SONLU CİSİMLER ÜZERİNDE TATE NORMAL FORMLAR

Buse ÇAPA

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER ÜZERİNDE TATE NORMAL FORMLAR

BUSE ÇAPA

Prof. Dr. Osman BİZİM

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA, 2011

TEZ ONAYI

Buse Çapa tarafından hazırlanan "Sonlu Cisimler Üzerinde Tate Normal Formlar" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/~~oy çokluğu~~ ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Prof. Dr. Osman BİZİM

Başkan : Prof. Dr. Osman BİZİM
Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye : Doç. Dr. Orhan GÜRLER
Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Fizik Anabilim Dalı

Üye : Doç. Dr. Ahmet TEKCAN
Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Kadri ARSLAN
Enstitü Müdürü
13../06./...2011

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

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

beyan ederim.

30/05/2011

Buse ÇAPA

ÖZET

Yüksek Lisans Tezi

SONLU CİSİMLER ÜZERİNDE TATE NORMAL FORMLAR

Buse ÇAPA

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Osman BİZİM

Bu çalışmada özel bir eğri ailesi olan Tate normal formdaki eliptik eğriler sonlu cisimler üzerinde ele alınmış ve bu eğriler üzerindeki noktaların oluşturduğu grupların yapıları belirlenmiştir.

Çalışmanın birinci bölümünde, ikinci ve üçüncü bölümlere temel oluşturacak kavramlar verilmiştir. Cebirin ve sayılar teorisinin temel kavramları ve temel teoremleri bu bölümde ele alınmıştır.

Çalışmanın ikinci bölümünde, eliptik eğriler, singüler eğriler ve bu eğrilerin sonlu cisimler üzerindeki özellikleri incelenmiştir.

Üçüncü bölüm ise çalışmanın ana kısmını oluşturmaktadır. Bu bölümde, öncelikle, eliptik eğrilerin Tate normal form kavramı tanımlanmıştır. Daha sonra sırasıyla p asal sayı olmak üzere sonlu $\mathbb{F}_p$ cismi üzerinde tanımlı Tate normal formdaki eliptik eğriler üzerindeki noktalar elde edilerek, eğrilerin mertebeleri belirlenmiştir. Elde edilen sonuçlara göre eğriler mertebelerine göre sınıflandırılmıştır. Son olarak, eğri üzerindeki noktaların mertebeleri kullanılarak, eğri üzerindeki noktaların oluşturduğu grupların yapıları belirlenmiştir.

Anahtar Kelimeler: Eliptik eğriler, Sonlu cisimler üzerinde tanımlı eliptik eğriler, Tate normal form, Sonlu cisimler üzerinde Tate normal formlar.

2011, viii + 91 sayfa.

ABSTRACT

MSc Thesis

TATE NORMAL FORMS OVER FINITE FIELDS

Buse ÇAPA

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

Supervisor: Prof. Dr. Osman BİZİM

In this work, Tate normal forms of elliptic curves defined over finite fields are discussed and the structure of groups of points on these curves are given.

In the first chapter, the concepts form the basis for the second and third chapters are given. The basic concepts and theorems of algebra and number theory are discussed in this chapter.

In the second chapter, elliptic curves, singular curves and properties of these curves defined over finite fields are considered.

Third chapter is the main part of the work. First, the concept of Tate normal form of elliptic curves are defined. Then by obtaining the points on the Tate normal form of the elliptic curves defined over finite fields $\mathbb{F}_p$ (where p is a prime), the orders of these curves are determined. According to these results curves are classified with respect to the orders. The group structures of the points on these curves are given by using the order of the points on the curves.

Key words: Elliptic curves, Elliptic curves defined over finite fields, Tate normal form, Tate normal form over finite fields.

2011, viii + 91 pages.

TEŞEKKÜR

Yüksek lisans çalışmam esnasında her türlü bilgi ve deneyimini benden esirgemeyen ve her zaman bana destek olan değerli danışman hocam Prof. Dr. Osman BİZİM'e en içten teşekkürlerimi sunarım. Çalışmama katkılarından ve yardımlarından dolayı Öğr. Gör. Dr. Betül GEZER ve Arş. Gör. İlker İNAM'a teşekkür ederim.

Buse Çapa
30/05/2011

İÇİNDEKİLER

SİMGELER DİZİNİ

Simgeler	Açıklama
$\left(\frac{a}{p}\right)$	a nın modülo p de Legendre sembolü ($p > 2$)
$\left(\frac{a}{n}\right)$	a nın modülo n de Jacobi sembolü
$\left(\frac{\Delta}{n}\right)$	Δ nın modülo n de Kronecker sembolü
$\mathbb{F}$	Cisim
$\phi(m)$	Euler Phi fonksiyonu
$j(E)$	E eliptik eğrisinin j-değişmezi
$\Delta(E)$	E eliptik eğrisinin diskriminantı
$E[n]$	E eliptik eğrisi üzerindeki n. mertebeden büküm (torsiyon) noktası
$E_{ns}(\mathbb{F})$	E eliptik eğrisi üzerindeki singüler olmayan noktaların oluşturduğu küme
$\mathbb{F}^*$	$\mathbb{F}$ cisminin sıfırdan farklı elemanlarının oluşturduğu çarpımsal grup
$\overline{\mathbb{F}}$	$\mathbb{F}$ cisminin cebirsel kapanışı
$E(\mathbb{F})$	$\mathbb{F}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktaların kümesi
$E(\mathbb{F}_p)$	$\mathbb{F}_p$ sonlu cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktaların kümesi
$\#E(\mathbb{F}_p)$	$\mathbb{F}_p$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar kümesinin eleman sayısı
R	Halka
$\mathbb{Z}_n$	Modülo n de tamsayıların halkası
Q_p	Modülo p de ikinci derece kalanların kümesi
K_p	Modülo p de üçüncü derece kalanların kümesi
$\mathbb{F}_p$	p elemanlı sonlu cisim
$\mathbb{F}_p^*$	p elemanlı sonlu cismin çarpımsal grubu

$E(\mathbb{Q})$	$\mathbb{Q}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{Z}$	Tam sayılar kümesi
U_n	$\mathbb{Z}_n$ deki birimlerin kümesi

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bu bölümde çalışmada kullanılacak olan bazı temel kavramlar tanımlanacak ve bazı temel teoremler verilecektir, bu bölüm diğer bölümler için bir taban oluşturacaktır. Kısım 1.1 de grup teori ile ilgili bazı kavramlar ele alınacaktır. Kısım 1.2 de sonlu cisimlerin temel özellikleri üzerinde durulacaktır. Daha sonraki kısımlarda ise özellikle sayılar teorisi ile ilgili kavramlarla ilgilenilecektir. Kısım 1.3 de bir $\mathbb{Z}_n$ halkasındaki ikinci dereceden kalan kavramı verildikten sonra sonlu cisimler üzerinde ikinci dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir. Kısım 1.4 de ise sonlu cisimler üzerinde üçüncü dereceden kalan kavramı ve temel özellikleri verilecektir.

1.1 Temel Kavramlar

Bu kısımda çalışmada gerekli olacak grup teorisi ile ilgili bazı kavramların tanımları ve örnekleri verilecektir. Grup ve alt gruplarının mertebeleri arasındaki ilişkiyi belirten Lagrange teoremi grup teorinin en iyi bilinen ve en çok kullanılan teoremlerinden biridir.

1.1.1 Teorem (Lagrange). *G* bir grup ve *H*, *G* nin bir alt grubu olsun. Bu durumda *H* nin mertebesi *G* nin mertebesini böler (Fraleigh 1982).

Bu teoremin önemli sonuçları ise aşağıdaki teoremlerde verilmektedir.

1.1.2 Teorem. Mertebesi asal olan her grup bir devirli gruptur, yani bu grup bir tek eleman ile üretilebilir (Fraleigh 1982).

1.1.3 Teorem. Sonlu mertebeli bir grubun her hangi bir elemanın mertebesi grubun mertebesini böler (Fraleigh 1982).

1.1.4 Tanım. $\overline{u}$, *R* halkasının bir elemanı olmak üzere, $\overline{u}$ nin çarpmaya göre tersi,

$$\overline{u}\overline{v} = \overline{v}\overline{u} = \overline{1}$$

olacak şekilde bir $\overline{v} \in R$ elemanıdır. R halkasında çarpmaya göre tersi olan bir elemana *birim (unit)* denir ve R halkasındaki birimlerin kümesi $\boldsymbol{U}(R)$ veya kısaca $\boldsymbol{U}$ ile gösterilir. Örneğin $\mathbb{Z}$ tamsayılar halkasındaki birimler 1 ve –1 dir. Aşağıdaki teorem, $\mathbb{Z}_n$ halkasındaki birimleri belirlemektedir.

1.1.5 Teorem. $\overline{u} \in \mathbb{Z}_n$ nin bir birim olması için gerek ve yeter şart $(u, n) = 1$ olmasıdır (Fraleigh 1982).

Örneğin, $\mathbb{Z}_6$ daki birimler $\boldsymbol{U}_6 = \{ \overline{1}, \overline{5} \}$ ve $\mathbb{Z}_8$ deki birimler $\boldsymbol{U}_8 = \{ \overline{1}, \overline{3}, \overline{5}, \overline{7} \}$ dir.

1.1.6 Tanım. $\overline{g} \in \mathbb{Z}_n$, $\boldsymbol{U_n}$ yi üretiyorsa g ye modülo n de bir *ilkel kök* denir.

Eğer $\overline{g}$ bir ilkel kök ise $\overline{g}$ nin 0 ile $n - 1$ arasındaki tüm kuvvetleri birbirinden farklıdır ve bunlar $\boldsymbol{U_n}$ yi oluştururlar. Örneğin, modülo 5 de $\overline{2}$ ve $\overline{3}$ birer ilkel köktür, bu iki elemanın kuvvetleri $\boldsymbol{U}_5$ i oluşturur.

İlkel kök teoremi, her bir asal sayının ilkel bir kökünün var olduğunu ve üstelik modülo p de bunların sayısının tam olarak $\phi(p - 1)$ tane olduğunu belirtir, burada

$$\phi(m) = \#\{ a \mid 1 \le a \le m \text{ ve } (a, m) = 1 \}$$

Euler Phi fonksiyonudur. Örneğin, modülo 11 de $\phi(10) = 4$ olduğundan 4 tane ilkel kök vardır ve bunlar 2, 6, 7 ve 8 sayılarıdır.

Halkalar teorisinde, R halkasındaki her $a \in R$ için $n \cdot a = 0$ olacak biçimde bir $n \in \mathbb{N}$ sayısının varlığı oldukça önemlidir. Burada $n \cdot a$, n tane a nın toplamını belirtmektedir, yani

$$a + a + \ldots + a = n \cdot a$$

dır.

1.1.7 Tanım. R bir halka olmak üzere her $a \in R$ için $n \cdot a = 0$ olacak biçimde bir $n \in \mathbb{N}$ sayısı varsa bu şekildeki sayıların en küçüğüne R halkasının *karakteristiği* denir. Eğer böyle bir sayı yok ise R halkasının karakteristiği 0 olarak alınır.

Örneğin, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ ve $\mathbb{C}$ halkalarının karakteristiği 0, $\mathbb{Z}_n$ halkasının karakteristiği ise n dir. Aşağıdaki teorem bir birimli halkanın karakteristiğinin nasıl belirleneceğini göstermektedir.

1.1.8 Teorem. R birimli (birimi 1) halka olsun. R nin karakteristiğinin $n > 0$ olabilmesi için gerek ve yeter şart n sayısının $n \cdot 1 = 0$ olacak biçimdeki en küçük pozitif tamsayı olmasıdır (Fraleigh 1982).

1.1.9 Tanım. $\mathbb{F}$ ve $\mathbb{L}$, $\mathbb{F} \subset \mathbb{L}$ özelliğinde iki cisim ve $\alpha \in \mathbb{L}$ olsun. $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ ve

$$f(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + X^n$$

olmak üzere $f(\alpha) = 0$ olacak biçimde bir f polinomu varsa α ya $\mathbb{F}$ cisminde bir *cebirsel sayı* denir. Eğer $\mathbb{L}$ nin her elemanı $\mathbb{F}$ de bir cebirsel sayı ise $\mathbb{L}$ cismine $\mathbb{F}$ nin bir *cisim genişlemesi* denir. $\mathbb{L}$, $\mathbb{F}$ nin bir cisim genişlemesi olmak üzere

$$\overline{\mathbb{F}} = \{ \alpha \in \mathbb{L} \mid \alpha, \mathbb{F} \text{ de cebirsel sayı} \} \subset \mathbb{L}$$

kümesine $\mathbb{F}$ nin bir *kapanışı* denir.

Örneğin, $\sqrt{1+\sqrt{3}}$ sayısı $\mathbb{Q}$ da bir cebirsel sayıdır ve $\mathbb{C}$, $\mathbb{Q}$ nun bir cisim genişlemesidir. $\mathbb{Q}$ ile $\mathbb{C}$ nin kapanışları ise $\mathbb{C}$ dir.

1.2 Sonlu Cisimler

p bir asal sayı olmak üzere modülo p deki tamsayılar mertebesi p olan $\mathbb{F}_p$ cismini oluştururlar. Her bir p asal sayısı ve $n \in \mathbb{N}$ için mertebesi p^n olan bir sonlu cisim vardır. Bu cisim literatürde mertebesi p^n olan *Galois cismi* olarak bilinir ve $GF(p^n)$ ile gösterilir.

$\mathbb{E}$, $\mathbb{F}$ cisminin n. dereceden bir cisim genişlemesi ve $\mathbb{F}$ cisminin eleman sayısı p ise $\mathbb{E}$ cisminin p^n tane elemanı vardır. Bunun sonucu olarak, $\mathbb{E}$, karakteristiği p olan bir sonlu cisim ise belli bir $n \in \mathbb{N}$ için $\mathbb{E}$ nin p^n tane elemanı vardır.

1.2.1 Tanım. $\mathbb{F}$ sonlu bir cisim ve $\alpha \in \mathbb{F}$ olmak üzere $\alpha^n = 1$ ise α ya $\mathbb{F}$ cisminin *n. kökü* denir, eğer n bu özellikteki en küçük pozitif tamsayı ise α ya *birimin n. ilkel kökü* denir.

Örneğin $x^3 = 1$ için

$$x^3 - 1 = (x - 1)\cdot(x^2 + x + 1) = 0$$

olduğundan birimin üçüncü ilkel kökleri,

$$x_1 = 1, x_2 = \frac{-1-\sqrt{3}i}{2} \text{ ve } x_3 = \frac{-1+\sqrt{3}i}{2}$$

dir.

Birimin ilkel kökü tanımı dikkate alınırsa, p^n elemanlı sonlu bir $\mathbb{F}$ cisminin sıfırdan farklı olan tüm elemanları birimin $p^n - 1$. kökleridir.

1.3 İkinci Dereceden Kalanlar

Bu kısımda ilk olarak bir $\mathbb{Z}_n$ halkasındaki ikinci dereceden kalanlar ele alınacak, daha sonra p bir asal sayı olmak üzere $\mathbb{F}_p$ sonlu cismi üzerinde ikinci dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir.

1.3.1 Tanım. $a \in \mathbb{Z}$, $n \in \mathbb{N}$ ve $(a, n) = 1$ olmak üzere

$$x^2 \equiv a \pmod{n} \tag{1.1}$$

olacak biçimde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$ ye modülo n de bir *ikinci dereceden kalan* denir. Modülo n de ikinci dereceden kalanların kümesi $\boldsymbol{Q}_n$ ile gösterilir.

Eğer (1.1) denkliğinin bir çözümü yoksa bu durumda $a \in \mathbb{Z}$ ye modülo n de bir *ikinci dereceden kalan değildir* denir.

Örneğin modülo 11 deki ve modülo 8 deki ikinci dereceden kalanların kümesi, sırasıyla,

$$\boldsymbol{Q}_{11} = \{ \overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9} \} \text{ ve } \boldsymbol{Q}_8 = \{ \overline{1} \}$$

dir.

Çalışmada $n = p$ asal sayı olması hali ile ilgileneceğinden aşağıda bu durumla ilgili bazı teoremler verilmiştir.

1.3.2 Teorem. $p > 2$ asal sayı olmak üzere modülo p de $\frac{p-1}{2}$ tane ikinci dereceden kalan ve $\frac{p-1}{2}$ tane ikinci dereceden kalan olmayan eleman vardır (Silverman 2006).

1.3.3 Teorem (Çarpım Teoremi). p bir tek asal sayı olmak üzere

i. Modülo p de iki tane ikinci dereceden kalan sayının çarpımı bir ikinci dereceden kalan sayıdır.

ii. Modülo p de bir ikinci dereceden kalan ve bir ikinci dereceden kalan olmayan sayının çarpımı bir ikinci dereceden kalan değildir.

iii. Modülo p de iki tane ikinci dereceden kalan olmayan sayının çarpımı bir ikinci dereceden kalan sayıdır (Silverman 2006).

Verilen bir $a \in \mathbb{Z}$ sayısının ikinci dereceden kalan olup olmadığını belirlemek için adına

Legendre sembolü adı verilen bir sembol kullanılır ve bu sembol aşağıdaki gibi tanımlanır:

1.3.4 Tanım (Legendre Sembolü). $a \in \mathbb{Z}$ ve bir $p > 2$ asal sayısı için a tamsayısının

Legendre sembolü

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & x^2 \equiv a \pmod{p} \text{ nin bir çözümü var} \\ 0 & p \mid a \\ -1 & x^2 \equiv a \pmod{p} \text{ nin çözümü yoktur} \end{cases}$$

$$= \begin{cases} +1 & a \text{ bir ikinci dereceden kalan} \\ 0 & p \mid a \\ -1 & a \text{ bir ikinci dereceden kalan degil} \end{cases}$$

olarak tanımlanır.

Örneğin, $p = 11$ ise

$$\left(\frac{a}{11}\right) = \begin{cases} +1, & a \equiv 1,3,4,5,9 \pmod{11} \\ 0, & 11 \mid a \\ -1, & a \equiv 2,6,7,8,10 \pmod{11}. \end{cases}$$

dir.

Aşağıdaki teorem, $x^2 \equiv -1 \pmod{p}$ denkliğinin hangi asal sayılar için bir çözümü olduğunu göstermektedir.

1.3.5 Teorem. –1 sayısının modülo p de ikinci dereceden bir kalan olması için gerek ve yeter şart $p \equiv 1 \pmod 4$ olmasıdır (Silverman 2006 ve Mollin 2000).

1.3.6 Teorem. $p > 2$ asal sayı ve $p \nmid a$ olmak üzere a nın modülo p de bir ikinci dereceden kalan olması için gerekli ve yeter şart $a^{\frac{(p-1)}{2}} \equiv 1 \pmod p$ olmasıdır (Silverman 2006).

Jacob Jacobi, Legendre sembolünü bileşik modlar için genelleştirmiş ve Jacobi sembolünü aşağıdaki gibi tanımlamıştır.

1.3.7 Tanım (Jacobi Sembolü). $n \in \mathbb{N}$ bir tek sayı, $a \in \mathbb{Z}$ ve $(a, n) = 1$ olsun. p_j ler asal sayılar olmak üzere $n = \prod_{j=1}^{k} p_j$ olsun. Bu durumda n sayısı için a tamsayısının *Jacobi sembolü*

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k}\left(\frac{a}{p_j}\right)$$

olarak tanımlanır, bu eşitliğin sağ tarafındaki sembol Legendre sembolünü belirtmektedir.

Örneğin, $n = 105 = 3 \cdot 5 \cdot 7$ ise $a = 2$ tamsayısı için,

$$\left(\frac{2}{105}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{7}\right) = (-1)(-1)(1) = 1$$

dir.

Kronecker sembolü adı verilen sembol yukarıdaki sembollerin en genelidir. Dikkat edilirse, Jacobi sembolü n sayısının bir tek sayı olması halinde tanımlıdır, Kronecker sembolü ise herhangi bir n doğal sayısı için tanımlıdır.

1.3.8 Tanım (Kronecker Sembolü). $n \in \mathbb{N}$ ve $\Delta \in \mathbb{Z}$ sayısı $\Delta \equiv 0, 1 \pmod 4$ özelliğinde bir tam kare olmayan sayı olsun. Bu durumda m tek sayı ve $n = 2^{\alpha}m$ özelliğinde bir sayı olmak üzere,

$$\left(\frac{\Delta}{n}\right) = \begin{cases} 0 & (\Delta, n) > 1 \\ \left(\frac{\Delta}{2}\right)^{\alpha}\left(\frac{\Delta}{m}\right) & (\Delta, n) = 1 \end{cases}$$

olarak tanımlanır, burada

$$\left(\frac{\Delta}{2}\right) = \begin{cases} +1, & \Delta \equiv 1 \pmod 8 \\ -1, & \Delta \equiv 5 \pmod 8 \end{cases}$$

ve $\left(\frac{\Delta}{m}\right)$, Jacobi sembolünü belirtir. Özel olarak, $\Delta = 2^k d$ ($d \in \mathbb{Z}$ tek) ve $(n, \Delta) = 1$ olmak üzere

$$\left(\frac{\Delta}{n}\right) = \left(\frac{2}{n}\right)^{k} \left(\frac{n}{|d|}\right)(-1)^{\frac{d-1}{2}\frac{n-1}{2}}$$

olur, burada $\left(\frac{n}{|d|}\right)$, Jacobi sembolünü belirtmektedir.

Örneğin, $n = 2831453 = 1033 \cdot 2741$ ve $\Delta = -21484 = -4 \cdot 41 \cdot 131 = -4 \cdot 5371$ için

$$\left(\frac{\Delta}{n}\right) = \left(\frac{2}{n}\right)^{2} \left(\frac{2831453}{5371}\right)(-1)^{\frac{5371-1}{2}\frac{2831453-1}{2}} = \left(\frac{2831453}{5371}\right)$$

ve $2831453 \equiv 936 \pmod{5371}$ olduğundan

$$\left(\frac{2831453}{5371}\right) = \left(\frac{936}{5371}\right) = \left(\frac{2}{5371}\right)^{3}\left(\frac{3}{5371}\right)^{2}\left(\frac{13}{5371}\right)$$

yazılabilir ve $5371 \equiv 3 \pmod 8$ olduğundan

$$-\left(\frac{13}{5371}\right) = -\left(\frac{5371}{13}\right) = -\left(\frac{2}{5371}\right) = 1$$

olarak bulunur.

Özellikle denkliklerin çözümlerinde kullanılan Fermat'ın küçük teoremi sayılar teorisinin en iyi bilinen teoremlerinden biridir.

1.3.9 Teorem (Fermat'ın Küçük Teoremi). p bir asal sayı ve a, modülo p de sıfırdan farklı bir sayı olsun. Bu durumda

$$a^{p-1} \equiv 1 \pmod{p}$$

dir (Silverman 2006).

1.4 Üçüncü Dereceden Kalanlar

Bu kısımda $\mathbb{F}_p$ sonlu cismi üzerinde üçüncü dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir.

1.4.1 Tanım. p bir asal sayı olmak üzere

$$x^3 \equiv a \pmod{p} \tag{1.2}$$

olacak biçimde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$ ye modülo p de bir *üçüncü dereceden kalan* denir.

Modülo p de üçüncü dereceden kalanların kümesi $\boldsymbol{K_p}$ ile gösterilir. Eğer (1.2) denkliğinin bir çözümü yoksa bu durumda $a \in \mathbb{Z}$ ye modülo p de bir *üçüncü dereceden kalan değildir* denir.

1.4.2 Teorem. $p \equiv 1 \pmod 3$ bir asal sayı olmak üzere $x^3 \equiv a \pmod{p}$ denkliğinin çözülebilmesi için gerek ve yeter şart $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ olmasıdır (Namlı 2001).

1.4.3 Teorem. Modülo p de farklı üçüncü dereceden kalanların sayısı,

$$p \equiv 1 \pmod 3 \text{ ise } \frac{p+2}{3},$$

$$p \equiv 2 \pmod 3 \text{ ise } p$$

dir (Namlı 2001)

2. ELİPTİK EĞRİLER

Bu bölümde eliptik eğriler hakkında bazı ön bilgiler verilecektir. Kısım 2.1 de eliptik eğrilerin nasıl ortaya çıktığı üzerinde durulacak ve eliptik eğri kavramı tanımlanacaktır. Kısım 2.2 de bir cisim üzerinde tanımlanmış olan bir E eliptik eğrisinin noktalarının oluşturduğu küme üzerinde toplama işlemi tanımlanacak ve bu kümenin bir grup yapısına sahip olduğu gösterilecektir. Kısım 2.3 de eliptik eğriler üzerindeki sonlu mertebeli noktalarla ilgilenilecek ve bir E eliptik eğrisi üzerinde mertebesi iki ve üç olan noktaların grup yapısı verilerek n-mertebeli noktaların grup yapısı ile ilgili sonuçlar ele alınacaktır. Kısım 2.4 de singüler eğri kavramı ile ilgilenilecek ve singüler eğriler üzerinde bulunan singüler olmayan noktaların grup yapısı ile ilgilenilecektir. Kısım 2.5 de $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisinin özellikleri belirtilecektir. Kısım 2.6 da sonlu bir cisim üzerinde tanımlı eliptik eğriler ele alınacaktır. Kısım 2.7 de bir E eliptik eğrisinin indirgemesi kavramı üzerinde durulacaktır.

2.1 Eliptik Eğriler

Eliptik eğriler teorisi, Fermat'ın son teoreminin çözümündeki rolünün öneminden dolayı matematiğin oldukça popüler bir çalışma alanı haline gelmiştir. Eliptik eğriler, çok uzun zamandır çözülemeyen problemlerin bile çözülmesinde rol oynayan cebirin en modern kavramlarından birisidir. Eliptik eğrilerin, matematik dünyasına girişi, ilk olarak Diophant'ın Arithmetica'sının dördüncü kitabındaki yirmi dördüncü problemde görülür. Burada ki problem şu şekildedir; verilen bir a sayısı, öyle iki parçaya ayrılsın ki, bu iki parçanın çarpımı başka bir sayının küpü ile kendisinin farkına eşit olsun, yani

$$y\,(a-y) = x^3 - x \tag{2.1}$$

özelliğinde x ve y sayıları bulunabilir mi? Diophant bu problemi, $a = 6$ için $k = 3$ olmak üzere,

$$x = ky - 1$$

alarak çözmüştür. Böylece (2.1) denklemi,

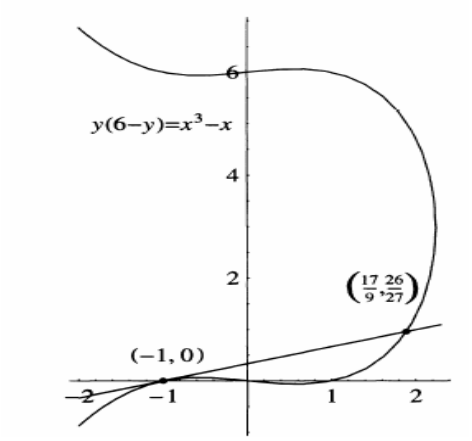
$$y\,(6-y) = (3y-1)^3 - 3y + 1$$

haline gelir ki, bu denklemin çözümleri $y = 0$ katlı kök ve $y = \frac{26}{27}$ biçimindedir. $y = 0$ katlı kökü göz önüne alınmazsa, $y = \frac{26}{27}$ için $x = \frac{17}{9}$ olarak bulunur.

Diophant'ın probleminin çözümüne modern bir yaklaşım şu şekildedir: (2.1) eşitliğinin katlı kökü olan 0 yardımıyla eğri üzerindeki (–1, 0) noktası elde edilir. Bu noktadan bir teğet doğru çizilirse bu doğru (2.1) eşitliğinin belirttiği eğriyi $\left(\frac{17}{9}, \frac{26}{27}\right)$ noktasında keser. Dolayısıyla, problemin çözümü $\frac{26}{27}$, $\frac{136}{27}$ $\left(6 = \frac{26}{27} + \frac{136}{27}\right)$ olup bu sayıların çarpımı da

$$\left(\frac{17}{9}\right)^3 - \frac{17}{9}$$

sayısına eşittir. Aşağıdaki grafikte, (2.1) eşitliğinin belirttiği eğri ve ele alınan eşitliği gerçekleyen nokta görülmektedir.



Şekil 2.1. $y\,(6 - y) = x^3 - x$ eğrisi

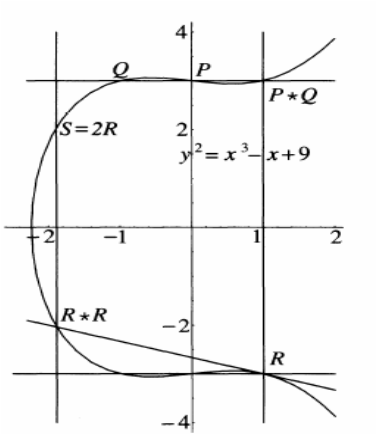
Eğer (2.1) denkleminde $a = 6$ alınır, her iki taraftan 9 çıkarılır ve

$$x \to -x \text{ ve } y \to y + 3$$

değişken değişimleri uygulanırsa,

$$E : y^2 = x^3 - x + 9$$

eğrisi elde edilir. Dikkat edilirse, $x^3 - x + 9$ denkleminin farklı kökleri vardır. (–1, 0) ve $\left(\frac{17}{9}, \frac{26}{27}\right)$ noktaları ise $E : y^2 = x^3 - x + 9$ eğrisi üzerinde sırasıyla, $R = (1, -3)$ ve $R * R = \left(-\frac{17}{9}, -\frac{55}{27}\right)$ noktalarına karşılık gelir. $R * R$ noktasının x eksenine göre simetriği alınarak E üzerinde, $2R = \left(-\frac{17}{9}, \frac{55}{27}\right)$ noktası elde edilir.



Şekil 2.2. $E : y^2 = x^3 - x + 9$ eğrisi

Yukarıdaki şekilde yeni eğri ve R, $R * R$ noktaları görülmektedir. Diophant bu işlemleri yaparken ileride adına eliptik eğriler teorisi denilecek olan bir teorinin temellerini de atmıştır. Yaptığı bu işlemler ile eğri üzerindeki noktaların oluşturduğu kümenin toplamsal bir grup olduğu daha sonra görülmüştür.

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

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

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

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

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

dir.

Kısım 2.2 de bir eliptik eğri üzerindeki noktaların kümesinin bir grup ve "*sonsuzdaki nokta*" adı verilen, $\boldsymbol{O} = (\infty, \infty)$ ile gösterilen noktanın bu grubun birim elemanı olduğu görülecektir. Bu nedenle bu noktanın daima E eliptik eğrisi üzerinde olduğu kabul edilecektir.

Üstelik $x^3 + Ax + B$ kübik polinomu katlı köke sahip olmamalıdır, yani E bir eliptik eğri ise

$$4A^3 + 27B^2 \neq 0$$

dir. Örneğin;

$$y^2 = x^3 + 1 \text{ ve } y^2 = x^3 - x$$

birer eliptik eğri belirttiği halde

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

eşitlikleri (x^3 ve $x^3 + x^2$ katlı köke sahip olduğundan) birer eliptik eğri belirtmez.

Bununla birlikte $x^3 + Ax + B$ kübik polinomunun katlı kök bulunması hali de oldukça ilginç bir durumdur. Eğer kübik polinomun katlı kökleri var ise $y^2 = x^3 + Ax + B$ eşitliği adına singüler eğriler denilen eğrileri belirtir.

Bir eliptik eğrinin Weierstrass uzun formu aşağıdaki gibi verilir.

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

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

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

Bu denklem için *Tate değerleri*

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

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

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

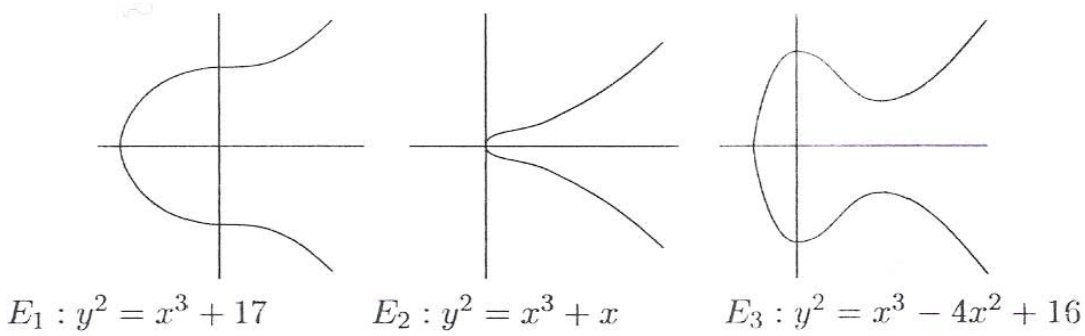
$$b_8 = a_1^2\, a_6 - a_1\, a_3\, a_4 + 4a_2\, a_6 + a_2\, a_3^2 - a_4^2$$

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

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

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

olarak tanımlanır.



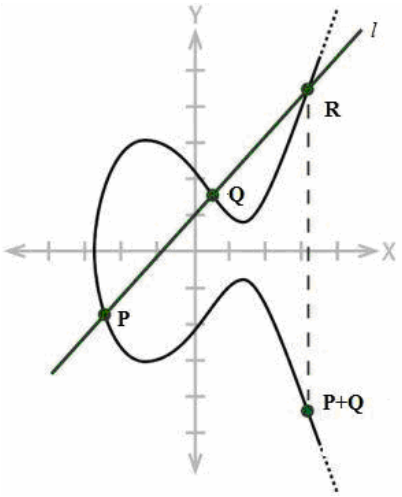
Şekil 2.3. Eliptik eğri örnekleri

2.2 Eliptik Eğrilerin Grup Yapısı

Bu kısımda şu ana kadar yalnızca nokta kümesi olarak ele alınan eliptik eğrilerin, üzerinde tanımlanan toplama işlemi yardımıyla aslında bir abel grubu olduğu görülecektir. Böylece eliptik eğriler üzerinde cebirsel işlemler de yapılabilecektir.

2.2.1 Tanım. E bir eliptik eğri, $\boldsymbol{O} = (\infty, \infty)$ ve $P, Q \in E$ olsun (Şekil 2.4). P ve Q noktalarından geçen doğru l olarak adlandırılsın. E eliptik eğrisinin Weierstrass

eşitliğinin derecesi 3 olduğundan l doğrusu ile E eliptik eğrisi P ve Q dışında R gibi üçüncü bir noktada kesişir. P ve Q noktalarının toplamı olan $P + Q$, az önce elde edilen R noktasının x eksenine göre simetriği olarak tanımlanır.



Şekil 2.4. Eliptik eğri üzerindeki toplama işlemi

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

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

denklemlerinden

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

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

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

noktasıdır.

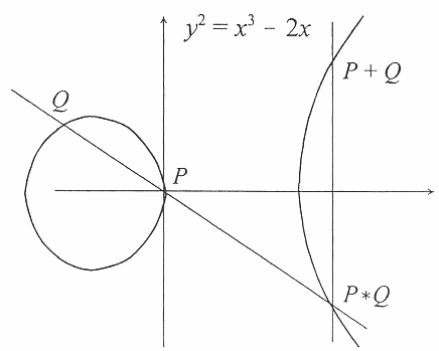
Bu şekilde tanımlanan toplama işlemi örnekler yardımıyla aşağıdaki şekilde açıklanabilir; ilk olarak

$$E_1 : y^2 = x^3 - 2x$$

eğrisi ve bu eğri üzerindeki $P = (0, 0)$ ve $Q = (–1, 1)$ noktaları dikkate alınırsa P ve Q noktalarından geçen l doğrusunun denklemi $y = –x$ olur. O halde, bu eğri ve l doğrusunun kesiştikleri noktalar

$$x^3 – x^2 – 2x = 0$$

denkleminden (0, 0), (–1, 1) ve (2, –2) olarak bulunur. Dolayısıyla, $P * Q = (2, –2)$ ve bu noktanın x eksenine göre simetriği olan nokta, yani $P + Q = (2, 2)$ dır. Aşağıdaki şekilde E_1 eğrisi üzerindeki P, Q, $P * Q$ ve $P + Q$ noktaları görülmektedir.

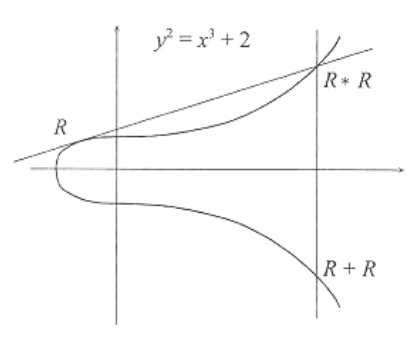


Şekil 2.5. $P = (0, 0)$ ve $Q = (–1, 1)$ noktalarının toplamı

Yukarıda farklı iki noktanın toplamı ile ilgili bir örnek ele alınmıştır, şimdi

$$E_2 : y^2 = x^3 + 2$$

eğrisi üzerindeki $R = (–1, 1)$ noktasının kendisi ile toplamı dikkate alınacaktır. Bu durumda E_2 eğrisinin R noktasındaki teğeti olan l doğrusunun denklemi $y = \frac{3x+5}{2}$ dir. E_2 eğrisi ile l teğet doğrusunun kesiştikleri noktalar $(x + 1)^2 \left(x – \frac{17}{4}\right) = 0$ eşitliği yardımıyla, (–1, 1) ve $\left(\frac{17}{4}, \frac{71}{8}\right)$ olarak bulunur. Dolayısıyla $R * R = \left(\frac{17}{4}, \frac{71}{8}\right)$ ve böylece $R + R = \left(\frac{17}{4}, -\frac{71}{8}\right)$ olarak elde edilir. Aşağıdaki şekilde E_2 eğrisi üzerindeki R, $R * R$ ve $R + R$ noktaları görülmektedir.



Şekil 2.6. $R = (-1, 1)$ noktasının kendisi ile toplamı

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

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

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

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

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

Yukarıda verilen teorem, E eliptik eğrisi üzerindeki noktaların oluşturduğu kümenin toplama işlemine göre bir değişmeli grup olduğunu belirtmektedir. Daha önce de belirtildiği gibi sonsuzdaki nokta "$\boldsymbol{O}$" bu grubun birim elemanıdır.

Weierstrass uzun formda verilen bir eliptik eğri üzerindeki toplama işlemi aşağıdaki gibi verilir.

2.2.3 Tanım. (Schmitt ve Zimmer 2003) $\mathbb{F}$ cismi üzerinde tanımlı Weierstrass uzun formda verilen

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

eliptik eğrisi için $P_1(x_1, y_1),\ P_2(x_2, y_2) \in E(\mathbb{F})$ olmak üzere,

i. $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$

ii. $P_1 = -P_2$ ise, yani $x_1 = x_2$ ve $y_2 + y_1 + a_1x_1 + a_3 = 0$ ise

$$P_1 + P_2 = \boldsymbol{O}$$

iii. $P_1 \neq -P_2$ ise,

a) $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} = y_1 - \lambda x_1$$

b) $x_1 = x_2$ ise

$$\lambda = \frac{3x_1^{\,2} + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \qquad \nu = \frac{-x_1^{\,3} + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

olmak üzere, $P_1 + P_2 = P_3 = (x_3, y_3)$ ise

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$$

dür.

2.2.4 Örnek. Weierstrass uzun formda verilen

$$y^2 + xy - y = x^3 - x^2$$

eliptik eğrisi üzerinde bulunan $P_1 = (0, 1)$ ve $P_2 = (1, 0)$ noktalarının toplamını elde etmek için,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{0 - 1}{1 - 0} = \frac{-1}{1} = -1$$

ve

$$\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} = \frac{1.1 - 0.0}{1 - 0} = 1$$

olarak bulunur. Böylece

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = (-1)^2 + 1.(-1) - (-1) - 0 - 1 = 0$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3 = -(-1+1).0 - 1 - (-1) = 0$$

olup, P_1 ve P_2 noktalarının toplamı $P_3 = (0, 0)$ olarak elde edilir.

2.3 Eliptik Eğriler Üzerindeki Sonlu Mertebeli Noktalar

Bu kısımda, E eliptik eğrileri üzerindeki sonlu mertebeli noktalar, yani büküm (torsiyon) noktaları ile ilgilenilecektir. İlk olarak sonlu mertebeli nokta kavramı açıklanacak daha sonra bir E eliptik eğrisi üzerinde mertebesi iki ve üç olan noktaların grup yapısı verilecek ve son olarak n-mertebeli noktaların grup yapısı ile ilgili sonuçlar ele alınacaktır.

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

$$nP = \boldsymbol{O}$$

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

2.3.2 Tanım. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ve $n \in \mathbb{N}$ olmak üzere

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

kümesine E eliptik eğrisinin *n. mertebeden noktalarının kümesi* ya da *n-büküm noktalarının kümesi* denir.

Dikkat edilirse $E[n]$ kümesi $E(\overline{\mathbb{F}})$ üzerinde tanımlanmıştır. Ayrıca $E[n]$ nin E nin bir alt grubu olduğu açıktır. Burada her $n \in \mathbb{N}$ için $\boldsymbol{O} \in E[n]$ dir.

Bir eliptik eğri üzerindeki iki mertebeli noktaların oluşturduğu grubun yapısı aşağıdaki önermede belirtilmiştir:

2.3.3 Önerme. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Eğer, $\mathbb{F}$ karakteristiği ikiden farklı bir cisim ise

$$E[2] \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$$

dir. Eğer $\mathbb{F}$ karakteristiği iki olan bir cisim ise

$$E[2] \cong \{ \boldsymbol{O} \} \text{ veya } \mathbb{Z}_2$$

dir (Washington 2003).

Aşağıdaki önermede bir eliptik eğri üzerindeki üç mertebeli noktaların oluşturduğu grubun yapısı belirtilmiştir:

2.3.4 Önerme. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Eğer, $\mathbb{F}$ karakteristiği iki ve üçten farklı bir cisim ise

$$E[3] \cong \mathbb{Z}_3 \otimes \mathbb{Z}_3$$

dür. Eğer $\mathbb{F}$ karakteristiği üç olan bir cisim ise

$$E[3] \cong \{ \boldsymbol{O} \} \text{ veya } \mathbb{Z}_3$$

dür (Washington 2003).

Aşağıdaki teoremde ise bir eliptik eğri üzerindeki n mertebeli noktaların oluşturduğu grubun yapısı belirtilmektedir:

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

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

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

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

dir (Washington 2003).

2.3.6 Uyarı. Karakteristiği p olan bir cisim üzerinde tanımlı E eliptik eğrisi için $E[p] \cong \mathbb{Z}_p$ ise E eliptik eğrisine *sıradan* (*ordinary*) eğri ve $E[p] \cong \{ \boldsymbol{O} \}$ ise *süpersingüler* eğri denir.

2.4 Singüler Eğriler

$x^3 + Ax + B = 0$ kübik denkleminin birbirinden farklı kökleri ya da katlı kökleri bulunabilir. Eğer bu kübik denklemin katlı kökü var ise $y^2 = x^3 + Ax + B$ eşitliğinin belirttiği eğrinin bir eliptik eğri olmadığı daha önce belirtilmişti. Acaba $x^3 + Ax + B = 0$ kübik denklemi katlı kök bulunduruyorsa ne olur? Toplama kuralı bu durumda da geçerli olur mu? Bu kısımda bu sorulara yanıtlar aranacak, bu durumda eliptik eğrinin noktalarının oluşturduğu küme üzerindeki toplama işleminin, $\mathbb{F}$ nin elemanlarının toplamı, $\mathbb{F}^* = \mathbb{F} \setminus \{\bar{0}\}$ ın elemanlarının çarpımı veya $\mathbb{F}$ nin bir genişlemesindeki elemanlarının çarpımına dönüştüğü görülecektir. İlk olarak bu katlı kökler yardımıyla elde edilen eğri üzerindeki noktalar adlandırılacak ve bu noktaların karakteri belirlenecektir.

2.4.1 Tanım. C cebirsel eğrisi $f(x, y) = 0$ denklemiyle verilsin. Bu durumda $P = (x_o, y_o) \in C$ noktasının C eğrisinin bir *singüler noktası* olması için gerek ve yeter şart

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

olmasıdır.

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

2.4.2 Önerme. Weierstrass uzun formunda verilen eliptik eğriler aşağıdaki gibi sınıflandırılabilir:

i. Eğri singüler değildir $\Leftrightarrow \Delta \neq 0$. Diğer durumda eğri tek bir singüler noktaya sahiptir,

ii. Eğrinin bir *düğümü* vardır $\Leftrightarrow \Delta = 0$ ve $c_4 \neq 0$ dır,

iii. Eğrinin bir *çıkıntısı* vardır $\Leftrightarrow \Delta = 0$ ve $c_4 = 0$ dır (Silverman 1986).

Örneğin $E_1 : y^2 = x^3$ ve $E_2 : y^2 = x^3 + ax^2$ ($a \in \mathbb{F}^*$) denklemleriyle verilen eğriler birer singüler eğridirler. $P = (0, 0)$ ve $\boldsymbol{O}$ noktasının bu eğriler üzerinde olduğu açıktır. Ayrıca $\Delta_{E_1} = \Delta_{E_2} = 0$ olduğundan bu eğrilerin j değişmezleri tanımlı değildir. Üstelik $c_{4,E_1} = 0$ ve $c_{4,E_2} = 16a^2$ olduğundan E_1 eğrisinin çıkıntısı ve E_2 eğrisinin düğümü vardır. Her iki halde de singüler nokta $P = (0, 0)$ noktasıdır. Bu noktanın singüler nokta olduğu kısmi türevler yardımıyla görülebilir. Örneğin E_1 eğrisi için,

$$f(x, y) = y^2 - x^3 = 0$$

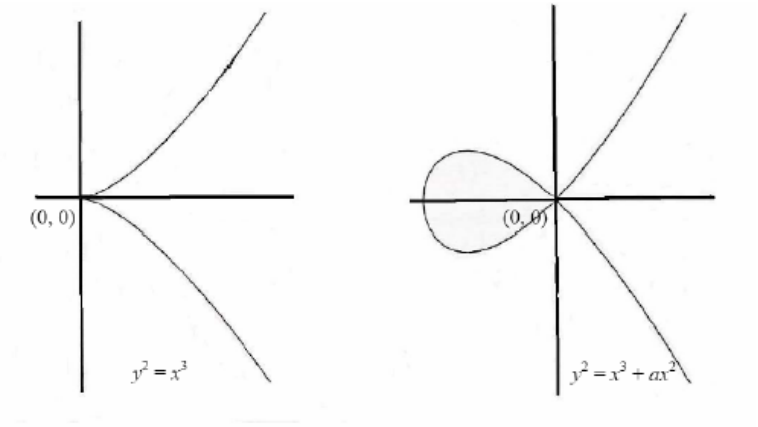
fonksiyonun kısmi türevleri

$$\frac{\partial f}{\partial x} = -3x^2, \qquad \frac{\partial f}{\partial y} = 2y$$

dir. O halde

$$y^2 - x^3 = 0, \qquad -3x^2 = 0, \qquad 2y = 0$$

denklemleri birlikte düşünülürse karakteristik ne olursa olsun bu üç denklemin bir tek çözümünün $x = y = 0$ olduğu görülür.



$P = (0, 0)$ noktası bir çıkıntıdır. $P = (0, 0)$ noktası bir düğümdür.

Şekil 2.7. Singüler eğriler

İlk olarak $E_1 : y^2 = x^3$ denklemi ile verilen singüler eğri ele alınacak ve bu singüler eğrinin özellikleri üzerinde durulacaktır. Dikkat edilirse, $P = (0, 0)$ noktası E_1 üzerindeki tek singüler noktadır. Bu noktadan geçen herhangi bir doğru E_1 eğrisini bu noktadan başka en çok bir noktada kesebileceğinden $P = (0, 0)$ noktası ile eğrinin herhangi bir noktasının toplanması mümkün değildir, yani bu singüler nokta ile eğrinin singüler olmayan noktaları toplanamaz. Bu nedenle eğri üzerindeki singüler olmayan noktalar ve sonsuzdaki nokta olan $\boldsymbol{O}$ noktasının oluşturduğu noktaların kümesi dikkate alınır, bu noktaların kümesi $E_{ns}(\mathbb{F})$ ile gösterilir. Bu kümenin noktaları ile toplama işlemi yapılır ve bu noktalar için toplama işlemi daha önceki gibi tanımlıdır. Bu durumda eğrinin singüler olmayan herhangi iki noktasından geçen doğru hiçbir zaman $P = (0, 0)$ noktasından geçmez.

Aşağıdaki teorem bu singüler eğrinin üzerindeki singüler olmayan noktaların oluşturduğu $E_{ns}(\mathbb{F})$ kümesinin bir toplamsal grup olduğunu göstermektedir:

2.4.3 Teorem. $\mathbb{F}$ cismi üzerinde tanımlı $E_1 : y^2 = x^3$ eğrisi verilsin. $E_{ns}(\mathbb{F})$, $\boldsymbol{O}$ noktası ile birlikte E üzerindeki singüler olamayan noktaların kümesi olsun. Bu durumda

$$E_{ns}(\mathbb{F}) \to \mathbb{F}, \quad (x, y) \to \frac{x}{y}, \ \boldsymbol{O} \to 0$$

dönüşümü bir izomorfizmidir ve $E_{ns}(\mathbb{F})$ bir toplamsal gruptur (Washington 2003, Silverman ve Tate 1992).

Benzer şekilde, $E_2 : y^2 = x^3 + ax^2$ denklemi ile verilen singüler eğri için de $P = (0, 0)$ noktası tek singüler noktadır. $\alpha^2 = a$ olmak üzere E_2 eğrisinin denklemi

$$\left(\frac{y}{x}\right)^2 = a + x$$

olarak da yazılabilir. x, 0 noktasına yaklaştıkça bu eşitliğin sağ tarafı a ya yaklaşır. O halde $x = 0$ olduğunda eğri

$$\left(\frac{y}{x}\right)^2 = a \text{ veya } \frac{y}{x} = \pm\alpha$$

olur. Bu ise (0, 0) noktasından geçen teğetlerin

$$y = \alpha x \text{ ve } y = -\alpha x$$

olduğunu gösterir. Böylece, bu durumda $E_{ns}(\mathbb{F})$ kümesinin grup yapısı sıradaki teorem ile verilebilir.

2.4.4 Teorem. $a \in \mathbb{F}^*$ olmak üzere $E_2 : y^2 = x^3 + ax^2$ eğrisi verilsin. Bu durumda $\alpha^2 = a$ olmak üzere ϕ dönüşümü

$$\phi : (x, y) \to \frac{y + \alpha x}{y - \alpha x}\ ,\ \boldsymbol{O} \to 1$$

olarak tanımlı olsun. Bu durumda,

i. $\alpha \in \mathbb{F}$ ise ϕ dönüşümü $E_{ns}(\mathbb{F})$ ve $\mathbb{F}^*$ arasında bir izomorfizmdir,

ii. $\alpha \notin \mathbb{F}$ ise ϕ dönüşümü $E_{ns}(\mathbb{F})$ ve $\{ u + \alpha v \mid u, v \in \mathbb{F}, u^2 - av^2 = 1\}$ arasında bir izomorfizmdir, bu küme çarpma işlemi altında bir gruptur (Washington 2003, Silverman ve Tate 1992).

2.5 $\mathbb{Q}$ Üzerinde Tanımlı Eliptik Eğriler

E eliptik eğrisinin $\mathbb{Q}$ üzerinde tanımlı olması durumunda akla gelen ilk soru eliptik eğri üzerindeki rasyonel noktaların sayısı olmuştur. Bu sayının sonsuz olması beklenen bir cevap olduğu halde bu sayı sonlu da olabilir, özellikle bu sayının sonlu olması durumları oldukça ilginçtir. Diğer yandan $E(\mathbb{Q})$, E nin bir abelyen alt grubu olduğundan $E(\mathbb{Q})$ nun grup yapısının belirlenmesi de bu durumun önemli problemlerinden birisidir. $E(\mathbb{Q})$ nun grup yapısıyla ilgili olarak verilen aşağıdaki teorem $\mathbb{Q}$ cismi için verildiği halde her hangi bir sayı cismi üzerinde de geçerlidir.

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

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

2.5.3 Uyarı 1. E eliptik eğrisi için

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

dir.

2. Trygve Nagell ve Elisabeth Lutz'in 1930'larda bağımsız olarak ispatladığı aşağıdaki teorem kullanılarak bir E eliptik eğrisi verildiğinde $E_{\text{tors}}(\mathbb{Q})$ u belirlemek mümkündür.

2.5.4 Lutz-Nagell Teoremi. (Washington 2003)

$$E : y^2 = x^3 + Ax + B, \ \ (A, B \in \mathbb{Z})$$

$\mathbb{Q}$ üzerinde bir eliptik eğri, $P = (x, y) \in E(\mathbb{Q})$ noktası ise sonlu mertebeli olsun. Bu durumda $x, y \in \mathbb{Z}$'dir ve $y \neq 0$ olması halinde

$$y^2 \mid 4A^3+27B^2$$

olur.

2.5.5 Sonuç. (Washington 2003) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda $E_{\text{tors}}(\mathbb{Q})$ sonludur.

2.5.6 Uyarı 1. $r = 0$ durumunda $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi üzerinde sonlu tane rasyonel nokta olacağı, yani $E(\mathbb{Q})$ nun sonlu olacağı açıktır.

2. $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi verildiğinde $E_{\text{tors}}(\mathbb{Q})$ nun izomorf olabileceği tüm gruplar Barry Mazur'un (1977) ve (1978) aşağıdaki teoremiyle verilmiştir.

2.5.7 Teorem. (Mazur 1977, 1978) E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

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

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

2.6 Sonlu Cisimler Üzerinde Tanımlı Eliptik Eğriler

Bu kısımda sonlu bir cisim üzerinde tanımlı eliptik eğriler ele alınacaktır. $\mathbb{F}_p$, p bir asal sayı olmak üzere p elemanlı sonlu bir cisim ve E eliptik eğrisi $\mathbb{F}_p$ cismi üzerinde tanımlı olsun. Bu durumda $x, y \in \mathbb{F}_p$ olacak biçimdeki E üzerindeki (x, y) ikilileri sonlu çoklukta olduğundan $E(\mathbb{F}_p)$ mutlaka sonlu bir grup oluşturur.

2.6.1 Örnek. $\mathbb{F}_5$ cismi üzerinde tanımlı $y^2 = x^3 + x + 1$ eliptik eğrisi dikkate alındığında, $E(\mathbb{F}_5)$ kümesini elde etmek için aşağıdaki tablo oluşturulabilir:

x	$x^3 + x + 1$	y	Noktalar
0	1	± 1	(0, 1), (0, 4)
1	3	-	-
2	1	± 1	(2, 1), (2, 4)
3	1	± 1	(3, 1), (3, 4)
4	4	± 2	(4, 2), (4, 3)
∞		∞	$\boldsymbol{O}$

Böylece eğrinin mertebesinin 9 olduğu görülür.

Sonlu cisimler üzerinde tanımlı eliptik eğrilerle ilgili çalışmaların büyük bir kısmı bu eğriler üzerindeki noktaların sayısının belirlenmesi ve bu noktaların oluşturduğu grupların yapıları ile ilgilidir. Yukarıda da belirtildiği ve örnekte de görüldüğü gibi sonlu cisimler üzerinde tanımlı eliptik eğriler üzerindeki noktaların kümesi sonlu bir gruptur. Sonlu bir cisim üzerinde tanımlı bir eliptik eğri üzerindeki noktaların sayısı için şöyle bir tahminde bulunulabilir; her bir x değeri için, eliptik eğrinin denklemini gerçekleyen en çok iki y değeri bulunacağından eğri üzerindeki noktaların sayısı için bir üst sınır $2p + 1$ olarak düşünülebilir, bu toplama sonsuzdaki $\boldsymbol{O}$ noktası da dahildir. Diğer yandan eğrinin bu denklemini gerçekleyen sonlu bir cisimdeki elemanların ikinci

dereceden bir kalan olma olasılığı yüzde elli olduğundan bu noktaların sayısı p tane olacaktır. Böylece eğri üzerindeki noktaların sayısı için bir üst sınır, $\boldsymbol{O}$ noktası ile birlikte $p + 1$ olur.

Diğer yandan Artin tarafından konjektür olarak verilen ve 1930'lu yıllarda Helmut Hasse tarafından ispatlanan aşağıdaki teorem $E(\mathbb{F}_p)$ nin eleman sayısı için literatürdeki en iyi sınırdır.

2.6.2 Hasse Teoremi (Silverman 1986)**.** E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

dır. Burada $\#E(\mathbb{F}_p)$, $\mathbb{F}_p$ cismi üzerinde tanımlı eğri üzerindeki noktaların sayısını göstermektedir.

2.6.3 Örnek 1. $\mathbb{F}_{101}$ cismi üzerinde $E : y^2 = x^3 + 7x + 1$ eliptik eğrisi göz önüne alınırsa (0, 1) noktasının bu eğri üzerinde olduğu açıktır. Doğrudan hesaplama yöntemiyle (0, 1) noktasının mertebesinin 116 olduğu görülebilir (ancak bu işlem verilen toplama işlemi kullanılarak oldukça uzun sürer). Lagrange Teoremi gereği noktanın mertebesi grubun mertebesini böleceğinden, $k \in \mathbb{Z}$ olmak üzere $\#E(\mathbb{F}_{101}) = 116 \cdot k$ olur.

Diğer yandan Hasse Teoremi gereği

$$101 + 1 - 2\sqrt{101} \leq \#E(\mathbb{F}_{101}) \leq 101 + 1 + 2\sqrt{101}$$

olur. Böylece $82 \leq \#E(\mathbb{F}_{101}) \leq 122$ elde edilir. Bu eşitsizlikten de $\#E(\mathbb{F}_{101}) = 116$ olduğu görülür.

2. $\mathbb{F}_{103}$ cismi üzerinde $E : y^2 = x^3 + 7x + 12$ eliptik eğrisi göz önüne alınırsa (–1, 2) ve (19, 0) noktalarının E eğrisi üzerinde olduğu görülebilir. Yine doğrudan hesaplama yöntemiyle (–1, 2) noktasının mertebesinin 13 ve (19, 0) noktasının mertebesinin de 2 olduğu bulunabilir. Dolayısıyla $k \in \mathbb{Z}$ olmak üzere $\#E(\mathbb{F}_{103}) = 26 \cdot k$ olur. Hasse Teoremi gereği

$$84 \leq \#E(\mathbb{F}_{103}) \leq 124$$

eşitsizliği elde edilir, bu eşitsizlikten de $\#E(\mathbb{F}_{103}) = 104$ olarak bulunur.

2.6.4 Uyarı 1. Yeterince büyük p asal sayıları için eğri üzerindeki noktanın mertebesini bulma problemi zorlaştığı gibi, "Hasse aralığı" olarak adlandırılan

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}$$

aralığı da genişler. Bu durumda eliptik eğri üzerinde birkaç nokta daha bulunup, mertebeleri hesaplanarak olasılıklar en aza indirgenebilir.

2. $E(\mathbb{F}_p)$ nin mertebesini hesaplamak kadar, sonlu mertebeye sahip olduğundan, $E(\mathbb{F}_p)$ nin izomorf olduğu grupları, yani grup yapılarının ne olduğunu bilmek de oldukça önemlidir.

2.6.5 Teorem. (Washington 2003) E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

i. Belirli bir $n \geq 1$ tamsayısı için

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n,$$

ii. $n_1 \mid n_2$ özelliğindeki $n_1, n_2 \geq 1$ tamsayıları için

$$E(\mathbb{F}_p) \cong \mathbb{Z}_{n_1} \otimes \mathbb{Z}_{n_2}$$

dir.

2.6.6 Örnek. $\mathbb{F}_2$ üzerinde tanımlı $y^2 + xy = x^3 + 1$ eğrisi üzerindeki noktalar basit bir hesaplama ile

$$E(\mathbb{F}_2) = \{ \boldsymbol{O}, (0, 1), (1, 0), (1, 1) \}$$

olarak elde edilir. Dolayısıyla $E(\mathbb{F}_2)$, 4 mertebeli devirli bir gruptur. (1, 0) ve (1, 1) noktalarının mertebesi 4, (0, 1) noktasının mertebesi ise 2 olarak bulunur. O halde

$$E(\mathbb{F}_2) \cong \mathbb{Z}_4$$

olur. $E(\mathbb{F}_4)$ nokta kümesi dikkate alındığında, ω, $\omega^2 + \omega + 1 = 0$ eşitliğinin bir çözümü olmak üzere $\mathbb{F}_4 = \{ 0, 1, \omega, \omega^2 \}$ olarak yazılabilir. Buna göre,

$$\begin{aligned}
&x = 0 \Rightarrow y^2 = 1 \Rightarrow y = 1 \\
&x = 1 \Rightarrow y^2 + y = 0 \Rightarrow y = 0,1 \\
&x = \omega \Rightarrow y^2 + \omega y = 0 \Rightarrow y = 0, \omega \\
&x = \omega^2 \Rightarrow y^2 + \omega^2 y = 0 \Rightarrow y = 0, \omega^2 \\
&x = \infty \Rightarrow y = \infty
\end{aligned}$$

olarak elde edilir. Böylece,

$$E(\mathbb{F}_4) = \{ \boldsymbol{O}, (0, 1), (1, 0), (1, 1), (\omega, 0), (\omega, \omega), (\omega^2, 0), (\omega^2, \omega^2) \}$$

olarak bulunur. Karakteristik 2 olduğundan mertebesi 2 olan en çok bir nokta vardır. Gerçekten de basit bir hesaplama ile (0, 1) noktasının mertebesinin 2 olduğu görülebilir. Dolayısıyla $E(\mathbb{F}_4)$ mertebesi 8 olan devirli bir gruptur. ω ya da ω^2 değerlerinden birini içeren dört noktadan biri ise üreteçtir.

2.6.7 Örnek. $\mathbb{F}_7$ üzerinde $E : y^2 = x^3 + 2$ eliptik eğrisi göz önüne alındığında basit bir hesaplama ile

$$E(\mathbb{F}_7) = \{ \boldsymbol{O}, (0, 3), (0, 4), (3, 1), (3, 6), (5, 1), (5, 6), (6, 1), (6, 6) \}$$

olduğu bulunabilir. E üzerindeki tüm noktalar 3 mertebelidir. Biri diğerinin katı olmayan E üzerindeki iki nokta $E(\mathbb{F}_7)$ nin 9 mertebeli bir alt grubunu üretir. Hasse Teoremi gereği

$$3 \leq \#E(\mathbb{F}_7) \leq 13$$

olduğu görülür. Böylece $\#E(\mathbb{F}_7) = 9$ olup

$$E(\mathbb{F}_7) \cong \mathbb{Z}_3 \otimes \mathbb{Z}_3$$

olur. Bu durum ise aşağıdaki teorem ile açıklanabilir.

2.6.8 Teorem. (Washington 2003) E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri ve

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \otimes \mathbb{Z}_n$$

olsun. Bu durumda ya $p = n^2 + 1$, ya $p = n^2 \pm n + 1$ ya da $p = (n \pm 1)^2$ dir.

2.6.9 Uyarı 1. Bu çalışmada, özellikle Tate normal formdaki eliptik eğriler dikkate alınacak ve yukarıdaki teorem kullanılarak bu eğriler üzerindeki noktaların oluşturduğu kümelerin grup yapıları belirlenecektir.

2. $A, B \in \mathbb{F}_p$ olmak üzere $y^2 = x^3 + Ax + B$ eliptik eğrisi üzerindeki rasyonel noktaların sayısını hesaplamak için farklı yöntemler geliştirilmiştir. Yeterince küçük p asalları dikkate alındığında $\#E(\mathbb{F}_p)$ yi hesaplamak için Legendre sembolünün kullanılması bu yöntemlerden birisidir, bu sembol kullanılarak eğrinin mertebesi aşağıdaki teorem yardımıyla hesaplanabilir.

3. p asal sayısı büyütüldüğünde bu teoremde verilen yöntem kullanılarak nokta sayısını hesaplamak zaman alabilir. Literatürde yer alan diğer yöntemlerin kullanılması halinde de yeterince büyük p asalı için $\mathbb{F}_p$ üzerinde tanımlı eliptik eğrilerin nokta sayısını hesaplamak bazen zor, bazen de imkansız olabilir.

2.6.10 Teorem. (Washington 2003) $A, B \in \mathbb{F}_p$ olmak üzere, $E : y^2 = x^3 + Ax + B$ olsun. Bu durumda

$$\#\, E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p} \right)$$

olur.

2.6.11 Örnek. $\mathbb{F}_5$ cismi üzerinde tanımlı $y^2 = x^3 + x + 1$ eğrisi üzerindeki noktaların sayısı yukarıdaki teorem yardımıyla

$$\#\, E(\mathbb{F}_5) = 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5} \right)$$

$$= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right)$$

$$= 6 + 1 - 1 + 1 + 1 + 1$$

$$= 9$$

olarak elde edilir.

2.6.12 Sonuç. (Washington 2003) $A, B \in \mathbb{F}_p$ olmak üzere $x^3 + Ax + B$ polinomu göz önüne alınırsa

$$\left| \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p} \right) \right| \leq 2\sqrt{p}$$

olur.

2.6.13 Uyarı. İlerleyen teknoloji ile birlikte bilgisayar tabanlı hesaplamalarda yüzlerce haneye sahip p asalları için $\mathbb{F}_p$ üzerinde tanımlı E eliptik eğrisinin üzerindeki rasyonel nokta sayısı süratli bir şekilde hesaplanabilmektedir.

2.6.14 Uygulama. MAGMA cebir programı (Bosma ve ark. 1997) kullanılarak, sonlu cisimler üzerinde tanımlı singüler olmayan eliptik eğrilerin rasyonel noktaları ve bunların sayısı aşağıdaki şekilde hesaplanır:

Girdi. a_1, a_2, a_3, a_4, a_6 ve p

Çıktı. $\mathbb{F}_p$ üzerinde tanımlı $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ için $\#E(\mathbb{F}_p)$

Komutlar ise

```
>E:=EllipticCurve([GF(p) | a1, a2, a3, a4, a6]);
>A:=RationalPoints;
>#E;
>#A;
```

dır. Örneğin $\mathbb{F}_7$ üzerinde tanımlı $E : y^2 - xy + y = x^3 - x^2 + x + 2$ eliptik eğrisi üzerindeki rasyonel noktaların sayısını bulan komutlar ve programın çıktısı

```
>E:=EllipticCurve([GF(7) | –1 , –1, 1, 1, 2]);
>#E;
>5
```

dir. Diğer yandan E eliptik eğrisi üzerindeki rasyonel noktalar projektif düzlem koordinatlarında aşağıdaki komutlar yardımıyla bulunabilir:

```
>E:=EllipticCurve([GF(7) | –1 , –1, 1, 1, 2]);
>A:=RationalPoints;
>A;
> { @ (0 : 1 : 0), (0 : 1 : 1), (0 : 5 : 1), (6 : 1 : 1), (6 : 6 : 1) @ }
```

Burada $(0 : 1 : 0)$, $\boldsymbol{O}$ noktasıdır. Elde edilen koordinatları kullanabilmek için, çıktıdaki projektif $(X : Y : Z)$ koordinatlarının

$$x = \frac{X}{Z} \text{ ve } y = \frac{Y}{Z}$$

dönüşümü kullanılarak dik koordinat sistemine dönüştürülmesi gerekir. ***O*** noktası hariç projektif koordinatlara sahip eğri üzerindeki tüm rasyonel noktaların Z bileşenlerinin 1 olması, projektif düzlemin özelliklerinden kaynaklanmaktadır.

2.7 Bir Eliptik Eğrinin İndirgemesi

$E : y^2 = x^3 + Ax + B$ eliptik eğrisi $\mathbb{Q}$ cismi üzerinde tanımlı bir eğri ve p bir asal sayı olsun. Bu durumda modülo p de bir indirgeme dönüşümü vardır. İndirgeme dönüşümü kullanılarak E eğrisinden

$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$$

eliptik eğrisi elde edilir, burada $\tilde{A}, \tilde{B} \in \mathbb{F}_p$ dir. Bu eğri için aşağıdaki üç halden biri söz konusudur ve dolayısıyla E eliptik eğrisi aşağıdaki biçimde sınıflandırılabilir:

2.7.1 Tanım. $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$ ($\tilde{A}, \tilde{B} \in \mathbb{F}_p$), E eğrisinin modülo p deki indirgemesi olsun. Bu durumda

i. $\tilde{E}$ singüler olmayan bir eğri ise E *iyi indirgemeye* sahiptir,

ii. $\tilde{E}$ eğrisinin düğümü (node) varsa E *çarpımsal indirgemeye* sahiptir,

iii. $\tilde{E}$ eğrisinin çıkıntısı (cusp) varsa E *toplamsal indirgemeye* sahiptir.

Son iki haldeki gibi bir indirgeme söz konusu ise E eliptik eğrisi *kötü indirgemeye* sahiptir denir. Eğer E çarpımsal indirgemeye sahip ve düğümden geçen teğetlerin eğimleri $\mathbb{F}_p$ (ya da $\mathbb{F}_p$ de değilse) de ise bu indirgemeye *dağılan çarpımsal indirgeme* (ya da *dağılmayan çarpımsal indirgeme*) denir.

2.7.2 Örnek. $\mathbb{Q}$ cismi üzerinde tanımlı

$$E : y^2 = x(x + 35)(x - 55)$$

eliptik eğrisi dikkate alınırsa, bu durumda E eğrisinin

$\mathbb{F}_5$ deki indirgemesi $\quad \tilde{E} : y^2 = x^3$

$\mathbb{F}_7$ deki indirgemesi $\quad \tilde{E} : y^2 = x^2(x + 1)$

$\mathbb{F}_{11}$ deki indirgemesi $\quad \tilde{E} : y^2 = x^2(x + 2)$

olarak elde edilir. E eğrisinin modülo 5 deki indirgemesi olan $\tilde{E}$ eğrisinin çıkıntısı vardır ve dolayısıyla E, $\mathbb{F}_5$ de toplamsal indirgemeye sahiptir. E eğrisinin modülo 7 deki indirgemesi olan $\tilde{E}$, $\mathbb{F}_7$ de dağılan çarpımsal indirgemeye sahiptir. Son olarak E eğrisinin modülo 11 deki indirgemesi olan $\tilde{E}$ eğrisi, (0, 0) noktasındaki teğetinin eğimi $\alpha \notin \mathbb{F}_{11}$ olduğundan, $\mathbb{F}_{11}$ de dağılmayan çarpımsal indirgemeye sahiptir. Dikkat edilirse her üç indirgemede de (0, 0) noktası eğri için bir singüler noktadır.

Eğer p asal sayısı 13 ten büyük bir asal sayı ise bu durumda eğriyi belirten kübik polinomun $\mathbb{F}_p$ de farklı kökleri olacaktır ve dolayısıyla E eğrisi $\mathbb{F}_p$ üzerinde singüler olmayan bir eğri olacaktır. Böylece E eğrisi $p > 13$ için iyi indirgemeye sahiptir (35 ve 55 sayılarının asal çarpanları dikkate alınırsa $p > 13$ asallarının bu çarpanlar içinde olmadığı açıktır).

Yukarıdaki örnekte de görüldüğü gibi, E eğrisi singüler bir eğri olmadığı halde bu eğrinin modülo p deki indirgemeleri singüler eğri olabilir.

3. TATE NORMAL FORMLAR

3.1 Giriş

Daha önce de belirtildiği gibi, çalışmanın temeli Tate Normal Formdaki eliptik eğrileri sonlu cisimler üzerinde ele almak, bu eğriler üzerindeki noktaların kümesini ve grup yapısını belirlemektir. Tate normal formların seçilmesinin nedeni bu eğri ailesinin özel bir eğri ailesi oluşudur. Eğer Mazur teoremi dikkate alınırsa, bir eliptik eğri üzerindeki sonlu mertebeli noktaların mertebesinin ancak 2, 3, 4, 5, 6, 7, 8, 9, 10 veya 12 olabileceği görülür. Bu ailedeki her bir eğri için, özellikle $P = (0, 0)$ noktası en büyük mertebeye sahip nokta olur. Örneğin bir eliptik eğri üzerinde 8 mertebeli bir $Q = (x, y)$ noktası bulunuyor ise bu eğri uygun dönüşümler yardımıyla üzerinde 8 mertebeli nokta olarak $P = (0, 0)$ noktasını bulunduran bir Tate normal formdaki eğriye dönüştürülebilir.

İlk olarak Tate normal formdaki eğri tanımı verilecektir, daha sonra bu eğriler ile ilgili temel özellikler üzerinde durulacaktır. Sonlu cisimler üzerinde bu eğri ailesinin özellikleri ele alınacaktır.

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

Weierstrass uzun formda verilmiş bir eğri olsun. Eğer $a_6 \neq 0$ ise $P = (0, 0)$ noktasının bu eğri üzerinde olmayacağı açıktır. Diğer yandan $P = (0, 0)$ noktası bu eğri üzerinde ise $a_6 = 0$ dır. Dolayısıyla $P = (0, 0)$ noktasını bulunduran eliptik eğri ailesindeki her bir eğri

$$E_0 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

biçimindedir. Bu eşitlikten türev alınarak,

$$(2y + a_1x + a_3)y' = 3x^2 + 2a_2x + a_4 - a_1y$$

olarak elde edilir. Buradan E_0 eğrisi üzerinde bulunan $P = (0, 0)$ noktasındaki teğetin eğimi

$$y'\big|_{(0,0)} = \frac{a_4}{a_3}$$

olur. Bu eğri yardımıyla

"E_0 üzerindeki $P = (0, 0)$ noktası singüler noktadır $\Leftrightarrow a_3 = a_4 = 0$"

olduğu görülür. Diğer yandan,

"E_0 üzerinde $P = (0, 0)$, 2 mertebeli singüler olmayan bir noktadır $\Leftrightarrow a_3 = 0, a_4 \neq 0$"

Dikkat edilirse bu halde $P = (0, 0)$ noktasındaki teğet x-eksenine diktir. Dolayısıyla 2 mertebeli ve singüler olmayan $P = (0, 0)$ noktasını bulunduran eğriler

$$E_{00} : y^2 + a_1xy = x^3 + a_2x^2 + a_4x$$

biçiminde ifade edilebilir.

Eğer $P = (0, 0)$ noktasının singüler olmayan bir nokta ve üstelik mertebesinin 2 den farklı olduğu kabul edilirse,

$$y = y' + \left(\frac{a_2}{a_3}\right)x' \quad \text{ve} \quad x = x'$$

değişken değişimleri yapılarak E_0 eğrisi

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

haline gelir.

Dikkat edilirse bu halde eğrinin $P = (0, 0)$ noktasındaki teğetinin eğimi 0 olduğundan, teğet x-eksenine paraleldir. Dolayısıyla,

"E' eğrisi üzerindeki $P = (0, 0)$ noktasının mertebesi 3 tür $\Leftrightarrow a_2 = 0, a_3 \neq 0$"

olarak elde edilir. Bu durumda E' eğrisinin, $P = (0, 0)$ noktasındaki teğeti olan $y = 0$ doğrusu üzerinde, 3 mertebeli bir noktasının olduğu görülür. Bu eğri ailesi de

$$E(a_1, a_3) : y^2 + a_1xy + a_3y = x^3$$

biçiminde ifade edilebilir.

(0, 0) noktası E' eğrisi üzerinde, teğetinin eğimi sıfır olan bir nokta olmak üzere E' eğrisi

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

eşitliği ile verilsin. İlk olarak (0, 0) noktasının mertebesinin 2 olmadığını varsayalım. Bu durumda, "(0, 0) noktasının mertebesinin 3 olması için gerekli ve yeterli koşul $a_2 = 0$ ve $a_3 \neq 0$ olmasıdır." Bu nedenle (0, 0) noktasının mertebesinin 2 veya 3 olmadığı kabul edilirse a_2 ve a_3 katsayılarının sıfırdan farklı alınması gerektiği sonucu elde edilir. Bu durumda x yerine u^2x ve y yerine u^3y değişken değişimleri yapılarak, E' eğrisini belirten eşitlik

$$u^6y^2 + a_1u^5xy + a_3u^3y = u^6x^3 + a_2u^4x^2$$

haline gelir. Bu eşitlikte gerekli sadeleştirmeler yapılırsa

$$y^2 + \frac{a_1}{u}xy + \frac{a_3}{u^3}y = x^3 + \frac{a_2}{u^2}x^2$$

elde edilir. Burada $a_2' = a_3' = -b$ olarak alınırsa

$$\frac{a_2}{u^2} = \frac{a_3}{u^3}$$

eşitliği yardımıyla

$$u = \frac{a_3}{a_2}$$

olarak bulunur. Ayrıca

$$a_1' = \frac{a_1}{u} = 1 - c$$

alınarak E' eliptik eğrisi

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

biçiminde ifade edilir. Dikkat edilirse, böylece E' eliptik eğrisi, b ve c gibi, sadece iki parametre ile ifade edilmiş olur.

Örneğin,

$$E' : y^2 + 17xy - 120y = x^3 - 60x^2$$

eliptik eğrisi için x yerine u^2x ve y yerine u^3y değişken değişimleri yapılırsa

$$y^2 + \frac{17}{u}xy - \frac{120}{u^3}y = x^3 - \frac{60}{u^2}x^2$$

ve dolayısıyla

$$\frac{-120}{u^3} = \frac{-60}{u^2}$$

eşitliğinden $u = 2$ elde edilir. Böylece E' eğrisi

$$E' : y^2 + \frac{17}{2}xy - 15y = x^3 - 15x^2$$

biçiminde ifade edilebilir. $P = (0, 0)$ noktası bu eğri üzerinde 8 mertebeli bir noktadır, üstelik diğer tamsayı koordinatlı noktalar

$$\boldsymbol{O}, (0, 15), (-3, 36), (6, -18), (-10, 50), (15, 0), (60, 225), (60, -720)$$

ve bunların mertebeleri sırasıyla 1, 8, 4, 2, 2, 4, 8, 8 dir. Görüldüğü gibi $P = (0, 0)$ noktası bu eğri üzerindeki en büyük mertebeye sahip tamsayı koordinatlı noktalardan biridir.

Üzerinde sonlu mertebeli noktalar bulunduran eliptik eğrilerin bu şekilde sadece iki parametre ile temsil edilmesine özel bir isim verilir.

3.1.1 Tanım. $P = (0, 0)$ noktalı E eliptik eğrisinin *Tate normal formu*

$$E = E(b, c) : y^2 + (1-c)xy - by = x^3 - bx^2$$

olarak tanımlanır.

Bu E eliptik eğrisinin diskriminantı, bu iki parametre yardımıyla

$$\Delta(b, c) = (1-c)^4 b^3 - (1-c)^3 b^3 - 8(1-c)^2 b^4 + 36(1-c)b^4 - 27b^4 + 16b^5$$

olur.

3.1.2 Uyarı. Daha önce verilmiş olan, eğri üzerindeki noktaların toplamı formülleri ve

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

Tate normal formdaki eliptik eğrisi üzerindeki P = (0, 0) noktası yardımıyla P noktasının katları olan noktalar elde edilebilir. Bu noktaların bilinmesi P = (0, 0) noktasının mertebesinin n = 4, 5, 6, 7, 8, 9, 10 ve 12 olması halinde b ve c parametrelerinin de bilinmesini sağlayacaktır.

$d = \frac{b}{c}$, $e = \frac{c}{d-1}$ ve $f = \frac{d-e}{e-1}$ olmak üzere,

$P = (0, 0)$, $\quad -P = (0, b)$

$2P = (b, bc)$, $\quad -2P = (b, 0)$

$3P = (c, b-c)$, $\quad -3P = (c, c^2)$

$4P = (d(d-1),\ d^2(c-d+1))$, $\quad -4P = (d(d-1),\ d(d-1)^2)$

$5P = (de(e-1),\ de^2(d-e))$, $\quad -5P = (de(e-1),\ d^2e(e-1)^2)$

$6P = (ef(1+f),\ e^2(f+1)^2(-2f+ef+e-1))$, $\quad -6P = (ef(1+f),\ e^2f^2(1+f))$

dir (Husemöller 2004).

Dikkat edilirse bu noktaların koordinatları tamamen b ve c sayılarına bağlı olarak ifade edilebilmektedir. b ve c sayılarının neler olduklarının belirlenebilmesi için yukarıda verilen noktaların kullanılması gereklidir. Bu noktalar yardımıyla n = 4, 5, 6, 7, 8, 9, 10 ve 12 için

$$nP = \boldsymbol{O}$$

denklemi çözülerek bulunan b ve c parametreleri ile Tate normal formdaki eğriler sınıflandırılacaktır. Belirtilen n değerleri için $nP = \boldsymbol{O}$ denklemi P = (0, 0) noktasının mertebesinin n olduğunu gösterir. Böylece tüm sonlu mertebeli noktaları bulunduran Tate normal formlar belirlenmiş olur. n = 2, 3 hallerinde ise Tate normal form olmadığından bu haller ele alınmamıştır.

1. *n* = 4 Hali: Bu halde, $P = (0, 0)$ noktası E üzerinde 4 mertebeli bir nokta olduğunda E eğrisinin Tate normal formu belirlenecektir. Eğer $4P = \boldsymbol{O}$ eşitliği $2P = -2P$ olarak yazılırsa

$$(b, bc) = (b, 0)$$

eşitliğinden $c = 0$ elde edilir.

2. *n* = 5 Hali: $P = (0, 0)$ nin E üzerinde 5 mertebeli bir nokta olması halinde E eğrisinin Tate normal formu belirlenecektir. Bunun için $5P = \boldsymbol{O}$ eşitliği $3P = -2P$ olarak yazıldığında

$$(c, b - c) = (b, 0)$$

eşitliğinden $b = c$ elde edilir.

3. *n* = 6 Hali: Bu halde $6P = \boldsymbol{O}$ denklemi $3P = -3P$ olarak yazıldığında

$$(c, b - c) = (c, c^2)$$

eşitliğinden $b = c^2 + c$ elde edilir.

4. *n* = 7 Hali: $7P = \boldsymbol{O}$ denklemi $4P = -3P$ olarak yazıldığında

$$(d(d-1), d^2(c - d + 1)) = (c, c^2)$$

eşitliğinden $c = d(d-1)$ ve dolayısıyla $c^2 = d^2(d-1)^2 = d^2(c - d + 1)$ eşitliğinden de $d^2 - 2d + 1 = c - d + 1$ elde edilir. Gerekli sadeleştirmeler yapılırsa, $c = d^2 - d$ ve $d = \frac{b}{c}$ olduğundan $b = d^3 - d^2$ olarak bulunur.

5. *n* = 8 Hali: $8P = \boldsymbol{O}$ denklemi $4P = -4P$ olarak yazıldığında

$$(d(d-1), d^2(c - d + 1)) = (d(d-1), d(d-1)^2)$$

eşitliğinden

$$d^2(c-d+1) = d(d-1)^2 \Rightarrow d(c-d+1) = (d-1)^2$$

ve böylece

$$c = \frac{(d-1)(2d-1)}{d} \text{ ve } b = cd = (d-1)(2d-1)$$

olarak bulunur.

6. *n* = 9 Hali: $9P = \boldsymbol{O}$ denklemi $5P = -4P$ olarak yazıldığında

$$(de(e-1), de^2(d-e)) = (d(d-1), d(d-1)^2)$$

eşitliğinden

$$de(e-1) = d(d-1) \Rightarrow e(e-1) = d-1$$

$$\Rightarrow d = e^2 - e + 1$$

bulunur. Buradan

$$c = de - e = e^3 - e^2$$

ve

$$b = cd = (e^3 - e^2)(e^2 - e + 1) = e^5 - 2e^4 + 2e^3 - e^2$$

olarak elde edilir.

7. *n* = 10 Hali: $10P = \boldsymbol{O}$ denklemi $5P = -5P$ olarak yazıldığında

$$(de(e-1), de^2(d-e)) = (de(e-1), d^2e(e-1)^2)$$

eşitliğinden

$$de^2(d-e) = d^2e(e-1)^2 \Rightarrow e(d-e) = d(e-1)^2$$

elde edilir, gerekli işlemler yapılırsa

$$d = \frac{-e^2}{e^2 - 3e + 1}$$

olarak bulunur. Buradan

$$c = de - e = \frac{2e^3 - 3e^2 + e}{e - (e-1)^2} \quad \text{ve} \quad b = \frac{ce^2}{e - (e-1)^2}$$

elde edilir.

8. *n* = 12 Hali: $12P = \boldsymbol{O}$ denklemi $6P = -6P$ olarak yazıldığında

$$(ef(1+f),\, e^2(f+1)^2(-2f + ef + e - 1)) = (ef(1+f),\, e^2 f^2 (f+1))$$

eşitliğinden

$$e = \frac{3f^2 + 3f + 1}{(f+1)^2}$$

olarak bulunur. Buradan

$$c = \frac{(3f^2 - 3f + 1)(f - 2f^2)}{(f-1)^3}$$

ve

$$b = \frac{c(2f - 2f^2 - 1)}{f - 1}$$

olarak elde edilir.

3.1.3 Sonuç. Yukarıdaki haller dikkate alındığında, *n, P* = (0, 0) noktasının mertebesini göstermek üzere,

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

denklemi ile verilen Tate normal formlar, α parametresine bağlı olarak, aşağıdaki gibi sınıflandırılabilir:

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

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

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

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

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

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

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

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

Yukarıda verilen b ve c parametrelerine göre her bir hal için Tate normal formdaki eliptik eğrilerin denklemleri ve bu eğrilerin diskriminantları ise aşağıdaki gibidir:

1. $n=4$ için $y^2+xy-\alpha y=x^3-\alpha x^2$ ve $\Delta=\alpha^4+16\alpha^5$

2. $n=5$ için $y^2+(1-\alpha)xy-\alpha y=x^3-\alpha x^2$ ve $\Delta=\alpha^5(-1-11\alpha+\alpha^2)$

3. $n=6$ için $y^2+(1-\alpha)xy-(\alpha+\alpha^2)y=x^3-(\alpha+\alpha^2)x^2$ ve $\Delta=\alpha^4(1+16\alpha)$

4. $n=7$ için $y^2+(1+\alpha-\alpha^2)xy-(\alpha^3-\alpha^2)y=x^3-(\alpha^3-\alpha^2)x^2$ ve

$$\Delta=\alpha^7(\alpha^3-8\alpha^2+5\alpha+1)(\alpha-1)^7$$

5. $n=8$ için $y^2+\left(1-\dfrac{(2\alpha-1)(\alpha-1)}{\alpha}\right)xy-(2\alpha-1)(\alpha-1)y=x^3-(2\alpha-1)(\alpha-1)x^2$ ve

$$\Delta=\frac{(2\alpha-1)^4(\alpha-1)^8(8\alpha^2-8\alpha+1)}{\alpha^4}$$

6. $n=9$ için $y^2+(1-\alpha^2(\alpha-1))xy-(\alpha^2(\alpha-1)(\alpha(\alpha-1)+1))y=x^3-(\alpha^2(\alpha-1)(\alpha(\alpha-1)+1))x^2$

$$\Delta=\alpha^9(\alpha^3-6\alpha^2+3\alpha+1)(\alpha^2-\alpha+1)^3(\alpha-1)^9$$

7. $n=10$ için $y^2+\left(1-\dfrac{2\alpha^3-3\alpha^2+\alpha}{\alpha-(\alpha-1)^2}\right)xy-\dfrac{(2\alpha^3-3\alpha^2+\alpha)\alpha^2}{(\alpha-(\alpha-1)^2)^2}y=x^3-\dfrac{(2\alpha^3-3\alpha^2+\alpha)\alpha^2}{(\alpha-(\alpha-1)^2)^2}x^2$

$$\Delta=\frac{\alpha^{10}(2\alpha-1)^5(\alpha-1)^{10}(-1-2\alpha+4\alpha^2)}{(-3\alpha+\alpha^2+1)^{10}}$$

8. $n=12$ için

$$y^2+\left(1-\frac{(3\alpha^2-3\alpha+1)(\alpha-\alpha^2)}{(\alpha-1)^3}\right)xy-\frac{(3\alpha^2-3\alpha+1)(\alpha-\alpha^2)(2\alpha-2\alpha^2-1)}{(\alpha-1)^4}y$$

$$= x^3 - \frac{(3\alpha^2 - 3\alpha + 1)(\alpha - \alpha^2)(2\alpha - 2\alpha^2 - 1)}{(\alpha - 1)^4} x^2$$

$$\Delta = \frac{(3\,\alpha^2 - 3\,\alpha + 1)^4\,\alpha^{12}\,(-1 + 2\,\alpha)^6\,(-2\,\alpha + 2\,\alpha^2 + 1)^3\,(6\,\alpha^2 - 6\,\alpha + 1)}{(\alpha - 1)^{24}}$$

3.1.4 Uyarı. Tate normal formda verilen eliptik eğri sonlu cisim üzerinde ele alındığında, bu eğri iyi veya kötü indirgemeye sahip olabilir. Örneğin

$$y^2 - 4xy - 30y = x^3 - 30x^2$$

eğrisinin $p = 23$ için $\mathbb{F}_{23}$ deki indirgemesi

$$y^2 - 4xy - 7y = x^3 - 7x^2$$

dir ve bu eğri için $\Delta = 0$ olduğundan bu indirgeme kötü, $p = 29$ için $\mathbb{F}_{29}$ daki indirgemesi

$$y^2 - 4xy - y = x^3 - x^2$$

dir ve $\Delta \neq 0$ olduğundan bu indirgeme iyidir.

Çalışmada sadece iyi indirgeme hali dikkate alınacaktır ve bu tip eğriler üzerindeki noktalar, noktaların oluşturduğu grupların yapıları üzerinde durulacaktır.

3.2 Tate Normal Formdaki Eliptik Eğriler Üzerindeki Noktaların Belirlenmesi

Bu kısımda $\mathbb{F}_p$ ($p \leq 47$asal) sonlu cisimleri üzerinde tanımlı Tate normal formda verilen eliptik eğrilerin üzerindeki noktaların neler olduğu belirlenmiştir. Bu noktalar MAPLE12 programı kullanılarak, ekte verilen program yardımıyla, bulunmuştur. Yukarıda da belirtildiği gibi $P = (0, 0)$ noktasının mertebesine bağlı olarak eğriler Tate normal formlardaki eğri sınıflarına ayrılmıştır. Aşağıdaki örnekte, $P = (0, 0)$ noktasının 4 mertebeli olması halinde Tate normal formdaki eğrilerin $\mathbb{F}_{17}$ üzerinde ele alınması ile elde edilen noktalar verilmiştir. Benzer sonuçlar $P = (0, 0)$ noktasının mertebesinin 4 ten farklı olması hallerinde de elde edilmiş, ancak çalışmayı gereksiz büyüteceğinden bu sonuçlara burada yer verilmemiştir.

3.2.1 Örnek. $n = 4$ olsun, yani üzerinde 4 mertebeli $P = (0, 0)$ noktasını bulunduran

$$y^2 + xy - \alpha y = x^3 - \alpha x^2$$

Tate normal formdaki eliptik eğrileri dikkate alalım, dikkat edilirse bu eşitlik α parametresine bağlı bir eliptik eğri ailesi belirtir. Bu ailedeki eğrilerin $p = 17$ ve $\alpha \in \mathbb{F}_{17}$ için $\mathbb{F}_{17}$ deki indirgemeleri ve üzerindeki noktalar aşağıdaki gibidir.

$\alpha = 1$ için E eğrisi

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

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_1} = \{ \boldsymbol{O}, (0, 0), (0, 1), (1, 0), (2, 8), (3, 5), (3, 10), (5, 4), (5, 9), (9, 14), (9, 12),$$
$$(10, 11), (10, 14), (14, 8), (14, 13), (16, 5), (16, 14) \}.$$

$\alpha = 2$ için E eğrisi

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

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_2} = \{ \boldsymbol{O}, (0, 0), (0, 2), (2, 0), (4, 3), (4, 12), (7, 3), (7, 9), (8, 3), (8, 8), (10, 13),$$
$$(11, 4), (13, 10), (13, 13), (14, 6), (14, 14) \}.$$

$\alpha = 3$ için E eğrisi

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

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_3} = \{ \boldsymbol{O}, (0, 0), (0, 3), (1, 5), (1, 14), (2, 6), (2, 12), (3, 0), (5, 16), (6, 5), (6, 9), (7, 7),$$
$$(7, 6), (8, 2), (8, 10), (9, 3), (9, 8), (11, 3), (11, 6), (13, 2), (13, 5), (15, 7),$$
$$(15, 15), (16, 2) \}.$$

$\alpha = 4$ için E eğrisi

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

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_4} = \{ \boldsymbol{O}, (0, 0), (0, 4), (3, 7), (3, 11), (4, 0), (5, 6), (5, 10), (7, 4), (7, 10), (9, 2), (9, 10), (14, 3), (14, 4), (15, 9), (15, 14) \}.$$

$\boldsymbol{\alpha = 5}$ için E eğrisi

$$E : y^2 + xy - 5y = x^3 - 5x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_5} = \{ \boldsymbol{O}, (0, 0), (0, 5), (1, 2), (3, 1), (5, 0), (6, 1), (6, 15), (10, 3), (10, 9), (11, 12), (11, 16), (12, 14), (12, 13), (13, 1), (13, 8) \}.$$

$\boldsymbol{\alpha = 6}$ için E eğrisi

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

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_6} = \{ \boldsymbol{O}, (0, 0), (0, 6), (6, 0), (10, 7), (10, 6), (13, 4), (13, 16), (15, 3), (15, 5), (16, 11), (16, 13) \}.$$

$\boldsymbol{\alpha = 7}$ için E eğrisi

$$E : y^2 + xy - 7y = x^3 - 7x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_7} = \{ \boldsymbol{O}, (0, 0), (0, 7), (2, 7), (2, 15), (3, 8), (3, 13), (4, 9), (4, 11), (5, 7), (5, 12), (7,0), (8, 5), (8, 11), (10, 4), (10, 10), (12, 1),(12, 11),(16, 9), (16, 16) \}.$$

$\boldsymbol{\alpha = 8}$ için E eğrisi

$$E : y^2 + xy - 8y = x^3 - 8x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_8} = \{ \boldsymbol{O}, (0, 0), (0, 8), (1, 11), (1, 13), (2, 9), (2, 14), (3, 6), (3, 16), (4, 7), (4, 14), (5, 5), (5, 15), (7, 2), (7, 16), (8, 0), (9, 5), (9, 11), (11, 5), (11, 9), (12, 4), (12, 9), (15, 11), (15, 16) \}.$$

$\alpha = 9$ için E eğrisi

$$E : y^2 + xy - 9y = x^3 - 9x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_9} = \{ \boldsymbol{O}, (0, 0), (0, 9), (1, 9), (1, 16), (6, 7), (6, 13), (8, 9), (9, 0), (13, 15), (14, 14), (14, 15), (15, 1), (15, 10), (16, 12), (16, 15) \}.$$

$\alpha = 10$ için E eğrisi

$$E : y^2 + xy - 10y = x^3 - 10x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{10}} = \{ \boldsymbol{O}, (0, 0), (0, 10), (2, 3), (2, 5), (3, 3), (3, 4), (4, 10), (4, 13), (5, 2), (5, 3), (6, 10), (6, 11), (7, 8), (7, 12), (8, 4), (8, 15), (9, 9), (10, 0), (11, 1), (11, 15), (12, 16), (16, 4), (16, 7) \}.$$

$\alpha = 11$ için E eğrisi

$$E : y^2 + xy - 11y = x^3 - 11x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{11}} = \{ \boldsymbol{O}, (0, 0), (0, 11), (1, 12), (1, 15), (4, 2), (4, 5), (6, 8), (6, 14), (9, 4), (9, 15), (10, 2), (10, 16), (11, 0), (12, 6), (12, 10), (13, 3), (13, 12), (14, 2), (14, 12) \}.$$

$\alpha = 12$ için E eğrisi

$$E : y^2 + xy - 12y = x^3 - 12x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{12}} = \{ \boldsymbol{O}, (0, 0), (0, 12), (1, 4), (1, 7), (2, 11), (2, 16), (12, 0), (14, 5), (14, 10), (16, 3), (16, 10) \}.$$

$\alpha = 13$ için E eğrisi

$$E : y^2 + xy - 13y = x^3 - 13x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{13}} = \{ \boldsymbol{O}, (0, 0), (0, 13), (2, 1), (2, 10), (4, 1), (4, 8), (7, 1), (7, 5), (10, 8), (10, 12), (13, 0), (15, 2), (15, 13), (16, 6), (16, 8) \}.$$

$\boldsymbol{\alpha = 14}$ için E eğrisi

$$E : y^2 + xy - 14y = x^3 - 14x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{14}} = \{ \boldsymbol{O}, (0, 0), (0, 14), (1, 3), (1, 10), (4, 4), (4, 6), (6, 4), (8, 7), (8, 16), (11, 7), (11, 13), (12, 7), (12, 12), (14, 0), (15, 8) \}.$$

$\boldsymbol{\alpha = 15}$ için E eğrisi

$$E : y^2 + xy - 15y = x^3 - 15x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{15}} = \{ \boldsymbol{O}, (0, 0), (0, 15), (1, 6), (1, 8), (3, 14), (3, 15), (5, 13), (5, 14), (6, 3), (6, 6), (7, 11), (7, 14), (8, 1), (8, 6), (9, 7), (9, 16), (11, 10), (11, 11), (12, 5), (12, 15), (14, 7), (14, 11), (15, 0) \}.$$

$\boldsymbol{\alpha = 16}$ için E eğrisi

$$E : y^2 + xy - 16y = x^3 - 16x^2$$

ve bu eğri üzerindeki noktaların kümesi

$$E_{\alpha_{16}} = \{ \boldsymbol{O}, (0, 0), (0, 16), (7, 13), (9, 1), (9, 6), (10, 1), (10, 5), (11, 8), (11, 14), (13, 9), (13, 11), (14, 1), (15, 6), (15, 12), (16, 0) \}$$

olarak elde edilir.

3.2.2 Uyarı 1. $n = 4$, yani üzerinde 4 mertebeli $P = (0, 0)$ noktasını bulunduran

$$y^2 + xy - \alpha y = x^3 - \alpha x^2$$

Tate normal formdaki eliptik eğrilerin üzerindeki noktaların neler olduğu, α parametresine bağlı olarak $\mathbb{F}_{17}$ için yukarıda belirlenmiştir. $p \leq 47$ olmak üzere bu eğri ailesi $\mathbb{F}_p$ için dikkate alındığında bulunan noktaların sayısının, $k \in \mathbb{Z}$ olmak üzere

i. $p \equiv 1 \pmod 4$ ise $\#E(\mathbb{F}_p) = p - 1 - 4k$

ii. $p \equiv 3 \pmod 4$ ise $\#E(\mathbb{F}_p) = p - 3 - 4k$

olduğu görülmüştür.

2. Benzer çalışma n sayısının 4 ten farklı olması halinde de yapıldığında, $k \in \mathbb{Z}$ olmak üzere,

n* = 5** için, ***i. $p \equiv 1 \pmod 5$ ise $\#E(\mathbb{F}_p) = p - 1 - 5k$

ii. $p \equiv 2 \pmod 5$ ise $\#E(\mathbb{F}_p) = p - 2 - 5k$

iii. $p \equiv 3 \pmod 5$ ise $\#E(\mathbb{F}_p) = p - 3 - 5k$

iv. $p \equiv 4 \pmod 5$ ise $\#E(\mathbb{F}_p) = p - 4 - 5k$

n* = 6** için, ***i. $p \equiv 1 \pmod 6$ ise $\#E(\mathbb{F}_p) = p - 1 - 6k$

ii. $p \equiv 5 \pmod 6$ ise $\#E(\mathbb{F}_p) = p - 5 - 6k$

n* = 7** için, ***i. $p \equiv 1 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 1 - 7k$

ii. $p \equiv 2 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 2 - 7k$

iii. $p \equiv 3 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 3 - 7k$

iv. $p \equiv 4 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 4 - 7k$

v. $p \equiv 5 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 5 - 7k$

vi. $p \equiv 6 \pmod 7$ ise $\#E(\mathbb{F}_p) = p - 6 - 7k$

$n = 8$ için, ***i.*** $p \equiv 1 \pmod 8$ ise $\#E(\mathbb{F}_p) = p - 1 - 8k$

ii. $p \equiv 3 \pmod 8$ ise $\#E(\mathbb{F}_p) = p - 3 - 8k$

iii. $p \equiv 5 \pmod 8$ ise $\#E(\mathbb{F}_p) = p - 5 - 8k$

iv. $p \equiv 7 \pmod 8$ ise $\#E(\mathbb{F}_p) = p - 7 - 8k$

$n = 9$ için, ***i.*** $p \equiv 1 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 1 - 9k$

ii. $p \equiv 2 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 2 - 9k$

iii. $p \equiv 4 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 4 - 9k$

iv. $p \equiv 5 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 5 - 9k$

v. $p \equiv 7 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 7 - 9k$

vi. $p \equiv 8 \pmod 9$ ise $\#E(\mathbb{F}_p) = p - 8 - 9k$

$n = 10$ için, ***i.*** $p \equiv 1 \pmod{10}$ ise $\#E(\mathbb{F}_p) = p - 1 - 10k$

ii. $p \equiv 3 \pmod{10}$ ise $\#E(\mathbb{F}_p) = p - 3 - 10k$

iii. $p \equiv 7 \pmod{10}$ ise $\#E(\mathbb{F}_p) = p - 7 - 10k$

iv. $p \equiv 9 \pmod{10}$ ise $\#E(\mathbb{F}_p) = p - 9 - 10k$

n* = 12** için, ***i. $p \equiv 1 \pmod{12}$ ise $\#E(\mathbb{F}_p) = p - 1 - 12k$

ii. $p \equiv 5 \pmod{12}$ ise $\#E(\mathbb{F}_p) = p - 5 - 12k$

iii. $p \equiv 7 \pmod{12}$ ise $\#E(\mathbb{F}_p) = p - 7 - 12k$

iv. $p \equiv 11 \pmod{12}$ ise $\#E(\mathbb{F}_p) = p - 11 - 12k$

sonuçları elde edilmiştir.

Tate normal formdaki eliptik eğrilerin üzerinde bulunan noktalar dikkate alınarak eğrilerin üzerindeki noktaların oluşturduğu grubun mertebeleri MAGMA cebir programı kullanılarak, ekte verilen program yardımıyla, $p < 200$ asalları için elde edilmiştir. Aşağıdaki örnekte $n = 8$ ve $p \leq 47$ için bu durum ele alınmaktadır.

3.2.3 Örnek. $n = 8$ olsun. Bu durumda

$$E: y^2 + \left(1 - \left(\frac{(2\alpha - 1)(\alpha - 1)}{\alpha}\right)\right)xy - (2\alpha - 1)(\alpha - 1)y = x^3 - (2\alpha - 1)(\alpha - 1)x^2$$

Tate normal formdaki eliptik eğrilerin $p \leq 47$ asalları ve $\alpha \in \mathbb{F}_p$ katsayıları için grup mertebeleri aşağıdaki çizelgede verilmiştir. Bu çizelgede E eliptik eğrisinin singüler olması hali "Sin." ile gösterilmiştir ve bu halde nokta sayıları dikkate alınmamıştır.

Çizelge 3.1. Grup mertebeleri

$n = 8$	$p = 3$	$p = 5$	$p = 7$	$P = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	Sin.	8	8	16	16	Sin.	16	24	40	24	40	32	32	48
$\alpha = 3$		Sin.	Sin.	16	16	16	16	32	32	32	32	48	48	48
$\alpha = 4$		8	Sin.	16	16	24	16	24	24	32	48	40	48	48
$\alpha = 5$			Sin.	8	8	16	16	Sin.	32	40	40	48	48	48
$\alpha = 6$			8	Sin.	16	16	24	16	32	32	32	48	32	48
$\alpha = 7$				8	Sin.	16	24	32	32	32	48	32	48	48
$\alpha = 8$				16	16	24	16	16	24	40	40	48	40	40
$\alpha = 9$				16	8	Sin.	16	16	24	32	40	48	48	56
$\alpha = 10$				16	16	24	Sin.	32	32	32	32	32	40	48
$\alpha = 11$					16	16	16	24	32	32	32	48	48	56
$\alpha = 12$					16	16	16	Sin.	32	24	32	32	48	48
$\alpha = 13$						16	24	24	24	32	48	48	48	48
$\alpha = 14$						24	24	32	32	Sin.	48	48	32	Sin.
$\alpha = 15$						16	16	16	Sin.	32	32	Sin.	48	48
$\alpha = 16$						Sin.	16	16	32	Sin.	32	40	40	48
$\alpha = 17$							16	32	24	32	40	32	40	56
$\alpha = 18$							16	16	32	Sin.	32	40	48	40
$\alpha = 19$								Sin.	32	32	Sin.	32	56	48
$\alpha = 20$								24	32	24	32	40	48	40
$\alpha = 21$								32	24	32	40	Sin.	48	48
$\alpha = 22$								24	24	32	32	40	Sin.	48
$\alpha = 23$									32	32	32	32	48	48
$\alpha = 24$									32	40	48	40	48	Sin.
$\alpha = 25$									32	32	48	32	56	48
$\alpha = 26$									24	32	32	40	48	48
$\alpha = 27$									32	40	32	Sin.	40	48
$\alpha = 28$									40	32	32	48	40	40
$\alpha = 29$										32	40	48	48	48
$\alpha = 30$										24	40	32	32	40
$\alpha = 31$											48	48	48	56
$\alpha = 32$											32	32	48	48
$\alpha = 33$											40	48	48	48
$\alpha = 34$											48	48	40	Sin.
$\alpha = 35$											32	32	48	48
$\alpha = 36$											40	48	40	48
$\alpha = 37$												48	48	56
$\alpha = 38$												40	32	48
$\alpha = 39$												48	48	56
$\alpha = 40$												32	48	40
$\alpha = 41$													48	48
$\alpha = 42$													32	48
$\alpha = 43$														48
$\alpha = 44$														48
$\alpha = 45$														48
$\alpha = 46$														48

Yukarıdaki çizelge dikkate alınarak $\boldsymbol{n = 8}$ hali için, $k \in \mathbb{Z}$ olmak üzere, Tate normal formdaki eliptik eğrilerin üzerindeki noktaların oluşturduğu grupların mertebeleri aşağıdaki gibi sınıflandırılır.

Çizelge 3.2. Verilen mertebeye sahip olan eğrilerin sayıları

$n = 8$									
			$p = 73$	$p = 97$	$p = 193$				
	$p \equiv 1 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı			8	$2k$			
		$p - 17$ mertebeli eğrilerin sayısı		8	16	$2k$			
		$p - 9$ mertebeli eğrilerin sayısı	32	12	16	$2k$			
		$p - 1$ mertebeli eğrilerin sayısı	12	48	80	$2k$			
		$p + 7$ mertebeli eğrilerin sayısı	16	8	16	$2k$			
		$p + 15$ mertebeli eğrilerin sayısı	8	16	40	$2k$			
		$p + 23$ mertebeli eğrilerin sayısı			12	$2k$			
			$p = 29$	$p = 53$	$p = 101$	$p = 149$	$p = 173$	$p = 197$	
	$p \equiv 5 \pmod{24}$	$p - 21$ mertebeli eğrilerin sayısı				16	8	24	$2k$
		$p - 13$ mertebeli eğrilerin sayısı		2	8	10	48	8	$2k$
		$p - 5$ mertebeli eğrilerin sayısı	8	24	48	48	32	80	$2k$
		$p + 3$ mertebeli eğrilerin sayısı	16	8	10	8	24	18	$2k$
		$p + 11$ mertebeli eğrilerin sayısı	2	16	24	48	8	24	$2k$
		$p + 19$ mertebeli eğrilerin sayısı			8	16	48	24	$2k$
		$p + 27$ mertebeli eğrilerin sayısı					2	16	$2k$
			$p = 31$	$p = 79$	$p = 103$	$p = 127$	$p = 151$	$p = 199$	
	$p \equiv 7 \pmod{24}$	$p - 23$ mertebeli eğrilerin sayısı					6	24	$2k$
		$p - 15$ mertebeli eğrilerin sayısı		12	8	30	12	16	$2k$
		$p - 7$ mertebeli eğrilerin sayısı	4	10	36	16	48	48	$2k$
		$p + 1$ mertebeli eğrilerin sayısı	18	30	10	30	14	18	$2k$
		$p + 9$ mertebeli eğrilerin sayısı	4	10	36	16	48	48	$2k$
		$p + 17$ mertebeli eğrilerin sayısı		12	8	30	12	16	$2k$
		$p + 25$ mertebeli eğrilerin sayısı					6	24	$2k$
			$p = 59$	$p = 83$	$p = 107$	$p = 131$	$p = 179$		
	$p \equiv 11 \pmod{24}$	$p - 19$ mertebeli eğrilerin sayısı			2	18	30	$2k$	
		$p - 11$ mertebeli eğrilerin sayısı	18	10	42	16	20	$2k$	
		$p - 13$ mertebeli eğrilerin sayısı	8	30	10	30	42	$2k$	
		$p + 5$ mertebeli eğrilerin sayısı	24	10	30	10	14	$2k$	
		$p + 13$ mertebeli eğrilerin sayısı	6	30	14	48	60	$2k$	
		$p + 21$ mertebeli eğrilerin sayısı			6	6	10	$2k$	
			$p = 37$	$p = 61$	$p = 109$	$p = 157$	$p = 181$		
	$p \equiv 13 \pmod{24}$	$p -$ 21 mertebeli eğrilerin sayısı				10	32	$2k$	
		$p - 13$ mertebeli eğrilerin sayısı		8	32	32	16	$2k$	
		$p - 5$ mertebeli eğrilerin sayısı	16	8	10	8	24	$2k$	
		$p + 3$ mertebeli eğrilerin sayısı	10	32	32	64	24	$2k$	

Çizelge 3.2. Verilen mertebeye sahip olan eğrilerin sayıları (devam)

		$p+11$ mertebeli eğrilerin sayısı	8	10	16	16	64	$2k$
		$p+19$ mertebeli eğrilerin sayısı			16	24	10	$2k$
		$p+27$ mertebeli eğrilerin sayısı					8	$2k$
			$p=41$	$p=89$	$p=113$	$p=137$		
	$p \equiv 17 \pmod{24}$	$p-17$ mertebeli eğrilerin sayısı		4	24	16	$2k$	
		$p-9$ mertebeli eğrilerin sayısı	12	16	8	48	$2k$	
		$p-1$ mertebeli eğrilerin sayısı	8	8	16	16	$2k$	
		$p+7$ mertebeli eğrilerin sayısı	16	48	24	32	$2k$	
		$p+15$ mertebeli eğrilerin sayısı		8	36	8	$2k$	
		$p+23$ mertebeli eğrilerin sayısı				12	$2k$	
			$p=43$	$p=67$	$p=139$	$p=163$		
	$p \equiv 19 \pmod{24}$	$p-19$ mertebeli eğrilerin sayısı			8	30	$2k$	
		$p-11$ mertebeli eğrilerin sayısı	6	6	30	10	$2k$	
		$p-3$ mertebeli eğrilerin sayısı	8	30	16	60	$2k$	
		$p+5$ mertebeli eğrilerin sayısı	24	10	48	20	$2k$	
		$p+13$ mertebeli eğrilerin sayısı	2	18	10	30	$2k$	
		$p+21$ mertebeli eğrilerin sayısı			24	10	$2k$	
			$p=23$	$p=47$	$p=71$	$p=167$	$p=191$	
	$p \equiv 23 \pmod{24}$	$p-23$ mertebeli eğrilerin sayısı				18	10	$2k$
		$p-15$ mertebeli eğrilerin sayısı			2	10	30	$2k$
		$p-7$ mertebeli eğrilerin sayısı	6	6	24	42	14	$2k$
		$p+1$ mertebeli eğrilerin sayısı	6	30	14	22	78	$2k$
		$p+9$ mertebeli eğrilerin sayısı	6	6	24	42	14	$2k$
		$p+17$ mertebeli eğrilerin sayısı			2	10	30	$2k$
		$p+25$ mertebeli eğrilerin sayısı				18	10	$2k$

3.3 Tate Normal Formdaki Eliptik Eğriler Üzerindeki Noktaların Oluşturduğu Grupların Yapısı

Tate normal formdaki eliptik eğrilerin üzerinde bulunan noktaların mertebeleri MAGMA cebir programı kullanılarak, ekte verilen program yardımıyla, $p < 200$ asalları için elde edilmiştir. Bu şekilde noktaların mertebeleri ve bu noktaların oluşturduğu grubun mertebesi dikkate alınarak bu grupların grup yapıları belirlenmiştir. Aşağıdaki örnekte, bir uygulama olarak, $\boldsymbol{n = 8}$ hali için Tate normal formdaki eliptik eğrilerin üzerindeki noktaların oluşturduğu grupların yapısı verilmiştir.

3.3.1 Örnek. *n* = 8 olsun. Bu durumda

$$y^2 + \left(1 - \left(\frac{(2\alpha - 1)(\alpha - 1)}{\alpha}\right)\right)xy - (2\alpha - 1)(\alpha - 1)y = x^3 - (2\alpha - 1)(\alpha - 1)x^2$$

Tate normal formdaki eliptik eğrilerin üzerindeki noktaların oluşturduğu grupların yapısı $p \leq 47$ asalları ve $\alpha \in \mathbb{F}_p$ katsayıları için aşağıdaki çizelgede verilmiştir.

Çizelge 3.3. Grup yapıları

$n = 8$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler	Singüler
$\alpha = 2$	Singüler	C_8	C_8	C_{16}	$C_2 \times C_8$	Singüler	$C_2 \times C_8$	C_{24}	C_{40}	C_{24}	C_{40}	C_{32}	$C_2 \times C_{16}$	$C_2 \times C_{24}$
$\alpha = 3$		Singüler	Singüler	$C_2 \times C_8$	$C_2 \times C_8$	$C_2 \times C_8$	$C_2 \times C_8$	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_2 \times C_{24}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 4$		C_8	Singüler	$C_2 \times C_8$	C_{16}	C_{24}	C_{16}	C_{24}	C_{24}	$C_2 \times C_{16}$	C_{48}	C_{40}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 5$			Singüler	C_8	C_8	$C_2 \times C_8$	$C_2 \times C_8$	Singüler	$C_4 \times C_8$	C_{40}	C_{40}	C_{48}	C_{48}	C_{48}
$\alpha = 6$			C_8	Singüler	C_{16}	C_{16}	C_{24}	C_{16}	$C_2 \times C_{16}$	C_{32}	C_{32}	$C_2 \times C_{24}$	C_{32}	$C_2 \times C_{24}$
$\alpha = 7$				C_8	Singüler	C_{16}	C_{24}	C_{32}	C_{32}	C_{32}	$C_2 \times C_{24}$	$C_2 \times C_{16}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 8$				$C_2 \times C_8$	C_{16}	C_{24}	C_{16}	$C_2 \times C_8$	C_{24}	C_{40}	C_{40}	$C_2 \times C_{24}$	C_{40}	C_{40}
$\alpha = 9$				$C_2 \times C_8$	C_8	Singüler	$C_2 \times C_8$	$C_2 \times C_8$	C_{24}	$C_2 \times C_{16}$	C_{40}	C_{48}	C_{48}	C_{56}
$\alpha = 10$				C_{16}	C_{16}	C_{24}	Singüler	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_2 \times C_{16}$	C_{32}	C_{32}	C_{40}	$C_2 \times C_{24}$
$\alpha = 11$					$C_2 \times C_8$	C_{16}	$C_2 \times C_8$	C_{24}	C_{32}	C_{32}	$C_2 \times C_{16}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$	C_{56}
$\alpha = 12$					$C_2 \times C_8$	C_{16}	C_{16}	Singüler	$C_2 \times C_{16}$	C_{24}	$C_2 \times C_{16}$	$C_2 \times C_{16}$	$C_2 \times C_{24}$	C_{48}
$\alpha = 13$						$C_2 \times C_8$	C_{24}	C_{24}	C_{24}	$C_2 \times C_{16}$	$C_2 \times C_{24}$	C_{48}	C_{48}	$C_2 \times C_{24}$
$\alpha = 14$						C_{24}	C_{24}	$C_2 \times C_{16}$	$C_4 \times C_8$	Singüler	C_{48}	C_{48}	$C_2 \times C_{16}$	Singüler
$\alpha = 15$						$C_2 \times C_8$	$C_2 \times C_8$	$C_2 \times C_8$	Singüler	$C_2 \times C_{16}$	$C_4 \times C_8$	Singüler	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 16$						Singüler	C_{16}	$C_2 \times C_8$	$C_4 \times C_8$	Singüler	$C_4 \times C_8$	C_{40}	C_{40}	C_{48}
$\alpha = 17$							$C_2 \times C_8$	C_{32}	C_{24}	$C_2 \times C_{16}$	C_{40}	$C_4 \times C_8$	C_{40}	C_{56}
$\alpha = 18$							$C_2 \times C_8$	C_{16}	$C_2 \times C_{16}$	Singüler	$C_4 \times C_8$	C_{40}	$C_2 \times C_{24}$	C_{40}
$\alpha = 19$								Singüler	C_{32}	$C_2 \times C_{16}$	Singüler	$C_4 \times C_8$	C_{56}	C_{48}
$\alpha = 20$								C_{24}	$C_4 \times C_8$	C_{24}	$C_4 \times C_8$	C_{40}	$C_2 \times C_{24}$	C_{40}
$\alpha = 21$								$C_2 \times C_{16}$	C_{24}	C_{32}	C_{40}	Singüler	C_{48}	$C_2 \times C_{24}$
$\alpha = 22$								C_{24}	C_{24}	$C_2 \times C_{16}$	$C_4 \times C_8$	C_{40}	Singüler	C_{48}
$\alpha = 23$									C_{32}	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_4 \times C_8$	C_{48}	$C_2 \times C_{24}$
$\alpha = 24$									$C_2 \times C_{16}$	C_{40}	C_{48}	C_{40}	$C_2 \times C_{24}$	Singüler
$\alpha = 25$									$C_4 \times C_8$	C_{32}	$C_2 \times C_{24}$	$C_4 \times C_8$	C_{56}	$C_2 \times C_{24}$
$\alpha = 26$									C_{24}	C_{32}	$C_2 \times C_{16}$	C_{40}	$C_2 \times C_{24}$	C_{48}
$\alpha = 27$									$C_4 \times C_8$	C_{40}	$C_2 \times C_{16}$	Singüler	C_{40}	$C_2 \times C_{24}$
$\alpha = 28$									C_{40}	$C_2 \times C_{16}$	C_{32}	C_{48}	C_{40}	C_{40}
$\alpha = 29$										$C_2 \times C_{16}$	C_{40}	C_{48}	$C_2 \times C_{24}$	C_{48}
$\alpha = 30$										C_{24}	C_{40}	$C_2 \times C_{16}$	$C_2 \times C_{16}$	C_{40}
$\alpha = 31$											$C_2 \times C_{24}$	$C_2 \times C_{24}$	C_{48}	C_{56}
$\alpha = 32$											C_{32}	C_{32}	$C_2 \times C_{24}$	C_{48}
$\alpha = 33$											C_{40}	C_{48}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 34$											C_{48}	$C_2 \times C_{24}$	C_{40}	Singüler
$\alpha = 35$											$C_4 \times C_8$	$C_2 \times C_{16}$	C_{48}	$C_2 \times C_{24}$
$\alpha = 36$											C_{40}	$C_2 \times C_{24}$	C_{40}	C_{48}
$\alpha = 37$												C_{48}	$C_2 \times C_{24}$	C_{56}
$\alpha = 38$												C_{40}	C_{32}	$C_2 \times C_{24}$
$\alpha = 39$												$C_2 \times C_{24}$	C_{48}	C_{56}
$\alpha = 40$												C_{32}	$C_2 \times C_{24}$	C_{40}
$\alpha = 41$													$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 42$													$C_2 \times C_{16}$	$C_2 \times C_{24}$
$\alpha = 43$														C_{48}
$\alpha = 44$														$C_2 \times C_{24}$
$\alpha = 45$														$C_2 \times C_{24}$
$\alpha = 46$														$C_2 \times C_{24}$

3.3.2 Uyarı. Teorem 2.6.8 in sonucu olarak ve yukarıdaki grup yapısı tablosu dikkate alınarak belirlenen $C_n \times C_n$ grup yapılarının görüldüğü asallar aşağıdaki gibidir.

1. $n = 4$ için, $13 = 4^2 - 4 + 1 = n^2 - n + 1$ ve $17 = 4^2 + 1 = n^2 + 1$ olduğundan

$$E(\mathbb{F}_{13}) \cong C_4 \times C_4 \text{ ve } E(\mathbb{F}_{17}) \cong C_4 \times C_4,$$

2. $n = 5$ için, $31 = 5^2 + 5 + 1 = n^2 + n + 1$ olduğundan

$$E(\mathbb{F}_{31}) \cong C_5 \times C_5,$$

3. $n = 6$ için, $31 = 6^2 - 6 + 1 = n^2 - n + 1$, $37 = 6^2 + 1 = n^2 + 1$ ve $43 = 6^2 + 6 + 1 = n^2 + n + 1$ olduğundan

$$E(\mathbb{F}_{31}) \cong C_6 \times C_6, E(\mathbb{F}_{37}) \cong C_6 \times C_6, E(\mathbb{F}_{43}) \cong C_6 \times C_6,$$

4. $n = 7$ için, $43 = 7^2 - 7 + 1 = n^2 - n + 1$ olduğundan

$$E(\mathbb{F}_{43}) \cong C_7 \times C_7,$$

5. $n = 8$ için, $73 = 8^2 + 8 + 1 = n^2 + n + 1$ olduğundan

$$E(\mathbb{F}_{73}) \cong C_8 \times C_8,$$

6. $n = 9$ için, $73 = 9^2 - 9 + 1 = n^2 - n + 1$ olduğundan

$$E(\mathbb{F}_{73}) \cong C_9 \times C_9,$$

7. $n = 10$ için, $101 = 10^2 + 1$ olduğundan

$$E(\mathbb{F}_{101}) \cong C_{10} \times C_{10},$$

8. $n = 12$ için, $157 = 12^2 + 12 + 1$ olduğundan

$$E(\mathbb{F}_{157}) \cong C_{12} \times C_{12}$$

dir.

KAYNAKLAR

Artin, E. 1921. Quadratische Körper im Gebiete der höheren Kongruenzen. *Ph.D. Thesis*, University of Leipzig, Germany.

Bosma, W., Cannon, J., Playoust, C. 1997. The Magma algebra system. I. The user language. *J. Symbolic Comput.*. 24(3-4): 235-265. http://magma.maths.usyd.edu.au/calc/

Fraleigh, J. B. 1982. A First Course In Abstract Algebra. Addison Wesley P.C., USA, 478 pp.

Garcia, I., Olalla, A. M., Tornero, J. M. 2002. Computing the Rational torsion of elliptic curve using Tate normal form. *Journal of Number Theory*, 96(1):76-88.

Husemöller, D. 2004. Elliptic Curves. Springer, Germany, 487 pp.

Mollin, R. A. 2000. Fundamental Number Theory with Applications, Chapman&Hall / CRC, USA, 439 pp.

Namlı, D. 2001. Kübik Rezidüler, Doktora Tezi, Balıkesir Üniversitesi (yayımlanmamış), Balıkesir Üniversitesi.

Silverman, J. H. 1986. The Arithmetic of Elliptic Curves. Springer-Verlag, USA, 402 pp.

Silverman, J.H. 2006. A Friendly Introduction to Number Theory. PrenticeHall, USA, 434 pp.

Silverman, J. H., Tate, J. 1992. Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics. Springer, USA, 283 pp.

Schmitt, S., Zimmer, H. G. 2003. Elliptic Curves, Graduate Texts in Mathematics. Walter de Gruyter, Germany, 367 pp.

Washington, J., L. 2003, Elliptic curves, Number Theory and Cryptography. Chapman &Hall/CRC, Florida, USA, 429 pp.

EKLER

EK 1 Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların MAPLE12 Programı İle Bulunması

EK 2 Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların Sayısının MAGMA Cebir Programı İle Bulunması

EK 3 Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların Mertebesinin MAGMA Cebir Programı İle Bulunması

EK 4 Tate Normal Formdaki Eliptik Eğrilerin $p \leq 47$ Asalları İçin Grup Mertebeleri

EK 5 Tate Normal Formdaki Eliptik Eğrilerin $p < 200$ Asalları İçin Grup Mertebelerine Göre Sınıflandırılması

EK 6 Tate Normal Formdaki Eliptik Eğrilerin $p \leq 47$ Asalları İçin Grup Yapıları

EK 1.

Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların MAPLE12 Programı İle Bulunması

```
> restart;
> p:=7;
```

$$p := 7$$

```
> c:=((3*alpha^2-3*alpha+1)*(alpha-2*alpha^2))/(alpha-1)^3;
```

$$c := \frac{\left(3\,\alpha^2 - 3\,\alpha + 1\right)\left(\alpha - 2\,\alpha^2\right)}{\left(\alpha - 1\right)^3}$$

```
> b:=c*((2*alpha-2*alpha^2-1)/(alpha-1));
```

$$b := \frac{\left(3\,\alpha^2 - 3\,\alpha + 1\right)\left(\alpha - 2\,\alpha^2\right)\left(2\,\alpha - 2\,\alpha^2 - 1\right)}{\left(\alpha - 1\right)^4}$$

```
> for alpha from 2 to p-1 do
for x from 0 to p-1 do
print("alpha"=alpha, "x"=x, "y"=Roots(y^2+(1-c)*x*y-b*y-x^3+b*x^2) mod p);
> end do;
> end do;
```

"alpha"= 2, "x"= 0, "y"= [[0, 2]]

"alpha"= 2, "x"= 1, "y"= [ ]

"alpha"= 2, "x"= 2, "y"= [[2, 1], [3, 1]]

"alpha"= 2, "x"= 3, "y"= [ ]

"alpha"= 2, "x"= 4, "y"= [ ]

"alpha"= 2, "x"= 5, "y"= [[1, 2]]

"alpha"= 2, "x"= 6, "y"= [[3, 1], [5, 1]]

"alpha"= 3, "x"= 0, "y"= [[0, 1], [1, 1]]

"alpha"= 3, "x"= 1, "y"= [[0, 1], [2, 1]]

"alpha"= 3, "x"= 2, "y"= [[4, 1], [6, 1]]

"alpha"= 3, "x"= 3, "y"= [[1, 1], [3, 1]]

"alpha"= 3, "x"= 4, "y"= [[6, 2]]

"alpha"= 3, "x"= 5, "y"= [[1, 1], [5, 1]]

"alpha"= 3, "x"= 6, "y"= [ ]

"alpha"= 4, "x"= 0, "y"= [[0, 2]]

"alpha"= 4, "x"= 1, "y"= [ ]

"alpha"= 4, "x"= 2, "y"= [[2, 1], [3, 1]]

"alpha"= 4, "x"= 3, "y"= [ ]

"alpha"= 4, "x"= 4, "y"= [ ]

"alpha"= 4, "x"= 5, "y"= [[1, 2]]

"alpha"= 4, "x"= 6, "y"= [[3, 1], [5, 1]]

"alpha"= 5, "x"= 0, "y"= [[0, 1], [5, 1]]

"alpha"= 5, "x"= 1, "y"= [[5, 2]]

"alpha"= 5, "x"= 2, "y"= [[2, 1], [6, 1]]

"alpha"= 5, "x"= 3, "y"= [ ]

"alpha"= 5, "x"= 4, "y"= [[5, 1], [6, 1]]

"alpha"= 5, "x"= 5, "y"= [[0, 1], [2, 1]]

"alpha"= 5, "x"= 6, "y"= [[1, 1], [6, 1]]

"alpha"= 6, "x"= 0, "y"= [[0, 2]]

"alpha"= 6, "x"= 1, "y"= [ ]

"alpha"= 6, "x"= 2, "y"= [[2, 1], [3, 1]]

"alpha"= 6, "x"= 3, "y"= [ ]

"alpha"= 6, "x"= 4, "y"= [ ]

"alpha"= 6, "x"= 5, "y"= [[1, 2]]

"alpha"= 6, "x"= 6, "y"= [[3, 1], [5, 1]]

EK 2.

Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların Sayısının MAGMA Cebir Programı İle Bulunması

```
B:=[2..200];
A:=[a : a in B | IsPrime(a) ];
L:=[];
for p in A do;
 D:=[1..p-1];
 for m in D do;
 b:=m;
 c:=0;
   a:=((1-c)^4)*b^3-((1-c)^3)*b^3-8*((1-c)^2)*b^4+36*(1-c)*b^4-27*b^4+16*b^5;
   if a mod p ne 0 then
    E:=EllipticCurve([GF(p) | 1-c,-b,-b,0,0]);
    Append(~L,<p,m,#E>);
   end if;
 end for;
end for;
PrintFile("C:\\Users\\DELL\\nesittir4.txt",L);
```

EK 3.

Tate Normal Formda Verilen Eliptik Eğri Üzerindeki Noktaların Mertebesinin MAGMA Cebir Programı İle Bulunması

```
B:=[2..200];
A:=[a : a in B | IsPrime(a) ];
L:=[];
for p in A do;
 D:=[1..p-1];
 for m in D do;
  b:=m;
  c:=0;
  a:=((1-c)^4)*b^3-((1-c)^3)*b^3-8*((1-c)^2)*b^4+36*(1-c)*b^4-27*b^4\
+16*b^5;
  if a mod p ne 0 then
   E:=EllipticCurve([GF(p) | 1-c,-b,-b,0,0]);
   R:=RationalPoints(E);
   for k in R do;
    Append(~L,<p,m,Order(k)>);
   end for;
  end if;
 end for;
end for;
PrintFile("C:\\Users\\DELL\\mertebe4.txt",L);
```

EK 4.

Tate Normal Formdaki Eliptik Eğrilerin $p \leq 47$ Asalları İçin Grup Mertebeleri

$n=4$	$p=3$	$p=5$	$p=7$	$P=11$	$p=13$	$p=17$	$p=19$	$p=23$	$p=29$	$p=31$	$p=37$	$p=41$	$p=43$	$p=47$
$a=1$	4	8	4	12	16	Sin.	24	20	24	28	40	48	40	48
$a=2$	Sin.	4	12	Sin.	20	16	16	20	24	32	32	48	40	60
$a=3$		8	Sin.	8	16	24	16	24	32	32	32	40	48	48
$a=4$		Sin.	8	12	Sin.	16	28	28	32	36	32	32	44	40
$a=5$			8	16	16	16	16	24	32	32	48	32	40	40
$a=6$			8	8	12	12	20	20	32	40	44	36	48	56
$a=7$				16	16	20	20	24	24	32	40	48	48	52
$a=8$				8	8	24	24	28	24	40	36	40	Sin.	44
$a=9$				12	8	16	12	28	Sin.	28	32	40	48	48
$a=10$				16	16	24	24	Sin.	32	28	40	48	52	40
$a=11$					12	20	24	24	28	40	32	36	52	48
$a=12$					16	12	16	32	36	24	40	36	40	44
$a=13$						16	Sin.	24	32	40	36	48	52	48
$a=14$						16	24	32	24	40	40	40	56	56
$a=15$						24	24	24	24	24	36	40	36	40
$a=16$						16	20	16	32	24	40	48	44	60
$a=17$							16	32	36	40	36	36	48	60
$a=18$							16	24	40	24	40	32	32	48
$a=19$								16	20	36	32	32	48	56
$a=20$								24	40	36	40	40	48	48
$a=21$								16	36	24	32	48	48	40
$a=22$								24	32	32	36	48	40	48
$a=23$									24	24	40	Sin.	32	56
$a=24$									24	32	44	32	40	48
$a=25$									32	28	48	48	40	40
$a=26$									36	32	32	44	48	48
$a=27$									28	32	32	48	48	36
$a=28$									32	36	32	40	56	36
$a=29$										Sin.	40	44	48	56
$a=30$										32	Sin.	52	40	40
$a=31$											48	48	40	48
$a=32$											28	32	40	52
$a=33$											48	48	56	48
$a=34$											48	52	40	56
$a=35$											28	44	44	48
$a=36$											48	40	52	52
$a=37$												48	32	44
$a=38$												44	36	40
$a=39$												48	48	56
$a=40$												32	36	56
$a=41$													36	48
$a=42$													40	36
$a=43$														48
$a=44$														Sin.
$a=45$														56
$a=46$														40

$n = 5$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$a = 1$	5	5	10	Sin.	10	20	20	25	30	25	35	50	50	40
$a = 2$	5	10	5	10	15	15	Sin.	25	35	40	40	50	40	40
$a = 3$		Sin.	5	10	15	20	25	30	20	35	40	50	45	50
$a = 4$		5	10	15	15	10	20	20	Sin.	35	30	40	55	35
$a = 5$			10	10	20	25	25	20	30	Sin.	45	45	35	50
$a = 6$			10	15	15	15	25	20	30	Sin.	40	40	50	55
$a = 7$				10	10	20	15	15	Sin.	40	30	45	50	55
$a = 8$				15	10	15	15	30	30	30	40	45	40	60
$a = 9$				15	20	15	Sin.	20	40	30	30	50	45	45
$a = 10$				Sin.	20	25	15	30	25	35	35	40	40	50
$a = 11$					10	20	20	25	30	25	35	50	50	40
$a = 12$					10	20	20	30	20	40	40	40	40	50
$a = 13$						20	20	15	25	30	30	30	45	40
$a = 14$						15	20	20	35	25	40	Sin.	45	50
$a = 15$						15	25	30	30	40	35	40	55	40
$a = 16$						20	20	30	40	30	40	40	40	45
$a = 17$							15	20	40	40	30	40	35	40
$a = 18$							20	20	30	40	40	40	40	40
$a = 19$								20	20	30	40	35	45	60
$a = 20$								30	25	40	45	50	55	55
$a = 21$								30	30	25	30	45	40	45
$a = 22$								25	35	40	45	30	40	60
$a = 23$									30	35	40	40	45	40
$a = 24$									30	30	45	45	35	60
$a = 25$									35	25	45	40	40	40
$a = 26$									25	25	40	50	40	45
$a = 27$									30	30	40	50	50	45
$a = 28$									30	25	30	35	45	50
$a = 29$										30	40	45	45	40
$a = 30$										25	40	40	40	55
$a = 31$											50	35	40	50
$a = 32$											35	50	55	60
$a = 33$											30	30	45	45
$a = 34$											45	40	35	40
$a = 35$											40	45	50	35
$a = 36$											35	30	40	55
$a = 37$												35	40	45
$a = 38$												Sin.	40	45
$a = 39$												45	50	55
$a = 40$												50	45	45
$a = 41$													40	60
$a = 42$													50	60
$a = 43$														50
$a = 44$														45
$a = 45$														60
$a = 46$														40

$n = 6$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	6	Sin.	6	12	12	24	24	18	24	36	36	36	54	54
$\alpha = 2$	Sin.	6	12	12	18	12	Sin.	30	24	30	42	36	48	42
$\alpha = 3$		6	Sin.	18	12	18	24	30	24	24	36	30	48	36
$\alpha = 4$		Sin.	6	12	12	12	18	24	24	42	Sin.	48	48	54
$\alpha = 5$			12	12	12	12	18	Sin.	24	36	30	36	36	36
$\alpha = 6$			Sin.	Sin.	18	18	12	18	24	36	30	36	48	36
$\alpha = 7$				12	18	12	18	24	36	36	36	36	36	60
$\alpha = 8$				12	18	12	24	24	30	30	36	36	48	54
$\alpha = 9$				6	12	24	18	18	24	36	36	Sin.	54	48
$\alpha = 10$				Sin.	Sin.	24	24	24	30	36	36	48	42	48
$\alpha = 11$					12	18	18	24	30	24	36	42	42	48
$\alpha = 12$					Sin.	18	24	18	24	36	48	36	48	60
$\alpha = 13$						24	12	30	36	24	42	42	54	48
$\alpha = 14$						24	24	24	36	24	30	42	36	48
$\alpha = 15$						Sin.	24	24	24	36	36	42	42	48
$\alpha = 16$						Sin.	18	24	Sin.	24	36	48	36	48
$\alpha = 17$							24	24	30	36	36	48	54	42
$\alpha = 18$							Sin.	30	36	36	36	48	48	48
$\alpha = 19$								24	30	30	48	48	Sin.	48
$\alpha = 20$								24	36	36	36	36	48	36
$\alpha = 21$								24	36	36	36	36	36	42
$\alpha = 22$								Sin.	36	24	36	54	36	48
$\alpha = 23$									24	24	36	48	36	60
$\alpha = 24$									36	Sin.	30	42	54	54
$\alpha = 25$									36	42	48	48	54	48
$\alpha = 26$									36	24	36	36	48	Sin.
$\alpha = 27$									30	36	48	42	48	60
$\alpha = 28$									Sin.	30	36	48	36	54
$\alpha = 29$										36	48	42	36	48
$\alpha = 30$										Sin.	48	48	48	36
$\alpha = 31$											42	48	36	48
$\alpha = 32$											36	48	48	42
$\alpha = 33$											36	48	48	48
$\alpha = 34$											36	42	48	54
$\alpha = 35$											42	30	48	48
$\alpha = 36$											Sin.	36	42	42
$\alpha = 37$												36	36	36
$\alpha = 38$												54	36	48
$\alpha = 39$												36	36	48
$\alpha = 40$												Sin.	48	48
$\alpha = 41$													36	60
$\alpha = 42$													Sin.	42
$\alpha = 43$														60
$\alpha = 44$														48
$\alpha = 45$														48
$\alpha = 46$														Sin.

$n = 7$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$P = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	7	7	7	14	Sin.	21	14	28	28	28	35	42	49	35
$\alpha = 3$		7	7	14	14	21	21	28	Sin.	28	35	49	35	49
$\alpha = 4$		7	7	7	21	14	21	28	35	42	28	42	Sin.	49
$\alpha = 5$			Sin.	14	14	14	14	21	21	28	42	35	49	56
$\alpha = 6$			7	14	14	14	21	21	28	21	49	Sin.	49	56
$\alpha = 7$				7	Sin.	21	21	21	21	28	49	42	49	56
$\alpha = 8$				14	14	21	28	28	35	35	28	Sin.	49	42
$\alpha = 9$				7	14	21	21	21	28	28	42	35	42	42
$\alpha = 10$				14	7	14	14	21	35	42	28	35	49	56
$\alpha = 11$					14	14	28	28	28	28	28	42	42	42
$\alpha = 12$					Sin.	21	21	28	21	42	28	42	42	56
$\alpha = 13$						21	28	28	21	28	35	35	35	56
$\alpha = 14$						21	14	21	Sin.	42	28	42	Sin.	42
$\alpha = 15$						14	21	28	28	28	42	42	35	56
$\alpha = 16$						21	14	28	35	28	35	49	42	42
$\alpha = 17$							28	21	28	35	28	35	49	56
$\alpha = 18$							14	28	28	28	35	42	49	42
$\alpha = 19$								21	35	42	35	42	49	56
$\alpha = 20$								21	Sin.	28	42	49	42	42
$\alpha = 21$								28	21	35	28	42	35	56
$\alpha = 22$								28	28	35	49	42	49	42
$\alpha = 23$									28	28	42	35	42	49
$\alpha = 24$									21	42	28	49	56	35
$\alpha = 25$									28	28	42	42	35	42
$\alpha = 26$									28	28	42	42	42	56
$\alpha = 27$									35	28	49	42	56	42
$\alpha = 28$									28	35	42	49	56	56
$\alpha = 29$										35	42	42	42	56
$\alpha = 30$										28	28	49	42	42
$\alpha = 31$											35	42	49	49
$\alpha = 32$											35	42	49	49
$\alpha = 33$											42	42	Sin.	42
$\alpha = 34$											42	42	35	42
$\alpha = 35$											42	Sin.	56	56
$\alpha = 36$											35	42	56	49
$\alpha = 37$												42	49	42
$\alpha = 38$												42	56	42
$\alpha = 39$												42	42	56
$\alpha = 40$												42	42	56
$\alpha = 41$													42	42
$\alpha = 42$													49	42
$\alpha = 43$														56
$\alpha = 44$														56
$\alpha = 45$														42
$\alpha = 46$														35

$n = 9$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	Sin.	9	9	9	18	18	18	18	36	27	36	36	54	54
$\alpha = 3$		9	Sin.	9	9	Sin.	18	18	36	36	27	54	45	36
$\alpha = 4$		9	9	18	Sin.	18	Sin.	27	36	36	45	54	36	54
$\alpha = 5$			Sin.	9	9	18	27	18	36	36	36	45	45	45
$\alpha = 6$			9	9	9	18	Sin.	27	27	Sin.	36	36	45	36
$\alpha = 7$				18	18	18	18	27	36	36	36	36	Sin.	36
$\alpha = 8$				9	18	Sin.	Sin.	18	36	27	36	36	45	54
$\alpha = 9$				18	18	18	18	27	36	27	36	45	36	54
$\alpha = 10$				9	Sin.	18	18	18	36	36	45	45	54	45
$\alpha = 11$					18	18	27	18	27	36	Sin.	54	36	36
$\alpha = 12$					18	Sin.	Sin.	18	27	27	45	45	54	45
$\alpha = 13$						18	27	18	27	27	27	36	54	54
$\alpha = 14$						18	27	27	36	27	45	45	36	36
$\alpha = 15$						18	Sin.	27	36	36	27	36	45	45
$\alpha = 16$						18	27	18	36	27	36	36	36	54
$\alpha = 17$							27	18	36	36	45	36	45	45
$\alpha = 18$							18	27	36	27	27	45	45	36
$\alpha = 19$								27	36	27	36	45	54	54
$\alpha = 20$								27	36	27	Sin.	54	36	54
$\alpha = 21$								18	27	36	36	36	45	36
$\alpha = 22$								18	27	27	36	45	54	45
$\alpha = 23$									27	36	36	36	36	36
$\alpha = 24$									36	36	36	36	54	54
$\alpha = 25$									27	27	Sin.	45	54	54
$\alpha = 26$									27	Sin.	36	45	54	45
$\alpha = 27$									36	27	Sin.	54	45	54
$\alpha = 28$									36	27	36	54	54	36
$\alpha = 29$										36	27	45	36	45
$\alpha = 30$										27	45	36	36	45
$\alpha = 31$											36	36	54	54
$\alpha = 32$											36	36	45	36
$\alpha = 33$											27	36	36	45
$\alpha = 34$											36	36	54	45
$\alpha = 35$											Sin.	36	54	45
$\alpha = 36$											36	36	45	54
$\alpha = 37$												36	Sin.	45
$\alpha = 38$												36	45	45
$\alpha = 39$												45	54	36
$\alpha = 40$												36	36	36
$\alpha = 41$													36	54
$\alpha = 42$													54	54
$\alpha = 43$														54
$\alpha = 44$														45
$\alpha = 45$														54
$\alpha = 46$														54

$n = 10$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$P = 43$	$P = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	Sin.	10	10	Sin.	10	20	20	30	20	40	40	40	40	50
$\alpha = 3$		Sin.	10	10	10	20	20	20	Sin.	30	40	50	40	40
$\alpha = 4$		T. D	Sin.	Sin.	10	20	20	30	30	30	30	40	40	40
$\alpha = 5$			10	T. D	20	20	20	20	30	30	30	50	50	40
$\alpha = 6$			10	Sin.	10	20	T. D	20	40	30	30	40	40	40
$\alpha = 7$				10	Sin.	10	20	30	T. D	40	40	40	40	60
$\alpha = 8$				10	20	20	20	30	20	40	40	T. D	40	50
$\alpha = 9$				T. D	10	Sin.	20	20	20	40	40	50	40	40
$\alpha = 10$				10	20	20	Sin.	20	20	40	40	50	50	50
$\alpha = 11$					20	20	20	30	40	40	30	40	40	60
$\alpha = 12$					20	20	Sin.	Sin.	Sin.	40	30	40	40	40
$\alpha = 13$						20	20	20	40	40	40	40	40	50
$\alpha = 14$						20	20	20	20	T. D	40	40	50	40
$\alpha = 15$						20	20	20	Sin.	40	40	30	40	40
$\alpha = 16$						20	T. D	20	30	Sin.	40	30	50	50
$\alpha = 17$							Sin.	20	30	40	40	40	40	40
$\alpha = 18$							20	30	30	40	40	40	50	60
$\alpha = 19$								30	30	30	Sin.	30	40	40
$\alpha = 20$								20	30	T. D	40	40	40	60
$\alpha = 21$								30	40	40	30	Sin.	40	60
$\alpha = 22$								20	30	Sin.	50	40	Sin.	40
$\alpha = 23$									30	30	30	50	40	50
$\alpha = 24$									30	40	30	Sin.	50	Sin.
$\alpha = 25$									T. D	Sin.	40	50	40	40
$\alpha = 26$									40	40	40	50	40	60
$\alpha = 27$									30	30	40	50	40	60
$\alpha = 28$									30	30	40	40	40	60
$\alpha = 29$										40	40	40	40	60
$\alpha = 30$										40	40	40	40	40
$\alpha = 31$											40	40	50	60
$\alpha = 32$											40	40	40	40
$\alpha = 33$											40	30	40	60
$\alpha = 34$											40	40	40	40
$\alpha = 35$											40	50	40	40
$\alpha = 36$											40	T. D	40	50
$\alpha = 37$												50	40	40
$\alpha = 38$												Sin.	50	40
$\alpha = 39$												40	40	40
$\alpha = 40$												40	40	40
$\alpha = 41$													40	40
$\alpha = 42$													40	40
$\alpha = 43$														60
$\alpha = 44$														40
$\alpha = 45$														50
$\alpha = 46$														40

$n = 12$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$P = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$P = 37$	$P = 41$	$P = 43$	$p = 47$
$\alpha = 1$	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D
$\alpha = 2$	Sin.	Sin.	Sin.	12	Sin.	12	24	24	24	36	48	36	36	48
$\alpha = 3$		Sin.	12	12	Sin.	12	Sin.	24	36	24	Sin.	48	48	48
$\alpha = 4$		Sin.	Sin.	12	12	24	24	24	24	36	Sin.	48	36	60
$\alpha = 5$			12	Sin.	12	24	12	24	36	24	48	Sin.	48	48
$\alpha = 6$			Sin.	Sin.	Sin.	24	24	24	24	24	36	36	36	60
$\alpha = 7$				Sin.	Sin.	Sin.	24	Sin.	24	36	36	48	48	48
$\alpha = 8$				12	Sin.	24	24	24	24	36	36	48	36	60
$\alpha = 9$				12	12	Sin.	24	24	Sin.	Sin.	48	36	36	48
$\alpha = 10$				12	12	24	Sin.	24	24	24	48	48	48	48
$\alpha = 11$					Sin.	Sin.	24	24	36	24	36	48	48	36
$\alpha = 12$					Sin.	24	24	Sin.	24	36	48	48	48	48
$\alpha = 13$						24	24	24	24	36	36	48	48	48
$\alpha = 14$						24	24	24	36	24	48	36	36	48
$\alpha = 15$						12	12	24	Sin.	36	36	48	48	48
$\alpha = 16$						12	24	24	36	Sin.	Sin.	48	48	48
$\alpha = 17$							Sin.	Sin.	24	36	36	48	Sin.	36
$\alpha = 18$							24	24	24	24	36	48	48	48
$\alpha = 19$								24	36	36	Sin.	48	36	48
$\alpha = 20$								24	24	36	36	48	48	48
$\alpha = 21$								24	Sin.	24	36	Sin.	48	36
$\alpha = 22$								24	24	24	Sin.	48	Sin.	Sin.
$\alpha = 23$									24	Sin.	36	48	48	48
$\alpha = 24$									24	36	48	48	48	Sin.
$\alpha = 25$									36	36	36	48	36	48
$\alpha = 26$									24	24	48	48	48	Sin.
$\alpha = 27$									36	24	36	48	Sin.	36
$\alpha = 28$									24	36	48	36	48	48
$\alpha = 29$										24	48	48	48	48
$\alpha = 30$										36	36	48	36	48
$\alpha = 31$											36	48	48	36
$\alpha = 32$											36	48	48	48
$\alpha = 33$											48	36	48	48
$\alpha = 34$											Sin.	48	48	48
$\alpha = 35$											Sin.	48	36	48
$\alpha = 36$											48	36	36	48
$\alpha = 37$												Sin.	48	36
$\alpha = 38$												48	36	48
$\alpha = 39$												48	48	48
$\alpha = 40$												36	36	60
$\alpha = 41$													48	48
$\alpha = 42$													36	60
$\alpha = 43$														48
$\alpha = 44$														60
$\alpha = 45$														48
$\alpha = 46$														48

EK 5.

Tate Normal Formdaki Eliptik Eğrilerin $p < 200$ Asalları İçin Grup Mertebelerine Göre Sınıflandırılması

$n = 4$									
			$p = 17$	$p = 97$	$p = 113$	$p = 193$			
	$p \equiv 1\ (16)$	p -- 25 mertebeli eğrilerin sayısı				8	$2k$		
		p – 21 mertebeli eğrilerin sayısı				6	$2k$		
		p – 17 mertebeli eğrilerin sayısı		7	14	20	$2k, 7k$		
		p – 13 mertebeli eğrilerin sayısı		4	4	10	$2k$		
		p – 9 mertebeli eğrilerin sayısı		12	8	16	$2k$		
		p – 5 mertebeli eğrilerin sayısı	2	4	12	8	$2k$		
		p – 1 mertebeli eğrilerin sayısı	7	28	20	36	$2k, 7k$		
		p + 3 mertebeli eğrilerin sayısı	2	8	4	8	$2k$		
		p + 7 mertebeli eğrilerin sayısı	4	8	24	16	$2k$		
		p + 11 mertebeli eğrilerin sayısı		6	4	8	$2k$		
		p + 15 mertebeli eğrilerin sayısı		16	17	35	$2k, 5k, 17k$		
		p + 19 mertebeli eğrilerin sayısı		2	4	4	$2k$		
		p + 23 mertebeli eğrilerin sayısı				12	$2k$		
		p + 27 mertebeli eğrilerin sayısı				4	$2k$		
			$p = 19$	$p = 67$	$p = 83$	$p = 131$	$p = 163$	$p = 179$	
	$p \equiv 3\ (16)$	p – 23 mertebeli eğrilerin sayısı					3	6	$3k$
		p – 19 mertebeli eğrilerin sayısı				9	15	15	$3k$
		p – 15 mertebeli eğrilerin sayısı		1	3	3	9	6	$3k, 1$
		p – 11 mertebeli eğrilerin sayısı		9	15	24	15	30	$3k$
		p – 7 mertebeli eğrilerin sayısı	1	6	3	6	7	3	$3k, 7k, 1$
		p – 3 mertebeli eğrilerin sayısı	6	15	15	15	30	21	$3k$
		p + 1 mertebeli eğrilerin sayısı	3	3	9	15	3	15	$3k$
		p + 5 mertebeli eğrilerin sayısı	6	15	15	15	30	21	$3k$
		p + 9 mertebeli eğrilerin sayısı	1	6	3	6	7	3	$3k, 7k, 1$
		p + 13 mertebeli eğrilerin sayısı		9	15	24	15	30	$3k$
		p + 17 mertebeli eğrilerin sayısı		1	3	3	9	6	$3k, 1$
		p + 21 mertebeli eğrilerin sayısı				9	15	15	$3k$
		p + 25 mertebeli eğrilerin sayısı					3	6	$3k$
			$p = 37$	$p = 53$	$p = 101$	$p = 149$	$p = 181$	$p = 197$	
	$p \equiv 5\ (16)$	p – 25 mertebeli eğrilerin sayısı					2	2	$2k$
		p – 21 mertebeli eğrilerin sayısı				10	20	18	$2k$
		p – 17 mertebeli eğrilerin sayısı			4	8	5	12	$2k, 5k$
		p – 13 mertebeli eğrilerin sayısı		2	8	10	16	8	$2k$
		p – 9 mertebeli eğrilerin sayısı	2	2	6	6	8	6	$2k$
		p – 5 mertebeli eğrilerin sayısı	10	18	30	36	18	50	$2k$
		p – 1 mertebeli eğrilerin sayısı	5	4	5	4	12	9	$2k, 3k, 5k$
		p + 3 mertebeli eğrilerin sayısı	10	8	10	8	24	18	$2k$
		p + 7 mertebeli eğrilerin sayısı	2	6	6	12	6	10	$2k$
		p + 11 mertebeli eğrilerin sayısı	6	10	18	30	40	18	$2k, 1$
		p + 15 mertebeli eğrilerin sayısı		1	4	5	8	4	$2k, 5k$
		p + 19 mertebeli eğrilerin sayısı			8	16	10	24	$2k$
		p + 23 mertebeli eğrilerin sayısı				2	4	6	$2k$
		p + 27 mertebeli eğrilerin sayısı					6	10	$2k$
			$p = 23$	$p = 71$	$p = 103$	$p = 151$	$p = 167$	$p = 199$	
	$p \equiv 7\ (16)$	p – 27 mertebeli eğrilerin sayısı						1	1
		p – 23 mertebeli eğrilerin sayısı				3	9	12	$3k$

		p – 19 mertebeli eğrilerin sayısı			1	6	3	9	**1, 3*k***
		p – 15 mertebeli eğrilerin sayısı		3	12	18	15	24	**3*k***
		p – 11 mertebeli eğrilerin sayısı		6	3	6	15	3	**3*k***
		p – 7 mertebeli eğrilerin sayısı	3	12	18	24	21	24	**3*k***
		p – 3 mertebeli eğrilerin sayısı	3	3	9	7	3	12	**3*k*, 7*k***
		p + 1 mertebeli eğrilerin sayısı	9	21	15	21	33	27	**3*k***
		p + 5 mertebeli eğrilerin sayısı	3	3	9	7	3	12	**3*k*, 7*k***
		p + 9 mertebeli eğrilerin sayısı	3	12	18	24	21	24	**3*k***
		p + 13 mertebeli eğrilerin sayısı		6	3	6	15	3	**3*k***
		p + 17 mertebeli eğrilerin sayısı		3	12	18	15	24	**3*k***
		p + 21 mertebeli eğrilerin sayısı			1	6	3	9	**1, 3*k***
		p + 25 mertebeli eğrilerin sayısı				3	9	12	**3*k***
		p + 29 mertebeli eğrilerin sayısı						1	**1**
			p = 41	**p = 73**	**p = 89**	**p = 137**			
	$p \equiv 9$ (16)	p – 21 mertebeli eğrilerin sayısı				2	**2*k***		
		p – 17 mertebeli eğrilerin sayısı			4	16	**2*k***		
		p – 13 mertebeli eğrilerin sayısı		4	4	4	**2*k***		
		p – 9 mertebeli eğrilerin sayısı	7	16	17	20	**2*k*, 7*k*, 17*k***		
		p – 5 mertebeli eğrilerin sayısı	4	4	8	8	**2*k***		
		p – 1 mertebeli eğrilerin sayısı	8	12	8	16	**2*k***		
		P + 3 mertebeli eğrilerin sayısı	4	6	4	8	**2*k***		
		P + 7 mertebeli eğrilerin sayısı	14	17	28	34	**2*k*, 17*k***		
		p + 11 mertebeli eğrilerin sayısı	2	4	4	4	**2*k***		
		P + 15 mertebeli eğrilerin sayısı		8	8	8	**2*k***		
		P + 19 mertebeli eğrilerin sayısı			2	8	**2*k***		
		p + 23 mertebeli eğrilerin sayısı				7	**7*k***		
			p = 43	**p = 59**	**p = 107**	**p = 139**			
	$p \equiv 11$ (16)	p – 19 mertebeli eğrilerin sayısı			3	12	**3*k***		
		p – 15 mertebeli eğrilerin sayısı			3	7	**3*k*, 7*k***		
		p – 11 mertebeli eğrilerin sayısı	3	9	21	15	**3*k***		
		p – 7 mertebeli eğrilerin sayısı	4	3	6	6	**2*k*, 3*k***		
		p – 3 mertebeli eğrilerin sayısı	12	12	15	24	**3*k***		
		p + 1 mertebeli eğrilerin sayısı	3	9	9	9	**3*k***		
		p + 5 mertebeli eğrilerin sayısı	12	12	15	24	**3*k***		
		p + 9 mertebeli eğrilerin sayısı	4	3	6	6	**2*k*, 3*k***		
		p + 13 mertebeli eğrilerin sayısı	3	9	21	15	**3*k***		
		p + 17 mertebeli eğrilerin sayısı			3	7	**3*k*, 7*k***		
		p + 21 mertebeli eğrilerin sayısı			3	12	**3*k***		
			p = 29	**p = 61**	**p = 109**	**p = 157**	**p = 173**		
	$p \equiv 13$ (16)	p – 25 mertebeli eğrilerin sayısı					1	**1**	
		p – 21 mertebeli eğrilerin sayısı				10	8	**2*k***	
		p – 17 mertebeli eğrilerin sayısı			2	6	6	**2*k***	
		p – 13 mertebeli eğrilerin sayısı		6	20	24	30	**2*k***	
		p – 9 mertebeli eğrilerin sayısı	1	5	8	8	4	**2*k*, 5*k*, 1**	
		p – 5 mertebeli eğrilerin sayısı	8	8	10	8	32	**2*k***	
		p – 1 mertebeli eğrilerin sayısı	2	4	8	8	6	**2*k***	
		p + 3 mertebeli eğrilerin sayısı	10	20	24	40	18	**2*k***	
		p + 7 mertebeli eğrilerin sayısı	4	4	5	4	16	**2*k*, 5*k***	
		p + 11 mertebeli eğrilerin sayısı	2	10	16	16	8	**2*k***	
		p + 15 mertebeli eğrilerin sayısı		2	4	8	6	**2*k***	
		p + 19 mertebeli eğrilerin sayısı			10	18	30	**2*k***	
		p + 23 mertebeli eğrilerin sayısı				5	4	**2*k*, 5*k***	
		p + 27 mertebeli eğrilerin sayısı					2	**2*k***	

			$p = 31$	$p = 47$	$p = 79$	$p = 127$	$p = 191$		
	$p \equiv 15$ (16)	$p - 23$ mertebeli eğrilerin sayısı					15	$3k$	
		$p - 19$ mertebeli eğrilerin sayısı				4	6	$2k$	
		$p - 15$ mertebeli eğrilerin sayısı			6	15	15	$3k$	
		$p - 11$ mertebeli eğrilerin sayısı		3	3	6	12	$3k$	
		$p - 7$ mertebeli eğrilerin sayısı	6	9	15	24	21	$3k$	
		$p - 3$ mertebeli eğrilerin sayısı	4	3	7	6	6	$2k, 3k, 7k$	
		$p + 1$ mertebeli eğrilerin sayısı	9	15	15	15	39	$3k$	
		$p + 5$ mertebeli eğrilerin sayısı	4	3	7	6	6	$2k, 3k, 7k$	
		$p + 9$ mertebeli eğrilerin sayısı	6	9	15	24	21	$3k$	
		$p + 13$ mertebeli eğrilerin sayısı		3	3	6	12	$3k$	
		$p + 17$ mertebeli eğrilerin sayısı			6	15	15	$3k$	
		$p + 21$ mertebeli eğrilerin sayısı				4	6	$2k$	
		$p + 25$ mertebeli eğrilerin sayısı					15	$3k$	

$n = 5$									
			$p = 41$	$p = 61$	$p = 101$	$p = 181$			
	$p \equiv 1 \pmod{20}$	p – 21 mertebeli eğrilerin sayısı				16	$2k$		
		p – 16 mertebeli eğrilerin sayısı			4	8	$2k$		
		p – 11 mertebeli eğrilerin sayısı	4	10	16	16	$2k$		
		p – 6 mertebeli eğrilerin sayısı	4	8	8	32	$2k$		
		p – 1 mertebeli eğrilerin sayısı	12	16	30	36	$2k$		
		p + 4 mertebeli eğrilerin sayısı	8	4	16	8	$2k$		
		p + 9 mertebeli eğrilerin sayısı	10	12	8	16	$2k$		
		p + 14 mertebeli eğrilerin sayısı		8	4	8	$2k$		
		p + 19 mertebeli eğrilerin sayısı			12	30	$2k$		
						8	$2k$		
			$p = 23$	$p = 43$	$p = 83$	$p = 103$	$p = 163$		
	$p \equiv 3 \pmod{20}$	p – 23 mertebeli eğrilerin sayısı					8	$2k$	
		p – 18 mertebeli eğrilerin sayısı				4	8	$2k$	
		p – 13 mertebeli eğrilerin sayısı			8	16	16	$2k$	
		p – 8 mertebeli eğrilerin sayısı	2	4	14	6	10	$2k$	
		p – 3 mertebeli eğrilerin sayısı	8	16	20	24	40	$2k$	
		p + 2 mertebeli eğrilerin sayısı	4	10	6	12	16	$2k$	
		p + 7 mertebeli eğrilerin sayısı	8	8	20	16	16	$2k$	
		p + 12 mertebeli eğrilerin sayısı		4	6	8	18	$2k$	
		p + 17 mertebeli eğrilerin sayısı			8	16	24	$2k$	
		p + 22 mertebeli eğrilerin sayısı					6	$2k$	
			$p = 47$	$p = 67$	$p = 107$	$p = 127$	$p = 167$		
	$p \equiv 5 \pmod{20}$	p – 22 mertebeli eğrilerin sayısı					6	$2k$	
		p – 17 mertebeli eğrilerin sayısı				12	8	20	$2k$
		p – 12 mertebeli eğrilerin sayısı	2	6	8	12	6	$2k$	
		p – 7 mertebeli eğrilerin sayısı	12	16	16	32	28	$2k$	
		p – 2 mertebeli eğrilerin sayısı	10	8	18	6	22	$2k$	
		p + 3 mertebeli eğrilerin sayısı	8	16	12	24	20	$2k$	
		p + 8 mertebeli eğrilerin sayısı	6	8	6	16	10	$2k$	
		p + 13 mertebeli eğrilerin sayısı	8	12	28	16	40	$2k$	
		p + 18 mertebeli eğrilerin sayısı			6	8	6	$2k$	
		p + 23 mertebeli eğrilerin sayısı				4	8	$2k$	
			$p = 29$	$p = 89$	$p = 109$	$p = 149$			
	$p \equiv 7 \pmod{20}$	p – 19 mertebeli eğrilerin sayısı			5	9	$3k, 5k$		
		p -- 14 mertebeli eğrilerin sayısı		10	6	16	$2k$		
		p – 19 mertebeli eğrilerin sayısı	3	15	24	24	$2k, 3k$		
		p – 4 mertebeli eğrilerin sayısı	4	6	12	10	$2k$		
		p + 1 mertebeli eğrilerin sayısı	12	24	12	28	$2k$		
		p + 6 mertebeli eğrilerin sayısı	4	6	12	10	$2k$		
		p + 11 mertebeli eğrilerin sayısı	3	15	24	24	$2k, 3k$		
		p + 16 mertebeli eğrilerin sayısı		10	6	16	$2k$		
		p + 21 mertebeli eğrilerin sayısı			5	9	$3k, 5k$		
			$p = 11$	$p = 31$	$p = 71$	$p = 131$	$p = 151$	$p = 191$	
	$p \equiv 11 \pmod{20}$	p – 26 mertebeli eğrilerin sayısı						4	$2k$
		p – 21 mertebeli eğrilerin sayısı				4	8	8	$2k$
		p – 16 mertebeli eğrilerin sayısı				4	12	20	$2k$
		p – 11 mertebeli eğrilerin sayısı			16	32	16	32	$2k$
		p – 6 mertebeli eğrilerin sayısı		8	4	20	8	8	$2k$
		p – 1 mertebeli eğrilerin sayısı	4	8	8	8	40	8	$2k$
		p + 4 mertebeli eğrilerin sayısı	4	4	20	12	8	24	$2k$

		$p+9$ mertebeli eğrilerin sayısı		8	16	16	32	48	$2k$
		$p+14$ mertebeli eğrilerin sayısı			4	8	8	8	$2k$
		$p+19$ mertebeli eğrilerin sayısı				24	8	24	$2k$
		$p+24$ mertebeli eğrilerin sayısı					8	4	$2k$
			$p=53$	$p=73$	$p=113$	$p=173$	$p=193$		
	$p \equiv 13 \pmod{20}$	$p-23$ mertebeli eğrilerin sayısı				12	9	$2k, 3k$	
		$p-18$ mertebeli eğrilerin sayısı			4	6	12	$2k$	
		$p-13$ mertebeli eğrilerin sayısı	3	12	15	24	35	$3k, 5k$	
		$p-8$ mertebeli eğrilerin sayısı	10	6	16	20	10	$2k$	
		$p-3$ mertebeli eğrilerin sayısı	9	16	12	13	32	$2k, 3k, 13k$	
		$p+2$ mertebeli eğrilerin sayısı	6	8	12	10	12	$2k$	
		$p+7$ mertebeli eğrilerin sayısı	20	15	36	48	24	$2k, 3k$	
		$p+12$ mertebeli eğrilerin sayısı	4	10	6	10	16	$2k$	
		$p+17$ mertebeli eğrilerin sayısı		5	9	12	24	$2k, 3k, 5k$	
		$p+22$ mertebeli eğrilerin sayısı			2	14	6	$2k$	
		$p+27$ mertebeli eğrilerin sayısı				3	12	$2k, 3k$	
			$p=37$	$p=97$	$p=137$	$p=157$	$p=197$		
	$p \equiv 17 \pmod{20}$	$p-27$ mertebeli eğrilerin sayısı					1	1	
		$p-22$ mertebeli eğrilerin sayısı			2	6	8	$2k$	
		$p-17$ mertebeli eğrilerin sayısı		7	24	20	36	$2k, 7k$	
		$p-12$ mertebeli eğrilerin sayısı		8	6	16	10	$2k$	
		$p-7$ mertebeli eğrilerin sayısı	8	17	13	16	20	$2k, 13k, 17k$	
		$p-2$ mertebeli eğrilerin sayısı	6	6	18	10	20	$2k$	
		$p+3$ mertebeli eğrilerin sayısı	15	28	24	32	27	$2k, 3k$	
		$p+8$ mertebeli eğrilerin sayısı	6	12	6	16	10	$2k$	
		$p+13$ mertebeli eğrilerin sayısı	1	12	28	13	32	$2k, 13k, 1$	
		$p+18$ mertebeli eğrilerin sayısı		6	8	12	6	$2k$	
		$p+23$ mertebeli eğrilerin sayısı			7	15	20	$2k, 3k, 7k$	
		$p+28$ mertebeli eğrilerin sayısı					6	$2k$	
			$p=19$	$p=59$	$p=79$	$p=139$	$p=179$	$p=199$	
	$p \equiv 19 \pmod{20}$	$p-24$ mertebeli eğrilerin sayısı					4	10	$2k$
		$p-19$ mertebeli eğrilerin sayısı				16	20	24	$2k$
		$p-14$ mertebeli eğrilerin sayısı		2	4	6	18	10	$2k$
		$p-9$ mertebeli eğrilerin sayısı		8	16	16	16	24	$2k$
		$p-4$ mertebeli eğrilerin sayısı	4	6	8	18	10	12	$2k$
		$p+1$ mertebeli eğrilerin sayısı	8	24	20	24	40	36	$2k$
		$p+6$ mertebeli eğrilerin sayısı	4	6	8	18	10	12	$2k$
		$p+11$ mertebeli eğrilerin sayısı		8	16	6	16	24	$2k$
		$p+16$ mertebeli eğrilerin sayısı		2	4	6	18	10	$2k$
		$p+21$ mertebeli eğrilerin sayısı				16	20	24	$2k$
		$p+26$ mertebeli eğrilerin sayısı					4	10	$2k$

$n = 6$									
			$p = 73$	$p = 97$	$p = 193$				
	$p \equiv 1 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı			10	$2k$			
		$p - 19$ mertebeli eğrilerin sayısı			4	$2k$			
		$p - 13$ mertebeli eğrilerin sayısı	10	14	56	$2k$			
		$p - 7$ mertebeli eğrilerin sayısı	4	16	4	$2k$			
		$p - 1$ mertebeli eğrilerin sayısı	30	26	30	$2k$			
		$p + 5$ mertebeli eğrilerin sayısı	8	4	28	$2k$			
		$p + 11$ mertebeli eğrilerin sayısı	14	30	20	$2k$			
		$p + 17$ mertebeli eğrilerin sayısı	4	4	12	$2k$			
		$p + 23$ mertebeli eğrilerin sayısı			30	$2k$			
			$p = 29$	$p = 53$	$p = 101$	$p = 149$	$p = 173$	$p = 197$	
	$p \equiv 5 \pmod{24}$	$p - 23$ mertebeli eğrilerin sayısı				2	6	6	$2k$
		$p - 17$ mertebeli eğrilerin sayısı			10	20	24	30	$2k$
		$p - 11$ mertebeli eğrilerin sayısı		4	8	8	8	16	$2k$
		$p - 5$ mertebeli eğrilerin sayısı	10	18	24	36	40	40	$2k$
		$p + 1$ mertebeli eğrilerin sayısı	6	6	14	14	14	10	$2k$
		$p + 7$ mertebeli eğrilerin sayısı	10	18	24	36	40	40	$2k$
		$p +$ 13 mertebeli eğrilerin sayısı		4	8	8	8	16	$2k$
		$p + 19$ mertebeli eğrilerin sayısı			10	20	24	30	$2k$
		$p + 25$ mertebeli eğrilerin sayısı				2	6	6	$2k$
			$p = 31$	$p = 79$	$p = 103$	$p = 127$	$p = 151$	$p = 199$	
	$p \equiv 7 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı						4	$2k$
		$p - 19$ mertebeli eğrilerin sayısı			2	14	12	36	$2k$
		$p - 13$ mertebeli eğrilerin sayısı		4	14	4	4	10	$2k$
		$p - 7$ mertebeli eğrilerin sayısı	8	32	24	32	56	32	$2k$
		$p - 1$ mertebeli eğrilerin sayısı	4	4	4	24	10	16	$2k$
		$p + 5$ mertebeli eğrilerin sayısı	14	14	36	12	14	24	$2k$
		$p + 11$ mertebeli eğrilerin sayısı	2	14	4	4	24	12	$2k$
		$p + 17$ mertebeli eğrilerin sayısı		8	16	32	24	56	$2k$
		$p + 23$ mertebeli eğrilerin sayısı				2	4	4	$2k$
		$p + 29$ mertebeli eğrilerin sayısı						2	$2k$
			$p = 59$	$p = 83$	$p = 107$	$p = 131$	$p = 179$		
	$p \equiv 11 \pmod{24}$	$p - 23$ mertebeli eğrilerin sayısı					12	$2k$	
		$p - 17$ mertebeli eğrilerin sayısı		1	6	7	9	$3k, 7k, 1$	
		$p - 11$ mertebeli eğrilerin sayısı	12	20	28	32	40	$2k$	
		$p - 5$ mertebeli eğrilerin sayısı	7	10	9	10	12	$2k, 3k, 7k$	
		$P + 1$ mertebeli eğrilerin sayısı	18	18	18	30	30	$2k$	
		$P + 7$ mertebeli eğrilerin sayısı	7	10	9	10	12	$2k, 3k, 7k$	
		$P + 13$ mertebeli eğrilerin sayısı	12	20	28	32	40	$2k$	
		$P + 19$ mertebeli eğrilerin sayısı		1	6	7	9	$3k, 7k, 1$	
		$P + 25$ mertebeli eğrilerin sayısı					12	$2k$	
			$p = 37$	$p = 61$	$p = 109$	$p = 157$	$p = 181$		
	$p \equiv 13 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı					6	$2k$	
		$p - 19$ mertebeli eğrilerin sayısı			4	4	16	$2k$	
		$p - 13$ mertebeli eğrilerin sayısı		6	16	42	20	$2k$	
		$p - 7$ mertebeli eğrilerin sayısı	4	12	4	8	8	$2k$	
		$p - 1$ mertebeli eğrilerin sayısı	20	16	42	32	60	$2k$	
		$p + 5$ mertebeli eğrilerin sayısı	4	4	8	24	4	$2k$	
		$p + 11$ mertebeli eğrilerin sayısı	6	20	20	20	32	$2k$	

		$p+17$ mertebeli eğrilerin sayısı			12	4	16	$2k$	
		$p+23$ mertebeli eğrilerin sayısı				20	16	$2k$	
			$p=41$	$p=89$	$p=113$	$p=137$			
	$p \equiv 17 \pmod{24}$	$p-17$ mertebeli eğrilerin sayısı		5	13	20	$2k, 5k, 13k$		
		$p-11$ mertebeli eğrilerin sayısı	2	6	8	14	$2k$		
		$p-5$ mertebeli eğrilerin sayısı	13	26	30	29	$2k, 13k, 29k$		
		$p+1$ mertebeli eğrilerin sayısı	8	12	8	8	$2k$		
		$p+7$ mertebeli eğrilerin sayısı	13	26	30	29	$2k, 13k, 29k$		
		$p+13$ mertebeli eğrilerin sayısı	2	6	8	14	$2k$		
		$p+19$ mertebeli eğrilerin sayısı		5	13	20	$2k, 5k, 13k$		
			$p=43$	$p=67$	$p=139$	$p=163$			
	$p \equiv 19 \pmod{24}$	$p-19$ mertebeli eğrilerin sayısı			16	32	$2k$		
		$p-13$ mertebeli eğrilerin sayısı		6	16	8	$2k$		
		$p-7$ mertebeli eğrilerin sayısı	14	12	12	14	$2k$		
		$p-1$ mertebeli eğrilerin sayısı	4	8	8	18	$2k$		
		$p+5$ mertebeli eğrilerin sayısı	16	32	56	40	$2k$		
		$p+11$ mertebeli eğrilerin sayısı	6	4	8	8	$2k$		
		$p+17$ mertebeli eğrilerin sayısı		2	14	36	$2k$		
		$p+23$ mertebeli eğrilerin sayısı			6	4	$2k$		
			$p=23$	$p=47$	$p=71$	$p=167$	$p=191$		
	$p \equiv 23 \pmod{24}$	$p-23$ mertebeli eğrilerin sayısı				12	20	$2k$	
		$p-17$ mertebeli eğrilerin sayısı				10	12	$2k$	
		$p-11$ mertebeli eğrilerin sayısı		6	12	30	24	$2k$	
		$p-5$ mertebeli eğrilerin sayısı	4	6	8	8	12	$2k$	
		$p+1$ mertebeli eğrilerin sayısı	12	20	28	44	52	$2k$	
		$p+7$ mertebeli eğrilerin sayısı	4	6	8	8	12	$2k$	
		$p+13$ mertebeli eğrilerin sayısı		6	12	30	24	$2k$	
		$p+19$ mertebeli eğrilerin sayısı				10	12	$2k$	
		$p+25$ mertebeli eğrilerin sayısı				12	20	$2k$	

$n = 7$							
			$p = 29$	$p = 113$	$p = 197$		
	$p \equiv 1 \pmod{28}$	$p - 22$ mertebeli eğrilerin sayısı			12	$2k$	
		$p - 15$ mertebeli eğrilerin sayısı		24	12	$2k$	
		$p - 8$ mertebeli eğrilerin sayısı	6	24	18	$2k$	
		$p - 1$ mertebeli eğrilerin sayısı	12	24	72	$2k$	
		$p + 6$ mertebeli eğrilerin sayısı	6	6	12	$2k$	
		$p + 13$ mertebeli eğrilerin sayısı		24	48	$2k$	
		$p + 20$ mertebeli eğrilerin sayısı		6	6	$2k$	
		$p + 27$ mertebeli eğrilerin sayısı			12	$2k$	
			$p = 31$	$p = 59$	$p = 199$		
	$p \equiv 3 \pmod{28}$	$p - 24$ mertebeli eğrilerin sayısı			15	$3k$	
		$p - 17$ mertebeli eğrilerin sayısı			18	$3k$	
		$p - 10$ mertebeli eğrilerin sayısı	1	6	28	$2k, 1$	
		$p - 3$ mertebeli eğrilerin sayısı	16	24	48	$2k$	
		$p + 4$ mertebeli eğrilerin sayısı	6	15	15	$3k$	
		$p + 11$ mertebeli eğrilerin sayısı	6	12	36	$3k$	
		$p + 18$ mertebeli eğrilerin sayısı			13	$13k$	
		$p + 25$ mertebeli eğrilerin sayısı			24	$3k$	
			$p = 61$	$p = 89$	$p = 173$		
	$p \equiv 5 \pmod{28}$	$p - 19$ mertebeli eğrilerin sayısı			12	$3k$	
		$p - 12$ mertebeli eğrilerin sayısı	7	6	15	$3k, 7k$	
		$p - 5$ mertebeli eğrilerin sayısı	18	42	72	$3k$	
		$p + 2$ mertebeli eğrilerin sayısı	13	12	15	$3k, 13k$	
		$p + 9$ mertebeli eğrilerin sayısı	18	12	18	$3k$	
		$p + 16$ mertebeli eğrilerin sayısı	3	15	21	$3k$	
		$p + 23$ mertebeli eğrilerin sayısı			18	$3k$	
			$p = 37$	$p = 149$			
	$p \equiv 9 \pmod{28}$	$p - 23$ mertebeli eğrilerin sayısı		6	$3k$		
		$p - 16$ mertebeli eğrilerin sayısı		9	$3k$		
		$p - 9$ mertebeli eğrilerin sayısı	10	36	$2k$		
		$p - 2$ mertebeli eğrilerin sayısı	9	21	$3k$		
		$p + 5$ mertebeli eğrilerin sayısı	12	24	$2k$		
		$p + 12$ mertebeli eğrilerin sayısı	4	15	$2k, 3k$		
		$p + 19$ mertebeli eğrilerin sayısı		36	$2k$		
			$p = 67$	$p = 151$	$p = 179$		
	$p \equiv 11 \pmod{28}$	$p - 25$ mertebeli eğrilerin sayısı			6	$3k$	
		$p - 18$ mertebeli eğrilerin sayısı		13	12	$3k, 13k$	
		$p - 11$ mertebeli eğrilerin sayısı	18	24	60	$3k$	
		$p - 4$ mertebeli eğrilerin sayısı	13	24	15	$3k, 13k$	
		$p + 3$ mertebeli eğrilerin sayısı	24	30	24	$3k$	
		$p + 10$ mertebeli eğrilerin sayısı	6	15	30	$3k$	
		$p + 17$ mertebeli eğrilerin sayısı	4	36	24	$2k, 3k$	
		$p + 24$ mertebeli eğrilerin sayısı		7	6	$3k, 7k$	
			$p = 41$	$p = 97$	$p = 181$		
	$p \equiv 13 \pmod{28}$	$p - 20$ mertebeli eğrilerin sayısı			9	$3k$	
		$p - 13$ mertebeli eğrilerin sayısı		22	36	$2k$	
		$p - 6$ mertebeli eğrilerin sayısı	6	18	28	$2k$	
		$p + 1$ mertebeli eğrilerin sayısı	24	12	30	$2k$	
		$p + 8$ mertebeli eğrilerin sayısı	6	18	28	$2k$	
		$p + 15$ mertebeli eğrilerin sayısı		22	36	$2k$	
		$p + 22$ mertebeli eğrilerin sayısı			9	$3k$	

			$p = 43$	$p = 71$	$p = 127$		
	$p \equiv 15 \pmod{28}$	$p - 15$ mertebeli eğrilerin sayısı		6	30	$2k$	
		$p - 8$ mertebeli eğrilerin sayısı	6	12	6	$2k$	
		$p - 1$ mertebeli eğrilerin sayısı	12	12	36	$2k$	
		$p + 6$ mertebeli eğrilerin sayısı	14	12	12	$2k$	
		$p + 13$ mertebeli eğrilerin sayısı	6	24	24	$2k$	
		$p + 20$ mertebeli eğrilerin sayısı			14	$2k$	
			$p = 73$	$p = 101$	$p = 157$		
	$p \equiv 17 \pmod{28}$	$p - 24$ mertebeli eğrilerin sayısı			1	1	
		$p - 17$ mertebeli eğrilerin sayısı		18	30	$2k$	
		$p - 10$ mertebeli eğrilerin sayısı	15	9	13	$3k$, $13k$	
		$p - 3$ mertebeli eğrilerin sayısı	24	12	36	$2k$	
		$p + 4$ mertebeli eğrilerin sayısı	9	24	15	$2k$, $3k$	
		$p + 11$ mertebeli eğrilerin sayısı	22	30	36	$2k$	
		$p + 18$ mertebeli eğrilerin sayısı	1	6	18	$2k$, 1	
		$p + 25$ mertebeli eğrilerin sayısı			6	$2k$	
			$p = 47$	$p = 103$	$p = 131$		
	$p \equiv 19 \pmod{28}$	$p - 19$ mertebeli eğrilerin sayısı		4	18	$2k$	
		$p - 12$ mertebeli eğrilerin sayısı	3	13	12	$3k$, $13k$	
		$p - 5$ mertebeli eğrilerin sayısı	18	24	30	$2k$	
		$p + 2$ mertebeli eğrilerin sayısı	6	18	15	$3k$	
		$p + 9$ mertebeli eğrilerin sayısı	18	36	24	$2k$	
		$p + 16$ mertebeli eğrilerin sayısı		6	24	$2k$	
		$p + 23$ mertebeli eğrilerin sayısı			6	$2k$	
			$p = 79$	$p = 107$	$p = 163$	$p = 191$	
	$p \equiv 23 \pmod{28}$	$p - 23$ mertebeli eğrilerin sayısı			12	30	$3k$
		$p - 16$ mertebeli eğrilerin sayısı	4	9	13	15	$2k$, $3k$, $13k$
		$p - 9$ mertebeli eğrilerin sayısı	24	12	24	30	$3k$
		$p - 2$ mertebeli eğrilerin sayısı	9	27	9	36	$3k$
		$p + 5$ mertebeli eğrilerin sayısı	28	30	60	24	$2k$
		$p + 12$ mertebeli eğrilerin sayısı	12	9	27	9	$3k$
		$p + 19$ mertebeli eğrilerin sayısı		18	12	36	$3k$
		$p + 26$ mertebeli eğrilerin sayısı			4	9	$2k$, $3k$
			$p = 53$	$p = 109$	$p = 137$	$p = 193$	
	$p \equiv 25 \pmod{28}$	$p - 25$ mertebeli eğrilerin sayısı				18	$3k$
		$p - 18$ mertebeli eğrilerin sayısı		7	6	18	$3k$, $7k$
		$p - 11$ mertebeli eğrilerin sayısı	12	12	42	18	$3k$
		$p - 4$ mertebeli eğrilerin sayısı	6	18	15	27	$3k$
		$p + 3$ mertebeli eğrilerin sayısı	18	40	36	46	$2k$, $3k$
		$p + 10$ mertebeli eğrilerin sayısı	15	12	21	15	$3k$
		$p + 17$ mertebeli eğrilerin sayısı		18	12	36	$3k$
		$p + 24$ mertebeli eğrilerin sayısı			3	13	$3k$, $13k$
			$p = 83$	$p = 139$	$p = 167$		
	$p \equiv 27 \pmod{28}$	$p - 20$ mertebeli eğrilerin sayısı		6	15	$3k$	
		$p - 13$ mertebeli eğrilerin sayısı	12	30	18	$3k$	
		$p - 6$ mertebeli eğrilerin sayısı	9	13	15	$3k$, $13k$	
		$p + 1$ mertebeli eğrilerin sayısı	36	36	66	$3k$	
		$p + 8$ mertebeli eğrilerin sayısı	9	13	15	$3k$, $13k$	
		$p + 15$ mertebeli eğrilerin sayısı	12	30	18	$3k$	
		$p + 22$ mertebeli eğrilerin sayısı		6	15	$3k$	

$n = 9$											
			$p = 19$	$p = 37$	$p = 73$	$p = 109$	$p = 127$	$p = 163$	$p = 181$	$p = 199$	
	$p \equiv 1 \pmod{18}$	$p - 19$ mertebeli eğrilerin sayısı				6	24	24	54	24	$3k$
		$p - 10$ mertebeli eğrilerin sayısı		6	12	12	12	18	12	42	$3k$
		$p - 1$ mertebeli eğrilerin sayısı	6	18	18	60	24	72	36	24	$3k$
		$p + 8$ mertebeli eğrilerin sayısı	6	6	30	12	36	12	42	18	$3k$
		$p + 17$ mertebeli eğrilerin sayısı			6	12	24	24	24	72	$3k$
		$p + 26$ mertebeli eğrilerin sayısı						6	6	12	$3k$
			$p = 23$	$p = 59$	$p = 113$	$p = 131$	$p = 149$	$p = 167$			
	$p \equiv 5 \pmod{18}$	$p - 23$ mertebeli eğrilerin sayısı					6	18	$3k$		
		$p - 14$ mertebeli eğrilerin sayısı		3	15	24	24	15	$3k$		
		$p - 5$ mertebeli eğrilerin sayısı	12	21	54	30	60	24	$3k$		
		$p + 4$ mertebeli eğrilerin sayısı	9	15	15	18	21	33	$3k$		
		$p + 13$ mertebeli eğrilerin sayısı		18	24	48	24	60	$3k$		
		$p + 22$ mertebeli eğrilerin sayısı			3	9	12	15	$3k$		
			$p = 43$	$p = 61$	$p = 79$	$p = 97$	$p = 151$				
	$p \equiv 7 \pmod{18}$	$p - 16$ mertebeli eğrilerin sayısı			3	15	30	$3k$			
		$p - 7$ mertebeli eğrilerin sayısı	12	30	24	18	36	$3k$			
		$p + 2$ mertebeli eğrilerin sayısı	12	9	30	12	12	$3k$			
		$p + 11$ mertebeli eğrilerin sayısı	15	18	18	45	60	$3k$			
		$p + 20$ mertebeli eğrilerin sayısı				3	9	$3k$			
			$p = 29$	$p = 47$	$p = 83$	$p = 101$	$p = 137$	$p = 173$	$p = 191$		
	$p \equiv 11 \pmod{18}$	$p - 20$ mertebeli eğrilerin sayısı					9	21	12	$3k$	
		$p - 11$ mertebeli eğrilerin sayısı		12	30	24	42	24	48	$3k$	
		$p - 2$ mertebeli eğrilerin sayısı	9	15	12	24	27	15	36	$3k$	
		$p + 7$ mertebeli eğrilerin sayısı	18	18	30	36	45	72	36	$3k$	
		$p + 16$ mertebeli eğrilerin sayısı			9	15	12	21	27	$3k$	
		$p + 25$ mertebeli eğrilerin sayısı						18	30	$3k$	
			$p = 31$	$p = 67$	$p = 103$	$p = 139$	$p = 157$	$p = 193$			
	$p \equiv 13 \pmod{18}$	$p - 22$ mertebeli eğrilerin sayısı				3	15	9	$3k$		
		$p - 13$ mertebeli eğrilerin sayısı		15	18	24	30	42	$3k$		
		$p - 4$ mertebeli eğrilerin sayısı	15	9	12	45	12	45	$3k$		
		$p + 5$ mertebeli eğrilerin sayısı	12	24	60	36	60	36	$3k$		
		$p + 14$ mertebeli eğrilerin sayısı		15	9	12	18	12	$3k$		
		$p + 23$ mertebeli eğrilerin sayısı				15	18	45	$3k$		
			$p = 53$	$p = 71$	$p = 89$	$p = 107$	$p = 179$	$p = 197$			
	$p \equiv 17 \pmod{18}$	$p - 26$ mertebeli eğrilerin sayısı						9	$3k$		
		$p - 17$ mertebeli eğrilerin sayısı			9	18	27	54	$3k$		
		$p - 8$ mertebeli eğrilerin sayısı	15	12	15	15	30	18	$3k$		
		$p + 1$ mertebeli eğrilerin sayısı	18	42	36	36	60	30	$3k$		
		$p + 10$ mertebeli eğrilerin sayısı	15	12	15	15	30	18	$3k$		
		$p + 19$ mertebeli eğrilerin sayısı			9	18	27	54	$3k$		
		$p + 28$ mertebeli eğrilerin sayısı						9	$3k$		

$n = 10$									
			$p = 41$	$p = 61$	$p = 101$	$p = 181$			
	$p \equiv 1 \pmod{20}$	$p - 21$ mertebeli eğrilerin sayısı				32	$2k$		
		$p - 11$ mertebeli eğrilerin sayısı	4	10	16	16	$2k$		
		$p - 1$ mertebeli eğrilerin sayısı	20	32	50	60	$2k$		
		$p + 9$ mertebeli eğrilerin sayısı	10	12	8	16	$2k$		
		$p + 19$ mertebeli eğrilerin sayısı			20	50	$2k$		
			$p = 23$	$p = 43$	$p = 83$	$p = 103$	$p = 163$		
	$p \equiv 3 \pmod{20}$	$p - 23$ mertebeli eğrilerin sayısı					12	$4k$	
		$p - 13$ mertebeli eğrilerin sayısı			8	16	16	$4k$	
		$p - 3$ mertebeli eğrilerin sayısı	12	32	40	36	80	$4k$	
		$p + 7$ mertebeli eğrilerin sayısı	8	8	20	16	16	$4k$	
		$p + 17$ mertebeli eğrilerin sayısı			12	32	36	$4k$	
			$p = 47$	$p = 67$	$p = 107$	$p = 127$	$p = 167$		
	$p \equiv 7 \pmod{20}$	$p - 17$ mertebeli eğrilerin sayısı			12	8	20	$4k$	
		$p - 7$ mertebeli eğrilerin sayısı	24	24	24	64	56	$4k$	
		$p + 3$ mertebeli eğrilerin sayısı	8	16	12	24	20	$4k$	
		$p + 13$ mertebeli eğrilerin sayısı	12	24	56	24	60	$4k$	
		$p + 23$ mertebeli eğrilerin sayısı				4	8	$4k$	
			$p = 29$	$p = 89$	$p = 109$	$p = 149$			
	$p \equiv 9 \pmod{20}$	$p - 19$ mertebeli eğrilerin sayısı			5	9	$3k$, $5k$		
		$p - 9$ mertebeli eğrilerin sayısı	5	29	40	48	$3k$, $5k$, $29k$		
		$p + 1$ mertebeli eğrilerin sayısı	12	24	12	28	$2k$, $3k$		
		$p + 11$ mertebeli eğrilerin sayısı	5	29	40	48	$3k$, $5k$, $29k$		
		$p + 21$ mertebeli eğrilerin sayısı			5	9	$3k$, $5k$		
			$p = 31$	$p = 71$	$p = 131$	$p = 151$	$p = 191$		
	$p \equiv 11 \pmod{20}$	$p - 21$ mertebeli eğrilerin sayısı			4	8	8	$4k$	
		$p - 11$ mertebeli eğrilerin sayısı		24	64	24	48	$4k$	
		$p - 1$ mertebeli eğrilerin sayısı	8	8	8	40	8	$4k$	
		$p + 9$ mertebeli eğrilerin sayısı	16	32	24	64	96	$4k$	
		$p + 19$ mertebeli eğrilerin sayısı			24	8	24	$4k$	
			$p = 53$	$p = 73$	$p = 113$	$p = 173$	$p = 193$		
	$p \equiv 13 \pmod{20}$	$p - 23$ mertebeli eğrilerin sayısı				12	9	$3k$	
		$p - 13$ mertebeli eğrilerin sayısı	5	20	29	48	65	$2k$, $5k$, $29k$	
		$p - 3$ mertebeli eğrilerin sayısı	9	16	12	13	32	$2k$, $3k$, $13k$	
		$p + 7$ mertebeli eğrilerin sayısı	36	29	60	80	40	$2k$, $29k$	
		$p + 17$ mertebeli eğrilerin sayısı		5	9	12	24	$3k$, $5k$	
		$p + 27$ mertebeli eğrilerin sayısı				5	20	$5k$	
			$p = 17$	$p = 37$	$p = 97$	$p = 137$	$p = 157$	$p = 197$	
	$p \equiv 17 \pmod{20}$	$p - 27$ mertebeli eğrilerin sayısı						1	1
		$p - 17$ mertebeli eğrilerin sayısı			13	40	36	60	$2k$, $13k$
		$p - 7$ mertebeli eğrilerin sayısı	1	8	17	13	16	20	$2k$, $13k$, $17k$, 1
		$p + 3$ mertebeli eğrilerin sayısı	13	25	52	40	64	45	$2k$, $5k$, $13k$
		$p + 13$ mertebeli eğrilerin sayısı		1	12	28	13	32	$2k$, $13k$, 1
		$p + 23$ mertebeli eğrilerin sayısı				13	25	36	$2k$, $5k$, $13k$
			$p = 19$	$p = 59$	$p = 79$	$p = 139$	$p = 179$	$p = 199$	
	$p \equiv 19 \pmod{20}$	$p - 19$ mertebeli eğrilerin sayısı				32	40	36	$4k$
		$p - 9$ mertebeli eğrilerin sayısı		8	16	16	16	24	$4k$
		$p + 1$ mertebeli eğrilerin sayısı	12	36	40	36	60	72	$4k$
		$p + 11$ mertebeli eğrilerin sayısı		8	16	16	16	24	$4k$
		$p + 21$ mertebeli eğrilerin sayısı				32	40	36	$4k$

$n = 12$									
			$p = 73$	$p = 97$	$p = 193$				
	$p \equiv 1 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı			16	$2k$			
		$p - 13$ mertebeli eğrilerin sayısı	8	8	32	$2k$			
		$p - 1$ mertebeli eğrilerin sayısı	48	56	72	$2k$			
		$p + 11$ mertebeli eğrilerin sayısı	8	24	16	$2k$			
		$p + 23$ mertebeli eğrilerin sayısı			48	$2k$			
			$p = 29$	$p = 53$	$p = 101$	$p = 149$	$p = 173$	$p = 197$	
	$p \equiv 2 \pmod{24}$	$p - 17$ mertebeli eğrilerin sayısı			8	16	12	24	$2k$
		$p - 5$ mertebeli eğrilerin sayısı	16	36	60	72	64	100	$2k$
		$p + 7$ mertebeli eğrilerin sayısı	8	12	12	24	32	20	$2k$
		$p + 19$ mertebeli eğrilerin sayısı			16	32	60	48	$2k$
			$p = 31$	$p = 79$	$p = 103$	$p = 127$	$p = 151$	$p = 199$	
	$p \equiv 7 \pmod{24}$	$p - 19$ mertebeli eğrilerin sayısı			2	14	12	36	$2k$
		$p - 7$ mertebeli eğrilerin sayısı	12	48	36	48	84	48	$2k$
		$p + 5$ mertebeli eğrilerin sayısı	14	14	36	12	14	24	$2k$
		$p + 17$ mertebeli eğrilerin sayısı		12	24	48	36	84	$2k$
		$p + 29$ mertebeli eğrilerin sayısı						2	$2k$
			$p = 59$	$p = 83$	$p = 107$	$p = 131$	$p = 179$		
	$p \equiv 11 \pmod{24}$	$p - 23$ mertebeli eğrilerin sayısı					12	$2k$	
		$p - 11$ mertebeli eğrilerin sayısı	18	30	42	48	60	$2k$	
		$p + 1$ mertebeli eğrilerin sayısı	18	18	18	30	30	$2k$	
		$p + 13$ mertebeli eğrilerin sayısı	18	30	42	48	60	$2k$	
		$p + 25$ mertebeli eğrilerin sayısı					12	$2k$	
			$p = 37$	$p = 61$	$p = 109$	$p = 157$	$p = 181$		
	$p \equiv 13 \pmod{24}$	$p - 25$ mertebeli eğrilerin sayısı					4	$2k$	
		$p - 13$ mertebeli eğrilerin sayısı		12	40	84	32	$2k$	
		$p - 1$ mertebeli eğrilerin sayısı	16	8	28	16	48	$2k$	
		$p + 11$ mertebeli eğrilerin sayısı	12	32	32	32	80	$2k$	
		$p + 23$ mertebeli eğrilerin sayısı				16	8	$2k$	
			$p = 41$	$p = 89$	$p = 113$	$p = 137$			
	$p \equiv 17 \pmod{24}$	$p - 17$ mertebeli eğrilerin sayısı		8	28	32	$2k$		
		$p - 5$ mertebeli eğrilerin sayısı	8	16	24	16	$2k$		
		$p + 7$ mertebeli eğrilerin sayısı	28	56	48	68	$2k$		
		$p + 19$ mertebeli eğrilerin sayısı		4	8	16	$2k$		
			$p = 43$	$p = 67$	$p = 139$	$p = 163$			
	$p \equiv 19 \pmod{24}$	$p - 19$ mertebeli eğrilerin sayısı			24	48	$2k$		
		$p - 7$ mertebeli eğrilerin sayısı	14	12	12	14	$2k$		
		$p + 5$ mertebeli eğrilerin sayısı	24	48	84	60	$2k$		
		$p + 17$ mertebeli eğrilerin sayısı		2	14	36	$2k$		
			$p = 23$	$p = 47$	$p = 71$	$p = 167$	$p = 191$		
	$p \equiv 23 \pmod{24}$	$p - 23$ mertebeli eğrilerin sayısı				18	30	$2k$	
		$p - 11$ mertebeli eğrilerin sayısı		6	12	30	24	$2k$	
		$p + 1$ mertebeli eğrilerin sayısı	18	30	42	66	78	$2k$	
		$p + 13$ mertebeli eğrilerin sayısı		6	12	30	24	$2k$	
		$p + 25$ mertebeli eğrilerin sayısı				18	30	$2k$	

EK 6.

Tate Normal Formdaki Eliptik Eğrilerin $p \leq 47$ Asalları İçin Grup Yapıları

$n = 4$	$P = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	C_4	C_8	C_4	C_{12}	$C_2 \times C_8$	Sin.	$C_2 \times C_{12}$	C_{20}	C_{24}	C_{28}	C_{40}	C_{48}	$C_2 \times C_{20}$	$C_2 \times C_{24}$
$\alpha = 2$	Sin.	C_4	C_{12}	Sin.	C_{20}	$C_4 \times C_4$	C_{16}	C_{20}	$C_2 \times C_{12}$	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_2 \times C_{24}$	C_{40}	C_{60}
$\alpha = 3$		$C_2 \times C_4$	Sin.	$C_2 \times C_4$	$C_2 \times C_8$	$C_2 \times C_{12}$	$C_2 \times C_8$	$C_2 \times C_{12}$	$C_4 \times C_8$	$C_2 \times C_{16}$	$C_4 \times C_8$	$C_2 \times C_{20}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 4$		Sin.	$C_2 \times C_4$	C_{12}	Sin.	C_{16}	C_{28}	C_{28}	$C_4 \times C_8$	C_{36}	$C_2 \times C_{16}$	C_{32}	C_{44}	$C_2 \times C_{20}$
$\alpha = 5$			$C_2 \times C_4$	$C_2 \times C_8$	$C_4 \times C_4$	$C_4 \times C_4$	$C_2 \times C_8$	$C_2 \times C_{12}$	$C_4 \times C_8$	$C_2 \times C_{16}$	$C_4 \times C_{12}$	$C_4 \times C_8$	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 6$			C_8	$C_2 \times C_4$	C_{12}	C_{12}	C_{20}	C_{20}	C_{32}	$C_2 \times C_{20}$	C_{44}	C_{36}	$C_2 \times C_{24}$	$C_2 \times C_{28}$
$\alpha = 7$				$C_2 \times C_8$	$C_4 \times C_4$	C_{20}	C_{20}	C_{24}	C_{24}	$C_2 \times C_{16}$	C_{40}	$C_4 \times C_{12}$	C_{48}	C_{52}
$\alpha = 8$				C_8	$C_2 \times C_4$	C_{24}	C_{24}	C_{28}	$C_2 \times C_{12}$	$C_2 \times C_{20}$	C_{36}	C_{40}	Sin.	C_{44}
$\alpha = 9$				C_{12}	C_8	$C_2 \times C_8$	C_{12}	C_{28}	Sin.	C_{28}	$C_4 \times C_8$	C_{40}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 10$				C_{16}	C_{16}	$C_2 \times C_{12}$	$C_2 \times C_{12}$	Sin.	$C_4 \times C_8$	C_{28}	C_{40}	C_{48}	C_{52}	C_{40}
$\alpha = 11$					C_{12}	C_{20}	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{28}	C_{40}	C_{32}	C_{36}	C_{52}	$C_2 \times C_{24}$
$\alpha = 12$					C_{16}	C_{12}	C_{16}	$C_2 \times C_{16}$	C_{36}	$C_2 \times C_{12}$	C_{40}	C_{36}	$C_2 \times C_{20}$	C_{44}
$\alpha = 13$						C_{16}	Sin.	$C_2 \times C_{12}$	$C_2 \times C_{16}$	C_{40}	C_{36}	$C_4 \times C_{12}$	C_{52}	$C_2 \times C_{24}$
$\alpha = 14$						$C_4 \times C_4$	$C_2 \times C_{12}$	$C_2 \times C_{16}$	$C_2 \times C_{12}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{28}$	$C_2 \times C_{28}$
$\alpha = 15$						C_{24}	C_{24}	C_{24}	$C_2 \times C_{12}$	C_{24}	$C_3 \times C_{12}$	$C_2 \times C_{20}$	C_{36}	$C_2 \times C_{20}$
$\alpha = 16$						$C_2 \times C_8$	C_{20}	$C_2 \times C_8$	$C_4 \times C_8$	$C_2 \times C_{12}$	C_{40}	C_{48}	C_{44}	C_{60}
$\alpha = 17$							$C_2 \times C_8$	C_{32}	C_{36}	$C_2 \times C_{20}$	C_{36}	C_{36}	$C_2 \times C_{24}$	C_{60}
$\alpha = 18$							$C_2 \times C_8$	$C_2 \times C_{12}$	$C_2 \times C_{20}$	$C_2 \times C_{12}$	$C_2 \times C_{20}$	$C_2 \times C_{16}$	$C_2 \times C_{16}$	$C_2 \times C_{24}$
$\alpha = 19$								$C_2 \times C_8$	C_{20}	$C_3 \times C_{12}$	$C_4 \times C_8$	$C_4 \times C_8$	$C_2 \times C_{24}$	C_{56}
$\alpha = 20$								C_{24}	C_{40}	C_{36}	$C_2 \times C_{20}$	C_{40}	C_{48}	C_{48}
$\alpha = 21$								C_{16}	C_{36}	C_{24}	$C_2 \times C_{16}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$	$C_2 \times C_{20}$
$\alpha = 22$								$C_2 \times C_{12}$	$C_2 \times C_{16}$	C_{32}	C_{36}	$C_4 \times C_{12}$	$C_2 \times C_{20}$	$C_2 \times C_{24}$
$\alpha = 23$									C_{24}	$C_2 \times C_{12}$	$C_2 \times C_{20}$	Sin.	$C_2 \times C_{16}$	C_{56}
$\alpha = 24$									C_{24}	C_{32}	C_{44}	$C_4 \times C_8$	$C_2 \times C_{20}$	$C_2 \times C_{24}$
$\alpha = 25$									$C_4 \times C_8$	C_{28}	C_{48}	$C_2 \times C_{24}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 26$									C_{36}	$C_2 \times C_{16}$	$C_4 \times C_8$	C_{44}	C_{48}	C_{48}
$\alpha = 27$									C_{28}	C_{32}	$C_4 \times C_8$	$C_4 \times C_{12}$	C_{48}	C_{36}
$\alpha = 28$									C_{32}	C_{36}	C_{32}	$C_2 \times C_{20}$	C_{56}	C_{36}
$\alpha = 29$										Sin.	$C_2 \times C_{20}$	C_{44}	$C_2 \times C_{24}$	$C_2 \times C_{28}$
$\alpha = 30$										$C_2 \times C_{16}$	Sin.	C_{52}	C_{40}	C_{40}
$\alpha = 31$											$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{20}$	$C_2 \times C_{24}$
$\alpha = 32$											C_{28}	$C_2 \times C_{16}$	$C_2 \times C_{20}$	C_{52}
$\alpha = 33$											$C_2 \times C_{24}$	$C_4 \times C_{12}$	$C_2 \times C_{28}$	$C_2 \times C_{24}$
$\alpha = 34$											$C_2 \times C_{24}$	C_{52}	C_{40}	$C_2 \times C_{28}$
$\alpha = 35$											C_{28}	C_{44}	C_{44}	C_{48}
$\alpha = 36$											C_{48}	C_{40}	C_{52}	C_{52}
$\alpha = 37$												C_{48}	C_{32}	C_{44}
$\alpha = 38$												C_{44}	$C_3 \times C_{12}$	C_{40}
$\alpha = 39$												$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{28}$
$\alpha = 40$												C_{32}	C_{36}	C_{56}
$\alpha = 41$													C_{36}	C_{48}
$\alpha = 42$													C_{40}	C_{36}
$\alpha = 43$														C_{48}
$\alpha = 44$														Sin.
$\alpha = 45$														$C_2 \times C_{28}$
$\alpha = 46$														$C_2 \times C_{20}$

$n = 5$	$P = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	C_5	C_5	C_{10}	Sin.	C_{10}	C_{20}	C_{20}	C_{25}	C_{30}	C_{25}	C_{35}	C_{50}	C_{50}	$C_2 \times C_{20}$
$\alpha = 2$	C_5	C_{10}	C_5	C_{10}	C_{15}	C_{15}	Sin.	C_{25}	C_{35}	C_{40}	$C_2 \times C_{20}$	$C_5 \times C_{10}$	C_{40}	$C_2 \times C_{20}$
$\alpha = 3$		Sin.	C_5	C_{10}	C_{15}	C_{20}	C_{25}	C_{30}	C_{20}	C_{35}	$C_2 \times C_{20}$	C_{50}	C_{45}	C_{50}
$\alpha = 4$		C_5	C_{10}	C_{15}	C_{15}	C_{10}	$C_2 \times C_{10}$	C_{20}	Sin.	C_{35}	C_{30}	C_{40}	C_{55}	C_{35}
$\alpha = 5$			C_{10}	C_{10}	$C_2 \times C_{10}$	C_{25}	C_{25}	$C_2 \times C_{10}$	C_{30}	Sin.	C_{45}	C_{45}	C_{35}	C_{50}
$\alpha = 6$			C_{10}	C_{15}	C_{15}	C_{15}	C_{25}	C_{20}	C_{30}	Sin.	$C_2 \times C_{20}$	C_{40}	C_{50}	C_{55}
$\alpha = 7$				C_{10}	C_{10}	$C_2 \times C_{10}$	C_{15}	C_{15}	Sin.	$C_2 \times C_{20}$	C_{30}	C_{45}	C_{50}	C_{55}
$\alpha = 8$				C_{15}	C_{10}	C_{15}	C_{15}	C_{30}	C_{30}	C_{30}	C_{40}	C_{45}	$C_2 \times C_{20}$	C_{60}
$\alpha = 9$				C_{15}	C_{20}	C_{15}	Sin.	$C_2 \times C_{10}$	C_{40}	C_{30}	C_{30}	$C_5 \times C_{10}$	C_{45}	C_{45}
$\alpha = 10$				Sin.	C_{20}	C_{25}	C_{15}	C_{30}	C_{25}	C_{35}	C_{35}	C_{40}	C_{40}	C_{50}
$\alpha = 11$					C_{10}	C_{20}	C_{20}	C_{25}	C_{30}	$C_5 \times C_5$	C_{35}	$C_5 \times C_{10}$	C_{50}	$C_2 \times C_{20}$
$\alpha = 12$					C_{10}	$C_2 \times C_{10}$	C_{20}	C_{30}	$C_2 \times C_{10}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}	C_{50}
$\alpha = 13$						$C_2 \times C_{10}$	C_{20}	C_{15}	C_{25}	C_{30}	C_{30}	C_{30}	$C_3 \times C_{15}$	C_{40}
$\alpha = 14$						C_{15}	$C_2 \times C_{10}$	C_{20}	C_{35}	$C_5 \times C_5$	C_{40}	Sin.	C_{45}	C_{50}
$\alpha = 15$						C_{15}	C_{25}	C_{30}	C_{30}	C_{40}	C_{35}	C_{40}	C_{55}	C_{40}
$\alpha = 16$						C_{20}	C_{20}	C_{30}	C_{40}	C_{30}	C_{40}	C_{40}	$C_2 \times C_{20}$	C_{45}
$\alpha = 17$							C_{15}	C_{20}	$C_2 \times C_{20}$	C_{40}	C_{30}	$C_2 \times C_{20}$	C_{35}	$C_2 \times C_{20}$
$\alpha = 18$							C_{20}	C_{20}	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}
$\alpha = 19$								C_{20}	C_{20}	C_{30}	C_{40}	C_{35}	C_{45}	$C_2 \times C_{30}$
$\alpha = 20$								C_{30}	C_{25}	C_{40}	C_{45}	$C_5 \times C_{10}$	C_{55}	C_{55}
$\alpha = 21$								C_{30}	C_{30}	$C_5 \times C_5$	C_{30}	C_{45}	C_{40}	C_{45}
$\alpha = 22$								C_{25}	C_{35}	$C_2 \times C_{20}$	C_{45}	C_{30}	$C_2 \times C_{20}$	C_{60}
$\alpha = 23$									C_{30}	C_{35}	C_{40}	C_{40}	C_{45}	$C_2 \times C_{20}$
$\alpha = 24$									C_{30}	C_{30}	C_{45}	C_{45}	C_{35}	C_{60}
$\alpha = 25$									C_{35}	C_{25}	$C_3 \times C_{15}$	$C_2 \times C_{20}$	C_{40}	C_{40}
$\alpha = 26$									C_{25}	C_{25}	C_{40}	$C_5 \times C_{10}$	$C_2 \times C_{20}$	C_{45}
$\alpha = 27$									C_{30}	C_{30}	C_{40}	C_{50}	C_{50}	C_{45}
$\alpha = 28$									C_{30}	$C_5 \times C_5$	C_{30}	C_{35}	C_{45}	C_{50}
$\alpha = 29$										C_{30}	C_{40}	C_{45}	C_{45}	C_{40}
$\alpha = 30$										C_{25}	C_{40}	C_{40}	C_{40}	C_{55}
$\alpha = 31$											C_{50}	C_{35}	$C_2 \times C_{20}$	C_{50}
$\alpha = 32$											C_{35}	$C_5 \times C_{10}$	C_{55}	C_{60}
$\alpha = 33$											C_{30}	C_{30}	$C_3 \times C_{15}$	C_{45}
$\alpha = 34$											$C_3 \times C_{15}$	C_{40}	C_{35}	C_{40}
$\alpha = 35$											C_{40}	C_{45}	C_{50}	C_{35}
$\alpha = 36$											C_{35}	C_{30}	C_{40}	C_{55}
$\alpha = 37$												C_{35}	C_{40}	C_{45}
$\alpha = 38$												Sin.	$C_2 \times C_{20}$	C_{45}
$\alpha = 39$												C_{45}	C_{50}	C_{55}
$\alpha = 40$												C_{50}	C_{45}	C_{45}
$\alpha = 41$													$C_2 \times C_{20}$	C_{60}
$\alpha = 42$													C_{50}	$C_2 \times C_{30}$
$\alpha = 43$														C_{50}
$\alpha = 44$														C_{45}
$\alpha = 45$														C_{60}
$\alpha = 46$														$C_2 \times C_{20}$

$n=6$	$P=3$	$p=5$	$p=7$	$p=11$	$p=13$	$p=17$	$p=19$	$p=23$	$p=29$	$p=31$	$p=37$	$p=41$	$p=43$	$p=47$
$\alpha=1$	C_6	Sin.	C_6	$C_2\times C_6$	C_{12}	C_{24}	$C_2\times C_{12}$	C_{18}	$C_2\times C_{12}$	$C_2\times C_{18}$	$C_3\times C_{12}$	$C_2\times C_{18}$	C_{54}	C_{54}
$\alpha=2$	Sin.	C_6	$C_2\times C_6$	C_{12}	C_{18}	C_{12}	Sin.	C_{30}	$C_2\times C_{12}$	C_{30}	C_{42}	$C_2\times C_{18}$	$C_2\times C_{24}$	C_{42}
$\alpha=3$		C_6	Sin.	C_{18}	C_{12}	C_{18}	$C_2\times C_{12}$	C_{30}	$C_2\times C_{12}$	$C_2\times C_{12}$	$C_2\times C_{18}$	C_{30}	C_{48}	$C_2\times C_{18}$
$\alpha=4$		Sin.	C_6	$C_2\times C_6$	$C_2\times C_6$	$C_2\times C_6$	$C_3\times C_6$	$C_2\times C_{12}$	C_{24}	C_{42}	Sin.	$C_2\times C_{24}$	$C_2\times C_{24}$	C_{54}
$\alpha=5$			C_{12}	$C_2\times C_6$	$C_2\times C_6$	$C_2\times C_6$	$C_3\times C_6$	Sin.	C_{24}	$C_6\times C_6$	C_{30}	C_{36}	C_{36}	C_{36}
$\alpha=6$			Sin.	Sin.	C_{18}	C_{18}	$C_2\times C_6$	C_{18}	C_{24}	C_{36}	C_{30}	$C_2\times C_{18}$	$C_2\times C_{24}$	$C_2\times C_{18}$
$\alpha=7$				C_{12}	$C_3\times C_6$	$C_2\times C_6$	$C_3\times C_6$	$C_2\times C_{12}$	C_{36}	$C_6\times C_6$	$C_3\times C_{12}$	$C_2\times C_{18}$	$C_3\times C_{12}$	$C_2\times C_{30}$
$\alpha=8$				C_{12}	$C_3\times C_6$	C_{12}	$C_2\times C_{12}$	$C_2\times C_{12}$	C_{30}	C_{30}	$C_6\times C_6$	$C_2\times C_{18}$	C_{48}	C_{54}
$\alpha=9$				C_6	$C_2\times C_6$	$C_2\times C_{12}$	C_{18}	C_{18}	C_{24}	$C_2\times C_{18}$	$C_3\times C_{12}$	Sin.	$C_3\times C_{18}$	$C_2\times C_{24}$
$\alpha=10$				Sin.	Sin.	$C_2\times C_{12}$	C_{24}	$C_2\times C_{12}$	C_{30}	$C_6\times C_6$	C_{36}	C_{48}	C_{42}	$C_2\times C_{24}$
$\alpha=11$					$C_2\times C_6$	C_{18}	C_{18}	$C_2\times C_{12}$	C_{30}	C_{24}	$C_6\times C_6$	C_{42}	C_{42}	$C_2\times C_{24}$
$\alpha=12$					Sin.	C_{18}	$C_2\times C_{12}$	C_{18}	$C_2\times C_{12}$	$C_3\times C_{12}$	$C_4\times C_{12}$	$C_2\times C_{18}$	$C_2\times C_{24}$	$C_2\times C_{30}$
$\alpha=13$						C_{24}	C_{12}	C_{30}	$C_2\times C_{18}$	$C_2\times C_{12}$	C_{42}	C_{42}	$C_3\times C_{18}$	$C_2\times C_{24}$
$\alpha=14$						$C_2\times C_{12}$	$C_2\times C_{12}$	C_{24}	$C_2\times C_{18}$	$C_2\times C_{12}$	C_{30}	C_{42}	$C_6\times C_6$	$C_2\times C_{24}$
$\alpha=15$						Sin.	C_{24}	C_{24}	$C_2\times C_{12}$	C_{36}	$C_2\times C_{18}$	C_{42}	C_{42}	$C_2\times C_{24}$
$\alpha=16$						Sin.	$C_3\times C_6$	$C_2\times C_{12}$	Sin.	$C_2\times C_{12}$	C_{36}	$C_4\times C_{12}$	$C_6\times C_6$	$C_2\times C_{24}$
$\alpha=17$							$C_2\times C_{12}$	$C_2\times C_{12}$	C_{30}	$C_3\times C_{12}$	$C_6\times C_6$	$C_2\times C_{24}$	C_{54}	C_{42}
$\alpha=18$							Sin.	C_{30}	$C_2\times C_{18}$	$C_6\times C_6$	$C_2\times C_{18}$	C_{48}	$C_2\times C_{24}$	$C_2\times C_{24}$
$\alpha=19$								$C_2\times C_{12}$	C_{30}	C_{30}	$C_2\times C_{24}$	$C_2\times C_{24}$	Sin.	$C_2\times C_{24}$
$\alpha=20$								$C_2\times C_{12}$	C_{36}	$C_2\times C_{18}$	$C_2\times C_{18}$	C_{36}	$C_2\times C_{24}$	C_{36}
$\alpha=21$								C_{24}	$C_2\times C_{18}$	$C_3\times C_{12}$	$C_2\times C_{18}$	$C_2\times C_{18}$	$C_2\times C_{18}$	C_{42}
$\alpha=22$								Sin.	$C_2\times C_{18}$	$C_2\times C_{12}$	$C_6\times C_6$	C_{54}	$C_3\times C_{12}$	$C_2\times C_{24}$
$\alpha=23$									$C_2\times C_{12}$	$C_2\times C_{12}$	$C_6\times C_6$	$C_2\times C_{24}$	$C_2\times C_{18}$	C_{60}
$\alpha=24$									C_{36}	Sin.	C_{30}	C_{42}	$C_3\times C_{18}$	C_{54}
$\alpha=25$									C_{36}	C_{42}	$C_2\times C_{24}$	C_{48}	$C_3\times C_{18}$	$C_2\times C_{24}$
$\alpha=26$									$C_2\times C_{18}$	C_{24}	C_{36}	$C_2\times C_{18}$	$C_2\times C_{24}$	Sin.
$\alpha=27$									C_{30}	$C_3\times C_{12}$	C_{48}	C_{42}	$C_2\times C_{24}$	$C_2\times C_{30}$
$\alpha=28$									Sin.	C_{30}	$C_6\times C_6$	$C_2\times C_{24}$	C_{36}	C_{54}
$\alpha=29$										C_{36}	$C_2\times C_{24}$	C_{42}	$C_3\times C_{12}$	C_{48}
$\alpha=30$										Sin.	C_{48}	$C_2\times C_{24}$	$C_2\times C_{24}$	C_{36}
$\alpha=31$											C_{42}	C_{48}	$C_6\times C_6$	C_{48}
$\alpha=32$											$C_2\times C_{18}$	$C_4\times C_{12}$	C_{48}	C_{42}
$\alpha=33$											C_{36}	$C_4\times C_{12}$	C_{48}	$C_2\times C_{24}$
$\alpha=34$											$C_3\times C_{12}$	C_{42}	$C_2\times C_{24}$	C_{54}
$\alpha=35$											C_{42}	C_{30}	$C_2\times C_{24}$	$C_2\times C_{24}$
$\alpha=36$											Sin.	C_{36}	C_{42}	C_{42}
$\alpha=37$												$C_2\times C_{18}$	C_{36}	$C_2\times C_{18}$
$\alpha=38$												C_{54}	$C_6\times C_6$	C_{48}
$\alpha=39$												C_{36}	$C_3\times C_{12}$	$C_2\times C_{24}$
$\alpha=40$												Sin.	$C_2\times C_{24}$	C_{48}
$\alpha=41$													$C_2\times C_{18}$	C_{60}
$\alpha=42$													Sin.	C_{42}
$\alpha=43$														C_{60}
$\alpha=44$														C_{48}
$\alpha=45$														$C_2\times C_{24}$
$\alpha=46$														Sin.

$n=7$	$P=3$	$p=5$	$p=7$	$p=11$	$p=13$	$p=17$	$p=19$	$p=23$	$p=29$	$p=31$	$p=37$	$p=41$	$p=43$	$p=47$
$\alpha=1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha=2$	C_7	C_7	C_7	C_{14}	Sin.	C_{21}	C_{14}	C_{28}	C_{28}	$C_2\times C_{14}$	C_{35}	C_{42}	$C_7\times C_7$	C_{35}
$\alpha=3$		C_7	C_7	C_{14}	C_{14}	C_{21}	C_{21}	C_{28}	Sin.	C_{28}	C_{35}	C_{49}	C_{35}	C_{49}
$\alpha=4$		C_7	C_7	C_7	C_{21}	C_{14}	C_{21}	$C_2\times C_{14}$	C_{35}	C_{42}	C_{28}	C_{42}	Sin.	C_{49}
$\alpha=5$			Sin.	C_{14}	C_{14}	C_{14}	C_{14}	C_{21}	C_{21}	C_{28}	C_{42}	C_{35}	C_{49}	$C_2\times C_{28}$
$\alpha=6$			C_7	C_{14}	C_{14}	C_{14}	C_{21}	C_{21}	C_{28}	C_{21}	C_{49}	Sin.	$C_7\times C_7$	C_{56}
$\alpha=7$				C_7	Sin.	C_{21}	C_{21}	C_{21}	C_{21}	C_{28}	C_{49}	C_{42}	$C_7\times C_7$	$C_2\times C_{28}$
$\alpha=8$				C_{14}	C_{14}	C_{21}	$C_2\times C_{14}$	C_{28}	C_{35}	C_{35}	C_{28}	Sin.	$C_7\times C_7$	C_{42}
$\alpha=9$				C_7	C_{14}	C_{21}	C_{21}	C_{21}	$C_2\times C_{14}$	C_{28}	C_{42}	C_{35}	C_{42}	C_{42}
$\alpha=10$				C_{14}	C_7	C_{14}	C_{14}	C_{21}	C_{35}	C_{42}	C_{28}	C_{35}	C_{49}	C_{56}
$\alpha=11$					C_{14}	C_{14}	C_{28}	$C_2\times C_{14}$	$C_2\times C_{14}$	C_{28}	$C_2\times C_{14}$	C_{42}	C_{42}	C_{42}
$\alpha=12$					Sin.	C_{21}	C_{21}	$C_2\times C_{14}$	C_{21}	C_{42}	C_{28}	C_{42}	C_{42}	$C_2\times C_{28}$
$\alpha=13$						C_{21}	C_{28}	$C_2\times C_{14}$	C_{21}	C_{28}	C_{35}	C_{35}	C_{35}	C_{56}
$\alpha=14$						C_{21}	C_{14}	C_{21}	Sin.	C_{42}	$C_2\times C_{14}$	C_{42}	Sin.	C_{42}
$\alpha=15$						C_{14}	C_{21}	$C_2\times C_{14}$	C_{28}	C_{28}	C_{42}	C_{42}	C_{35}	C_{56}
$\alpha=16$						C_{21}	C_{14}	$C_2\times C_{14}$	C_{35}	$C_2\times C_{14}$	C_{35}	C_{49}	C_{42}	C_{42}
$\alpha=17$							C_{28}	C_{21}	$C_2\times C_{14}$	C_{35}	$C_2\times C_{14}$	C_{35}	$C_7\times C_7$	$C_2\times C_{28}$
$\alpha=18$							C_{14}	$C_2\times C_{14}$	$C_2\times C_{14}$	C_{28}	C_{35}	C_{42}	C_{49}	C_{42}
$\alpha=19$								C_{21}	C_{35}	C_{42}	C_{35}	C_{42}	C_{49}	C_{56}
$\alpha=20$								C_{21}	Sin.	C_{28}	C_{42}	C_{49}	C_{42}	C_{42}
$\alpha=21$								$C_2\times C_{14}$	C_{21}	C_{35}	C_{28}	C_{42}	C_{35}	$C_2\times C_{28}$
$\alpha=22$								$C_2\times C_{14}$	$C_2\times C_{14}$	C_{35}	C_{49}	C_{42}	$C_7\times C_7$	C_{42}
$\alpha=23$									C_{28}	C_{28}	C_{42}	C_{35}	C_{42}	C_{49}
$\alpha=24$									C_{21}	C_{42}	C_{28}	C_{49}	$C_2\times C_{28}$	C_{35}
$\alpha=25$									C_{28}	C_{28}	C_{42}	C_{42}	C_{35}	C_{42}
$\alpha=26$									$C_2\times C_{14}$	$C_2\times C_{14}$	C_{42}	C_{42}	C_{42}	C_{56}
$\alpha=27$									C_{35}	C_{28}	C_{49}	C_{42}	C_{56}	C_{42}
$\alpha=28$									C_{28}	C_{35}	C_{42}	C_{49}	$C_2\times C_{28}$	C_{56}
$\alpha=29$										C_{35}	C_{42}	C_{42}	C_{42}	$C_2\times C_{28}$
$\alpha=30$										$C_2\times C_{14}$	$C_2\times C_{14}$	C_{49}	C_{42}	C_{42}
$\alpha=31$											C_{35}	C_{42}	C_{49}	C_{49}
$\alpha=32$											C_{35}	C_{42}	C_{49}	C_{49}
$\alpha=33$											C_{42}	C_{42}	Sin.	C_{42}
$\alpha=34$											C_{42}	C_{42}	C_{35}	C_{42}
$\alpha=35$											C_{42}	Sin.	$C_2\times C_{28}$	$C_2\times C_{28}$
$\alpha=36$											C_{35}	C_{42}	C_{56}	C_{49}
$\alpha=37$												C_{42}	$C_7\times C_7$	C_{42}
$\alpha=38$												C_{42}	C_{56}	C_{42}
$\alpha=39$												C_{42}	C_{42}	$C_2\times C_{28}$
$\alpha=40$												C_{42}	C_{42}	C_{56}
$\alpha=41$													C_{42}	C_{42}
$\alpha=42$													$C_7\times C_7$	C_{42}
$\alpha=43$														C_{56}
$\alpha=44$														$C_2\times C_{28}$
$\alpha=45$														C_{42}
$\alpha=46$														C_{35}

$n = 9$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	Sin.	C_9	C_9	C_9	C_{18}	C_{18}	C_{18}	C_{18}	$C_2 \times C_{18}$	C_{27}	C_{36}	C_{36}	C_{54}	C_{54}
$\alpha = 3$		C_9	Sin.	C_9	C_9	Sin.	C_{18}	C_{18}	C_{36}	C_{36}	C_{27}	C_{54}	C_{45}	C_{36}
$\alpha = 4$		C_9	C_9	C_{18}	Sin.	C_{18}	Sin.	C_{27}	$C_2 \times C_{18}$	C_{36}	C_{45}	C_{54}	C_{36}	C_{54}
$\alpha = 5$			Sin.	C_9	C_9	C_{18}	C_{27}	C_{18}	C_{36}	$C_2 \times C_{18}$	C_{36}	C_{45}	C_{45}	C_{45}
$\alpha = 6$			C_9	C_9	C_9	C_{18}	Sin.	C_{27}	C_{27}	Sin.	$C_2 \times C_{18}$	$C_2 \times C_{18}$	C_{45}	C_{36}
$\alpha = 7$				C_{18}	C_{18}	C_{18}	C_{18}	C_{27}	C_{36}	$C_2 \times C_{18}$	$C_2 \times C_{18}$	C_{36}	Sin.	C_{36}
$\alpha = 8$				C_9	C_{18}	Sin.	Sin.	C_{18}	$C_2 \times C_{18}$	$C_3 \times C_9$	C_{36}	$C_2 \times C_{18}$	C_{45}	C_{54}
$\alpha = 9$				C_{18}	C_{18}	C_{18}	C_{18}	C_{27}	C_{36}	$C_3 \times C_9$	C_{36}	C_{45}	$C_2 \times C_{18}$	C_{54}
$\alpha = 10$				C_9	Sin.	C_{18}	C_{18}	C_{18}	C_{36}	C_{36}	C_{45}	C_{45}	$C_3 \times C_{18}$	C_{45}
$\alpha = 11$					C_{18}	C_{18}	$C_3 \times C_9$	C_{18}	C_{27}	C_{36}	Sin.	C_{54}	C_{36}	$C_2 \times C_{18}$
$\alpha = 12$					C_{18}	Sin.	Sin.	C_{18}	C_{27}	$C_3 \times C_9$	C_{45}	C_{45}	$C_3 \times C_{18}$	C_{45}
$\alpha = 13$						C_{18}	$C_3 \times C_9$	C_{18}	C_{27}	C_{27}	C_{27}	$C_2 \times C_{18}$	C_{54}	C_{54}
$\alpha = 14$						C_{18}	C_{27}	C_{27}	C_{36}	$C_3 \times C_9$	C_{45}	C_{45}	C_{36}	$C_2 \times C_{18}$
$\alpha = 15$						C_{18}	Sin.	C_{27}	$C_2 \times C_{18}$	C_{36}	$C_3 \times C_9$	C_{36}	C_{45}	C_{45}
$\alpha = 16$						C_{18}	C_{27}	C_{18}	C_{36}	C_{27}	C_{36}	$C_2 \times C_{18}$	$C_2 \times C_{18}$	C_{54}
$\alpha = 17$							$C_3 \times C_9$	C_{18}	C_{36}	C_{36}	C_{45}	$C_2 \times C_{18}$	C_{45}	C_{45}
$\alpha = 18$							C_{18}	C_{27}	C_{36}	C_{27}	C_{27}	C_{45}	C_{45}	$C_2 \times C_{18}$
$\alpha = 19$								C_{27}	$C_2 \times C_{18}$	$C_3 \times C_9$	C_{36}	C_{45}	$C_3 \times C_{18}$	C_{54}
$\alpha = 20$								C_{27}	C_{36}	C_{27}	Sin.	C_{54}	$C_2 \times C_{18}$	C_{54}
$\alpha = 21$								C_{18}	C_{27}	C_{36}	C_{36}	C_{36}	C_{45}	C_{36}
$\alpha = 22$								C_{18}	C_{27}	$C_3 \times C_9$	$C_2 \times C_{18}$	C_{45}	C_{54}	C_{45}
$\alpha = 23$									C_{27}	$C_2 \times C_{18}$	C_{36}	$C_2 \times C_{18}$	C_{36}	C_{36}
$\alpha = 24$									C_{36}	C_{36}	C_{36}	$C_2 \times C_{18}$	$C_3 \times C_{18}$	C_{54}
$\alpha = 25$									C_{27}	$C_3 \times C_9$	Sin.	C_{45}	C_{54}	C_{54}
$\alpha = 26$									C_{27}	Sin.	$C_2 \times C_{18}$	C_{45}	$C_3 \times C_{18}$	C_{45}
$\alpha = 27$									C_{36}	$C_3 \times C_9$	Sin.	C_{54}	C_{45}	C_{54}
$\alpha = 28$									$C_2 \times C_{18}$	$C_3 \times C_9$	$C_2 \times C_{18}$	C_{54}	$C_3 \times C_{18}$	C_{36}
$\alpha = 29$										C_{36}	$C_3 \times C_9$	C_{45}	C_{36}	C_{45}
$\alpha = 30$										C_{27}	C_{45}	$C_2 \times C_{18}$	C_{36}	C_{45}
$\alpha = 31$											C_{36}	C_{36}	$C_3 \times C_{18}$	C_{54}
$\alpha = 32$											C_{36}	C_{36}	C_{45}	C_{36}
$\alpha = 33$											$C_3 \times C_9$	C_{36}	C_{36}	C_{45}
$\alpha = 34$											$C_2 \times C_{18}$	C_{36}	C_{54}	C_{45}
$\alpha = 35$											Sin.	$C_2 \times C_{18}$	$C_3 \times C_{18}$	C_{45}
$\alpha = 36$											C_{36}	C_{36}	C_{45}	C_{54}
$\alpha = 37$												C_{36}	Sin.	C_{45}
$\alpha = 38$												C_{36}	C_{45}	C_{45}
$\alpha = 39$												C_{45}	$C_3 \times C_{18}$	C_{36}
$\alpha = 40$												C_{36}	C_{36}	C_{36}
$\alpha = 41$													C_{36}	C_{54}
$\alpha = 42$													C_{54}	C_{54}
$\alpha = 43$														C_{54}
$\alpha = 44$														C_{45}
$\alpha = 45$														C_{54}
$\alpha = 46$														C_{54}

$n = 10$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.	Sin.
$\alpha = 2$	Sin.	C_{10}	C_{10}	Sin.	C_{10}	$C_2 \times C_{10}$	C_{20}	C_{30}	$C_2 \times C_{10}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}	C_{50}
$\alpha = 3$		Sin.	C_{10}	C_{10}	C_{10}	$C_2 \times C_{10}$	C_{20}	C_{20}	Sin.	C_{30}	$C_2 \times C_{20}$	C_{50}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 4$		T. D	Sin.	Sin.	C_{10}	C_{20}	$C_2 \times C_{10}$	C_{30}	C_{30}	C_{30}	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 5$			C_{10}	T. D	C_{20}	$C_2 \times C_{10}$	C_{20}	C_{20}	C_{30}	C_{30}	C_{30}	$C_5 \times C_{10}$	C_{50}	$C_2 \times C_{20}$
$\alpha = 6$			C_{10}	Sin.	C_{10}	$C_2 \times C_{10}$	T. D	C_{20}	$C_2 \times C_{20}$	C_{30}	C_{30}	C_{40}	C_{40}	C_{40}
$\alpha = 7$				C_{10}	Sin.	C_{10}	$C_2 \times C_{10}$	C_{30}	T. D	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{30}$
$\alpha = 8$				C_{10}	$C_2 \times C_{10}$	$C_2 \times C_{10}$	C_{20}	C_{30}	C_{20}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	T. D	$C_2 \times C_{20}$	C_{50}
$\alpha = 9$				T. D	C_{10}	Sin.	$C_2 \times C_{10}$	C_{20}	$C_2 \times C_{10}$	$C_2 \times C_{20}$	C_{40}	$C_5 \times C_{10}$	$C_2 \times C_{20}$	C_{40}
$\alpha = 10$				C_{10}	$C_2 \times C_{10}$	C_{20}	Sin.	$C_2 \times C_{10}$	$C_2 \times C_{10}$	$C_2 \times C_{20}$	C_{40}	C_{50}	C_{50}	C_{50}
$\alpha = 11$					$C_2 \times C_{10}$	$C_2 \times C_{10}$	C_{20}	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{60}
$\alpha = 12$					C_{20}	$C_2 \times C_{10}$	Sin.	Sin.	Sin.	$C_2 \times C_{20}$	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}
$\alpha = 13$						C_{20}	C_{20}	C_{20}	C_{40}	C_{40}	C_{40}	C_{40}	$C_2 \times C_{20}$	C_{50}
$\alpha = 14$						$C_2 \times C_{10}$	$C_2 \times C_{10}$	C_{20}	C_{20}	T. D	C_{40}	$C_2 \times C_{20}$	C_{50}	$C_2 \times C_{20}$
$\alpha = 15$						C_{20}	$C_2 \times C_{10}$	$C_2 \times C_{10}$	Sin.	C_{40}	$C_2 \times C_{20}$	C_{30}	C_{40}	$C_2 \times C_{20}$
$\alpha = 16$						$C_2 \times C_{10}$	T. D	$C_2 \times C_{10}$	C_{30}	Sin.	$C_2 \times C_{20}$	C_{30}	C_{50}	C_{50}
$\alpha = 17$							Sin.	$C_2 \times C_{10}$	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 18$							$C_2 \times C_{10}$	C_{30}	C_{30}	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	C_{50}	C_{60}
$\alpha = 19$								C_{30}	C_{30}	C_{30}	Sin.	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 20$								$C_2 \times C_{10}$	C_{30}	T. D	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}	C_{60}
$\alpha = 21$								C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{30}	Sin.	$C_2 \times C_{20}$	$C_2 \times C_{30}$
$\alpha = 22$								$C_2 \times C_{10}$	C_{30}	Sin.	C_{50}	$C_2 \times C_{20}$	Sin.	$C_2 \times C_{20}$
$\alpha = 23$									C_{30}	C_{30}	C_{30}	$C_5 \times C_{10}$	$C_2 \times C_{20}$	C_{50}
$\alpha = 24$									C_{30}	C_{40}	C_{30}	Sin.	C_{50}	Sin.
$\alpha = 25$									T. D	Sin.	$C_2 \times C_{20}$	C_{50}	$C_2 \times C_{20}$	C_{40}
$\alpha = 26$									C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_5 \times C_{10}$	$C_2 \times C_{20}$	C_{60}
$\alpha = 27$									C_{30}	C_{30}	$C_2 \times C_{20}$	$C_5 \times C_{10}$	$C_2 \times C_{20}$	C_{60}
$\alpha = 28$									C_{30}	C_{30}	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{30}$
$\alpha = 29$										C_{40}	C_{40}	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{30}$
$\alpha = 30$										$C_2 \times C_{20}$	$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 31$											C_{40}	$C_2 \times C_{20}$	C_{50}	$C_2 \times C_{30}$
$\alpha = 32$											C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 33$											$C_2 \times C_{20}$	C_{30}	$C_2 \times C_{20}$	$C_2 \times C_{30}$
$\alpha = 34$											$C_2 \times C_{20}$	C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 35$											$C_2 \times C_{20}$	C_{50}	C_{40}	$C_2 \times C_{20}$
$\alpha = 36$											C_{40}	T. D	$C_2 \times C_{20}$	C_{50}
$\alpha = 37$												$C_5 \times C_{10}$	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 38$												Sin.	C_{50}	$C_2 \times C_{20}$
$\alpha = 39$												C_{40}	$C_2 \times C_{20}$	C_{40}
$\alpha = 40$												C_{40}	$C_2 \times C_{20}$	$C_2 \times C_{20}$
$\alpha = 41$													C_{40}	$C_2 \times C_{20}$
$\alpha = 42$													C_{40}	C_{40}
$\alpha = 43$														C_{60}
$\alpha = 44$														$C_2 \times C_{20}$
$\alpha = 45$														C_{50}
$\alpha = 46$														$C_2 \times C_{20}$

$n = 12$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$	$p = 19$	$p = 23$	$p = 29$	$p = 31$	$p = 37$	$p = 41$	$p = 43$	$p = 47$
$\alpha = 1$	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D	T. D
$\alpha = 2$	Sin.	Sin.	Sin.	C_{12}	Sin.	C_{12}	C_{24}	C_{24}	$C_2 \times C_{12}$	$C_3 \times C_{12}$	$C_4 \times C_{12}$	C_{36}	C_{36}	$C_2 \times C_{24}$
$\alpha = 3$		Sin.	C_{12}	C_{12}	Sin.	C_{12}	Sin.	C_{24}	C_{36}	$C_2 \times C_{12}$	Sin.	C_{48}	C_{48}	C_{48}
$\alpha = 4$		Sin.	Sin.	C_{12}	C_{12}	C_{24}	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{24}	$C_3 \times C_{12}$	Sin.	$C_4 \times C_{12}$	$C_3 \times C_{12}$	C_{60}
$\alpha = 5$			C_{12}	Sin.	C_{12}	C_{24}	C_{12}	$C_2 \times C_{12}$	C_{36}	$C_2 \times C_{12}$	$C_2 \times C_{24}$	Sin.	$C_2 \times C_{24}$	C_{48}
$\alpha = 6$			Sin.	Sin.	Sin.	$C_2 \times C_{12}$	C_{24}	$C_2 \times C_{12}$	C_{24}	$C_2 \times C_{12}$	$C_3 \times C_{12}$	C_{36}	$C_3 \times C_{12}$	C_{60}
$\alpha = 7$				Sin.	Sin.	Sin.	$C_2 \times C_{12}$	Sin.	$C_2 \times C_{12}$	$C_3 \times C_{12}$	C_{36}	$C_2 \times C_{24}$	C_{48}	C_{48}
$\alpha = 8$				C_{12}	Sin.	$C_2 \times C_{12}$	$C_2 \times C_{12}$	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{36}	$C_3 \times C_{12}$	$C_4 \times C_{12}$	$C_3 \times C_{12}$	C_{60}
$\alpha = 9$				C_{12}	C_{12}	Sin.	$C_2 \times C_{12}$	$C_2 \times C_{12}$	Sin.	Sin.	$C_2 \times C_{24}$	C_{36}	C_{36}	C_{48}
$\alpha = 10$				C_{12}	C_{12}	$C_2 \times C_{12}$	Sin.	C_{24}	C_{24}	C_{24}	C_{48}	C_{48}	$C_2 \times C_{24}$	C_{48}
$\alpha = 11$					Sin.	Sin.	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{36}	$C_2 \times C_{12}$	$C_3 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$	C_{36}
$\alpha = 12$					Sin.	$C_2 \times C_{12}$	$C_2 \times C_{12}$	Sin.	C_{24}	$C_3 \times C_{12}$	C_{48}	$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 13$						C_{24}	$C_2 \times C_{12}$	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{36}	C_{36}	$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 14$						C_{24}	C_{24}	C_{24}	C_{36}	C_{24}	$C_4 \times C_{12}$	C_{36}	$C_3 \times C_{12}$	$C_2 \times C_{24}$
$\alpha = 15$						C_{12}	C_{12}	$C_2 \times C_{12}$	Sin.	C_{36}	$C_3 \times C_{12}$	C_{48}	C_{48}	$C_2 \times C_{24}$
$\alpha = 16$						C_{12}	$C_2 \times C_{12}$	$C_2 \times C_{12}$	C_{36}	Sin.	Sin.	$C_2 \times C_{24}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 17$							Sin.	Sin.	$C_2 \times C_{12}$	C_{36}	C_{36}	$C_4 \times C_{12}$	Sin.	C_{36}
$\alpha = 18$							C_{24}	$C_2 \times C_{12}$	C_{24}	C_{24}	C_{36}	$C_2 \times C_{24}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 19$								$C_2 \times C_{12}$	C_{36}	C_{36}	Sin.	$C_4 \times C_{12}$	C_{36}	$C_2 \times C_{24}$
$\alpha = 20$								$C_2 \times C_{12}$	C_{24}	$C_3 \times C_{12}$	C_{36}	C_{48}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 21$								C_{24}	Sin.	$C_2 \times C_{12}$	C_{36}	Sin.	C_{48}	C_{36}
$\alpha = 22$								C_{24}	$C_2 \times C_{12}$	C_{24}	Sin.	C_{48}	Sin.	Sin.
$\alpha = 23$									$C_2 \times C_{12}$	Sin.	$C_3 \times C_{12}$	$C_4 \times C_{12}$	C_{48}	$C_2 \times C_{24}$
$\alpha = 24$									C_{24}	C_{36}	$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$	Sin.
$\alpha = 25$									C_{36}	$C_3 \times C_{12}$	C_{36}	$C_4 \times C_{12}$	C_{36}	$C_2 \times C_{24}$
$\alpha = 26$									C_{24}	$C_2 \times C_{12}$	C_{48}	$C_2 \times C_{24}$	$C_2 \times C_{24}$	Sin.
$\alpha = 27$									C_{36}	$C_2 \times C_{12}$	$C_3 \times C_{12}$	C_{48}	Sin.	C_{36}
$\alpha = 28$									$C_2 \times C_{12}$	$C_3 \times C_{12}$	C_{48}	C_{36}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 29$										$C_2 \times C_{12}$	$C_2 \times C_{24}$	$C_4 \times C_{12}$	C_{48}	$C_2 \times C_{24}$
$\alpha = 30$										$C_3 \times C_{12}$	$C_3 \times C_{12}$	$C_4 \times C_{12}$	$C_3 \times C_{12}$	$C_2 \times C_{24}$
$\alpha = 31$											C_{36}	$C_2 \times C_{24}$	$C_2 \times C_{24}$	C_{36}
$\alpha = 32$											$C_3 \times C_{12}$	C_{48}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 33$											$C_2 \times C_{24}$	C_{36}	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 34$											Sin.	$C_4 \times C_{12}$	$C_2 \times C_{24}$	$C_2 \times C_{24}$
$\alpha = 35$											Sin.	$C_2 \times C_{24}$	C_{36}	$C_2 \times C_{24}$
$\alpha = 36$											$C_4 \times C_{12}$	C_{36}	$C_3 \times C_{12}$	$C_2 \times C_{24}$
$\alpha = 37$												Sin.	C_{48}	C_{36}
$\alpha = 38$												$C_4 \times C_{12}$	$C_3 \times C_{12}$	C_{48}
$\alpha = 39$												C_{48}	$C_2 \times C_{24}$	C_{48}
$\alpha = 40$												C_{36}	$C_3 \times C_{12}$	C_{60}
$\alpha = 41$													C_{48}	C_{48}
$\alpha = 42$													C_{36}	C_{60}
$\alpha = 43$														C_{48}
$\alpha = 44$														C_{60}
$\alpha = 45$														C_{48}
$\alpha = 46$														$C_2 \times C_{24}$

ÖZGEÇMİŞ

Adı Soyadı : Buse ÇAPA
Doğum Yeri ve Tarihi : Eskişehir – 29.06.1988
Yabancı Dili : İngilizce

Eğitim Durumu
Lise : Eskişehir Muzaffer Çil Anadolu Lisesi – 2005
Lisans : Uludağ Üniversitesi – 2009
Yüksek Lisans : Uludağ Üniversitesi Fen Bilimleri Enstitüsü, 2011

Çalıştığı Kurum/Kurumlar ve Yıl :
İletişim :
Yayınları :

Form No: YL-05

ULUDAĞ ÜNİVERSİTESİ

TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	Buse ÇAPA
Tez Adı	Sonlu Cisimler Üzerinde Tate Normal Formlar
Enstitü	Fen Bilimleri Enstitüsü
Anabilim Dalı	Matematik
Tez Türü	Yüksek Lisans
Tez Danışman(lar)ı	Prof. Dr. Osman BİZİM
Çoğaltma (Fotokopi Çekim) izni	☒ Tezimden fotokopi çekilmesine izin veriyorum ☐ Tezimin sadece içindekiler, özet, kaynakça ve içeriğinin % 10 bölümünün fotokopi çekilmesine izin veriyorum ☐ Tezimden fotokopi çekilmesine izin vermiyorum
Yayımlama izni	☒ Tezimin elektronik ortamda yayımlanmasına izin Veriyorum ☐ Tezimin elektronik ortamda yayımlanmasının ertelenmesini istiyorum 1 yıl ☐ 2 yıl ☐ 3 yıl ☐ ☐ Tezimin elektronik ortamda yayımlanmasına izin vermiyorum

Hazırlamış olduğum tezimin belirttiğim hususlar dikkate alınarak, fikri mülkiyet haklarım saklı kalmak üzere Uludağ Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı tarafından hizmete sunulmasına izin verdiğimi beyan ederim.

Tarih : 01/06/2011

İmza :