rekurrent dizilerin kümesi ise $L^*(f)$ ile gösterilir. Eğer g polinomu f polinomunu bölüyor ise $L(g) \subset L(f)$ dir. f polinomu indirgenemez ise $L^*(f)$ kümesi, $L(f)$ kümesindeki sıfır dizisi dışındaki tüm dizileri içerir. Tanımlanan bu kümelerin özellikleri aşağıdaki teorem ile özetlenebilir:

1.1.1 Teorem. f ve g aynı cisim üzerinde tanımlı iki polinom olsun.

i. $\{c(x) : c(x) = a(x) + b(x),\ a \in L(f),\ b \in L(g)\} = L(\text{okek}(f, g))$,

ii. $L(f) \cap L(g) = L(\text{obeb}(f, g))$,

iii. $L(g) \subset L(f) \Leftrightarrow f \mid g$.

$a \in L(f)$, $b \in L(g)$ olmak üzere, eğer $c(x) = a(x)b(x)$ ise c yine bir lineer rekurrent dizi belirtir, ancak bu dizinin karakteristik polinomu doğrudan f ve g polinomları ile elde edilemez (Everest ve ark. 2003).

δ_{ij}, Kronecker delta fonksiyonu olmak üzere, başlangıç değerleri

$$a_i(j) = \delta_{ij} \qquad i, j = 1, \ldots, n$$

olan a_i dizilerine *temel dizi* denir, bu dizilerin sayısının n tane olduğu açıktır. Verilen (1.1) bağıntısını gerçekleyen herhangi bir dizi, uygun temel dizilerin

$$a(x) = \sum_{i=1}^{n} a(i)a_i(x), \quad x \in \mathbb{N}$$

biçiminde lineer terkibi olarak bir tek şekilde ifade edilebilir. Bunu görmek için eşitliğin sağ tarafının (1.1) bağıntısını gerçeklediğini göstermek yeterlidir. Dolayısıyla $L(f)$ dizi kümesi n boyutlu bir lineer uzaydır.

Son eşitlikte, $x + h$ kayması yapılarak

$$a(x + h) = \sum_{i=1}^{n} a(h + i)a_i(x), \quad x \in \mathbb{N}, h \in \mathbb{Z}^+$$

eşitliği elde edilebilir.

$L(f)$ dizi kümesi bir lineer uzay olduğu gibi aynı zamanda, dizilerin denklik sınıfları

kullanılarak bir grup olarak da düşünülebilir. Özel olarak tekrar etmeyen, yani katlı olmayan köklerin dikkate alınması halinde, f polinomu karakteristiği 0 olan $\mathbb{F}$ cismi üzerinde tanımlı monik kare serbest bir polinom olacaktır. Doğal olarak dizinin her iki yanını dikkate almak daha uygundur. $a, b \in L(f)$ olmak üzere, belli bir $\lambda \in \mathbb{F}^*$, $l \in \mathbb{Z}$ ve her $x \in \mathbb{Z}$ için

$$\lambda a(x+l) = b(x)$$

ise a ve b dizilerine *denk diziler* denir.

Tanım dikkate alındığında, denk dizilerin birbirlerinden sadece kayma ve terimlerinin sıfırdan farklı sabit katı kadar farklı oldukları görülür. Bu şekilde tanımlanan bağıntının bir denklik bağıntısı olduğu açıktır. Bu denklik bağıntısının $L(f)$ üzerinde belirlemiş olduğu denklik sınıfları $G(f)$ ile gösterilir. $G(f)$ üzerindeki grup yapısını belirlemek için, determinantı Δ ile gösterilen, $n \times n$ tipindeki $W = (\alpha_j^{i-1})_{i,j=1}^{n}$ Vandermonde matrisi kullanılacaktır. Vandermonde matrisi, $\alpha_j \in R$ olmak üzere

$$W = \begin{bmatrix} 1 & \alpha_1 & {\alpha_1}^2 & \dots & {\alpha_1}^{n-1} \\ 1 & \alpha_2 & {\alpha_2}^2 & \dots & {\alpha_2}^{n-1} \\ 1 & \alpha_3 & {\alpha_3}^2 & \dots & {\alpha_3}^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & {\alpha_n}^2 & \dots & {\alpha_n}^{n-1} \end{bmatrix}$$

biçimindedir. W matrisinin j. sütununu $(0, \dots, 0, 1)^t$ ile değiştirerek elde edilen matrisin determinantı ise Δ_j ile gösterilsin. Bu durumda her $a \in L(f)$ dizisinin

$$a(x) = \frac{1}{\Delta} \sum_{i=1}^{n} \Delta_i a_i \alpha_i^x$$

şeklinde tek türlü temsili vardır.

a ve b dizileri $a \leftrightarrow [a_1, \dots, a_n]$ ve $b \leftrightarrow [b_1, \dots, b_n]$ biçiminde yazılarak a ve b dizilerinin çarpımı olan c dizisi $c \leftrightarrow [a_1 b_1, \dots, a_n b_n]$ olarak tanımlanabilir. Bu durumda bu iki denklik sınıfının çarpımı, temsillerinin çarpımı olarak tanımlanırsa bu işlem ile $G(f)$ değişmeli bir grup olur.

1.2 Bilineer Rekurrent Diziler

$\lfloor x \rfloor$, x sayısının tam değeri olmak üzere, eğer belli k ve $a_1, a_2, ..., a_{\lfloor \frac{k}{2} \rfloor}$ sabitleri için

$$u(x)u(x-k) = \sum_{i+j=k;1\le i\le j} a_i u(x-i)u(x-j)$$

sonlu bağıntısı gerçekleniyor ise u dizisine, *bilineer rekurrent dizi* denir.

$k = 4$ ve $k = 5$ olması halinde u dizisi *ikili*; $k = 6$ ve $k = 7$ olması halinde ise *üçlü* olarak adlandırılır. Dikkat edilirse mertebesi k olan her lineer rekurrent dizi, mertebesi k olan bir bilineer rekurrent dizi belirtir. Örneğin,

0, 1, 1, –1, 1, 2, –1, –3, –5, 7, –4, –23, 29, 59, 129, –314, –65, 1529, –3689, –8209, …

olarak verilen lineer rekurrent dizi aynı zamanda,

$$u(x)u(x-6) = -u(x-1)u(x-5) + 2u(x-2)u(x-4) + 2u(x-3)^2$$

bağıntısı ile ifade edilebileceğinden, üçlü bilineer rekurrent dizi olarak da düşünülebilir. Daha genel olarak, tanımı daha sonra verilecek olan, iki eliptik bölünebilir dizinin çarpımı dörtlü bilineer dizi belirtir.

Diğer yandan N. Stephen tarafından verilen bir sonuç bilineer rekurrent diziler ile eliptik eğriler üzerindeki noktalar yardımıyla elde edilen diziler arasındaki ilişkiyi ortaya koyar; $k = 4$ halinde tanımlanan her bilineer rekurrent dizi ya bir eliptik bölünebilir dizi belirtir ya da uygun bir eliptik eğri üzerinde alınan $P = (0, 0)$ ve Q noktaları için $(x_n, y_n) = Q + [n]P$ olmak üzere

$$u(n) = (-1)^{n(n+1)/2} x_{n-1} {x_{n-2}}^2 {x_{n-3}}^3 \ldots {x_1}^{n-1} {x_0}^n$$

dizisini belirtir. Burada $Q + [n]P$ ile, eğri üzerindeki P noktasının n katı ile Q noktasının toplamları olan nokta belirtilmektedir (ayrıntılar 1.5 kısmında ele alınacaktır).

Morgan Ward

$$a(x+y)a(x-y) = a(y+1)a(y-1)a(x)^2 - a(x+1)a(x-1)a(y)^2$$

bağıntısını gerçekleyen -iki yönlü- dizileri dikkate almıştır. Çalışmalar sonucunda bu dizilerin eliptik fonksiyonlar ile ifade edilebileceği ve bu dizilerin eliptik eğriler ile aralarında ilişkiler olduğu sonucuna varmıştır. Bundan dolayı bu dizilere *eliptik diziler* adını vermiştir.

$\left(\frac{x}{n}\right)$, modülo n de x tamsayısının Legendre sembolü olmak üzere $a(x) = x$, $b(x) = \left(\frac{x}{3}\right)$ ve $\alpha_1 \neq \alpha_2$ için

$$c(x) = (\alpha_1\alpha_2)^{-(x-1)/2}\,\frac{\alpha_1{}^x - \alpha_2{}^x}{\alpha_1 - \alpha_2}$$

olarak tanımlanan diziler yukarıda verilen bağıntıyı gerçekler.

u bir tamsayı dizisi olmak üzere $m \mid n$ olması halinde $u(m) \mid u(n)$ ve her $m \geq n \geq 1$ için u dizisi

$$u(m+n)u(m-n) = u(m+1)u(m-1)u(n)^2 - u(n+1)u(n-1)u(m)^2 \qquad (1.2)$$

rekurrent bağıntısını gerçekliyor ise u dizisine *eliptik bölünebilir dizi* denir.

$n = 2$ olması halinde u eliptik bölünebilir dizisi bir ikili bilineer rekurrent dizi olur.

Bazı diziler yukarıda verilen (1.2) bağıntısını aşikar olarak gerçekler. Örneğin, her $n \geq 0$ tamsayısı için $u(n) = n$ tamsayı dizisi ve

$$0, 1, -1, 0, 1, -1, \ldots$$

dizisi (1.2) bağıntısını gerçekler. Diğer yandan rekurrent bağıntısı

$$u(n+2) = 4u(n+1) - u(n)$$

olan

$$0, 1, 4, 15, 56, 209, 780, \ldots$$

dizisi de (1.2) bağıntısını gerçekler. Ward bu şekildeki dizilere *singüler dizi* adını vermiş ve (1.2) bağıntısını gerçekleyen bu singüler dizilerin, $a + b \in \mathbb{Z}$ ve $ab = 1$ olmak üzere

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

formundaki Lucas dizileri olduğunu göstermiştir.

Örneğin, $a = 2 + \sqrt{3}$ ve $b = 2 - \sqrt{3}$ olarak alındığında yukarıda verilen 0, 1, 4, 15, … dizisi elde edilir. Böylece tüm singüler diziler belli bir $\theta \in \mathbb{Q}$ için,

$$u(n) = \frac{\sin(n\theta)}{\sin\theta}$$

formundadır. Ayrıca σ, Weierstrass σ-fonksiyonu olmak üzere,

$$\tau_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

olarak tanımlanan $\tau_n(z)$ fonksiyonu da (1.2) bağıntısını gerçekler.

(1.2) bağıntısının hesaplanması (1.1) bağıntısına göre daha kolaydır. (1.2) bağıntısından,

$$u(2n+1) = u(n+2)u(n)^3 - u(n-1)u(n+1)^3 \tag{1.3}$$

$$u(2n)u(2) = u(n+2)u(n)u(n-1)^2 - u(n)u(n-2)u(n+1)^2 \tag{1.4}$$

bağıntıları elde edilir. Bu iki bağıntı,

$$u(n)u\left(\left\lfloor \frac{n}{\left\lfloor \frac{n+1}{2} \right\rfloor} \right\rfloor\right) = u\left(\left\lfloor \frac{n+4}{2} \right\rfloor\right)u\left(\left\lfloor \frac{n-1}{2} \right\rfloor\right)^2 - u\left(\left\lfloor \frac{n+1}{2} \right\rfloor\right)u\left(\left\lfloor \frac{n-3}{2} \right\rfloor\right)u\left(\left\lfloor \frac{n+2}{2} \right\rfloor\right)^2$$

biçiminde tek bir bağıntı altında toplanabilir.

Ward,

$$u(0) = 0,\ u(1) = 1 \text{ ve } u(2)u(3) \neq 0$$

ise (1.2) bağıntısının çözümlerini *has çözüm* olarak isimlendirmiştir. Bu şekildeki has çözümün eliptik bölünebilir dizi olması için gerek ve yeter şart $u(2)$, $u(3)$ ve $u(4)$

terimlerinin tamsayı olması, $u(2) \mid u(4)$ ve (1.3) ile (1.4) bağıntılarının her $n \geq 0$ tamsayısı için gerçeklenmesidir. Böylece $0 \leq i \leq 4$ için $u(i)$ terimleri bir tek eliptik bölünebilir dizi tanımlar ve bu terimler dizinin başlangıç terimleri olarak adlandırılır.

Eliptik bölünebilir diziler 2. bölümde ayrıntılı bir şekilde ele alınacaktır.

1.3 Periyodiklik

$a(x)$ bir dizi olmak üzere belli $t \in \mathbb{N}$ ve her $x \geq x_0$ için

$$a(x + t) = a(x)$$

eşitliği gerçekleniyor ise a dizisine bir *periyodik dizi* denir. Bu eşitliği gerçekleyen en küçük $t > 0$ değerine ise a dizisinin *periyodu* denir. Eğer periyodiklik bağıntısı $x_0 = 0$ için gerçekleniyor ise diziye *tam periyodik dizi* denir.

Her tam periyodik dizi bir lineer rekurrent dizi belirtir. Diğer yandan bir cisim üzerinde tanımlı olan periyodik dizi de bir lineer rekurrent dizi belirtir.

g^x üstel fonksiyonunun periyodu *çarpımsal mertebesi* veya *kuvvetidir*; g fonksiyonunun periyodu ise (g^x) dizisinin periyodudur.

Sonlu bir R halkası üzerinde tanımlı mertebesi n olan lineer rekurrent bir dizi periyodiktir ve periyodu $t \leq |R|^n - 1$ dir. Eğer dizinin ardışık n tane terimi sıfır ise sonraki tüm terimleri de sıfırdır ve böylece bu dizinin periyodu 1 olur. R üzerinde tanımlı bir dizide sıfırdan farklı olan en çok $|R|^n - 1$ tane n-liler olabilir. Böylece belli $1 \leq l < k \leq |R|^n$ için,

$$(a(k),...,a(k+n-1)) = (a(l),...,a(l+n-1))$$

şeklinde birbirine özdeş olan iki tane n-li vardır. Dolayısıyla $x \geq l$ için,

$$a(x) = a(x+k-l)$$

olur. Eğer f_0, R halkasında tersi olan bir eleman ise dizi ters yönde de devam eder ve böylece her $x \geq 1$ için $a(x) = a(x+l-k)$ olur. Periyodu en çok $|R|^n$ olan diziler R üzerinde tanımlı *M-dizileri* olarak adlandırılır.

Özel olarak sonlu bir R halkası üzerinde tanımlanmış lineer olmayan rekurrent dizinin periyodu en çok $|R|^n$ olabilir. Ayrıca,

$$a(x+n) = s_1(x)a(x+n-1) + ... + s_{n-1}(x)a(x+1) + s_n(x)a(x)$$

bağıntısını gerçekleyen bir tamsayı dizisi de herhangi $m \in \mathbb{N}$ için modülo m de periyodiktir ve periyodu $t \leq m^{n+1}$ dir.

Periyodun uzunluğu aslında $\{\alpha_1,...,\alpha_n\}$ karakteristik köklerinin özellikleri ile ilişkilidir. $R = \mathbb{F}$ ve karakteristik polinom kare serbest (karesiz) olduğunda, $i = 1, \ldots, n$ için, eğer t

$$\alpha_i^{\,t} = 1$$

eşitliğini gerçekleyen en küçük negatif olmayan tamsayı ise dizinin periyodu t olur.

$f(0) \neq 0$ özelliğindeki her $f \in \mathbb{F}_q[X]$ polinomu için

$$f(X) \mid (X^T - 1)$$

olacak şekilde en küçük $T \in \mathbb{N}$ sayısı belirlenebilir, bu T değerine f polinomunun periyodu denir ve $T = \text{per}(f)$ olarak gösterilir.

f polinomunun kökleri $\alpha_1,...,\alpha_n$ ve bu köklerin katlılıkları da $n_1,...,n_m$ ile gösterilsin. $N = \text{maks}\{n_1,...,n_m\}$ olmak üzere f polinomunun periyodu

$$\text{per}(f) = p^{\lfloor \log_p N \rfloor} \text{okek}(\text{per}(\alpha_1), \ldots, \text{per}(\alpha_m))$$

olarak elde edilir. Eğer f polinomu kare serbest monik polinom ise $L^*(f)$ kümesindeki her bir dizinin periyodu,

$$t = \text{per}(f) \mid (q^n - 1)$$

olur.

1.3.1 Teorem. Bir cisim üzerinde tanımlanmış $f(0) \neq 0$ özelliğindeki f monik polinomu için aşağıdaki özellikler gerçeklenir.

- $L^*(f)$ kümesinden alınan her bir dizinin periyodu aynı olup t = per(f) olarak gösterilir,
- $L(f)$ kümesinden alınan bir dizinin periyodu t değerini böler,
- $L(f)$ kümesinde olup en küçük T periyoduna sahip dizilerin sayısı,

$$\mu(n) = \begin{cases} 1 & n \text{ çift sayıda asal çarpana sahip olan karesiz sayı} \\ -1 & n \text{ tek sayıda asal çarpana sahip olan karesiz sayı} \\ 0 & n \text{ asal çarpanların karesi} \end{cases}$$

olmak üzere,

$$\sum_{d|T} \mu(T/d) q^{\text{der}(\text{obeb}(f(X),\ X^d-1))}$$

dir (Everest ve ark. 2003).

1.4 Lineer Rekurrent Dizilerde Asal Terimler

$\mathbb{P}$ asal sayıların kümesi olmak üzere herhangi bir a dizisi ve belli bir $N \in \mathbb{N}$ için $x \leq N$ ve $a(x) \in \mathbb{P}$ özelliğindeki terimlerin sayısı $P_a(N)$ olarak gösterilir. Genellikle $N \to \infty$ halinde $P_a(N) \to \infty$ olur. Ancak bazı özel dizilerde $P_a(N)$ değeri için bir üst sınır bulunabilir. Örneğin, $a_+(x) = 2^x + 1$ ve $a_-(x) = 2^x - 1$ dizileri dikkate alındığında, $a_+(x)$ dizisinin terimleri, sadece $x = 2^h$ olarak alınması halinde asal olabilir. Dolayısıyla

$$P_{a_+}(N) \leq \log N$$

olarak elde edilir. İkinci dizinin terimleri ise sadece $x = p \in \mathbb{P}$ olarak alındığında asal değerler verir ve böylece

$$P_{a_-}(N) = O(N/\log N)$$

olarak elde edilir.

Hatırlanacağı gibi, $k \in \mathbb{N}$ olmak üzere $2^{2^h} + 1$ biçimindeki asal sayılara *Fermat asalları*, $p \in \mathbb{P}$ olmak üzere $M_p = 2^p - 1$ biçimindeki asal sayılara ise *Mersenne asalları* denir.

Bilinen genel sonuçlardan birisi de

$$N - P_a(N) \to \infty$$

olduğudur. Bu sonuç, dizinin, aynı zamanda sonsuz çoklukta asal olmayan teriminin de olduğunu gösterir.

Daha sonra ele alınacak olan eliptik bölünebilir bir a dizisi için $P_a(N)$ değeri bir üst sınıra sahiptir.

Dubner ve Keller, Fibonacci dizisinin 10^5. terimine kadar olan asalları belirlemişlerdir. Fibonacci dizisinin bilinen en büyük asal terimi ise $a(81839)$ terimidir.

Bir başka örnek olarak

$$a(n) = (a(n-1)a(n-6) + a(n-3)a(n-4)) / a(n-7)$$

bağıntısını gerçekleyen

1, 1, 1, 1, 1, 1, 1, 2, 3, 4, 6, 12, 24, 72, 144, 288, 864, 3456, …

dizisinin her bir terimi 2^a3^b formundadır, dolayısıyla bu dizinin sadece 2 tane asal terimi vardır.

1.4.1 Uyarı. Gösterim kolaylığı olması için bundan sonra bir a dizisinin n. terimini göstermek için $a(n)$ gösterimi yerine a_n gösterimi kullanılacaktır.

1.5 Eliptik Eğriler

Bu kısımda hem eliptik bölünebilir diziler ile hem de Somos dizileri ile ilişkili olan eliptik eğri kavramı üzerinde durulacaktır.

1.5.1 Tanım. $\mathbb{F}$ karakteristiği 2 ve 3 ten farklı bir cisim olsun. $A, B \in \mathbb{F}$ olmak üzere

$$E : y^2 = x^3 + Ax + B$$

biçimindeki denklemin tüm çözümlerinin oluşturduğu sıralı ikililerin kümesine bir *eliptik eğri* denir. Bu denkleme E eliptik eğrisinin *Weierstrass normal formu* veya sadece *Weierstrass formu* denir.

Eğer E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ise E eğrisi üzerindeki noktaların kümesi $E(\mathbb{F})$ ile belirtilir, yani

$$E(\mathbb{F}) = \{\boldsymbol{O}\} \cup \{ (x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + Ax + B \}$$

dir. $\boldsymbol{O} = (\infty, \infty)$ ile gösterilen ve "*sonsuzdaki nokta*" adı verilen noktanın daima E eliptik eğrisi üzerinde olduğu kabul edilir.

1.5.2 Tanım. $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ olmak üzere

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

biçimindeki denkleme E eliptik eğrisinin *Weierstrass uzun formu* denir.

Weierstrass uzun formda verilmiş olan bir E eğrisi için *Tate değerleri*

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = a_1\, a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2\, a_6 - a_1\, a_3\, a_4 + 4a_2\, a_6 + a_2\, a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24b_4$$

olarak tanımlanır. Bundan başka E eliptik eğrisinin *diskriminantı* ve *j değişmezi*

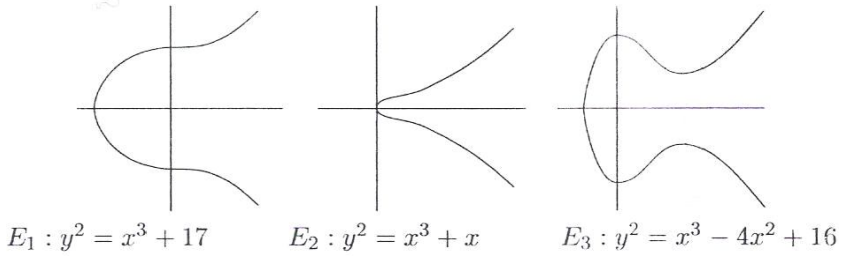
$$\Delta(E) = -\, b_2^2\, b_8 - 8\, b_4^3 - 27\, b_6^2 + 9 b_2\, b_4\, b_6 \quad \text{ve} \quad j = \frac{c_4^3}{\Delta}$$

olarak tanımlanır.

1.5.3 Tanım. E eliptik eğrisi $f(x, y) = 0$ denklemiyle verilmiş olsun. Bu durumda $P = (x_0, y_0) \in E$ noktasının E eğrisinin bir *singüler noktası* olması için gerek ve yeter şart

$$\frac{\partial f}{\partial x}(x_0, y_0) = 0 \text{ ve } \frac{\partial f}{\partial y}(x_0, y_0) = 0$$

olmasıdır.

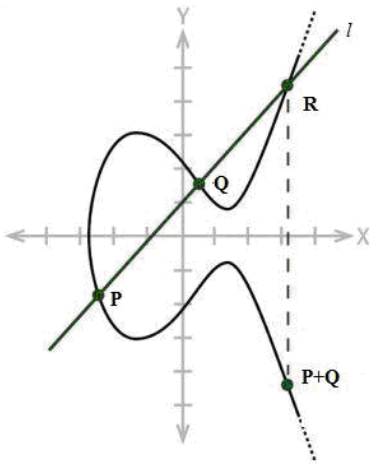


Şekil 1.1 Eliptik eğri örnekleri

Eğer $P = (x_0, y_0)$ noktasında birinci kısmi türevler sıfırsa singüler nokta katlı bir noktadır. Bu katlı nokta, iki farklı teğetinin olması halinde *düğüm (node) noktası,* iki teğetinin çakışması halinde *çıkıntı (cusp*) *noktası* olarak adlandırılır. Singüler noktaları olan eğriye *singüler eğri*, singüler noktaları olmayan bir eğriye de *singüler olmayan eğri* denir.

Eliptik eğriler, üzerinde tanımlanan toplama işlemi yardımıyla aslında bir değişmeli grup belirtmektedirler. Böylece eliptik eğriler üzerinde cebirsel işlemler de yapılabilmektedir.

1.5.4 Tanım. E eliptik eğri, $\boldsymbol{O} = (\infty, \infty)$ ve $P, Q \in E$ olmak üzere P ve Q noktalarından geçen l doğrusunu dikkate alınsın (Şekil 1.2). E eliptik eğrisini belirten Weierstrass eşitliğinin derecesi 3 olduğundan l doğrusu ile E eliptik eğrisi, P ve Q noktalarından



Şekil 1.2 Eliptik eğri üzerindeki toplama işlemi

farklı R gibi üçüncü bir noktada daha kesişir. P ve Q noktalarının toplamı, yani $P + Q$ noktası, az önce elde edilen R noktasının x eksenine göre simetriği olarak tanımlanır.

Bu toplama işlemi analitik olarak şöyle ifade edilebilir: $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$, E eliptik eğrisi üzerinde farklı iki nokta ve bu iki noktadan geçen l doğrusunun denklemi $y = mx + b$ ise

$$y^2 = x^3 + Ax + B \text{ ve } y = mx + b$$

denklemlerinden

$$x^3 - m^2 x^2 + (A - 2mb)x + B - b^2 = 0$$

eşitliği elde edilir. Bu kübik polinomun kökleri x_1, x_2 ve x_3 olmak üzere $R = (x_3, y_3)$ noktasının x eksenine göre simetriği olan nokta

$$P + Q = (x_3, -y_3)$$

noktasıdır.

Eğer $P = (x_1, y_1)$ ve $Q = (x_1, y_2)$ noktaları E eliptik eğrisi üzerinde apsisleri aynı olan farklı iki nokta ise bu durumda P ve Q noktalarından geçen doğru x-eksenine diktir, dolayısıyla E eliptik eğrisi ile P ve Q noktalarından geçen doğru sonsuzdaki $\boldsymbol{O}$ noktasında kesişir. Böylece bu durumda $P + Q = \boldsymbol{O}$ olur.

E eliptik eğrisi üzerindeki $P = (x_1, y_1)$ noktasının kendisiyle toplamının bulunması halinde E eliptik eğrisinin bu noktadan geçen teğetinin kullanılması gerekir. Bu durumda, bu teğet doğrunun denklemi ile E eliptik eğrisinin denkleminin ortak çözümünden elde edilen kübik polinomun kökleri $x_1 = x_2$ ve x_3 olmak üzere $R = (x_3, y_3)$ noktasının x eksenine göre simetriği olan nokta

$$P + P = 2P = (x_3, -y_3)$$

noktasıdır. Özel olarak $y_1 = 0$ ise bu noktadan geçen teğet doğru x-eksenine dik olacaktır. Bu durumda $P + P = 2P = \boldsymbol{O}$ olarak elde edilir.

E eliptik eğrisi üzerindeki herhangi bir $P = (x_1, y_1)$ noktası ile sonsuzdaki $\boldsymbol{O}$ noktasından geçen doğru E eliptik eğrisini belli bir $P' = (x_1, -y_1)$ noktasında keser. Bu durumda P'

noktasının x-eksenine göre simetriği yine P noktası olduğundan $P + \boldsymbol{O} = P$ olarak elde edilir.

1.5.5 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda E eliptik eğrisi üzerindeki noktalar aşağıdaki özellikleri gerçeklerler:

i. Her $P_1, P_2 \in E(\mathbb{F})$ için $P_1 + P_2 = P_2 + P_1$ dir (değişme özelliği),

ii. Her $P \in E(\mathbb{F})$ için $P + \boldsymbol{O} = P$ dir (birim eleman özelliği),

iii. Her $P \in E(\mathbb{F})$ için $P + P' = \boldsymbol{O}$ olacak biçimde bir $P' \in E(\mathbb{F})$ vardır ve $P' = -P$ dir (ters eleman özelliği),

iv. Her $P_1, P_2, P_3 \in E(\mathbb{F})$ için $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ dir (birleşme özelliği) (Washington 2003).

Yukarıda verilen teorem, E eliptik eğrisi üzerindeki noktaların oluşturduğu kümenin toplama işlemine göre bir değişmeli grup ve sonsuzdaki nokta "$\boldsymbol{O}$" noktasının da bu grubun bu toplama işlemine göre birim elemanı olduğunu belirtmektedir.

Eliptik eğrinin Weierstrass uzun formda verilmesi halinde de toplama işlemi analitik olarak benzer şekilde ifade edilir.

1.5.6 Tanım. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ve $n \in \mathbb{N}$ olsun. Bu durumda

$$nP = \boldsymbol{O}$$

olacak biçimdeki $P \in E(\mathbb{F})$ noktasına bir *büküm* (*torsiyon*) *noktası* ya da bir *sonlu mertebeli nokta* denir. Bu şartı gerçekleyen en küçük n sayısına P noktasının *mertebesi* denir. Eğer P noktası bir büküm noktası değilse bu nokta *sonsuz mertebeli nokta* olarak adlandırılır.

$$E[n] = \{ P \in E(\overline{\mathbb{F}}) \mid nP = \boldsymbol{O} \}$$

kümesine ise E eliptik eğrisinin *n büküm noktalarının kümesi* denir.

Dikkat edilirse $E[n]$ kümesi $E(\overline{\mathbb{F}})$ üzerinde tanımlanmıştır ve üstelik $E[n]$, $E(\overline{\mathbb{F}})$ grubunun bir alt grubudur. Burada her $n \in \mathbb{N}$ için $\boldsymbol{O} \in E[n]$ olduğu açıktır. Aşağıdaki teorem $E[n]$ grubunun grup yapısını ortaya koymaktadır.

1.5.7 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri, $n \in \mathbb{N}$ olmak üzere $\mathbb{F}$ cisminin karakteristiği n sayısını bölmüyor veya sıfır ise

$$E[n] \cong \mathbb{Z}_n \otimes \mathbb{Z}_n$$

dir. Eğer $\mathbb{F}$ cisminin karakteristiği $p > 0$ ve $p \mid n$ ise $p \nmid m$ olmak üzere $n = p^r m$ için

$$E[n] \cong \mathbb{Z}_m \otimes \mathbb{Z}_m \text{ veya } E[n] \cong \mathbb{Z}_n \otimes \mathbb{Z}_m$$

dir (Washington 2003).

E eliptik eğrisinin üzerinde tanımlı olduğu cisim oldukça önemlidir. Bu cisim eliptik eğrinin noktaları kümesinin grup yapısını doğrudan ilgilendirir. Eliptik eğrinin üzerinde tanımlanmış olduğu cismin $\mathbb{Q}$ cismi olarak seçilmesi halinde akla gelen ilk soru eliptik eğri üzerindeki rasyonel noktaların sayısının ne olduğu olmuştur. Bu halde eliptik eğri üzerindeki rasyonel noktaların sayısının sonsuz olması beklenen bir cevap olduğu halde bu sayı sonlu da olabilir, özellikle bu sayının sonlu olması durumu oldukça ilginçtir. Diğer yandan $E(\mathbb{Q})$, $E(\mathbb{F})$ grubunun bir değişmeli alt grubu olduğundan $E(\mathbb{Q})$ grubunun grup yapısının belirlenmesi de bu halin önemli problemlerinden birisi olmuştur. $E(\mathbb{Q})$ grubunun grup yapısıyla ilgili olarak verilen aşağıdaki teorem $\mathbb{Q}$ cismi için verildiği halde her hangi bir sayı cismi üzerinde de geçerlidir.

1.5.8 Mordell-Weil Teoremi. E, $\mathbb{Q}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda $E(\mathbb{Q})$ sonlu üreteçli bir abelyen gruptur (Silverman 1986).

1.5.9 Tanım. E, $\mathbb{Q}$ cismi üzerinde tanımlı bir eliptik eğri olsun. E eğrisinin sonlu mertebeli noktalarının oluşturduğu alt gruba E eliptik eğrisinin *torsiyon alt grubu* denir ve bu alt grup $E_{\text{tors}}(\mathbb{Q})$ ile gösterilir. $r \geq 0$ tamsayı olmak üzere $E_{\text{tors}}(\mathbb{Q}) \otimes \mathbb{Z}^r$ grubuna E eliptik eğrisinin *Mordell-Weil grubu* ve r sayısına da E eliptik eğrisinin *rankı* denir.

1.5.10 Uyarı 1. Sonlu üreteçli abelyen grupların temel teoremi gereği, E eliptik eğrisi için

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \otimes \mathbb{Z}^r$$

dir (Washington 2003).

2. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri ise $E_{\text{tors}}(\mathbb{Q})$ sonludur (Washington 2003).

3. $r = 0$ olması durumunda $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi üzerinde sonlu tane rasyonel nokta olacağı, yani $E(\mathbb{Q})$ grubunun sonlu olacağı açıktır.

4. $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi verildiğinde $E_{\text{tors}}(\mathbb{Q})$ nun izomorf olabileceği tüm gruplar B. Mazur'un aşağıdaki teoremiyle verilmiştir.

1.5.11 Teorem. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$E_{\text{tors}}(\mathbb{Q}) = \begin{cases} \mathbb{Z}_n & : 1 \le n \le 10, n = 12 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2n} & : 1 \le n \le 4 \end{cases}$$

olur. Bundan başka bu gruplardan her birisi için $E_{\text{tors}}(\mathbb{Q})$ bu gruplara izomorf olacak şekilde bir E eliptik eğrisi de vardır (Mazur 1978).

Verilen bir E eliptik eğrisi uygun birasyonel dönüşümlerle E eğrisinden daha basit bir yapıya sahip bir E' eliptik eğrisine dönüştürülebilir.

1.5.12 Tanım. $\mathbb{F}$ cismi üzerinde tanımlı

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

ve

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

eliptik eğrileri verilsin. Bu durumda E eğrisini E' eğrisine dönüştüren

$$x = u^2\, x' + r, \quad y = u^3\, y' + u^2\, s\, x' + t \qquad (u, r, s, t \in \mathbb{F}, u \neq 0) \qquad (1.5)$$

dönüşümleri varsa E ve E' eliptik eğrilerine $\mathbb{F}$ cismi üzerinde *birasyonel denktir* denir.

Bu dönüşümlerin tersleri vardır ve tersleri

$$x' = \frac{1}{u^2}(x-r),\ y' = \frac{1}{u^3(y-sx+sr-t)}$$

biçimindedir. Bu dönüşümlere birasyonel denmesinin nedeni kendisi ve tersinin rasyonel dönüşümler olmasıdır. Bu durumda (1.5) de verilen dönüşümler E ve E' eliptik eğrileri arasında birebir-örten bir dönüşüm belirtir ve böylece $\mathbb{F}$ cismi üzerindeki birasyonel denklik ilişkisi bir denklik bağıntısı olur. Bu eğriler arasındaki bu birebir-örten dönüşüm $E(\mathbb{F})$ ve $E'(\mathbb{F})$ grupları arasında bir izomorfizm oluşturur. Bu durumun tersi doğru değildir, yani E ve E' eğrileri $\mathbb{F}$ cismi üzerinde birasyonel denk olmasalar bile $E(\mathbb{F})$ ve $E'(\mathbb{F})$ grupları izomorf olabilir.

Aşağıdaki teoremler dikkate alındığında bir eliptik eğrinin bölüm polinomları ile bu bölüm polinomları ile elde edilen eliptik bölünebilir diziler arasındaki ilişkiler görülmektedir.

1.5.13 Teorem. $\mathbb{F}$ cismi üzerinde tanımlı

$$E : y^2 = x^3 + Ax + B$$

eliptik eğrisinin $\psi_n \in \mathbb{Z}[A, B, x, y]$ bölüm polinomları

$$\psi_o = 0,$$
$$\psi_1 = 1,$$
$$\psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

ve $n \geq 2$ için,

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3,$$
$$\psi_{2n} = \left(\frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{\psi_2}\right)$$

ve $n < 0$ için

$$\psi_{-n} = -\psi_n$$

biçimindedir (Washington 2003).

1.5.14 Teorem. Bir eliptik eğrinin bölüm polinomları her $n, m \in \mathbb{Z}$ için

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2$$

eşitliğini gerçeklerler (Charlap ve Robbins 1988).

E eliptik eğrisi sonlu mertebeli ve mertebesi N olan bir $Q = (x, y)$ noktasını bulunduran bir eliptik eğri olsun. E eliptik eğrisi uygun bir birasyonel dönüşüm ile sonlu mertebeli ve mertebesi N olan $P = (0, 0)$ noktasını bulunduran bir eliptik eğriye dönüştürülebilir. Bu şekilde hareket edilerek, sonlu mertebeli noktalar bulunduran her bir eliptik eğri sonlu mertebeli noktası $P = (0, 0)$ noktası olan özel eliptik eğrilere dönüştürülebilir. $P = (0, 0)$ noktasını sonlu mertebeli bir nokta olarak bulunduran eliptik eğriler ailesi Tate normal formdaki eliptik eğriler olarak adlandırılır.

1.5.15 Tanım. $P = (0, 0)$ sonlu mertebeli bir nokta ve mertebesi N olmak üzere P noktasını bulunduran E eliptik eğrisinin *Tate normal formu*

$$E_N:\ y^2 + (1-c)xy - by = x^3 - bx^2$$

olarak tanımlanır.

Eğer Mazur teoremi dikkate alınırsa, bir eliptik eğri üzerindeki sonlu mertebeli noktaların mertebelerinin ancak 2, 3, 4, 5, 6, 7, 8, 9, 10 veya 12 olabileceği görülür. Tate normal formdaki her bir eliptik eğri için $P = (0, 0)$ noktası en büyük mertebeye sahip noktadır.

$N = 2, 3, 4, 5, 6, 7, 8, 9, 10$ veya 12 ve $P = (0, 0)$ noktası

$$E_N:\ y^2 + (1-c)xy - by = x^3 - bx^2$$

eliptik eğrisi üzerinde en yüksek mertebeye sahip olan nokta olmak üzere, Tate normal formdaki eliptik eğriler, bir $\alpha \in \mathbb{Z}$ parametresine bağlı olarak

1. $N = 4 \Rightarrow b = \alpha$ ve $c = 0$
2. $N = 5 \Rightarrow b = \alpha$ ve $c = \alpha$
3. $N = 6 \Rightarrow b = \alpha + \alpha^2$ ve $c = \alpha$
4. $N = 7 \Rightarrow b = \alpha^3 - \alpha^2$ ve $c = \alpha^2 - \alpha$

5. $N = 8 \Rightarrow b = (2\alpha - 1)(\alpha - 1)$ ve $c = \dfrac{b}{\alpha}$

6. $N = 9 \Rightarrow b = c(\alpha(\alpha - 1) + 1)$ ve $c = \alpha^2(\alpha - 1)$

7. $N = 10 \Rightarrow b = \dfrac{c\alpha^2}{\alpha - (\alpha - 1)^2}$ ve $c = \dfrac{2\alpha^3 - 3\alpha^2 + \alpha}{\alpha - (\alpha - 1)^2}$

8. $N = 12 \Rightarrow b = \dfrac{c(2\alpha - 2\alpha^2 - 1)}{\alpha - 1}$ ve $c = \dfrac{(3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)}{(\alpha - 1)^3}$.

biçiminde sınıflandırılır (Husemöller 2004).

2. BÖLÜM

ELİPTİK BÖLÜNEBİLİR DİZİLER

Bu bölümde eliptik bölünebilir diziler ele alınacaktır. Kısım 2.1 de eliptik dizi ve eliptik bölünebilir dizi kavramları tanımlanarak bu dizilerin temel özellikleri üzerinde durulacaktır. Kısım 2.2 de denk dizi kavramı açıklanacaktır. Kısım 2.3 de özel bir eliptik dizi sınıfı olan Lucas dizileri ve singüler dizi kavramı ele alınacak ve bu dizilerin özellikleri belirtilecektir. Kısım 2.4 de eliptik bölünebilir diziler ve eliptik eğriler arasındaki ilişkiler incelenecektir. Kısım 2.5 de modülo p de indirgenmiş eliptik bölünebilir dizilerin simetri ve periyodiklik özellikleri ile ilgili olan bazı teorem ve konjektürler verilecektir. Son olarak Kısım 2.6 da ise eliptik bölünebilir dizilerdeki kare ve küp terimlerin belirlenmesi ile ilgili elde edilen sonuçlar verilecektir.

2.1 Eliptik Bölünebilir Diziler

2.1.1 Tanım. Terimleri rasyonel sayı olan bir (h_n) dizisi $m, n \in \mathbb{Z}$ olmak üzere

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^{\,2} - h_{n+1}h_{n-1}h_m^{\,2} \tag{2.1}$$

bağıntısını gerçekliyor ise (h_n) dizisine bir *eliptik dizi* denir.

(h_n) eliptik dizisinin tüm terimleri birer tamsayı ve $n \mid m$ özelliğindeki her $m, n \in \mathbb{Z}$ için $h_n \mid h_m$ ise (h_n) eliptik dizisine bir *eliptik bölünebilir dizi* denir.

2.1.2 Örnek 1. Terimleri

$$\ldots, 0, 1, -2, 3, -701, 5581, \frac{1407231}{2}, -688793515, \frac{96215981423}{4}, \ldots$$

olarak verilen dizi bir eliptik dizidir. Ancak bölünebilirlik özelliği gerçeklenmediğinden bir eliptik bölünebilir dizi değildir.

2. $n \in \mathbb{Z}$ olmak üzere $(h_n) = n$ olarak tanımlanan, $\mathbb{Z}$ tamsayılar dizisi eliptik bölünebilir diziler için en temel örnektir.

3. Başlangıç terimleri $F_0 = 0$, $F_1 = 1$ olan ve $n \geq 2$ için

$$F_n = F_{n+1} + F_{n-2}$$

lineer bağıntısı ile tanımlanan

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

Fibonacci dizisi bir bölünebilir dizidir. Bu dizi yardımıyla elde edilen ve $n \geq 0$ için

$$h_n = (-1)^{\frac{1}{2}(n-1)(n-2)} F_n \quad \text{ve} \quad h_{-n} = -h_n$$

bağıntısı ile tanımlanan

$$\ldots, 3, 2, -1, -1, 0, 1, 1, -2, -3, 5, 8, -13, -21, \ldots$$

(h_n) dizisi ise bir eliptik bölünebilir dizidir.

Bir eliptik bölünebilir dizinin terimlerinin bulunması için, adına duplikasyon formülleri denen formüller kullanılır. İlk olarak

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^{\,2} - h_{n+1}h_{n-1}h_m^{\,2}$$

bağıntısında $n = 2$ olarak alınırsa, her $m \in \mathbb{Z}$ için

$$h_{m+2}h_{m-2} = h_{m+1}h_{m-1}h_2^{\,2} - h_3h_1h_m^{\,2} \tag{2.2}$$

toplama formülü elde edilir. Diğer yandan

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^{\,2} - h_{n+1}h_{n-1}h_m^{\,2}$$

bağıntısında $m = n + 1$, $n = n$ ve daha sonra $m = n + 1$, $n = n - 1$ olarak alınırsa, sırasıyla

$$h_{2n+1}h_1 = h_{n+2}h_n^{\,3} - h_{n-1}h_{n+1}^{\,3} \tag{2.3a}$$

$$h_{2n}h_2 = h_n(h_{n+2}h_{n-1}^{\,2} - h_{n-2}h_{n+1}^{\,2}) \tag{2.3b}$$

duplikasyon formülleri elde edilir.

2.1.3 Uyarı 1. Her $n > 0$ için h_n terimleri sıfırdan farklı ise (2.3a) bağıntısı yardımıyla başlangıç terimleri

$$h_0 = 0, h_1 = 1, h_2, h_3, h_4$$

olan (h_n) eliptik bölünebilir dizisi bir tek şekilde belirlenir, $h_2 \neq 0$ ise (2.3b) bağıntıları yardımıyla başlangıç terimleri

$$h_0 = 0, h_1 = 1, h_2, h_3, h_4$$

olan (h_n) eliptik bölünebilir dizisi bir tek şekilde belirlenir.

2. Daha önce 1. bölümde de belirtildiği gibi,

$$h_0 = 0, h_1 = 1, h_2 h_3 \neq 0$$

olmak üzere (2.1) bağıntısının bir çözümü Ward tarafından *has çözüm* olarak adlandırılmıştır. Bu şekildeki bir has çözümün bir eliptik bölünebilir dizi olması için gerek ve yeter şart $h_2 | h_4$ olmak üzere h_2, h_3, h_4 terimlerinin birer tamsayı olmasıdır.

2.2 Denk Eliptik Bölünebilir Diziler

2.2.1 Teorem. (h_n) bir eliptik bölünebilir dizi olsun. Bu durumda sıfırdan farklı olan herhangi bir $\theta \in \mathbb{R}$ sayısı ve her $n \in \mathbb{Z}$ için,

$$h_n' = \theta^{n^2-1} h_n$$

olarak tanımlanan (h_n') dizisi de bir eliptik bölünebilir dizidir (Ward 1948).

Bu teoremin bir sonucu olarak Ward, eliptik bölünebilir dizilerdeki denklik kavramını aşağıdaki gibi ifade etmiştir.

2.2.2 Tanım. (h_n) ve (h_n') iki eliptik bölünebilir dizi olsun. Eğer her $n \in \mathbb{Z}$ için,

$$h_n' = \theta^{n^2-1} h_n$$

eşitliğini gerçekleyen sıfırdan farklı bir $\theta \in \mathbb{R}$ sayısı varsa, (h_n) ve (h_n') dizilerine *denk diziler* denir.

2.2.3 Uyarı 1. Ward yukarıda verilen denklik kavramını ifade ederken θ sayısıyla ilgili bir kısıtlama belirtmediği halde gerçekte θ sabiti bir rasyonel sayıdır. Gerçektende, $h_2 h_3 \neq 0$ ise $\theta^3 = \frac{h_2'}{h_2}$ ve $\theta^8 = \frac{h_3'}{h_3}$ sayıları birer rasyonel sayı olacağından $\frac{(\theta^3)^3}{\theta^8} = \theta$ sayısı da bir rasyonel sayıdır.

2. $h_2 h_3 \neq 0$ özelliğindeki her bir (h_n) eliptik dizisi bir eliptik bölünebilir diziye denktir (Ward 1948).

2.3 Lucas Dizileri ve Singüler Diziler

Eliptik bölünebilir diziler, daha önce Edouard Lucas tarafından çalışılmış olan bölünebilir dizilerin bir genelleştirilmesidirler. Ward, Lucas dizileri için verilen sonuçları eliptik bölünebilir diziler için genişletmiştir.

2.3.1 Tanım. c bir rasyonel sayı ve a, b sayıları $x^2 - cx + 1$ polinomunun kökleri olsun. Her $n \in \mathbb{Z}$ için $a \neq b$ ise,

$$l_n = \frac{a^n - b^n}{a - b}$$

ve $a = b$ ise,

$$l_n = na^{n-1}$$

olarak tanımlanan (l_n) dizisine c ile parametrelendirilen *Lucas dizisi* denir.

Her bir (l_n) Lucas dizisi (2.1) bağıntısını gerçekler ve böylece her bir (l_n) Lucas dizisi bir eliptik dizidir. Bununla birlikte bir (l_n) Lucas dizisinin eliptik bölünebilir dizi olması için gerek ve yeter şart c sayısının bir tamsayı olmasıdır.

2.3.2 Tanım. $h_2 h_3 \neq 0$ olmak üzere (h_n) eliptik bölünebilir dizisinin *diskriminantı*,

$$\Delta(h_2, h_3, h_4) = \frac{1}{h_2^{\,8} h_3^{\,3}}(-h_4^{\,4} - 3h_2^{\,5} h_4^{\,3} + (-3h_2^{\,10} - 8h_2^{\,2} h_3^{\,3})h_4^{\,2} + (20h_2^{\,7} h_3^{\,3} - h_2^{\,15})h_4 + h_2^{\,12} h_3^{\,3} - 16h_2^{\,4} h_3^{\,6})$$

olmak üzere $\Delta(h_2, h_3, h_4) = 0$ ise (h_n) dizisine bir *singüler dizi*, aksi halde bir *singüler olmayan dizi* denir. Özel olarak, p bir asal sayı olmak üzere $\Delta(h_2, h_3, h_4) = 0 \pmod p$ ise (h_n) dizisine *modülo p de singüler dizi* denir.

2.3.3 Uyarı 1. (h_n) ve (h_n') denk dizilerinin diskriminantları arasındaki ilişki,

$$\Delta(h_2, h_3, h_4) = \theta^{12}\Delta(h_2', h_3', h_4')$$

şeklindedir. Dolayısıyla (h_n') dizisinin singüler olması için gerek ve yeter şart (h_n) dizisinin singüler olmasıdır.

2. (h_n) bir singüler eliptik bölünebilir dizi ve r, s tamsayıları $s \neq 1$ için $h_2 = r$, $h_3 = s(r^2 - s^3)$, $h_4 = rs^3(r^2 - 2s^3)$ özelliğindeki tamsayılar olmak üzere

$$c = \frac{r\sqrt{s}}{s^2} \quad \text{ve} \quad \theta^2 = s$$

olsun. Bu durumda (l_n) bir Lucas dizisidir ve her $n \in \mathbb{Z}$ için $\theta \neq 0$ olmak üzere,

$$h_n = \theta^{n^2-1} l_n$$

dir (Ward 1948). Dolayısıyla her bir singüler eliptik bölünebilir dizi bir Lucas dizisidir veya bir Lucas dizisine denktir. O halde $\mathbb{Z}$ tamsayılar dizisi de özel bir Lucas dizisi olduğuna göre (c = 2 olması hali) her bir singüler eliptik bölünebilir dizi $\mathbb{Z}$ tamsayılar dizisine denktir.

2.4 Eliptik Bölünebilir Diziler ve Eliptik Eğriler Arasındaki İlişkiler

Daha önce belirtildiği gibi, $\mathbb{Q}$ cismi üzerinde tanımlı bir eliptik eğrinin bölüm polinomları her $m, n \in \mathbb{Z}$ için

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^{\,2} - \psi_{n+1}\psi_{n-1}\psi_m^{\,2}$$

bağıntısını gerçekler. Dolayısıyla eliptik eğri üzerindeki herhangi bir $P = (x_1, y_1)$ rasyonel noktası da bu bağıntıyı gerçekler. Böylece her $n \in \mathbb{Z}$ için

$$h_n = \psi_n(x_1, y_1)$$

olarak tanımlanan (h_n) dizisi bir eliptik dizi olur. Bu durumun tersinin de doğru olduğunu Ward aşağıdaki teorem ile ifade etmiştir.

2.4.1 Teorem. $h_2 h_3 \neq 0$ olmak üzere (h_n) bir eliptik dizi olsun. Bu durumda $\mathbb{Q}$ üzerinde tanımlı

$$E : y^2 = x^3 + Ax + B$$

eliptik eğrisi ve ψ_n, E eliptik eğrisinin n. bölüm polinomunu göstermek üzere her $n \in \mathbb{Z}$ için,

$$h_n = \psi_n(x_1, y_1)$$

olacak biçimde E eliptik eğrisi üzerinde bir $P = (x_1, y_1)$ rasyonel noktası vardır.

Özel olarak (h_n) eliptik dizisi ile eşleşen E eliptik eğrisinin A ve B katsayıları ve $P = (x_1, y_1)$ rasyonel noktasının koordinatları, (h_n) eliptik dizisinin h_2, h_3, h_4 başlangıç terimleri yardımıyla aşağıdaki gibi ifade edilebilir;

$$A = -\frac{1}{2^4 3 h_2^8 h_3^4}\left(h_2^{20} + 4h_2^{15}h_4 - 16h_2^{12}h_3^3 + 6h_2^{10}h_4^2 - 8h_2^7 h_3^3 h_4 + 4h_2^5 h_4^3 + 16h_2^4 h_3^6 + 8h_2^2 h_3^3 h_4^2 + h_4^4\right),$$

$$B = \frac{1}{2^5 3^3 h_2^{12} h_3^6}\left(h_2^{30} + 6h_2^{25}h_4 - 24h_2^{22}h_3^3 + 15h_2^{20}h_4^2 - 60h_2^{17}h_3^3 h_4 + 20h_2^{15}h_4^3 + 120h_2^{14}h_3^6\right.$$

$$\left. - 36h_2^{12}h_3^3 h_4^2 + 15h_2^{10}h_4^4 - 48h_2^9 h_3^6 h_4 + 12h_2^7 h_3^3 h_4^3 + 64h_2^6 h_3^9 + 6h_2^5 h_4^5 + 48h_2^4 h_3^6 h_4^2 + 12h_2^2 h_3^3 h_4^4 + h_4^6\right),$$

$$P = (x_1, y_1) = \left(\left(\frac{h_4 + h_2^5}{h_2^2 h_3}\right)^2 + \frac{h_3}{3h_2^2},\ \frac{1}{2}h_2\right)$$

dir (Ward 1948).

2.4.2 Uyarı 1. $A, B \in \mathbb{Q}$ olmak üzere, $h_3 \neq 0$ özelliğindeki bir (h_n) eliptik dizisinin

$$E : y^2 = x^3 + Ax + B$$

eliptik eğrisinin belli bir P noktasında hesaplanan bölüm polinomlarının dizisi olması için gerek ve yeter şart $h_4 = -h_2^5$ olmasıdır (Ward 1948).

2. E eliptik eğrisi bir singüler eğri olsa dahi teoremde belirtilen P noktası bir singüler nokta olamaz. Çünkü eliptik eğri üzerindeki bir singüler noktanın y-koordinatı sıfır olur; ancak teoremde de belirtildiği gibi P noktasının y-koordinatı $\frac{1}{2}h_2 \neq 0$ dır.

3. R. Shipsey (2000) doktora tezinde yukarıda belirtilen singüler olmayan P noktasını $P = (0, 0)$ noktası alarak ve bu noktadaki $h_n = \psi_n(0, 0)$ bölüm polinomlarını kullanarak dizinin terimleri için daha basit olan alternatif formül tanımlamıştır.

Eliptik dizinin eşleşmiş olduğu eliptik eğrinin uzun formu dizinin terimleri yardımıyla bulunmak istenirse aşağıdaki teorem yardımıyla bu eğrinin katsayıları belirlenebilir.

2.4.3 Teorem. $h_2 h_3 \neq 0$ olmak üzere (h_n) bir eliptik dizi olsun. Bu durumda (h_n) eliptik dizisi ile eşleşen

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

eliptik eğrisinin katsayıları, dizinin başlangıç terimleri yardımıyla aşağıdaki gibi ifade edilir:

$$a_4 = \text{keyfi}$$

$$a_3 = h_2$$

$$a_2 = \frac{h_2 {h_3}^2 + (h_4 + {h_2}^5)a_4 - h_2 h_3 {a_4}^2}{{h_2}^3 h_3}$$

$$a_1 = \frac{h_4 + {h_2}^5 - 2h_2 h_3 a_4}{{h_2}^2 h_3}$$

dir (Swart 2003).

2.4.4 Uyarı 1. Daha önce eliptik eğriler bölümünde tanımlanan eliptik eğrinin Tate değerleri de (h_n) dizisinin başlangıç terimleri yardımıyla aşağıdaki gibi ifade edilir:

$$b_8 = h_3$$

$$b_6 = {h_2}^2$$

$$b_4 = \frac{h_4 + {h_2}^5}{h_2 h_3}$$

$$b_2 = \frac{{b_4}^2 + 4h_3}{{h_2}^2}.$$

2. (h_n) dizisinin eliptik bölünebilir dizi olması halinde eliptik eğrinin katsayılarının özel seçilmesi gerekir. Bu durumda, (h_n) eliptik dizisinin bir eliptik bölünebilir dizi olması için gerek ve yeter şart dizinin eşleştiği eliptik eğrinin a_3, b_8 ve b_4b_8 katsayılarının tamsayı olmasıdır.

Ward aşağıdaki teorem ile birasyonel denk olan eliptik eğrilerin denk eliptik diziler ile eşleştiğini göstermiştir.

2.4.5 Teorem. $h_2 h_3 \neq 0$ ve $h_2' h_3' \neq 0$ özelliğindeki (h_n) ve (h_n') eliptik dizilerinin eşleştiği eliptik eğriler E ve E' olsun. Bu durumda (h_n) ve (h_n') eliptik dizilerinin $\theta \neq 0$ olmak üzere her $n \in \mathbb{Z}$ için

$$h_n' = \theta^{n^2-1} h_n$$

eşitliği altında denk olması için gerek ve yeter şart $u = \frac{1}{\theta}$ sabiti ve belli $s \in \mathbb{Q}$ rasyonel sayısı için (0, 0) noktasını (0, 0) noktasına resmeden

$$x = u^2 x' \quad \text{ve} \quad y = u^3 y' + u^2 s x'$$

değişken değişimleri altında E ve E' eliptik eğrilerinin birasyonel denk olmasıdır (Ward 1948).

Ward aşağıdaki teorem ile bir eliptik dizi ve bu dizinin eşleştiği eliptik eğrinin diskriminantının aynı olduğunu göstermiştir.

2.4.6 Teorem. $h_2 h_3 \neq 0$ olacak şekilde (h_n) eliptik dizi ve E ise bu dizi ile eşleşen eliptik eğri olsun. Bu durumda (h_n) eliptik dizisinin diskriminantı ile E eliptik eğrisinin diskriminantı aynıdır. Böylece (h_n) eliptik dizisinin singüler olması için gerek ve yeter şart E eliptik eğrisinin singüler olmasıdır (Ward 1948).

2.4.7 Örnek. $(h_n) = n$ olarak tanımlanan $\mathbb{Z}$ tamsayı dizisi bir singüler dizidir. Bu dizi ile eşleşen eliptik eğrinin Tate değerleri,

$$b_8 = h_3 = 3$$

$$b_6 = {h_2}^2 = 4$$

$$b_4 = \frac{h_4 + {h_2}^5}{h_2 h_3} = 6$$

$$b_2 = \frac{{b_4}^2 + 4h_3}{{h_2}^2} = 12$$

olarak elde edilir. Böylece E eliptik eğrisinin diskriminantı,

$$\Delta(E) = -{b_2}^2 b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2 b_4 b_6 = 0$$

olup, E singüler eğridir.

2.5 Modülo *p* de İndirgenmiş Eliptik Bölünebilir Diziler

Bu kısımda Ward ve Shipsey tarafından verilen, simetri ve periyodiklik özellikleri ile ilgili olan bazı teorem ve konjektürler ele alınacaktır.

2.5.1 Tanım. (h_n) bir eliptik bölünebilir dizi ve p bir asal sayı olmak üzere

$$h_n \equiv 0 \mod p^r \Leftrightarrow n \equiv 0 \pmod N$$

olacak şekildeki belli en küçük N pozitif tamsayısına p^r sayısının (h_n) eliptik bölünebilir dizisindeki *rankı* denir ve p^r sayısının rankı N_r olarak gösterilir.

2.5.2 Örnek. Başlangıç terimleri 0, 1, –1, –2, 5 ve terimleri

…, 0, 1, –1, –2, 5, 3, –44, 101, 835, –5446, –19191, 428647, –1913560, …

olarak elde edilen (h_n) dizisinin modülo 5 deki rankı $N_1 = 4$ dür.

Aşağıdaki teoremi Ward, $p > 3$ hali için eliptik eğrileri kullanarak ispat etmiştir. Ancak daha sonra Swart $p = 2$ ve $p = 3$ hallerini de kapsayan daha genel bir ispat vermiştir.

2.5.3 Teorem. (h_n), tek sıfır terimi h_0 olan bir eliptik bölünebilir dizi, p asal sayısı için $N_1 \geq 4$ ve dizinin h_{N_1} terimini bölen en büyük asal kuvvet p^w olsun. Bu durumda

i. p tek asal sayı veya $p = 2$ ve üstelik $w \geq 2$ ise $N_r = \begin{cases} N_1 & r \leq w \\ pN_{r-1} & r > w \end{cases}$,

ii. eğer $p = 2$ ve $w = 1$ ise belli $v \geq 2$ için $N_r = \begin{cases} N_1 & r = 1 \\ 2N_1 & 2 \leq r \leq v \\ 2N_{r-1} & r > v \end{cases}$ dir (Ward 1948, Swart 2003).

Ward tarafından, eliptik bölünebilir diziler için sadece s, $t > 0$ sayıları kullanılarak ifade edilen simetri formülü daha sonra Swart tarafından s, $t \in \mathbb{Z}$ sayıları için genişletilmiştir.

2.5.4 Teorem. (h_n) bir eliptik bölünebilir dizi ve p asal sayısı için $N_1 \geq 4$ olsun. Bu durumda her s, $t \in \mathbb{Z}$ için,

$$h_{t+sN_1} \equiv c_1^{\,st} (-b_1)^{s^2} h_t \pmod{p}$$

olacak şekilde b_1 ve c_1 tamsayıları vardır ve üstelik

$$b_1 = \frac{(h_{N_1-1})^2 h_2}{h_{N_1-2}} \pmod{p} \qquad \text{ve} \qquad c_1 = \frac{h_{N_1-1} h_2}{h_{N_1-2}} \pmod{p}$$

dir (Ward 1948, Swart 2003).

2.5.5 Tanım. (h_n) bir eliptik bölünebilir dizi olsun. Eğer yeterince büyük n sayıları için

$$h_{n+\pi} \equiv h_n \pmod{m}$$

olacak biçimde pozitif bir π sayısı varsa (h_n) eliptik bölünebilir dizisi modülo m de *periyodiktir* denir. Eğer bu denklik her $n \in \mathbb{Z}$ için gerçekleniyorsa bu durumda (h_n) eliptik bölünebilir dizisi modülo m de *tamamen periyodiktir* denir. Bu denkliği gerçekleyen en küçük pozitif π sayısına (h_n) eliptik bölünebilir dizisinin modülo m deki *periyotu* denir.

2.5.6 Örnek. Başlangıç terimleri 0, 1, –1, –2, 5 ve terimleri

…, 0, 1, –1, –2, 5, 3, –44, 101, 835, –5446, –19191, 428647, –1913560, …

olarak elde edilen (h_n) dizisinin modülo 5 deki periyotu $\pi = 16$ dır.

b_1 ve c_1, daha önce verilen simetri teoremindeki tamsayılar olmak üzere, Ward aşağıdaki teorem yardımıyla bir eliptik bölünebilir dizinin rankı ile periyodu arasındaki ilişkiyi ortaya koymuştur.

2.5.7 Teorem. (h_n) bir eliptik bölünebilir dizi ve p asal sayısı için $N_1 \geq 4$ olsun. Bu durumda

$$c_1^{\tau_1} \equiv 1 \pmod{p} \quad \text{ve} \quad (-b_1)^{\tau_1^2} \equiv 1 \pmod{p}$$

olacak şekilde bir en küçük τ_1 pozitif tamsayısı varsa, (h_n) eliptik bölünebilir dizisi modülo p de periyodiktir ve periyot $\tau_1 N_1$ dir. Bundan başka $\tau_1 \mid (p-1)$ (Ward 1948).

Ward, p tek asal sayı olmak üzere τ_1 değerinin tam olarak belirlenebildiğini aşağıdaki teoremi ile ifade etmiştir.

2.5.8 Teorem. (h_n) bir eliptik bölünebilir dizi ve p tek asal sayısı için $N_1 \geq 4$ olsun.

$$\frac{h_2}{h_{N_1-2}} \pmod p \quad \text{ve} \quad h_{N_1-1} \pmod p$$

sayılarının $\mathbb{Z}_p^*$ kümesindeki mertebeleri sırasıyla ε ve κ olsun. α sabiti,

$$\alpha = \begin{cases} 1 & \varepsilon \text{ ve } \kappa \text{ tek sayı ise} \\ -1 & \varepsilon \text{ ve } \kappa, 2 \text{ nin aynı kuvvetleri ile bölünebili yorsa} \\ 0 & \text{diğer hallerde} \end{cases}$$

olmak üzere

$$\tau_1 = 2^{\alpha} \operatorname{okek}(\varepsilon, \kappa)$$

dir (Ward 1948).

Bu teoremde p asal sayısının tek olma kısıtlaması gereklidir. Çünkü $p = 2$ olarak alınırsa $\tau_1 \mid (p-1)$ özelliği gereği $\tau_1 = 1$ olur. Ancak teorem gereği $\tau_1 = 2$ dir.

2.5.9 Örnek. Başlangıç terimleri $h_0 = 0$, $h_1 = 1$, $h_2 = 3$, $h_3 = 18$ ve $h_4 = 7$ olarak seçilen eliptik bölünebilir dizinin $p = 5$ asal sayısı için modülo 5 de indirgenmiş terimleri

…, 0, 1, 3, 3, 2, 2, 4, 0, 1, 3, 3, 2, 2, 4, 0, …

olarak elde edilir. Dikkat edilirse $N_1 = 7$ dir. Bununla birlikte,

$$\frac{h_2}{h_{N_1-2}} = 4 \ (5) \ \text{ve} \ h_{N_1-1} = 4 \ (5)$$

olarak belirlenebilir. Modülo 5 te 4 sayısının mertebesi 2 olduğundan $\varepsilon = \kappa = 2$ olarak elde edilir. Böylece $\alpha = -1$ olup $\tau_1 = 1$ dir. Dolayısıyla $\pi = \tau_1 N_1 = 7$ olarak bulunur. Eğer dizinin terimleri dikkate alınırsa periyotun 7 olduğu görülmektedir.

Yukarıda verilen dizinin, $p = 5$, 7 ve 11 asal sayıları dikkate alınarak belirlenen ε, κ, α ve τ_1 sabitleri ile rank ve periyot değerleri aşağıdaki tabloda verilmektedir.

p	N_1	ε	κ	α	τ_1	π
5	7	2	2	−1	1	7
7	4	1	3	1	6	24
11	10	10	10	−1	5	50

Ward, (h_n) eliptik bölünebilir dizisinin modülo p de rankının $N_1 = 2$ veya $N_1 = 3$ olması halinde (h_n) eliptik bölünebilir dizisinin genel terimi için aşağıdaki teoremi ifade etmiştir.

2.5.10 Teorem. (h_n) eliptik bölünebilir dizi olsun. p asal sayısının dizideki rankı $N_1 = 2$ ise,

$$h_n \equiv \begin{cases} 0 \pmod{p} & n = 2k \\ (-1)^{\frac{1}{2}k(k-1)} h_3{}^{\frac{1}{2}k(k+1)} \pmod{p} & n = 2k+1 \end{cases}$$

eğer $N_1 = 3$ ise,

$$h_n \equiv \begin{cases} 0 \pmod{p} & n = 3k \\ (-h_2)^{\frac{1}{2}k(k-1)} h_4{}^{\frac{1}{2}k(k+1)} \pmod{p} & n = 3k+1 \\ -(-h_2)^{\frac{1}{2}(k+1)(k+2)} h_4{}^{\frac{1}{2}k(k+1)} \pmod{p} & n = 3k+2 \end{cases}$$

dir (Ward 1948).

C. Swart (2003) doktora tezinde daha önce Ward ve Shipsey tarafından simetri ve periyodiklik ile ilgili modülo p de verilen bazı teoremleri modülo p^r için genişletmiştir. Teorem 2.5.4 de verilen Ward'ın simetri formülü modülo p^r ye aşağıdaki gibi genişletilmiştir.

2.5.11 Teorem. (h_n) bir eliptik bölünebilir dizi ve p asal sayısı için $N_1 \geq 4$ olsun. Bu durumda her $s, t \in \mathbb{Z}$ ve $r \in \mathbb{N}$ için

$$h_{t+sN_r} \equiv c_r{}^{st} (-b_r)^{s^2} h_t \pmod{p^r}$$

olacak şekilde b_r ve c_r tamsayıları vardır ve üstelik

$$b_r = -\left(\frac{h_{N_r-1}}{h_{-1}}\right)^2 \frac{h_{-2}}{h_{N_r-2}} \pmod{p^r} \quad \text{ve} \quad c_r = \frac{h_{N_r-1}}{h_{-1}} \frac{h_{-2}}{h_{N_r-2}} \pmod{p^r}$$

dir (Swart 2003).

Dikkat edilirse p asal sayısı h_2 terimini bölmediğinden, h_{N_r-2} terimini de bölmez. Böylece b_r ve c_r sabitleri tanımlıdır.

Swart, Teorem 2.5.7 de Ward tarafından (h_n) eliptik bölünebilir dizisinin periyodikliği ile ilgili verilen teoremi modülo p^r için aşağıdaki gibi genişletmiştir.

2.5.12 Teorem. (h_n) bir eliptik bölünebilir dizi ve p asal sayısı için $N_1 \geq 4$ olsun. Bu durumda

$$c_r^{\tau_r} \equiv 1 \pmod{p^r} \quad \text{ve} \quad (-b_r)^{\tau_r^2} \equiv 1 \pmod{p^r}$$

olacak şekilde bir en küçük τ_r pozitif tamsayısı varsa, (h_n) eliptik bölünebilir dizisi modülo p^r de periyodik ve periyodu $\tau_r N_r$ dir. Bundan başka $\tau_r \mid p^{r-1}(p-1)$ dir (Swart 2003).

2.6 Eliptik Bölünebilir Dizilerde Kare ve Küp Terimler

Eliptik bölünebilir diziler, terimleri tamsayı olan bölünebilir Lucas dizilerinin bir genellemesidir. Bu sebeple öncelikle Lucas dizilerinin kare terimlerinin belirlenmesi ile ilgili yapılan çalışmaları ele almak bu kısmın daha iyi kavranmasını sağlayacaktır. Çalışmanın bundan sonraki kısmında, bir dizinin kare terimleri "□" ve küp terimleri "*C*" simgeleri ile gösterilecektir.

P ve Q sıfırdan farklı aralarında asal tamsayılar ve $U_0 = 0$, $U_1 = 1$ olmak üzere $n \geq 2$ için $\{U_n(P, Q)\}$ *Lucas dizisi*,

$$U_n = PU_{n-1} - QU_{n-2}$$

rekurrent bağıntısı ile tanımlanır. Birçok matematikçi hangi özellikteki P ve Q tamsayılarından elde edilen $U_n(P, Q)$ teriminin □ veya C olabileceği sorusuna cevap aramıştır.

İlk olarak T. N. Shorey ve R. Tijdeman (1986), $\{U_n(P, Q)\}$ Lucas dizisinde sonlu tane □ terim bulunabileceğini göstermiştir.

P. Ribenboim ve W. L. McDaniel (1996), öncelikle P ve Q tek tamsayı ve $P^2 - 4Q > 0$ olmak üzere $n = 0, 1, 2, 3, 6, 12$ için $U_n =$ □ olduğunu göstermiştir. Ardından daha sonra ki çalışmalarında şu sonuçları elde etmişlerdir:

1. P çift tamsayı ve $Q \equiv 1 \pmod 4$ olmak üzere $n > 0$ için n bir □ veya bir kare sayının iki katı ise $U_n(P, Q) =$ □ dir ve bununla birlikte n doğal sayısının tüm asal çarpanları $P^2 - 4Q$ ifadesini böler.
2. $p^{2t} \mid n$ özelliğindeki p asalı ve $u = 1, \ldots, t$ için $U_{p^{2u}} =$ □ dir.
3. Eğer n çift tamsayı ve P sayısı □ veya bir kare sayının iki katı ise $U_n =$ □ dir.
4. $U_{p^2} =$ □ olacak şekilde P, Q tamsayı çifti ve p tek asalı yoktur.

A. Bremner ve N. Tzanakis (2004), yukarıda Ribenboim ve McDaniel tarafından verilmiş olan sonuçları genelleştirerek $n = 2, 3, 6, 12$ için $U_n = (P, Q)$ terimlerini $a, b \in \mathbb{Z}$ olmak üzere aşağıdaki gibi belirlemişlerdir:

i. $U_2 =$ □ $\Leftrightarrow P = a^2$

ii. $U_3 =$ □ $\Leftrightarrow P = a^2, Q = a^2 - b^2$

iii. $U_6 =$ □ $\Leftrightarrow P = 3a^2b^2,\ Q = \dfrac{-a^8 + 12a^4b^4 - 9b^8}{2}$

iv. $U_{12} =$ □ $\Leftrightarrow (P, Q) = (1, -1)$

Dolayısıyla, bu sonuçlardan 12. terimi □ olan tek Lucas dizisinin Fibonacci dizisi olduğu ve bundan başka

$$U_9 = \square \Leftrightarrow (P, Q) = (\pm 2, 1)$$

ve böylece 9. terimi □ olan dizilerin $U_n = n$ ve $U_{n-1} = (-1)^{n+1}$ özelliğindeki diziler olduğu sonucunu elde etmişlerdir. Bremner ve Tzanakis tarafından verilen diğer sonuçlar şu şekildedir: $Q = 1$ ise $P \neq \pm 1, \pm 2$ olmak üzere P ve Q sıfırdan farklı aralarında asal tamsayılar olsun. Bu durumda,

i. $n = 2, \ldots, 7$ ise sonsuz çoklukta (P, Q) tamsayı çifti için $U_n(P, Q) =$ □ dir.

ii. $n = 8, \ldots, 12$ ise $U_n(P, Q) =$ □ olacak şekildeki terimler sadece $U_8(1, -4) = 21^2$, $U_8(4, -17) = 620^2$ ve $U_{12}(1, -1) = 12^2$ dir.

Gezer (2013), Tate normal formdaki eliptik eğriler ile eşleşen sıfır terim bulunduran eliptik bölünebilir dizilerin genel terimlerini belirleyerek bu dizilerin tüm kare ve küp terimlerinin neler olduğunu belirlemiştir.

$N \in \{4, \ldots, 10, 12\}$ olmak üzere N. terimi sıfır olan eliptik bölünebilir (h_n) dizisinin genel terimleri aşağıdaki gibidir (Gezer 2013):

1. $N = 4$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,5,6 \pmod 8 \\ -1 & n \equiv 2,3,7 \pmod 8 \end{cases} \qquad p = \begin{cases} 3 & n \equiv 1,3 \pmod 4 \\ 4 & n \equiv 2 \pmod 4 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\left\{(3n^2-p)/8\right\}},$$

2. $N = 5$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,7,8 \pmod{10} \\ -1 & n \equiv 2,3,6,9 \pmod{10} \end{cases} \qquad p = \begin{cases} 2 & n \equiv 1,4 \pmod 5 \\ 3 & n \equiv 2,3 \pmod 5 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\left\{(2n^2-p)/5\right\}},$$

3. $N = 6$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,5,9,10 \pmod{12} \\ -1 & n \equiv 2,3,7,8,11 \pmod{12} \end{cases} \qquad p = \begin{cases} 5 & n \equiv 1,5 \pmod 6 \\ 8 & n \equiv 2,4 \pmod 6 \\ 9 & n \equiv 9 \pmod 6 \end{cases}$$

$$k = \begin{cases} +1 & n \equiv 1,2,4,5 \pmod 6 \\ 0 & n \equiv 3 \pmod 6 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(5n^2-p)/12\}}(\alpha+1)^{\{(n^2-k)/3\}},$$

4. $N = 7$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,5 \pmod 7 \\ -1 & n \equiv 2,3,6 \pmod 7 \end{cases} \qquad p = \begin{cases} 5 & n \equiv 1,6 \pmod 7 \\ 6 & n \equiv 2,5 \pmod 7 \\ 3 & n \equiv 3,4 \pmod 7 \end{cases}$$

$$q = \begin{cases} 3 & n \equiv 1,6 \pmod 7 \\ 5 & n \equiv 2,5 \pmod 7 \\ 6 & n \equiv 3,4 \pmod 7 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(5n^2-p)/7\}}(\alpha-1)^{\{(3n^2-q)/7\}},$$

5. $N = 8$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,5,9,10,13,14 \pmod{16} \\ -1 & n \equiv 2,3,6,7,11,12,15 \pmod{16} \end{cases}$$

$$p = \begin{cases} 15 & n \equiv 1,7 \pmod 8 \\ 12 & n \equiv 2,6 \pmod 8 \\ 7 & n \equiv 3,5 \pmod 8 \\ 16 & n \equiv 4 \pmod 8 \end{cases} \qquad q = \begin{cases} 7 & n \equiv 1,7 \pmod 8 \\ 12 & n \equiv 2,6 \pmod 8 \\ 15 & n \equiv 3,5 \pmod 8 \\ 16 & n \equiv 4 \pmod 8 \end{cases}$$

$$k = \begin{cases} 3 & n \equiv 1,3,5,7 \pmod 8 \\ 4 & n \equiv 2,6 \pmod 8 \\ 0 & n \equiv 4 \pmod 8 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(15n^2-p)/16\}}(\alpha-1)^{\{(7n^2-q)/16\}}(2\alpha-1)^{\{(3n^2-k)/8\}},$$

6. $N = 9$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,5,8,11,12,15,16 \pmod{18} \\ -1 & n \equiv 2,3,6,7,10,13,14,17 \pmod{18} \end{cases}$$

$$p = \begin{cases} 7 & n \equiv 1,8 \pmod 9 \\ 10 & n \equiv 2,7 \pmod 9 \\ 9 & n \equiv 3,6 \pmod 9 \\ 4 & n \equiv 4,5 \pmod 9 \end{cases} \qquad q = \begin{cases} 4 & n \equiv 1,8 \pmod 9 \\ 7 & n \equiv 2,7 \pmod 9 \\ 9 & n \equiv 3,6 \pmod 9 \\ 10 & n \equiv 4,5 \pmod 9 \end{cases}$$

$$k = \begin{cases} 0 & n \equiv 3,6 \pmod 9 \\ 1 & n \equiv 0,1,2,4,5,7,8 \pmod 9 \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(7n^2-p)/9\}}(\alpha-1)^{\{(4n^2-q)/9\}}(\alpha^2-\alpha+1)^{\{(n^2-k)/3\}},$$

7. $N = 10$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,4,5,8,9,13,14,17,18 \pmod{20} \\ -1 & n \equiv 2,3,6,7,11,12,15,16,19 \pmod{20} \end{cases}$$

$$p = \begin{cases} 21 & n \equiv 1,9 \pmod{10} \\ 24 & n \equiv 2,8 \pmod{10} \\ 9 & n \equiv 3,7 \pmod{10} \\ 16 & n \equiv 4,6 \pmod{10} \\ 25 & n \equiv 5 \pmod{10} \end{cases} \qquad q = \begin{cases} 9 & n \equiv 1,9 \pmod{10} \\ 16 & n \equiv 2,8 \pmod{10} \\ 21 & n \equiv 3,7 \pmod{10} \\ 24 & n \equiv 4,6 \pmod{10} \\ 25 & n \equiv 5 \pmod{10} \end{cases}$$

$$k = \begin{cases} 2 & n \equiv 1,4,6,9 \pmod{10} \\ 3 & n \equiv 2,3,7,8 \pmod{10} \\ 0 & n \equiv 5 \pmod{10} \end{cases} \qquad s = \begin{cases} 5 & n \equiv 1,3,5,7,9 \pmod{10} \\ 4 & n \equiv 2,4,6,8 \pmod{10} \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(21n^2-p)/20\}}(\alpha-1)^{\{(9n^2-q)/20\}}(2\alpha-1)^{\{(2n^2-k)/5\}}\left[(\alpha-1)(2\alpha-1)\right]^{\{(5n^2-s)/4\}},$$

8. $N = 12$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 1,5,9,13,14,16,17,18,20,21,22 \pmod{24} \\ -1 & n \equiv 2,3,4,6,7,8,10,11,15,19,23 \pmod{24} \end{cases}$$

$$p = \begin{cases} 1 & n \equiv 1,11 \pmod{12} \\ 4 & n \equiv 2,10 \pmod{12} \\ 9 & n \equiv 3,9 \pmod{12} \\ 16 & n \equiv 4,8 \pmod{12} \\ 13 & n \equiv 5,7 \pmod{12} \\ 12 & n \equiv 6 \pmod{12} \end{cases} \qquad q = \begin{cases} 59 & n \equiv 1,11 \pmod{12} \\ 44 & n \equiv 2,10 \pmod{12} \\ 51 & n \equiv 3,9 \pmod{12} \\ 56 & n \equiv 4,8 \pmod{12} \\ 35 & n \equiv 5,7 \pmod{12} \\ 60 & n \equiv 6 \pmod{12} \end{cases}$$

$$k = \begin{cases} 1 & n \equiv 1,5,7,11 \pmod{12} \\ 4 & n \equiv 2,10 \pmod{12} \\ 9 & n \equiv 3,9 \pmod{12} \\ 16 & n \equiv 4,8 \pmod{12} \\ 12 & n \equiv 6 \pmod{12} \end{cases}$$

$$s = \begin{cases} 3 & n \equiv 1,3,5,7,9,11 \pmod{12} \\ 4 & n \equiv 2,6,10 \pmod{12} \\ 0 & n \equiv 4,8 \pmod{12} \end{cases} \qquad t = \begin{cases} 1 & n \equiv 1,2,4,5,7,8,10,11 \pmod{12} \\ 0 & n \equiv 3,6,9 \pmod{12} \end{cases}$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(n^2-p)/12\}}(\alpha-1)^{\{(59n^2-q)/24\}}(2\alpha-1)^{\{(n^2-k)/24\}} \times((3\alpha^2-3\alpha+1)(\alpha-2\alpha^2))^{\{(3n^2-s)/8\}}(2\alpha-2\alpha^2-1)^{\{(n^2-t)/3\}}$$

dir.

$N \in \{4, \ldots, 10, 12\}$ olmak üzere N. terimi sıfır olan eliptik bölünebilir (h_n) dizisinin kare ve küp terimleri ise aşağıdaki gibi belirlenmiştir:

***N* = 4 Hali.**

2.6.1 Teorem. (h_n), her $n \equiv 0 \pmod 4$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,7 \pmod 8$ ise her $\alpha \neq 0$ için $h_n =$ □ dir.

ii. $\alpha = \square \Leftrightarrow$ her $n \geq 0$ için $h_n = \square$ dir.

2. *i.* $n \equiv 1,3,5,7 \pmod 8$ ise her $\alpha \neq 0$ için $h_n = C$ dir.

ii. $\alpha = C \Leftrightarrow$ her $n \geq 0$ için $h_n = C$ dir (Gezer 2013).

***N* = 5 Hali.**

2.6.2 Teorem. (h_n), her $n \equiv 0 \pmod 5$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,4,6,9 \pmod{10}$ ise her $\alpha \neq 0$ için $h_n = \square$ dir.

ii. $\alpha = \square \Leftrightarrow$ her $n \geq 0$ için $h_n = \square$ dir.

2. *i.* $n \equiv 1,3,4,11,12,14 \pmod{15}$ ise her $\alpha \neq 0$ için $h_n = C$ dir.

ii. $\alpha = C \Leftrightarrow$ her $n \geq 0$ için $h_n = C$ dir (Gezer 2013).

***N* = 6 Hali.**

2.6.3 Teorem. (h_n), her $n \equiv 0 \pmod 6$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,5,7,11 \pmod{12}$ ise her $\alpha \neq -1,0$ için $h_n = \square$ dir.

ii. $n \equiv 4,8 \pmod{12}$ ise $h_n = \square \Leftrightarrow \alpha + 1 = \square$ dir.

iii. Diğer hallerde, her $\alpha \neq -1,0$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,3,9,15,17 \pmod{18}$ ise her $\alpha \neq -1,0$ için $h_n = C$ dir.

ii. $n \equiv 4,14 \pmod{18}$ ise $h_n = C \Leftrightarrow \alpha + 1 = C$ dir.

iii. $n \equiv 8,10 \pmod{18}$ ise $h_n = C \Leftrightarrow \alpha = C$ dir.

iv. Diğer hallerde, her $\alpha \neq -1,0$ için $h_n \neq C$ dir (Gezer 2013).

***N* = 7 Hali.**

2.6.4 Teorem. (h_n), her $n \equiv 0 \pmod 7$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,13 \pmod{14}$ ise her $\alpha \neq 0,1$ için $h_n = \square$ dir.

ii. $n \equiv 2,3,11,12 \pmod{14}$ ise $h_n = \square \Leftrightarrow \alpha - 1 = \square$ dir.

iii. $n \equiv 4,5,9,10 \pmod{14}$ ise $h_n = \square \Leftrightarrow \alpha = \square$ dir.

iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,3,8,13,18,20 \pmod{21}$ ise her $\alpha \neq 0,1$ için $h_n = C$ dir.

ii. $n \equiv 4,6,10,11,15,17 \pmod{21}$ ise $h_n = C \Leftrightarrow \alpha = C$ dir.

iii. $n \equiv 9,12 \pmod{21}$ ise $h_n = C \Leftrightarrow \alpha - 1 = C$ dir.

iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq C$ dir (Gezer 2013).

***N* = 8 Hali.**

2.6.5 Teorem. (h_n), her $n \equiv 0 \pmod 8$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,4,12,15 \pmod{16}$ ise her $\alpha \neq 0,1$ için $h_n = \square$ dir.

ii. $n \equiv 3,13 \pmod{16}$ ise $h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1) = \square$ dir.

iii. $n \equiv 5,11 \pmod{16}$ ise $h_n = \square \Leftrightarrow \alpha(2\alpha - 1) = \square$ dir.

iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,7,17,23 \pmod{24}$ ise her $\alpha \neq 0,1$ için $h_n = C$ dir.

ii. $n \equiv 3,4,20,21 \pmod{24}$ ise $h_n = C \Leftrightarrow \alpha = C$ dir.

iii. $n \equiv 6,18 \pmod{24}$ ise $h_n = C \Leftrightarrow 2\alpha - 1 = C$ dir.

iv. $n \equiv 9,15 \pmod{24}$ ise $h_n = C \Leftrightarrow \alpha - 1 = C$ dir.

v. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq C$ dir (Gezer 2013).

***N* = 9 Hali.**

2.6.6 Teorem. (h_n), her $n \equiv 0 \pmod 9$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,17 \pmod{18}$ ise her $\alpha \neq 0,1$ için $h_n = \square$ dir.

ii. $n \equiv 5,13 \pmod{18}$ ise $h_n = \square \Leftrightarrow \alpha = \square$ dir.

iii. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,3,6,12,15,21,24,26 \pmod{27}$ ise her $\alpha \neq 0,1$ için $h_n = C$ dir.

ii. $n \equiv 4,23 \pmod{27}$ ise $h_n = C \Leftrightarrow (\alpha^2 - \alpha + 1)^2 = C$ dir.

iii. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq C$ dir (Gezer 2013).

N = 10 Hali.

2.6.7 Teorem. (h_n), her $n \equiv 0 \pmod{10}$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,9,11,19 \pmod{20}$ ise her $\alpha \neq 0,1$ için $h_n = \square$ dir.

   ii. $n \equiv 4,16 \pmod{20}$ ise $h_n = \square \Leftrightarrow -\alpha^2 + 3\alpha - 1 = \square$ dir.

   iii. $n \equiv 5,15 \pmod{20}$ ise $h_n = \square \Leftrightarrow \alpha = \square$ dir.

   iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,11,19,29 \pmod{30}$ ise $h_n = C$ dir.

   ii. $n \equiv 3,27 \pmod{30}$ ise $h_n = C \Leftrightarrow -\alpha^2 + 3\alpha - 1 = C$ dir.

   iii. $n \equiv 7,13,17,23 \pmod{30}$ ise $h_n = C \Leftrightarrow 2\alpha - 1 = C$ dir.

   iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq C$ dir (Gezer 2013).

N = 12 Hali.

2.6.8 Teorem. (h_n), her $n \equiv 0 \pmod{12}$ için $h_n = 0$ olacak şekilde eliptik bölünebilir dizi olsun. Bu durumda,

1. *i.* $n \equiv 1,23 \pmod{24}$ ise her $\alpha \neq 0,1$ için $h_n = \square$ dir.

   ii. $n \equiv 5,19 \pmod{24}$ ise $h_n = \square \Leftrightarrow 3\alpha^2 - 3\alpha + 1 = \square$ dir.

   iii. $n \equiv 4,8,16,20 \pmod{24}$ ise $h_n = \square \Leftrightarrow \alpha = -3$ dür.

   iv. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq \square$ dir.

2. *i.* $n \equiv 1,35 \pmod{36}$ ise her $\alpha \neq 0,1$ için $h_n = C$ dir.

   ii. $n \equiv 3,9,15,21,27,33 \pmod{36}$ ise $h_n = C \Leftrightarrow \alpha - 1 = C$ dir.

   iii. Diğer hallerde, her $\alpha \neq 0,1$ için $h_n \neq C$ dir (Gezer 2013).

2.6.9 Örnek. N = 12 hali için α = 2 olarak seçilmesi durumunda elde edilen Tate normal formdaki

$$E : y^2 + 43xy - 210y = x^3 - 210x^2$$

eliptik eğrisi ile eşleşen eliptik bölünebilir dizinin n = 20, …, 35 için elde edilen terimleri aşağıdaki gibidir:

$$h_{20} = 2^{182}\,3^{166}\,5^{133}\,7^{150}$$
$$h_{21} = 2^{201}\,3^{183}\,5^{147}\,7^{165}$$
$$h_{22} = 2^{221}\,3^{201}\,5^{161}\,7^{181}$$
$$h_{23} = -2^{242}\,3^{220}\,5^{176}\,7^{198}$$
$$h_{24} = 0$$
$$h_{25} = 2^{286}\,3^{260}\,5^{208}\,7^{234}$$
$$h_{26} = -2^{309}\,3^{281}\,5^{225}\,7^{253}$$
$$h_{27} = -2^{333}\,3^{303}\,5^{243}\,7^{273}$$
$$h_{28} = -2^{358}\,3^{326}\,5^{261}\,7^{294}$$
$$h_{29} = 2^{384}\,3^{350}\,5^{280}\,7^{315}$$
$$h_{30} = -2^{411}\,3^{375}\,5^{300}\,7^{337}$$
$$h_{31} = -2^{439}\,3^{400}\,5^{320}\,7^{360}$$
$$h_{32} = -2^{468}\,3^{426}\,5^{341}\,7^{384}$$
$$h_{33} = 2^{498}\,3^{453}\,5^{363}\,7^{408}$$
$$h_{34} = -2^{529}\,3^{481}\,5^{385}\,7^{433}$$
$$h_{35} = -2^{561}\,3^{510}\,5^{408}\,7^{459}$$

Dikkat edilirse α = 2 için $3\alpha^2 - 3\alpha + 1$ ifadesi bir tam kare sayı belirtmediğinden dizinin sadece $n \equiv 1, 23 \pmod{24}$ özelliğindeki

$$h_{23} = -2^{242}\,3^{220}\,5^{176}\,7^{198} \text{ ve } h_{25} = 2^{286}\,3^{260}\,5^{208}\,7^{234}$$

terimleri birer tam kare sayıdır. Diğer yandan $n \equiv 1, 35 \pmod{36}$ özelliğindeki terimlerden biri olan $h_{35} = -2^{561}\,3^{510}\,5^{408}\,7^{459}$ terimi de bir küp sayıdır. Bununla birlikte $\alpha = 2$ için $\alpha - 1$ ifadesi bir küp sayı olduğundan Teorem 2.6.8 de belirtildiği gibi

$$h_{21} = 2^{201}\,3^{183}\,5^{147}\,7^{165},\ h_{27} = -2^{333}\,3^{303}\,5^{243}\,7^{273},\ h_{33} = 2^{498}\,3^{453}\,5^{363}\,7^{408}$$

terimleri birer küp sayıdır.

3. BÖLÜM

SOMOS DİZİLERİ ve BU DİZİLERİN TAMSAYI OLMA ÖZELLİĞİ

Bu bölümde Somos dizileri ele alınacaktır. Kısım 3.1 de genel olarak Somos dizilerinin tanımı verilecek ve ardından çalışmanın da temelini oluşturan Somos 4 dizileri ile ilgili bazı temel kavramların üzerinde durulacaktır. Kısım 3.2 de modülo p^r de indirgenmiş olan Somos 4 dizileri incelenecektir. Kısım 3.3 de Somos 4 dizilerinde periyodiklik kavramı açıklanacak ve Robinson'un Somos(4) dizileri için verdiği konjektürler ele alınacaktır. Kısım 3.4 de Somos 4 dizileri ile eliptik eğriler arasındaki ilişkiler incelenecektir. Kısım 3.5 de Tate normal formdaki eliptik eğriler ile eşleşen Somos 4 dizilerinin genel terimleri verilecek ve bu genel terim formülleri yardımıyla bu dizilerin tüm terimlerinin tamsayı olduğu gösterilecektir. Kısım 3.6 da ise Tate normal formdaki eliptik eğriler ile eşleşen Somos 4 dizilerinin terimlerinden hangilerinin bir tam kare veya tam küp oldukları belirlenecektir.

3.1 Somos Dizileri

3.1.1 Tanım. (h_n) bir rasyonel sayı dizisi olsun. Eğer (h_n) dizisi, $k,\ n \in \mathbb{Z},\ k \geq 4$ ve $i = 1,2,...,\left\lfloor \frac{k}{2} \right\rfloor$ için $\lambda_i \in \mathbb{Q}$ olmak üzere

$$h_n h_{n-k} = \sum_{i=1}^{\left\lfloor \frac{k}{2} \right\rfloor} \lambda_i h_{n-i} h_{n-k+i}$$

bağıntısını gerçekliyor ise (h_n) dizisine katsayıları λ_i ve başlangıç terimleri $h_0, h_1, ..., h_{k-1}$ olan bir *Somos k dizisi* denir. Özel olarak tüm katsayıları ve başlangıç terimleri 1 olan (h_n) Somos dizisi Somos(k) ile gösterilir.

Çalışmanın temeli Somos 4 dizileri üzerine olduğundan ilk olarak bu dizilerin genel özellikleri üzerinde durulacaktır.

Mertebesi iki olan bir lineer bağıntıdan elde edilen tüm rasyonel diziler birer Somos 4 dizisi belirtirler. Örneğin A ve B rasyonel katsayılar olmak üzere her n tamsayısı için

$$h_{n+1} = Ah_n + Bh_{n-1}$$

lineer bağıntısı yardımıyla elde edilen (h_n) dizisi dikkate alındığında,

$$h_{n+2}h_{n-2} = (Ah_{n+1} + Bh_n)\left(\frac{h_n - Ah_{n-1}}{B}\right)$$

$$= (h_{n+1} - Bh_{n-1})\frac{A}{B}h_n - \frac{A^2}{B}h_{n+1}h_{n-1} + {h_n}^2$$

$$= (Ah_n)\frac{A}{B}h_n - \frac{A^2}{B}h_{n+1}h_{n-1} + {h_n}^2$$

$$= -\frac{A^2}{B}h_{n+1}h_{n-1} + \left(\frac{A^2}{B} + 1\right){h_n}^2$$

olacak şekilde düzenleme yapılabilir ve böylece

$$\lambda_1 = -\frac{A^2}{B} \text{ ve } \lambda_2 = -\lambda_1 + 1$$

katsayıları ile beraber (h_n) bir Somos 4 dizisi belirtir. Bundan başka

$$F_{n+1} = F_n + F_{n-1}$$

lineer bağıntısı ile tanımlanan Fibonacci dizisi, katsayıları $\lambda_1 = -1$ ve $\lambda_2 = 2$ olan bir Somos 4 dizisi,

$$M_n = 2^n - 1 = 3M_{n-1} - 2M_{n-2}$$

lineer bağıntısı ile tanımlanan Mersenne dizisi de katsayıları $\lambda_1 = \frac{9}{2}$ ve $\lambda_2 = -\frac{7}{2}$ olan bir Somos 4 dizisi belirtirler.

Diğer yandan her bir Somos 4 dizisi bir lineer bağıntı gerçeklemek zorunda değildir, bununla birlikte, (h_n) Somos 4 dizisinin $A, B \in \mathbb{Q}$ olmak üzere mertebesi iki olan

$$h_{n+1} = Ah_n + Bh_{n-1}$$

lineer bağıntısını gerçeklemesi için gerek ve yeter şart katsayıların

$$A = \frac{h_0 h_3 - h_1 h_2}{h_0 h_2 - {h_1}^2} \quad \text{ve} \quad B = \frac{{h_2}^2 - h_1 h_3}{h_0 h_2 - {h_1}^2}$$

olarak seçilmesidir.

3.1.2 Tanım. $t \in \mathbb{Z}$ ve (h_n) bir Somos 4 dizisi olmak üzere

$$l_n = h_{n+t}$$

olarak tanımlanan (l_n) Somos 4 dizisine, (h_n) dizisinin bir *t-kayması* denir.

3.1.3 Örnek 1. Somos(4) dizisinin terimleri

…, 314, 59, 23, 7, 3, 2, 1, 1, 1, 1, 2, 3, 7, 23, 59, 314, 1529, 8209, …

şeklindedir.

2. Başlangıç terimleri 1, 2, 5, 8 ve katsayıları $\lambda_1 = 3$ ve $\lambda_2 = 2$ olan

$$1, 2, 5, 8, 98, 799, \frac{38384}{5}, \frac{8834453}{20}, \frac{2401378997}{200}, \frac{1834494860211}{1000}, \ldots$$

Somos 4 dizisinin hiçbir terimi sıfır olmadığından, bu dizi ve bu dizinin herhangi bir kayması bir eliptik dizi denklemini gerçeklemez.

3.1.4 Teorem. (h_n) ve (h_n') Somos 4 dizilerinin denk dizi olması için gerek ve yeter şart $D \in \mathbb{Q}$ olmak üzere her $n \in \mathbb{Z}$ için

$$h_n' = \alpha^{n^2} \beta^n \gamma\, h_n$$

olacak şekilde $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{D})$ sayılarının var olmasıdır. Buna göre, (h_n) Somos 4 dizisinin

…, 1, 1, 1, …

sabit dizisine denk olması için gerek ve yeter şart

$$\frac{h_{-2}h_0}{h_{-1}^{\,2}} = \frac{h_{-1}h_1}{h_0^{\,2}} = \frac{h_0h_2}{h_1^{\,2}}$$

eşitliğinin gerçeklenmesidir (Swart 2003).

3.1.5 Tanım. p bir asal sayı olsun. Eğer (h_n) Somos 4 dizisinin tüm terim ve katsayılarının paydasındaki tamsayılar p ile aralarında asal ise p asal sayısına (h_n) Somos 4 dizisi için *kabul edilebilir asal sayı* denir.

Swart doktora tezinde aşağıda verilecek olan teoremi ifade ve ispat ederek Somos 4 dizileri için kabul edilebilir olmayan asal sayıların hangi özellikte olduklarını belirlemiştir.

3.1.6 Teorem. (h_n) bir Somos 4 dizisi ve p, (h_n) Somos 4 dizisi için kabul edilebilir olmayan asal sayı olsun. Bu durumda p asalı ya λ_1 ve λ_2 katsayılarından birinin paydasını böler ya da indis kümesinden seçilen herhangi $t \in \mathbb{Z}$ için $h_t, h_{t+1}, h_{t+2}, h_{t+3}$ terimlerinden birinin pay ya da paydasından birini böler (Swart 2003).

Örneğin, başlangıç terimleri 2, 3, 5, 7 ve katsayıları $\lambda_1 = 2,\ \lambda_2 = 8$ olan Somos 4 dizisi

$$2, 3, 5, 7, 121, 534, \frac{124604}{5}, \frac{41560408}{5.7}, \frac{9019812896}{5^2.7}, \frac{158849002341504}{5^3.7^2}, \ldots$$

olarak elde edilir. Böylece bu dizi için kabul edilebilir olmayan asal sayılar 5 ve 7 olarak belirlenir.

3.2 Modülo p^r de İndirgenmiş Somos 4 Dizileri

Bu kısımda Somos 4 dizilerinin modülo p^r deki özellikleri üzerinde durulacaktır. İlk olarak daha önce eliptik bölünebilir diziler için modülo p de verilen rank tanımı Somos 4 dizileri için modülo p^r de aşağıdaki gibi yeniden düzenlenebilir.

3.2.1 Tanım. (h_n) Somos 4 dizisinin belli bir h_k terimini bölen p^r kabul edilebilir sayısı için,

$$h_n \equiv 0 \pmod{p^r} \iff n \equiv k \pmod{N}$$

olacak şekilde N pozitif tamsayısı var ve üstelik N sayısı bu özellikteki en küçük sayı ise bu N sayısına p^r sayısının (h_n) dizisindeki *rankı* denir. Genel olarak p^r sayısının (h_n) dizisindeki rankı N_r ile gösterilir.

3.2.2 Örnek. Katsayıları $\lambda_1 = 1,\ \lambda_2 = 2$ ve başlangıç terimleri 3, 3, 3, 3 olan Somos 4 dizisinin modülo 5 te terimleri

…, 0, 4, 3, 3, 3, 3, 4, 0, 4, 2, 3, 2, 3, 1, 0, 1, 2, 2, 2, 2, 1, 0, 1, 3, 2, 3, 2, 4,
0, 4, 3, 3, 3, 3, 4, 0, …

biçimindedir. Böylece elde edilen Somos 4 dizisinin modülo 5 te rankı $N_1 = 7$ dir.

3.2.3 Teorem. (h_n), katsayıları λ_1, λ_2 olan Somos 4 dizisi olmak üzere bu dizinin kabul edilebilir p asal sayısı dizinin en az iki terimini bölsün ve üstelik N, belli k indisi için $p \mid h_k$ ve $p \mid h_{k+N}$ olacak şekildeki en küçük pozitif tamsayı olsun. Bu durumda,

1. $N = 1$ ise ya p asal sayısı dizinin tüm terimlerini böler ya da $p \mid \lambda_2$ dir.

2. $N = 2$ ise p asal sayısı λ_1 katsayısını böler ancak λ_2 katsayısını bölmez ve p asal sayısı için rank 2 dir.

3. $N = 3$ ise p asal sayısı λ_2 katsayısını böler ancak λ_1 katsayısını bölmez ve p asal sayısı için rank 3 tür.

4. $N \geq 4$ ise p asal sayısı λ_1 ve λ_2 katsayılarını bölmez (Swart 2003).

3.3 Somos 4 Dizilerinde Periyodiklik

3.3.1 Tanım. (h_n) bir Somos 4 dizisi olsun. $h_t, h_{t+1}, h_{t+2}, h_{t+3}$ terimleri ile aralarında asal olan belli kabul edilebilir p asal sayısı ve belli s, t indisleri için $j = 0, 1, 2, 3$ olmak üzere

$$h_{t+j} \equiv h_{s+j} \pmod{p^r}$$

denkliği gerçekleniyor ise (h_n) Somos 4 dizisi modülo p^r de *periyodiktir* denir.

Eğer (h_n) Somos 4 dizisi modülo p^r de periyodik ise dizinin periyodu $t-s$ sayısını böler.

3.3.2 Örnek. Katsayıları $\lambda_1 = 1,\ \lambda_2 = 2$ ve başlangıç terimleri 3, 3, 3, 3 olan Somos 4 dizisinin modülo 5 te terimleri

…, 0, 4, 3, 3, 3, 3, 4, 0, 4, 2, 3, 2, 3, 1, 0, 1, 2, 2, 2, 2, 1, 0, 1, 3, 2, 3, 2, 4,
0, 4, 3, 3, 3, 3, 4, 0, …

biçimindedir. Böylece modülo 5 te periyot $\pi_1 = 28$ olarak elde edilir.

Swart doktora tezinde rankı 4 ten büyük olan Somos 4 dizilerinin periyodikliği ile ilgili aşağıdaki teoremi ifade ve ispat etmiştir.

3.3.3 Teorem. (h_n), en çok bir tane terimi sıfır olan bir Somos 4 dizisi ve p, p sayısının herhangi iki katı arasında (h_n) dizisinin p ile aralarında asal olan en az dört terimi var olacak şekildeki bir kabul edilebilir asal sayı olsun. Bu durumda her $r \in \mathbb{N}$ için (h_n) Somos 4 dizisi modülo p^r de periyodiktir (Swart 2003).

Robinson (1992), Somos(4) dizileri için bazı konjektürler vermiş ve ardından Swart bu konjektürlerin bazılarının ispatlarını da içeren teoremleri ifade ve ispat etmiştir.

Robinson tarafından verilmiş olan ilk konjektürler, Somos(4) dizisinin rankı ile ilgili olan konjektürlerdir.

3.3.4 Konjektür. p tek asal sayısı Somos(4) dizisinin belli bir terimini bölüyor ise her $r \in \mathbb{N}$ için p^r sayısı bu dizinin belli bir terimini böler (Robinson 1992).

Burada p asal sayısının tek olma kısıtlaması gereklidir, bu koşul kaldırılamaz bir koşuldur. Örneğin (h_n) bir Somos(4) dizisi ise $2 \mid h_5$ olduğu halde (h_n) dizisinin 4 ile bölünebilen hiçbir terimi yoktur. Swart, tezinde bu konjektürü Somos 4 dizileri için aşağıdaki şekilde ifade ve ispat etmiştir. Ancak konjektür, halen Somos(4) dizisi için ispatlanabilmiş değildir.

3.3.5 Teorem. (h_n) bir Somos 4 dizisi ve p, $\lambda_1\lambda_2$ ile aralarında asal olan ve dizinin tüm terimlerini değil sadece belli bir terimini bölen kabul edilebilir tek asal sayı olsun. Bu durumda ya (h_n) dizisinde p asalının tüm katları p sayısının tam olarak aynı kuvveti ile bölünür ya da (h_n) dizisinin belli bir terimi her $r \in \mathbb{N}$ için p^r ile bölünür (Swart 2003).

3.3.6 Konjektür. Somos(4) dizisinin belli bir terimini bölen her asal kuvvet Somos(4) dizisinde düzgündür, yani bu asal kuvvet için dizinin rankı mevcuttur (Robinson 1992).

Örneğin, Somos(4) dizisindeki her bir 17. terim 11 asal sayısı ile bölünebilir.

3.3.7 Teorem. (h_n) başlangıç terimleri sıfırdan farklı olan bir Somos 4 dizisi ve p, dizinin en az iki terimini bölen kabul edilebilir bir asal sayı olsun. Bu durumda p asalının düzgün asal olmaması için gerek ve yeter şart p sayısının dizinin tüm terimlerini değil ancak belli ardışık iki terimini bölmesidir. Ayrıca bu halde $p|\lambda_2$ olur (Swart 2003).

Eğer p, $\lambda_1\lambda_2$ ile aralarında asal ise (h_n) dizisinin belli bir terimini bölen p sayısının her bir kuvvetinin (h_n) dizisinde düzgün olduğu gösterilmiştir. Somos(4) dizisi için $\lambda_1 = \lambda_2 = 1$ olduğundan bu teorem ile ikinci konjektürün ispatı verilmiş olur. Diğer yandan p, $\lambda_1\lambda_2$ sayısını bölen bir düzgün asal sayı ve p^r, (h_n) dizisinin belli bir terimini bölüyor ise p^r sayısının da düzgün olduğu henüz ispatlanmış değildir.

Aşağıdaki konjektür, dizinin rankı ile düzgün asal sayı arasındaki ilişkiyi ortaya koymaktadır.

3.3.8 Konjektür. p, Somos(4) dizisinde rankı N_1 olan düzgün asal sayı ise N_1 sayısının belli bir katı p asalına çok yakındır (Robinson 1992).

Robinson, Somos(4) dizisinin belli bir terimini bölen her bir $p < 2000$ asalının rankının $N_1 < 1.1p + 6$ olduğunu bulmuştur.

3.3.9 Teorem. (h_n) bir Somos 4 dizisi ve p, (h_n) dizisinde rankı N_1 olan düzgün asal olsun. Bu durumda

$$N_1 \leq p + 1 - 2\sqrt{p}$$

olur (Swart 2003).

Swart tarafından elde edilmiş olan bu sınır Robinson tarafından verilmiş olan $N_1 < 1.1p + 6$ sınırından daha iyi bir sınırdır.

3.3.10 Konjektür. p, Somos(4) dizisinde rankı N_1 olan bir tek asal ve p^w, p asal sayısının Somos(4) dizisinde p nin tüm katlarını bölen en büyük asal kuvvet olsun. Eğer $r > w$ için p^r sayısı Somos(4) dizisinde herhangi bir terimi bölüyorsa dizinin rankı

$$N_r = p^{r-w} N_1$$

ve $r \leq w$ için $N_r = N_1$ olur (Robinson 1992).

Swart, $N_1 \geq 4$ kısıtlaması ile aşağıdaki teoremi ispatlamıştır. Diğer yandan Somos(4) dizisindeki her bir düzgün p asalı için $N_1 \geq 5$ olduğundan bu teorem, 4. konjektürün ispatını gerçekler.

3.3.11 Teorem. (h_n), en çok bir tane sıfır terim bulunduran bir Somos 4 dizisi ve p, rankı $N_1 \geq 4$ olan düzgün bir asal sayı olsun. p^w, (h_n) dizisinde p nin tüm katlarını bölen en büyük asal kuvvet olmak üzere dizinin belli terimi p^{w+1} ile bölünsün. Her $r \in \mathbb{N}$ için p^r düzgün ve (h_n) dizisindeki rankı N_r olsun. Bu durumda, eğer p tek asal veya $p = 2$ ve $w \geq 2$ ise

$$N_r = \begin{cases} N_1 & r \leq w \\ pN_{r-1} & r > w \end{cases}$$

dir, eğer $p = 2$ ve $w = 1$ ise belli $v \geq 2$ için

$$N_r = \begin{cases} N_1 & r = 1 \\ 2N_1 & 2 \leq r \leq v \\ 2N_{r-1} & r > v \end{cases}$$

dir (Swart 2003).

Robinson tarafından Somos(4) dizilerinin periyodikliği ile ilgili verilmiş konjektürler de vardır. Aşağıda verilen konjektürler söz edilen konjektürlerdir.

3.3.12 Konjektür. (h_n), Somos(4) dizisi olsun. Her p tek asalı ve her $r \in \mathbb{N}$ için (h_n) dizisinin modülo p^r deki periyodu, (h_n) dizisinin modülo p deki periyodunun p^{r-1} katıdır (Robinson 1992).

$p = 2$ hali oldukça farklıdır. Robinson tarafından, her $r \in \mathbb{N}$ için (h_n) Somos(4) dizisinin modülo 2^r deki periyotlarının

$$\pi_1 = 5, \pi_2 = 10, \pi_3 = 10, \pi_4 = 20, \pi_5 = 40, \pi_6 = 80, \ldots$$

olduğu, yani (h_n) dizisinin modülo 4 ve modülo 8 deki periyotlarının aynı olduğu gösterilmiştir.

3.3.13 Teorem. (h_n) bir Somos 4 dizisi ve p, (h_n) dizisinde rankı $N_1 \geq 5$ olacak biçimdeki düzgün tek asal sayı olsun. Bundan başka $r \in \mathbb{N}$ olmak üzere, p^r dizinin belli terimini bölen bir sayı ve p^w, (h_n) dizisinde p sayısının tüm katlarını bölen en büyük asal kuvvet olsun. Bu durumda (h_n) dizisinin modülo p^r deki periyodu

$$\pi_r = \begin{cases} \pi_1 & r \leq u \\ p^{r-u}\pi_1 & r \geq u \end{cases}$$

olacak biçimde bir $u \leq w$ pozitif tamsayısı vardır (Swart 2003).

Somos(4) dizisinin belli bir terimini bölen her bir p asal sayısı için dizinin rankı $N_1 \geq 5$ olduğundan $w = 1$ olarak alınması halinde bu teorem Robinson'un 5. konjektürünü ispatlamış olur.

3.3.14 Konjektür. (h_n), Somos(4) dizisi ve p, (h_n) dizisinde rankı N_1 olan düzgün asal sayı olsun. Bu durumda (h_n) dizisinin modülo p deki periyodu N_1 sayısının bir katıdır ve $(p-1)N_1$ sayısının bir bölenidir (Robinson 1992).

Swart bu konjektürün Somos 4 dizileri için gerçeklenmediğini bir örnek ile göstermiştir. (h_n), başlangıç terimleri 1, 4, 6, 6 ve katsayıları $\lambda_1 = -1$, $\lambda_2 = 3$ olan Somos 4 dizisi ve $p = 7$ olarak alınırsa, dizinin terimleri

…, 0, 1, 4, 6, 6, 0, 6, 1, 4, 6, 0, 3, 6, 1, 4, 0, 1, 3, 6, 1, 0, 1, 1, 3, 6, 0, 3, 1, 1, 3, 0, 6, 3, 1,

1, 0, 1, 6, 3, 1, 0, 4, 1, 6, 3, 0, 6, 4, 1, 6, 0, 6, 6, 4, 1, 0, 4, 6, 6, 4, 0, 1, 4, 6, 6, 0, …

olarak elde edilir. Böylece (h_n) Somos 4 dizisinin $p = 7$ için rankın $N_1 = 5$ ve periyotu $\pi_1 = 60$ olduğu halde dizinin periyotu, $(p-1)N_1 = 30$ değerini bölmemektedir, yani Robinson tarafından Somos(4) dizileri için verilen bu konjektür Somos 4 dizileri için gerçeklenmemektedir.

3.4 Somos 4 Dizileri ile Eliptik Eğriler Arasındaki İlişkiler

Bu kısımda verilen bir eliptik eğriye karşılık gelen Somos 4 dizisi ve verilen bir Somos 4 dizisine karşılık gelen eliptik eğrinin nasıl elde edildiği üzerinde durulacaktır.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$\mathbb{Q}$ cismi üzerinde tanımlı bir eliptik eğri, $P = (\bar{x}, \bar{y})$ ve $Q = (x_0, y_0)$ rasyonel noktaları da bu eliptik eğri üzerinde singüler olmayan farklı iki nokta olsun. $Q + [n]P \neq \boldsymbol{O}$ olacak şekildeki her $n \in \mathbb{Z}$ için $Q + [n]P = (x_n, y_n)$ olarak gösterilsin. Bu şekilde tanımlanan (x_n, y_n) noktalarının x_n koordinatları

$$\ldots,\ x_{-1},\ x_0,\ x_1,\ \ldots$$

şeklinde rasyonel sayıların bir dizisini oluşturur.

Diğer yandan $Q + [n]P = (x_n, y_n)$ noktasının koordinatları kullanılarak s_{-1} ve s_0 sıfırdan farklı rasyonel sayılar olmak üzere

$$s_{n+1} = -\frac{(x_n - \bar{x})s_n^{\,2}}{s_{n-1}},\ n \geq 0$$

$$s_{n-1} = -\frac{(x_n - \bar{x})s_n^{\,2}}{s_{n+1}},\ n \leq -1$$

olarak tanımlanan (s_n) dizilerinin oluşturduğu dizi ailesi $S_{E,Q,P}$ dizi ailesi olarak adlandırılır. Bu dizi ailesinden seçilen herhangi bir dizinin, E eliptik eğrisi üzerindeki $Q+[n]P$ noktalarının x-koordinatlarının oluşturduğu dizi ile eşleştiği açıktır.

3.4.1 Uyarı 1. $S_{E,Q,P}$ dizi ailesinden seçilen bir dizinin sıfır terim bulundurması için gerek ve yeter şart $\langle P\rangle$, singüler olmayan P noktası ile üretilen grup olmak üzere $Q \in \langle P\rangle$ olmasıdır.

2. Herhangi bir (s_n) dizisinin $S_{E,Q,P}$ dizi ailesine ait olması için gerek ve yeter şart

$$s_n = 0 \Leftrightarrow Q+[n]P = \boldsymbol{O} \quad \text{ve} \quad x_n - \bar{x} = -\frac{s_{n-1}s_{n+1}}{s_n^{\,2}}$$

olmasıdır.

$S_{E,Q,P}$ dizi ailesindeki diziler ile Somos 4 dizileri arasındaki ilişki, Swart tarafından aşağıdaki teorem ile ortaya konmuştur.

3.4.2 Teorem. $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

olsun. $P = (0, 0)$ ve $Q = (x_0, y_0)$ noktaları da E eliptik eğrisi üzerinde singüler olmayan rasyonel noktalar olmak üzere $Q+[n]P \neq \boldsymbol{O}$ olacak şekildeki her $n \in \mathbb{Z}$ için $Q+[n]P = (x_n, y_n)$ olarak gösterilsin. Bu durumda $S_{E,Q,P}$ dizi ailesinden seçilen (s_n) dizisi, katsayıları

$$\lambda_1 = a_3^{\,2} \qquad \text{ve} \qquad \lambda_2 = a_4(a_4 + a_1a_3) - a_3^{\,2}a_2$$

ve başlangıç terimleri,

s_{-1} ve s_0 sıfırdan farklı keyfi rasyonel sayı

$$s_1 = -\frac{x_0 s_0^{\,2}}{s_{-1}}$$

$$s_2 = -\frac{(a_4 x_0 - a_3 y_0) s_0^{\,3}}{s_{-1}^{\,2}}$$

olan bir Somos 4 dizisidir (Swart 2003).

3.4.3 Örnek. E eliptik eğrisi

$$E : y^2 - 2xy + 4y = x^3 + x^2 + 6x$$

ve eğri üzerindeki singüler olmayan rasyonel noktalar P = (0, 0) ve Q = (1, 2) olsun. $s_{-1} = s_0 = 1$ olarak seçilirse

$$\lambda_1 = a_3^{\,2} = 16 \qquad \text{ve} \qquad \lambda_2 = a_4(a_4 + a_1 a_3) - a_3^{\,2} a_2 = -28$$

ile

$$s_1 = -\frac{x_0 s_0^{\,2}}{s_{-1}} = -1 \qquad \text{ve} \qquad s_2 = -\frac{(a_4 x_0 - a_3 y_0) s_0^{\,3}}{s_{-1}^{\,2}} = 2$$

olarak elde edilir. Böylece E eliptik eğrisi ile eşleşen Somos 4 dizisinin katsayıları λ_1 = 16 ve λ_2 = –28, başlangıç terimleri ise 1, 1, –1, 2 olup elde edilen

…, 1, 1, –1, 2, 4, –176, 6080, –239104, –90435584, 59081555968, …

Somos 4 dizisi $S_{E,Q,P}$ dizi ailesine ait bir dizidir.

3.4.4 Uyarı 1. Eliptik eğri ile eşleşen Somos 4 dizisinin λ_1 ve λ_2 katsayıları sadece eliptik eğrinin katsayılarına bağlı olduğu halde dizinin başlangıç terimleri Q noktasına, eliptik eğrinin katsayılarına ve s_{-1} ile s_0 terimlerinin seçimine bağlıdır.

2. Eliptik eğrinin katsayıları tamsayı ise dizinin λ_1 ve λ_2 katsayılarının da tamsayı oldukları açıktır. Bundan başka $(\lambda_1, \lambda_2) = 1 \Leftrightarrow (a_3, a_4) = 1$ dir.

3. Q noktası yerine $t \in \mathbb{Z}$ olmak üzere $Q' = Q + [t]P$ noktasının seçilmesi halinde bu noktanın koordinatları yardımıyla elde edilen dizi $S_{E,Q+[t]P,P}$ ailesine ait olan bir dizidir, bu dizi $S_{E,Q,P}$ dizi ailesine ait olan bir dizinin t-kayması olur.

4. s_{-1} ve s_0 terimleri yerine, farklı s_{-1}' ve s_0' seçiminin yapılması halinde elde edilen dizi, $S_{E,Q,P}$ dizi ailesindeki dizilerden bir tanesine denk olan dizidir.

N. Stephens, verilen bir Somos 4 dizisinin katsayılarını ve başlangıç terimlerini kullanarak bu dizi ile eşleşen eliptik eğrinin nasıl belirleneceğini ortaya koymuş ve bu durum Swart (2003) tarafından aşağıdaki teorem ile ifade ve ispat edilmiştir.

3.4.5 Teorem. (s_n), λ_1 katsayısı pozitif tam kare sayı olan bir Somos 4 dizisi olsun. (s_n) Somos 4 dizisi ile eşleşen E eliptik eğrisinin katsayıları ve bu eğri üzerindeki singüler olmayan $Q=(x_0,y_0)$ noktasının koordinatları,

a_4 keyfi

$$a_3 = \pm\sqrt{\lambda_1}$$

$$a_1 = \frac{1}{a_3}\left(-2a_4 + \frac{h_0h_3}{h_1h_2} + \frac{\lambda_1 {h_1}^2}{h_0h_2} + \frac{h_{-1}h_2}{h_0h_1}\right)$$

$$a_2 = -\frac{{a_4}^2 + \lambda_2}{\lambda_1} + \frac{a_4({h_0}^2h_3 + h_{-1}{h_2}^2 + \lambda_1{h_1}^3)}{\lambda_1 h_0 h_1 h_2}$$

$$x_0 = -\frac{h_0h_2}{{h_1}^2} \quad \text{ve} \quad y_0 = \frac{-a_4h_0h_1h_2 + {h_0}^2h_3}{a_3{h_1}^3}$$

dır (Swart 2003).

3.4.6 Örnek. Katsayıları $\lambda_1 = 1$, $\lambda_2 = 2$ ve başlangıç terimleri 1, 1, –2, –3 olan Somos 4 dizisi ile eşleşen eliptik eğrinin katsayıları yukarıda verilen teorem yardımıyla

$a_4 = -1$ (keyfi)

$$a_3 = \pm\sqrt{\lambda_1} = 1$$

$$a_1 = \frac{1}{a_3}\left(-2a_4 + \frac{h_0h_3}{h_1h_2} + \frac{\lambda_1 {h_1}^2}{h_0h_2} + \frac{h_{-1}h_2}{h_0h_1}\right) = 3$$

$$a_2 = -\frac{{a_4}^2 + \lambda_2}{\lambda_1} + \frac{a_4({h_0}^2 h_3 + h_{-1}{h_2}^2 + \lambda_1 {h_1}^3)}{\lambda_1 h_0 h_1 h_2} = -4$$

olarak elde edilir. Böylece E eliptik eğrisinin

$$E : y^2 + 3xy + y = x^3 - 4x^2 - x$$

olduğu görülür. Bu eğri üzerindeki singüler olmayan $Q = (x_0, y_0)$ noktasının koordinatları eğrinin katsayıları ve dizinin terimleri kullanılarak

$$x_0 = -\frac{h_0 h_2}{{h_1}^2} = \frac{3}{4} \qquad \text{ve} \qquad y_0 = \frac{-a_4 h_0 h_1 h_2 + {h_0}^2 h_3}{a_3 {h_1}^3} = -\frac{11}{8}$$

olarak bulunur. Bu durumda katsayıları $\lambda_1 = 1,\ \lambda_2 = 2$ ve başlangıç terimleri 1, 1, –2, –3 olan Somos 4 dizisi, P = (0, 0) olmak üzere $S_{E,Q,P}$ dizi ailesine aittir.

3.4.7 Uyarı. a_4 katsayısı veya a_3 katsayısının işareti ile ilgili yapılan farklı seçimler sonucunda farklı eliptik eğriler elde edileceği açıktır. Ancak bu halde elde edilen eliptik eğriler birasyonel denk eğrilerdir.

3.4.8 Teorem. $(s_n) \in S_{E,Q,(0,0)}$ ve $(s_n') \in S_{E',Q',(0,0)}$ dizileri verilsin. Sıfırdan farklı belli $\alpha, \beta, \gamma \in \mathbb{Q}\backslash\{0\}$ sabitleri ve her $n \in \mathbb{Z}$ için,

$$s_n' = \alpha^{n^2} \beta^n \gamma\, s_n$$

olmak üzere (s_n) ve (s_n') Somos 4 dizilerinin denk olması için gerek ve yeter şart E ve E' eliptik eğrilerinin, $u = \pm\left(\frac{1}{\alpha}\right)$ olmak üzere belli $s \in \mathbb{Q}$ için

$$x = u^2 x' \text{ ve } \ y = u^3 y' + u^2 s x'$$

değişken değişimi altında birasyonel denk olmasıdır (Swart 2003).

3.5 Somos 4 Dizilerinde Tamsayılık Özelliği

Somos k dizilerinin tanımı dikkate alındığında, dizinin terimlerinin elde edildiği bağıntının bölme işlemi içerdiği ve dolayısıyla da bu dizilerin katsayıları ve başlangıç

terimleri birer tamsayı seçildiği halde bu dizilerin terimlerinin her zaman birer tamsayı belirtmeyeceği açıktır. Örneğin katsayıları $\lambda_1 = 1,\ \lambda_2 = 2$ ve başlangıç terimleri 2, 3, 5, 7 olan Somos 4 dizisinin terimleri

$$\ldots, \frac{1184}{9}, \frac{128}{3}, \frac{40}{3}, 4, 4, 2, 3, 5, 7, \frac{71}{2}, \frac{551}{6}, \frac{1898}{3}, \frac{101125}{18}, \ldots$$

olarak elde edilir.

Bu nedenle tüm terimleri tamsayı olan Somos *k* dizilerinin belirlenmesi önemli bir problem olduğu gibi bu dizilerin belirlenmesi üzerine yapılan çalışmalar halen sürmektedir. Bu diziler ile ilgilenen ilk kişi M. Somos (1989), Somos(6) dizisinin tüm terimlerinin tamsayı olduğunu göstermiştir. Daha sonra J. Malouf (1992), Somos(4) dizisinin tüm terimlerinin tamsayı olduğunu gösteren ilk kişidir. Benzer şekilde D. Gale (1991), Somos(*k*) dizilerinin tamsayı özellikleri ile ilgili çalışmalar yapmıştır.

Somos dizileri üzerine yapılan diğer çalışmalar ve uygulamalar şu şekildedir; N. Elkies, Somos dizileri ile eliptik eğriler arasındaki ilişkiyi kurmuştur. A. J. Van Der Porten (2006), sürekli kesirleri kullanarak, her Somos 4 dizisinin bir Somos *k* dizisi olduğunu göstermiştir. Fomin ve Zelevinsky (2002), Somos 4 dizisinin tüm terimlerinin Laurent polinomları ile ifade edilebileceğini göstermiştir. A. Hone ve Swart (2008), Somos 4 dizileri ve bu diziler ile eşleşen eliptik eğrilerin üzerindeki noktaların koordinatlarının dizisi arasında ilişkiyi kurmuşlardır. Bu ilişkiyi kullanarak Somos 4 dizilerinin Laurent özelliğinden daha güçlü bir bağıntıyı gerçeklediğini göstermişlerdir.

Şu ana kadar *k* = 4, 5, 6, 7 halleri için Somos(*k*) dizilerinin birer tamsayı dizisi olduğu bilinmektedir. Ancak bu durum *k* = 8 hali için doğru değildir. Gerçekten de *k* = 8 için Somos(8) dizisinin terimleri

$$\ldots, 13, 7, 4, 1, 1, 1, 1, 1, 1, 1, 1, 4, 7, 13, 25, 61, 187, 775, 5827,$$

$$14815, \frac{420514}{7}, \frac{28670773}{91}, \frac{6905822101}{2275}, \ldots$$

biçimindedir.

Bu çalışmada da Somos 4 dizilerinin tamsayı olma özelliği ele alınmış ve Tate normal formdaki

$$E_N:\ y^2+(1-c)xy-by=x^3-bx^2$$

eliptik eğrileri ile eşleşen Somos 4 dizilerinin tüm terimlerinin tamsayı oldukları belirlenmiştir.

Eliptik eğriler kısmında Tate normal formların α parametresine bağlı olarak

1. $N=4 \Rightarrow b=\alpha$ ve $c=0$

2. $N=5 \Rightarrow b=\alpha$ ve $c=\alpha$

3. $N=6 \Rightarrow b=\alpha+\alpha^2$ ve $c=\alpha$

4. $N=7 \Rightarrow b=\alpha^3-\alpha^2$ ve $c=\alpha^2-\alpha$

5. $N=8 \Rightarrow b=(2\alpha-1)(\alpha-1)$ ve $c=\dfrac{b}{\alpha}$

6. $N=9 \Rightarrow b=c(\alpha(\alpha-1)+1)$ ve $c=\alpha^2(\alpha-1)$

7. $N=10 \Rightarrow b=\dfrac{c\alpha^2}{\alpha-(\alpha-1)^2}$ ve $c=\dfrac{2\alpha^3-3\alpha^2+\alpha}{\alpha-(\alpha-1)^2}$

8. $N=12 \Rightarrow b=\dfrac{c(2\alpha-2\alpha^2-1)}{\alpha-1}$ ve $c=\dfrac{(3\alpha^2-3\alpha+1)(\alpha-2\alpha^2)}{(\alpha-1)^3}$

şeklinde sınıflandırıldığı belirtilmişti. Ancak bu durumda N = 8, 10, 12 hallerinde

$$E_N:\ y^2+(1-c)xy-by=x^3-bx^2$$

denklemi ile ifade edilen Tate normal formdaki eliptik eğrinin katsayıları birer rasyonel sayıdır. Fakat çalışmada katsayıları tamsayı olan eliptik eğriler dikkate alınacağından uygun dönüşümler yardımıyla

$$\beta=(2\alpha-1)(\alpha-1)$$

$$\varsigma=\alpha-(\alpha-1)^2$$

$$\tau=(3\alpha^2-3\alpha+1)(\alpha-2\alpha^2)$$

$$\theta=2\alpha-2\alpha^2-1$$

olmak üzere, E_8, E_{10} ve E_{12} eliptik eğrilerine birasyonel denk olan tamsayı katsayılı

$$E_8':\ y^2+(\alpha-\beta)xy-\alpha^3\beta y=x^3-\alpha^2\beta x^2$$

$$E_{10}'\colon y^2 + (\varsigma^2 - \alpha\beta\varsigma)xy - \alpha^3\beta\varsigma^4 y = x^3 - \alpha^3\beta\varsigma^2 x^2$$

$$E_{12}'\colon y^2 + (\alpha-1)((\alpha-1)^3 - \tau)xy - (\alpha-1)^8\tau\theta y = x^3 - (\alpha-1)^4\tau\theta x^2$$

eliptik eğrileri elde edilir. E_8', E_{10}', E_{12}' eğrileri kullanılacağı halde gösterimde bir karışıklık olmaması için bu eğriler yerine sırasıyla tekrar E_8, E_{10} ve E_{12} gösterimi kullanılacaktır.

3.5.1 Teorem. E_N, mertebesi N olan $P = (0, 0)$ noktasını ve her $n \in \mathbb{Z}$ için $Q + nP \neq \boldsymbol{O}$ olacak biçimdeki tamsayı koordinatlı $Q = (x, y)$ noktasını singüler olmayan nokta olarak bulunduran Tate normal formdaki eliptik eğri olmak üzere (h_n), $h_{-1} = \pm 1$ olacak şekilde E_N eliptik eğrisi ile eşleşen Somos 4 dizisi olsun. Bu durumda (h_n) Somos 4 dizisinin $n \geq 0$ için tüm terimleri tamsayıdır (Gezer ve ark. 2015).

İspat. P ve Q teoremde ifade edilen tamsayı koordinatlı noktalar, h_0 sıfırdan farklı keyfi tamsayı olmak üzere $\beta, \varsigma, \tau, \theta$ daha önce ifade edilen sabitler ve

N	λ_1	λ_2	h_1	h_2
4	α^2	α^3	$-xh_{-1}^{-1}h_0^2$	$-\alpha y h_{-1}^{-2}h_0^3$
5	α^2	α^3	$-xh_{-1}^{-1}h_0^2$	$-\alpha y h_{-1}^{-2}h_0^3$
6	$\alpha^2(\alpha+1)^2$	$\alpha^3(\alpha+1)^3$	$-xh_{-1}^{-1}h_0^2$	$-\alpha(\alpha+1) y h_{-1}^{-2}h_0^3$
7	$\alpha^4(\alpha-1)^2$	$\alpha^6(\alpha-1)^3$	$-xh_{-1}^{-1}h_0^2$	$-\alpha^2(\alpha-1) y h_{-1}^{-2}h_0^3$
8	$\alpha^6\beta^2$	$\alpha^8\beta^3$	$-xh_{-1}^{-1}h_0^2$	$-\alpha^3\beta y h_{-1}^{-2}h_0^3$
9	γ^2	γ^3	$-xh_{-1}^{-1}h_0^2$	$-\gamma y h_{-1}^{-2}h_0^3$
10	$\alpha^6\beta^2\varsigma^8$	$\alpha^9\beta^3\varsigma^{10}$	$-xh_{-1}^{-1}h_0^2$	$-\alpha^3\beta\varsigma^4 y h_{-1}^{-2}h_0^3$
12	$(\alpha-1)^{16}\tau^2\theta^2$	$(\alpha-1)^{20}\tau^3\theta^3$	$-xh_{-1}^{-1}h_0^2$	$-(\alpha-1)^8\tau\theta y h_{-1}^{-2}h_0^3$

$$\gamma = \alpha^2(\alpha-1)(\alpha^2-\alpha+1)$$

olsun. Bu durumda Tate normal formdaki E_N eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin λ_1, λ_2 katsayıları ve h_1, h_2 başlangıç terimleri Teorem 3.4.2 yardımıyla yukarıdaki gibi elde edilir.

Tekrardan kaçınmak amacıyla, teoremin ispatı N sayısının her değeri için yapılmak yerine sadece $N = 8$ hali için verilecektir. Diğer haller benzer şekilde elde edilebilir. $N = 8$ olması halinde yukarıdaki tablodan E_8 eliptik eğrisi ile eşleşen Somos 4 dizisinin katsayıları

$$\lambda_1 = \alpha^6\beta^2, \quad \lambda_2 = \alpha^8\beta^3$$

ve başlangıç terimleri

$$h_1 = -\frac{x{h_0}^2}{h_{-1}}, \quad h_2 = -\frac{\alpha^3\beta y{h_0}^3}{{h_{-1}}^2}$$

olarak elde edilir. Böylece,

$$h_{n+2}h_{n-2} = \lambda_1 h_{n+1}h_{n-1} + \lambda_2 {h_n}^2$$

bağıntısı kullanılarak

$$h_3 = \frac{\alpha^8\beta^3(x^2-\alpha y){h_0}^4}{{h_{-1}}^3}$$

$$h_4 = \frac{-\alpha^{14}\beta^5(x^3-\alpha xy-y^2){h_0}^5}{{h_{-1}}^4}$$

$$h_5 = \frac{-\alpha^{23}\beta^8(\alpha\beta x^4+x^3y-2\alpha^2\beta x^2y-\alpha xy^2+\alpha^3\beta y^2-y^3){h_0}^6}{x{h_{-1}}^5}$$

olarak bulunur. Dikkat edilirse dizinin h_3 ve h_4 terimleri $\mathbb{Z}[\alpha, x, y, {h_{-1}}^{\pm 1}, h_0]$ katsayılar halkasının birer elemanı olmasına rağmen h_5 teriminin paydasında Q noktasının birinci bileşeni olan sıfırdan farklı x sayısı olduğundan h_5 terimi bu katsayılar halkasının bir elemanı değildir. Ancak

$$E_8 : y^2 + (\alpha-\beta)xy - \alpha^3\beta y = x^3 - \alpha^2\beta x^2$$

denklemi kullanılarak gerekli düzenlemeler yapılması halinde, x değeri h_5 teriminin payını böler ve böylece

$$h_5 = -\frac{\alpha^{23}\beta^{9}(\alpha x^3 - \alpha^2 xy - y^2)h_0{}^6}{h_{-1}{}^5}$$

olarak bulunur. Benzer şekilde hareket edilerek, Somos 4 dizilerinin genel bağıntısı yardımıyla

$$\begin{aligned} h_6 = \alpha^{33}\beta^{12}(&-x^6 + \alpha^2\beta x^5 + 2\alpha x^4 y + 2x^3 y^2 - 2\alpha^3\beta x^3 y - \alpha\beta x^2 y^2 \\ &- \alpha^2 x^2 y^2 + \alpha^4\beta x y^2 - 2\alpha x y^3 + \alpha^2\beta y^3 - y^4)h_0{}^7 / y h_{-1}{}^6 \end{aligned}$$

terimi elde edilir. Bu durumda da h_6 teriminin paydasında Q noktasının ikinci bileşeni olan sıfırdan farklı y sayısı olduğundan h_6 terimi de $\mathbb{Z}[\alpha, x, y, h_{-1}{}^{\pm 1}, h_0]$ katsayılar halkasının bir elemanı değildir. Benzer şekilde

$$E_8 : y^2 + (\alpha - \beta)xy - \alpha^3\beta y = x^3 - \alpha^2\beta x^2$$

denklemi kullanılarak ve gerekli düzenlemeler yapılarak

$$h_6 = \frac{\alpha^{33}\beta^{13}(\alpha^2\beta x^3 + (\alpha^2 - \alpha - \beta)x^2 y - \alpha^3\beta xy - (\alpha^3 - \alpha^2)y^2)h_0{}^7}{h_{-1}{}^6}$$

olarak elde edilir. Benzer durum (h_n) Somos 4 dizisinin h_7 terimi için de söz konusudur. Dolayısıyla yukarıdaki gibi hareket edilerek (h_n) Somos 4 dizisinin yedinci terimi

$$\begin{aligned} h_7 = -\alpha^{45}\beta^{18}((&\alpha^4\beta - \alpha^5\beta)x^3 + (\alpha^4 - \alpha^3 + \alpha^3\beta - 2\alpha^2\beta)x^2 y - (\alpha^3 - \alpha^2 - \beta)xy^2 \\ &+ (\alpha^6\beta - \alpha^5\beta)xy - (\alpha^5 - \alpha^4 - \alpha^3\beta)y^2)h_0{}^8 / h_{-1}{}^7 \end{aligned}$$

olarak elde edilir.

P noktasının mertebesi 8 olduğundan dizinin ardışık her bir terimi daha önceki 9 terim yardımıyla elde edilebilir. Böylece E_8 eliptik eğrisi ile eşleşen Somos 4 dizisinin genel terimi;

$$\varepsilon = \begin{cases} +1 & n \equiv 0,3,6,8,9,13,14,15 \pmod{16} \\ -1 & n \equiv 1,2,4,5,7,10,11,12 \pmod{16} \end{cases}$$

$$p=\begin{cases}0 & n\equiv 0 \pmod 8\\ 7 & n\equiv 3,5 \pmod 8\\ 12 & n\equiv 2,6 \pmod 8\\ 15 & n\equiv 1,7 \pmod 8\\ 16 & n\equiv 4 \pmod 8\end{cases} \qquad q=\begin{cases}-3 & n\equiv 3 \pmod 8\\ 0 & n\equiv 0,2 \pmod 8\\ 8 & n\equiv 4,6 \pmod 8\\ 1 & n\equiv 1,5 \pmod 8\\ 13 & n\equiv 7 \pmod 8\end{cases}$$

$$r=\begin{cases}0 & n\equiv 0 \pmod 8\\ 3 & n\equiv 1,3,5,7 \pmod 8\\ 4 & n\equiv 2,6 \pmod 8\\ 8 & n\equiv 4 \pmod 8\end{cases} \qquad m=\begin{cases}k & n\equiv k \pmod 8, k\neq 7\\ -1 & n\equiv k \pmod 8, k=7\end{cases}$$

$$P_8(\alpha,x,y)=\begin{cases}1 & n\equiv 0,7 \pmod 8\\ x & n\equiv 1 \pmod 8\\ y & n\equiv 2 \pmod 8\\ x^2-\alpha y & n\equiv 3 \pmod 8\\ x^3-\alpha xy-y^2 & n\equiv 4 \pmod 8\\ \alpha x^3-\alpha^2 xy-y^2 & n\equiv 5 \pmod 8\\ \alpha^2\beta x^3-(\alpha-1)^2x^2y-\alpha^3\beta xy-\alpha^2(\alpha-1)y^2 & n\equiv 6 \pmod 8\end{cases}$$

$$Q_8=-\alpha^4\beta(\alpha-1)x^3+2\alpha^2(\alpha-1)^3x^2y+\alpha^5\beta(\alpha-1)xy-(\alpha-1)^3xy^2+\alpha^3(\alpha-1)^2y^2$$

olmak üzere

$$\begin{aligned}h_n=\varepsilon\alpha^{\{(15n^2-p)/16\}}(\alpha-1)^{\{(7n^2-6n-q)/16\}}(2\alpha-1)^{\{(3n^2-r)/8\}}\\ \times P_8(\alpha,x,y)[Q_8(\alpha,x,y)]^{\{(n-m)/8\}}h_{-1}{}^{-n}h_0{}^{n+1}\end{aligned} \tag{3.1}$$

olarak elde edilir. Böylece $N = 8$ için $h_{-1} = h_0 = \pm 1$ olması halinde (h_n) Somos 4 dizisinin tüm terimlerinin birer tamsayı olduğu sonucu elde edilmiş olur. Diğer haller de buna benzer şekilde gösterilebilir.

3.5.2 Teorem. E_N, mertebesi N olan $P = (0, 0)$ noktasını ve her $n \in \mathbb{Z}$ için $Q + nP \neq \boldsymbol{O}$ olacak biçimdeki tamsayı koordinatlı $Q = (x, y)$ noktasını singüler olmayan noktalar olarak bulunduran Tate normal formdaki eliptik eğri olsun. ς, τ, θ ve γ daha önce tanımlanan sabitler, (h_n), daha önce tabloda belirtilen katsayılara ve başlangıç

terimlerine sahip olan Somos 4 dizisi ise (h_n) Somos 4 dizilerinin genel terimleri aşağıdaki gibidir:

1. $N = 4$ için

$$\varepsilon = \begin{cases} -1 & n \equiv 1,2,4,5 \pmod 8 \\ +1 & n \equiv 0,3,6,7 \pmod 8 \end{cases}$$

$$p = \begin{cases} 0 & n \equiv 0 \pmod 4 \\ 3 & n \equiv 1,3 \pmod 4 \\ 4 & n \equiv 2 \pmod 4 \end{cases} \qquad m = \begin{cases} k & n \equiv k \pmod 4, k \neq 3 \\ -1 & n \equiv k \pmod 4, k = 3 \end{cases}$$

$$P_4 = \begin{cases} 1 & n \equiv 0,3 \pmod 4 \\ x & n \equiv 1 \pmod 4 \\ y & n \equiv 2 \pmod 4 \end{cases}$$

$$Q_4 = x^2 - y$$

olmak üzere

$$h_n = \varepsilon \alpha^{\left\{(3n^2-p)/8\right\}} P_4(\alpha, x, y) \left[Q_4(\alpha, x, y)\right]^{\left\{(n-m)/4\right\}} h_{-1}{}^{-n} h_0{}^{n+1}$$

dir.

2. $N = 5$ için

$$\varepsilon = \begin{cases} -1 & n \equiv 1,2,4,5,8 \pmod{10} \\ +1 & n \equiv 0,3,6,7,9 \pmod{10} \end{cases}$$

$$p = \begin{cases} 0 & n \equiv 0 \pmod 5 \\ 2 & n \equiv 1,4 \pmod 5 \\ 3 & n \equiv 2,3 \pmod 5 \end{cases} \qquad m = \begin{cases} k & n \equiv k \pmod 5, k \neq 4 \\ -1 & n \equiv k \pmod 5, k = 4 \end{cases}$$

$$P_5 = \begin{cases} 1 & n \equiv 0,4 \pmod 5 \\ x & n \equiv 1 \pmod 5 \\ y & n \equiv 2 \pmod 5 \\ x^2 - y & n \equiv 3 \pmod 5 \end{cases}$$

$$Q_5 = x^2 - xy - y$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(2n^2-p)/5\}} P_5(\alpha,x,y)\left[Q_5(\alpha,x,y)\right]^{\{(n-m)/5\}} {h_{-1}}^{-n} {h_0}^{n+1}$$

dir.

3. $N = 6$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 0,3,6,7,11 \pmod{12} \\ -1 & n \equiv 1,2,4,5,8,9,10 \pmod{12} \end{cases}$$

$$p = \begin{cases} 0 & n \equiv 0 \pmod 6 \\ 3 & n \equiv 1,3 \pmod 6 \\ 4 & n \equiv 2 \pmod 6 \\ 7 & n \equiv 5 \pmod 6 \\ 12 & n \equiv 4 \pmod 6 \end{cases} \qquad q = \begin{cases} 0 & n \equiv 0,3 \pmod 6 \\ 1 & n \equiv 1,2,4,5 \pmod 6 \end{cases}$$

$$m = \begin{cases} k & n \equiv k \pmod 6, k \neq 5 \\ -1 & n \equiv k \pmod 6, k = 5 \end{cases}$$

$$P_6 = \begin{cases} 1 & n \equiv 0,5 \pmod 6 \\ x & n \equiv 1 \pmod 6 \\ y & n \equiv 2 \pmod 6 \\ x^2 - y & n \equiv 3 \pmod 6 \\ x^3 - xy - y^2 & n \equiv 4 \pmod 6 \end{cases}$$

$$Q_6 = (\alpha+1)x^3 - (\alpha+1)xy - y^2$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(5n^2-2n-p)/12\}} (\alpha+1)^{\{(n^2-q)/3\}} P_6(\alpha,x,y)\left[Q_6(\alpha,x,y)\right]^{\{(n-m)/6\}} {h_{-1}}^{-n} {h_0}^{n+1}$$

dir.

4. $N = 7$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 0,3,6,7,10,13 \pmod{14} \\ -1 & n \equiv 1,2,4,5,8,9,11,12 \pmod{14} \end{cases}$$

$$p=\begin{cases}0 & n\equiv 0 \pmod 7\\ 3 & n\equiv 3 \pmod 7\\ 5 & n\equiv 1,6 \pmod 7\\ 6 & n\equiv 2,5 \pmod 7\\ 10 & n\equiv 4 \pmod 7\end{cases} \qquad q=\begin{cases}0 & n\equiv 0 \pmod 7\\ 2 & n\equiv 1 \pmod 7\\ 3 & n\equiv 2,3 \pmod 7\\ 4 & n\equiv 6 \pmod 7\\ 7 & n\equiv 5 \pmod 7\\ 9 & n\equiv 4 \pmod 7\end{cases}$$

$$m=\begin{cases}k & n\equiv k \pmod 7, k\neq 6\\ -1 & n\equiv k \pmod 7, k=6\end{cases}$$

$$P_7=\begin{cases}1 & n\equiv 0,6 \pmod 7\\ x & n\equiv 1 \pmod 7\\ y & n\equiv 2 \pmod 7\\ x^2-y & n\equiv 3 \pmod 7\\ x^3-xy-y^2 & n\equiv 4 \pmod 7\\ \alpha x^3-\alpha xy-y^2 & n\equiv 5 \pmod 7\end{cases}$$

$$Q_7=\alpha^2x^3-(\alpha-1)x^2y-\alpha^2xy-y^2$$

olmak üzere

$$h_n=\varepsilon\alpha^{\{(5n^2-p)/7\}}(\alpha-1)^{\{(3n^2-n-q)/7\}}P_7(\alpha,x,y)\left[Q_7(\alpha,x,y)\right]^{\{(n-m)/7\}}h_{-1}{}^{-n}h_0{}^{n+1}$$

dir.

5. $N=8$ için

$$\varepsilon=\begin{cases}+1 & n\equiv 0,3,6,8,9,13,14,15 \pmod{16}\\ -1 & n\equiv 1,2,4,5,7,10,11,12 \pmod{16}\end{cases}$$

$$p=\begin{cases}0 & n\equiv 0 \pmod 8\\ 7 & n\equiv 3,5 \pmod 8\\ 12 & n\equiv 2,6 \pmod 8\\ 15 & n\equiv 1,7 \pmod 8\\ 16 & n\equiv 4 \pmod 8\end{cases} \qquad q=\begin{cases}-3 & n\equiv 3 \pmod 8\\ 0 & n\equiv 0,2 \pmod 8\\ 8 & n\equiv 4,6 \pmod 8\\ 1 & n\equiv 1,5 \pmod 8\\ 13 & n\equiv 7 \pmod 8\end{cases}$$

$$r=\begin{cases}0 & n\equiv 0 \pmod 8\\ 3 & n\equiv 1,3,5,7 \pmod 8\\ 4 & n\equiv 2,6 \pmod 8\\ 8 & n\equiv 4 \pmod 8\end{cases} \qquad m=\begin{cases}k & n\equiv k \pmod 8, k\neq 7\\ -1 & n\equiv k \pmod 8, k=7\end{cases}$$

$$P_8(\alpha,x,y)=\begin{cases}1 & n\equiv 0,7 \pmod 8\\ x & n\equiv 1 \pmod 8\\ y & n\equiv 2 \pmod 8\\ x^2-\alpha y & n\equiv 3 \pmod 8\\ x^3-\alpha xy-y^2 & n\equiv 4 \pmod 8\\ \alpha x^3-\alpha^2 xy-y^2 & n\equiv 5 \pmod 8\\ \alpha^2\beta x^3-(\alpha-1)^2x^2y-\alpha^3\beta xy-\alpha^2(\alpha-1)y^2 & n\equiv 6 \pmod 8\end{cases}$$

$$Q_8=-\alpha^4\beta(\alpha-1)x^3+2\alpha^2(\alpha-1)^3x^2y+\alpha^5\beta(\alpha-1)xy-(\alpha-1)^3xy^2+\alpha^3(\alpha-1)^2y^2$$

olmak üzere

$$h_n=\varepsilon\alpha^{\{(15n^2-p)/16\}}(\alpha-1)^{\{(7n^2-6n-q)/16\}}(2\alpha-1)^{\{(3n^2-r)/8\}}P_8(\alpha,x,y)\left[Q_8(\alpha,x,y)\right]^{\{(n-m)/8\}}h_{-1}{}^{-n}h_0{}^{n+1}$$

dir.

6. $N=9$ için

$$\varepsilon=\begin{cases}+1 & n\equiv 0,3,6,7,10,11,13,14,17 \pmod{18}\\ -1 & n\equiv 1,2,4,5,8,9,12,15,16 \pmod{18}\end{cases}$$

$$p=\begin{cases}0 & n\equiv 0 \pmod 9\\ 5 & n\equiv 1 \pmod 9\\ 6 & n\equiv 2 \pmod 9\\ 3 & n\equiv 3,5 \pmod 9\\ 14 & n\equiv 4,7 \pmod 9\\ -3 & n\equiv 6 \pmod 9\\ 9 & n\equiv 8 \pmod 9\end{cases} \qquad q=\begin{cases}0 & n\equiv 0 \pmod 9\\ 2 & n\equiv 1 \pmod 9\\ 3 & n\equiv 2,3 \pmod 9\\ 11 & n\equiv 4,7 \pmod 9\\ 9 & n\equiv 5 \pmod 9\\ 6 & n\equiv 6,8 \pmod 9\end{cases}$$

$$r=\begin{cases}1 & n\equiv 1,2,4,5,7,8 \pmod 9\\ 0 & n\equiv 0,3,6 \pmod 9\end{cases} \qquad m=\begin{cases}k & n\equiv k \pmod 9, k\neq 8\\ -1 & n\equiv k \pmod 9, k=8\end{cases}$$

$$P_9=\begin{cases}1 & n\equiv 0,8 \pmod 9\\ x & n\equiv 1 \pmod 9\\ y & n\equiv 2 \pmod 9\\ x^2-y & n\equiv 3 \pmod 9\\ x^3-xy-y^2 & n\equiv 4 \pmod 9\\ (\alpha^2-\alpha+1)x^3-(\alpha^2-\alpha+1)xy-y^2 & n\equiv 5 \pmod 9\\ (\alpha^3-\alpha^2+\alpha)x^3-(\alpha-1)x^2y-(\alpha^3-\alpha^2+\alpha)xy-y^2 & n\equiv 6 \pmod 9\\ (\alpha^4-\alpha^3+\alpha^2)x^4+x^3y-(\alpha^4-\alpha^3+\alpha^2)x^2y-(\alpha^2+1)xy^2-y^3 & n\equiv 7 \pmod 9\end{cases}$$

$$Q_9=\alpha^2(\alpha^2-\alpha+1)^2x^4-(\alpha^4-2\alpha^3+\alpha^2-1)x^3y-\alpha^2(\alpha^2-\alpha+1)^2x^2y-(\alpha^3+1)xy^2-y^3$$

olmak üzere

$$h_n=\varepsilon\alpha^{\{(7n^2-2n-p)/9\}}(\alpha-1)^{\{(4n^2-2n-q)/9\}}(\alpha^2-\alpha+1)^{\{(n^2-r)/3\}}P_9(\alpha,x,y)\left[Q_9(\alpha,x,y)\right]^{\{(n-m)/9\}}h_{-1}{}^{-n}h_0{}^{n+1}$$

dir.

7. $N=10$ için

$$\varepsilon=\begin{cases}+1 & n\equiv 0,3,6,7,9,12,13,14,17,18,19 \pmod{20}\\ -1 & n\equiv 1,2,4,5,8,10,11,15,16 \pmod{20}\end{cases}$$

$$p=\begin{cases}0 & n\equiv 0 \pmod{10}\\ 21 & n\equiv 1,9 \pmod{10}\\ 24 & n\equiv 2,8 \pmod{10}\\ 9 & n\equiv 3,7 \pmod{10}\\ 36 & n\equiv 4 \pmod{10}\\ 25 & n\equiv 5 \pmod{10}\\ 16 & n\equiv 6 \pmod{10}\end{cases} \qquad q=\begin{cases}0 & n\equiv 0 \pmod{10}\\ 7 & n\equiv 1 \pmod{10}\\ 12 & n\equiv 2 \pmod{10}\\ 15 & n\equiv 3 \pmod{10}\\ 36 & n\equiv 4 \pmod{10}\\ 35 & n\equiv 5 \pmod{10}\\ 32 & n\equiv 6 \pmod{10}\\ 27 & n\equiv 7 \pmod{10}\\ 20 & n\equiv 8 \pmod{10}\\ 11 & n\equiv 9 \pmod{10}\end{cases}$$

$$r=\begin{cases}0 & n\equiv 0 \pmod{10}\\ 2 & n\equiv 1,6,9 \pmod{10}\\ 3 & n\equiv 2,3,7,8 \pmod{10}\\ 7 & n\equiv 4 \pmod{10}\\ 5 & n\equiv 5 \pmod{10}\end{cases} \qquad s=\begin{cases}0 & n\equiv 0 \pmod{10}\\ 5 & n\equiv 1,3,5,7,9 \pmod{10}\\ 4 & n\equiv 2,6,8 \pmod{10}\\ 8 & n\equiv 4 \pmod{10}\end{cases}$$

$$m=\begin{cases}k & n\equiv k \pmod{10}, k\neq 9\\ -1 & n\equiv k \pmod{10}, k=9\end{cases}$$

$$P_{10}=\begin{cases}
1 & n\equiv 0,9 \pmod{10}\\
x & n\equiv 1 \pmod{10}\\
y & n\equiv 2 \pmod{10}\\
x^2-\varsigma^2 y & n\equiv 3 \pmod{10}\\
x^3-\varsigma^2 xy-y^2 & n\equiv 4 \pmod{10}\\
\alpha^2 x^3-\alpha^2\varsigma^2 xy-\varsigma y^2 & n\equiv 5 \pmod{10}\\
\alpha^3\varsigma x^3-(\alpha-1)x^2 y-\alpha^3\varsigma^3 xy-\varsigma^2 y^2 & n\equiv 6 \pmod{10}\\
\alpha^4(2\alpha-1)\varsigma^2 x^3-\alpha(\alpha-1)(3\alpha-1)\varsigma x^2 y & \\
+(\alpha-1)xy^2-\alpha^4(2\alpha-1)\varsigma^4 xy-\alpha\varsigma^4 y^2 & n\equiv 7 \pmod{10}\\
\alpha^7(2\alpha-1)\varsigma^3 x^3-(\alpha-1)x^3 y & \\
-\alpha^3(\alpha-1)(2\alpha^2+2\alpha-1)\varsigma^2 x^2 y-\alpha^7(2\alpha-1)\varsigma^5 xy & \\
+(\alpha-1)(2\alpha^2+2\alpha-1)\varsigma xy^2-\alpha^3\varsigma^5 y^2 & n\equiv 8 \pmod{10}
\end{cases}$$

$$Q_{10}=-\alpha^9(2\alpha-1)\varsigma^4 x^3+(\alpha-1)(2\alpha^2+2\alpha-1)\varsigma x^3 y+\alpha^3(\alpha-1)(2\alpha^4+6\alpha^2-5\alpha+1)\varsigma^3 x^2 y$$
$$-(\alpha-1)x^2 y^2+\alpha^9(2\alpha-1)\varsigma^6 xy+(\alpha^4-10\alpha^3+4\alpha-1)(\alpha-1)\varsigma^2 xy^2+\alpha^3\varsigma^7 y^2$$

olmak üzere

$$h_n = \varepsilon\alpha^{\{(21n^2-p)/20\}}(\alpha-1)^{\{(9n^2-2n-q)/20\}}(2\alpha-1)^{\{(2n^2-r)/5\}}\varsigma^{\{(5n^2-s)/4\}}$$
$$\times P_{10}(\alpha,x,y)[Q_{10}(\alpha,x,y)]^{\{(n-m)/10\}}h_{-1}{}^{-n}h_0{}^{n+1}$$

dir.

8. $N = 12$ için

$$\varepsilon = \begin{cases} +1 & n \equiv 0,3,8,9,13,14,16,17,18,19,22,23 \pmod{24} \\ -1 & n \equiv 1,2,4,5,6,7,10,11,12,15,20,21 \pmod{24} \end{cases}$$

$$p = \begin{cases} 0 & n \equiv 0,2 \pmod{12} \\ -1 & n \equiv 1 \pmod{12} \\ 3 & n \equiv 3,11 \pmod{12} \\ 8 & n \equiv 4,10 \pmod{12} \\ 15 & n \equiv 5,9 \pmod{12} \\ 12 & n \equiv 6 \pmod{12} \\ 23 & n \equiv 7 \pmod{12} \\ 24 & n \equiv 8 \pmod{12} \end{cases} \qquad q = \begin{cases} 0 & n \equiv 0 \pmod{12} \\ 59 & n \equiv 1,11 \pmod{12} \\ 44 & n \equiv 2,10 \pmod{12} \\ 51 & n \equiv 3,9 \pmod{12} \\ 80 & n \equiv 4 \pmod{12} \\ 35 & n \equiv 5,7 \pmod{12} \\ 60 & n \equiv 6 \pmod{12} \\ 56 & n \equiv 8 \pmod{12} \end{cases}$$

$$r = \begin{cases} 0 & n \equiv 0 \pmod{12} \\ 1 & n \equiv 1,11 \pmod{12} \\ 4 & n \equiv 2,10 \pmod{12} \\ 9 & n \equiv 3,9 \pmod{12} \\ 16 & n \equiv 4,8 \pmod{12} \\ 25 & n \equiv 5,7 \pmod{12} \\ 12 & n \equiv 6 \pmod{12} \end{cases} \qquad s = \begin{cases} 0 & n \equiv 0,8 \pmod{12} \\ 3 & n \equiv 1,3,5,7,9,11 \pmod{12} \\ 4 & n \equiv 2,6,10 \pmod{12} \\ 8 & n \equiv 4 \pmod{12} \end{cases}$$

$$t = \begin{cases} 1 & n \equiv 1,2,4,5,7,8,10,11 \pmod{12} \\ 0 & n \equiv 0,3,6,9 \pmod{12} \end{cases} \qquad m = \begin{cases} k & n \equiv k \pmod{12}, k \neq 11 \\ -1 & n \equiv k \pmod{12}, k = 11 \end{cases}$$

$$\begin{aligned} Q_{12} &= \alpha^2(12\alpha^4 - 42\alpha^3 + 58\alpha^2 - 37\alpha + 10)(\alpha-1)^6 x^5 \\ &\quad - \theta(3\alpha^2 - 3\alpha + 1)(30\alpha^5 - 66\alpha^4 + 63\alpha^3 - 31\alpha^2 + 8\alpha - 1)(\alpha-1)^{11} x^4 \\ &\quad + 2\alpha^2(3\alpha^2 - 4\alpha + 2)(\alpha-1)^3 x^4 y + \alpha^2 x^3 y^2 \\ &\quad - \alpha^2(12\alpha^6 - 138\alpha^5 + 362\alpha^4 - 457\alpha^3 + 319\alpha^2 - 121\alpha + 20)(\alpha-1)^8 x^3 y \\ &\quad + \theta(3\alpha^2 - 3\alpha + 1)(28\alpha^5 - 60\alpha^4 + 56\alpha^3 - 27\alpha^2 + 7\alpha - 1)(\alpha-1)^{15} x^2 y \\ &\quad - \theta(12\alpha^3 - 16\alpha^2 + 8\alpha - 1)(\alpha-1)^{14} x y^2 - \theta^2\alpha(3\alpha^2 - 3\alpha + 1)(\alpha-1)^{21} y^2, \end{aligned}$$

$$P_{12}=\begin{cases}
1 & n\equiv 0,11 \pmod{12}\\
x & n\equiv 1 \pmod{12}\\
y & n\equiv 2 \pmod{12}\\
x^2-(\alpha-1)^4 y & n\equiv 3 \pmod{12}\\
x^3-(\alpha-1)^4 xy-y^2 & n\equiv 4 \pmod{12}\\
\theta x^3-\theta(\alpha-1)^4 xy-(\alpha-1)y^2 & n\equiv 5 \pmod{12}\\
\theta(\alpha-1)^3(3\alpha^2-3\alpha+1)x^3-(2\alpha^2-\alpha)x^2y & \\
-\theta(\alpha-1)^7(3\alpha^2-3\alpha+1)xy-(\alpha-1)^6 y^2 & n\equiv 6 \pmod{12}\\
\theta(\alpha-1)x^4+\theta(\alpha^2+\alpha-1)(\alpha-1)^3 x^2y & \\
-(3\alpha^2-3\alpha+1)xy^2-\theta\alpha(2\alpha-1)(\alpha-1)^7 y^2 & n\equiv 7 \pmod{12}\\
\theta^2(\alpha-1)^3 x^4+\alpha^2 x^3 y+\theta(\alpha^2-\alpha+1)(\alpha-1)^7 x^2 y & \\
+(2\alpha-1)(\alpha-1)^5 xy^2+\theta\alpha(\alpha-1)^{12} y^2 & n\equiv 8 \pmod{12}\\
\theta^2(3\alpha^2-3\alpha+1)(\alpha-1)^6 x^4 & \\
+(6\alpha^2-7\alpha+3)\alpha^2(\alpha-1)^3 x^3 y+\alpha^2 x^2 y^2 & \\
+\theta(2\alpha^2-\alpha+1)(3\alpha^2-3\alpha+1)(\alpha-1)^{10} x^2 y & \\
-(\alpha-1)^7(8\alpha^3-11\alpha^2+6\alpha-1)xy^2 & \\
-\theta\alpha(3\alpha^2-3\alpha+1)(\alpha-1)^{14} y^2 & n\equiv 9 \pmod{12}\\
2\alpha^2(3\alpha^2-4\alpha+2)(\alpha-1)^3 x^5+\theta(3\alpha^2-3\alpha+1) & \\
\times(14\alpha^5-36\alpha^4+40\alpha^3-23\alpha^2+7\alpha-1)(\alpha-1)^7 x^4 & \\
+\alpha^2 x^4 y-\alpha^2(3\alpha^2-4\alpha+2) & \\
\times(12\alpha^3-24\alpha^2+18\alpha-5)(\alpha-1)^4 x^3 y-\theta(3\alpha^2-3\alpha+1) & \\
\times(12\alpha^5-30\alpha^4+33\alpha^3-19\alpha^2+6\alpha-1)(\alpha-1)^{11} x^2 y & \\
+\theta(9\alpha^3-13\alpha^2+7\alpha-1)(\alpha-1)^{10} xy^2 & \\
+\theta^2\alpha(3\alpha^2-3\alpha+1)(\alpha-1)^{17} y^2 & n\equiv 10 \pmod{12}
\end{cases}$$

olmak üzere

$$h_n=\varepsilon\alpha^{\{(n^2-2n-p)/12\}}(\alpha-1)^{\{(59n^2-q)/24\}}(2\alpha-1)^{\{(n^2-r)/24\}}\tau^{\{(3n^2-s)/8\}}\theta^{\{(n^2-t)/3\}}$$
$$\times P_{12}(\alpha,x,y)\left[Q_{12}(\alpha,x,y)\right]^{\{(n-m)/12\}}{h_{-1}}^{-n}{h_0}^{n+1}$$

dir (Gezer ve ark. 2015).

İspat. n üzerinden tümevarım yöntemi uygulanarak, sadece $N = 8$ hali ispat edilecektir. Diğer haller benzer şekilde elde edilebilir. $n = 7$ için (3.1) eşitliğinden

$$h_7 = -\alpha^{45}\beta^{18}((\alpha^4\beta - \alpha^5\beta)x^3 + (\alpha^4 - \alpha^3 + \alpha^3\beta - 2\alpha^2\beta)x^2y - (\alpha^3 - \alpha^2 - \beta)xy^2 + (\alpha^6\beta - \alpha^5\beta)xy - (\alpha^5 - \alpha^4 - \alpha^3\beta)y^2)h_0^{\,8} / h_{-1}^{\,7}$$

olarak bulunur. Bu terim, Teorem 3.4.2 ve Somos 4 dizisinin terimlerini veren genel bağıntıdan elde edilen h_7 terimi ile karşılaştırıldığında eşitliğin $n = 7$ için gerçeklendiği görülür. $n > 7$ ve $n \equiv 0 \pmod 8$, $n \not\equiv 0 \pmod{16}$ olmak üzere (3.1) eşitliğinin $n + 1$ için gerçeklendiği kabul edilsin. (3.1) eşitliği yardımıyla, $k \in \mathbb{N}$ olmak üzere

$$h_{n+2} = -\alpha^{60k^2+30k+3}(\alpha-1)^{28k^2+11k+1}(2\alpha-1)^{24k^2+12k+1}yQ_8^{\,k}h_{-1}^{\,-(8k+2)}h_0^{\,8k+3}$$

olarak elde edilir. Diğer yandan, tümevarım hipotezi gereği,

$$h_{n-2} = \alpha^{60k^2-30k+3}(\alpha-1)^{28k^2-17k+2}(2\alpha-1)^{24k^2-12k+1} \times (\alpha^2\beta x^3 - (\alpha-1)^2x^2y - \alpha^3\beta xy - \alpha^2(\alpha-1)y^2)Q_8^{\,k-1}h_{-1}^{\,-(8k-2)}h_0^{\,8k-1}$$

$$h_{n-1} = -\alpha^{60k^2-15k}(\alpha-1)^{28k^2-10k}(2\alpha-1)^{24k^2-6k}Q_8^{\,k}h_{-1}^{\,-(8k-1)}h_0^{\,8k}$$

$$h_n = \alpha^{60k^2}(\alpha-1)^{28k^2-3k}(2\alpha-1)^{24k^2}Q_8^{\,k}h_{-1}^{\,-8k}h_0^{\,8k+1}$$

$$h_{n+1} = \alpha^{60k^2+15k}(\alpha-1)^{28k^2+4k}(2\alpha-1)^{24k^2+6k}xQ_8^{\,k}h_{-1}^{\,-(8k+1)}h_0^{\,8k+2}$$

olduğundan bu terimler ve $\lambda_1 = \alpha^6\beta^2$, $\lambda_2 = \alpha^8\beta^3$ katsayıları bir araya getirilerek E_8 eliptik eğrisinin denklemi yardımıyla, $n \equiv 0 \pmod 8$, $n \not\equiv 0 \pmod{16}$ halinde

$$h_{n+2} = -\alpha^{60k^2+30k+3}(\alpha-1)^{28k^2+11k+1}(2\alpha-1)^{24k^2+12k+1}P_{8,2}Q_8^{\,k}h_{-1}^{\,-(8k+2)}h_0^{\,8k+3}$$

olarak elde edilir. $n \equiv 0 \pmod{16}$ olması halinde de benzer sonuç elde edilecektir. Böylece $n \equiv 0 \pmod 8$ olmak üzere $n + 2$ için (3.1) eşitliğinin gerçeklendiği ispat edilmiş olur. Diğer haller de benzer şekilde gösterilebilir. Böylece ispat tamamlanmış olur.

3.5.3 Sonuç. Yukarıdaki teoremden de görüldüğü gibi, Tate normal formdaki eliptik eğriler ile eşleşen (h_n) Somos 4 dizisinin her bir terimi

$$R = \mathbb{Z}[\alpha, x, y, h_{-1}^{\,\pm 1}, h_0]$$

halkasının birer elemanıdır. Özel olarak $h_{-1} = \pm 1$ ise (h_n) Somos 4 dizisinin $n \geq 0$ için tüm terimleri tamsayıdır.

3.5.4 Örnek. Aşağıdaki tabloda $N = 8$ halinde E_8 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin $n = 1222, \ldots, 1231$ için Teorem 3.5.2 yardımıyla elde edilen ε, p, q, r, m değerleri ve P_8 polinomları verilmiştir.

n	$\equiv \pmod{16}$	$\equiv \pmod{8}$	ε	P	q	r	$P_8(\alpha, x, y)$	m
1222	6	6	+1	12	8	4	$\alpha^2\beta x^3 - (\alpha-1)^2x^2y - \alpha^3\beta xy - \alpha^2(\alpha-1)y^2$	6
1223	7	7	–1	15	13	3	1	–1
1224	8	0	+1	0	0	0	1	0
1225	9	1	+1	15	1	3	X	1
1226	10	2	–1	12	0	4	Y	2
1227	11	3	–1	7	–3	3	$x^2 - \alpha y$	3
1228	12	4	–1	16	8	8	$x^3 - \alpha xy - y^2$	4
1229	13	5	+1	7	1	3	$\alpha x^3 - \alpha^2 xy - y^2$	5
1230	14	6	+1	12	8	4	$\alpha^2\beta x^3 - (\alpha-1)^2x^2y - \alpha^3\beta xy - \alpha^2(\alpha-1)y^2$	6
1231	15	7	+1	15	13	3	1	–1

Tabloda verilen değerler kullanılarak E_8 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin 1222. terimi, daha önceki terimlere ihtiyaç duyulmadan,

$$h_{1222} = \varepsilon\alpha^{\{(15.1222^2-p)/16\}}(\alpha-1)^{\{(7.1222^2-6.1222-q)/16\}}(2\alpha-1)^{\{(3.1222^2-r)/8\}} \times P_8(\alpha,x,y)\left[Q_8(\alpha,x,y)\right]^{\{(1222-m)/8\}} h_{-1}{}^{-n} h_0{}^{n+1}$$

genel terim formülü ile doğrudan hesaplanabilir. Örneğin $\alpha = -9$ olarak seçilmesi halinde elde edilen

$$E_8 : y^2 - 199xy + 138510y = x^3 - 15390x^2$$

eliptik eğrisi ve bu eğri üzerindeki $P = (0, 0)$ noktası ile singüler olmayan $Q = (-210, -3900)$ noktası kullanılarak E_8 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin 1222. terimi $h_{-1} = h_0 = 1$ olmak üzere

$$h_{1222} = (+1)(-9)^{\{(15.1222^2-12)/16\}}(-10)^{\{(7.1222^2-6.1222-8)/16\}}(-19)^{\{(3.1222^2-4)/8\}}$$
$$\times P_8(-9,-210,-3900)\left[Q_8(-9,-210,-3900)\right]^{\{(1222-6)/8\}}$$

$$= -2^{65431}\,3^{2800365}\,5^{653923}\,19^{559981}$$

olarak elde edilir. Benzer şekilde (h_n) Somos 4 dizisinin tabloda verilen diğer dokuz terimi de genel terim formülünden aşağıdaki gibi elde edilebilir:

$$h_{1223} = -2^{655299}\,3^{2804949}\,5^{654993}\,19^{560898},$$
$$h_{1224} = 2^{656370}\,3^{2809539}\,5^{656064}\,19^{561816},$$
$$h_{1225} = -2^{657442}\,3^{2814130}\,5^{657136}\,7\,19^{562734},$$
$$h_{1226} = -2^{658515}\,3^{2818726}\,5^{658209}\,13\,19^{563653},$$
$$h_{1227} = -2^{659589}\,3^{2823327}\,5^{659283}\,19^{564573},$$
$$h_{1228} = 2^{660664}\,3^{2827929}\,5^{660358}\,19^{565494},$$
$$h_{1229} = -2^{661740}\,3^{2832537}\,5^{661433}\,19^{566415},$$
$$h_{1230} = -2^{662819}\,3^{2837148}\,5^{662509}\,19^{567337},$$
$$h_{1231} = 2^{663894}\,3^{2841762}\,5^{663586}\,19^{568260}.$$

Dizinin terimlerinin indisleri büyüdükçe, dizinin terimlerinin de oldukça büyük sayılardan oluştuğu görülmektedir. Somos 4 dizileri için verilen indirgeme bağıntısı kullanılarak bu dizinin istenen bir teriminin bulunması, bu terimden önceki terimlerin de bulunmasını gerektirdiğinden, bilgisayar kullanılsa da, bu işlem oldukça uzun bir zaman almaktadır. Bununla birlikte yukarıda verilen genel terim kullanılarak dizinin istenen herhangi terimi küçük bir hesaplama sonrasında çok kısa bir zamanda elde edilebilmektedir. Örnekte dizinin 1222, …, 1231. terimleri verildiği halde çok daha büyük indise sahip terimlerinin de, benzer şekilde, küçük bir hesaplama sonrasında çok kısa bir zamanda elde edilebileceği açıktır.

3.5.5 Uyarı. Somos 4 dizilerini tanımlayan

$$h_{n+2}h_{n-2} = \lambda_1 h_{n+1}h_{n-1} + \lambda_2 h_n^{\,2}$$

bağıntısı yardımıyla (h_n) Somos 4 dizisinin negatif indisli terimleri de elde edilebilir. Ancak $n < 0$ için (h_n) Somos 4 dizisinin terimleri tamsayı olmayabilir. Örneğin,

$$E_{12} : y^2 + 586xy - 948480y = x^3 - 59280x^2$$

eliptik eğrisi ve bu eğri üzerindeki P = (0, 0) ile singüler olmayan Q = (–21945, 9828225) noktaları dikkate alındığı taktirde E_{12} eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin katsayıları

$$\lambda_1 = 899614310400\,,\ \ \lambda_2 = 53329136320512000$$

ve başlangıç terimleri

$$h_{-1} = h_0 = 1, h_1 = 21945, h_2 = -9321874848000$$

olarak elde edilir. Bu durumda E_{12} eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin negatif indisli terimlerinin bazıları

$$\ldots, \frac{75751032939797362507776000000}{14641}, \frac{2806796648448000}{1331}, \frac{-948480}{121}, 1, 1, 21945, \ldots$$

biçimindedir. Görüldüğü gibi, dizinin h_{-2}, h_{-3} ve h_{-4} terimleri birer tamsayı değildirler.

İki veya üç mertebeli torsiyon noktaya sahip olan Tate normal formda eliptik eğri yoktur. Ancak D. S. Kubert ikinci ve üçüncü mertebeden torsiyon noktaya sahip olan eliptik eğrileri sırasıyla

$$E_2 : y^2 = x^3 + a_2x^2 + a_4x \quad \text{ve} \quad E_3 : y^2 + a_1xy + a_3y = x^3$$

olarak belirlemiştir (Kubert 1976). Dolayısıyla h_{-1} ve h_0 sıfırdan farklı keyfi tamsayılar olmak üzere E_2 ve E_3 eliptik eğrileri ile eşleşen Somos 4 dizilerinin h_1, h_2 başlangıç terimleri ve λ_1, λ_2 katsayıları sırasıyla

$$\lambda_1 = 0, \lambda_2 = {a_4}^2 \qquad \text{ve} \qquad h_1 = -x{h_{-1}}^{-1}{h_0}^2,\ h_2 = -a_4x{h_{-1}}^{-2}{h_0}^3$$

$$\lambda_1 = {a_3}^2, \lambda_2 = 0 \qquad \text{ve} \qquad h_1 = -x{h_{-1}}^{-1}{h_0}^2,\ h_2 = a_3y{h_{-1}}^{-2}{h_0}^3$$

biçimindedir. Böylece E_2 ve E_3 eliptik eğrileri ile eşleşen Somos 4 dizilerinin genel terimleri, bu dizilerin başlangıç terimleri ve katsayıları kullanılarak basit bir hesaplama sonucu aşağıdaki gibi elde edilir.

3.5.6 Teorem. E_N, mertebesi N olan $P = (0, 0)$ noktasını ve her $n \in \mathbb{Z}$ için $Q + nP \neq O$ olacak biçimdeki tamsayı koordinatlı $Q = (x, y)$ noktasını singüler olmayan noktalar olarak bulunduran E_2 veya E_3 eliptik eğrileri olsun. E_N eliptik eğrisi ile eşleşen ve başlangıç terimleri ile katsayıları yukarıdaki gibi ifade edilen (h_n) Somos 4 dizisinin genel terimleri:

i. $N = 2$ ise

$$\varepsilon = \begin{cases} +1 & n \equiv 0,3 \pmod 4 \\ -1 & n \equiv 1,2 \pmod 4 \end{cases} \qquad p = \begin{cases} 0 & n \equiv 0 \pmod 2 \\ 1 & n \equiv 1 \pmod 2 \end{cases} \qquad q = \begin{cases} 0 & n \equiv 0 \pmod 2 \\ -1 & n \equiv 1 \pmod 2 \end{cases}$$

olmak üzere

$$h_n = \varepsilon a_4^{\{(n^2-p)/4\}} x^{\{(n-q)/2\}} h_{-1}^{-n} h_0^{n+1} \tag{3.2}$$

dir.

ii. $N = 3$ ise

$$\varepsilon = \begin{cases} +1 & n \equiv 0,2 \pmod 3 \\ -1 & n \equiv 1 \pmod 3 \end{cases} \qquad p \equiv \begin{cases} 1 & n \equiv 1,2 \pmod 3 \\ 0 & n \equiv 0 \pmod 3 \end{cases}$$

$$q = \begin{cases} 1 & n \equiv 1 \pmod 3 \\ 0 & n \equiv 0,2 \pmod 3 \end{cases} \qquad r = \begin{cases} 0 & n \equiv 0 \pmod 3 \\ 1 & n \equiv 1 \pmod 3 \\ -1 & n \equiv 2 \pmod 3 \end{cases}$$

olmak üzere

$$h_n = \varepsilon a_3^{\{(n^2-p)/3\}} x^q y^{\{(n-r)/3\}} h_{-1}^{-n} h_0^{n+1}$$

dir (Gezer ve ark. 2015).

İspat. n üzerinden tümevarım yöntemi uygulanarak sadece $N = 2$ hali için ispat verilecektir. $N = 3$ hali benzer şekilde ispat edilebilir. $n = 2$ için

$$h_n = \varepsilon a_4^{\{(n^2-p)/4\}} x^{\{(n-q)/2\}} h_{-1}^{-n} h_0^{n+1}$$

eşitliği kullanılarak $h_2 = -a_4 x h_{-1}^{-2} h_0^{3}$ olarak elde edilir. Bu terim Teorem 3.4.2 den elde edilen h_2 terimi ile karşılaştırıldığında teoremin $n = 2$ için gerçeklendiği görülür. $n > 2$

ve $n \equiv 0 \pmod 2$, $n \not\equiv 0 \pmod 4$ olmak üzere (3.2) eşitliğinin $n + 1$ için gerçeklendiği kabul edilsin. (3.2) eşitliği yardımıyla $k \in \mathbb{N}$ olmak üzere

$$h_{n+2} = a_4^{\{(n^2+4n+4)/4\}} x^{\{(n+2)/2\}} h_{-1}^{-n-2} h_0^{n+3}$$

olarak elde edilir. Benzer şekilde

$$h_{n-2} = a_4^{\{(n^2-4n+4)/4\}} x^{\{(n-2)/2\}} h_{-1}^{-n+2} h_0^{n-1}$$

$$h_{n-1} = -a_4^{\{(n^2-2n)/4\}} x^{\{n/2\}} h_{-1}^{-n+1} h_0^{n}$$

$$h_n = -a_4^{\{n^2/4\}} x^{\{n/2\}} h_{-1}^{-n} h_0^{n+1}$$

$$h_{n+1} = a_4^{\{(n^2+2n)/4\}} x^{\{(n+2)/2\}} h_{-1}^{-n-1} h_0^{n+2}$$

olduğundan bu terimler ve $\lambda_1 = 0, \lambda_2 = a_4^{\,2}$ katsayıları kullanılarak indirgeme bağıntısı yardımıyla

$$h_{n+2} = a_4^{\{(n^2+4n+4)/4\}} x^{\{(n+2)/2\}} h_{-1}^{-n-2} h_0^{n+3}$$

olarak elde edilir. $n \equiv 0 \pmod 4$ olarak alınması halinde de benzer sonuç elde edilecektir. Böylece $n \equiv 0 \pmod 2$ olmak üzere $n + 2$ için (3.2) eşitliğinin gerçeklendiği ispat edilmiş olur. Diğer haller de benzer şekilde gösterilebilir. Böylece ispat tamamlanmış olur.

3.5.7 Örnek. Aşağıdaki tabloda $N = 2$ halinde E_2 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin $n = 1801, \ldots, 1806$ için Teorem 3.5.6 yardımıyla elde edilen ε, p, q değerleri verilmiştir.

n	$\equiv \pmod 4$	$\equiv \pmod 2$	ε	p	q
1801	1	1	−1	+1	−1
1802	2	0	−1	0	0
1803	3	1	+1	+1	−1
1804	0	0	+1	0	0
1805	1	1	−1	+1	−1
1806	2	0	−1	0	0

Tabloda verilen değerler kullanılarak E_2 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin 1801. terimi, daha önceki terimlere ihtiyaç duyulmadan,

$$h_{1801} = \varepsilon a_4^{\{(1801^2-p)/4\}} x^{\{(1801-q)/2\}} h_{-1}{}^{-n} h_0{}^{n+1}$$

genel terim formülü ile doğrudan hesaplanabilir. Örneğin

$$E_2 : y^2 = x^3 + 6x^2 - 18x$$

eliptik eğrisi ve bu eğri üzerindeki $P = (0, 0)$ noktası ile singüler olmayan $Q = (-8, 4)$ noktası kullanılarak E_2 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin 1801. terimi $h_{-1} = h_0 = 1$ olmak üzere

$$h_{1801} = -(-18)^{\{(1801^2-1)/4\}}(-8)^{\{(1801+1)/2\}}$$

$$= 2^{813603}\, 3^{1621800}$$

olarak elde edilir. Benzer şekilde (h_n) Somos 4 dizisinin tabloda verilen diğer beş terimi de genel terim formülünden aşağıdaki gibi elde edilebilir:

$$h_{1802} = -2^{814504}\, 3^{1623602},$$
$$h_{1803} = 2^{815408}\, 3^{1625404},$$
$$h_{1804} = 2^{816310}\, 3^{1627208},$$
$$h_{1805} = 2^{817215}\, 3^{1629012},$$
$$h_{1806} = -2^{818118}\, 3^{1630818}.$$

3.6 Tate Normal Formdaki Eliptik Eğriler İle Eşleşen Somos 4 Dizilerindeki Kare ve Küp Terimler

Bu kısımda, bir uygulama olarak Tate normal formdaki eliptik eğriler ile eşleşen Somos 4 dizilerinin terimlerinden hangilerinin bir tam kare veya tam küp oldukları belirlenecektir. Hemen belirtmek gerekirse bu dizilerin terimleri içinde sonsuz çoklukta tam kare ve tam küp terim vardır. Dizinin terimlerinden hangilerinin bir tam kare ve bir tam küp olduğu sorusuna aşağıdaki teorem ile yanıt verilmektedir. Daha önce belirtildiği gibi, dizinin tam kare ve tam küp terimleri, sırası ile, "□" ve "C" gösterimleri ile belirtilecektir.

3.6.1 Teorem. (h_n), $h_{-1} = \pm 1$ olmak üzere herhangi Tate normal formdaki bir eliptik eğri ile eşleşen Somos 4 dizisi olsun. Bu durumda $N \in \{4, \ldots, 10, 12\}$ olmak üzere

i. $n \equiv -1 \pmod{2N}$ ise sıfırdan farklı her α, x, y için $h_n =$ □ dir,

ii. $n \equiv -1 \pmod{3N}$ ise sıfırdan farklı her α, x, y için $h_n = C$ dir (Gezer ve ark. 2015).

İspat. (h_n), $h_{-1} = \pm 1$ olmak üzere Tate normal formdaki eliptik eğri ile eşleşen Somos 4 dizisi olsun. Sonuç 3.5.3 gereği (h_n) Somos 4 dizisinin her bir terimi $P(\alpha, x, y, h_0)$ polinomlarının çarpımıdır ve üstelik bu polinomlar ikişer ikişer aralarında asaldır. Bu durumda her bir çarpan kare ise h_n terimi karedir. Benzer durumun küp olma hali için de geçerli olduğu açıktır. Burada $N = 8$ hali için ispat verilecektir.

i. hali için $n \equiv -1 \pmod{16}$ ise $k \in \mathbb{N}$ olmak üzere $n = 16k - 1$ dir. Buradan (3.1) eşitliği yardımıyla,

$$h_n = \alpha^{30k(8k-1)}(\alpha - 1)^{4k(28k-5)}(2\alpha - 1)^{12k(8k-1)} {Q_8}^{2k} {h_0}^{16k}$$

olarak elde edilir. Bu eşitlikten $h_n =$ □ olduğu görülür.

ii. hali için $n \equiv -1 \pmod{24}$ ise $k \in \mathbb{N}$ olmak üzere $n = 24k - 1$ dir. Buradan (3.1) eşitliği yardımıyla,

$$h_n = \varepsilon\alpha^{45k(12k-1)}(\alpha - 1)^{6k(42k-5)}(2\alpha - 1)^{18k(12k-1)} {Q_8}^{3k} {h_0}^{24k}$$

olarak elde edilir. Bu eşitlikten $h_n = C$ olduğu görülür.

3.6.2 Uyarı. Yukarıdaki teorem $N = 2, 3$ için E_2 ve E_3 eliptik eğrileri ile eşleşen (h_n) Somos 4 dizileri için de geçerlidir.

3.6.3 Uyarı. Teorem 3.6.1 de, $n \equiv -1 \pmod{2N}$ ise sıfırdan farklı her α, x, y için $h_n =$ □ ve $n \equiv -1 \pmod{3N}$ ise sıfırdan farklı her α, x, y için $h_n = C$ olduğu ifade edildi. Aşağıdaki teoremlerde, Tate normal formdaki eliptik eğriler ile eşleşen Somos 4 dizilerindeki kare ve küp terimlerin hangi özellikteki terimler oldukları genel olarak belirtilmiştir.

3.6.4 Teorem. (h_n), $h_{-1} = \pm 1$ ve $h_0 = \square$ olmak üzere Tate normal formdaki herhangi bir eliptik eğri ile eşleşen Somos 4 dizisi olsun. Bu durumda,

***N* = 2 Hali:** $n \equiv 0 \pmod 4$ için "$h_n = \square$",

$n \equiv 1 \pmod 4$ için "$h_n = \square \Leftrightarrow x = \square$" ,

$n \equiv 2 \pmod 4$ için "$h_n = \square \Leftrightarrow a_4 x = \square$" .

***N* = 3 Hali:** $n \equiv 0 \pmod 6$ için "$h_n = \square$",

$n \equiv 1 \pmod 6$ için "$h_n = \square \Leftrightarrow x = \square$",

$n \equiv 2,3 \pmod 6$ için "$h_n = \square \Leftrightarrow a_3 y = \square$",

$n \equiv 4 \pmod 6$ için "$h_n = \square \Leftrightarrow a_3 xy = \square$".

***N* = 4 Hali:** $n \equiv 0 \pmod 8$ için "$h_n = \square$",

$n \equiv 1 \pmod 8$ için "$h_n = \square \Leftrightarrow P_4 = \square$",

$n \equiv 2 \pmod 8$ için "$h_n = \square \Leftrightarrow \alpha P_4 = \square$",

$n \equiv 3 \pmod 8$ için "$h_n = \square \Leftrightarrow \alpha Q_4 = \square$",

$n \equiv 4 \pmod 8$ için "$h_n = \square \Leftrightarrow Q_4 = \square$",

$n \equiv 5,6 \pmod 8$ için "$h_n = \square \Leftrightarrow \alpha P_4 Q_4 = \square$".

***N* = 5 Hali:** $n \equiv 0 \pmod{10}$ için "$h_n = \square$",

$n \equiv 1 \pmod{10}$ için "$h_n = \square \Leftrightarrow P_5 = \square$",

$n \equiv 2,3 \pmod{10}$ için "$h_n = \square \Leftrightarrow \alpha P_5 = \square$",

$n \equiv 4,5 \pmod{10}$ için "$h_n = \square \Leftrightarrow Q_5 = \square$",

$n \equiv 6 \pmod{10}$ için "$h_n = \square \Leftrightarrow P_5 Q_5 = \square$",

$n \equiv 7,8 \pmod{10}$ için "$h_n = \square \Leftrightarrow \alpha P_5 Q_5 = \square$".

***N* = 6 Hali:** $n \equiv 0 \pmod{12}$ için "$h_n = \square$",

$n \equiv 1 \pmod{12}$ için "$h_n = \square \Leftrightarrow P_6 = \square$",

$n \equiv 2,4 \pmod{12}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha + 1) P_6 = \square$",

$n \equiv 3 \pmod{12}$ için "$h_n = \square \Leftrightarrow (\alpha + 1) P_6 = \square$",

$n \equiv 5 \pmod{12}$ için "$h_n = \square \Leftrightarrow \alpha Q_6 = \square$",

$n \equiv 6 \pmod{12}$ için "$h_n = \square \Leftrightarrow Q_6 = \square$",

$n \equiv 7 \pmod{12}$ için "$h_n = \square \Leftrightarrow \alpha P_6 Q_6 = \square$",

$n \equiv 8,9,10 \pmod{12}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha+1) P_6 Q_6 = \square$".

$N = 7$ Hali: $n \equiv 0 \pmod{14}$ için "$h_n = \square$",

$n \equiv 1 \pmod{14}$ için "$h_n = \square \Leftrightarrow P_7 = \square$",

$n \equiv 2,3,4 \pmod{14}$ için "$h_n = \square \Leftrightarrow (\alpha-1) P_7 = \square$",

$n \equiv 5 \pmod{14}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha-1) P_7 = \square$",

$n \equiv 6,7 \pmod{14}$ için "$h_n = \square \Leftrightarrow \alpha Q_7 = \square$",

$n \equiv 8 \pmod{14}$ için "$h_n = \square \Leftrightarrow \alpha P_7 Q_7 = \square$",

$n \equiv 9,10,11 \pmod{14}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha-1) P_7 Q_7 = \square$",

$n \equiv 12 \pmod{14}$ için "$h_n = \square \Leftrightarrow (\alpha-1) P_7 Q_7 = \square$".

$N = 8$ Hali: $n \equiv 0 \pmod{16}$ için "$h_n = \square$",

$n \equiv 1 \pmod{16}$ için "$h_n = \square \Leftrightarrow P_8 = \square$",

$n \equiv 2,5,6 \pmod{16}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha-1)(2\alpha-1) P_8 = \square$",

$n \equiv 3,4 \pmod{16}$ için "$h_n = \square \Leftrightarrow (\alpha-1)(2\alpha-1) P_8 = \square$",

$n \equiv 7 \pmod{16}$ için "$h_n = \square \Leftrightarrow \alpha Q_8 = \square$",

$n \equiv 8 \pmod{16}$ için "$h_n = \square \Leftrightarrow (\alpha-1) Q_8 = \square$",

$n \equiv 9 \pmod{16}$ için "$h_n = \square \Leftrightarrow \alpha P_8 Q_8 = \square$",

$n \equiv 10,14 \pmod{16}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha-1) P_8 Q_8 = \square$",

$n \equiv 11 \pmod{16}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha-1)(2\alpha-1) P_8 Q_8 = \square$",

$n \equiv 12 \pmod{16}$ için "$h_n = \square \Leftrightarrow (2\alpha-1) P_8 Q_8 = \square$",

$n \equiv 13 \pmod{16}$ için "$h_n = \square \Leftrightarrow (\alpha-1)(2\alpha-1) P_8 Q_8 = \square$".

$N = 9$ Hali: $n \equiv 0 \pmod{18}$ için "$h_n = \square$",

$n \equiv 1 \pmod{18}$ için "$h_n = \square \Leftrightarrow P_9 = \square$",

$n \equiv 2,3,4 \pmod{18}$ için "$h_n = \square \Leftrightarrow (\alpha-1)(\alpha^2-\alpha+1) P_9 = \square$",

$n \equiv 5 \pmod{18}$ için "$h_n = \square \Leftrightarrow (\alpha-1) P_9 = \square$",

$n \equiv 6 \pmod{18}$ için "$h_n = \square \Leftrightarrow \alpha P_9 = \square$",

$n \equiv 7 \pmod{18}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha-1) P_9 = \square$",

$n \equiv 8,9,10 \pmod{18}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha^2 - \alpha + 1)Q_9 = \square$",

$n \equiv 11,12,13 \pmod{18}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha - 1)P_9Q_9 = \square$",

$n \equiv 14 \pmod{18}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha - 1)(\alpha^2 - \alpha + 1)P_9Q_9 = \square$",

$n \equiv 15 \pmod{18}$ için "$h_n = \square \Leftrightarrow (\alpha^2 - \alpha + 1)P_9Q_9 = \square$",

$n \equiv 16 \pmod{18}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(\alpha^2 - \alpha + 1)\, P_9Q_9 = \square$".

$N = 10$ Hali: $n \equiv 0 \pmod{20}$ için "$h_n = \square$",

$n \equiv 1 \pmod{20}$ için "$h_n = \square \Leftrightarrow P_{10} = \square$",

$n \equiv 2,3,4,5 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha - 1)(2\alpha - 1)P_{10} = \square$",

$n \equiv 6 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha P_{10} = \square$",

$n \equiv 7 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha - 1)P_{10} = \square$",

$n \equiv 8 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha - 1)\varsigma\, P_{10} = \square$",

$n \equiv 9 \pmod{20}$ için "$h_n = \square \Leftrightarrow Q_{10} = \square$",

$n \equiv 10 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha\varsigma\, Q_{10} = \square$",

$n \equiv 11 \pmod{20}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)P_{10}Q_{10} = \square$",

$n \equiv 12,14 \pmod{20}$ için $(\alpha - 1)(2\alpha - 1)\varsigma\, P_{10}Q_{10} = \square$",

$n \equiv 13,15 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha - 1)P_{10}Q_{10} = \square$",

$n \equiv 16 \pmod{20}$ için "$h_n = \square \Leftrightarrow \varsigma\, P_{10}Q_{10} = \square$",

$n \equiv 17,18 \pmod{20}$ için "$h_n = \square \Leftrightarrow \alpha\,(\alpha - 1)(2\alpha - 1)P_{10}Q_{10} = \square$".

$N = 12$ Hali: $n \equiv 0 \pmod{24}$ için "$h_n = \square$",

$n \equiv 1 \pmod{24}$ için "$h_n = \square \Leftrightarrow P_{12} = \square$",

$n \equiv 2,3,4,10 \pmod{24}$ için "$h_n = \square \Leftrightarrow \lambda\theta\, P_{12} = \square$",

$n \equiv 5 \pmod{24}$ için "$h_n = \square \Leftrightarrow \lambda\, P_{12} = \square$",

$n \equiv 6 \pmod{24}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha - 1)\,\lambda\, P_{12} = \square$",

$n \equiv 7 \pmod{24}$ için "$h_n = \square \Leftrightarrow \alpha(\alpha - 1)(2\alpha - 1)P_{12} = \square$",

$n \equiv 8 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)\,\theta\, P_{12} = \square$",

$n \equiv 9 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1)\,\theta\, P_{12} = \square$",

$n \equiv 11 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1)\,\lambda\, Q_{12} = \square$",

$n \equiv 12 \pmod{24}$ için "$h_n = \square \Leftrightarrow Q_{12} = \square$",

$n \equiv 13 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1)\lambda P_{12}Q_{12} = \square$",

$n \equiv 14,16,21,22 \pmod{24}$ için "$h_n = \square \Leftrightarrow \lambda\theta P_{12}Q_{12} = \square$",

$n \equiv 15 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1)\theta P_{12}Q_{12} = \square$",

$n \equiv 17 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)(2\alpha - 1)P_{12}Q_{12} = \square$",

$n \equiv 18 \pmod{24}$ için "$h_n = \square \Leftrightarrow \alpha(2\alpha - 1)\lambda P_{12}Q_{12} = \square$",

$n \equiv 19 \pmod{24}$ için "$h_n = \square \Leftrightarrow \alpha\lambda P_{12}Q_{12} = \square$",

$n \equiv 20 \pmod{24}$ için "$h_n = \square \Leftrightarrow (\alpha - 1)\theta P_{12}Q_{12} = \square$".

İspat. (h_n), $h_{-1} = \pm 1$ ve $h_0 = \square$ olmak üzere Tate normal formdaki eliptik eğri ile eşleşen Somos 4 dizisi olsun. Sonuç 3.5.3 gereği (h_n) Somos 4 dizisinin her bir terimi $P(\alpha, x, y, h_0)$ polinomlarının çarpımıdır ve üstelik bu polinomlar ikişer ikişer aralarında asaldır. Bu durumda her bir çarpan kare ise h_n terimi karedir. Burada tekrardan kaçınmak amacıyla sadece $N = 4$ hali için ispat verilecektir. Diğer haller de genel terim formülü kullanılarak benzer şekilde ispat edilebilir.

1. $n \equiv 0 \pmod{8}$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k$ dır. Teorem 3.5.2 de $N = 4$ hali için verilen genel terim formülü kullanılarak,

$$h_n = \alpha^{24k^2} Q_4^{2k}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square$" olduğu görülür.

2. $n \equiv 1 \pmod{8}$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 1$ dir. Teorem 3.5.2 de $N = 4$ hali için verilen genel terim formülü kullanılarak,

$$h_n = -\alpha^{24k^2+6k} P_4 Q_4^{2k}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow P_4 = \square$" olduğu görülür.

3. $n \equiv 2 \pmod{8}$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 2$ dir. Genel terim formülü yardımıyla,

$$h_n = -\alpha^{24k^2+12k+1} P_4 Q_4^{2k}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow \alpha P_4 = \square$" olduğu görülür.

4. $n \equiv 3\ (8)$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 3$ dür. Genel terim formülü yardımıyla,

$$h_n = \alpha^{24k^2+18k+3} Q_4^{2k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow \alpha Q_4 = \square$" olduğu görülür.

5. $n \equiv 4\ (\mathrm{mod}\, 8)$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 4$ dür. Genel terim formülü yardımıyla,

$$h_n = -\alpha^{24k^2+24k+6} Q_4^{2k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow Q_4 = \square$" olduğu görülür.

6. $n \equiv 5\ (\mathrm{mod}\, 8)$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 5$ dir. Genel terim formülü yardımıyla,

$$h_n = -\alpha^{24k^2+30k+9} P_4 Q_4^{2k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow \alpha P_4 Q_4 = \square$" olduğu görülür.

7. $n \equiv 6\ (\mathrm{mod}\, 8)$ ise $k \in \mathbb{N}$ olmak üzere $n = 8k + 6$ dır. Genel terim formülü yardımıyla,

$$h_n = \alpha^{24k^2+36k+13} P_4 Q_4^{2k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = \square \Leftrightarrow \alpha P_4 Q_4 = \square$" olduğu görülür.

3.6.5 Teorem. (h_n), $h_{-1} = \pm 1$ ve $h_0 = C$ olmak üzere Tate normal formdaki eliptik eğri ile eşleşen Somos 4 dizisi olsun.

***N* = 2 Hali:** $n \equiv 0\ (\mathrm{mod}\, 6)$ için "$h_n = C$",

$n \equiv 1\ (\mathrm{mod}\, 6)$ için "$h_n = C \Leftrightarrow x = C$",

$n \equiv 2\ (\mathrm{mod}\, 6)$ için "$h_n = C \Leftrightarrow a_4 x = C$",

$n \equiv 3\ (\mathrm{mod}\, 6)$ için "$h_n = C \Leftrightarrow a_4^2 x^2 = C$",

$n \equiv 4\ (\mathrm{mod}\, 6)$ için "$h_n = C \Leftrightarrow a_4 x^2 = C$".

***N* = 3 Hali:** $n \equiv 0\ (\mathrm{mod}\, 9)$ için "$h_n = C$",

$n \equiv 1\ (\mathrm{mod}\, 9)$ için "$h_n = C \Leftrightarrow x = C$",

$n \equiv 2 \pmod 9$ için "$h_n = C \Leftrightarrow a_3 y = C$",

$n \equiv 3 \pmod 9$ için "$h_n = C \Leftrightarrow y = C$",

$n \equiv 4 \pmod 9$ için "$h_n = C \Leftrightarrow a_3^2 xy = C$",

$n \equiv 5 \pmod 9$ için "$h_n = C \Leftrightarrow a_3^2 y^2 = C$",

$n \equiv 6 \pmod 9$ için "$h_n = C \Leftrightarrow y^2 = C$",

$n \equiv 7 \pmod 9$ için "$h_n = C \Leftrightarrow a_3 x y^2 = C$".

$N = 4$ Hali: $n \equiv 0 \pmod{12}$ için "$h_n = C$",

$n \equiv 1 \pmod{12}$ için "$h_n = C \Leftrightarrow P_4 = C$",

$n \equiv 2 \pmod{12}$ için "$h_n = C \Leftrightarrow \alpha P_4 = C$",

$n \equiv 3,4 \pmod{12}$ için "$h_n = C \Leftrightarrow Q_4 = C$",

$n \equiv 5 \pmod{12}$ için "$h_n = C \Leftrightarrow P_4 Q_4 = C$",

$n \equiv 6 \pmod{12}$ için "$h_n = C \Leftrightarrow \alpha P_4 Q_4 = C$",

$n \equiv 7,8 \pmod{12}$ için "$h_n = C \Leftrightarrow Q_4^2 = C$",

$n \equiv 9 \pmod{12}$ için "$h_n = C \Leftrightarrow P_4 Q_4^2 = C$",

$n \equiv 10 \pmod{12}$ için "$h_n = C \Leftrightarrow \alpha P_4 Q_4^2 = C$".

$N = 5$ Hali: $n \equiv 0 \pmod{15}$ için "$h_n = C$",

$n \equiv 1,3 \pmod{15}$ için "$h_n = C \Leftrightarrow P_5 = C$",

$n \equiv 2 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha P_5 = C$",

$n \equiv 4 \pmod{15}$ için "$h_n = C \Leftrightarrow Q_5 = C$",

$n \equiv 5 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha Q_5 = C$",

$n \equiv 6 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha^2 Q_5 = C$",

$n \equiv 7,8 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha P_5 Q_5 = C$",

$n \equiv 9 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha^2 Q_5^2 = C$",

$n \equiv 10 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha Q_5^2 = C$",

$n \equiv 11,12 \pmod{15}$ için "$h_n = C \Leftrightarrow P_5 Q_5^2 = C$",

$n \equiv 13 \pmod{15}$ için "$h_n = C \Leftrightarrow \alpha P_5 Q_5^2 = C$".

$N = 6$ Hali: $n \equiv 0 \pmod{18}$ için "$h_n = C$",

$n \equiv 1,3 \pmod{18}$ için "$h_n = C \Leftrightarrow P_6 = C$",

$n \equiv 2 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha(\alpha+1)P_6 = C$",

$n \equiv 4 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha+1)^2P_6 = C$",

$n \equiv 5 \pmod{18}$ için "$h_n = C \Leftrightarrow (\alpha+1)^2Q_6 = C$",

$n \equiv 6 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha^2Q_6 = C$",

$n \equiv 7 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha(\alpha+1)P_6Q_6 = C$",

$n \equiv 8 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha P_6Q_6 = C$",

$n \equiv 9 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha^2P_6Q_6 = C$",

$n \equiv 10 \pmod{18}$ için "$h_n = C \Leftrightarrow P_6Q_6 = C$",

$n \equiv 11 \pmod{18}$ için "$h_n = C \Leftrightarrow (\alpha+1)Q_6^2 = C$",

$n \equiv 12 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha Q_6^2 = C$",

$n \equiv 13 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha+1)^2P_6Q_6^2 = C$",

$n \equiv 14 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha(\alpha+1)^2P_6Q_6^2 = C$",

$n \equiv 15 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha P_6Q_6^2 = C$",

$n \equiv 16 \pmod{18}$ için "$h_n = C \Leftrightarrow \alpha(\alpha+1)P_6Q_6^2 = C$".

$N = 7$ Hali: $n \equiv 0 \pmod{21}$ için "$h_n = C$",

$n \equiv 1,3 \pmod{21}$ için "$h_n = C \Leftrightarrow P_7 = C$",

$n \equiv 2 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)P_7 = C$",

$n \equiv 4 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2P_7 = C$",

$n \equiv 5 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2P_7 = C$",

$n \equiv 6 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2Q_7 = C$",

$n \equiv 7 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2Q_7 = C$",

$n \equiv 8,12 \pmod{21}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2P_7Q_7 = C$",

$n \equiv 9 \pmod{21}$ için "$h_n = C \Leftrightarrow P_7Q_7 = C$",

$n \equiv 10 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2P_7Q_7 = C$",

$n \equiv 11 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)P_7Q_7 = C$",

$n \equiv 13 \pmod{21}$ için "$h_n = C \Leftrightarrow (\alpha-1)Q_7^2 = C$",

$n \equiv 14 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)Q_7^2 = C$",

$n \equiv 15 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)P_7Q_7^2 = C$",

$n \equiv 16 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2P_7Q_7^2 = C$",

$n \equiv 17,19 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)P_7Q_7^2 = C$",

$n \equiv 18 \pmod{21}$ için "$h_n = C \Leftrightarrow \alpha^2P_7Q_7^2 = C$".

$N = 8$ Hali: $n \equiv 0 \pmod{24}$ için "$h_n = C$",

$n \equiv 1 \pmod{24}$ için "$h_n = C \Leftrightarrow P_8 = C$",

$n \equiv 2,6 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)P_8 = C$",

$n \equiv 3,5 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2P_8 = C$",

$n \equiv 4 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2(2\alpha-1)^2P_8 = C$",

$n \equiv 7 \pmod{24}$ için "$h_n = C \Leftrightarrow Q_8 = C$",

$n \equiv 8 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)Q_8 = C$",

$n \equiv 9 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2P_8Q_8 = C$",

$n \equiv 10 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)P_8Q_8^2 = C$",

$n \equiv 11,19 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)P_8Q_8^2 = C$",

$n \equiv 12 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)(2\alpha-1)^2P_8Q_8 = C$",

$n \equiv 13 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2P_8Q_8 = C$",

$n \equiv 14 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)P_8Q_8 = C$",

$n \equiv 15 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2Q_8^2 = C$",

$n \equiv 16 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)Q_8^2 = C$",

$n \equiv 17 \pmod{24}$ için "$h_n = C \Leftrightarrow P_8Q_8^2 = C$",

$n \equiv 18 \pmod{24}$ için "$h_n = C \Leftrightarrow (2\alpha-1)P_8Q_8^2 = C$",

$n \equiv 20 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2(2\alpha-1)^2P_8Q_8^2 = C$",

$n \equiv 21 \pmod{24}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2P_8Q_8^2 = C$",

$n \equiv 22 \pmod{24}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)P_8Q_8^2 = C$".

$N = 9$ Hali: $n \equiv 0 \pmod{27}$ için "$h_n = C$",

$n \equiv 1,3 \pmod{27}$ için "$h_n = C \Leftrightarrow P_9 = C$",

$n \equiv 2,7 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)(\alpha^2-\alpha+1)P_9 = C$",

$n \equiv 4 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(\alpha^2-\alpha+1)^2P_9 = C$",

$n \equiv 5 \pmod{27}$ için "$h_n = C \Leftrightarrow (\alpha^2-\alpha+1)^2P_9 = C$",

$n \equiv 6 \pmod{27}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2P_9 = C$",

$n \equiv 8 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2Q_9 = C$",

$n \equiv 9 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)Q_9 = C$",

$n \equiv 10 \pmod{27}$ için "$h_n = C \Leftrightarrow P_9Q_9 = C$",

$n \equiv 11 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha^2-\alpha+1)P_9Q_9 = C$",

$n \equiv 12 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)P_9Q_9 = C$",

$n \equiv 13 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(\alpha^2-\alpha+1)^2P_9Q_9 = C$",

$n \equiv 14 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2(\alpha^2-\alpha+1)^2P_9Q_9 = C$",

$n \equiv 15 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha P_9Q_9 = C$",

$n \equiv 16 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)(\alpha^2-\alpha+1)P_9Q_9 = C$",

$n \equiv 17 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)Q_9^2 = C$",

$n \equiv 18 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2(\alpha^2-\alpha+1)Q_9^2 = C$",

$n \equiv 19 \pmod{27}$ için "$h_n = C \Leftrightarrow P_9Q_9^2 = C$",

$n \equiv 20 \pmod{27}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(\alpha^2-\alpha+1)P_9Q_9^2 = C$",

$n \equiv 21 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)^2P_9Q_9^2 = C$",

$n \equiv 22 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(\alpha^2-\alpha+1)^2P_9Q_9^2 = C$",

$n \equiv 23 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)(\alpha^2-\alpha+1)^2P_9Q_9^2 = C$",

$n \equiv 24 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)P_9Q_9^2 = C$",

$n \equiv 25 \pmod{27}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha-1)(\alpha^2-\alpha+1)P_9Q_9^2 = C$".

$N = 10$ Hali: $n \equiv 0 \pmod{30}$ için "$h_n = C$",

$n \equiv 1 \pmod{30}$ için "$h_n = C \Leftrightarrow P_{10} = C$",

$n \equiv 2 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)\varsigma P_{10} = C$",

$n \equiv 3 \pmod{30}$ için "$h_n = C \Leftrightarrow \varsigma P_{10} = C$",

$n \equiv 4 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)^2P_{10} = C$",

$n \equiv 5 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha P_{10} = C$",

$n \equiv 6 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(2\alpha-1)^2\varsigma^2 P_{10} = C$",

$n \equiv 7 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)P_{10} = C$",

$n \equiv 8 \pmod{30}$ için "$h_n = C \Leftrightarrow (2\alpha-1)\varsigma P_{10} = C$",

$n \equiv 9 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)^2\varsigma Q_{10} = C$",

$n \equiv 10 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)\varsigma^2 Q_{10} = C$",

$n \equiv 11 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2 P_{10}Q_{10} = C$",

$n \equiv 12 \pmod{30}$ için "$h_n = C \Leftrightarrow \varsigma^2 P_{10}Q_{10} = C$",

$n \equiv 13 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)P_{10}Q_{10} = C$",

$n \equiv 14 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)^2 P_{10}Q_{10} = C$",

$n \equiv 15 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(2\alpha-1)^2\varsigma P_{10}Q_{10} = C$",

$n \equiv 16 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)\varsigma P_{10}Q_{10} = C$",

$n \equiv 17 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)P_{10}Q_{10} = C$",

$n \equiv 18 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2\varsigma^2 P_{10}Q_{10} = C$",

$n \equiv 19 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)Q_{10}^2 = C$",

$n \equiv 20 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)\varsigma^2 Q_{10}^2 = C$",

$n \equiv 21 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)^2\varsigma P_{10}Q_{10}^2 = C$",

$n \equiv 22 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2(2\alpha-1)\varsigma P_{10}Q_{10}^2 = C$",

$n \equiv 23 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)P_{10}Q_{10}^2 = C$",

$n \equiv 24 \pmod{30}$ için "$h_n = C \Leftrightarrow (2\alpha-1)\varsigma P_{10}Q_{10}^2 = C$",

$n \equiv 25 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)P_{10}Q_{10}^2 = C$",

$n \equiv 26 \pmod{30}$ için "$h_n = C \Leftrightarrow \alpha\varsigma P_{10}Q_{10}^2 = C$",

$n \equiv 27 \pmod{30}$ için "$h_n = C \Leftrightarrow \varsigma P_{10}Q_{10}^2 = C$",

$n \equiv 28 \pmod{30}$ için "$h_n = C \Leftrightarrow (\alpha-1)(2\alpha-1)\varsigma P_{10}Q_{10}^2 = C$".

$N = 12$ Hali: $n \equiv 0 \pmod{36}$ için "$h_n = C$",

$n \equiv 1 \pmod{36}$ için "$h_n = C \Leftrightarrow P_{12} = C$",

$n \equiv 2 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2\lambda\theta P_{12} = C$",

$n \equiv 3 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)^2 P_{12} = C$",

$n \equiv 4 \pmod{36}$ için "$h_n = C \Leftrightarrow \lambda^2 \theta^2 P_{12} = C$",

$n \equiv 5 \pmod{36}$ için "$h_n = C \Leftrightarrow \theta^2 P_{12} = C$",

$n \equiv 6 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2(2\alpha - 1)\lambda P_{12} = C$",

$n \equiv 7 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2(2\alpha - 1)\theta P_{12} = C$",

$n \equiv 8 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)^2(2\alpha - 1)^2 P_{12} = C$",

$n \equiv 9 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2 P_{12} = C$",

$n \equiv 10 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)(2\alpha - 1)\lambda P_{12} = C$",

$n \equiv 11 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)(2\alpha - 1)^2 \theta Q_{12} = C$",

$n \equiv 12 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha Q_{12} = C$",

$n \equiv 13 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)^2(2\alpha - 1)\theta^2 P_{12}Q_{12} = C$",

$n \equiv 14 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(2\alpha - 1)^2 \lambda\theta^2 P_{12}Q_{12} = C$",

$n \equiv 15 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2 P_{12}Q_{12} = C$",

$n \equiv 16 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)^2(2\alpha - 1)\lambda^2 \theta P_{12}Q_{12} = C$",

$n \equiv 17 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)(2\alpha - 1)^2 P_{12}Q_{12} = C$",

$n \equiv 18 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)^2(2\alpha - 1)\lambda P_{12}Q_{12} = C$",

$n \equiv 19 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2(2\alpha - 1)^2 P_{12}Q_{12} = C$",

$n \equiv 20 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(2\alpha - 1)\theta P_{12}Q_{12} = C$",

$n \equiv 21 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)^2 P_{12}Q_{12} = C$",

$n \equiv 22 \pmod{36}$ için "$h_n = C \Leftrightarrow (2\alpha - 1)^2 \lambda\theta^2 P_{12}Q_{12} = C$",

$n \equiv 23 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2(2\alpha - 1)\theta^2 {Q_{12}}^2 = C$",

$n \equiv 24 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2 {Q_{12}}^2 = C$",

$n \equiv 25 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)(2\alpha - 1)^2 \theta P_{12}{Q_{12}}^2 = C$",

$n \equiv 26 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)(2\alpha - 1)\lambda P_{12}{Q_{12}}^2 = C$",

$n \equiv 27 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha^2(\alpha - 1)^2 P_{12}{Q_{12}}^2 = C$",

$n \equiv 28 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha - 1)(2\alpha - 1)^2 \lambda^2 P_{12}{Q_{12}}^2 = C$",

$n \equiv 29 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha - 1)^2(2\alpha - 1)\theta P_{12}{Q_{12}}^2 = C$",

$n \equiv 30 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha(\alpha-1)^2(2\alpha-1)\lambda P_{12}{Q_{12}}^2 = C$",

$n \equiv 31 \pmod{36}$ için "$h_n = C \Leftrightarrow \alpha\theta^2 P_{12}{Q_{12}}^2 = C \Rightarrow h_n = C$",

$n \equiv 32 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha-1)\theta^2 P_{12}{Q_{12}}^2 = C$",

$n \equiv 33 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2\theta^2 P_{12}{Q_{12}}^2 = C$",

$n \equiv 34 \pmod{36}$ için "$h_n = C \Leftrightarrow (\alpha-1)^2\lambda\theta P_{12}{Q_{12}}^2 = C$".

İspat. Tekrardan kaçınmak amacıyla sadece $N = 4$ hali için ispat verilecektir. Diğer haller de genel terim formülü kullanılarak benzer şekilde ispat edilebilir.

i. $n \equiv 0 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k$ dır. Teorem 3.5.2 de $N = 4$ hali için verilen genel terim formülü kullanılarak

$$h_n = \alpha^{18k^2}{Q_4}^{3k}$$

olarak elde edilir. Bu eşitlikten "$h_n = C$" olduğu görülür.

ii. $n \equiv 1 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 1$ dir. Teorem 3.5.2 de $N = 4$ hali için verilen genel terim formülü kullanılarak,

$$h_n = \alpha^{54k^2+9k} P_4 {Q_4}^{3k}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow P_4 = C$" olduğu görülür.

iii. $n \equiv 2 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 2$ dir. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+18k+1} P_4 {Q_4}^{3k}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow \alpha P_4 = C$" olduğu görülür.

iv. $n \equiv 3 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 3$ dür. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+27k+3} {Q_4}^{3k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow Q_4 = C$" olduğu görülür.

v. $n \equiv 4 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 4$ dür. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+36k+6} {Q_4}^{3k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow Q_4 = C$" olduğu görülür.

vi. $n \equiv 5 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 5$ dir. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+45k+9} P_4 Q_4^{3k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow P_4Q_4 = C$" olduğu görülür.

vii. $n \equiv 6 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 6$ dır. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+54k+13} P_4 Q_4^{3k+1}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow \alpha P_4Q_4 = C$" olduğu görülür.

viii. $n \equiv 7 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 7$ dir. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+63k+18} Q_4^{3k+2}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow Q_4^2 = C$" olduğu görülür.

ix. $n \equiv 8 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 8$ dir. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+72k+24} Q_4^{3k+2}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow Q_4^2 = C$" olduğu görülür.

x. $n \equiv 9 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 9$ dur. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+81k+30} P_4 Q_4^{3k+2}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow P_4Q_4^2 = C$" olduğu görülür.

xi. $n \equiv 10 \pmod{12}$ ise $k \in \mathbb{N}$ olmak üzere $n = 12k + 10$ dur. Genel terim formülü yardımıyla,

$$h_n = \alpha^{54k^2+90k+37} P_4 Q_4^{3k+2}$$

olarak elde edilir. Bu eşitlikten "$h_n = C \Leftrightarrow \alpha P_4Q_4^2 = C$" olduğu görülür.

3.6.6 Örnek. $N = 5$ için $\alpha = 5$ olarak seçilmesi halinde

$$E_5 : y^2 - 4xy - 5y = x^3 - 5x^2$$

eliptik eğrisi elde edilir. Bu eliptik eğri üzerindeki $P = (0, 0)$ ve singüler olmayan $Q = (2, 12)$ noktaları kullanılarak E_5 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisinin $n = 150, \ldots, 160$ için Teorem 3.5.2 yardımıyla elde edilen terimleri, $h_{-1} = h_0 = 1$ olmak üzere, aşağıdaki gibi elde edilir:

$$h_{150} = 2^{150}\, 5^{9000}$$
$$h_{151} = -2^{151}\, 5^{9120}$$
$$h_{152} = -2^{152}\, 3\, 5^{9241}$$
$$h_{153} = -2^{153}\, 5^{9363}$$
$$h_{154} = 2^{155}\, 5^{9486}$$
$$h_{155} = 2^{155}\, 5^{9610}$$
$$h_{156} = -2^{156}\, 5^{9734}$$
$$h_{157} = -2^{157}\, 3\, 5^{9859}$$
$$h_{158} = -2^{158}\, 5^{9985}$$
$$h_{159} = 2^{160}\, 5^{10112}$$
$$h_{160} = 2^{160}\, 5^{10240}$$

Dizinin yukarıdaki terimleri dikkate alındığında, dizinin h_{150}, h_{156}, h_{160} ve h_{159} terimlerinin birer tam kare oldukları görülmektedir.

$150 \equiv 0 \pmod{10}$, $160 \equiv 0 \pmod{10}$ olduğundan dizinin h_{150} ve h_{160} terimlerinin kare olması için herhangi bir seçim gerekmemektedir. Benzer durum $159 \equiv -1 \pmod{10}$ olduğundan h_{159} terimi için de söz konusudur. Diğer yandan, $156 \equiv 6 \pmod{10}$ olduğundan h_{156} teriminin bir tam kare olması için gerekli ve yeterli koşulun $P_5Q_5 = \square$ olduğu görülür, bu halde E_5 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisi için

$$P_5 = x = 2 \text{ ve } Q_5 = x^2 - xy - y = -32$$

olduğundan $P_5Q_5 = \square$ dir.

Dikkat edilirse, (h_n) Somos 4 dizisinin h_{150} terimi bir küp sayıdır ve üstelik $150 \equiv 0 \pmod{15}$ denkliği gerçeklenmektedir. Dizinin bir diğer küp terimi ise h_{153} terimidir ve Teorem 3.6.5 gereği $P_5 = C$ olması beklenir. Gerçekten de E_5 eliptik eğrisi ile eşleşen (h_n) Somos 4 dizisi için $n = 153$ olmak üzere

$$P_5 = x^2 - y = 2^2 - 12 = -8$$

olarak elde edilir ve böylece $P_5 = C$ dir.

KAYNAKLAR

Bremner, A., Tzanakis, N. 2004. Lucas sequences whose 12th and 9th term is a square. *Journal of Number Theory*, 107: 215-227.

Bremner, A., Tzanakis, N. 2007. On squares in Lucas sequences. *Journal of Number Theory*, 124: 511-520.

Charlap, L. S., Robbins, D. P. 1988. An elementary introduction to elliptic curves. Technical Report 31, Institute for Defense Analysis, Princeton.

Dubner, H., Keller, W. 1999. New Fibonacci and Lucas primes. *Math. Comp*, 68(225): 417-427.

Everest, G., Van der Poorten, A. J., Shparlinski, I., Ward, T. 2003. Recurrence sequences. American Mathematical Society, USA, 320 pp.

Fomin, S., Zelevinsky, A. 2002. The Laurent phenomenon. *Adv. Appl. Math.*, 28: 119-144.

Gale, D. 1991. The strange and suprising saga of the Somos sequences. *Mathematical Intelligencer*, 13(1): 40-42.

Gale, D. 1991. Somos sequence update. *Mathematical Intelligencer*, 13(4): 49-50.

Gezer, B. 2013. Elliptic divisibility sequences, squares and cubes. *Publ. Math. Debrecen*, 83(3): 481-515.

Gezer, B., Capa, B., Bizim, O. 2015. A family of integer Somos sequences. *Mathematical Reports*. (Kabul edildi)

Hone, A. N. W., Swart, C. 2008. Integrality and the Laurent phenomenon for Somos 4 and Somos 5 sequences. *Math. Proc. of the Cambridge Phil. Soc.*, 145: 65-85.

Husemöller, D. 2004. Elliptic curves, Springer, Germany, 487 pp.

Kubert, D. S. 1976. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc.*, 33(3): 193-237.

Malouf, J. L. 1992. An integer sequence from a rational recursion. *Discrete Mathematic*, 110: 257-261.

Mazur, B. 1978. Modular curves and the Eisenstein ideal. *IHES Publ. Math.*, 47: 33-186.

Propp, J. The Somos sequence site, www.math.wisc.edu/propp/somos.html.

Ribenboim, P., McDaniel, W. L. 1996. The square terms in Lucas sequences. *Journal of Number Theory*, 58: 104-123.

Robinson, R. M. 1992. Periodicity of Somos sequences. *Proc. Amer. Math. Soc*, 116: 613-619.

Shipsey, R. 2000. Elliptic divisibility sequences. *Ph.D. Thesis*, Department of Mathematical and Computing Sciences, Goldsmith's College, University of London, UK.

Shorey, T. N., Tijdeman, R. 1986. Exponential Diophantine equations, Cambridge University Press, Cambridge, 252 pp.

Silverman, J. H. 1986. The arithmetic of elliptic curves, Springer, Germany, 402 pp.

Somos, M. 1989. Problem 1470. *Crux Mathematicorum*, 15: 208.

Swart, C. S. 2003. Elliptic curves and related sequences. *Ph.D. Thesis*, Royal Holloway and Bedford New College, University of London, UK.

Van der Porten, A. J., 2006. Hyperelliptic curves, continued fractions and Somos sequences. *IMS Lecture Notes-Monograph Series. Dynamics & Stochastics*, 48: 212-224.

Ward, M. 1948. Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70: 31-74.

Ward, M. 1948. The law of repetition of primes in an elliptic divisibility sequences. *Duke Mathematical Journal*, 15: 941-946.

Washington, J. L., 2003. Elliptic curves, number theory and cryptography. Chapman&Hall/CRC, USA, 429 pp.

ÖZGEÇMİŞ

Adı Soyadı : Buse UZATICI
Doğum Yeri ve Tarihi : Eskişehir – 29.06.1988
Yabancı Dili : İngilizce

Eğitim Durumu
Lise : Eskişehir Muzaffer Çil Anadolu Lisesi, 2005
Lisans : Uludağ Üniversitesi Fen Edebiyat Fakültesi, 2009
Yüksek Lisans : Uludağ Üniversitesi Fen Bilimleri Enstitüsü, 2011
Doktora : Uludağ Üniversitesi Fen Bilimleri Enstitüsü, 2015

Çalıştığı Kurum/Kurumlar ve Yıl :
İletişim : capabuse@hotmail.com
Yayınları : **Gezer, B., Capa, B., Bizim, O. 2015.** A family of integer Somos sequences. *Mathematical Reports*. (Kabul edildi)