T.C.
KIRIKKALE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI
YÜKSEK LİSANS TEZİ

FİBONACCİ SAYILARININ BÖLÜNEBİLİRLİK ÖZELLİKLERİ

Elif KORAL

TEMMUZ 2018

Matematik Anabilim Dalında Elif KORAL tarafından hazırlanan FİBONACCİ SAYILARININ BÖLÜNEBİLİRLİK ÖZELLİKLERİ adlı Yüksek Lisans Tezinin Anabilim Dalı standartlarına uygun olduğunu onaylarım.

Anabilim Dalı Başkanı
Prof. Dr. Kerim KOCA

Bu tezi okuduğumu ve tezin **Yüksek Lisans Tezi** olarak bütün gereklilikleri yerine getirdiğini onaylarım.

Danışman
Doç. Dr. İlker AKKUŞ

Jüri Üyeleri

Başkan	:	Dr. Öğr. Üyesi Nil MANSUROĞLU
Üye	:	Doç. Dr. İlker AKKUŞ
Üye	:	Dr. Öğr. Üyesi Semih YILMAZ

05/07/2018

Bu tez ile Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onaylamıştır.

Prof. Dr. Mustafa YİĞİTOĞLU
Fen Bilimleri Enstitüsü Müdürü

Sevgilerle Canım Ailem...

ÖZET

FİBONACCİ SAYILARININ BÖLÜNEBİLİRLİK ÖZELLİKLERİ

KORAL, Elif
Kırıkkale Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı, Yüksek Lisans Tezi
Danışman: Doç. Dr. İlker AKKUŞ
Temmuz 2018, 82 sayfa

Bu tezde ilk önce çalışılan konu ve incelenen kaynaklar hakkında genel bilgiler verilerek, tam sayılarda bölünebilme ve özellikleri hakkında kısa bilgiler ifade edilmiş ve Fibonacci, Lucas ve genelleştirilmiş Fibonacci dizilerinin tanımları yapılmıştır.

Üçüncü bölümde Fibonacci sayılarının basit bölünebilirlik kuralları incelenmiş, ardından Fibonacci ve genelleştirilmiş Fibonacci sayılarının m modülüne göre periyot uzunluğu ve bunlar arasındaki ilişkiler incelenmiştir.

Takip eden bölümde Fibonacci dizisinin bazı aritmetik özellikleri, temel matris cebiri kullanılarak incelenmiş ve yine bu bölümde m modülüne göre periyot, kısıtlı periyot ve çarpan tanımları verilmiştir. Hemen ardından m modülüne göre periyot ve kısıtlı periyot arasındaki bağıntılar üzerinde durulmuştur.

Son bölümde Fibonacci dizisinin genel bölünebilirlik özellikleri ve Fibonacci sayılarının bir tam sayının kuvvetine bölündüğü zaman elde edilen kalan dizisinin periyodik yapısı ile ilgilenilmiştir.

Anahtar Kelimeler: Fibonacci dizisi, genelleştirilmiş Fibonacci dizisi, Lucas dizisi, periyot, kısıtlı periyot, m modülüne göre kalan dizisi, Fibonacci matrisi, katlı asal çarpan, basit asal çarpan.

ABSTRACT

DIVISIBILITY PROPERTIES OF THE FIBONACCI NUMBERS

KORAL, Elif
Kırıkkale University
Graduate School of Natural and Applied Sciences
Department of Mathematics, Master Thesis
Supervisor: Assoc. Prof. Dr. İlker AKKUŞ
July 2018, 82 pages

In this thesis, firstly the general information about the subject and the references that are examined are given, a brief information about the divisibility in integers and its properties are expressed and the Fibonacci, Lucas and the generalized Fibonacci sequences are defined.

In the third section, the simple divisibility rules of the Fibonacci numbers are examined, then the length of the period according to the modulo m of Fibonacci and generalized Fibonacci numbers and their relations are examined.

In the following section, some arithmetic properties of the Fibonacci sequence are examined using basic matrix algebra, and again in this section, period, restricted period and factor definitions are given according to modulo m. Immediately thereafter, the relation between the period and the restricted period according to the modulo m is focused on.

In the last part, general divisibility properties of Fibonacci sequence and the periodic structure of the remainder sequence obtained when the Fibonacci numbers are divided by a power of an integer are dealed.

Key Words: Fibonacci sequence, generalized Fibonacci sequence, Lucas sequence, period, restricted period, remainder sequence according to modulo m, Fibonacci matrix, multiple prime factor, simple prime factor.

TEŞEKKÜR

Tezimin hazırlanması süresince ve çalışmalarım esnasında hiçbir yardımını esirgemeyen, bana yol gösteren, büyük sabır ve anlayış sergileyen, tez yöneticisi hocam, Sayın Doç. Dr. İlker AKKUŞ'a, büyük fedakarlıklarla bana destek olan aileme, son olarak birçok konuda olduğu gibi, tezimi hazırlamam esnasında da yardımlarını esirgemeyen ve bilgilerini benimle paylaşan arkadaşım Hacer BOZDAĞ'a teşekkürlerimi sunuyorum.

İÇİNDEKİLER DİZİNİ

Sayfa

1. GİRİŞ

İtalyan Matematikçi Leonardo Fibonacci 1170 yılında Pisa'da doğmuştur ve çocukluğunun büyük kısmını babasının çalışmakta olduğu Cezayir'de geçirmiştir. Babasının yoğun ısrarı üzerine Arap bir hocadan matematik dersleri alarak matematik ile ilk burada tanışmıştır. Böylece Avrupa'da Roma rakamları kullanılırken ve sıfır kavramı ortada yokken küçük yaşlarda Arap rakamlarını ve sıfır rakamını yani ilk matematik bilgilerini Müslüman eğitimcilerden edinmiştir. Fibonacci Arap sayı sisteminin mükemmelliği karşısında öğrendiklerini abaküs kitabı veya hesaplama kitabı anlamına gelen "Liber Abaci" adlı kitabında toplamıştır. Böylece bu kitap matematiğin Müslümanlardan taşındığı ilk eser olmuştur. Fibonacci ticaret ile ilgili olan bu kitapta aritmetik işlemler ve cebir konularına yer vermiştir. Ayrıca Arap sayı sistemini yani bugün kullanılan ondalık sayı sistemini bu kitapta tanıtmıştır. Bu kitapta bulunan "Tavşan Problemi", Fibonaccinin günümüzde en önemli matematikçilerden biri olmasını sağlamıştır. Fibonacci bu kitabında kapalı bir ortamda bulunan tavşan ailesinin artışını her ay gözlemlemiştir ve sonuçları notlar halinde toparlamıştır. Leonardo "Her tavşan çifti ayda bir kez bir çift tavşan yavrularsa ve bu yavrular da ikinci aydan itibaren yavrulamaya başlarsa bir yıl sonunda kaç çift tavşan olur?" problemi ile her aydaki tavşan çift sayısının rastgele olmayıp bir aydaki çift sayısının önceki iki ayın toplamına eşit olduğunu fark etmiştir. Bu durumda tavşan çift sayıları aylara göre bir yıl içinde $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$ olacaktır. Böylece her sayının kendinden önce gelen sayı ile toplanarak bir sonrakinin elde edildiği meşhur sayı dizisi ortaya çıkmıştır.

Fibonacci sayılarının daha küçük elemanları bitkilerde, böceklerde, çiçeklerde vb. doğadaki birçok oluşumun düzeninde bulunmaktadır.

Ayrıca bu sayı dizisi "Altın Oranı" kapsar ve birçok bilimsel araştırmaya dayanak teşkil eder. Fibonacci dizisinin bir terimi öncekine bölündüğünde ve sayı büyüdükçe bölümün bir irrasyonel sayı olan $(1 + \sqrt{5})/2 = 1{,}61803398 \ldots$ sayısına yakınsadığı görülür ve bu sayıya "Altın Oranı" denir. Bu oran oyun kartlarından piramitlerin yapımına kadar birçok alanda kullanılmıştır.

Son olarak Fibonacci sayıları pek çok sayı teorisinde kullanılmıştır. Fibonacci sayıları ile ilgili araştırma yapmak için Fibonacci Derneği kurulmuştur. 1963 yılından beri "The Fibonacci Quarterly" dergisinde bu sayı dizisi ile ilgili araştırmalar yayınlanmaktadır. Bu araştırmaların bazısı bilinen, bazısı ileri sürülüp ispatlanamayan ve bilinmeyip keşfedilmeyi bekleyen pek çok özelliğe sahiptir.

Bu sayı dizisinin terimleri, ilk iki terim bilindiğinde $F_{n+2} = F_n + F_{n+1}$ bağıntısı kullanılarak hesaplanmaktadır. Fibonacci dizisi $F_0 = 0$ ve $F_1 = 1$ ile başlar. Ancak başlangıç değerlerinin özel bir yanı olmadığından başka değerler de alınabilir ve tümüyle farklı bir sayı dizisi elde edilebilir. Fransız matematikçi Edward Lucas başlangıç değerleri için $L_0 = 2,\ L_1 = 1$ sayılarını alarak Lucas sayı dizisini elde etmiştir.

1.1. Kaynak Özetleri

Bu tezin hazırlanışında öncelikle [1, 5-8] nolu kaynaklardan Fibonacci sayılarının temel özellikleri, bölünebilirlik özellikleri hakkında bilgi edinildi. [2] nolu kaynaktan Fibonacci ve genelleştirilmiş Fibonacci sayılarının m modülüne göre kalan dizisinin periyodu ve bunlar arasındaki ilişki hakkında bilgi edinildi. [3] nolu kaynaktan yararlanarak Fibonacci sayılarının bazı özellikleri temel matris cebiri kullanılarak incelendi. [3-5] nolu kaynaklardan Fibonacci sayılarının m modülüne göre periyodikliği, buna bağlı temel kavramları ve ilişkileri hakkında bilgi edinildi.

1.2. Tezin Amacı

Bu tezin amacı Fibonacci dizileri ve genelleştirilmiş Fibonacci dizilerinin bölünebilirlik özelliklerini incelemektir. Ayrıca kendi içinde ve aralarında m modülüne göre periyot ve kısıtlı periyotları arasında ilişki kurmaktır.

2. TEMEL KAVRAMLAR

2.1. Tam Sayılarda Bölünebilme ve Özellikleri

2.1.1. Bölme Algoritması

Bir a tam sayısı pozitif bir b tam sayısı ile bölündüğünde $0 \leq r < b$ olmak üzere bir q bölümü ve r kalanı vardır. Burada a ya bölünen, b ye bölen sayı denir ve $0 \leq r < b$ için $a = bq + r$ şeklinde yazılır.

Bölme algoritmasında $r = 0$ alınırsa $a = bq$ bulunur. Bu ifade "b böler a yı" veya "b, a nın bir çarpanı" şeklinde okunur ve $b \mid a$ ile gösterilir. Eğer b, a nın bir çarpanı değilse "b, a yı bölmez" denir ve $b \nmid a$ ile gösterilir.

2.1.2. Bölünebilme Özellikleri

1. a ve b pozitif tam sayıları için $a \mid b$ ve $b \mid a$ ise $a = b$ dir.

2. Herhangi a, b, c, m ve n tam sayıları için

(i) $a \mid b$ ve $b \mid c$ ise $a \mid c$,

(ii) $a \mid b$ ise $a \mid bc$,

(iii) $a \mid b$ ve $a \mid c$ ise $a \mid (bm + cn)$ dir.

2.1.3. En Büyük Ortak Bölen

Sıfırdan farklı a ve b tam sayılarını ortak bölen tam sayılar arasında en büyük olan tam sayıya en büyük ortak bölen denir ve (a, b) ile gösterilir.

1. $(a, b) = d$ ise $d \mid a$ ve $d \mid b$,

2. $(a, b) = 1$ ve $a \mid bc$ ise $a \mid c$ dir.

3. $(a, b) = d$ ise $am + bn = d$ olacak şekilde m ve n pozitif tam sayıları vardır.

4. p asal sayısı için $p \mid ab$ ise $p \mid a$ veya $p \mid b$ dir.

2.1.4. En Küçük Ortak Kat

Sıfırdan farklı a ve b tam sayılarının ortak katı olan tam sayılar arasında en küçük olan pozitif tam sayıya en küçük ortak kat denir ve $[a, b]$ ile gösterilir.

1. $[a, b] = d$ ise $a \mid d$ ve $b \mid d$,

2. a ve b pozitif tam tam sayı olmak üzere $(a, b)[a, b] = ab$ dir.

3. $(a, b) = 1$ olması için gerek ve yeter şart $[a, b] = ab$ olmasıdır.

2.1.5. Binom Teoremi

x, y reel sayı ve n doğal sayı olmak üzere

$$(x + y)^n = \sum_{t=0}^{n} \binom{n}{t} y^t x^{n-t}$$

dir.

2.2. Fibonacci, Lucas ve Genelleştirilmiş Fibonacci Sayıları

2.2.1. Fibonacci Dizisi

Fibonacci sayıları arasındaki ilişki $n \geq 2$ olmak üzere $F_0 = 0$ ve $F_1 = 1$ için $F_n = F_{n-1} + F_{n-2}$ lineer rekürans bağıntısı ile tanımlanır ve n. tam sayıya karşılık gelen Fibonacci sayısı F_n ile gösterilir. Bu bağıntı ile dizinin terimleri 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, … olacaktır.

2.2.2. Lucas Dizisi

Lucas sayıları arasındaki ilişki $n \geq 2$ olmak üzere $L_0 = 2$ ve $L_1 = 1$ için $L_n = L_{n-1} + L_{n-2}$ lineer rekürans bağıntısı ile tanımlanır ve n. tam sayıya karşılık

gelen Lucas sayısı L_n ile gösterilir. Bu bağıntı ile dizinin terimleri $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$ olacaktır.

2.2.3. Genelleştirilmiş Fibonacci Dizisi

Genelleştirilmiş Fibonacci sayıları arasındaki ilişki $n \geq 2$ olmak üzere $G_0 = a$ ve $G_1 = b$ için $G_n = G_{n-1} + G_{n-2}$ lineer rekürans bağıntısı ile tanımlanır ve n. tam sayıya karşılık gelen genelleştirilmiş Fibonacci sayısı G_n ile gösterilir. Bu bağıntı ile dizinin terimleri $a, b, a+b, a+2b, 2a+3b, 3a+5b, \ldots$ olacaktır. Ayrıca genelleştirilmiş Fibonacci sayıları ile Fibonacci sayıları arasındaki ilişki $G_n = bF_n + aF_{n-1}$ şeklinde verilir.

2.3. Fibonacci ve Lucas Dizilerinin Binet Formülleri

$x^2 - x - 1 = 0$ karakteristik denkleminin kökleri

$$A = \frac{1+\sqrt{5}}{2} \text{ ve } B = \frac{1-\sqrt{5}}{2}$$

ve $n \in \mathbb{N}$ olmak üzere

1. $F_0 = 0$ ve $F_1 = 1$ için n. Fibonacci sayısı $F_n = \frac{A^n - B^n}{A-B}$ binet formülüyle

2. $L_0 = 2$ ve $L_1 = 1$ için n. Lucas sayısı $L_n = \frac{A^n + B^n}{A+B}$, $A + B = 1$ olduğundan $L_n = A^n + B^n$ şeklinde binet formülü ile ifade edilir.

3. FİBONACCİ SAYILARININ BASİT BÖLÜNEBİLİRLİK KURALLARI

Fibonacci sayılarının bölünebilirlik özelliklerinden önce Fibonacci ve Lucas sayıları ile ilgili bazı özdeşlikler verilecektir.

Özdeşlik 1. $F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$ dir. (Cassini Özdeşliği)

Özdeşlik 2. $m \geq n \geq 1$ olmak üzere $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ dir.

Özdeşlik 3. $L_n = F_{n-1} + F_{n+1}$ dir.

Özdeşlik 4. $F_{2n} = F_nL_n$ dir.

Özdeşlik 5. $(F_m, F_{m-1}) = 1$ dir.

Bölünebilirlik Özellikleri

$F_{2n} = F_nL_n$ bağıntısından $F_n \mid F_{2n}$ dir. Bu durumda "Hangi koşul altında $F_i \mid F_j$ şeklinde bir genelleme yapılabilir?" sorusu merak konusu olmuştur. Bu koşulun bir sonraki teoremde $i \mid j$ olduğu gösterilecektir. Yani $i \mid j$ ise $F_i \mid F_j$ olur.

Teorem 3.1. $F_m \mid F_{mn}$ dir. [1]

İspat: Tümevarım yöntemi ile $F_m \mid F_{mn}$ ifadesi $n = 1$ için doğrudur. Bu ifadenin $n = k \geq 1$ olmak üzere 1 den k ya kadar olan tüm tam sayılar için doğru olduğunu kabul edelim. Bu durumda $k \geq 1$ ve her i için $1 \leq i \leq k$ olmak üzere $F_m \mid F_{mi}$ dir. Yani $F_m \mid F_{mk}$ dır. Son olarak $n = k + 1$ için $F_m \mid F_{m(k+1)}$ olduğunu gösterelim. Bunun için Özdeşlik 2 kullanılırsa

$$F_{m(k+1)} = F_{mk-1}F_m + F_{mk}F_{m+1}$$

elde edilir. Bu eşitlikte $F_m \mid F_m$ ve kabulden $F_m \mid F_{mk}$ olduğundan $F_m \mid F_{m(k+1)}$ bulunur. Sonuç olarak bu ifadenin $n \geq 1$ olmak üzere tüm tam sayılar için geçerli olduğu görülür. □

Sonuç 3.1. İndisi m nin katı olan her Fibonacci sayısı F_m ile bölünebilir. [1]

Teorem 3.2. $F_m \mid F_n$ ise $m \mid n$ dir. [1]

İspat: $F_m \mid F_n$ olsun. $m \geq n - m \geq 1$ olmak üzere Özdeşlik 2 kullanılırsa

$$F_n = F_{m+(n-m)} = F_{m-1}F_{n-m} + F_m F_{n-m+1}$$

elde edilir. Bu eşitlikte $F_m \mid F_m$ ve kabulden $F_m \mid F_n$ olduğundan $F_m \mid F_{m-1}F_{n-m}$ elde edilir. $(F_m, F_{m-1}) = 1$ olması nedeniyle $F_m \mid F_{n-m}$ olur. Benzer şekilde $m \geq n - 2m \geq 1$ için Özdeşlik 2 kullanılırsa

$$F_{n-m} = F_{m+(n-2m)} = F_{m-1}F_{n-2m} + F_m F_{n-2m+1}$$

elde edilir ve $F_m \mid F_{n-m}$ ve $F_m \mid F_m$ olduğundan $F_m \mid F_{n-2m}$ olur. Bu şekilde devam edilirse $F_m \mid F_{n-qm}$ bulunur. Bölme algoritmasından $0 \leq t < m$ olmak üzere $n = qm + t$ için $n - qm = t$ ve $F_m \mid F_{n-qm}$ ifadesinden $F_m \mid F_t$ olur. Burada $0 \leq t < m$ olduğundan $t = 0$ olmalıdır. Böylece $n = qm$ olur ve $m \mid n$ bulunur. □

Sonuç 3.2. Teorem 3.1 ve Teorem 3.2 den $F_m \mid F_n$ olması için gerek ve yeter şart $m \mid n$ olmasıdır. [1]

Örnek 3.1. $k \geq 3$ olduğunda F_n nin başka bir F_k ya bölünebilir olma olasılığını bulalım. [1]

Çözüm: Sonuç 3.1 ile $F_3 \mid F_{3m}$ olur. Yani indisi üçün katı olan her Fibonacci sayısı 2 ile bölünebilir. Bu durumda F_n nin $F_3 = 2$ ile bölünebilme olasılığı $1/3$ ve F_n nin $F_4 = 3$ ile bölünebilme olasılığı $1/4$ olur. F_n nin $F_4 = 3$ ile bölünebilme ve $F_3 = 2$ ile bölünememe olasılığı $1/4 \cdot 2/3 = 2/(3 \cdot 4)$ bulunur. F_n nin $F_5 = 5$ ile bölünebilme ve 2 ya da 3 ile bölünememe olasılığı $1/5 \cdot 2/3 \cdot 3/4 = 2/(4 \cdot 5)$ olur. $3 \leq j < k$ iken F_n nin F_k ile bölünebilme ve F_j ile bölünememe olasılığı genellenirse $2/[(k-1)k]$ olur. $k \geq 3$ iken F_n nin F_k ile bölünebilme olasılıklarının toplamı

$$\sum_{i=2}^{k-1} \frac{2}{i(i+1)} = 2\sum_{i=2}^{k-1}\left(\frac{1}{i} - \frac{1}{i+1}\right)$$

$$= 2\left(\frac{1}{2} - \frac{1}{k}\right) = \frac{k-2}{k}$$

elde edilir ve bu toplam $k \to \infty$ iken 1 e yaklaşır.

Lemma 3.1. $\left(F_{qn-1}, F_n\right) = 1$ dir. [1]

İspat: $d \in \mathbb{Z}^+$ için $d = (F_{qn-1}, F_n)$ olsun. Böylece $d \mid F_{qn-1}$ ve $d \mid F_n$ olur. Buradan $d \mid F_n$ ve Teorem 3.1 den $F_n \mid F_{qn}$ olduğundan $d \mid F_{qn}$ bulunur. Sonuç olarak $d \mid F_{qn-1}$, $d \mid F_{qn}$ ve $\left(F_{qn-1}, F_{qn}\right) = 1$ olduğundan $d \mid \left(F_{qn-1}, F_{qn}\right) = 1$ olmalıdır. Yani $\left(F_{qn-1}, F_n\right) = d = 1$ dir. □

Lemma 3.2. $m = qn + t$ olmak üzere $(F_m, F_n) = (F_n, F_t)$ dir. [1]

İspat: $(F_m, F_n) = \left(F_{qn+t}, F_n\right) = (F_{qn-1}F_t + F_{qn}F_{t+1}, F_n)$ (Özdeşlik 2 ile)

$= (F_{qn-1}F_t, F_n)$ (Lemma 3.1 ile)

$= (F_t, F_n)$. □

Teorem 3.3. $(F_m, F_n) = F_{(m,n)}$ dir. [1]

İspat: Öklid bölme algoritmasından, $m \geq n$ ve "m" bölünen, "n" bölen olsun. m sayısı n sayısı ile bölünerek

$$\begin{aligned} m &= q_0 n + t_1, & 0 \leq t_1 < n \\ n &= q_1 t_1 + t_2, & 0 \leq t_2 < t_1 \\ t_1 &= q_2 t_2 + t_3, & 0 \leq t_3 < t_2 \\ &\vdots \\ t_{n-2} &= q_{n-1} t_{n-1} + t_n, & 0 \leq t_n < t_{n-1} \\ t_{n-1} &= q_n t_n + 0 \end{aligned}$$

olur ve Lemma 3.2 den $(F_m, F_n) = \left(F_n, F_{t_1}\right) = \left(F_{t_1}, F_{t_2}\right) = \cdots = (F_{t_{n-1}}, F_{t_n})$ yazılır. Ayrıca $t_n \mid t_{n-1}$ olduğundan Teorem 3.1 den $F_{t_n} \mid F_{t_{n-1}}$ olur. Böylece $\left(F_{t_{n-1}}, F_{t_n}\right) = F_{t_n}$ olur ve $(F_m, F_n) = (F_{t_{n-1}}, F_{t_n})$ olduğundan $(F_m, F_n) = F_{t_n}$ elde edilir. Son olarak Öklid bölme algoritması ile $(m, n) = t_n$ olduğundan $(F_m, F_n) = F_{(m,n)}$ bulunur. □

Sonuç 3.3. m ile n aralarında asal sayı ise F_m ile F_n Fibonacci sayıları da aralarında asal sayı olur. [1]

İspat: $(m, n) = 1$ ise Teorem 3.3 den $(F_m, F_n) = F_{(m,n)} = F_1 = 1$ olur. Yani $(F_m, F_n) = 1$ dir. □

Sonuç 3.4. $(m, n) = 1$ ise $F_m F_n \mid F_{mn}$ dir. [1]

İspat: $(m, n) = 1$ olsun. Teorem 3.1 den $F_m \mid F_{mn}$ ve $F_n \mid F_{mn}$ olduğundan $[F_m, F_n] \mid F_{mn}$ olur. Sonuç 3.3 den $(F_m, F_n) = 1$ olduğundan $[F_m, F_n] = F_m F_n$ bulunur ve $[F_m, F_n] \mid F_{mn}$ olduğundan $F_m F_n \mid F_{mn}$ elde edilir. □

Sonuç 3.5. $F_m \mid F_n$ ise $m \mid n$ dir. [1]

Alternatif İspat: $F_m \mid F_n$ olsun. Bu durumda $(F_m, F_n) = F_m$ olur. Teorem 3.3 den $(F_m, F_n) = F_{(m,n)} = F_m$ elde edilir. Böylece $F_{(m,n)} = F_m$ ifadesinden $(m, n) = m$ olur ve $m \mid n$ bulunur. □

Sonuç 3.6. Sonsuz çoklukta asal sayı vardır. [1]

İspat: Sonlu çoklukta $p_1, p_2, \dots, p_k$ olacak şekilde k tane asal sayı olduğunu varsayalım. Bu asal sayıları $F_{p_1}, F_{p_2}, \dots, F_{p_k}$ şeklindeki Fibonacci sayıları ile eşleştirelim. Asal sayılar $p_1, p_2, \dots, p_k$ aralarında asal olduğundan Sonuç 3.3 den Fibonacci sayılarının herhangi ikisi de aralarında asal sayı olur. Bu durumda k tane Fibonacci sayısı arasından her birinin diğer $(k-1)$ tane Fibonacci sayısıyla aralarında asal olduğu görülür. Böylece herhangi ikisinin ortak çarpanı yoktur. Bu durumda her birinin tek asal çarpanı olmalıdır. Ama $F_{19} = 4181 = 37 \cdot 113$ sayısının tek çarpanı olmadığından bir çelişki ortaya çıkmaktadır. Bu çelişkinin sebebi başta kabul ettiğimiz asal sayıların sonlu çoklukta olmasıdır. Yani asal sayılar sonsuz çokluktadır. □

Teorem 3.4. (Weinstein, 1966) Bir S kümesi alalım ve $F_1, F_2, \dots, F_{2n}$ Fibonacci sayıları arasından seçtiğimiz $(n+1)$ tane eleman ile S kümesini oluşturalım. Bu durumda S kümesinin içinde biri diğerini bölen iki eleman vardır. [6]

İspat: $1 \leq a_i \leq 2n$, $1 \leq i \leq n+1$ olmak üzere $S = \{F_{a_1}, F_{a_2}, \dots, F_{a_n}, F_{a_{n+1}}\}$ kümesi oluşturalım. Erdös Teoremi ile $A = \{a_1, a_2, \dots, a_n, a_{n+1}\} \subseteq \{1, 2, \dots, 2n\}$ olmak üzere $a_i \mid a_j$ olacak şekilde a_i ve a_j gibi iki eleman içerir. Böylece $a_i \mid a_j$ olduğundan $(a_i, a_j) = a_i$ ve Teorem 3.3 ile $(F_{a_i}, F_{a_j}) = F_{(a_i, a_j)} = F_{a_i}$ olur. Sonuç olarak $F_{a_i} \mid F_{a_j}$ bulunur. □

Teorem 3.5. $m \geq 2$ iken $2m \mid n$ olması için gerek ve yeter şart $L_m \mid F_n$ olmasıdır. [1]

İspat: $m \geq 2$ ve $2m \mid n$ olsun. Bu durumda $2m \mid n$ olduğundan Teorem 3.1 den $F_{2m} \mid F_n$ olur ve $F_{2m} = F_m L_m$ özdeşliğinden $L_m \mid F_{2m}$ olduğundan $L_m \mid F_n$ bulunur. □

Herhangi iki doğal sayı arasında belli bir oran varsa bunların Ebob ve Ekokları arasında ilişki vardır. Cross ve Renzi, $a:b = 2:3$ ise $[a,b] - (a,b) = a + b$ ve $a:b = 3:5$ ise $[a,b] + (a,b) = 2(a+b)$ olduğunu ispatladı. [8]

Buna göre $a:b = F_n : F_{n+1}$ ya da $a:b = L_n : L_{n+1}$ olduğunda $[a,b]$, (a,b) ve $(a+b)$ arasındaki ilişki Teorem 3.6 ve Teorem 3.7 de incelenecektir.

Teorem 3.6. (Freeman, 1967) a, b, c ve $d > 0$ olmak üzere
1. $a:b = F_n : F_{n+1}$ ve $n \geq 2$ için $(a+b)F_{n-1} = [a,b] + (-1)^n (a,b)$ dur.
2. $a:b = c:d$ ve $(c,d) = 1$ ve $n \geq 3$ için $(a+b)F_{n-1} = [a,b] + (-1)^n (a,b)$ ise $c:d$ oranının çözümlerinin sayısı $F_n F_{n-2}$ nin pozitif çarpanlarının sayısının yarısı kadardır ve $c:d$ oranlarından birisi de $F_n : F_{n+1}$ dir. [7]

İspat: a, b, c ve $d > 0$ olmak üzere
1. $a:b = F_n : F_{n+1}$ olsun. $(F_n, F_{n+1}) = 1$ olduğundan bazı $k \in \mathbb{Z}^+$ için $a = F_n k$ ve $b = F_{n+1} k$ olmak üzere $(a,b) = k$ ve $[a,b] = F_n F_{n+1} k$ olur. Böylece

$$(a+b) = F_n k + F_{n+1} k = k(F_n + F_{n+1})$$

$$(a+b)F_{n-1} = k(F_n + F_{n+1})F_{n-1}$$

$$= kF_{n+2}(F_{n+1} - F_n) = F_{n+1}F_{n+2}k - F_n F_{n+2} k$$

$$= F_{n+1}(F_n + F_{n+1})k - F_n F_{n+2} k$$

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

$$= F_{n+1}F_n k + k[F_{n+1}^2 - F_n F_{n+2})] \qquad \text{(Cassini özdeşliği ile)}$$

$$= F_{n+1}F_n k + k[-(-1)^{n+1}]$$

$$= [a,b] + (a,b)(-1)^n \text{ dir. } \square$$

2. $a:b=c:d$ ve $(c,d)=1$ olsun ve bazı $k\in\mathbb{Z}^+$ için $a=ck,\ b=dk$ olmak üzere $(a,b)=k$ ve $[a,b]=cdk$ olur ve Teorem 3.6 nın birinci kısmından

$$(a+b)F_{n-1}=[a,b]+(-1)^n(a,b)$$

$$(ck+dk)F_{n-1}=cdk+(-1)^nk$$

$$c\,(F_{n-1}-d)=(-1)^n-dF_{n-1}$$

$$c=\frac{dF_{n-1}-(-1)^n}{d-F_{n-1}}$$

$$c=\frac{dF_{n-1}-F_{n-1}^2+F_{n-1}^2-(-1)^n}{d-F_{n-1}}$$

$$c=F_{n-1}+\frac{F_{n-1}^2-(-1)^n}{d-F_{n-1}}$$

elde edilir ve Cassini özdeşliği ile $F_{n-2}F_n=F_{n-1}^2-(-1)^n$ olduğundan

$$c=F_{n-1}+\frac{F_{n-2}F_n}{d-F_{n-1}} \tag{3.1}$$

olur. Eğer $0<d<F_{n-1}$ olursa $c<0$ olur ve bu durum $c>0$ olması ile çelişir. Böylece $d>F_{n-1}$ olur ve c bir tam sayı olduğundan $(d-F_{n-1})\mid(F_{n-2}\,F_n)$ olur. Böylece Eşitlik 3.1 den $F_{n-2}F_n$ nin her pozitif çarpanı için c nin bir değeri bulunur ve $c:d$ oranının bir çözümü $c=A,\ d=B$ için $c=B,\ d=A$ olduğundan $c:d$ oranının farklı değerlerinin sayısı, $F_{n-2}F_n$ nin pozitif çarpanların sayısının yarısına eşittir.

Özel olarak Eşitlik 3.1 de $d=F_{n+1}$ alalım.

$$c=F_{n-1}+\frac{F_{n-2}F_n}{F_n}$$

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

elde edilir ve $c:d=F_n:F_{n+1}$ oranı bulunur. Böylece Teorem 3.6 daki ikinci önermenin özel halinin birinci önerme olduğu görülür. □

Örnek 3.2.

1. $a:b = F_n:F_{n+1}$, $n = 9$ ise $a:b = F_9:F_{10} = 34:55$ bulunur. Böylece $a = 34k$ ve $b = 55k$, $k = 7$ için $a = 238$, $b = 385$ alınırsa

$$[a,b] + (-1)^9(a,b) = 13090 - 7$$

$$= 13083 = (238 + 385) \cdot 21 = (a+b)F_8 \text{ dir.}$$

2. $[a,b] + (-1)^9(a,b) = (a+b)F_8$ olduğundan ve Eşitlik 3.1 de $n = 9$ alınırsa

$$c = F_8 + \frac{F_9F_7}{d - F_8}$$

$$c = 21 + \frac{34 \cdot 13}{d - 21} = 21 + \frac{442}{d - 21}$$

olur. Böylece $442 = 2 \cdot 13 \cdot 17$ olarak asal çarpanlarına ayrılırsa 1, 2, 13, 17, 26, 34, 221 ve 442 olmak üzere sekiz tane pozitif çarpana sahiptir. Bu durumda $(d - 21)$ ifadesi 1, 2, 13, 17, 26, 34, 221 ve 442 değerlerini aldığından d sayısı 22, 23, 34, 38, 47, 55, 242 ve 463 olmak üzere sekiz tane pozitif değere sahip olur. Sonuç olarak $c:d$ nin değerleri, $463:22$, $242:23$, $55:34$, $47:38$, $38:47$, $34:55$, $23:242$ ve $22:463$ dir. Dikkat edilirse pay ve paydalar yer değiştirmiştir. Bu durumda $c:d$ nin payı paydasından küçük olan dört farklı değeri $38:47$, $34:55$, $23:242$ ve $22:463$ dür. Ayrıca $c:d$ oranlarından birisi de $F_n:F_{n+1} = F_9:F_{10} = 34:55$ olduğu görülür.

Lemma 3.3. $n \geq 2$ için $F_{2n-1} = F_{n+1}L_{n+2} - L_nL_{n+1}$ dir. [1]

Lemma 3.4. $F_{2n-1} = F_nF_{n+1} - F_{n-2}F_{n-1}$ dir. [1]

Teorem 3.7. (Freeman, 1967)

1. $a:b = L_n:L_{n+1}$ alındığında $n \geq 2$ için $(a+b)F_{n+1} = [a,b] + (a,b)F_{2n-1}$,

2. $a:b = F_{n-2}:F_{n-1}$ alındığında $n \geq 3$ için $(a+b)F_{n+1} = [a,b] + (a,b)F_{2n-1}$ dir.

3. $a:b = c:d$ ve $(c,d) = 1$ alındığında ve $n \geq 2$ için

$(a+b)F_{n+1} = [a,b] + (a,b)F_{2n-1}$ ise $c:d$ oranları $F_{n+1}^2 - F_{2n-1}$ in pozitif çarpanları ile belirlenir. Bunlardan biri $L_n : L_{n+1}$ dir. Ayrıca $n \geq 3$ için $F_{n-2} : F_{n-1}$ de bir çözümdür. [7]

İspat:

1. $a:b = L_n : L_{n+1}$ olsun. $(L_n, L_{n+1}) = 1$ olduğundan bazı $k \in \mathbb{Z}^+$ için $a = L_n k$ ve $b = L_{n+1}k$ olmak üzere $(a,b) = k$ ve $[a,b] = L_n L_{n+1} k$ olur.

$$(a+b) = L_n k + L_{n+1}k = k(L_n + L_{n+1})$$

$$(a+b)F_{n+1} = k(L_n + L_{n+1})F_{n+1}$$

$$= kL_{n+2}F_{n+1} \qquad \text{(Lemma 3.3 ile)}$$

$$= (F_{2n-1} + L_n L_{n+1})k$$

$$= [a,b] + (a,b)F_{2n-1}. \square$$

2. $a:b = F_{n-2} : F_{n-1}$ olsun. $(F_{n-2}, F_{n-1}) = 1$ olduğundan bazı $k \in \mathbb{Z}^+$ için $a = F_{n-2}k$ ve $b = F_{n-1}k$ olmak üzere $(a,b) = k$ ve $[a,b] = F_{n-1}F_{n-2}k$ olur.

$$(a+b) = F_{n-2}k + F_{n-1}k = k(F_{n-2} + F_{n-1})$$

$$(a+b)F_{n+1} = kF_nF_{n+1} \qquad \text{(Lemma 3.4 ile)}$$

$$= (F_{2n-1} + F_{n-2}F_{n-1})k$$

$$= [a,b] + (a,b)F_{2n-1}. \square$$

3. $a:b = c:d$ ve $(c,d) = 1$ alındığında bazı $k \in \mathbb{Z}^+$ için $a = ck$ ve $b = dk$ olmak üzere $(a,b) = k$ ve $[a,b] = cdk$ olur ve Teorem 3.7 deki birinci kısımdan

$$(a+b)F_{n+1} = [a,b] + (a,b)F_{2n-1}$$

$$(ck+dk)F_{n+1} = cdk + kF_{2n-1}$$

$$c = \frac{dF_{n+1} - F_{n+1}^2 - F_{2n-1} + F_{n+1}^2}{d - F_{n+1}}$$

$$c = \frac{F_{n+1}(d - F_{n+1})}{d - F_{n+1}} + \frac{F_{n+1}^2 - F_{2n-1}}{d - F_{n+1}}$$

$$c = F_{n+1} + \frac{F_{n+1}^2 - F_{2n-1}}{d - F_{n+1}} \tag{3.2}$$

elde edilir. c ve d pozitif tam sayı olmak üzere $F_{n+1}^2 - F_{2n-1}$ in pozitif çarpanları $c:d$ oranını gösterir.

Özel olarak Eşitlik 3.2 de $d = L_{n+1}$ alınırsa ve Lemma 3.3 kullanılırsa

$$c = F_{n+1} + \frac{F_{n+1}^2 - (F_{n+1}L_{n+2} - L_n\, L_{n+1})}{L_{n+1} - F_{n+1}}$$

$$c = \frac{F_{n+1}L_{n+1} - F_{n+1}^2 + F_{n+1}^2 - F_{n+1}L_{n+2} + L_nL_{n+1}}{L_{n+1} - F_{n+1}}$$

$$c = \frac{F_{n+1}(L_{n+1} - L_{n+2}) + L_nL_{n+1}}{L_{n+1} - F_{n+1}}$$

$$c = \frac{-F_{n+1}L_n + L_nL_{n+1}}{L_{n+1} - F_{n+1}}$$

$$c = \frac{L_n(-F_{n+1} + L_{n+1})}{L_{n+1} - F_{n+1}} = L_n$$

olur ve $c:d = L_n:L_{n+1}$ oranı yine elde edilmiş olur. Yani bu oranın bir çözümü de $L_{n+1}:L_n$ dir. Böylece Teorem 3.7 deki üçüncü önermenin özel halinin birinci önerme olduğu görülür.

Teorem 3.6 dan farklı olarak $d > F_{n+1}$ için Teorem 3.7 ile tüm çözümler elde edilemez.

Eşitlik 3.2 de $d = F_{n-1}$ alalım.

$$c = F_{n+1} + \frac{F_{n+1}^2 - F_{2n-1}}{F_{n-1} - F_{n+1}}$$

$$c = \frac{F_{n+1}F_{n-1} - F_{n+1}^2 + F_{n+1}^2 - F_{2n-1}}{F_{n-1} - F_{n+1}}$$

Lemma 3.4 kullanılırsa

$$c = \frac{F_{n+1}F_{n-1} - (F_nF_{n+1} - F_{n-2}F_{n-1})}{F_{n-1} - F_{n+1}}$$

$$c = \frac{F_{n+1}F_{n-1} - F_nF_{n+1} + F_{n-2}F_{n-1}}{-F_n}$$

$$c = -\frac{F_{n+1}(F_{n-1} - F_n) + F_{n-2}F_{n-1}}{F_n}$$

$$c = -\frac{-F_{n+1}F_{n-2} + F_{n-2}F_{n-1}}{F_n}$$

$$c = \frac{F_{n+1}F_{n-2} - F_{n-2}F_{n-1}}{F_n}$$

$$c = \frac{F_{n-2}(F_{n+1} - F_{n-1})}{F_n} = \frac{F_{n-2}F_n}{F_n} = F_{n-2}$$

olur ve $c:d = F_{n-2}:F_{n-1}$ oranı yine elde edilmiş olur. Böylece Teorem 3.7 deki üçüncü önermenin özel halinin ikinci önerme olduğu görülür. Kısaca üçüncü önerme kullanılarak birinci ve ikinci önermeler elde edilebilir. □

Örnek 3.3. $n = 8$ alalım. $F_{n+1} = F_9 = 34$ ve $F_{2n-1} = F_{15} = 610$ olur.

1. $a:b = L_n:L_{n+1}$ ise $L_8:L_9 = 47:76$ dır. Böylece $a = 47k$ ve $b = 76k$, $k = 5$ için $a = 235$ ve $b = 380$ alınırsa

$$[a,b] + (a,b)F_{2n-1} = [235,380] + (235,380) \cdot 610 = 17860 + 5 \cdot 610$$
$$= 20910 = (235 + 380) \cdot 34 = (a+b)F_{n+1} \text{ dir.}$$

2. $a:b = F_{n-2}:F_{n-1} = F_6:F_7 = 8:13$ dür. Böylece $a = 8k$ ve $b = 13k$, $k = 12$ için $a = 96$ ve $b = 156$ alınırsa

$$[a,b] + (a,b)F_{2n-1} = [96,156] + 12 \cdot 610$$
$$= 8568 = (96 + 156) \cdot 34 = (a+b)F_{n+1} \text{ dir.}$$

3. $a:b = 180:204 = 15:17$ olduğundan $c:d = 15:17$ ve $(c,d) = 1$ için Eşitlik 3.2 den

$$c = F_9 + \frac{F_9^2 - F_{15}}{d - F_9} = 34 + \frac{34^2 - 610}{d - 34} = 34 + \frac{546}{d - 34}$$

olur. $546 = 2 \cdot 3 \cdot 7 \cdot 13$ olarak asal çarpanlarına ayrıldığında 1, 2, 3, 6, 7, 13, 14, 21, 26, 39, 42, 78, 91, 182, 273 ve 546 olmak üzere on altı tane pozitif çarpana sahiptir. $(d - 34)$ ifadesinden d sayısı 35, 36, 37, 40, 41, 47, 48, 55, 60, 73, 76, 112, 125, 216, 307 ve 580 olmak üzere on altı tane pozitif değere sahiptir. Sonuç olarak $c{:}\,d$ nin değerleri $35{:}\,580$, $36{:}\,307$, $37{:}\,216$, $40{:}\,125$, $41{:}\,112$, $47{:}\,76$, $48{:}\,73$, $55{:}\,60$, $60{:}\,55$, $73{:}\,48$, $76{:}\,47$, $112{:}\,41$, $125{:}\,40$, $216{:}\,37$, $307{:}\,36$ ve $580{:}\,35$ dir. Ama on altı tane oran içinde sekiz farklı oran vardır ve $(c, d) = 1$ olduğundan bu oranlar $7{:}\,116$, $8{:}\,25$, $11{:}\,12$, $36{:}\,307$, $37{:}\,216$, $41{:}\,112$, $47{:}\,76$ ve $48{:}\,73$ dür. Bulduğumuz bu oranlar arasında $L_8{:}\,L_9 = 47{:}\,76$ vardır. Ama $F_6{:}\,F_7 = 8{:}\,13$ oranı yoktur. Yani bu oran da çözüme dahil edilmelidir. Çünkü $d > F_{n+1}$ için Teorem 3.6 nın aksine Teorem 3.7 ile tüm çözümler elde edilmez.

4. m MODÜLÜNE GÖRE FİBONACCİ DİZİLERİ

Bu bölüm Fibonacci sayılarının ve genelleştirilmiş Fibonacci sayılarının m modülüne göre indirgenmiş dizisinin periyot uzunluğu ve bunlar arasındaki ilişki ile ilgilidir. Bu nedenle öncelikle başlangıç değerlerinin ve modülün bir fonksiyonu olan periyot uzunluğu ile ilgili birkaç özellik verilecektir.

Genelleştirilmiş Fibonacci dizisinin m modülüne göre negatif olmayan en küçük kalanlarının oluşturduğu tekrar eden dizisinin periyot uzunluğunu $\mu = \mu(m)$ ile gösterelim. F_n dizisinin m modülüne göre periyot uzunluğunu da a, b ve m ye bağlı olan μ den farklı, $\delta = \delta(m)$ ile gösterelim.

Ayrıca p asal sayı olmak üzere a, b ve m keyfi tam sayı olabilir. Bu şekilde genellemeyi bozmaksızın $(a, b, m) = 1$ olduğunu kabul edelim.

Örnek 4.1. Fibonacci dizisinin 7 modülüne göre kalanlarının dizisi

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, \ldots$$

olmak üzere bu dizinin periyodu $\delta(7) = 16$ olur. Bu kalan dizisinde $F_8 \equiv 0\ (mod\ 7)$ olduğundan periyottaki 16 terim, her biri 8 terimden oluşan iki kümeden oluşur ve 16 terimin ikinci yarımındaki 8 terim, birinci yarımındaki 8 terimin (-1) katı olmaktadır. Bu ilişki daha sonraki bölümlerde ele alınacaktır.

Teorem 4.1. $m \geq 2$ olmak üzere G_n dizisi m modülüne göre basit bir periyodik dizidir. [2]

İspat: m modülüne göre (G_n, G_{n+1}) sıralı tam sayı çifti en fazla m^2 tane farklı değer alır. Bu durumda m modülüne göre $(m^2 + 1)$ tane $G_0, G_1, \ldots, G_{m^2+1}$ sayıları ile oluşturulan sıralı ardışık çiftlerden biri, m^2 tane farklı durumdan birine denk olmalıdır. Böylece (G_t, G_{t+1}) ile (G_s, G_{s+1}) çiftleri m modülüne göre denk alınırsa

$$G_{t+1} \equiv G_{s+1}\ (mod\ m) \text{ ve } G_t \equiv G_s\ (mod\ m)$$

yazılır. Genelleştirilmiş Fibonacci dizisinin rekürans bağıntısından

$$G_t + G_{t-1} \equiv G_s + G_{s-1}\ (mod\ m)$$

olur ve $G_t \equiv G_s\ (mod\ m)$ olduğundan $G_{t-1} \equiv G_{s-1}\ (mod\ m)$ elde edilir. Benzer şekilde devam edilirse $G_{t+1} \equiv G_{s+1}\ (mod\ m)$, $G_t \equiv G_s\ (mod\ m)$, $G_{t-1} \equiv G_{s-1}\ (mod\ m)$,…, $G_{t-s+1} \equiv G_1\ (mod\ m)$ ve $G_{t-s} \equiv G_0\ (mod\ m)$ elde edilir. Böylece başlangıç koşulları elde edildiğinden dizinin tekrar ettiği görülür ve basit periyodik dizi olur. □

Sonuç 4.1. $F_\delta \equiv 0\ (mod\ m)$ dir. [2]

Teorem 4.2. p asal ve m asal çarpanlarına ayrılırsa

$$m = \prod_{i=1}^{s} {p_i}^{e_i}$$

şeklinde yazılır. Ayrıca G_n dizisinin ${p_i}^{e_i}$ modülüne göre periyot uzunluğunu μ_i ile gösterelim. Bu durumda bütün i değerleri için μ_i periyotlarının en küçük ortak katı μ periyodunu verir. Yani $i = 1, 2, \dots, s$ olmak üzere $\mu = [\mu_1, \mu_2, \dots, \mu_s]$ dur. [2]

İspat: "μ_i, G_n dizisinin ${p_i}^{e_i}$ modülüne göre periyot uzunluğudur" ifadesi G_n dizisinin ${p_i}^{e_i}$ modülüne göre $c\mu_i$ uzunluğunda da tekrar edeceği anlamına gelir. Ayrıca "μ, G_n dizisinin m modülüne göre periyot uzunluğudur" ifadesi G_n dizisinin bütün i değerleri için ${p_i}^{e_i}$ modülüne göre μ teriminden sonra da tekrar edeceği anlamına gelir. Bu durumda i nin bütün değerleri için μ, $c\mu_i$ formunda olmaktadır ve μ periyot olduğundan her $i = 1, 2, \dots, s$ için $\mu = [\mu_1, \mu_2, \dots, \mu_s]$ olması gerekir. □

Not: Teorem 4.2 den $m = p^e$ formunda yazılabilir. F_n ile G_n arasındaki ilişki $G_n = bF_n + aF_{n-1}$ olduğundan G_n dizisi de m modülüne göre δ terimden sonra tekrar eder. Ayrıca G_n dizisinin m modülüne göre periyodu μ olduğundan $\mu \mid \delta$ olur. [2]

Teorem 4.3. $F_n \equiv 0\ (mod\ m)$ olmak üzere bunu sağlayan Fibonacci sayılarının indisleri basit aritmetik formdadır. Yani $n \in \mathbb{N}$ ve $F_n \equiv 0\ (mod\ m)$ olmak üzere $x = 0, 1, 2, \ldots$ ve belli bir $\alpha = \alpha(m)$ pozitif tam sayısı için $n = x\alpha$ formundadır. [2]

İspat: $i \geq j$ olmak üzere Özdeşlik 2 kullanılırsa $F_{i+j} = F_{i-1}F_j + F_iF_{j+1}$ olur ve burada $F_i \equiv 0\ (mod\ m)$ ve $F_j \equiv 0\ (mod\ m)$ alınırsa $F_{i+j} \equiv 0\ (mod\ m)$ bulunur. Ayrıca Özdeşlik 2 den $F_i = F_{(i-j)+j} = F_{i-j-1}F_j + F_{i-j}F_{j+1}$ olur ve $F_i \equiv 0\ (mod\ m)$, $F_j \equiv 0\ (mod\ m)$ alınırsa $F_{i-j}F_{j+1} \equiv 0\ (mod\ m)$ bulunur. Burada $\left(F_j, F_{j+1}\right) = 1$ ve $F_j \equiv 0\ (mod\ m)$ olduğundan $F_{j+1} \not\equiv 0\ (mod\ m)$ olur. Böylece $F_{i-j} \equiv 0\ (mod\ m)$ elde edilir. Bu durumda $F_i \equiv 0\ (mod\ m)$, $F_j \equiv 0\ (mod\ m)$, $F_{i+j} \equiv 0\ (mod\ m)$ ve $F_{i-j} \equiv 0\ (mod\ m)$ olmak üzere indisler $0, j, \ldots, i-j, i, i+j, \ldots$ şeklinde sıralanırsa aritmetik formda olur. Bu nedenle $F_n \equiv 0\ (mod\ m)$ denkliğini sağlayan terimlerin negatif olmayan indisleri $x = 0, 1, 2, \ldots$ için $n = x\alpha$ formundadır ve Sonuç 4.1 den $F_n \equiv 0\ (mod\ m)$ denkliğinin sadece F_0 iken olmadığı görülmektedir. □

Uyarı 4.1. $F_\delta \equiv 0\ (mod\ m)$ olduğundan $\delta = x\alpha$ formunda olur ve $\alpha \mid \delta$ bulunur. [2]

Teorem 4.4. $m > 2$ ise δ çift sayıdır. [2]

İspat: F_n dizisinin $m > 2$ için m modülüne göre periyodu $\delta = 2x + 1$ şeklinde tek sayı olsun. Periyot olmasından $F_\delta \equiv 0\ (mod\ m)$ ve $F_{\delta+1} \equiv 1\ (mod\ m)$ olmak üzere F_n dizisi m modülüne göre

$$-F_\delta \equiv 0 = F_0\ (mod\ m),$$

$F_{\delta+1} = F_{\delta-1} + F_\delta$ reküransından

$$F_{\delta-1} \equiv 1 = F_1 \ (mod\ m),$$

$F_\delta = F_{\delta-2} + F_{\delta-1}$ reküransından $-F_{\delta-2} = -F_\delta + F_{\delta-1}$ bulunur ve burada $-F_\delta \equiv F_0 \ (mod\ m)$ ve $F_{\delta-1} \equiv F_1 \ (mod\ m)$ olduğundan

$$-F_{\delta-2} = -F_\delta + F_{\delta-1} \equiv F_0 + F_1 = F_2 \ (mod\ m),$$

$$\vdots$$

$$(-1)^{t-1}F_{\delta-t} = (-1)^{t-1}F_{\delta-t+2} + (-1)^t F_{\delta-t+1} \equiv F_{t-2} + F_{t-1} = F_t \ (mod\ m),$$

$$\vdots$$

şeklinde devam eder. $(-1)^{t-1}F_{\delta-t} \equiv F_t \ (mod\ m)$ denkliğinde $\delta = 2x+1$, $t = x-1$ alınırsa

$$(-1)^{x-2}F_{x+2} \equiv F_{x-1} \ (mod\ m) \tag{4.1}$$

bulunur. $(-1)^{t-1}F_{\delta-t} \equiv F_t \ (mod\ m)$ denkliğinde $\delta = 2x+1$, $t = x$ alınırsa

$$(-1)^{x-1}F_{x+1} \equiv F_x \ (mod\ m) \tag{4.2}$$

bulunur. Denklik 4.2 de x çift alınırsa $-F_{x+1} \equiv F_x \ (mod\ m)$ olur ve $F_{x+2} \equiv 0 \ (mod\ m)$ elde edilir. Denklik 4.1 de x çift alınırsa $F_{x+2} \equiv F_{x-1} \ (mod\ m)$ elde edilir. Böylece $F_{x-1} \equiv 0 \ (mod\ m)$ elde edilir. Denklik 4.2 de x tek alınırsa $F_{x+1} \equiv F_x \ (mod\ m)$ olur ve $F_{x+1} = F_x + F_{x-1}$ olduğundan $F_{x-1} \equiv 0 \ (mod\ m)$ elde edilir. Böylece x çift veya tek sayı olsun her durumda $F_{x-1} \equiv 0 \ (mod\ m)$ olduğundan ve Teorem 4.3 den $x-1 = x\alpha$ formunda olur. Yani $\alpha \mid (x-1)$ olup $\alpha \mid (2x-2)$ bulunur. Ayrıca $\alpha \mid \delta$ olduğundan $\alpha \mid (2x+1)$ olur. Bu durumda $\alpha \mid [(2x+1)-(2x-2)]$ olduğundan $\alpha \mid 3$ elde edilir. Yani $\alpha = 3$ ve Teorem 4.3 den $F_\alpha = F_3 = 2 \equiv 0 \ (mod\ m)$ olur. Bunun için $m = 2$ olmalıdır. Bu durum $m > 2$ olması ile çeliştiğinden δ sayısı tek değil çift sayı olmalıdır. □

Teorem 4.5. p asal sayı, $\delta(p^2) \neq \delta(p)$ ise $\delta(p^e) = p^{e-1}\delta(p)$ olur. Ayrıca $\delta(p^f) \neq \delta(p)$ eşitliğini sağlayan en büyük tam sayı f ise $e > f$ için $\delta(p^e) = p^{e-f}\delta(p)$ dir. [2]

İspat: Öncelikle $x^2 = x + 1$ denkleminin kökleri A ve B olmak üzere A^n ve B^n için F_n ve L_n dizilerinin $F_n = (A^n - B^n)/\sqrt{5}$ ve $L_n = A^n + B^n$ binet formülleri taraf tarafa toplanırsa $A^n = (\sqrt{5}F_n + L_n)/2$ ve bu formüller taraf tarafa çıkarılırsa $B^n = (-\sqrt{5}F_n + L_n)/2$ olur. $F_{an} = (A^{an} - B^{an})/\sqrt{5}$ olmak üzere $A^n = (\sqrt{5}F_n + L_n)/2$ ve $B^n = (-\sqrt{5}F_n + L_n)/2$ yerine yazılırsa

$$F_{an} = \left[\left(\sqrt{5}F_n + L_n\right)^a 2^{-a} - \left(-\sqrt{5}F_n + L_n\right)^a 2^{-a}\right]/\sqrt{5}$$

elde edilir. Binom Teoreminden

$$F_{an} = \frac{2^{-a}}{\sqrt{5}}\left[\sum_{j=0}^{a}\binom{a}{j}\left(\sqrt{5}F_n\right)^j L_n^{a-j} - \sum_{j=0}^{a}\binom{a}{j}\left(-\sqrt{5}F_n\right)^j L_n^{a-j}\right]$$

$$F_{an} = \frac{2^{-a}}{\sqrt{5}}\left[2\sum_{j\ tek}\binom{a}{j}\left(\sqrt{5}F_n\right)^j L_n^{a-j}\right]$$

$$F_{an} = 2^{1-a}\sum_{j\ tek}\binom{a}{j}5^{(j-1)/2}F_n^j L_n^{a-j} \tag{4.3}$$

bulunur. Ayrıca

$$F_{an} = 2^{1-a}F_n\left[aL_n^{a-1} + F_n^2\left(\binom{a}{3}5\,L_n^{a-3} + \cdots\right)\right]$$

ve $\left(\binom{a}{3}5\,L_n^{a-3} + \cdots\right) = K$ tam sayısı için

$$F_{an} = 2^{1-a}F_n(KF_n^2 + aL_n^{a-1}) \tag{4.4}$$

bulunur. Benzer şekilde $F_{an+1} = (A^{an+1} - B^{an+1})/\sqrt{5}$ olmak üzere $A^n = (\sqrt{5}F_n + L_n)/2$ ve $B^n = (-\sqrt{5}F_n + L_n)/2$ yerine yazılırsa

$$F_{an+1} = \left[\left(\sqrt{5}F_n + L_n\right)^a 2^{-a}A - \left(-\sqrt{5}F_n + L_n\right)^a 2^{-a}B\right]/\sqrt{5}$$

elde edilir. Binom Teoreminden

$$F_{an+1} = \frac{2^{-a}}{\sqrt{5}}\left[A\sum_{j=0}^{a}\binom{a}{j}\left(\sqrt{5}F_n\right)^j L_n^{a-j} - B\sum_{j=0}^{a}\binom{a}{j}\left(-\sqrt{5}F_n\right)^j L_n^{a-j}\right]$$

$$F_{an+1} = 5^{-1/2}2^{-a}\left[\sum_{j=0}^{a}\binom{a}{j}5^{j/2}F_n^j L_n^{a-j}\left[\frac{1+\sqrt{5}}{2}-(-1)^j\frac{1-\sqrt{5}}{2}\right]\right]$$

bulunur. Ayrıca

$$F_{an+1} = 2^{-a}\left[L_n^a + aF_nL_n^{a-1} + F_n^2\left(\binom{a}{2}5L_n^{a-2}+\cdots+\binom{a}{a}5^{(a-1)/2}F_n^{a-2}\left[\frac{1+\sqrt{5}}{2}-(-1)^a\frac{1-\sqrt{5}}{2}\right]\right)\right]$$

ve $\binom{a}{2}5L_n^{a-2}+\cdots+\binom{a}{a}5^{(a-1)/2}F_n^{a-2}\left[\frac{1+\sqrt{5}}{2}-(-1)^a\frac{1-\sqrt{5}}{2}\right] = M$ bir tam sayı olmak üzere

$$F_{an+1} = 2^{-a}(MF_n^2 + aF_nL_n^{a-1} + L_n^a) \tag{4.5}$$

bulunur. $p \neq 2$ ve asal sayı olmak üzere Teorem 4.5 in birinci kısmının ispatı için tümevarım kullanılırsa ilk kısım $e = 1$ için doğru olur ve $e = e$ için $\delta(p^e) = p^{e-1}\delta(p)$ olduğunu kabul edelim. Son olarak $e = e+1$ için $\delta(p^{e+1}) = p^e\delta(p)$ olduğunu gösterelim.

Bunun için öncelikle Özdeşlik 3 den yararlanarak $(L_n, F_n) = 1$ veya 2 olur. Ayrıca $F_n \equiv 0\ (mod\ p^e)$ ve $F_n \not\equiv 0\ (mod\ p^{e+1})$ denkliklerini sağlayan ilk terim F_n ise bu durumda $F_{pn} \equiv 0\ (mod\ p^{e+1})$ ve $F_{pn} \not\equiv 0\ (mod\ p^{e+2})$ denkliklerini sağlayan ilk terimin F_{pn} olduğunu gösterelim. $F_n \equiv 0\ (mod\ p^e)$ ve $F_n \not\equiv 0\ (mod\ p^{e+1})$ olsun. Denklik 4.4 de $a = p$ alınırsa

$$F_{pn} = 2^{1-p}F_n\left(KF_n^2 + pL_n^{p-1}\right)$$

olur. Burada $F_n \equiv 0\ (mod\ p^e)$ ve $(L_n, F_n) = 1$ veya 2 olduğundan $F_{pn} = p^{e+1}X$, $X \in \mathbb{Z}^+$ şeklinde yazılabilir. Böylece $F_{pn} \equiv 0\ (mod\ p^{e+1})$ bulunur. Ayrıca bu eşitlikte $F_n \not\equiv 0\ (mod\ p^{e+1})$, $(L_n, F_n) = 1$ veya 2 olduğundan $F_{pn} \not\equiv 0\ (mod\ p^{e+2})$ olur. Son olarak ilk terim $F_n \equiv 0\ (mod\ p^e)$ olduğundan Teorem 4.3 den $x = 0, 1, 2, \ldots$ için $F_{nx} \equiv 0\ (mod\ p^e)$ ve ilk terim $F_{pn} \equiv 0\ (mod\ p^{e+1})$ olduğundan $F_{pnx} \equiv 0\ (mod\ p^{e+1})$ olur. Böylece $F_{pnx+1} \equiv 1\ (mod\ p^{e+1})$ alınırsa periyot olmasından

$$\delta(p^{e+1}) = pnx \tag{4.6}$$

olur. Denklik 4.5 de $a = p$ ve $n = nx$ alınırsa

$$F_{pnx+1} = 2^{-p}\left(MF_{nx}^2 + pF_{nx}L_{nx}^{p-1} + L_{nx}^p\right) (mod\ p^{e+1})$$

olur ve $F_{nx} \equiv 0\ (mod\ p^e)$ olduğundan

$$F_{pnx+1} \equiv 2^{-p}L_{nx}^p = (L_{nx}/2)^p\ (mod\ p^{e+1})$$

olur ve $F_{pnx+1} \equiv 1\ (mod\ p^{e+1})$ olduğundan $(L_{nx}/2)^p \equiv 1\ (mod\ p^{e+1})$,

$$L_{nx} \equiv 2\ (mod\ p^e)$$

bulunur. Özdeşlik 3 den $L_{nx} = F_{nx-1} + F_{nx+1}$ eşitliğinde $F_{nx-1} = F_{nx+1} - F_{nx}$ alınırsa $L_{nx} = F_{nx+1} - F_{nx} + F_{nx+1}$ olur ve $F_{nx} \equiv 0\ (mod\ p^e)$ olduğundan

$$L_{nx} \equiv 2F_{nx+1}\ (mod\ p^e)$$

olur. Burada $L_{nx} \equiv 2\ (mod\ p^e)$ olduğundan $2 \equiv 2F_{nx+1}\ (mod\ p^e)$ ve $F_{nx+1} \equiv 1\ (mod\ p^e)$ elde edilir. Böylece $F_{nx} \equiv 0\ (mod\ p^e)$ ve $F_{nx+1} \equiv 1\ (mod\ p^e)$ olmak üzere periyot olmasından

$$\delta(p^e) = nx \tag{4.7}$$

olur. Sonuç olarak Denklik 4.6 ve 4.7 den $\delta(p^{e+1}) = p\delta(p^e)$ elde edilir. Ayrıca $\delta(p^e) = p^{e-1}\delta(p)$ kabulünden

$$\delta(p^{e+1}) = p \cdot p^{e-1}\delta(p) = p^e\delta(p)$$

bulunur. □

Benzer şekilde $p = 2$ için de Özdeşlik 4 ve Özdeşlik 2 den elde edilen $F_{2n} = F_n(F_{n-1} + F_{n+1})$ ve $F_{2n+1} = F_{n+1}^2 + F_n^2$ formülleri kullanılarak $\delta(2^e) = 2^{e-1}\delta(2)$ olduğu tümevarım ile ispatlanır. [2]

Lemma 4.1. p tek asal, (m/p) Legendre sembolü ve $m^{\frac{1}{2}(p-1)} \equiv (m/p)\ (mod\ p)$ olmak üzere $(m,p)=1$ ise $(m/p)=\pm 1$, aksi taktirde $(m/p)=0$ dır. [5]

Lemma 4.2. Fermat Teoremi, p asal ve $(m,p)=1$ için $m^{p-1} \equiv 1\ (mod\ p)$ dir. [5]

Teorem 4.6. p asal ve $m=p=10x\pm 1$ ise $\delta(p) \mid (p-1)$ dir. [2]

Not: Ayrıca p asal, $p=5k\pm 1$ ise $(5/p)=1$ ve $p=5k\pm 2$ ise $(5/p)=-1$ dir. [3]

Teorem 4.7. p asal ve $m=p=10x\pm 3$ ise $\delta(p) \mid (2p+2)$ dir. [2]

İspat: 5 sayısı, $p=10x\pm 3$ formundaki asallar için kuadratik bir kalan değildir. Lemma 4.1 den $5^{(p-1)/2} \equiv (5/p)\ (mod\ p)$ ve $(5,p)=1$ olduğundan $(5/p)=\pm 1$ olur. Ayrıca $p=10x\pm 3=5k\pm 2$ olduğundan $(5/p)=-1$ bulunur. Böylece $p=10x\pm 3$ için $5^{(p-1)/2} \equiv -1\ (mod\ p)$ olur. Eşitlik 4.3 de $n=1$ ve $a=n$ alınırsa

$$F_n = 2^{1-n} \sum_{j\ tek}^{n} \binom{n}{j} 5^{(j-1)/2}$$

$$F_n = 2^{1-n}\left[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots + 5^{(n-1)/2}\binom{n}{n}\right] \qquad (4.8)$$

elde edilir. Bu eşitlikte $n=p$ alınırsa ve $0<s<p$ için $p \mid \binom{p}{s}$ olduğundan

$$F_p = 2^{1-p}\left[\binom{p}{1} + 5\binom{p}{3} + 5^2\binom{p}{5} + \cdots + 5^{(p-1)/2}\binom{p}{p}\right] \equiv 2^{1-p}5^{(p-1)/2}\ (mod\ p)$$

olur ve $5^{(p-1)/2} \equiv -1\ (mod\ p)$ olduğundan $F_p \equiv -2^{1-p}\ (mod\ p)$ bulunur. Ayrıca Lemma 4.2 den $p=10x\pm 3$ tek asal ve $(m=2,p)=1$ olmak üzere $2^{p-1} \equiv 1\ (mod\ p)$ olduğundan $F_p \equiv -1\ (mod\ p)$ elde edilir.

Eşitlik 4.8 de $n=p+1$ alınırsa

$$F_{p+1} = 2^{-p}\left[\binom{p+1}{1} + 5\binom{p+1}{3} + 5^2\binom{p+1}{5} + \cdots + 5^{(p-1)/2}\binom{p+1}{p}\right] \ (mod\ p)$$

$$F_{p+1} \equiv 2^{-p}\left[\binom{p+1}{1} + 5^{(p-1)/2}\binom{p+1}{p}\right] \ (mod\ p)$$

olur ve $5^{(p-1)/2} \equiv -1\ (mod\ p)$ olduğundan

$$F_{p+1} \equiv 2^{-p}\left[\binom{p+1}{1} - \binom{p+1}{p}\right] \ (mod\ p)$$

bulunur ve $F_{p+1} \equiv 0\ (mod\ p)$ elde edilir. Son olarak $F_{p+2} = F_p + F_{p+1}$, $F_p \equiv -1\ (mod\ p)$ ve $F_{p+1} \equiv 0\ (mod\ p)$ olduğundan

$$F_{p+2} \equiv -1 = -F_1\ (mod\ p),$$

$F_{p+3} = F_{p+1} + F_{p+2}$, $F_{p+1} \equiv 0\ (mod\ p)$ ve $F_{p+2} \equiv -1 = -F_1\ (mod\ p)$ olduğundan

$$F_{p+3} \equiv -F_1 = -F_2\ (mod\ p),$$

$$\vdots$$

$F_{2p+1} = F_{(p+1)+p} = F_{p+2}F_p + F_{p+1}F_{p-1}$, $F_p \equiv -1\ (mod\ p)$ ve $F_{p+1} \equiv 0\ (mod\ p)$ olduğundan $F_{2p+1} \equiv -F_{p+2}\ (mod\ p)$ olur ve $F_{p+2} \equiv -F_1\ (mod\ p)$ olduğundan

$$F_{2p+1} \equiv F_1 = 1\ (mod\ p),$$

$F_{2p+2} = F_{(p+1)+(p+1)} = F_{p+2}F_{p+1} + F_{p+1}F_p$, $F_{p+1} \equiv 0\ (mod\ p)$ olduğundan

$$F_{2p+2} \equiv 0 = F_0\ (mod\ p)$$

olur. Böylece F_n dizisi m modülüne göre başa döner ve dizinin $(2p+2)$ terimde tekrar ettiği görülür. Sonuç olarak $\delta(p) \mid (2p+2)$ bulunur. □

Sonuç 4.2. p asal ve $p = 10x \pm 3$ ise $\delta(p) \equiv 0\ (mod\ 4)$ dir. [2]

İspat: p asal ve $p = 10x \pm 3$ ise $\delta(p) \not\equiv 0\ (mod\ 4)$ olsun. Bu durumda Teorem 4.4 den $\delta(p)$, $m = 4 > 2$ için çift olduğundan 2 nin tek katı olur ve Teorem 4.7 den $\delta(p) \mid (p+1)$ olur. Yani F_n dizisi m modülüne göre $(p+1)$ terimden sonra da tekrar

eder. Böylece $F_{p+1} \equiv 0\ (mod\ p)$ olduğundan $F_p \equiv 1\ (mod\ p)$ bulunur. Ancak bu durum Teorem 4.7 nin ispatında bulunan $F_p \equiv -1\ (mod\ p)$ ile çelişir. Böylece $\delta(p) \equiv 0\ (mod\ 4)$ olmalıdır. □

G_n için periyot uzunluğu olan μ nün en ilginç özelliklerinden biri başlangıç değerlerinden genellikle bağımsız olmasıdır. Şimdi μ ile δ arasında bir ilişki kurulmaya çalışılacaktır.

Teorem 4.8. p asal ve $p = 10x \pm 3$ ise $\mu(p^e) = \delta(p^e)$ dir. [2]

İspat: G_n dizisinin m modülüne göre μ periyodu ile tekrarlandığını gösteren denklikler aşağıdaki formda yazılabilir. $G_\mu = bF_\mu + aF_{\mu-1}$ ve $G_\mu \equiv a\ (mod\ p)$ olmak üzere

$$G_\mu - a = bF_\mu + a(F_{\mu-1} - 1) \equiv 0\ (mod\ m) \tag{4.9}$$

olur ve $G_{\mu+1} = bF_{\mu+1} + aF_\mu$ ve $G_{\mu+1} \equiv b\ (mod\ p)$ olmak üzere

$$G_{\mu+1} - b = b\left(F_\mu + F_{\mu-1}\right) + aF_\mu - \mathrm{b} \equiv 0\ (mod\ m)$$

$$G_{\mu+1} - b = (b+a)F_\mu + b(F_{\mu-1} - 1) \equiv 0\ (mod\ m) \tag{4.10}$$

elde edilir. Buradan Denklik 4.9 ve 4.10 ile

$$bF_\mu + aF_{\mu-1} \equiv a\ (mod\ m)$$

$$F_\mu(a+b) + bF_{\mu-1} \equiv b\ (mod\ m)$$

bulunur ve a, b değerleri kat sayı olarak alınırsa bu sistemin kat sayılar matrisinin determinantı $\Delta = b^2 - ab - a^2$ olur. $m = p^e$ olmak üzere $\Delta \equiv 0\ (mod\ p)$ ise $b^2 \equiv ab + a^2\ (mod\ p)$ bulunur ve

$$4a^2 + 4ab + b^2 = (2a+b)^2 = 4(a^2 + ab) + b^2$$

olur. Ayrıca $b^2 \equiv ab + a^2\ (mod\ p)$ olduğundan

$$4a^2 + 4ab + b^2 = (2a+b)^2 \equiv 5b^2\ (mod\ p)$$

elde edilir. Buradan $\Delta \equiv 0\ (mod\ p)$ olması için $b \equiv 0\ (mod\ p)$ olursa $a \equiv 0\ (mod\ p)$ olur ve bu durum $(a, b, m) = 1$ olması ile çeliştiğinden $b \not\equiv 0\ (mod\ p)$ olmalıdır. Bu nedenle $b \not\equiv 0\ (mod\ p)$ için $\Delta \equiv 0\ (mod\ p)$ denkliğine göre 5 sayısı, p asal sayıları için kuadratik kalandır. Ama 5 sayısı, $p = 10x \pm 3$ formundaki asal sayılar için kuadratik bir kalan olmadığından çelişki ortaya çıkar. Böylece $\Delta \not\equiv 0\ (mod\ p)$ dir. Yani $(\Delta, m) = 1$ olmalıdır. Bu durumda $\Delta \not\equiv 0\ (mod\ p)$ olduğundan sistemin tek bir çözümü vardır ve bu çözüm $F_\mu \equiv 0\ (mod\ p^e)$ ve $F_{\mu-1} \equiv 1\ (mod\ p^e)$ olur. Böylece F_n dizisi $m = p^e$ modülüne göre μ terimden sonra da tekrar ettiğinden $\delta(p^e) \mid \mu(p^e)$ bulunur ve $\mu(p^e) \mid \delta(p^e)$ olduğundan $\mu(p^e) = \delta(p^e)$ elde edilir. □

Sonuç 4.3. p asal ve $p = 10x \pm 3$, $\Delta = b^2 - ab - a^2$ için $(\Delta, m) = 1$ ise $\mu(m) = \delta(m)$ dir. [2]

Özel olarak $\Delta = b^2 - ab - a^2$ olmak üzere L_n dizisi için $a = 2$ ve $b = 1$ alınırsa $\Delta = -5$ olur. Bu durumda $(5, m = p^e) = 1$ olduğundan $\mu(m) = \delta(m)$ olur. Böylece L_n dizisinin m modülüne göre periyodu $\mu(m) = \delta(m)$ dir. [2]

Teorem 4.9. $m = 2^e$ ise $\mu(m) = \delta(m)$ dır. [2]

İspat: Teorem 4.8 de olduğu gibi determinant $\Delta = b^2 - ab - a^2$ olmak üzere $m = 2^e$ olsun ve $(a, b, 2) = 1$ için $\Delta \not\equiv 0\ (mod\ 2)$ olduğundan $(\Delta, 2^e) = 1$ olur ve Sonuç 4.3 den $\mu(m) = \delta(m)$ olur. □

Sonuç 4.4. p asal, $m = p^e$ ve μ tek sayı ise $p = 10x \pm 1$ veya $m = 2$ dir. [2]

Teorem 4.10. p asal, $m = p^e$, $p > 2$ ve (a, b) başlangıç değerleri için $\mu = 2t + 1$ ise $\delta = 4t + 2$ dir. [2]

İspat: p asal, $m = p^e, p > 2$ ve (a, b) çifti için $\mu = 2t + 1$ yani μ tek sayı olsun. Denklik 4.9 ve 4.10 kullanılarak

$$bF_\mu + a(F_{\mu-1} - 1) \equiv 0 \ (mod\ m)$$

$$b(F_{\mu+1} - 1) + aF_\mu \equiv 0 \ (mod\ m)$$

bulunur ve $(a, b, m) = 1$ için $\Delta = F_\mu^2 - \left(F_{\mu+1} - 1\right)\left(F_{\mu-1} - 1\right) \equiv 0 \ (mod\ m)$ olur.

$$F_\mu^2 - F_{\mu+1}F_{\mu-1} + F_{\mu+1} + F_{\mu-1} - 1 \equiv 0 \ (mod\ m)$$

ve Cassini özdeşliğinden $(-1)^{\mu-1} + F_{\mu+1} + F_{\mu-1} - 1 \equiv 0 \ (mod\ m)$ olur. Burada $F_{\mu+1} + F_{\mu-1} = L_\mu$ olduğundan $(-1)^{\mu-1} + L_\mu - 1 \equiv 0 \ (mod\ m)$,

$$L_\mu \equiv 1 + (-1)^\mu \ (mod\ m)$$

elde edilir. Burada $L_\mu = F_{2\mu}/F_\mu$ olduğundan

$$F_{\mu+1} + F_{\mu-1} = L_\mu = F_{2\mu}/F_\mu \equiv 1 + (-1)^\mu \ (mod\ m) \qquad (4.11)$$

bulunur ve $\mu = 2t + 1$ tek sayı olduğundan $L_\mu = F_{2\mu}/F_\mu \equiv 0 \ (mod\ m)$ olur. Böylece

$$F_{2\mu} \equiv 0 \ (mod\ m) \qquad (4.12)$$

elde edilir. Denklik 4.11 den yararlanarak

$$F_{2\mu+1} + F_{2\mu-1} = L_{2\mu} \equiv 1 + (-1)^{2\mu} \equiv 2 \ (mod\ m)$$

olur ve $F_{2\mu-1} = F_{2\mu+1} - F_{2\mu}$ olduğundan $F_{2\mu+1} + F_{2\mu+1} - F_{2\mu} \equiv 2 \ (mod\ m)$ bulunur. Burada $F_{2\mu} \equiv 0 \ (mod\ m)$ olduğundan $2F_{2\mu+1} \equiv 2 \ (mod\ m)$ ve

$$F_{2\mu+1} \equiv 1 \ (mod\ m) \qquad (4.13)$$

elde edilir. Son olarak Denklik 4.12 ve 4.13 den F_n dizisi m modülüne göre 2μ terimden sonra tekrar eder ve F_n dizisinin periyodu δ olduğundan $\delta \mid 2\mu$ olur. Ayrıca $\mu \mid \delta$ dır. Sonuç olarak μ tek sayı ve Teorem 4.4 den $m > 2$ için δ çift sayı olduğundan $\delta = 2\mu$ olur. Böylece $\delta = 2\mu$ ve $\mu = 2t + 1$ olduğundan $\delta = 2(2t + 1) = 4t + 2$ bulunur. □

Örnek 4.2. $m = 11$, $a = 1$, $b = 4$ için $\mu = 5$ ve $\delta(11) = 10$,
$m = 29$, $a = 1$, $b = 24$ için $\mu = 7$ ve $\delta(29) = 14$,
$m = 121$, $a = 1$, $b = 37$ için $\mu = 55$ ve $\delta(121) = 110$ dur.

Lemma 4.3. p asal, $\delta(p^e) = 4t + 2$ ise $F_{2t+2} \equiv -F_{2t}\ (mod\ p^e)$ dir. [2]

İspat: p asal, $p^e > 2$ olduğundan Teorem 4.4 den $\delta(p^e)$ çift sayı olur. Bu nedenle $\delta(p^e) = 4t + 2$ olsun. Teorem 4.4 deki zincirden $(-1)^{t-1}F_{\delta-t} \equiv F_t\ (mod\ p^e)$ olur. Burada $\delta(p^e) = 4t + 2$ ve t yerine $2t$ alınırsa $(-1)^{2t-1}F_{2t+2} \equiv F_{2t}\ (mod\ p^e)$ bulunur ve $F_{2t+2} \equiv -F_{2t}\ (mod\ p^e)$ elde edilir. □

Teorem 4.11. p asal, $m = p^e$, $p > 2$ ve $\delta = 4t + 2$ ise bazı (a, b) başlangıç değerleri için $\mu = 2t + 1$ dir. [2]

İspat: p asal, $m = p^e$, $p > 2$ ve $\delta = 4t + 2$ olsun. $G_n = bF_n + aF_{n-1}$ olmak üzere

$$a = G_0 \equiv -F_{2t+1} - F_0\ (mod\ p^e) \text{ ve } b = G_1 \equiv F_{2t} - F_1\ (mod\ p^e)$$

olsun. Bu durumlar genel hale getirilirse

$$G_n \equiv (-1)^{n-1}F_{2t+1-n} - F_n\ (mod\ p^e)$$

olur. Bu denklikte $n = 2t + 1$ alınırsa $G_{2t+1} \equiv -F_{2t+1} \equiv G_0 = a\ (mod\ p^e)$ bulunur ve $G_{2t+1} \equiv a\ (mod\ p^e)$ elde edilir. Aynı denklikte $n = 2t + 2$ alınırsa $G_{2t+2} \equiv -F_{-1} - F_{2t+2}\ (mod\ p^e)$ elde edilir ve Lemma 4.3 den $G_{2t+2} \equiv -F_1 + F_{2t} \equiv G_1 = b\ (mod\ p^e)$ bulunur. Yani $G_{2t+2} \equiv b\ (mod\ p^e)$ elde edilir. Elde edilen $G_{2t+1} \equiv a\ (mod\ p^e)$ ve $G_{2t+2} \equiv b\ (mod\ p^e)$ başlangıç koşulları olduğundan dizi $(2t + 1)$ terimde tekrar eder. Ayrıca G_n dizisinin periyodu μ olduğundan $\mu \mid (2t + 1)$ olur. Bu durumda μ tek sayı olduğundan Teorem 4.10 dan $\delta = 2\mu$ dür. Son olarak $(a, b, p^e) = 1$ olduğunu ispatlayalım. Bunun için $(a, b, p^e) \neq 1$ olsun. Buradan $a \equiv 0\ (mod\ p)$ ve $b \equiv 0\ (mod\ p)$ olduğundan

$$a \equiv -F_{2t+1} - F_0 \equiv b \equiv F_{2t} - F_1 \equiv 0\ (mod\ p)$$

olur. Buradan $F_{2t+1} \equiv 0\ (mod\ p)$ ve $F_{2t} \equiv 1\ (mod\ p)$ olduğundan $\delta(p) = 2t + 1$ olabilir. Ama bu durumun olması imkansızdır. Çünkü $\delta = 2\mu$ olmak üzere çift sayıdır. Bu çelişkinin olmaması için $(a, b, p^e) = 1$ olmalıdır. Böylece $\delta = 2\mu$ olmak üzere $\delta = 4t + 2$ alındığında bazı (a, b) çiftleri için $\mu = 2t + 1$ bulunur. □

Bu arada $p^e = 4$ için istisnai bir durum vardır. Çünkü $\delta(4) = 6 \equiv 2\ (mod\ 4)$ olur. Ancak hiçbir G_n dizisinin 4 modülüne göre periyodu $\mu = 3$ değildir.

Teorem 4.12. p asal, $m = p^e$, $p > 2$, $p \neq 5$ ve μ çift sayı ise $\mu(m) = \delta(m)$ dir. [2]

İspat: p asal, $m = p^e$, $p > 2$, $p \neq 5$ ve μ çift sayı olsun. Denklik 4.11 den $L_\mu \equiv 1 + (-1)^\mu\ (mod\ m)$ olmak üzere $L_\mu \equiv 2\ (mod\ m)$ olur ve $L_n = A^n + B^n$ kullanılırsa $A^\mu + B^\mu - 2 \equiv 0\ (mod\ m)$ elde edilir. Buradan

$$A^{2\mu} + B^{2\mu} + 4 + 2(AB)^\mu - 4B^\mu - 4A^\mu \equiv 0\ (mod\ m^2)$$

olur ve $AB = -1$, μ çift sayı olduğundan

$$A^{2\mu} + B^{2\mu} + 6 - 4L_\mu \equiv 0\ (mod\ m^2)$$

bulunur ve $L_\mu \equiv 2\ (mod\ m)$ olduğundan

$$(A^\mu - B^\mu)^2 \equiv 0\ (mod\ m^2) \qquad (4.14)$$

elde edilir. $F_n = (A^\mu - B^\mu)/\sqrt{5} \in \mathbb{Z}$ olduğundan $x \in \mathbb{Z}$ için $A^\mu - B^\mu = x\sqrt{5}$ formundadır ve $p \neq 5$ olduğundan $(A - B)^2 = 5 \not\equiv 0\ (mod\ m)$ olur. Böylece Denklik 4.14 ün her iki tarafı $(A - B)^2$ ile bölünürse

$$F_\mu^2 = \frac{(A^\mu - B^\mu)^2}{(A - B)^2} \equiv 0\ (mod\ m^2)$$

bulunur. Böylece $F_\mu \equiv 0\ (mod\ m)$ olur. Ayrıca $L_\mu = F_{\mu-1} + F_{\mu+1}$ özdeşliğinden $L_\mu = 2F_{\mu-1} + F_\mu$ olur ve $L_\mu \equiv 2\ (mod\ m)$, $F_\mu \equiv 0\ (mod\ m)$ olduğundan

$$F_{\mu+1} \equiv F_{\mu-1} \equiv 1\ (mod\ m)$$

elde edilir. Son olarak $F_\mu \equiv 0\ (mod\ m)$ ve $F_{\mu+1} \equiv 1\ (mod\ m)$ olduğundan F_n dizisi μ terimde tekrar eder ve F_n dizisinin periyodu δ olduğundan $\delta \mid \mu$ olur. Ayrıca $\mu \mid \delta$ olduğundan $\mu = \delta$ bulunur. □

Sonuç 4.5. p asal, $p \neq 5$ ve $\delta(p) \equiv 0\ (mod\ 4)$ ise $\mu(p^e) = \delta(p^e)$ dir. [2]

Örnek 4.3. $m = 10^{10}$ için δ değerini bulunuz.

Çözüm: Teorem 4.2 ye göre $m = 2^{10}5^{10}$ olacak şekilde yazılsın. Bu durumda $m_1 = 2^{10}$ ve $m_2 = 5^{10}$ olmak üzere Teorem 4.5 uygulanırsa $\delta(2) = 3 \neq \delta(2^2)$ ve $\delta(5) = 20 \neq \delta(5^2)$ olduğundan ve $\delta(p^e) = p^{e-1}\delta(p)$ eşitliğinden $\delta(2^{10}) = 2^9\delta(2) = 3 \cdot 2^9 = \delta_1$ ve $\delta(5^{10}) = 5^9\delta(5) = 20 \cdot 5^9 = \delta_2$ bulunur. Böylece $\delta = [\delta_1, \delta_2] = 15.10^9$ elde edilir.

5. m MODÜLÜNE GÖRE FİBONACCİ MATRİSİ

Bu bölümde Fibonacci dizisinin bazı aritmetik özellikleri, temel matris cebiri kullanılarak incelenmiştir ve dizinin m modülüne göre periyot ve kısıtlı periyot tanımları ele alınıp birkaç özellik matris gösterimi ile incelenmiştir.

İlk öncelikle basit bir örneği inceleyelim ve sonrasında tanımları ele alalım. Fibonacci dizisinin 8 modülüne göre kalanlarının dizisi

$$0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, 2, 3, 5, \ldots$$

olmak üzere bu indirgenmiş dizinin periyodik olduğu ve bu dizinin periyodunun 12 olduğu görülmektedir. Ayrıca indirgenmiş dizinin, periyottaki 12 teriminin her biri 6 terimden oluşan iki yarımı için ikinci yarımın terimleri, ilk yarıma karşılık gelen terimlerin 5 katını oluşturmaktadır. Böylece periyottaki terimler arasında da bir ilişki olduğu, bu durumda kısıtlı periyodun varlığı ve 6 olduğu gözlenir.

Ayrıca burada çarpan olan 5 sayısının kuvvetinin 2 olduğu da gözlenmiştir. Bunun anlamı her yarımdaki 6 terimin 5^2 ile çarpılmasıyla 8 modülüne göre aynı 6 terimin oluşmasıdır. Çünkü $5^2 \equiv 1\ (mod\ 8)$ dir.

Tanım 5.1. Herhangi bir $m > 1$ tam sayısı için $(F_n, F_{n+1}) \equiv (0, 1)\ (mod\ m)$ olacak şekilde en küçük $n = \delta(m)$ pozitif tam sayısına m modülüne göre Fibonacci dizisinin periyodu denir. [3]

Tanım 5.2. Herhangi bir $m > 1$ tam sayısı ve bazı u tam sayıları için $(F_n, F_{n+1}) \equiv u(0, 1)\ (mod\ m)$ olacak şekilde en küçük $n = \alpha(m)$ pozitif tam sayısına m modülüne göre Fibonacci dizisinin kısıtlı periyodu denir. [3]

Tanım 5.3. $0 < u(m) < m$ ve $\left(F_{\alpha(m)}, F_{\alpha(m)+1}\right) \equiv u(m)(0,1)\ (mod\ m)$ olmak üzere $u(m)$ ye m modülüne göre Fibonacci dizisinin çarpanı denir. Ayrıca bu denklikten $F_{\alpha(m)+1} \equiv u(m)\ (mod\ m)$ dir. [3]

Tanım 5.4. m modülüne göre $u(m)$ nin kuvveti $\beta(m)$ ile gösterilir,

$$u(m)^{\beta(m)} \equiv 1\ (mod\ m)$$

şeklinde ifade edilir ve $\beta(m)$ en küçük pozitif tam sayıdır. [3]

Doğrudan hesaplama ile aşağıdaki tablo elde edilir.

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\alpha(m)$	3	4	6	5	12	8	6	12	15	10	12	7	24	20	12	9	12	18
$\beta(m)$	1	2	1	4	2	2	2	2	4	1	2	4	2	2	2	4	2	1
$\delta(m)$	3	8	6	20	24	16	12	24	60	10	24	28	48	40	24	36	24	18

Tanım 5.5. (F_n, F_{n+1}) ile (F_{n-1}, F_n) sıralı ikilisi eşlenirse $F_{n+1} = F_{n-1} + F_n$ için bu eşlemenin matris gösterimi

$$(F_{n-1}, F_n)\mathrm{U} = (F_n, F_{n+1}) \text{ ve } \mathrm{U} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

şeklindedir ve U ya Fibonacci matrisi denir. Ayrıca n üzerinden tümevarımla

$$(F_n, F_{n+1}) = (0,1)\mathrm{U}^n \text{ ve } \mathrm{U}^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$$

elde edilir. [3]

Tanım 5.6. m modülüne göre -1 sayısının kuvveti $\gamma(m)$ ile gösterilir,

$$(-1)^{\gamma(m)} \equiv 1 \ (mod\ m)$$

şeklinde ifade edilir ve $\gamma(m)$ en küçük pozitif tam sayıdır. [3]

Teorem 5.1. $m > 1$ tam sayı olmak üzere $m \mid F_n$ ve $m \mid (F_{n+1} - 1)$ olması için gerek yeter şart $\delta(m) \mid n$ olmasıdır. [3]

İspat: $(F_n, F_{n+1}) \equiv (0,1) \ (mod\ m)$ ve $(F_n, F_{n+1}) = (0,1)\mathrm{U}^n$ olduğundan

$$(F_n, F_{n+1}) = (0,1)\mathrm{U}^n \equiv (0,1) \ (mod\ m)$$

olur ve $\mathrm{U}^n \equiv \mathrm{I} \ (mod\ m)$ bulunur. Böylece

$$(F_n, F_{n+1}) \equiv (0,1) \ (mod\ m) \Leftrightarrow \mathrm{U}^n \equiv \mathrm{I} \ (mod\ m) \qquad (5.1)$$

olur. Yani Fibonacci dizisinin m modülüne göre periyodu ile terimleri I, U, U^2, …, U^n şeklinde olan indirgenmiş matris dizisinin m modülüne göre periyodu eşdeğer olur ve bu indirgenmiş matris dizisinde sonlu sayıda farklı matris bulunduğundan $k + n > k \geq 0$ için $\mathrm{U}^{k+n} \equiv \mathrm{U}^k \ (mod\ m)$ olacak şekilde k ve n tam sayıları vardır. Ayrıca $det(\mathrm{U}^n) \equiv det\ \mathrm{I} \ (mod\ m)$ için $(det\ \mathrm{U})^n \equiv det\ \mathrm{I} \ (mod\ m)$ olur ve U nun determinantı -1 olduğundan bazı pozitif n tam sayıları için $(-1)^n \equiv 1 \ (mod\ m)$ bulunur. Yani sonuç olarak en az bir pozitif n tam sayısı için $\mathrm{U}^n \equiv \mathrm{I} \ (mod\ m)$ olur ve Tanım 5.1 den en küçük pozitif n tam sayısı $\delta(m)$ olduğundan her n pozitif tam sayısı $\delta(m)$ nin tam katı olur. Böylece $\mathrm{U}^n \equiv \mathrm{I} \ (mod\ m)$ olması için gerek ve yeter şart $\delta(m) \mid n$ dir ve Denklik 5.1 den $(F_n, F_{n+1}) \equiv (0,1) \ (mod\ m)$ olması için gerek ve yeter şart $\delta(m) \mid n$ olması bulunur. □

Teorem 5.2. $m > 1$ tam sayı olmak üzere $m \mid F_n$ olması için gerek ve yeter şart $\alpha(m) \mid n$ olmasıdır. [3]

İspat: $(F_n, F_{n+1}) \equiv u(0,1)\ (mod\ m)$ ve $(F_n, F_{n+1}) = (0,1)\mathrm{U}^n$ olduğundan

$$(F_n, F_{n+1}) = (0,1)\mathrm{U}^n \equiv u(0,1)\ (mod\ m)$$

olur ve $\mathrm{U}^n \equiv u\mathrm{I}\ (mod\ m)$ bulunur. Böylece

$$(F_n, F_{n+1}) \equiv u(0,1)\ (mod\ m) \Leftrightarrow \mathrm{U}^n \equiv u\mathrm{I}\ (mod\ m) \qquad (5.2)$$

olur. Benzer şekilde Tanım 5.2 den en küçük pozitif n tam sayısı $\alpha(m)$ olduğundan her n pozitif tam sayısı $\alpha(m)$ nin tam katı olur. Böylece $\mathrm{U}^n \equiv u\mathrm{I}\ (mod\ m)$ olması için gerek ve yeter şart $\alpha(m) \mid n$ dir ve Denklik 5.2 den $(F_n, F_{n+1}) \equiv u(0,1)\ (mod\ m)$ olması için gerek ve yeter şart $\alpha(m) \mid n$ olması bulunur. □

Teorem 5.3. $\delta(m) = \alpha(m)\beta(m) = \big(2, \beta(m)\big)[\gamma(m), \alpha(m)]$ ve $\gamma(2) = 1,\ m > 2$ için $\gamma(m) = 2$ dir. [3]

İspat:

1.

(i) $\mathrm{U}^n \equiv u\mathrm{I}\ (mod\ m)$ denkliğinde $n = \alpha(m)$ alınırsa $\mathrm{U}^{\alpha(m)} \equiv u(m)\mathrm{I}\ (mod\ m)$ bulunur ve Tanım 5.4 den

$$\mathrm{U}^{\alpha(m)\beta(m)} = (\mathrm{U}^{\alpha(m)})^{\beta(m)} \equiv (u(m)\mathrm{I})^{\beta(m)} \equiv \mathrm{I}\ (mod\ m)$$

elde edilir. Böylece $\mathrm{U}^{\alpha(m)\beta(m)} \equiv \mathrm{I}\ (mod\ m)$ olur ve $\mathrm{U}^n \equiv \mathrm{I}\ (mod\ m)$ denkliğini sağlayan en küçük n pozitif tam sayısı $\delta(m)$ olduğundan $\delta(m) \mid [\alpha(m)\beta(m)]$ bulunur.

(ii) $\mathrm{U}^{\alpha(m)} \equiv u(m)\mathrm{I}\ (mod\ m)$ ve $\mathrm{U}^{\delta(m)} \equiv \mathrm{I}\ (mod\ m)$ denkliklerinden

$$\mathrm{U}^{\alpha(m)+\delta(m)} \equiv u(m)\mathrm{I}\ (mod\ m)$$

olur ve $\mathrm{U}^n \equiv u(m)\mathrm{I}\ (mod\ m)$ denkliğini sağlayan en küçük n pozitif tam sayısı $\alpha(m)$ olduğundan $\alpha(m) \mid [\alpha(m) + \delta(m)]$ bulunur. Buradan $\alpha(m) \mid \delta(m)$ elde edilir. Böylece $k \in \mathbb{Z}^+$ için $\delta(m) = \alpha(m)k$ olmak üzere $\mathrm{U}^{\delta(m)} \equiv \mathrm{I}\ (mod\ m)$ denkliğinden

$$(\mathrm{U}^{\alpha(m)})^k \equiv \mathrm{I}\ (mod\ m)$$

olur ve $\mathrm{U}^{\alpha(m)} \equiv u(m)\mathrm{I}\ (mod\ m)$ olduğundan $u(m)^k \equiv 1\ (mod\ m)$ elde edilir. Buradan Tanım 5.4 den k sayısı $\beta(m)$ nin tam katıdır ve $r \in \mathbb{Z}^+$ için $k = \beta(m)r$ olmak üzere $\delta(m) = \alpha(m)k$ eşitliğinden $\delta(m) = \alpha(m)\beta(m)r$ bulunur. Böylece $[\alpha(m)\beta(m)] \mid \delta(m)$ elde edilir. (i) ve (ii) de elde edilen ifadelerden Teorem 5.3 ün ilk kısmı $\delta(m) = \alpha(m)\beta(m)$ dir. □

2. Üçüncü kısmın ispatı için Tanım 5.6 dan $m = 2$ için $(-1)^{\gamma(2)} \equiv 1\ (mod\ 2)$ olduğundan $\gamma(2) = 1$ olur. Ama $m > 2$ için $(-1)^{\gamma(m)} \equiv 1\ (mod\ m)$ olduğunda $\gamma(m) = 1$ olursa $m > 2$ olduğundan $-1 \equiv -1 + m \not\equiv 1\ (mod\ m)$ olur. Bu nedenle $\gamma(m) = 2$ olmalıdır. □

3. İkinci kısmın ispatı için $(det\ \mathrm{U})^{\alpha(m)} = det(\mathrm{U}^{\alpha(m)}) \equiv det(u(m)\mathrm{I})\ (mod\ m)$, $det\ \mathrm{U} = -1$ ve $det(u(m)\mathrm{I}) = (u(m))^2$ olduğundan

$$(-1)^{\alpha(m)} \equiv (u(m))^2\ (mod\ m) \tag{5.3}$$

bulunur. Özel olarak $(-1)^{\alpha(m)}$ ve $(u(m))^2$, m modülüne göre aynı kuvvete sahip olduklarından

$$\frac{\gamma(m)}{\big(\gamma(m), \alpha(m)\big)} = \frac{\beta(m)}{\big(2, \beta(m)\big)} \tag{5.4}$$

bulunur. Öncelikle Eşitlik 5.4 ü ispatlayalım.

(a) $m = 2$ için $\gamma(2) = 1, \alpha(2) = 3$ ve $\beta(2) = 1$ olmak üzere Eşitlik 5.4 ün doğru olduğu görülür.

(b) $m > 2$ için ise $\gamma(m) = 2$ olmak üzere

$$\frac{2}{\big(2, \alpha(m)\big)} = \frac{\beta(m)}{\big(2, \beta(m)\big)} \tag{5.5}$$

olmak üzere Denklik 5.3 de $\alpha(m)$ çift alınırsa $1 \equiv (u(m))^2\ (mod\ m)$ olur ve Tanım 5.4 den $\beta(m)$ en küçük olduğundan $\beta(m) \mid 2$ olur. Bu durumda $\alpha(m)$ çift için Eşitlik 5.5 in $\beta(m) = 1$ ve $\beta(m) = 2$ için doğru olduğu görülür. Ayrıca Denklik 5.3 de $\alpha(m)$ alınırsa $1 \equiv (u(m))^4\ (mod\ m)$ olur ve Tanım 5.4 den $\beta(m)$ en küçük olduğundan $\beta(m) \mid 4$ olur. Böylece $\alpha(m)$ tek için Eşitlik 5.5 in $\beta(m) = 4$ için de doğru olduğu görülür. Burada $\delta(m) = \alpha(m)\beta(m)$ olduğundan $\beta(m) = 1$ ve $\beta(m) = 2$ için $\alpha(m)$

çifttir ve tekrar incelenmez. Böylece $m = 2$ ve $m > 2$ için $\alpha(m)$ nin tek veya çift olması durumu ile Eşitlik 5.4 ispatlanır ve Eşitlik 5.4 den $\beta(m) = \frac{(2,\beta(m))\,\gamma(m)}{(\gamma(m),\alpha(m))}$ elde edilir ve $\delta(m) = \alpha(m)\beta(m)$ eşitliğinde yerine yazılırsa

$$\delta(m) = \alpha(m)\beta(m) = \big(2,\beta(m)\big)\frac{\gamma(m)\alpha(m)}{\big(\gamma(m),\alpha(m)\big)}$$

olur ve $\gamma(m)\alpha(m) = \big(\gamma(m),\alpha(m)\big)[\gamma(m),\alpha(m)]$ olduğundan

$$\delta(m) = \alpha(m)\beta(m) = \big(2,\beta(m)\big)[\gamma(m),\alpha(m)] \qquad (5.6)$$

olur. □

Not: $m > 2$ için $\gamma(m) = 2$ olduğundan Eşitlik 5.6 ile $\delta(m)$ çift sayı olur. Ayrıca Denklik 5.3 den

$$(-1)^{2\alpha(m)} \equiv (u(m))^4 \equiv 1\ (mod\ m)$$

olur ve Tanım 5.4 den $\beta(m)$ en küçük pozitif tam sayı olduğundan $\beta(m) \mid 4$ elde edilir. [3]

Teorem 5.4. $\delta([m_1,m_2]) = [\delta(m_1),\delta(m_2)]$ dir. [3]

İspat: Öncelikle $m' \mid m$ olsun. Bu durumda $U^{\delta(m)} \equiv I\ (mod\ m)$ olduğundan $U^{\delta(m)} \equiv I\ (mod\ m')$ olur ve $U^{\delta(m')} \equiv I\ (mod\ m')$ denkliğinden $\delta(m')$ en küçük pozitif tam sayı olduğundan $\delta(m') \mid \delta(m)$ bulunur. Yani $m' \mid m$ ise $\delta(m') \mid \delta(m)$ elde edilir. Böylece $m_1 \mid m$ ve $m_2 \mid m$ alınırsa $m_1 \mid [m_1,m_2]$ ve $m_2 \mid [m_1,m_2]$ olduğundan $\delta(m_1) \mid \delta([m_1,m_2])$ ve $\delta(m_2) \mid \delta([m_1,m_2])$ elde edilir. Bu durumda $\delta([m_1,m_2])$ sayısı $\delta(m_1)$ ve $\delta(m_2)$ sayılarının ortak katı olur.

Diğer taraftan $m_1 \mid m$ ve $m_2 \mid m$ alınırsa $\delta(m_1) \mid \delta(m)$ ve $\delta(m_2) \mid \delta(m)$ olur. Ayrıca $U^{\delta(m)} \equiv I\ (mod\ m_1)$, $U^{\delta(m)} \equiv I\ (mod\ m_2)$ bulunur. $[m_1,m_2] \mid m$ olduğundan $U^{\delta(m)} \equiv I\ (mod\ [m_1,m_2])$ olur. Buradan $U^{\delta([m_1,m_2])} \equiv I\ (mod\ [m_1,m_2])$

olduğundan $\delta([m_1, m_2]) \mid \delta(m)$ elde edilir. Böylece $\delta([m_1, m_2])$, $\delta(m_1)$ ve $\delta(m_2)$ sayılarının en küçük ortak katı olur. □

Teorem 5.5. $\alpha([m_1, m_2]) = [\alpha(m_1), \alpha(m_2)]$ dir. [3]

İspat: Benzer şekilde öncelikle $m' \mid m$ olsun. Bu durumda $\mathrm{U}^{\alpha(m)} \equiv u\mathrm{I}\ (mod\ m)$ olduğundan $\mathrm{U}^{\alpha(m)} \equiv u\mathrm{I}\ (mod\ m')$ olur ve $\mathrm{U}^{\alpha(m')} \equiv u\mathrm{I}\ (mod\ m')$ denkliğinden $\alpha(m')$ en küçük pozitif tam sayı olduğundan $\alpha(m') \mid \alpha(m)$ bulunur. Yani $m' \mid m$ ise $\alpha(m') \mid \alpha(m)$ elde edilir. Böyece $m_1 \mid m$ ve $m_2 \mid m$ alınırsa $m_1 \mid [m_1, m_2]$ ve $m_2 \mid [m_1, m_2]$ olduğundan $\alpha(m_1) \mid \alpha([m_1, m_2])$ ve $\alpha(m_2) \mid \alpha([m_1, m_2])$ elde edilir. Bu durumda $\alpha([m_1, m_2])$ sayısı $\alpha(m_1)$ ve $\alpha(m_2)$ sayılarının ortak katı olur.

Diğer taraftan $m_1 \mid m$ ve $m_2 \mid m$ alınırsa $\alpha(m_1) \mid \alpha(m)$ ve $\alpha(m_2) \mid \alpha(m)$ olur. Ayrıca $\mathrm{U}^{\alpha(m)} \equiv u\mathrm{I}\ (mod\ m_1)$, $\mathrm{U}^{\alpha(m)} \equiv u\mathrm{I}\ (mod\ m_2)$ bulunur. $[m_1, m_2] \mid m$ olduğundan $\mathrm{U}^{\alpha(m)} \equiv u\mathrm{I}\ (mod\ [m_1, m_2])$ olur. Buradan $\mathrm{U}^{\alpha([m_1, m_2])} \equiv u\mathrm{I}\ (mod\ [m_1, m_2])$ olduğundan $\alpha([m_1, m_2]) \mid \alpha(m)$ elde edilir. $\alpha([m_1, m_2])$, $\alpha(m_1)$ ve $\alpha(m_2)$ sayılarının en küçük ortak katı olur. □

Teorem 5.6. $\alpha(p^e) = \alpha(p)p^{max(0, e-e(p))}$ ve $\delta(p^e) = \delta(p)p^{max(0, e-e(p))}$ olacak şekilde her p tek asal sayısı için $e(p)$ pozitif tam sayısı vardır. [3]

İspat: p herhangi bir tek asal ve e herhangi bir pozitif tam sayı olsun. Bazı B matrisleri için $\mathrm{U}^{\delta(p^e)} = \mathrm{I} + p^e B$ eşitliğinden $\mathrm{U}^{\delta(p^e)} = \mathrm{I} + p^e B \equiv \mathrm{I}\ (mod\ p^e)$ bulunur. Bu denklikten

$$\mathrm{U}^{p\delta(p^e)} = (\mathrm{I} + p^e B)^p \equiv \mathrm{I}\ (mod\ p^{e+1})$$

elde edilir ve $\mathrm{U}^{\delta(p^{e+1})} \equiv \mathrm{I}\ (mod\ p^{e+1})$ denkliğinden $\delta(p^{e+1})$ en küçük pozitif tam sayı olduğundan $\delta(p^{e+1}) \mid p\delta(p^e)$ olur. Ayrıca $\mathrm{U}^{\delta(p^{e+1})} \equiv \mathrm{I}\ (mod\ p^{e+1})$ denkliğinden $p^e \mid p^{e+1}$ olduğundan

$$U^{\delta(p^{e+1})} \equiv I\ (mod\ p^e)$$

bulunur ve $U^{\delta(p^e)} \equiv I\ (mod\ p^e)$ denkliğinden $\delta(p^e)$ en küçük pozitif tam sayı olduğundan $\delta(p^e) \mid \delta(p^{e+1})$ olur. Sonuç olarak p tek asal sayısı için $\delta(p^{e+1}) \mid p\delta(p^e)$ ve $\delta(p^e) \mid \delta(p^{e+1})$ elde edilir. Böylece $k \in \mathbb{Z}^+$ için $\delta(p^{e+1}) = \delta(p^e)k \mid p\delta(p^e)$ olduğundan $k \mid p$ bulunur. Bu durumda $k = 1$ veya $k = p$ olur. Böylece $k \in \mathbb{Z}^+$ için $\delta(p^{e+1}) = \delta(p^e)k$ eşitliğinden

$$\delta(p^{e+1}) = \delta(p^e) \tag{5.7}$$

veya

$$\delta(p^{e+1}) = \delta(p^e)p \tag{5.8}$$

olmak üzere iki durum elde edilir. Özel olarak $\delta(p^e)/\delta(p)$ sayısı p nin negatif olmayan kuvvetine eşittir. Yani n negatif olmayan bir tam sayı olmak üzere $\frac{\delta(p^e)}{\delta(p)} = p^n$ dir. Bu eşitliğin ispatı tümevarım ile yapılırsa $e = 1$ için $\frac{\delta(p)}{\delta(p)} = 1 = p^n$ olacak şekilde negatif olmayan $n = 0$ tam sayısı bulunur ve $e = e$ için doğru olduğunu kabul edelim. Son olarak $e = e + 1$ için $\frac{\delta(p^{e+1})}{\delta(p)} = p^t$ olacak şekilde negatif olmayan bir t tam sayısı bulunduğunu gösterelim. Bunun için $\frac{\delta(p^{e+1})}{\delta(p)} = p^t$,

$$\delta(p^{e+1}) = \delta(p)p^t \tag{5.9}$$

eşitliğinde $\delta(p^{e+1}) = \delta(p^e)p$ yerine yazılırsa

$$\frac{\delta(p^e)}{\delta(p)} = \frac{p^t}{p}$$

elde edilir. Ayrıca $\frac{\delta(p^e)}{\delta(p)} = p^n$ kabulünden $p^n = p^{t-1}$ ve $n = t - 1$ olur. Böylece n negatif olmayan tam sayı olduğundan $t = n + 1$ olacak şekilde negatif olmayan bir tam sayı bulunur ve Eşitlik 5.9 da $\delta(p^{e+1}) = \delta(p^e)$ yerine yazılırsa

$$\frac{\delta(p^e)}{\delta(p)} = p^t$$

elde edilir. Ayrıca $\frac{\delta(p^e)}{\delta(p)} = p^n$ kabulünden $p^n = p^t$ ve $n = t$ olur. Böylece n negatif olmayan tam sayı olduğundan $t = n$ olacak şekilde negatif olmayan bir tam sayı bulunur ve ispat tamamlanır.

Benzer şekilde p herhangi bir tek asal ve e herhangi bir pozitif tam sayı olsun. Bazı B matrisleri için $\mathrm{U}^{\alpha(p^e)} = u\mathrm{I} + p^e B$ eşitliğinden $\mathrm{U}^{\alpha(p^e)} = u\mathrm{I} + p^e B \equiv u\mathrm{I}\ (mod\ p^e)$ bulunur. Bu denklikten

$$\mathrm{U}^{p\alpha(p^e)} = (u\mathrm{I} + p^e B)^p \equiv u\mathrm{I}\ (mod\ p^{e+1})$$

elde edilir ve $\mathrm{U}^{\alpha(p^{e+1})} \equiv u\mathrm{I}\ (mod\ p^{e+1})$ denkliğinden $\alpha(p^{e+1})$ en küçük pozitif tam sayı olduğundan $\alpha(p^{e+1}) \mid p\alpha(p^e)$ olur. Ayrıca $\mathrm{U}^{\alpha(p^{e+1})} \equiv u\mathrm{I}\ (mod\ p^{e+1})$ denkliğinden $p^e \mid p^{e+1}$ olduğundan

$$\mathrm{U}^{\alpha(p^{e+1})} \equiv u\mathrm{I}\ (mod\ p^e)$$

bulunur ve $\mathrm{U}^{\alpha(p^e)} \equiv u\mathrm{I}\ (mod\ p^e)$ denkliğinden $\alpha(p^e)$ en küçük pozitif tam sayı olduğundan $\alpha(p^e) \mid \alpha(p^{e+1})$ olur. Sonuç olarak p tek asal için $\alpha(p^{e+1}) \mid p\alpha(p^e)$ ve $\alpha(p^e) \mid \alpha(p^{e+1})$ elde edilir. Böylece $k \in \mathbb{Z}^+$ için $\alpha(p^{e+1}) = \alpha(p^e)k \mid p\alpha(p^e)$ olduğundan $k \mid p$ bulunur. Bu durumda $k = 1$ veya $k = p$ olur. Böylece $k \in \mathbb{Z}^+$ için $\alpha(p^{e+1}) = \alpha(p^e)k$ eşitliğinden $\alpha(p^{e+1}) = \alpha(p^e)$ veya $\alpha(p^{e+1}) = \alpha(p^e)p$ olmak üzere iki durum elde edilir. Özel olarak $\alpha(p^e)/\alpha(p)$ sayısı p nin negatif olmayan kuvvetine eşittir. Yani n negatif olmayan bir tam sayı olmak üzere $\frac{\alpha(p^e)}{\alpha(p)} = p^n$ dir. Bu eşitliğin ispatı tümevarım ile yapılırsa $e = 1$ için $\frac{\alpha(p)}{\alpha(p)} = 1 = p^n$ olacak şekilde negatif olmayan $n = 0$ tam sayısı bulunur ve $e = e$ için doğru olduğunu kabul edelim. Bu durumda $e = e + 1$ için $\frac{\alpha(p^{e+1})}{\alpha(p)} = p^t$ olacak şekilde negatif olmayan bir t tam sayısı bulunduğunu gösterelim. Bunun için $\frac{\alpha(p^{e+1})}{\alpha(p)} = p^t$,

$$\alpha(p^{e+1}) = \alpha(p)p^t \tag{5.10}$$

eşitliğinde elde edilen durumlardan $\alpha(p^{e+1}) = \alpha(p^e)p$ yerine yazılırsa

$$\frac{\alpha(p^e)}{\alpha(p)} = \frac{p^t}{p}$$

elde edilir. Ayrıca $\frac{\alpha(p^e)}{\alpha(p)} = p^n$ kabulünden $p^n = p^{t-1}$ ve $n = t - 1$ olur. Böylece n negatif olmayan tam sayı olduğundan $t = n + 1$ olacak şekilde negatif olmayan bir tam sayı bulunur. Eşitlik 5.10 da durumlardan $\alpha(p^{e+1}) = \alpha(p^e)$ yerine yazılırsa

$$\frac{\alpha(p^e)}{\alpha(p)} = p^t$$

elde edilir. Ayrıca $\frac{\alpha(p^e)}{\alpha(p)} = p^n$ kabulünden $p^n = p^t$ ve $n = t$ olur. Böylece n negatif olmayan tam sayı olduğundan $t = n$ olacak şekilde negatif olmayan bir tam sayı bulunur ve ispat tamamlanır.

Ayrıca p tek asal ve $\beta(m) = \delta(m)/\alpha(m) \mid 4$ olduğundan

$$\frac{\alpha(p^e)}{\alpha(p^e)} \cdot \frac{\delta(p^e)}{\alpha(p)} = \frac{\delta(p^e)}{\alpha(p)} \cdot \frac{\delta(p)}{\delta(p)}$$

$$\frac{\alpha(p^e)}{\alpha(p)} \cdot \frac{\delta(p^e)}{\alpha(p^e)} = \frac{\delta(p^e)}{\delta(p)} \cdot \frac{\delta(p)}{\alpha(p)}$$

elde edilir ve burada p tek asal olmak üzere $\alpha(p^e)/\alpha(p)$ ve $\delta(p^e)/\delta(p)$ oranı p nin kuvveti olur ve $\delta(p^e)/\alpha(p^e) = \beta(p^e) \mid 4$ ve $\delta(p)/\alpha(p) = \beta(p) \mid 4$ olduğundan $\delta(p^e)/\alpha(p^e)$ ile $\delta(p)/\alpha(p)$ oranı da 2 nin kuvveti olur. Böylece

$$\alpha(p^e)/\alpha(p) = \delta(p^e)/\delta(p) \text{ ve } \delta(p^e)/\alpha(p^e) = \delta(p)/\alpha(p)$$

bulunur. Burada $\delta(p^{e+1}) \neq \delta(p^e)$ olsun. Bu durumda Eşitlik 5.8 den $\delta(p^{e+1}) = p\delta(p^e)$ olur. $\mathrm{U}^{\delta(p^e)} = \mathrm{I} + p^e B,\ B \not\equiv 0\ (mod\ p)$ olmak üzere benzer şekilde $\mathrm{U}^{\delta(p^{e+1})} = \mathrm{I} + p^{e+1}B$ için

$$\mathrm{U}^{\delta(p^{e+1})} = \mathrm{I} + p^{e+1}B \equiv \mathrm{I}\ (mod\ p^{e+1})$$

bulunur ve $\delta(p^{e+1}) = p\delta(p^e)$ ve $B \not\equiv 0\ (mod\ p)$ olduğundan

$$\mathrm{U}^{p\delta(p^e)} = \mathrm{I} + p^{e+1}B \not\equiv \mathrm{I}\ (mod\ p^{e+2})$$

elde edilir. $\delta(p^{e+1}) = p\delta(p^e)$ ise $e = e + 1$ için $\delta(p^{e+2}) = p\delta(p^{e+1})$ olur. Eğer $\delta(p^e) = \delta(p)$ olacak şekilde $e(p)$ en büyük e sayısı ise $1 \leq e \leq e(p)$ için $\delta(p^e) = \delta(p)$ ve $e > e(p)$ için $\delta(p^e) = e^{e-e(p)}\delta(p)$ dir. □

Teorem 5.7. p tek asal ve $(5/p)$ Legendre sembolü iken $\alpha(p) \mid (p - (5/p))$ olur. Ayrıca $p \neq 5$ ise $\delta(p) \mid (p - 1)$ veya $\delta(p) \mid 2(p + 1)$ dir. [3]

İspat:

1. Herhangi bir p asalı modülüne göre U nun kısıtlanmış periyot grafını $R(p)$ ile gösterelim. Bu $R(p)$ grafı $P_0 = (0, 1)$, $P_1 = (1, 1)$, …, $P_{p-1} = (p - 1, 1)$, $P_\infty = (1, 0)$ olmak üzere $(p + 1)$ tane noktadan ve $P_i \to P_i$ ye yönlendirilmiş tüm köşelerden oluşmaktadır. Burada P_i, P_iU matris çarpımına lineer bağımlı olan bir noktadır. Görsel olarak $R(5)$ grafı $P_2 \to P_2$ ye 1 devirden ve $P_0 \to P_1 \to P_3 \to P_4 \to P_\infty \to P_0$ a 5 devirden oluşmaktadır. Genel olarak bu graf birebir eşlemeler ile tanımlanır ve ayrık devirlerin bütününden oluşur. Ayrıca her P_i nin 1 devire sahip olması için gerek ve yeter şart m modülüne göre U nun karakteristik vektörü P_i olmasıdır ya da eşlemede P_i sabit bir nokta olmalıdır. Bununla birlikte $\alpha > 1$ için P_i nin α tane devire sahip olduğu kabul edilirse ve $\{P_i, P_i\mathrm{U}\}$ şeklinde lineer bağımsız bir küme alınırsa $P_i\mathrm{U}^\alpha \equiv uP_i\ (mod\ p)$ denkliği $\mathrm{U}^\alpha \equiv u\mathrm{I}\ (mod\ p)$ anlamına gelir ve $\mathrm{U}^{\alpha(p)} \equiv u\mathrm{I}\ (mod\ p)$ denkliği ile $\alpha(p)$ en küçük pozitif tam sayı olduğundan $\alpha(p) \mid \alpha$ olur ve $\alpha \mid \alpha(p)$ olduğundan $\alpha = \alpha(p)$ bulunur. Böylece $R(p)$, bir devir olanlardan ve $\alpha(p)$ devirden oluşur. Sonuç olarak $R(p)$ nin bir devirli sayısı t olmak üzere $\alpha(p) \mid (p + 1 - t)$ olur ve t aynı zamanda m modülüne göre U nun lineer bağımsız karakteristik vektörlerinin sayısıdır veya U nun $\lambda^2 - \lambda - 1$ minimal polinomunun m modülüne göre farklı köklerinin sayısıdır. Bu kuadratiğin ayırt edici değeri 5 olduğundan t sayısı 0, 1 veya 2 olur. Bu durum Legendre sembolünün $(5/p) = -1$, 0 veya 1 olmasına benzer. Böylece her p tek asal sayısı için $\alpha(p) \mid (p - (5/p))$ elde edilir. □

2. p asal sayısına bağlı bazı u tam sayıları için $\mathrm{U}^{\alpha(p)} \equiv u\mathrm{I}\ (mod\ p)$ ve $\alpha(p) \mid (p-(5/p))$ olduğundan ve $\mathrm{U}^n \equiv \mathrm{I}\ (mod\ m)$ olması için gerek ve yeter şart $\delta(m) \mid n$ olması özelliğinden

$$\mathrm{U}^{(p-(5/p))} \equiv u\mathrm{I}\ (mod\ p) \tag{5.11}$$

$$\mathrm{U}^p \equiv u\mathrm{U}^{(5/p)}\ (mod\ p) \tag{5.12}$$

bulunur.

(i) $m = 5$ ve $p \neq 5$ asal sayı ise $(p, m) = 1$ olduğundan Lemma 4.1 den $(5/p) = 1$ olabilir. Böylece Denklik 5.12 den $\mathrm{U}^p \equiv u\mathrm{U}\ (mod\ p)$ dir ve $iz\ (\mathrm{U}^p) \equiv iz\ (u\mathrm{U})\ (mod\ p)$ olur. Buradan $iz\ (u\mathrm{U}) = u$ ve $(5/p) = 1$ olduğundan $iz\ (\mathrm{U}^p) \equiv (5/p)u\ (mod\ p)$ elde edilir.

(ii) $m = 5$ ve $p \neq 5$ asal sayı ise $(p, m) = 1$ olduğundan Lemma 4.1 den $(5/p) = -1$ olabilir. Böylece Denklik 5.12 den $\mathrm{U}^p \equiv u\mathrm{U}^{-1}\ (mod\ p)$ ve $iz\ (\mathrm{U}^p) \equiv iz\ (u\mathrm{U}^{-1})\ (mod\ p)$ olur. Buradan $iz\ (u\mathrm{U}^{-1}) = -u$ ve $(5/p) = -1$ olduğundan $iz\ (\mathrm{U}^p) \equiv (5/p)u\ (mod\ p)$ elde edilir. Yani (i) ve (ii) den $p \neq 5$ ise

$$iz\ (\mathrm{U}^p) \equiv (5/p)u\ (mod\ p) \tag{5.13}$$

bulunur.

(iii) $m = 5$ ve $p = 5$ ise $(p, m) \neq 1$ olduğundan Lemma 4.1 den $(5/p) = 0$ olur. Böylece Denklik 5.12 den

$$\mathrm{U}^5 \equiv u\mathrm{I}\ (mod\ 5) \tag{5.14}$$

ve $iz\ (\mathrm{U}^5) \equiv iz\ (u\mathrm{I})\ (mod\ 5)$ olur. Buradan $iz\ (u\mathrm{I}) = 2u$ olduğundan

$$iz\ (\mathrm{U}^5) \equiv 2u\ (mod\ 5) \tag{5.15}$$

elde edilir.

Her p tek asal sayısı için $\mathrm{U}^{-1} = \mathrm{U} - \mathrm{I}$ eşitliğinden $\mathrm{U}^{-p} \equiv \mathrm{U}^p - \mathrm{I}\ (mod\ p)$ bulunur ve $iz\ (\mathrm{U}^{-p}) \equiv iz\ (\mathrm{U}^p - \mathrm{I})\ (mod\ p)$ olur. Buradan $iz\ (\mathrm{U}^{-p}) = -iz\ (\mathrm{U}^p)$ olduğundan

$$-iz\,(\mathrm{U}^p) \equiv iz\,(\mathrm{U}^p) - 2\ (mod\ p)$$

$$iz\,(\mathrm{U}^p) \equiv 1\ (mod\ p) \tag{5.16}$$

elde edilir. Denklik 5.15 ve 5.16 dan $p = 5$ için $iz\,(\mathrm{U}^5) \equiv 2u \equiv 1\ (mod\ 5)$ olur ve $u < 5$ olmak üzere bu denkliği sağlayan $u = 3$ olmalıdır. Bu durumda Denklik 5.14 de $u = 3$ alınırsa $\mathrm{U}^5 \equiv 3\mathrm{I}\ (mod\ 5)$ elde edilir. Denklik 5.13 ve 5.16 dan $p \neq 5$ için $iz\,(\mathrm{U}^p) \equiv (5/p)u \equiv 1\ (mod\ p \neq 5)$ bulunur. Yani $(5/p) \equiv u\ (mod\ p)$ olur ve Denklik 5.11 de yerine yazılırsa

$$\mathrm{U}^{(p-(5/p))} \equiv (5/p)\mathrm{I}\ (mod\ p \neq 5) \tag{5.17}$$

elde edilir. Buradan $\mathrm{U}^p \equiv (5/p)\mathrm{U}^{(5/p)}\ (mod\ p \neq 5)$ olur ve $\mathrm{U}^p = \begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix}$ olduğundan

$$\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv (5/p)\mathrm{U}^{(5/p)}\ (mod\ p \neq 5) \tag{5.18}$$

elde edilir. Denklik 5.18 de $(5/p) = 1$ alınırsa $\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv \mathrm{U}\ (mod\ p \neq 5)$ olur ve $\mathrm{U} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ olduğundan $\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\ (mod\ p \neq 5)$ bulunur. Buradan $F_p \equiv 1\ (mod\ p \neq 5)$ dir. Sonuç olarak $(5/p) = 1$ için $F_p \equiv (5/p)\ (mod\ p \neq 5)$ elde edilir. Denklik 5.18 de $(5/p) = -1$ alınırsa $\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv -\mathrm{U}^{-1}\ (mod\ p \neq 5)$ olur ve $\mathrm{U} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ olduğundan $\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}\ (mod\ p \neq 5)$ bulunur. Burada $F_p \equiv -1\ (mod\ p \neq 5)$ dir. Sonuç olarak $(5/p) = -1$ için $F_p \equiv (5/p)\ (mod\ p \neq 5)$ elde edilir. Denklik 5.18 de $(5/p) = 0$ alınırsa $\begin{bmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\ (mod\ 5)$ bulunur ve $F_p \equiv 0\ (mod\ 5)$ dir. Sonuç olarak $p = 5$ için $(5/p) = 0$ olduğundan $F_p \equiv (5/p)\ (mod\ p)$ elde edilir. Yani bu üç durumdan her p tek asal sayısı için

$$F_p \equiv (5/p)\ (mod\ p) \tag{5.19}$$

bulunur.

Ayrıca $\alpha(p) \mid (p-(5/p))$ ve $p \neq 5$ için $(5/p)=1$ alınırsa $\alpha(p) \mid (p-1)$ olur ve Teorem 5.2 den $p \mid F_{p-1}$ bulunur. Denklik 5.19 dan $F_p \equiv 1\ (mod\ p)$ ve $p \mid (F_p-1)$ olur. Böylece $p \mid F_{p-1}$ ve $p \mid (F_p-1)$ olduğundan Teorem 5.1. den $\delta(p) \mid (p-1)$ bulunur. □

Son olarak $\alpha(p) \mid (p-(5/p))$ ve $p \neq 5$ için $(5/p)=-1$ alınırsa $\alpha(p) \mid (p+1)$ ve $\alpha(p) \mid 2(p+1)$ olur. Böylece Teorem 5.2 den $p \mid F_{2(p+1)}$ bulunur. Denklik 5.19 dan $F_p \equiv -1\ (mod\ p)$ olur ve $F_{2p} \equiv -1\ (mod\ p)$ olduğundan $F_{2p+3} \equiv 1\ (mod\ p)$ elde edilir. Böylece $p \mid F_{2(p+1)}$ ve $p \mid (F_{2p+3}-1)$ olduğundan Teorem 5.1 den $\delta(p) \mid 2(p+1)$ bulunur. □

6. m MODÜLÜNE GÖRE PERİYOT VE KISITLI PERİYOT

Daha önceki bölümde verilen tanımlar ve ilişkiler bu bölümde farklı biçimde ele alınacaktır.

Teorem 6.1. Fibonacci dizisi m modülüne göre periyot olduğundan

$$F_{k+n} \equiv F_n \ (mod\ m),\ n = 0, 1, 2, \ldots$$

olacak şekilde bir k tam sayısı vardır. [4]

İspat: Tümevarımla $F_{k+n} \equiv F_n \ (mod\ m)$ denkliğinde, $n = 0$ için $F_k \equiv 0 \ (mod\ m)$ olacak şekilde $k = 0$ tam sayısı vardır ve $n = r$ için $F_{k+r} \equiv F_r \ (mod\ m)$ doğru olsun. Bu durumda $F_{k+r-1} \equiv F_{r-1} \ (mod\ m)$ olur. Son olarak $n = r + 1$ için $F_{k+r+1} \equiv F_{r+1} \ (mod\ m)$ olduğunu gösterelim. $a \equiv b \ (mod\ m)$ ve $c \equiv d \ (mod\ m)$ ise $a + c \equiv b + d \ (mod\ m)$ olduğundan $F_{k+r} \equiv F_r \ (mod\ m)$ ve $F_{k+r-1} \equiv F_{r-1} \ (mod\ m)$ denklikleri taraf tarafa toplanırsa $F_{k+r} + F_{k+r-1} \equiv F_r + F_{r-1} \ (mod\ m)$ elde edilir ve Fibonacci sayılarının lineer rekürans bağıntısından $F_{k+r+1} \equiv F_{r+1} \ (modm)$ elde edilir. □

Tanım 6.1. m modülüne göre Teorem 6.1 deki denkliği sağlayan en küçük k pozitif tam sayısı periyot olup $\delta(m)$ ile gösterilir. [4]

Tanım 6.2. $F_k \equiv 0 \ (mod\ m)$ denkliğini sağlayan en küçük k pozitif tam sayısı kısıtlı periyot (görünme rankı) olup $\alpha(m)$ ile gösterilir. [4]

Teorem 6.2. $\alpha(m) \mid \delta(m)$ dir. [4]

İspat: Özel olarak Teorem 6.1 deki denklikte $k = \delta(m)$ ve $n = 0$ alınırsa $F_{\delta(m)} \equiv F_0 = 0 \ (mod\ m)$ olur. $m \mid F_{\delta(m)}$ olduğundan Teorem 5.2 den $\alpha(m) \mid \delta(m)$ elde edilir. □

Tanım 6.3. $\beta(m)$ fonksiyonu, $\alpha(m)\beta(m) = \delta(m)$ eşitliği ile tanımlanır. Ayrıca bütün m ler için $\beta(m)$ bir tam sayıdır. [4]

Teorem 6.3. $F_{n-1}^2 = F_n F_{n-2} + (-1)^n$ dir. [4]

İspat: Tümevarımla $n = 2$ için $F_1^2 = F_2 F_0 + (-1)^2$ ifadesinden $1 = 1$ doğru olur ve $n = k$ için $F_{k-1}^2 = F_k F_{k-2} + (-1)^k$ doğru olsun. Son olarak $n = k + 1$ için $F_k^2 - F_{k+1}F_{k-1} = (-1)^{k+1}$ olduğunu gösterelim.

$$\begin{aligned} F_k^2 - F_{k+1}F_{k-1} &= F_k^2 - (F_{k-1} + F_k)(F_k - F_{k-2}) \\ &= -F_{k-1}F_k + F_{k-1}F_{k-2} + F_k F_{k-2} \\ &= -F_{k-1}F_k + F_{k-1}F_{k-2} + F_{k-1}^2 - (-1)^k \\ &= -F_{k-1}F_k + F_{k-1}F_k - (-1)^k \\ &= -(-1)^k = (-1)^{k+1} \text{ dir. } \square \end{aligned}$$

Teorem 6.4. $F_{-n} = (-1)^{n+1}F_n$ dir. [4]

İspat:

(i) $F_n = \frac{A^n - B^n}{A-B}$, $A = (1 + \sqrt{5})/2$ ve $B = (1 - \sqrt{5})/2$ olduğundan $A \cdot B = -1$ olur.

$A \cdot B = -1$ olmak üzere $A = -B^{-1}$ ise $A^n = (-1)^n B^{-n}$

$B = -A^{-1}$ ise $B^n = (-1)^n A^{-n}$ olur.

Böylece bulunan değerler yerine yazılırsa

$$(-1)^{n+1}F_n = (-1)^{n+1}\frac{A^n - B^n}{A-B} = (-1)^{n+1}\frac{(-1)^n B^{-n} - (-1)^n A^{-n}}{A-B}$$

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

$$= \frac{A^{-n}-B^{-n}}{A-B} = F_{-n}. \square$$

Böylece Fibonacci dizisi n indisinin bütün tam sayı değerleri için tanımlanır ve bu bağıntı ile negatif indislerin Fibonacci sayılarının bölünebilirlik özelliklerine fazladan bir şey eklemediği görülür. Bu durumda genelleme bozulmayacağından sadece doğal sayı indisleri için Fibonacci dizisi ele alınacaktır.

Teorem 6.5. $F_{n\alpha(m)+r} \equiv F^n_{\alpha(m)-1} F_r \ (mod\ m)$ dir. [4]

İspat: Binet formülü kullanılarak

(i) $F_{k+1} - BF_k = \frac{A^{k+1}-B^{k+1}}{A-B} - \frac{BA^k-BB^k}{A-B} = \frac{A^{k+1}-BA^k}{A-B} = \frac{A^k(A-B)}{A-B} = A^k$ ve $A + B = 1$ olduğundan

$$A^k = F_{k+1} - BF_k = F_{k-1} + F_k - BF_k = F_{k-1} + F_k(1-B) = AF_k + F_{k-1},$$

(ii) $F_{k+1} - AF_k = \frac{A^{k+1}-B^{k+1}}{A-B} - \frac{AA^k-AB^k}{A-B} = \frac{-B^{k+1}+AB^k}{A-B} = \frac{B^k(A-B)}{A-B} = B^k$ ve $A + B = 1$ olduğundan

$$B^k = F_{k+1} - AF_k = F_{k-1} + F_k - AF_k = F_{k-1} + F_k(1-A) = BF_k + F_{k-1}$$

olur.

Ayrıca $A^k - B^k = (A-B)F_k$ ve $k = nk + r$ için

$$(A-B)F_{nk+r} = A^{nk+r} - B^{nk+r} = A^{nk}A^r - B^{nk}B^r$$

olur ve bu eşitlikte (i) ve (ii) de bulunan A^k ve B^k değeri yerine yazılırsa

$$(A-B)F_{nk+r} = (AF_k + F_{k-1})^n A^r - (BF_k + F_{k-1})^n B^r$$

elde edilir. Düzenlenirse $F_{nk+r} = \frac{(AF_k+F_{k-1})^n A^r-(BF_k+F_{k-1})^n B^r}{A-B}$ olur ve $n \geq 0$ için

$$F_{nk+r} = \binom{n}{0}\frac{(A^nA^rF_k^n - B^nB^rF_k^n)}{A-B} + \binom{n}{1}\frac{(A^{n-1}A^rF_k^{n-1}F_{k-1} - B^{n-1}B^rF_k^{n-1}F_{k-1})}{A-B} + \cdots +$$
$$\binom{n}{n}\frac{(F_{k-1}^nA^r - F_{k-1}^nB^r)}{A-B}$$
$$= \binom{n}{0}\frac{F_k^n(A^{n+r} - B^{n+r})}{A-B} + \binom{n}{1}\frac{F_k^{n-1}F_{k-1}(A^{n+r-1} - B^{n+r-1})}{A-B} + \cdots + \binom{n}{n}\frac{F_{k-1}^n(A^r - B^r)}{A-B}$$
$$= \binom{n}{0}F_k^nF_{k-1}^0F_{n+r} + \binom{n}{1}F_k^{n-1}F_{k-1}F_{n+r-1} + \cdots + \binom{n}{n}F_k^oF_{k-1}^nF_r$$

olur ve

$$F_{nk+r} = \sum_{j=0}^{n}\binom{n}{j}F_k^jF_{k-1}^{n-j}F_{r+j}$$

elde edilir. Bu eşitlikte $k = \alpha(m)$ alınırsa

$$F_{n\alpha(m)+r} = \sum_{j=0}^{n}\binom{n}{j}F_{\alpha(m)}^jF_{\alpha(m)-1}^{n-j}F_{r+j}$$

bulunur ve $m \mid F_{\alpha(m)}$ olduğundan Teorem 6.5 elde edilir. Bu denklik negatif ve negatif olmayan r değerleri için geçerlidir. □

Lemma 6.1. $F_{\alpha(m)-1}^n \equiv 1\ (mod\ m)$ denkliğini sağlayan en küçük pozitif n tam sayısı $\beta(m)$ dir. [4]

İspat: $F_{\alpha(m)-1}^n \equiv 1\ (mod\ m)$ olsun. Bu durumda Teorem 6.5 den bütün r ler için $F_{n\alpha(m)+r} \equiv F_r\ (mod\ m)$ olur. Teorem 6.1 den $k = n\alpha(m)$ dir ve Tanım 6.1 den $\delta(m)$ en küçük k pozitif tam sayısı olduğundan $\delta(m) \leq n\alpha(m)$ bulunur. Tanım 6.3 ile de $\beta(m) = \delta(m)/\alpha(m) \leq n$ olur. Teorem 6.5 deki denklikte $r = 1$ ve $n = \beta(m)$ alınırsa $F_{\beta(m)\alpha(m)+1} \equiv F_{\alpha(m)-1}^{\beta(m)}F_1\ (mod\ m)$ elde edilir ve $\delta(m) = \beta(m)\alpha(m)$ olduğundan $F_{\delta(m)+1} \equiv F_{\alpha(m)-1}^{\beta(m)}\ (mod\ m)$ bulunur. Teorem 6.1 deki denklikten

$$F_{\alpha(m)-1}^{\beta(m)} \equiv F_{\delta(m)+1} \equiv F_1 = 1\ (mod\ m),$$

$$F_{\alpha(m)-1}^{\beta(m)} \equiv 1\ (mod\ m)$$

olur. Ayrıca $\beta(m) = \delta(m)/\alpha(m)$ olmak üzere $\delta(m)$, $\alpha(m)$ en küçük pozitif tam sayı olduğundan $\beta(m)$ en küçük pozitif tam sayı olur. Kabul edilen $F_{\alpha(m)-1}^{n} \equiv 1\ (mod\ m)$ denkliğini sağlayan en küçük n pozitif tam sayısı $\beta(m)$ olur. □

Teorem 6.6. $m > 2$ için
(i) $\alpha(m)$ çift ise $\beta(m) = 1$ veya $\beta(m) = 2$,
(ii) $\alpha(m)$ tek ise $\beta(m) = 4$,
Ayrıca $\beta(1) = \beta(2) = 1$ dir. Tersine $\beta(m) = 4$ olursa $\alpha(m)$ tek, $\beta(m) = 2$ olursa $\alpha(m)$ çift ve $\beta(m) = 1$ olursa $\alpha(m)$ çift ya da $m = 1$ veya $m = 2$ dir. [4]

İspat: $m = 1$ veya $m = 2$ için $\beta(1) = 1$ ve $\beta(2) = 1$ dir. $m > 2$ olsun ve Teorem 6.3 deki eşitlikte $n = \alpha(m)$ alınırsa $F_{\alpha(m)-1}^{2} = F_{\alpha(m)}F_{\alpha(m)-2} + (-1)^{\alpha(m)}\ (mod\ m)$ olur. Burada $m \mid F_{\alpha(m)}$ olduğundan

$$F_{\alpha(m)-1}^{2} \equiv (-1)^{\alpha(m)}\ (mod\ m) \tag{6.1}$$

elde edilir.

(i) Denklik 6.1 de $\alpha(m)$ çift ise $F_{\alpha(m)-1}^{2} \equiv 1\ (mod\ m)$ olur. Buradan $F_{\alpha(m)-1} \equiv \pm 1\ (mod\ m)$ bulunur. $F_{\alpha(m)-1} \equiv 1\ (mod\ m)$ olursa Lemma 6.1 den $\beta(m) = 1$ olur ve $F_{\alpha(m)-1} \equiv -1\ (mod\ m)$ olursa $F_{\alpha(m)-1}^{2} \equiv 1\ (mod\ m)$ olduğundan Lemma 6.1 den $\beta(m) = 2$ elde edilir.

(ii) Denklik 6.1 de $\alpha(m)$ tek ise $F_{\alpha(m)-1}^{2} \equiv -1\ (mod\ m)$ olur. Bu durumda $F_{\alpha(m)-1}^{2} \not\equiv 1\ (mod\ m)$ ve $F_{\alpha(m)-1} \not\equiv \pm 1\ (mod\ m)$ olur. Böylece

$$F_{\alpha(m)-1}^{3} = F_{\alpha(m)-1}^{2}F_{\alpha(m)-1} \equiv -F_{\alpha(m)-1} \not\equiv \pm 1\ (mod\ m),$$

$$F_{\alpha(m)-1}^{4} \equiv -F_{\alpha(m)-1}F_{\alpha(m)-1} \equiv 1\ (mod\ m)$$

elde edilir. Böylece Lemma 6.1 den $\beta(m) = 4$ bulunur. Çift taraflı olarak karşıtı da doğru olur. □

Teorem 6.7. p tek asal sayı ve e herhangi bir pozitif tam sayı olmak üzere
(i) $2 \nmid \alpha(p)$ ise $\beta(p^e) = 4$,
(ii) $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ ise $\beta(p^e) = 1$,
(iii) $4 \mid \alpha(p)$ ise $\beta(p^e) = 2$,
(iv) $e \geq 3$ için $\beta(2^e) = 2$ ve $\beta(2) = \beta(2^2) = 1$ dir.
Tersine p herhangi bir tek asal sayı olmak üzere $\beta(p^e) = 4$ ise $\alpha(p)$ tektir. Yani $2 \nmid \alpha(p)$ olur. $\beta(p^e) = 2$ ise $4 \mid \alpha(p)$ veya $e \geq 3$ için $p = 2$ dir. $\beta(p^e) = 1$ ise $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ ya da $p^e = 2$ veya $p^e = 4$ olur. [4]

İspat: p tek asal sayı ve e herhangi bir pozitif tam sayı olsun. Bilinen

$$p^{n+1} \nmid F_{\alpha(p^n)} \text{ ise } \alpha(p^{n+1}) = p\alpha(p^n) \tag{6.2}$$

eşitlik ile bazı $k \in \mathbb{Z}^+ \cup \{0\}$ için $\alpha(p^e) = p^k\alpha(p)$ eşitliğini tümevarımla ispatlayalım. $e = 1$ için $\alpha(p) = p^k\alpha(p)$ olacak şekilde $k = 0 \in \mathbb{Z}^+ \cup \{0\}$ bulunur ve $e = e$ için $\alpha(p^e) = p^k\alpha(p)$ olacak şekilde en az bir $k \in \mathbb{Z}^+ \cup \{0\}$ olsun. Bu durumda $e = e + 1$ için $\alpha(p^{e+1}) = p^n\alpha(p)$ olacak şekilde en az bir $n \in \mathbb{Z}^+ \cup \{0\}$ olduğunu gösterelim. Eşitlik 6.2 de $n = e$ için $\alpha(p^{e+1}) = p\alpha(p^e)$ olur ve kabulden $\alpha(p^e) = p^k\alpha(p)$ yerine yazılırsa $\alpha(p^{e+1}) = p \cdot \alpha(p^e) = p \cdot p^k\alpha(p) = p^{k+1}\alpha(p)$ bulunur. Buradan en az bir $n = k + 1 \in \mathbb{Z}^+ \cup \{0\}$ elde edilir. Böylece $e = e + 1$ için

$$\alpha(p^e) = p^k\alpha(p) \tag{6.3}$$

ispatlanır.

Not: Bu eşitlikte p tek asal sayı olduğundan $\alpha(p^e)$ ve $\alpha(p)$, 2 nin aynı kuvveti ile bölünür. Bu durum ileri de defalarca kullanılmaktadır.

(i) $m = p$ tek asal sayı ve $\alpha(p)$ tek sayı için Eşitlik 6.3 den $\alpha(p^e)$ tek sayı olur. Teorem 6.6 dan $\alpha(p^e)$ tek ise $\beta(p^e) = 4$ bulunur.

(ii) $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ olsun. Eşitlik 6.3 den $\alpha(p^e)$ çift sayı ve Teorem 6.5 de $m = p^e$, $n = 1$ ve $r = -\frac{1}{2}\alpha(p^e)$ alınırsa

$$F_{\alpha(p^e)-\frac{1}{2}\alpha(p^e)} \equiv F_{\alpha(p^e)-1}F_{-\frac{1}{2}\alpha(p^e)} \ (mod\ p^e)$$

$$F_{\frac{1}{2}\alpha(p^e)} \equiv F_{\alpha(p^e)-1}F_{-\frac{1}{2}\alpha(p^e)} \ (mod\ p^e) \qquad (6.4)$$

elde edilir ve Teorem 6.4 den elde edilen $F_{-\frac{1}{2}\alpha(p^e)} = (-1)^{\frac{1}{2}\alpha(p^e)+1}F_{\frac{1}{2}\alpha(p^e)}$ değer Denklik 6.4 de yerine yazılırsa $F_{\frac{1}{2}\alpha(p^e)} \equiv F_{\alpha(p^e)-1}(-1)^{\frac{1}{2}\alpha(p^e)+1}F_{\frac{1}{2}\alpha(p^e)}\ (mod\ p^e)$,

$$F_{\alpha(p^e)-1}F_{\frac{1}{2}\alpha(p^e)} \equiv (-1)^{\frac{1}{2}\alpha(p^e)+1}F_{\frac{1}{2}\alpha(p^e)}\ (mod\ p^e) \qquad (6.5)$$

bulunur. Şimdi negatif olmayan bazı k tam sayıları için Eşitlik 6.3 den $\frac{1}{2}\alpha(p^e) = \frac{1}{2}p^k\alpha(p)$ elde edilir. Her iki taraf $\alpha(p)$ ile bölünürse $\frac{\frac{1}{2}\alpha(p^e)}{\alpha(p)} = \frac{1}{2}p^k$ ve p tek asal sayı olduğundan $\alpha(p) \nmid \frac{1}{2}\alpha(p^e)$ olur. Böylece $\alpha(p) \nmid \frac{1}{2}\alpha(p^e)$ olduğundan Teorem 5.2 den $p \nmid F_{\frac{1}{2}\alpha(p^e)}$ bulunur ve Denklik 6.5 in her iki tarafı $F_{\frac{1}{2}\alpha(p^e)}$ ile bölünürse

$$F_{\alpha(p^e)-1} \equiv (-1)^{\frac{1}{2}\alpha(p^e)+1}\ (mod\ p^e) \qquad (6.6)$$

elde edilir. $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ kabulünden $\frac{1}{2}\alpha(p)$ tek sayı ve Eşitlik 6.3 den $\frac{1}{2}\alpha(p^e)$ de tek sayı olur. Bu durumda Denklik 6.6 dan $F_{\alpha(p^e)-1} \equiv 1\ (mod\ p^e)$ olur. Lemma 6.1 den de $\beta(p^e) = 1$ bulunur.

(iii) $4 \mid \alpha(p)$ olsun. Bu durumda $\frac{1}{2}\alpha(p)$ çift sayı ve Eşitlik 6.3 den $\frac{1}{2}\alpha(p^e)$ de çift sayı olur. Böylece Denklik 6.6 dan $F_{\alpha(p^e)-1} \equiv -1\ (mod\ p^e)$ ve $F^2_{\alpha(p^e)-1} \equiv 1\ (mod\ p^e)$ olur. Böylece Lemma 6.1 den de $\beta(p^e) = 2$ bulunur.

(iv) $\beta(2) = 1$ ve $\beta(2^2) = 1$ olduğu açıktır ve $e \geq 3$ için $\beta(2^e) = 2$ nin ispatı yapılırken aşağıdaki iki hipotez kabul edilmiştir.

(a) $(q, r) = 1$ olmak üzere q herhangi bir asal sayı ve r herhangi bir pozitif tam sayı olmak üzere $q = 2$ ve $f = 1$ olmadığında $q^f \mid F_n$ ve $q^{f+1} \nmid F_n$ ise $q^{f+a} \mid F_{nrq^a}$ ve $q^{f+a+1} \nmid F_{nrq^a}$ dır.

(b) $\delta(q^f) = \delta(q)$ olacak şekilde q herhangi bir asal sayı ve f en büyük tam sayı olmak üzere $e \geq f$ için $\delta(q^e) = q^{e-f}\delta(q)$ dur.

(a) daki hipoteze göre $q = 2$, $f = 3$ ve $n = \alpha(2^3)$ alınırsa $2^3 \mid F_{\alpha(2^3)}$ ve $2^4 \nmid F_{\alpha(2^3)}$ olduğundan $2^{3+a} \mid F_{\alpha(2^3)r2^a}$ ve $2^{4+a} \nmid F_{\alpha(2^3)r2^a}$ olur. Burada $k = 2^a r$ alınırsa $2^a \mid k$ olur. Bu durumda $2^{3+a} \mid F_{k\alpha(2^3)}$ ve $2^{4+a} \nmid F_{k\alpha(2^3)}$ elde edilir. Teorem 5.2 den $\alpha(2^{3+a}) \mid k\alpha(2^3)$ ve $\alpha(2^{4+a}) \nmid k\alpha(2^3)$ olduğundan $\alpha(2^{4+a}) \nmid \alpha(2^{3+a})$ olur. Teorem 5.2 den

$$2^{3+(a+1)} \nmid F_{\alpha(2^{3+a})} \tag{6.7}$$

şeklinde yazılabilir. Ayrıca

$$\alpha(2^{3+a}) = 2^a\alpha(2^3) \tag{6.8}$$

eşitliğini tümevarımla ispatlayalım. $a = 1$ için $\alpha(2^4) = 2\alpha(2^3)$ doğrudur ve $a = a$ için $\alpha(2^{3+a}) = 2^a\alpha(2^3)$ doğru olsun. Bu durumda $a = a + 1$ için $\alpha\left(2^{3+(a+1)}\right) = 2^{a+1}\alpha(2^3)$ olduğunu gösterelim. İfade 6.7 ve Eşitlik 6.2 den $\alpha\left(2^{3+(a+1)}\right) = 2\alpha(2^{3+a})$ yazılır ve kabulden

$$\alpha\left(2^{3+(a+1)}\right) = \alpha\left(2^{(3+a)+1}\right) = 2\alpha(2^{3+a}) = 2 \cdot 2^a\alpha(2^3) = 2^{a+1}\alpha(2^3)$$

olur ve ispat tamamlanır ve

$$e \geq 3 \text{ için } \alpha(2^e) = 2^{e-2}\alpha(2) \tag{6.9}$$

eşitliğini tümevarımla ispatlayalım. $e = 3$ için $\alpha(2^3) = 2\alpha(2)$ doğrudur ve $e = e$ için $\alpha(2^e) = 2^{e-2}\alpha(2)$ doğru olsun. Bu durumda $e = e + 1$ için $\alpha(2^{e+1}) = 2^{e-1}\alpha(2)$ olduğunu gösterelim. İfade 6.7 de $a = e - 3$ alınırsa $2^{e+1} \nmid F_{\alpha(2^e)}$ olduğundan Eşitlik 6.2 de $n = e$ ve $p = 2$ alınırsa $\alpha(2^{e+1}) = 2\alpha(2^e)$ olur ve kabulden $\alpha(2^{e+1}) = 2\alpha(2^e) = 2 \cdot 2^{e-2}\alpha(2) = 2^{e-1}\alpha(2)$ elde edilerek ispat tamamlanır.

(b) hipotezinde $q = 2$ ve $f = 1$ alınırsa

$$e \geq 1 \text{ için } \delta(2^e) = 2^{e-1}\delta(2) \tag{6.10}$$

elde edilir. Böylece Eşitlik 6.9 ve 6.10 dan $e \geq 3$ için $\beta(2^e) = \frac{\delta(2^e)}{\alpha(2^e)} = \frac{2^{e-1}\delta(2)}{2^{e-2}\alpha(2)} = 2$ elde edilerek Teorem 6.7 nin son kısmı da bulunur. □

Lemma 6.2. m asal çarpanlarına ayrılırsa, yani $m = {q_1}^{\lambda_1}{q_2}^{\lambda_2} \dots {q_n}^{\lambda_n}$ ise
(i) $1 \leq i \leq n$ için $\delta(m) = ekok\left\{\delta({q_i}^{\lambda_i})\right\}$,
(ii) $1 \leq i \leq n$ için $\alpha(m) = ekok\left\{\alpha({q_i}^{\lambda_i})\right\}$ dir. [4]

İspat: $m = {q_1}^{\lambda_1}{q_2}^{\lambda_2} \dots {q_n}^{\lambda_n}$ olsun.
(i) Fibonacci dizisinin ${q_i}^{\lambda_i}$ modülüne göre periyodu $\delta({q_i}^{\lambda_i})$ dir. Yani Fibonacci dizisi ${q_i}^{\lambda_i}$ modülüne göre $c \cdot \delta({q_i}^{\lambda_i})$ uzunluğunda da tekrar eder. Bu dizinin m modülüne göre periyodu ise $\delta(m)$ olduğundan i nin tüm değerleri için bu dizi ${q_i}^{\lambda_i}$ modülüne göre $\delta(m)$ uzunluğunda da tekrar eder. Dolayısıyla i nin tüm değerleri için $\delta(m)$, $c \cdot \delta({q_i}^{\lambda_i})$ formundadır. Böylece $1 \leq i \leq n$ için $\delta(m) = ekok\left\{\delta({q_i}^{\lambda_i})\right\}$ elde edilir.

(ii) ${q_i}^{\lambda_i}$ ler aralarında asal sayı olmak üzere $m \mid F_k$ ile ${q_i}^{\lambda_i} \mid F_k$ $(i = 1, 2, \dots, n)$ ifadeleri denktir. ${q_i}^{\lambda_i} \mid F_k$ olduğundan Teorem 5.2 den $\alpha({q_i}^{\lambda_i}) \mid k$ $(i = 1, 2, \dots, n)$ olur. $1 \leq i \leq n$ için bu koşulları sağlayan en küçük $k = ekok\left\{\alpha({q_i}^{\lambda_i})\right\}$ bulunur. $\alpha(m)$ nin tanımından istenen sonuç ortaya çıkar. Yani $m \mid F_k$ ve k en küçük pozitif tam sayı olduğundan $\alpha(m) = k = ekok\left\{\alpha({q_i}^{\lambda_i})\right\}$ bulunur. □

Teorem 6.8.
(i) $m > 2$ ve $\alpha(m)$ tek sayı ise $\beta(m) = 4$ dür.
(ii) Herhangi bir p tek asal sayı olmak üzere $p \mid m$ için $8 \nmid m$, $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ olması için gerek ve yeterli şart $\beta(m) = 1$ olmasıdır.
(iii) m nin diğer durumlarında $\beta(m) = 2$ dir. [4]

İspat:

(a) Teorem 6.6 dan (i) doğrudur.

(b) $\beta(m) = 1$ için (ii) de verilen koşullar gerekli ve yeterlidir ve m nin asal çarpanlarına ayrılmış hali $m = {q_1}^{\lambda_1} {q_2}^{\lambda_2} \dots {q_n}^{\lambda_n}$ olsun. Ayrıca K_i tek tam sayı olmak üzere

$$\alpha({q_i}^{\lambda_i}) = 2^{\varepsilon_i} K_i \ \ (i = 1, 2, \dots, n)$$

olarak yazılabilir. Teorem 6.6 dan görülüyor ki $\varphi_i = 0$, 1 veya 2 olmak üzere

$$\beta\left({q_i}^{\lambda_i}\right) = 2^{\varphi_i} \ \ (i = 1, 2, \dots, n)$$

olarak yazılabilir. Tanım 6.3 den $\delta\left({q_i}^{\lambda_i}\right) = \alpha({q_i}^{\lambda_i})\beta({q_i}^{\lambda_i}) = 2^{\varepsilon_i + \varphi_i} K_i$ $(i = 1, 2, \dots, n)$ elde edilir. K_i tek tam sayı olmak üzere Lemma 6.2 den

$$\delta(m) = ekok\left\{\delta({q_i}^{\lambda_i})\right\} = 2^{max(\varepsilon_i + \varphi_i)} K$$

$$\alpha(m) = ekok\left\{\alpha({q_i}^{\lambda_i})\right\} = 2^{max(\varepsilon_i)} K$$

olur. Böylece

$$\beta(m) = \delta(m)/\alpha(m) = 2^{max(\varepsilon_i + \varphi_i) - max(\varepsilon_i)} \qquad (6.11)$$

bulunur. (ii) nin ispatı için p tek asal sayı olmak üzere $p \mid m$ için $p = q_k$ $(k = 1, 2, \dots, n)$ olur ve $\beta(m) = 1$ olsun. Bu durumda $m = {q_1}^{\lambda_1} {q_2}^{\lambda_2} \dots {q_n}^{\lambda_n}$ ve $p = q_k$ $(k = 1, 2, \dots, n)$ olduğundan m tek sayı olur. Böylece $8 \nmid m$ koşulu elde edilir. $\beta(m) = 1$ olduğundan Eşitlik 6.11 den $2^{max(\varepsilon_i + \varphi_i) - max(\varepsilon_i)} = 1$ olur ve $max(\varepsilon_i + \varphi_i) - max(\varepsilon_i) = 0$ bulunur. Yani $max(\varepsilon_i + \varphi_i) = max(\varepsilon_i)$ dır. $max(\varepsilon_i) = \varepsilon_k$ olarak alınırsa $\varepsilon_k \leq \varepsilon_k + \varphi_k \leq max(\varepsilon_i + \varphi_i) = max(\varepsilon_i) = \varepsilon_k$ ve $\varepsilon_k + \varphi_k \geq max(\varepsilon_i + \varphi_i)$ den dolayı $\varepsilon_k + \varphi_k = max(\varepsilon_i + \varphi_i)$ olur. Ayrıca $max(\varepsilon_i + \varphi_i) = max(\varepsilon_i) = \varepsilon_k$ olduğundan $\varepsilon_k + \varphi_k = \varepsilon_k$ olur. Bu durumda $\varphi_k = 0$ bulunur. Böylece $\beta({q_k}^{\lambda_k}) = 2^{\varphi_k} = 1$ olur. Teorem 6.7 nin (ii). kısmında $p = q_k$ ve $e = \lambda_k$ alınırsa $\beta({q_k}^{\lambda_k}) = 1$ olması için gerek ve yeter şart $2 \mid \alpha(q_k)$ ama $4 \nmid \alpha(q_k)$ olmasıdır. Buradan $\alpha(q_k)$ ve $\alpha({q_k}^{\lambda_k})$, 2 nin aynı kuvvetine bölündüğünden $2 \mid \alpha(q_k^{\lambda_k})$ ama $4 \nmid \alpha(q_k^{\lambda_k})$ koşulu da elde edilir. Böylece $\alpha(q_k^{\lambda_k}) = 2^{\varepsilon_k} K_k$ dan

$\varepsilon_k \leq 1$ bulunur ve $\varphi_i \leq max(\varepsilon_i + \varphi_i) = max(\varepsilon_i) = \varepsilon_k \leq 1$ olduğundan $\varphi_i \leq 1$ olur. $\varphi_i = 1$ olursa $\beta({q_i}^{\lambda_i}) = 2$ olur. Teorem 6.7. nin (iii). kısmında $p = q_k$ ve $e = \lambda_k$ alınırsa $\beta({q_k}^{\lambda_k}) = 2$ olması için gerek ve yeter şart $4 \mid \alpha(q_k)$ olmasıdır. Buradan $\alpha(q_k)$ ve $\alpha({q_k}^{\lambda_k})$, 2 nin aynı kuvvetine bölündüğünden $4 \mid \alpha(q_k^{\lambda_k})$ elde edilir. Böylece $\alpha(q_k^{\lambda_k}) = 2^{\varepsilon_k} K_k$ dan $\varepsilon_k > 1$ ve $\varepsilon_i > 1$ olur. Yani $\varphi_i = 1$ ve $\varepsilon_i > 1$ ile $\varepsilon_i + \varphi_i > 2$ elde edilir. Bu durum daha önceden bulunan $max(\varepsilon_i + \varphi_i) \leq 1$ ile çelişir. Yani $\varphi_i = 1$ olması imkansızdır. Böylece $\varphi_i = 0$ olmalıdır. Böylece $\beta({q_i}^{\lambda_i}) = 2^{\varphi_i} = 1$ olur. Teorem 6.7 nin (ii). kısmında $p = q_i$ ve $e = \lambda_i$ alınırsa $\beta({q_i}^{\lambda_i}) = 1$ olması için gerek ve yeter şart $2 \mid \alpha(q_i)$ ama $4 \nmid \alpha(q_i)$ olmasıdır. Buradan $p = q_i$ olduğundan $2 \mid \alpha(p)$ ama $4 \nmid \alpha(p)$ koşulu da elde edilir.

Teoremin karşıtı için (ii) de verilen p tek asal sayı olmak üzere $p \mid m$ için $p = q_i$ $(i = 1, 2, \dots, n)$, $8 \nmid m$, $2 \mid \alpha(q_i^{\lambda_i})$ ama $4 \nmid \alpha(q_i^{\lambda_i})$ koşulların yerine getirildiğini varsayalım. Bu durumda $2 \mid \alpha(q_i)$ ama $4 \nmid \alpha(q_i)$ olması için gerek ve yeter şart $\beta({q_i}^{\lambda_i}) = 1$ elde edilir. Böylece $\delta({q_i}^{\lambda_i}) = \alpha({q_i}^{\lambda_i})\beta({q_i}^{\lambda_i})$ eşitliğinden $\delta({q_i}^{\lambda_i}) = \alpha({q_i}^{\lambda_i})$ olur. Lemma 6.2 den $1 \leq i \leq n$ için

$$\delta(m) = ekok\left\{\delta({q_i}^{\lambda_i})\right\} = ekok\left\{\alpha({q_i}^{\lambda_i})\right\} = \alpha(m)$$

olur. Sonuç olarak $\delta(m) = \alpha(m)\beta(m)$ eşitliğinden $\beta(m) = 1$ bulunur ve ispat tamamlanır.

(c) Teorem 6.6 dan $\beta(m) = 1$, 2 veya 4 olduğundan m nin diğer durumları için tek bir durum kalıyor. Bu durum $\beta(m) = 2$ olmasıdır. □

Lemma 6.3. p tek asal sayı olsun. Bu durumda
(i) $p \equiv \pm 1 \ (mod\ 10)$ ise $\alpha(p) \mid (p - 1)$,
(ii) $p \equiv \pm 3 \ (mod\ 10)$ ise $\alpha(p) \mid (p + 1)$,
(iii) $p \equiv \pm 1 \ (mod\ 10)$ ise $\delta(p) \mid (p - 1)$,
(iv) $p \equiv \pm 3 \ (mod\ 10)$ ise $\delta(p) \nmid (p + 1)$ ve $\delta(p) \mid 2(p + 1)$ dir. [4]

İspat: Lucas (1878) de $p \equiv \pm 1 \ (mod\ 10)$ ise $p \mid F_{p-1}$ ve $p \equiv \pm 3 \ (mod\ 10)$ ise $p \mid F_{p+1}$ dir. Bu sonuçlar ile Teorem 5.2 den yaralanarak $p \equiv \pm 1 \ (mod\ 10)$ ise $p \mid F_{p-1}$ olması için gerek ve yeter şart $\alpha(p) \mid (p-1)$ bulunur. Böylece (i) elde edilir. $p \equiv \pm 3 \ (mod\ 10)$ ise $p \mid F_{p+1}$ olması için gerek ve yeter şart $\alpha(p) \mid (p+1)$ bulunur. Böylece (ii) elde edilir. Teorem 5.7 de (iii) ve Teorem 4.7 de (iv) ispatlandı. □

Teorem 6.9. p tek asal sayı ve e herhangi bir pozitif tam sayı olsun.
(i) $p \equiv 11$ veya $p \equiv 19 \ (mod\ 20)$ ise $\beta(p^e) = 1$,
(ii) $p \equiv 3$ veya $p \equiv 7 \ (mod\ 20)$ ise $\beta(p^e) = 2$,
(iii) $p \equiv 13$ veya $p \equiv 17 \ (mod\ 20)$ ise $\beta(p^e) = 4$,
(iv) $p \equiv 21$ veya $p \equiv 29 \ (mod\ 40)$ ise $\beta(p^e) \neq 2$ dir. [4]

İspat: Teorem 6.7 den $\beta(p^e)$ nin e değerinden bağımsız olduğu görülür. Böylece ispat boyunca $e = 1$ alınabilir. Tanım 6.2 den $p \mid F_{\alpha(p)}$ olur ve $(F_{\alpha(p)}, F_{\alpha(p)-1}) = 1$ olduğundan $p \nmid F_{\alpha(p)-1}$ bulunur. $m = F_{\alpha(p)-1}$ alınırsa Lemma 4.2 den $\left(F_{\alpha(p)-1}, p\right) = 1$ olduğundan

$$F_{\alpha(p)-1}^{p-1} \equiv 1 \ (mod\ p) \tag{6.12}$$

elde edilir. Sonra Lemma 6.1 den $F_{\alpha(p)-1}^{\beta(p)} \equiv 1 \ (mod\ p)$ olacak şekilde $\beta(p)$ en küçük olur. Bu durumda Denklik 6.12 den $\beta(p) \mid (p-1)$ bulunur. Ayrıca $p \equiv 3 \ (mod\ 4)$ için $p = 4k+3$ olduğundan $4 \nmid (p-1)$ olur ve $\beta(p) \mid (p-1)$ ifadesinden $\beta(p) \neq 4$ bulunur. Bu durumda $\beta(p) = 2$ ya da $\beta(p) = 1$ olabilir.

(i) $p \equiv 3 \ (mod\ 4)$ ise $4 \nmid (p-1)$ ve $\beta(p) \neq 4$ için $\beta(p) = 2$ olsun. Teorem 6.7 den $4 \mid \alpha(p)$ olur. Şimdi $p \equiv \pm 1 \ (mod\ 10)$ olduğu zamanlar Lemma 6.3 den $\alpha(p) \mid (p-1)$ bulunur. $4 \mid \alpha(p)$ ve $\alpha(p) \mid (p-1)$ ifadelerinden $4 \mid (p-1)$ elde edilir. Ama bu durum $4 \nmid (p-1)$ ile çelişir. Bu nedenle $\beta(p) \neq 2$ olmalıdır. Sonuç olarak $\beta(p) \neq 4$ ve $\beta(p) \neq 2$ olduğundan $\beta(p) = 1$ ispatlanır. Yani $p \equiv 3 \ (mod\ 4)$ için $p \equiv \pm 1 \ (mod\ 10)$ olduğu zamanlar, $p \equiv 11$ veya $p \equiv 19 \ (mod\ 20)$ dir. Böylece $p \equiv 11$ veya $p \equiv 19 \ (mod\ 20)$ ise $\beta(p^e) = 1$ olur.

(ii) $p \equiv 3\ (mod\ 4)$ ise $\beta(p) \neq 4$ dür. Şimdi $p \equiv \pm 3\ (mod\ 10)$ olduğu zamanlar Lemma 6.3 den $\alpha(p) \mid (p+1)$ ve $\delta(p) \nmid (p+1)$ bulunur. Yani $\delta(p) \neq \alpha(p)$ olur ve $\beta(p) = \frac{\delta(p)}{\alpha(p)} \neq 1$ elde edilir. Böylece $\beta(p) \neq 1$ ve $\beta(p) \neq 4$ olduğundan $\beta(p) = 2$ bulunur. Yani $p \equiv 3\ (mod\ 4)$ için $p \equiv \pm 3\ (mod\ 10)$ olduğu zamanlar, $p \equiv 3$ veya $p \equiv 7\ (mod\ 20)$ dir. Sonuç olarak $p \equiv 3$ veya $p \equiv 7\ (mod\ 20)$ ise $\beta(p^e) = 2$ olur.

(iii) $p \equiv \pm 3\ (mod\ 10)$ için $\beta(p) \neq 1$ ayrıca $\alpha(p) \mid (p+1)$ olduğu biliniyor. $p \equiv 1\ (mod\ 4)$ için $p = 4k+1$ olduğundan $4 \nmid (p+1)$ olur ve $\alpha(p) \mid (p+1)$ olduğundan $4 \nmid \alpha(p)$ dir. Teorem 6.7 den $4 \nmid \alpha(p)$ olması için gerek ve yeter şart $\beta(p^e) \neq 2$ yani $\beta(p) \neq 2$ bulunur. Böylece $\beta(p) \neq 1$ ve $\beta(p) \neq 2$ olduğundan $\beta(p) = 4$ olur. Sonuç olarak $\beta(p^e) = 4$ ispatlanır. Yani $p \equiv \pm 3\ (mod\ 10)$ için $p \equiv 1\ (mod\ 4)$ olduğu zamanlar, $p \equiv 13$ veya $p \equiv 17\ (mod\ 20)$ dir. Sonuç olarak $p \equiv 13$ veya $p \equiv 17\ (mod\ 20)$ ise $\beta(p^e) = 2$ olur.

(iv) $p \equiv 21\ (mod\ 40)$ ve $p \equiv 29\ (mod\ 40)$ ve $\beta(p) = 2$ olsun. Bu durumda $\delta(p) = \beta(p)\alpha(p)$ olduğundan $\delta(p) = 2\alpha(p)$ ve Teorem 6.7 den $4 \mid \alpha(p)$ olduğundan $8 \mid \delta(p)$ elde edilir. $p \equiv \pm 1\ (mod\ 10)$ alınırsa Lemma 6.3 den $\delta(p) \mid (p-1)$ olur. Böylece $8 \mid \delta(p)$ ve $\delta(p) \mid (p-1)$ olduğundan $8 \mid (p-1)$ bulunur. Ama kabulden $p-1 \equiv 20\ (mod\ 40)$ ve $p-1 \equiv 28\ (mod\ 40)$ olduğundan $p-1 \equiv 4\ (mod\ 8)$ olmalıdır. Bu durum $8 \mid (p-1)$ ile çelişir. Yani $\beta(p) \neq 2$ olmalıdır. □

Doğal olarak $p \equiv 1, 9, 21, 29\ (mod\ 40)$ için $\beta(p^e)$ ile ilgili aşağıdaki örnekler teoremin desteklendiğini gösterir.

$p \equiv\ 1\ (mod\ 40)\ :\ \beta(521) = 1,\ \beta(41) = 2,\ \beta(761) = 4,$
$p \equiv\ 9\ (mod\ 40)\ :\ \beta(809) = 1,\ \beta(409) = 2,\ \beta(89) = 4,$
$p \equiv 21\ (mod\ 40)\ :\ \beta(101) = 1,\ \beta(61) = 4,$
$p \equiv 29\ (mod\ 40)\ :\ \beta(29) = 1,\ \beta(109) = 4$ dür.

7. FİBONACCİ DİZİSİNİN GENEL BÖLÜNEBİLİRLİK ÖZELLİKLERİ

7.1. Fibonacci Sayılarının Temel Özellikleri

Bu bölümde belirli bir tam sayının kuvvetleri tarafından bölünebilen Fibonacci sayılarının alt dizisi ile ilgilenilecektir. Yani Fibonacci sayıları belirli bir tam sayının kuvvetine bölündüğü zaman elde edilen kalanların dizisinin periyodik yapısı ile ilgili tanımlar ve problemler ele alınacaktır.

Teorem 7.1.1. $n \geq 1$ için

$$F_n = \left(\frac{1}{2}\right)^{n-1} \sum_{s=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2s+1} 5^s$$

dir. [5]

Teorem 7.1.2. $k \geq 0$ ve $F_0 = 0$ için

$$F_{kn+r} = \sum_{h=0}^{k} \binom{k}{h} F_n^h F_{n-1}^{k-h} F_{r+h}$$

dir. [5]

Teorem 7.1.3.

$$F_{kn} = F_n \sum_{h=1}^{k} \binom{k}{h} F_n^{h-1} F_{n-1}^{k-h} F_h$$

dir. [5]

Teorem 7.1.4. $\binom{k+1}{h} = \binom{k}{h} + \binom{k}{h-1}$ dir. [5]

Teorem 7.1.5. $0 < s < p$ ve p asal sayı ise $p \mid \binom{p}{s}$ dir. [5]

Tanım 7.1.1. m^n ile bölünebilen pozitif indisli en küçük Fibonacci sayısının indisi α ile gösterilir. Yani $F_k \equiv 0\ (mod\ m^n)$ denkliğini sağlayan en küçük k pozitif tam sayısı kısıtlı periyot veya görünme rankı olarak adlandırılır ve α ile gösterilir. [5]
$F_\alpha \equiv 0\ (mod\ m^n)$ olmak üzere, bu denkliğin farklı gösterimleri

$$\alpha(m,n) = \alpha(m^n,1) = \alpha(m^n)$$

dir. [5]

Tanım 7.1.2. $F_k \equiv 0\ (mod\ m^n)$ ve $F_{k+1} \equiv 1\ (mod\ m^n)$ denkliklerini sağlayan en küçük k pozitif tam sayısı periyot veya karakteristik sayı olarak adlandırılır ve δ ile gösterilir. [5]
$F_\delta \equiv 0\ (mod\ m^n)$ ve $F_{\delta+1} \equiv 1\ (mod\ m^n)$ olmak üzere, bu denkliğin farklı gösterimleri $\delta(m,n) = \delta(m^n,1) = \delta(m^n)$ dir. [5]

Tanım 7.1.3. $\delta(m,n)/\alpha(m,n) = \beta(m,n) = \beta(m^n,1) = \beta(m^n)$ dir. [5]

Tanım 7.1.4. $F_{\alpha(m,n)} \equiv 0\ (mod\ m^t)$ denkliğini sağlayan en büyük t tam sayısı ϑ ile gösterilir. [5]
$F_\alpha \equiv 0\ (mod\ m^\vartheta)$ olmak üzere, bu denkliğin farklı gösterimleri

$$\vartheta(m,n) = \vartheta(m^n,1) = \vartheta(m^n)$$

dir. [5]

Teorem 7.1.6. $\alpha(m,n) = \alpha(m,n+1) = \cdots = \alpha\big(m,\vartheta(m,n)\big) < \alpha(m,\vartheta(m,n)+1)$ dir. [5]

Teorem 7.1.7. $\vartheta\big(m,\vartheta(m,n)\big) = \vartheta(m,n)$ dir. [5]

7.2. Bölünebilirlik Özellikleri İçin Yardımcı Bağıntılar

Lemma 7.2.1. F_n, F_{n+1} ve F_{n+2} daima aralarında asal sayıdır. [5]

İspat: h pozitif bir tam sayı olsun. Fibonacci lineer rekürans bağıntısında h, sayıların ikisini bölerse üçüncü sayıyı da böler. Bu durum Fibonacci dizisinin tüm terimleri için uygulanırsa h, bütün Fibonacci sayılarını böler. Böylece bütün terimleri bölen $h = 1$ olmak zorundadır. Yani F_n, F_{n+1} ve F_{n+2} aralarında asal sayı olur. □

Lemma 7.2.2. $n \geq 2$ alınırsa F_n, n nin kesinlikle artan pozitif fonksiyonudur. [5]

İspat: Rekürans bağıntısından $n \geq 2$ için $F_n = F_{n-1} + F_{n-2}$ ve $F_{n-2} \geq 0$, $F_{n-1} \geq 1$ olduğundan $F_n \geq 1$ olur. $F_{n+1} = F_n + F_{n-1}$, $F_n \geq 1$ ve $F_{n-1} \geq 1$ olduğundan $F_{n+1} \geq 2$ ve $F_{n+1} > F_n$ olur. Böylece $F_{n+1} > F_n \geq 1$ olduğundan F_n, n nin kesinlikle artan pozitif fonksiyonudur. □

Lemma 7.2.3. $n \geq 3$ ise $\alpha(F_n) = n$. Yani F_n ile bölünebilen en küçük pozitif indisli Fibonacci sayısının indisi n dir. [5]

Lemma 7.2.4. $(F_m, F_n) = F_{(m,n)}$ dir. [5]

İspat: $(m,n)=z$ ve $(F_m,F_n)=Z$ alalım. Ayrıca $z=(m,n)$ olduğundan $z=xm+yn$ olacak şekilde x ve y pozitif tam sayıları vardır. Teorem 7.1.2 de $kn+r$ yerine $xm+yn$ yazılırsa ($k=x, n=m$ ve $r=yn$) ve $x\geq 0$ için

$$F_z = F_{xm\,+\,yn} = \sum_{h=0}^{x} \binom{x}{h} F_m^h F_{m-1}^{x-h} F_{yn+h} \qquad (7.2.1)$$

elde edilir.

(i) $(F_m,F_n)=Z$ olduğundan $Z \mid F_n$ ve $n \mid ny$ ise $F_n \mid F_{ny}$ bulunur. Bu durumda $Z \mid F_n$ ve $F_n \mid F_{ny}$ ise $Z \mid F_{yn}$ elde edilir. Eşitlik 7.2.1 den

$$F_z = F_{m-1}^{x} F_{yn} + \sum_{h=1}^{x} \binom{x}{h} F_m^h F_{m-1}^{x-h} F_{yn+h}$$

bulunur. Elde edilen bu eşitlikte $Z \mid F_{yn}$ ve $Z \mid F_m$ olduğundan $Z \mid F_z$ ispatlanır. Sonuç olarak

$$F_z = F_{xm\,+\,yn} = \sum_{h=0}^{x} \binom{x}{h} F_m^h F_{m-1}^{x-h} F_{yn+h} \equiv 0\ (mod\ Z)$$

elde edilir.

(ii) $z=(m,n)$ ise $z \mid m$ ve $z \mid n$ ise $F_z \mid F_m$ ve $F_z \mid F_n$ olduğundan $F_z \mid (F_m,F_n)=Z$ olur ve $F_z \mid Z$ elde edilir. Böylece (i) ve (ii) den $Z \mid F_z$ ve $F_z \mid Z$ olduğundan $Z=F_z$ dir. Yani $(F_m,F_n)=F_{(m,n)}$ bulunur. □

Lemma 7.2.5. $F_n \mid F_m$ olması için gerek ve yeter şart $n \mid m$ veya $n=2$ olmasıdır. [5]

İspat: $F_n \mid F_m$ olsun. Bu durumda $(F_m,F_n)=F_n$ ve Lemma 7.2.4 den $(F_m,F_n)=F_{(m,n)}=F_n$ olur. Böylece $n=(m,n)$ olduğundan $n \mid m$ elde edilir. Karşıtı da doğrudur. Ya da $n=2$ olursa $F_2=1$ olduğundan $F_2=1 \mid F_m$ olur. □

Tanım 7.2.1. F_n nin m ile bölümünden kalan $F_n{}^{(m)}$ ile gösterilir. $0 \leq F_n{}^{(m)} < m$ için $F_n \equiv F_n{}^{(m)}\ (mod\ m)$ şeklindedir ve F_n nin m modülüne göre kalanı diye okunur. [5]

Lemma 7.2.6. $m \geq 2$ olacak şekilde herhangi bir tam sayı modülüne göre $F_n^{(m)}$ kalanların dizisi periyodiktir ve periyodu $\delta(m)$ dir. Bu durumda n doğal sayı ve k tam sayı olmak üzere

$$\begin{cases} F_{n+k\delta(m)}^{(m)} = F_n^{(m)} \\ \text{ya da} \\ F_{n+k\delta(m)} \equiv F_n\ (mod\ m) \end{cases}$$

şeklindedir. [5]

İspat: m modülüne göre $(F_n^{(m)}, F_{n+1}^{(m)})$ sıralı tam sayı çifti en fazla m^2 tane farklı değer alır. Böylece (m^2+1) tane $F_0^{(m)}$, $F_1^{(m)}$, …, $F_{m^2+1}^{(m)}$ sayılarından oluşan sıralı ardışık çiftlerden birinin tekrar etmesi gerekir. Yani bir ardışık çiftin eşi m^2 tane sıralı çiftten birine eşittir. Bu durumda rekürans bağıntısı da kullanılarak iki eşit çiftin indisleri üzerinden geriye doğru tümevarım yoluyla $2 \leq k \leq m^2$ için $\left(F_k^{(m)}, F_{k+1}^{(m)}\right) = \left(F_0^{(m)}, F_1^{(m)}\right) = (0,1)$ elde edilir. Yani baştaki çift bulunur ve dizi başa döner. Böylece Tanım 7.1.2 den bunu sağlayan en küçük k pozitif tam sayısı $\delta(m)$ olur. □

Lemma 7.2.7. m herhangi bir tam sayı olmak üzere, m ile bölünebilen bir F_n bulunabilir. [5]

İspat: m ve k herhangi bir tam sayı olmak üzere, Lemma 7.2.6 dan $m \mid F_{\delta(m)}$ ve $m \mid F_{k\delta(m)=n}$ dir. □

Lemma 7.2.8. $m \mid F_n$ olması için gerek ve yeter şart $\alpha(m) \mid n$ olmasıdır. [5]

İspat:

(i) $\alpha(m) \mid n$ olsun. Bu durumda $n = \alpha(m)t,\ t \in \mathbb{Z}$ olur. Tanım 7.1.1 den $F_{\alpha(m)} \equiv 0\ (mod\ m)$ dir. Bu durumda $F_{\alpha(m)} = mk, k \in \mathbb{Z}$ dır ve $\alpha(m) \mid n = \alpha(m)t$ ise Lemma 7.2.5 den $F_{\alpha(m)} \mid F_n$ olduğundan $F_n = F_{\alpha(m)}s,\ s \in \mathbb{Z}$ olur. Ayrıca $F_{\alpha(m)} = mk$ olduğundan $F_n = mks$ bulunur ve $m \mid F_n$ elde edilir.

(ii) $m \mid F_n$ ise $\alpha(m) \nmid n$ olsun. Yani $0 \leq r < \alpha(m)$ için $n = k\alpha(m) + r$ olmak üzere $k \geq 0$ tam sayısı için Teorem 7.1.2 de n yerine $\alpha(m)$ alınırsa

$$F_n = F_{k\alpha(m)+r} = \sum_{h=0}^{k} \binom{k}{h} F_{\alpha(m)}^{h} F_{\alpha(m)-1}^{k-h} F_{r+h}$$

$$F_n = \binom{k}{0} F_{\alpha(m)-1}^{k} F_r + \binom{k}{1} F_{\alpha(m)} F_{\alpha(m)-1}^{k-1} F_{r+1} + \cdots + \binom{k}{k} F_{\alpha(m)}^{k} F_{r+k}$$

bulunur ve $m \mid F_{\alpha(m)}$ olduğundan $F_n \equiv F_{\alpha(m)-1}^{k} F_r\ (mod\ m)$ olur. Ayrıca $m \mid F_n$ kabulünden

$$F_n \equiv F_{\alpha(m)-1}^{k} F_r \equiv 0\ (mod\ m) \qquad (7.2.2)$$

olur. Bu durumda $(F_{\alpha(m)}, F_{\alpha(m)-1}) = 1,\ m \mid F_{\alpha(m)}$ olduğundan $m \nmid F_{\alpha(m)-1}$ ve $m \nmid F_{\alpha(m)-1}^{k}$ elde edilir. Buradan $m \mid F_n$ ve $m \nmid F_{\alpha(m)-1}^{k}$ için Denklik 7.2.2 den $m \mid F_r$ olur. Yani $F_r \equiv 0\ (mod\ m)$ olur. Lemma 7.2.8 den $\alpha(m) \mid r$ dir ve $0 \leq r < \alpha(m)$ olduğundan $r = 0$ dır. Böylece $n = k\alpha(m) + r,\ r = 0$ için $n = k\alpha(m)$ ve $\alpha(m) \mid n$ elde edilir. (i) ve (ii) den $m \mid F_n$ olması için gerek ve yeter şart $\alpha(m) \mid n$ olur. □

Lemma 7.2.9. Herhangi bir m tam sayısı ve $r \geq s > 0$ olmak üzere $\alpha(m, s) \mid \alpha(m, r)$ dir. [5]

İspat: $r \geq s > 0$ için $m^s \mid m^r$ ve $m^r \mid F_{\alpha(m,r)}$ olduğundan $m^s \mid F_{\alpha(m,r)}$ bulunur. Sonuç olarak Lemma 7.2.8 den $\alpha(m, s) \mid \alpha(m, r)$ elde edilir. □

Lemma 7.2.10. $\alpha(m) \mid \delta(m)$ dir ve burada $\beta(m)$ bir tam sayıdır. [5]

İspat: Tanım 7.1.2 den $m \mid F_{\delta(m)}$ ve Lemma 7.2.8. den $\alpha(m) \mid \delta(m)$ olur. Tanım 7.1.3 den $\beta(m) = \frac{\delta(m)}{\alpha(m)}$ dir ve $\alpha(m) \mid \delta(m)$ olduğundan $\beta(m) = \frac{\delta(m)}{\alpha(m)} \in \mathbb{Z}$ elde edilir. □

Lemma 7.2.11. p tek asal sayı olmak üzere, F_p, F_{p-1} ve F_{p+1} sayılarından sadece birini böler. Ya da Lemma 4.1 den Legendre sembolü $(5/p) = +1, -1, 0$ olmak üzere $m = p - (5/p)$ için $p \mid F_m$ şeklinde de ifade edilebilir. [5]

İspat: Öncelikle Teorem 7.2.1, 7.2.2 ve 7.2.3 elde edilecektir ve sonrasında Lemma 7.2.11 in ispatı yapılacaktır.

Teorem 7.2.1.

$$F_p \equiv 2^{p-1}F_p = \sum_{s=0}^{\frac{1}{2}(p-1)} \binom{p}{2s+1} 5^s \equiv 5^{\frac{1}{2}(p-1)} \ (mod\ p)$$

dir. [5]

İspat: p tek asal sayı yani $(p, 2) = 1$ olmak üzere

(i) Teorem 7.1.1 de $n = p$ alınırsa $F_p = \left(\frac{1}{2}\right)^{p-1} \sum_{s=0}^{\left[\frac{1}{2}(p-1)\right]} \binom{p}{2s+1} 5^s$ elde edilir. Bu eşitliğin her iki tarafı da 2^{p-1} ile çarpılırsa

$$2^{p-1}F_p = \sum_{s=0}^{\left[\frac{1}{2}(p-1)\right]} \binom{p}{2s+1} 5^s$$

olur.

(ii) Lemma 4.2 de $m = 2$ alınırsa ve $(p, 2) = 1$ olduğundan $2^{p-1} \equiv 1\ (mod\ p)$ olur ve (i) de elde edilen eşitlikten

$$F_p \equiv 2^{p-1}F_p = \sum_{s=0}^{\left[\frac{1}{2}(p-1)\right]} \binom{p}{2s+1} 5^s \ (mod\ p)$$

bulunur. Ayrıca p tek asal sayısı için tam değerin içi daima tam sayı olduğundan $\left[\frac{1}{2}(p-1)\right] = \frac{1}{2}(p-1)$ dir. Böylece

$$F_p \equiv 2^{p-1}F_p = \sum_{s=0}^{\frac{1}{2}(p-1)} \binom{p}{2s+1} 5^s \ (mod\ p) \qquad (7.2.3)$$

olur ve $F_p \equiv 2^{p-1}F_p = p + \binom{p}{3}5^1 + \binom{p}{5}5^2 + \cdots + 5^{\frac{1}{2}(p-1)}\ (mod\ p)$ elde edilir. Teorem 7.1.5 den

$$F_p \equiv 2^{p-1}F_p \equiv 5^{\frac{1}{2}(p-1)}\ (mod\ p) \qquad (7.2.4)$$

bulunur. Son olarak Denklik 7.2.3 ve 7.2.4 birleştirilirse Teorem 7.2.1 bulunur. □

Ayrıca $m = 5$ iken $p \mid F_p$ olması için gerek ve yeter şart $(5/p) = 0$ dır. Bunun ispatı için Lemma 4.1 de $m = 5$ alınırsa $5^{\frac{1}{2}(p-1)} \equiv (5/p)\ (mod\ p)$ bulunur. Böylece Teorem 7.2.1 den $F_p \equiv 5^{\frac{1}{2}(p-1)} \equiv (5/p)\ (mod\ p)$ elde edilir. Buradan $p \mid F_p$ ise $(5/p) = 0$ ve $(5/p) = 0$ ise $p \mid F_p$ elde edilir. □

Sonuç olarak $m = p - (5/p)$, $m = 5$ ve $(5/p) = 0$ ise $p = 5$ olur. Yani $p = 5$ iken $p \mid F_p$ olması için gerek ve yeter şart $(5/p) = 0$ dır. □

Teorem 7.2.2.

$$2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\frac{1}{2}(p-1)} \left\{\binom{p}{2s+1} + \binom{p}{2s}\right\} 5^s \equiv 1 + 5^{\frac{1}{2}(p-1)}\ (mod\ p)$$

dir. [5]

İspat:

(i) Teorem 7.1.1 de $n = p + 1$ alınırsa $F_{p+1} = \left(\frac{1}{2}\right)^p \sum_{s=0}^{\left[\frac{p}{2}\right]} \binom{p+1}{2s+1} 5^s$ elde edilir. Bu eşitliğin her iki tarafı 2^p ile çarpılırsa

$$2^p F_{p+1} = \sum_{s=0}^{\left[\frac{p}{2}\right]} \binom{p+1}{2s+1} 5^s$$

bulunur.

(ii) Lemma 4.2 de $m = 2$ alınırsa ve $(p, 2) = 1$ olduğundan $2^{p-1} \equiv 1\ (mod\ p)$ den $2^p \equiv 2\ (mod\ p)$ olur ve (i) de elde edilen eşitlikten

$$2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\left[\frac{p}{2}\right]} \binom{p+1}{2s+1} 5^s\ (mod\ p)$$

bulunur. Ayrıca p tek asal sayısı için $\frac{p}{2}$ tam sayı olmadığından $\left[\frac{p}{2}\right] = \frac{1}{2}(p-1)$ dir. Böylece

$$2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\frac{1}{2}(p-1)} \binom{p+1}{2s+1} 5^s\ (mod\ p) \qquad (7.2.5)$$

olur ve $2F_{p+1} \equiv 2^p F_{p+1} = (p+1) + \binom{p+1}{3} 5^1 + \cdots + (p+1) 5^{\frac{1}{2}(p-1)}\ (mod\ p)$ elde edilir. Teorem 7.1.5 den

$$2F_{p+1} \equiv 2^p F_{p+1} \equiv 1 + 5^{\frac{1}{2}(p-1)}\ (mod\ p) \qquad (7.2.6)$$

bulunur. Son olarak Denklik 7.2.5 ve 7.2.6 birleştirilirse

$$2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\frac{1}{2}(p-1)} \binom{p+1}{2s+1} 5^s \equiv 1 + 5^{\frac{1}{2}(p-1)}\ (mod\ p)$$

ve Teorem 7.1.4 den

$$2F_{p+1} \equiv 2^p F_{p+1} = \sum_{s=0}^{\frac{1}{2}(p-1)} \left\{ \binom{p}{2s+1} + \binom{p}{2s} \right\} 5^s \equiv 1 + 5^{\frac{1}{2}(p-1)} \ (mod\ p)$$

olur ve Teorem 7.2.2 bulunur. □

Ayrıca $p \neq 5$ ise $p \mid F_{p+1}$ ifadesini ispatlayalım. $p \neq 5$ tek asal sayı olsun ve Lemma 4.1 de $m = 5$ için $(5, p) = 1$ olduğundan $(5/p) = \pm 1$ ve $5^{\frac{1}{2}(p-1)} \equiv \pm 1 \ (mod\ p)$ olur. Ayrıca Teorem 7.2.2 den $2F_{p+1} \equiv 1 + 5^{\frac{1}{2}(p-1)} \ (mod\ p)$ dir. Böylece $2F_{p+1} \equiv 0 \ (mod\ p)$ veya $2F_{p+1} \equiv 2 \ (mod\ p)$ elde edilir. Buradan p tek asal sayısı için $p \mid F_{p+1}$ olabilir. □

Teorem 7.2.3. $2F_{p-1} \equiv 1 - 5^{\frac{1}{2}(p-1)} \ (mod\ p)$ dir. [5]

İspat: $2F_{p-1} = 2F_{p+1} - 2F_p$ olmak üzere Teorem 7.2.1 ve Teorem 7.2.2 den

$$2F_{p-1} \equiv \left(1 + 5^{\frac{1}{2}(p-1)}\right) - 2 \cdot 5^{\frac{1}{2}(p-1)} \equiv 1 - 5^{\frac{1}{2}(p-1)} \ (mod\ p)$$

olur ve Teorem 7.2.3 bulunur. □

Ayrıca $p \neq 5$ ise $p \mid F_{p-1}$ ifadesini ispatlayalım. $p \neq 5$ tek asal sayı olsun ve Lemma 4.1 de $m = 5$ için $(5, p) = 1$ olduğundan $(5/p) = \pm 1$ ve $5^{\frac{1}{2}(p-1)} \equiv \pm 1 \ (mod\ p)$ olur. Ayrıca Teorem 7.2.3 den $2F_{p-1} \equiv 1 - 5^{\frac{1}{2}(p-1)} \ (mod\ p)$ dir. Böylece $2F_{p-1} \equiv 0 \ (mod\ p)$ veya $2F_{p-1} \equiv 2 \ (mod\ p)$ elde edilir. Böylece p tek asal sayısı için $p \mid F_{p-1}$ olabilir. □

Sonuç 7.2.1. p asal, $p = 5k \pm 1$ ise $(5/p) = 1$ ve $p = 5k \pm 2$ ise $(5/p) = -1$ dir. Yani $p \neq 5$ tek asal sayısı ya F_{p-1} sayısını böler ya da F_{p+1} sayısını böler. [3]

Sonuç 7.2.2. $p \neq 5$ ise $F_{p-1}F_{p+1} = F_p^2 - 1 \equiv 0\ (mod\ p)$ dir. [5]

İspat:

(i) Cassini özdeşliğinde $n = p - 1$ alınırsa $F_p^2 - F_{p-1}F_{p+1} = (-1)^{p+1}$ olur ve p tek asal sayı olduğundan $F_{p-1}F_{p+1} = F_p^2 - 1$ elde edilir.

(ii) Teorem 7.2.1 deki denkliğin her iki tarafının karesi alınırsa $F_p^2 \equiv 5^{p-1}\ (mod\ p)$ olur. $p \neq 5$ tek asal sayı ve $m = 5$ alınırsa Lemma 4.2 den $(5, p) = 1$ olduğundan $5^{p-1} \equiv 1\ (mod\ p)$ bulunur. Böylece $F_p^2 \equiv 5^{p-1} \equiv 1\ (mod\ p)$ elde edilir. Bu durumda (i) ve (ii) den ispat tamamlanır. □

Lemma 7.2.12. p tek asal sayı ise $\alpha(p) \mid (p - (5/p))$ olur. Ayrıca $p \neq 5$ iken $\alpha(p)$ asal sayı ise $\alpha(p) < p$ dir. [5]

İspat:

(i) p tek asal sayı olsun. Bu durumda Lemma 7.2.11 den $m = p - (5/p)$ olmak üzere $p \mid F_{m=p-(5/p)}$ olur ve Lemma 7.2.8 den $\alpha(p) \mid (p - (5/p))$ bulunur. □

(ii) $\alpha(p)$ asal sayı ve $p \neq 5$ tek asal olsun. Lemma 4.1 de $m = 5, p \neq 5$ tek asal sayısı için $(5, p) = 1$ olduğundan $(5/p) = \pm 1$ olur. Lemma 7.2.11 den $p \mid F_{p\pm1}$ dir. Lemma 7.2.8 den $\alpha(p) \mid (p \pm 1)$ elde edilir. Böylece $\alpha(p)$ asal ve $(p \pm 1)$ çift olup asal olmadığından $\alpha(p) < (p \pm 1)$ olur. Bu durumda $\alpha(p) < (p + 1)$ ve $\alpha(p) \neq p$ veya $\alpha(p) < (p - 1)$ olduğundan $\alpha(p) < p$ yazılabilir. □

Lemma 7.2.13. p_i ler farklı asallar ve $\lambda_i \in \mathbb{Z}^+$ olmak üzere $m = {p_1}^{\lambda_1}{p_2}^{\lambda_2} \dots {p_k}^{\lambda_k}$ için

$$\alpha(m, n) = [\alpha(p_1, n\lambda_1), \alpha(p_2, n\lambda_2), \dots, \alpha(p_k, n\lambda_k)]$$

dir. [5]

İspat: $m^n = {p_1}^{n\lambda_1}{p_2}^{n\lambda_2} \dots {p_k}^{n\lambda_k}$ ve $m^n \mid F_t$ olsun. Böylece her $i = 1, 2, \dots, k$ için ${p_i}^{n\lambda_i} \mid F_t$ olur. Lemma 7.2.8 den $\alpha(p_i, n\lambda_i) \mid t$ olur. Bu koşulu sağlayan en küçük

$t = [\alpha(p_i, n\lambda_i)\,]$ dir. Bu durumda Tanım 7.1.1 den m^n ile bölünebilen en küçük Fibonacci sayısı F_t olur ve $\alpha(m,n) = t = [\alpha(p_i, n\lambda_i)\,]$ elde edilir. □

Lemma 7.2.14. p_i ler farklı asallar ve $\lambda_i \in \mathbb{Z}^+$ olmak üzere $m = {p_1}^{\lambda_1}{p_2}^{\lambda_2} \dots {p_k}^{\lambda_k}$ için

$$\delta(m,n) = [\delta(p_1, n\lambda_1), \delta(p_2, n\lambda_2), \dots, \delta(p_k, n\lambda_k)]$$

dir. [5]

İspat: Lemma 7.2.6 dan $F_{s+t} \equiv F_s \ (mod\ {p_i}^{n\lambda_i})$ olması için gerek ve yeter şart t nin, her $i = 1, 2, \dots, k$ için $\delta(p_i, n\lambda_i)$ nin katı olmasıdır. Ayrıca Çin Kalan Teoremine göre $F_{s+t} \equiv F_s \ (mod\ m^n)$ olması için gerek ve yeter şart t nin, $\delta(m,n)$ nin katı olmasıdır. Böylece m^n modülüne göre $\delta(m,n)$ en küçük olduğundan her $i = 1, 2, \dots, k$ için $\delta(p_i, n\lambda_i)$ lerin en küçük ortak katı $\delta(m,n)$ olur. □

Tanım 7.2.2. N herhangi bir pozitif tam sayı ve $m^n \mid N$ için n en büyük tam sayı olmak üzere $n = pot_m N$ şeklindedir ve m tabanında n nin gücü olarak adlandırılır. [5]

Sonuç 7.2.3. Tanım 7.1.4 ve Tanım 7.2.2 den $\vartheta(m,n) = pot_m F_{\alpha(m,n)}$ dir. [5]

Lemma 7.2.15. $pot_m F_N = n$ olması için gerek ve yeter şart $\alpha(m,n) \mid N$ ve $\alpha(m, n+1) \nmid N$ olmasıdır. [5]

İspat:

(i) Tanım 7.2.2 den n en büyük tam sayı olmak üzere $pot_m F_N = n$ olsun. Böylece $m^n \mid F_N$ olduğundan Lemma 7.2.8 den $\alpha(m,n) \mid N$ olur. Ayrıca $\alpha(m, n+1) \mid N$ olsun. Böylece Lemma 7.2.8 den $m^{n+1} \mid F_N$ bulunur. Bu durumda $pot_m F_N > n$ olur ve bu durum kabul edilen $pot_m F_N = n$ ile çelişir. Bu çelişkinin olmaması için $\alpha(m, n+1) \nmid N$ olması gerekir.

(ii) $\alpha(m,n) \mid N$ ve $\alpha(m,n+1) \nmid N$ olsun. Bu durumda Lemma 7.2.8 den $m^n \mid F_N$ ve $m^{n+1} \nmid F_N$ olur. Tanım 7.2.2 den $pot_m F_N = n$ elde edilir. (i) ve (ii) den ispat tamamlanır. □

Lemma 7.2.16. k ve n pozitif tam sayı olmak üzere $(F_{kn}/F_n, F_n)$ ifadesi k nın çarpanıdır. [5]

İspat: Teorem 7.1.3 deki eşitliğin her iki tarafı F_n ile bölünürse

$$F_{kn}/F_n = \sum_{h=1}^{k} \binom{k}{h} F_n^{h-1} F_{n-1}^{k-h} F_h$$

$$F_{kn}/F_n = \binom{k}{1} F_{n-1}^{k-1} F_1 + \binom{k}{2} F_n F_{n-1}^{k-2} F_2 + \cdots + \binom{k}{k} F_n^{k-1} F_k \ (mod\ F_n)$$

$$F_{kn}/F_n \equiv k F_{n-1}^{k-1} \ (mod\ F_n) \qquad (7.2.7)$$

elde edilir. $(F_{kn}/F_n, F_n) = g$ olarak adlandırılırsa $g \mid (F_{kn}/F_n)$ ve $g \mid F_n$ olur. Böylece $g \mid (F_{kn}/F_n)$ olduğundan Denklik 7.2.7 den $g \mid k F_{n-1}^{k-1}$ bulunur. Ayrıca $g \mid F_n$, $(F_{n-1}, F_n) = 1$ olduğundan $g \nmid F_{n-1}$ olur ve $g \nmid F_{n-1}^{k-1}$ dir. Böylece $g \mid k F_{n-1}^{k-1}$ ifadesinde $g \nmid F_{n-1}^{k-1}$ olduğundan $g \mid k$ elde edilir. Yani $(F_{kn}/F_n, F_n) \mid k$ bulunur. □

Lemma 7.2.17. $k, n > 1$ ve tam sayı ise F_{kn}/F_n, n ve k nın kesinlikle artan fonksiyonudur. [5]

İspat: Teorem 7.1.3 deki eşitliğin her iki tarafı F_n ile bölünürse $F_{kn}/F_n = \sum_{h=1}^{k} \binom{k}{h} F_n^{h-1} F_{n-1}^{k-h} F_h$ elde edilir. Bu eşitlikteki her terim pozitiftir ve Lemma 7.2.2 den F_n ve F_{n-1}, n nin kesinlikle artan fonksiyonları olduğundan F_{kn}/F_n fonksiyonu da n ve k nın kesinlikle artan fonksiyonudur. □

7.3. Fibonacci Sayılarının Bölünebilirlik Düzeni

Teorem 7.3.1. p tek asal ve $n \geq v(p)$ olmak üzere

$$\alpha(p,n) = p^{n-v(p)}\alpha(p), \tag{7.3.1}$$

$$v(p,n) = n. \tag{7.3.2}$$

Eğer $p \neq 5$ ise $\big(p, \alpha(p)\big) = 1$ olur,
$p = 5$ için

$$\alpha(5,n) = 5^n. \tag{7.3.3}$$

Ayrıca $p = 2$ için

$$\alpha(2) = 3, \alpha(4) = 6 = \alpha(8) \tag{7.3.4}$$

olur ve $p = 2$ ve $n \geq 3$ için

$$\alpha(2,n) = 2^{n-2}\alpha(2) = 2^{n-2} \cdot 3 \tag{7.3.5}$$

dür. [5]

İspat: p asal sayı ve Lemma 7.2.9 da $m = p$ alınırsa $n > n-1$ olduğundan $\alpha(p,n-1) \mid \alpha(p,n)$ olur. $k \in \mathbb{Z}$ için

$$\alpha(p,n) = k\alpha(p,n-1) \tag{7.3.6}$$

olur. $p^n \mid F_{\alpha(p,n)}$ olduğundan $F_{\alpha(p,n)} = p^n X,\ X \in \mathbb{Z}^+$ bulunur ve $p^{(n-1)} \mid F_{\alpha(p,n-1)}$ olduğundan $F_{\alpha(p,n-1)} = p^{(n-1)}Y, Y \in \mathbb{Z}^+$ bulunur. Buradan

$$F^h_{\alpha(p,n-1)} = p^{h(n-1)}Y^h \tag{7.3.7}$$

yazılır. $F_{\alpha(p,n-1)-1} = T \in \mathbb{Z}^+$ olsun. Bu durumda

$$F^{k-h}_{\alpha(p,n-1)-1} = T^{k-h} \tag{7.3.8}$$

olur ve $F_{\alpha(p,n)} = p^n X$ eşitliğinin her iki tarafı p^{n-1} ile bölünürse

$$p^{-(n-1)}F_{\alpha(p,n)} = pX \tag{7.3.9}$$

elde edilir. Teorem 7.1.3 de $n = \alpha(p, n-1)$ alınırsa $F_{k\alpha(p,n-1)} = \sum_{h=1}^{k}\binom{k}{h} F_{\alpha(p,n-1)}^{h} F_{\alpha(p,n-1)-1}^{k-h} F_h$ elde edilir ve Eşitlik 7.3.6, 7.3.7 ve 7.3.8 den

$$F_{\alpha(p,n)} = \sum_{h=1}^{k}\binom{k}{h} p^{h(n-1)} Y^h T^{k-h} F_h$$

bulunur. Bu eşitliğin her iki tarafı $p^{-(n-1)}$ ile çarpılırsa

$$p^{-(n-1)}F_{\alpha(p,n)} = \sum_{h=1}^{k}\binom{k}{h} p^{(h-1)(n-1)} Y^h T^{k-h} F_h$$

olur ve Eşitlik 7.3.9 dan

$$pX = \sum_{h=1}^{k}\binom{k}{h} p^{(n-1)(h-1)} Y^h T^{k-h} F_h \tag{7.3.10}$$

elde edilir. Buradan

$$pX = \sum_{h=1}^{k}\binom{k}{h} p^{(n-1)(h-1)} Y^h T^{k-h} F_h \ (mod\ p)$$

yazılır ve $n > v(p) \geq 1$ ve $(p, T) = 1$ olduğundan $p \mid kY$ olur. Ayrıca $F_{\alpha(p,n-1)} = p^{(n-1)}Y$ ve $v(p, n-1) = n-1$ ise $(p, Y) = 1$ olur. Böylece $(p, Y) = 1$ ve $p \mid kY$ olduğundan $p \mid k$ elde edilir. $\alpha(p, n)$ ve k minimal olduğundan $k = p$ bulunur ve Eşitlik 7.3.10 nun her iki tarafı p ile bölünürse

$$X = \sum_{h=1}^{k}\binom{k}{h} p^{-1} p^{(n-1)(h-1)} Y^h T^{k-h} F_h$$

elde edilir. Bu eşitlik

$$X = \binom{k}{1} Y T^{k-1} p^{-1} + \binom{k}{2} p^{(n-1)} Y^2 T^{k-2} p^{-1} + \cdots + \binom{k}{k} p^{(n-1)(k-1)} p^{-1} Y^k F_k$$

şeklinde düzenlenir ve $k = p > 2$ alınırsa

$$X = \binom{p}{1} YT^{p-1}p^{-1} + \binom{p}{2} p^{(n-1)}Y^2T^{p-2}p^{-1} + \cdots + \binom{p}{p} p^{(n-1)(p-1)}p^{-1}Y^pF_p \ (mod\ p)$$

olur. $p > 2, n > 1$ ve Teorem 7.1.5 den $X \equiv YT^{p-1}\ (mod\ p)$ elde edilir. Bu denklikte $(p,T) = 1$ ve $(p,Y) = 1$ olduğundan $(p,X) = 1$ bulunur. $F_{\alpha(p,n)} = p^nX$ ve $(p,X) = 1$ olduğundan Eşitlik 7.3.2 elde edilir. $n \geq v(p)$ olmak üzere tümevarım ile $\alpha(p,n) = p^{n-v(p)}\alpha(p,v(p))$ bulunur. Böylece Teorem 7.1.7 den $\vartheta\big(p,\vartheta(p)\big) = \vartheta(p)$ ve Teorem 7.1.6 dan $\alpha(p,v(p)) = \alpha(p)$ olduğundan Eşitlik 7.3.1 ispatlanır. Lemma 7.2.12 den p tek asal sayı ise $\alpha(p) \mid (p - (5/p))$ olur. Böylece $p \neq 5$ ise $(p,\alpha(p)\,) = 1$ olur. Eşitlik 7.3.1 de $p = 5$ alınırsa $\alpha(5,n) = 5^{n-v(5)}\alpha(5)$ olur ve $v(5) = 1$ ve $\alpha(5) = 5$ olduğundan Eşitlik 7.3.3 elde edilir. Son olarak $p = 2$ alınırsa $k = p = 2$ ve $v(2,n-1) = n-1$ olur. Böylece Eşitlik 7.3.10 da $k = p = 2$ alınırsa $2X = \sum_{h=1}^{2}\binom{2}{h}2^{(n-1)(h-1)}Y^hT^{2-h}F_h$ dan $2X = 2YT + 2^{n-1}Y^2$ elde edilir. $(2,X) = 1$ ve $n \geq 3$ ise $v(2,n) = n$ ve Eşitlik 7.3.4 den $\alpha(2) = 3$ olur. Böylece Eşitlik 7.3.1 in ispatına benzer şekilde tümevarım ile Eşitlik 7.3.5 bulunur. □

Teorem 7.3.2. $pot_pF_m = n \geq 1$ olsun.

(i) Eğer p asal sayı ve $p^n \neq 2$ ise $r \geq 0$ ve $(p,t) = 1$ için $pot_pF_{p^rtm} = n + r$ dir.

(ii) $p^n = 2$, tm sayısı 3 sayısının tek katı ve F_{tm} sayısı da 2 sayısının tek katı olursa $r \geq 1$ için $pot_2F_{2^rtm} = r + 2$ dir. [5]

İspat:

(i) $n \geq 1$ ve $p^n \neq 2$ ise ya p tek asal sayı ve $n \geq v(p)$ ya da $p = 2$ ve $n \geq 3$ dür. Eşitlik 7.3.1 den $\alpha(p,n) = p^{n-v(p)}\alpha(p,v(p))$ bulunur. Burada $n = n + r$ ve $v(p) = n$ alınırsa

$$\alpha(p,n+r) = p^r\alpha(p,n) \qquad (7.3.11)$$

elde edilir. Burada $\alpha(p,n+r) = m$ ve $p^r = k$ alınırsa $m = k\alpha(p,n)$ elde edilir. Böylece Eşitlik 7.3.11 de $\alpha(p,n) = m/k$ yerine yazılırsa $k\alpha(p,n+r) = p^rm$ elde edilir ve $\alpha(p,n+r) \mid p^rm$ olur. Böylece $\alpha(p,n+r) \mid tmp^r$ yazılır. Lemma 7.2.8 den

$p^{n+r} \mid F_{p^r tm}$ bulunur ve $p^{n+r+1} \nmid F_{p^r tm}$ olur. Böylece Lemma 7.2.15 den $pot_p F_{p^r tm} = n + r$ bulunur. □

(ii) $p^n = 2$, tm ve m sayıları 3 ile bölünüp 6 ile bölünmez ise $pot_2 F_{tm} = 1$ olur. Bunun ispatı için Eşitlik 7.3.4 den $\alpha(2) = 3$ dür. $\alpha(2) = 3 \mid tm$ ise Lemma 7.2.8 den $2^1 \mid F_{tm}$ olur. Eşitlik 7.3.4 den $\alpha(4) = 6$ dır. $\alpha(4) = 6 \nmid tm$ ise $\alpha(2,2) \nmid tm$ olur. Lemma 7.2.8 den $2^2 \nmid F_{tm}$ olur. Böylece $2^1 \mid F_{tm}$ ve $2^2 \nmid F_{tm}$ olduğundan Lemma 7.2.15 den $pot_2 F_{tm} = 1$ elde edilir. Benzer şekilde $p^n = 2$, tm ve m sayıları 3 ile bölünüp 6 ile bölünmez ise $pot_2 F_{2^r tm} = r + 2$ olur. Bunun ispatı için Eşitlik 7.3.5 de $n = r + 2$ alınırsa $\alpha(2, r+2) = 2^r \cdot 3$ elde edilir. $3 \mid tm$ ise $(2^r \cdot 3) \mid (2^r tm)$ olduğundan $\alpha(2, r+2) \mid (2^r tm)$ olur. Lemma 7.2.8 den $2^{r+2} \mid F_{2^r tm}$ bulunur. Eşitlik 7.3.5 de $n = r + 3$ alınırsa $\alpha(2, r+3) = 2^{r+1} \cdot 3$ elde edilir. $6 \nmid tm$ ise $(2^r \cdot 6) \nmid (2^r tm)$ olduğundan $(2^{r+1} \cdot 3) \nmid (2^r tm)$ olur ve $\alpha(2, r+3) \nmid (2^r tm)$ bulunur. Böylece Lemma 7.2.8 den $2^{r+3} \nmid F_{2^r tm}$ elde edilir. Bu durumda $2^{r+2} \mid F_{2^r tm}$ ve $2^{r+3} \nmid F_{2^r tm}$ olduğundan Lemma 7.2.15 den $pot_2 F_{2^r tm} = r + 2$ bulunur. □

Teorem 7.3.3. p asal sayı ve $p^n \neq 2$, $r \geq 0$ ve $pot_p F_m = n \geq 1$ ise bütün p asalları için aralarında asal $l_s = l_s(m,p)$ $(s = 0, 1, 2, \dots)$ tam sayılarının tam olarak artan dizilimi

$$F_{p^r m} = p^{n+r} l_0 l_1 \dots l_r \tag{7.3.12}$$

dir. [5]

İspat: $r = 0$ olduğunda Tanım 7.2.2 den $pot_p F_m = n$ ise $(p, l_0) = 1$ olacak şekilde $F_m = p^n l_0$ dır. X, Y ve T pozitif tam sayı olmak üzere $r \geq 1$ ise Teorem 7.3.2 den
(i) $pot_p F_{p^r tm} = n + r$ eşitliğinde $t = 1$ alınırsa $p^{n+r} \mid F_{p^r m}$ olur. Buradan $(p, X) = 1$ için

$$F_{p^r m} = p^{n+r} X \tag{7.3.13}$$

elde edilir.

(ii) $pot_pF_{p^rtm} = n + r$ eşitliğinde $r = r - 1$ ve $t = 1$ alınırsa $p^{n+r-1} \mid F_{p^{r-1}m}$ olur. Buradan $(p, Y) = 1$ için

$$F_{p^{r-1}m} = p^{n+r-1}Y \tag{7.3.14}$$

elde edilir. Ayrıca

$$F_{p^{r-1}m-1} = T \tag{7.3.15}$$

dir. Lemma 7.2.1 den $(F_{p^{r-1}m}, F_{p^{r-1}m-1}) = 1$, $F_{p^{r-1}m} = p^{n+r-1}Y$ ve $F_{p^{r-1}m-1} = T$ olduğundan $(p^{n+r-1}Y, T) = 1$ bulunur. Bu durumda $(p, T) = 1$ ve $(Y, T) = 1$ olduğundan $(pY, T) = 1$ olur. Teorem 7.1.3 de $k = p$ ve $n = p^{r-1}m$ alınırsa $F_{p^rm} = F_{p^{r-1}m} \sum_{h=1}^{p} \binom{p}{h} F_{p^{r-1}m}^{h-1} F_{p^{r-1}m-1}^{p-h} F_h$ olur ve Eşitlik 7.3.13, 7.3.14 ve 7.3.15 den

$$p^{n+r}X = p^{n+r-1}Y \sum_{h=1}^{p} \binom{p}{h} p^{(n+r-1)(h-1)} Y^{h-1} T^{p-h} F_h$$

elde edilir. Bu eşitliğin her iki tarafı p^{n+r} ile bölünürse

$$X = Y \sum_{h=1}^{p} \binom{p}{h} p^{(n+r-1)(h-1)-1} Y^{h-1} T^{p-h} F_h \tag{7.3.16}$$

elde edilir. Teorem 7.3.1 in ispatında olduğu gibi $n \geq 1$ olursa sağdaki toplam bir tam sayı olur. Böylece $Y \mid X$ olur. Buradan da $X = Yl_r$ yazılır. Bu durumda indirgeme yöntemi ile benzer şekilde $Y = Dl_{r-1}$ den $Y = l_0 l_1 \dots l_{r-1}$ ifade edilip devam edilirse $X = l_0 l_1 \dots l_r$ elde edilir. Eşitlik 7.3.13 de $X = l_0 l_1 \dots l_r$ yazılırsa Eşitlik 7.3.12 bulunur. □

Son olarak $X = Yl_r$ ve Eşitlik 7.3.16 dan $X = \sum_{h=1}^{p} \binom{p}{h} p^{(n+r-1)(h-1)-1} Y^h T^{p-h} F_h$,

$$Yl_r = YT^{p-1} + pY^2 \sum_{h=2}^{p} \binom{p}{h} p^{(n+r-1)(h-1)-2} Y^{h-2} T^{p-h} F_h$$

bulunur. Bu eşitliğin her iki tarafı Y ile bölünürse

$$l_r = pY\sum_{h=2}^{p}\binom{p}{h}p^{(n+r-1)(h-1)-2}Y^{h-2}T^{p-h}F_h + T^{p-1} \qquad (7.3.17)$$

elde edilir. Bu eşitlikte ya $p \geq 3$ ve $n \geq 1$ ya da $p = 2$ ve $n \geq 3$ olduğunda eşitliğin sağ tarafındaki toplam bir tam sayı olur. Yani $l_r = T^{p-1} + pYk_r$ şeklinde yazılabilir. Buradan $l_r \equiv T^{p-1} + pYk_r\ (mod\ pY)$ ve $(T,p) = 1$ olduğundan $l_r \equiv T^{p-1}\ (mod\ pY)$ olur. $T \in \mathbb{Z}^+$ olduğundan l_r, pY nin pozitif tam sayı katını aşar. Yani $l_r > pY$ olur. $l_r > pY$ ve $Y = l_0 l_1 \dots l_{r-1}$ olduğundan $l_r > pl_0 l_1 \dots l_{r-1}$ olur. Burada $l_r \in \mathbb{Z}^+$ $(r = 0, 1, 2, \dots)$ olduğundan $pl_0 l_1 \dots l_{r-1} > l_{r-1}$ bulunur. Böylece $l_r > pl_0 l_1 \dots l_{r-1}$ ve $pl_0 l_1 \dots l_{r-1} > l_{r-1}$ olduğundan

$$l_r > pl_0 l_1 \dots l_{r-1} > l_{r-1} \qquad (7.3.18)$$

elde edilir. [5]

Tanım 7.3.1. $pot_p F_N = n$ ise $n \geq 1$ ve $p = 5$ ya da $n > v(p)$ ise p, F_N nin katlı asal çarpanı (mpf) olarak adlandırılır. Aksine $p \neq 5$ veya $n = v(p)$ ise p, F_N nin basit asal çarpanı (spf) olarak adlandırılır. [5]

Lemma 7.3.1. p, F_N nin katlı asal çarpanı olması için gerek ve yeter şart p hem F_N nin hem de N nin asal çarpanı olmasıdır. F_N nin bir asal çarpanı katlı değilse basit asal çarpandır. [5]

İspat: Tanım 7.3.1 den F_N nin bir asal çarpanı katlı değilse basit asal çarpanıdır. Tanım 7.3.1 den p, F_N nin katlı asal çarpanı olsun. Bu durumda $p \mid F_N$ olur ve Lemma 7.2.8 den $\alpha(p) \mid N$ bulunur. Böylece Teorem 7.3.1 den $p \mid N$ bulunur. □

Lemma 7.3.2. k ve n pozitif tam sayı ve p, F_n nin katlı asal çarpanı ise p, F_{kn} nin de katlı asal çarpanı olur. Diğer taraftan p, F_{kn} nin basit asal çarpanı ise p, F_n nin de basit asal çarpanı olur. [5]

İspat:

(i) k, n pozitif tam sayı ve p, F_n nin katlı asal çarpanı olsun. p, F_n nin katlı asal çarpanı olduğundan Lemma 7.3.1 den $p \mid F_n$ ve $p \mid n$ olur. $n \mid kn$ olduğundan Lemma 7.2.5 den $F_n \mid F_{kn}$ bulunur. Böylece $p \mid F_n$ ve $F_n \mid F_{kn}$ olduğundan $p \mid F_{kn}$ elde edilir. Ayrıca $p \mid n$ olduğundan $p \mid kn$ olur. Sonuç olarak $p \mid F_{kn}$ ve $p \mid kn$ olduğundan Lemma 7.3.1 den p, F_{kn} nin de katlı asal çarpanı olur.

(ii) Olmayana ergi yöntemi ile p, F_{kn} nin basit asal çarpanı ise p, F_n nin basit asal çarpanı olmasın. Bu durumda p, F_n nin katlı asal çarpanı olur ve Lemma 7.3.2 nin ilk kısmından p, F_{kn} nin de katlı asal çarpanı olur. Ama bu başta kabul ettiğimiz p, F_{kn} nin basit asal çarpanı olması durumuyla çelişir. Böylece p, F_{kn} nin basit asal çarpanı ise p, F_n nin de basit asal çarpanıdır. □

Teorem 7.3.4. $N = 1, 2, 5, 6$ veya 12 olmadığı sürece F_N nin en az bir tane basit asal çarpanı vardır. [5]

İspat: $N = 1, 2$ ise $F_1 = F_2 = 1$ olduğundan F_N nin asal çarpanı yoktur. Bu durumda basit asal çarpanı da yoktur.

$N \geq 3$ için Lemma 7.2.13 den $F_N = m$ alınırsa $F_N = {p_1}^{\lambda_1} {p_2}^{\lambda_2} \dots {p_k}^{\lambda_k}$ olur. Lemma 7.2.2 den F_N nin asal çarpanlarının kümesi P boş değildir. Eğer F_N nin sadece katlı asal çarpanları varsa $\lambda_1, \lambda_2, \dots, \lambda_k \neq 1$ olmalıdır. Ayrıca $i = 1, 2, \dots, k$ için p_i, F_N nin katlı asal çarpanı ise Lemma 7.3.1 den hem $p_i \mid F_N$ hem de $p_i \mid N$ olur. $p_i \mid N$ olduğundan Lemma 7.2.5 den $F_{p_i} \mid F_N$ ve $F_N = m$ olduğundan $F_{p_i} \mid m$ olur. P, her F_{p_i} nin asal çarpanlarını içerir.

Lemma 7.2.8, Teorem 7.3.1 den ve F_N nin sadece katlı asal çarpanları varsa $F_N = 2^r 3^s 5^t$ ve $r \leq 4$, $s \leq 2$, $t \leq 1$, $rt = 0$, $st = 0$ olmak üzere

$$r = 0, s = 0 \text{ ve } t = 1 \text{ ise } F_N = 5 \text{ ve } N = 5$$

olur. Tanım 7.3.1 den $n \geq 1$ için $p = 5$ özel olarak çok katlı asal çarpan alınır.

$$s = t = 0 \text{ ve } r = 3 \text{ ise } F_N = 8 = 2^3 \text{ ve } N = 6$$

olur. Lemma 7.3.1 den $2 \mid F_6$ ve $2 \mid N = 6$ olduğundan $p = 2$ çok katlı asal çarpandır.

$$t = 0, rs > 0, s = 2 \text{ ve } r = 4 \text{ ise } F_N = 144 = 2^4 3^2 \text{ ve } N = 12$$

olur. Lemma 7.3.1 den $2 \mid F_{12}$ ve $2 \mid N = 12$ olduğundan $p = 2$ çok katlı asal çarpandır. Ayrıca $3 \mid F_{12}$ ve $3 \mid N = 12$ olduğundan $p = 3$ de çok katlı asal çarpandır. Böylece $N = 5, 6$ veya 12 olduğunda basit asal çarpan bulunamaz. □

8. SONUÇLAR VE TARTIŞMA

Bu tezde Fibonacci ve genelleştirilmiş Fibonacci dizilerinin periyodik yapıda oldukları incelenmiş ve bununla ilgili temel kavramlar açıklanmıştır. Ayrıca bu periyodik yapının ortaya çıkardığı ilişkiler ve sonuçlar ele alınmıştır ve son olarak bu ilişkilerden yararlanarak Fibonacci dizisinin genel bölünebilirlik özellikleri incelenmiştir.

Fibonacci, Lucas ve genelleştirilmiş Fibonacci sayıları geçmişten günümüze kadar ilgi odağı olmuştur. Bu sayı dizileri üzerinde farklı araştırmalarda her geçen gün yeni tanımlamalar yapılmakta, yeni özellikleri keşfedilmekte ve bu özellikler teoremlerle ifade edilmektedir. Bu nedenle keşfedilen özellikleri ile git gide genişleyen, geliştirilebilir olan bu konuda birçok açık problemler bulunmaktadır.

Bu tez çalışması bu alanda yapılan teoremler ve çalışmaların bir derlemesi niteliğindedir. Bu konudaki çalışmaların daha anlaşılır olarak açıklanması, açık olanların ya da geliştirilebilir özelliklerin görülmesi bakımından önem arz etmektedir.

KAYNAKLAR

[1] Koshy, T., Fibonacci and Lucas Numbers with Applications. 196 – 205. John Wiley & Sons Inc., New York, 2001.

[2] Wall, D. D., Fibonacci Series Modulo m. The American Mathematical Monthly. 67(6): 525 – 532, 1960.

[3] Robinson, D. W., The Fibonacci Matrix Modulo m. The Fibonacci Quarterly.1(2): 29 – 36, 1963.

[4] Vinson, J., The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence. The Fibonacci Quarterly. 1(2): 37 – 45, 1963.

[5] Halton, J. H., On the Divisibility Properties of Fibonacci Numbers. The Fibonacci Quarterly. 4(3): 217 – 240, 1966.

[**6]** Weinstein, L., A Divisibility Property of Fibonacci Numbers. The Fibonacci Quarterly. 4(1): 83 – 84, 1966.

[7] Freeman, G.F., On Ratios of Fibonacci and Lucas Numbers. The Fibonacci Quarterly. 5(1): 99 – 106, 1967.

[8] Cross, G., and Renzi, H., Teachers Discover New Math Theorems, The Arithmetic Teacher. 12(8): 625-626, 1965.