T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

DİOPHANTİNE M-LİLERİ İLE OLUŞTURULAN ELİPTİK EĞRİLER ÜZERİNE

YÜKSEK LİSANS TEZİ

SALİH TOPÇU

TEZ DANIŞMANI
DOÇ. DR. İLKER İNAM

BİLECİK, 2022
10502274

T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

DİOPHANTİNE M-LİLERİ İLE OLUŞTURULAN ELİPTİK EĞRİLER ÜZERİNE

YÜKSEK LİSANS TEZİ

SALİH TOPÇU

TEZ DANIŞMANI
DOÇ. DR. İLKER İNAM

BİLECİK, 2022
10502274

BEYAN

"Diophantine M-lileri ile Oluşturulan Eliptik Eğriler Üzerine" adlı yüksek lisans tezinin hazırlık ve yazımı sırasında bilimsel araştırma ve etik kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmının Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunulmadığını, aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Bu çalışmanın, Bilimsel Araştırma Projeleri (BAP), TÜBİTAK veya benzeri kuruluşlarca desteklenmesi durumunda; projenin ve destekleyen kurumun adı proje numarası ile birlikte, ETİK KURUL onayı alınması durumunda ise ETİK KURUL tarih karar ve sayı bilgilerinin beyan edilmesi gerekmektedir.			
DESTEK ALINMIŞTIR		**DESTEK ALINMAMIŞTIR**	X
Destek alındı ise;			
Destekleyen kurum;			
Desteğin Türü		**Proje Numarası**	
1- BAP (Bilimsel Araştırma Projesi)			
2- TÜBİTAK			
Diğer;……			
ETİK KURUL onayı var ise;			
ETİK KURUL karar tarih/sayı:		**……/……**	

Salih TOPÇU

../../2022

İmza

ÖNSÖZ

Yüksek lisans tez dönemimde danışmanlığımı yürüten, bu tez konusunu çalışmamı sağlayan, çalışmanın yürütülmesinde bilgisi, tecrübesi ve önerileriyle beni yönlendirerek bana yol gösteren ve desteğini benden hiçbir zaman esirgemeyen kıymetli hocam Doç. Dr. İlker İNAM' a, yoğun çalışmalarım sırasında motivasyon desteği, ümit verici konuşmaları ve olağanüstü sabrı için eşime, yazım sırasında ve oluşan aksaklıklarda destek veren ve işleri yoluna koymaya gayret gösteren Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü personeline ve lisans hayatım boyunca matematik öğrenimim ve eğitimimde emekleri olan Yıldız Teknik Üniversitesi'ndeki kıymetli hocalarıma bana kattıkları her şey için teşekkürü bir borç bilirim.

Salih TOPÇU

2022

ÖZET

DİOPHANTİNE M-LİLERİ İLE OLUŞTURULAN ELİPTİK EĞRİLER ÜZERİNE

Diophantine denklemleri özellikle gündelik hayat uygulamaları ile birlikte tamsayılarla ilgili yapılan matematik çalışmalarının temelini oluşturmaktadır. Eliptik eğriler ise özellikle geniş uygulama alanına sahip olması ve üstelik Fermat'ın Son Teoremi'nin ispatında kullanılması nedeniyle son yıllarda bilim insanlarının ilgisini üzerinde tutmuştur. Bu çalışmada bu iki kavram aynı potada buluşturulmuştur. Diophantine *m*-lileri tarafından indirgenen eliptik eğrilerin rank ve torsiyon grupları araştırılmış olup derleme niteliğindeki bu çalışma *m* sayısının çeşitli değerleri için özelleşmiştir. Tez çalışması güncel bir makalenin çalışmasıyla bitmektedir.

Anahtar Kelimeler: Eliptik Eğriler, Rank, Torsiyon Grubu, Mordell-Weil Teoremi, Diophantine *M*-lileri, Diophantine Denklemleri

ABSTRACT

ON THE ELLIPTIC CURVES INDUCED BY THE DIOPHANTINE M-TUPLES

Diophantine equations form the basis of mathematical studies on integers, especially with daily life applications. Elliptic curves, on the other hand, have attracted the attention of scientists in recent years, especially because they have a wide application area and are used in the proof of Fermat's Last Theorem. In this study, these two concepts were brought together in the same pot. The rank and torsion groups of elliptic curves reduced by Diophantine m -tuples have been investigated, and this compilation study is specialized for various values of m. The thesis work ends with the study of a current article.

Keywords: Elliptic Curves, Rank, Torsion Group, Mordell-Weil Theorem, Diophantine *M*-tuples, Diophantine Equations

İÇİNDEKİLER

Sayfa No

ÖNSÖZ i

ÖZET ii

ABSTRACT iii

İÇİNDEKİLER iv

SİMGELER LİSTESİ vi

1. ELİPTİK EĞRİLER 1

1.1. Giriş ve Önbilgiler 1

1.2 Eliptik Eğrilerin Geometrik ve Cebirsel Yapısı 2

2. RASYONEL DİOPHANTİNE 3-LÜLERİNDEN İNDİRGENEN ELİPTİK EĞRİLER 5

2.1. Giriş 5

2.2. S Noktasının Sonlu Mertebeli Nokta Olma Koşulu 6

2.3. Karışık İşaretlere Sahip Üçlüler İçin Sıfır Ranklı Eğriler 8

3. POZİTİF ELEMANLARDAN OLUŞAN ÜÇLÜLER İÇİN SIFIR RANKLI BİR EĞRİ ÖRNEĞİ 10

4. RASYONEL DİOPHANTİNE ÜÇLÜLERİ TARAFINDAN İNDİRGENEN YÜKSEK RANKLI ELİPTİK EĞRİLER 12

5. 12 RANKA SAHİP BİR ELİPTİK EĞRİNİN KURULMASI 14

6. RANKI ≥ 7 OLAN ELİPTİK EĞRİLERİN SONSUZ AİLELERİ 19

7. RASYONEL DİOPHANTİNE 4-LÜLERİ TARAFINDAN İNDİRGENEN ELİPTİK EĞRİLER ÜZERİNE 21

7.1 Rasyonel Diophantine 4-lülerinin Parametrik Aileleri 22

7.2 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ **Torsiyon Grubu** 23

7.3 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ **Torsiyon Grubu** 24

7.4 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ **Torsiyon Grubu** 24

KAYNAKÇA 26

SİMGELER LİSTESİ

$\mathbb{R}$ **:** Reel Sayılar

$\mathbb{Z}$: Tam Sayılar

E : Eliptik Eğri

$E(\mathbb{Q})$: Eliptik Eğri Üzerindeki Rasyonel Noktalar Kümesi

$E_{tors}(\mathbb{Q})$: Torsiyon Alt Grubu

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 1.1. E: $y^2 = x^3 + 5x + 8$ eliptik eğrisinin grafiği 2

1. ELİPTİK EĞRİLER

1.1. Giriş ve Önbilgiler

Eliptik eğriler sayılar teorisinden kompleks analize, kriptolojiden matematiksel fiziğe matematiğin birçok dalında yaygın olarak çalışılan önemli bir konudur. İsminin elipsi andırması nedeniyle akla konikler gelebilir ancak konunun ismi eliptik integrallerle olan ilişkisinden gelmektedir. Geometrik olarak verilen nokta toplamı işlemi yardımıyla abelyen grup yapısı oluşturan eliptik eğriler aritmetik olarak oldukça zengin özellikler sahiptir. Konuyla ilgili olarak temel kaynaklar (Silverman,1986), (Washington, 2003) ve (Koblitz, 1984) olarak düşünülebilir.

Bir eliptik eğri $\mathbb{Q}, \mathbb{C}, \mathcal{R}$ ve p bir asal sayı olmak üzere $\mathcal{F}_p$ gibi farklı cisimler üzerinde tanımlanabilir ve farklı cisim üzerindeki her bir tanımlama yeni ve birbirinden farklı özellikleri ortaya çıkarmaktadır. Diğer yandan teori oldukça geniş bir zemine yayılmış olup birçok ilgili kavram bulunmaktadır. Ancak bu çalışmanın kapsamı $\mathbb{Q}$ cismi durumu ile "rank" ve "torsiyon grubu" kavramlarıyla sınırlı olup bu bölümde yalnızca temel giriş, bu kavramlar ve bunlarla bağlantılı kavramlar verilecektir.

İlk olarak eliptik eğri tanımı ile başlanacaktır, burada en genel tanım verilecektir.

Tanım 1.1.1. (Silverman, 1986: 45) $\mathcal{F}$ karakteristiği 2 ve 3'ten farklı bir cisim ve $a_1, a_2, a_3, a_4, a_6 \in \mathcal{F}$ olmak üzere,

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

eşitliğiyle tanımlanan E eğrisine $\mathcal{F}$ üzerinde bir eliptik eğri adı verilir.

Uyarı 1.1.2. (Silverman, 1986: 46) Cebirsel eğrilerin denklemlerinde uygun değişken değişimleri yapılarak ya daha basit hale getirilebilir ya da amaca uygun hale gelebilir. Bu bağlamda Tanım 1.1.1'de (Silverman, 1986:45-46)' daki değişimi ve ardından yapılacak işlemler yardımıyla eliptik eğrilerin kısa Weierstrass formu adı verilen aşağıdaki tanımı verilebilir.

Tanım 1.1.3. (Silverman, 1986: 46) $\mathcal{F}$ karakteristiği 2 ve 3'ten farklı bir cisim ve A ve B tamsayılar olsun. $\Delta := -16(4A^3 + 27B^2) \neq 0$ olmak üzere;

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

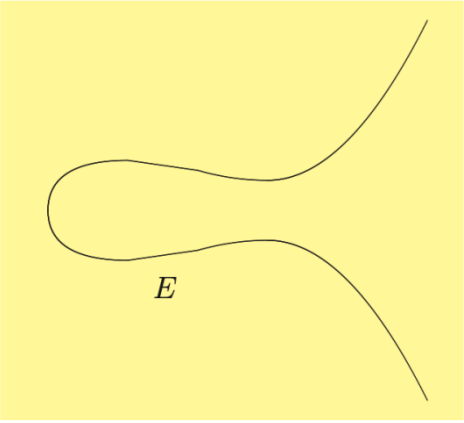
eşitliğiyle tanımlanan E eğrisine $\mathcal{F}$ üzerinde tanımlı kısa Weierstrass formundaki eliptik eğri denir.

Uyarı 1.1.4. Eliptik eğri üzerindeki nokta toplamının anlamlı olabilmesi için iki önemli koşul vardır. Bunlardan ilki Tanım 1.1.3'te verilen $\Delta \neq 0$ koşulu olup bu özelliğe sahip eğrilere "singüler olmayan eliptik eğri" denir. İkinci koşul ise grupta etkisiz eleman rolünü oynayacak olan sonsuz noktasının eliptik eğrinin denklemini sağlayan ve "rasyonel nokta" adı verilen noktaların kümesine eklenmesidir.

1.2 Eliptik Eğrilerin Geometrik ve Cebirsel Yapısı

Eliptik eğri denklemini sağlayan $(x, y) \in \mathbb{Q}$ ikilileri bu eliptik eğri üzerinde yer alan "rasyonel noktalar" olarak isimlendirilir. Örneğin $\mathbb{Q}$ üzerinde tanımlı bir E eliptik eğri üzerindeki rasyonel noktaların kümesi $E(\mathbb{Q})$ ile gösterilir. $E(\mathbb{Q})$ önemli özelliklerle sahiptir ve bu durum ilerideki kısımlarda net olarak görülecektir. Öte yandan aşağıdaki tanımda verilecek olan nokta toplamı işlemi yardımıyla $E(\mathbb{Q})$ bir abelyen grup olur. Çalışmanın kapsamı $\mathbb{Q}$ üzerinde tanımlı eliptik eğri olduğundan aslında daha genel cisimlerde de geçerli olmasına rağmen nokta toplamı tanımı $\mathbb{Q}$ durumuna özelleştirilmiştir.

Tanım 1.2.1. E, $\mathbb{Q}$ üzerinde $\Delta \neq 0$ özelliğinde bir eliptik eğri ve $P, Q \in E(\mathbb{Q})$ olsun. Bu durumda $P+Q$ rasyonel nokta toplamı şu şekilde tanımlanır: P ve Q'dan geçen doğru eliptik eğrinin denklemi üçüncü dereceden olduğundan eğriyi mutlaka bir üçüncü noktada keser, bu kestiği noktanın x-eksenine göre simetriği bu iki noktanın toplamı olarak tanımlanır.



Şekil 1.1 E: $y^2 = x^3 + 5x + 8$ eliptik eğrisinin grafiği

Teorem 1.2.2. (Silverman, 1986: 53) $E(\mathbb{Q}) \cup \{\infty\}$ yukarıdaki tanımla birlikte bir abelyen grup olur.

Uyarı 1.2.3. (a) Bir nokta kendisiyle toplanmak istediğinde $\Delta \neq 0$ katlı köklere izin vermediği için Tanım 1.2.1' deki doğru o noktadan eğriye çizilen teğet doğrusu olarak alınır. Toplanmak

istenen noktalar $P(x, y)$ ve $Q(x, -y)$ özelliğinde ise bu durumda P ve Q noktalarından geçen doğru eliptik eğri grafiğini $E(\mathbb{Q})$'ya ilave edilen sonsuz noktasında keser. Bu noktanın x-eksenine göre simetriği alındığında yine sonsuz noktası elde edilir. O halde $P+Q=\infty$ olur. Sonsuz noktası nokta toplama işleminin etkisiz elemanı olduğu için P ve Q noktaları birbirlerinin tersi olurlar.

(b) Bir grupta sonlu mertebeli noktalar o grubun alt grubunu oluştururlar. (Asar vd., 2021:115). Bu nedenle eliptik eğri üzerinde sonlu mertebeli noktaların alt grubuna torsiyon (büküm) alt grubu adı verilir. Örneği 2-torsiyon grubu $P(x, 0)$ biçimindeki noktalardan oluşur.

(c) E eliptik eğrisi sonlu cisim üzerinde tanımlandığında "nokta sayısı" kavramı ön plana çıkar, buradan elde edilecek aritmetik bilgi ise özellikle şifrelemede kullanılır. Ancak E, $\mathbb{Q}$ cismi üzerinde tanımlandığında bu eliptik eğri üzerindeki rasyonel noktaların sayılması problemi oldukça zor bir hal alır. Bu nedenle adına "rank" adı verilen kavram ortaya çıkar. Eliptik eğrinin rankı kabaca $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisinin rasyonel noktalarının kümesinin "büyüklüğünü" verir. Rank ve torsiyon grubu kavramlarının bir araya geldiği aşağıdaki Mordell-Weil Teoremi eliptik eğriler teorisinin kuşkusuz en önemli teoremlerinden birisidir.

Teorem 1.2.4. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

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

olur. Buradaki negatif olmayan r sayısına E eliptik eğrisinin (cebirsel) rankı adı verilir.

Uyarı 1.2.5. "Herhangi bir $r \geq 0$ sayısını rank kabul eden eliptik eğri var mıdır?", "Yeterince büyük r rankına sahip E eliptik eğrisi bulunabilir mi?" soruları eliptik eğriler teorisinin önemli sorularından ikisidir. Özellikle Hint asıllı ABD'li Fields ödüllü matematikçi Manjul Bhargava' nın çalışmaları bu sorulara ışık tutmaktadır.

2- RASYONEL DİOPHANTİNE 3-LÜLERİNDEN İNDİRGENEN ELİPTİK EĞRİLER

2.1. Giriş

Tanım 2.1.1. *a, b, c* rasyonel sayılar olsun. $a.b + 1$, $a.c + 1$, $b.c + 1$ tam kare olacak şekildeki (a, b, c) üçlülerine rasyonel Diophantine üçlüsü adı verilir. Üstelik bu üçlü $(c - b - a)^2 = 4(ab + c)$ koşulunu sağlıyorsa regüler Diophantine üçlüsü denir.

Örnek 2.1.2. (1, 3, 8) bir rasyonel Diophantine üçlüsü olup gerçekten de $a.b+1= 4$, $a.c+1 = 9$, $b.c+1 = 25$ olduğu görülür. Başka örnekler de benzer şekilde bulunabilir. Bu tanım aşağıdaki şekilde genelleştirilebilir.

Tanım 2.1.3. Her bir $1 \leq i \leq j \leq m$ için $a_i.a_j+1$ bir tam kare olacak şekilde birbirinden ve sıfırdan farklı m'nin $(a_1, \ldots, a_m)$ kümesine bir rasyonel Diophantine m'lisi denir.

Örnek 2.1.4. Diophantus $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}\frac{105}{16}\right\}$ kümesinin bir rasyonel Diophantine dörtlüsü olduğunu keşfetmiştir. Elemanları tamsayı olan Diophantine dörtlülerine ilk örneği $\{1, 3, 8, 120\}$ olarak Fermat vermiştir.

Euler sonsuz çoklukta rasyonel Diophantine 4-lüsünün bulunduğunu ispatlamıştır. Rasyonel Diophantine 6-lısına ilk örnek Gibbs (2006) tarafından verilmiş olup bu örnek kesin olarak $\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{1808}{16}\right\}$ kümesidir ve ardından bu özellikte sonsuz çoklukta Diophantine 6-lısı olduğuda (Dujella, vd., 2017)'de tarafından ispatlanmıştır. Daha genel Diophantine *m*-lilerinin araştırılması konusu halen yaygın olarak çalışılmaktadır.

Diophantine *m*'lileri ile bunlara karşılık gelen eliptik eğriler arasında sıkı bir ilişki vardır. Daha açık olarak $\{a, b, c\}$ bir rasyonel Diophantine üçlüsü olsun, bu takdirde öyle negatif olmayan *r, s, t* rasyonel sayıları vardır ki $a.b + 1 = r^2$, $a.c + 1 = s^2$, $b.c + 1 = t^2$ olur. $\{a, b, c\}$ Diophantine üçlüsünden bir Diophantine dörtlüsü elde edebilmek için $a.x + 1 = \square$, $b.x + 1 = \square$, $c.x + 1 = \square$ denklem sistemi çözülmek zorundadır. Burada $''\square''$ simgesi tam kare olmayı ifade etmektedir. Bu denklem sistemine bir E eliptik eğrisi karşılık getirilebilir:

$$E: y^2 = (ax + 1)(bx + 1)(cx + 1).$$

Bu durumda *E* eliptik eğrisi $\{a, b, c\}$ rasyonel Diophantine üçlüsü tarafından indirgenir denir.

Eliptik eğri üzerindeki 2-torsiyon noktaları kesin olarak ordinatı sıfır olan noktalardır. Bu nedenle eliptik eğrinin denklemi dikkate alınırsa $y = 0$ olduğunda buna karşılık 3 tane x değeri karşılık gelir. Böylece E eliptik eğrisi üzerinde; $A = \left(-\frac{1}{a}, 0\right), B = \left(-\frac{1}{b}, 0\right), C = \left(-\frac{1}{c}, 0\right)$ şeklinde 3 tane 2-torsiyon nokta vardır. Bu nedenle Mazur' un meşhur (1978) sonucu gereği $\mathbb{Q}$ üzerinde tanımlı bu özellikteki eliptik eğriler için $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/6\mathbb{Z}$ ve $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/8\mathbb{Z}$ şeklinde en fazla 4 olasılıkta torsiyon grubu vardır. Dujella (2007)'de tüm bu olası torsiyon gruplarının çıktığını ispatlamıştır. Üstelik $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/8\mathbb{Z}$ torsiyon grubuna sahip her bir eliptik eğrinin bir Diophantine üçlüsü tarafından indirgendiği gösterilmiştir.

Eliptik eğrilerin rankları ile bunlara karşılık gelen Diophantine üçlüleri arasındaki ilişki literatürdeki birçok makalede çalışılmıştır. Özel olarak bu teknik sayesinde $\mathbb{Q}$ üzerinde tanımlı bilinen en büyük ranka sahip eliptik eğri de oluşturulmuştur.

Bu bölümde rankın sıfır olması durumu ele alınacaktır.

2.2. *S* Noktasının Sonlu Mertebeli Nokta Olma Koşulu

E yukarıdaki gibi tanımlanmış bir eliptik eğri olsun. Bu eğri üzerinde A, B, C gibi 3 tane 2-torsiyon noktası dışında eliptik eğrinin denklemini sağlayan

$$P = (0,1), S = \left(\frac{1}{abc}, \frac{rst}{abc}\right)$$

şeklinde iki aşikar rasyonel nokta vardır.

Öte yandan $R = \left(\frac{rs+rt+st+1}{abc}, \frac{(r+s)(r+t)(s+t)}{abc}\right)$ olmak üzere $S = 2R$ dir. Eliptik eğri üzerindeki dublikasyon formülü kullanılarak $S = 2R$ olduğu gösterilebilir. O halde E eliptik eğrisinin rankının sıfır olması için gerekli koşul P ve S noktalarının sonlu mertebeli olması koşuluna denktir. Diğer yandan $\{a, b, c\}$ Diophantine üçlüsü regülerdir yani;

$$c = a + b \mp 2r \Leftrightarrow S = \mp 2P(\infty)$$

Mazur (1977) teoremi ve $S \in 2E(\mathbb{Q})$ olduğu dikkate alınırsa aşağıdaki durumlar söz konusudur.

- $mP = \infty$, $m = 3, 4, 6, 8$;
- $mP = \infty$, $m = 2, 3, 4$.

Özel olarak P noktası 2. mertebeden bir nokta olamayacağından E eliptik eğrisi aynı anda hem rankı sıfır olup hem de torsiyon grubu $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/2\mathbb{Z}$ olamaz.

E eliptik eğrisinin denkleminde $x \to \frac{x}{abc}$, $y \to \frac{y}{abc}$ değişken değişimi yapılarak E' ile gösterilen ve E' ye denk olan aşağıdaki eğri elde edilir.

$$E': y^2 = (x + ab)(x + ac)(x + bc)$$

Böylece E üzerindeki A, B, C ve S noktalarına karşılık E' üzerinde sırasıyla $A' = (-bc, 0)$,

$B' = (-ac, 0), C' = (-ab, 0), P' = (0, abc)$ ve $S' = (1, rst)$ noktaları elde edilir.

Aşağıdaki teoremde S noktasının sonlu mertebede olması için gerekli olan tüm olasılıklar verilmiştir.

Teorem 2.1.5. (Dujella ve Mikic, 2020)

$(\boldsymbol{i})$ $2S = \infty$ olma koşulu $(ab + 1)(ac + 1)(bc + 1) = 0$ olma koşuluna denktir.

(ii) $3S = \infty$ olma koşulu $3+4(ab+ac+bc)+6abc(a+b+c)+12(abc)^2 - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc) = 0$ olma koşuluna denktir.

(iii) *S* noktasının mertebesinin 4 olması için gerek ve yeter şart

$$((ab + 1)^2 - ab(c - a)(c - b))((ac + 1)^2 - ab(c - a)(c - b))(bc + 1)^2 - ab(c - a)(c - b)) = 0$$

olmasıdır.

İspat.

(i) $2S' = \infty$ olması koşulu $rst = -rst$ yani $rst = 0$ olmasını gerektirir ve buradan

$(ab + 1)(ac + 1)(bc + 1) = 0$ sonucu elde edilir ve istenilen gösterilmiş olur.

(ii) $3S' = \infty$ olması demek $X(2S') = X(-S') = X(S')$ olması demektir ve buradan eliptik eğrinin üzerindeki bir noktanın iki katını alma formülü gereği

$$3 + (ab + ac + bc)$$
$$= \frac{9 + 4(ab + ac + bc)^2 + \big(abc(a + b + c)\big)^2 + 12(ab + ac + bc)}{4r^2s^2t^2}$$
$$+ \frac{6abc(a + b + c) + 4abc(ab + ac + bc)(a + b + c)}{4r^2s^2t^2}$$

elde edilir. Buradan;

$4((abc)^2 + abc(a + b + c) + (ab + ac + bc) + 1)(3 + ab + ac + bc) = 9 + 12(ab + ac + bc) + \big(6abc(a + b + c)\big) + 4(ab + ac + bc)^2) + 4abc(ab + ac + bc)(a + b + c) + (abc(a + b + c))^2$ olur. Bu ise;

$3 + 4(ab + ac + bc) + 6abc(a + b + c) + 12(abc)^2 - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc) = 0$ olmasını gerektirir.

(iii) S' noktasının 4. mertebeden olma koşulu aslında $2S' \in \{A', B', C'\}$ olmasına denktir. İlk olarak $2S' = C'$ olması hali göz önüne alınsın. Bir kez daha eliptik eğrinin bir noktasının iki katını alma formülünü kullanarak

$$3 + (ab + ac + bc)$$
$$= \frac{9 + 4(ab + ac + bc)^2 + \big(abc(a + b + c)\big)^2 + 12(ab + ac + bc)}{4r^2s^2t^2}$$
$$+ \frac{6abc(a + b + c) + 4abc(ab + ac + bc)(a + b + c)}{4r^2s^2t^2}$$

elde edilir. Bu ise

$$(1 + 2ab - abc(c - a - b))^2 = 0$$

olmasına veya

$$(ab + 1)^2 = ab(c - a)(c - b)$$

olmasına denktir. Diğer iki durum (A', B') de benzer şekilde yapılabilir ve böylece ispat tamamlanmış olur.

2.3. Karışık İşaretlere Sahip Üçlüler İçin Sıfır Ranklı Eğriler

$mS = \infty$ için 3 olasılık göz önüne alınacaktır. İlk olarak $2S = \infty$ olsun. Bu durumda Teorem 2.1.5 (i) şıkkı gereği $(ab + 1)(ac + 1)(bc + 1) = 0$ elde edilir. Buradan *a*, *b* ve *c* nin aynı işarete sahip olamayacağı sonucuna varılır. Eğer karışık işarete sahip olunması göz önüne alınırsa, bu takdirde $b = -\frac{1}{a}$ olduğu kabul edilir. (Dujella, 2007) gereği $\left\{a, -\frac{1}{a}, c\right\}$ tipindeki rasyonel Diophantine üçlülerinin aşağıdaki parametrizasyonu elde edilir.

$$a = \frac{ut + 1}{t - u}, b = \frac{u - t}{ut + 1}, c = \frac{4ut}{(ut + 1)(t - u)}$$

Buradaki amaç rankı sıfır olan eliptik eğrileri elde etmek olduğu için $\left\{a, -\frac{1}{a}, c\right\}$ üçlüsünün regüler olduğu kabul edilsin. Bu koşul $(u^2 - 1)(t^2 - 1) = 0$ olmasını gerektirir ve böylece

$u = 1$ olarak alınabilir, örneğin $t = 2$ alınırsa rankı sıfır olan, torsiyonu $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/4\mathbb{Z}$ olan ve $\left\{3, -\frac{1}{3}, \frac{8}{3}\right\}$ üçlüsü tarafından indirgenen eliptik eğri elde edilir.

$3S = \infty$ olduğu kabul edilsin**.** Bu durumda aynı anda $3P = \infty$ oluyorsa $P = \mp S$ olduğu elde edilir ki bu bir çelişkidir. Bu nedenle eğer P sonlu mertebeli ise P için tek bir olasılık vardır bu da mertebesinin 6 olmasıdır. Buradan $2P = \mp S$ ve $c = a + b \mp 2r$ olduğu elde edilir.

Teorem 2.1.5 (ii) de b=$\frac{r^2-1}{a}$ ve c=a+b+2r yerine yazılırsa

$(2a\text{r-}1+2r^2)(-a + 2ar^2 - 2r + 2r^3)(2a^2r - a - 2r + 4ar^2 + 2r^3) = 0$ olur. O halde

$a = \frac{-2r(r^2-1)}{-1+2r^2}$ veya $a = \frac{-(-1+2r^2)}{2r}$ veya $a = \frac{1-4r^2 \pm \sqrt{1+8r^2}}{4r}$ elde edilir.

$(a, b, c) = (\frac{-2r(r-1)(r+1)}{-1+2r^2}, \frac{-(-1+2r^2)}{2r}, \frac{(-1+2r)(2r+1)}{2(-1+2r^2)r}$ olarak alınsın. Bu durumda $ab > 0$ olması koşulu ya $r > 1$ ya da $r < -1$ olması koşuluna denk iken $bc > 0$ olma koşulu $-\frac{1}{2} < r < \frac{1}{2}$ olması koşuluna denktir. Bu nedenle a, b, c aynı işarete sahip olamaz, a ve b yer değiştirdiğinde elde edilen $(a, b, c) = \left(\frac{-(-1+2r^2)}{2r}, \frac{-2r(r-1)(r+1)}{-1+2r^2}, \frac{(-1+2r)(2r+1)}{2(-1+2r^2)r}\right)$ durumu, önceki ile tamamen aynıdır.

Son olarak $8r^2 + 1 = (2rt + 1)^2$ olsun ki böylece 3. durumdaki karekökten uzak durulmuş olur. Bu ise $r = \frac{-t}{-2+t^2}$ olmasını gerektirir. Bu takdirde;

$$(a, b, c) = \left(\frac{-t(t - 2)(t + 2)}{2(-2 + t^2)}, \frac{2(t - 1)(t + 1)}{(-2 + t^2)t}, \frac{-(-2 + t^2)}{2t}\right)$$

olur. Burada a ve b yer değiştirilir. $ac > 0$ olması koşulu ya $t > 2$ ya da $t < -2$ olması koşuluna denk iken $bc > 0$ olması koşulu ise $-1 < t < 1$ olması koşuluna denktir. O halde bu durumda da a, b ve c' nin aynı işarete sahip olmadığı sonucuna varılır.

Eğer karışık işaretlere izin verilirse bu takdirde rankı sıfır olan örnekler elde edilir. Örneğin $t = 4$ alınırsa $r = \frac{-t}{-2+t^2}$ rankı sıfır, torsiyon grubu $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/6\mathbb{Z}$ olan ve $\left\{-\frac{12}{7}, \frac{15}{28}, -\frac{7}{4}\right\}$ üçlüsü tarafından indirgenen eliptik eğri elde edilir.

Geriye sadece S'nin 4 mertebeli olma durumu kalır. Bu takdirde $2R = S$ özelliğindeki R noktası 8. mertebede olup böylece eğrinin torsiyon grubu $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/8\mathbb{Z}$ olur. Daha önce belirtildiği gibi bu torsiyon grubuna sahip $\mathbb{Q}$ üzerinde tanımlı her bir eliptik eğri bir rasyonel Diophantine üçlüsü tarafından indirgenir. Daha kesin olarak bu özellikteki her bir eliptik eğri (S) tipindeki

$$\left\{\frac{2T}{T^2-1}, \frac{1-T^2}{2T}, \frac{6T^2-T^4-1}{2T(T^2-1)}\right\} \tag{2.1}$$

Diophantine üçlülerine indirgenir. (S) nin elemanlarının karışık işaretlere sahip olduğu açıktır. Örneğin $T = 2$ alınırsa rankı sıfır olan torsiyon grubu $\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/8\mathbb{Z}$ olan ve $\left\{\frac{4}{3}, -\frac{3}{4}, \frac{7}{12}\right\}$ tarafından indirgenen eliptik eğri elde edilir.

3. POZİTİF ELEMANLARDAN OLUŞAN ÜÇLÜLER İÇİN SIFIR RANKLI BİR EĞRİ ÖRNEĞİ

Önceki bölümde 3 elemanı da pozitif olan Diophantine üçlüsü için $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ veya $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ torsiyon grubuna sahip ve rankı sıfır olan bir eliptik eğrinin bulunamayacağı görülmüştü. Torsiyon grupları için geriye sadece $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ olasılığı kalır. Dikkat edilirse (2.1) eşitliğindeki Diophantine üçlüsünde ilk iki terim ters işaretlidir. Gerçekten de

$$\frac{2T}{T^2-1}\frac{1-T^2}{2T} = -1$$

olur. Öte yandan (2.1) eşitliği tarafından indirgenen tüm eğrilerin torsiyon grubu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ olur. Tüm bu durumlar göz önüne alındığında ilk bakışta bu torsiyon grubu için Diophantine üçlülerinin üçünün de pozitif olamayacağı akla gelebilir ancak (Dujella ve Peral, 2019) bunun böyle olamayacağını göstermiştir. Gerçekten de belli bir T rasyonel sayısı için tüm terimleri rasyonel olan ve (2.1) eşitliğindeki aynı eğriye indirgenen bir eğri bulunabilir.

Ancak bu çalışmada aynı anda rankı sıfır olan ve torsiyon grubu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ve terimleri pozitif olan Diophantine üçlüleri varlığı sorusu açık problem olarak kalmıştır. Bu problem ise (Dujella ve Mikic, 2020)'de çözülmüştür. Burada bu çözüm incelenecektir. İlk olarak S, eliptik eğri üzerinde 4 mertebeli bir nokta ve $b = \frac{r^2-1}{a}$, $c = a + b + 2r$ olsun. Bu değerler Teorem 2.1.5.(iii)' de $(ab+1)^2 - ab(c-a)(c-b)$ de yerine yazılırsa bilinmeyeni a olan 2. dereceden $(2r^3 - 2r)a^2 + (4r^4 - 6r^2 + 1)a + 2r^5 + 2r - 4r^3$ denklemi elde edilir. Bu denklemin diskriminantı $1 - 4r^4 + 4r^2$ olup bu değerin bir tam kare olması gerekir. Bu denklem tarafından tanımlanan kuartik eğri aslında rankı 1 ve üreteci $P_1 = (0,1)$ olan $E_1: Y^2 = X^3 + X^2 + X + 1$ olarak tanımlanan eliptik eğriye birasyonel olarak denktir. O halde E_1 üzerindeki P_1 noktasının katları hesaplanarak ardından bu sonuçlar kuartik denkleme aktarılarak problemin çözümü için gerekli olan çözüm adayları bulunmuş olur. Bununla beraber sağlanması gereken koşul eliptik eğriye karşılık gelen Diophantine üçlüsünün tüm terimlerinin pozitif olmasıdır. Bunun için tüm elemanların aynı işarete sahip olduğunu göstermek yeterlidir çünkü bir rasyonel Diophantine üçlüsünün tüm terimleri (-1) ile çarpılırsa yine bir rasyonel Diophantine üçlüsü elde edilir. Hepsi pozitif olan üçlülerden elde edilen P noktasının ilk iki katı $6P$ ve $11P$ dir. $6P$ noktası $r = -\frac{3855558}{3603685}$, ve $(a,b,c) = \left(\frac{1884586446094351}{25415891646864180}, \frac{14442883687791636}{7402559392524605}, \frac{60340495895762708555}{14487505263205637124}\right)$ üçlüsünü verir.

Bu eliptik eğrinin rankını hesaplamak oldukça zorlu olduğu için rankı belirlenememiştir. Magma cebir programı bir eliptik eğrinin rankı için 2 farklı çıktı vermektedir. Bunlardan ilki gerçek rank değeri olup ikincisi ise rank için bir alt sınır verir. Bu eğri için programın verdiği çıktı $0 \leq rank \leq 2$ şeklindedir. Öte yandan Parite Konjektürü'nün doğruluğu kabul edilirse rankın ya 0 ya da 2 olduğu sonucuna ulaşılır.

$11P$ noktası $r = \frac{35569516882766685106979}{32383819387240952672281}$ ve

$$a = \frac{69705492951192675600645567228019184577147632882703132983}{13201484334991246769290130383656126692130218445953676312 0},$$

$$b = \frac{47826829880079829075801189563942620732062701095548790400}{12233666942070950930363744264796639133659669494969835459327},$$

$$c = \frac{47982111146649404421749331709393501777791774558546217987550257759801}{15400090753918257364093484910580652390786084055043677020804056653840}$$

üçlüsünü verir.

İki eğrinin j-invaryantları karşılaştırılarak $T = \frac{18451786408106133183649}{41916048174422594852689}$ için (2.1) tarafından indirgenen aynı eğri elde edilir. Buna karşılık gelen eliptik eğri için hem **mwrank** hem de bir magma fonksiyonu olan **MordellWeilShaInformation** $0 \leq rank \leq 4$ sonucunu verir. Magma'da yazılan bazı spesifik kodlar yardımıyla bu eliptik eğrinin rankının sıfır olduğu görülür. Böylece istenilen özellikte (elemanların hepsi pozitif) ve rankı sıfır olan bir eliptik eğri bulunmuş olur.

4. RASYONEL DİOPHANTİNE ÜÇLÜLERİ TARAFINDAN İNDİRGENEN YÜKSEK RANKLI ELİPTİK EĞRİLER

Bu bölümde (Dujella ve Peral, 2020)'de yer alan sonuçlar incelenecektir. İçinde milenyum problemlerinden olan Birch ve Swinnertan-Dyer konjektürü bulunduran eliptik eğrilerin rankı konusu hakkında literatürde çok sayıda ilgi çekici makale bulunmaktadır. Bu çalışma tarihi itibariyle ulaşılabilen en yüksek rank 28 olup bir çok bilim insanı verilen bir sayıyı rank kabul eden bir eliptik eğrinin varlığı problemini çalışmaktadır. Bir kısım bilim insanı bu sorunun cevabının olumlu olduğunu düşünürken diğer bir kısım bilim insanı olumsuz olduğunu düşünmektedir. (Dujella ve Peral, 2020)'deki yaklaşım Rasyonel Diophantine üçlüleri kullanılarak yüksek ranklı eliptik eğri elde edilmesi üzerinedir.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ yi torsiyon grubu olarak kabul eden rankı 4, 5, 6, 7, 9 ve 11 olan ve Diophantine *m*-lileri tarafından indirgenen eliptik eğrilerin bir listesi (Dujella ve Peral, 2020)'de verilmiştir. Çok daha zengin sonuçlar elde edilebilmesi için daha geniş torsiyon grubuna sahip eliptik eğriler çalışılmalıdır. Buna dair iki örnek

$$\left\{\frac{301273}{556614}, -\frac{556614}{301273}, -\frac{535707232}{290125899}\right\} \text{ ve } \left\{\frac{181800}{127673}, -\frac{127673}{181800}, -\frac{996869751703}{2072406375000}\right\}$$

tarafından indirgenen ve rankı 9 olan $\mathbb{Q}$ üzerinde tanımlı iki eliptik eğridir (Dujella ve Peral, 2014; 2020). Bu iki eliptik eğrinin torsiyon grubu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ dir. Bu eliptik eğrilerin kuruluşunda $\left\{a, -\frac{1}{a}, c\right\}$ biçimindeki üçlüler kullanılır ve bu üçlüler tarafından indirgenen eliptik eğri üzerinde en az bir tane 4 mertebeli nokta bulunur. Çalışma tarihi itibariyle bir Diophantine üçlüsü tarafından indirgenen en büyük ranka ve en geniş torsiyon grubuna sahip olan eliptik eğri rankı 6 ve torsiyon grubu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ olan ve

$$\left\{\frac{31269599}{31628160}, -\frac{23721120}{31269599}, \frac{1461969791}{7144352640}\right\}$$

üçlüsü tarafından indirgenen eliptik eğridir (Dujella ve Peral, 2019).

Torsiyon grubu olarak en geniş gruba sahip olan eliptik eğri $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ torsiyon grubuna sahiptir. Özel olarak $\left\{\frac{408}{145}, -\frac{145}{408}, \frac{145439}{59160}\right\}$ üçlüsü tarafından indirgenen eliptik eğri bu torsiyon grubuna sahip olup $\mathbb{Q}$ üzerinde rankı 3 olan bir eliptik eğri indirger. Bu ise çalışma tarihi itibariyle bu özellikteki bilinen en yüksek ranka sahip olan eliptik eğridir. (Dujella ve Peral, 2020)' deki sonuçlar iki yönlü olup ilk olarak rankı 12 olan ve bir rasyonel Diophantine üçlüsü tarafından

indirgenen bir eliptik eğri oluşturulup ikinci olarak rankı ≥ 7 olan bu özellikteki eğrilerin sonsuz bir ailesi verilmiştir.

5. 12 RANKA SAHİP BİR ELİPTİK EĞRİNİN KURULMASI

$x \to \frac{x}{abc}$, $y \to \frac{y}{abc}$ koordinat dönüşümü E eğrisine uygulanırsa buna denk olan ilk bölümdeki E' eğrisi elde edilir. Dikkat edilirse E', $A = [-bc, 0]$, $B = [-ac, 0]$, $C = [-ab, 0]$ şeklinde 3 adet 2-rasyonel nokta ve $ab + 1 = r^2, ac + 1 = s^2, bc + 1 = t^2$ olmak üzere $P = [0, abc]$ ve $S = [1, rst]$ biçiminde 2 tane daha rasyonel noktaya sahiptir. Bu eliptik eğri için sonsuz mertebeli P ve S gibi iki noktanın varlığı beklenebilir. Böylece E' eğrisinin rankı en az 2 olur.

Hedeflenen rank 12 olduğu için rank artırılmalıdır. Bu ise Lasic (2017)'te yer alan Rasyonel Diophantine üçlülerinin farklı bir parametrizasyonu kullanılacaktır.

$$a = \frac{2t_1(1 + t_1t_2(1 + t_2t_3))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)}, \qquad b = \frac{2t_2(1 + t_2t_3(1 + t_3t_1))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)}, c = \frac{2t_3(1 + t_3t_1(1 + t_1t_2))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)}$$

Dikkat edilirse $t_3(t_3 - t_2)$ değeri bir tam kare ise bu eliptik eğrinin rankı artacaktır. Gerçekten de

$$x + ab = \frac{b(c - b)}{t_2t_3}$$

olduğu dikkate alınarak E': $y^2 = (x + ab)(x + ac)(x + bc)$ eşitliğindeki

$$x = -\frac{4(t_2^2t_3 - t_3 + t_2)(t_3t_1^2t_2 + 1 + t_3t_1)(t_2t_3 + t_2t_3^2t_1 + 1)}{t_3(-1 + t_1t_2t_3)^2(1 + t_1t_2t_3)^2}$$

yazılırsa;

$$y^2 = \frac{64(1 + t_3t_2)^2(t_1t_2t_3 - t_2t_3^2t_3 + t_3)^2(t_2t_3 + t_2t_3^2t_1 + 1)^2(1 + t_2t_3)^2((t_3{t_1}^2t_2 + 1 + t_3t_1)^2(t_3 - t_2)}{{t_3}^3(-1 + t_1t_2t_3)^6(1 + t_1t_2t_3)^6}$$

elde edilir.

Basit bir hesaplama yardımıyla bu eliptik eğri için $t_3(t_3 - t_2)$ değerinin bir tam kare olma koşulu sağlanır. O halde $t_3(t_3 - t_2)$, $t_1(t_1 - t_3)$, $t_2(t_2 - t_1)$ olacak şekilde hepsi birden tam kare özelliğinde rasyonel sayıların bir (t_1, t_2, t_3) üçlüsü bulunabilirse üzerinde çalışılan eliptik eğrinin rankının ≥ 5 olduğu beklenebilir. Önceki parametrizasyonla şu anda üzerinde çalışılan eliptik eğrinin rankının ≥ 2 olduğuna dikkat ediniz. $t_3(t_3 - t_2)$, $t_1(t_1 - t_3)$, $t_2(t_2 - t_1)$ koşullarının sağlanabilmesi için adına "Almost Perfect Cuboid"adı verilen bir metod kullanılacaktır. Gerçekten de

$$t_3 = {s_3}^2, t_1 = -{s_1}^2, t_2 = {s_2}^2, \; {s_3}^2 - {s_2}^2 = {s_4}^2 \qquad (5.1)$$

yazılırsa;

$$s_1{}^2 + s_2{}^2 = \square,\ s_2{}^2 + s_4{}^2 = \square,\ s_1{}^2 + s_2{}^2 + s_4{}^2 = \square \tag{5.2}$$

elde edilir.

Yalnızca bir diyagonal tam sayı olmadığı için bu parametrizasyonla beraber bir "Almost Perfect Cuboid" elde edilir. (Dujella , 2020)'de yer alan [5] numaradaki eşitliklerin bir parametrik çözümü;

$$s_1 = 2(m^2 + m + 1)(m^2 - 1)^2(m^2 + 1 + 4m),$$

$$s_2 = 4(m^2 + m + 1)(2m + 1)(m^2 - 1)(2m + m^2),$$

$$s_4 = (2m + 1)\ (2m + m^2)(3m^2 + 2m + 1)(m^2 + 2m + 3).$$

olarak bulunur. Bu ise

$$t_1 = -4(m^2 + 2m + 1)^2(m^2 - 1)^4(m^2 + 1 + 4m)^2,$$

$$t_2 = 16(m^2 + 2m + 1)^2(2m + 1)^2(m^2 - 1)^2(2m + m^2)^2,$$

$$t_3 = m^2(2m + 1)^2(m + 2)^2(5m^2 + 8m + 5)^2(m^2 + 1)^2.$$

çözümünü verir.

Yüksek ranktaki eliptik eğrilerin bulunabilmesi için gerekli olan nümerik hesaplamalara daha uygun olan ve bir 2-parametrik çözüme yol açan farklı bir yaklaşım ele alınacaktır. İlk olarak

$t_3(t_3 - t_2) = (t_3 + u)^2,\ t_1(t_1 - t_3) = (t_1 + v)^2$ yazılarak ilk iki koşulun sağlandığı görülür ve böylece

$$t_2 = \frac{u(2t_3 + u)}{t_3}, t_3 = -\frac{v(2t_1 + v)}{t_1}$$

elde edilir. O halde bu değerler $t_2(t_2 - t_1) = \square$'de yerine yazılırsa

$$(8uv^2 - 2u^2v){t_1}^3 + (-8u^3v + 15u^2v^2 + u^4 + 8uv^3){t_1}^2 + (-4u^3v^2 + 2v^4u + 16u^2v^3)t_1 + 4v^4u^2 = \square$$

elde edilir. Son eşitliğe $\mathbb{Q}(u, v)$ üzerinde tanımlı bir eliptik eğri gözüyle bakılabilir. Dikkat edilirse $P = [0,2u^2v^2]$ bu eliptik eğri üzerindeki bir aşikar noktadır. Bu noktanın iki katı alınarak $t_1 = \frac{v^2(-v+16u)}{8u(-4v+u)}$ bulunur. Bu ise

$$a = -\frac{v^2(-v + 16u)(16v^2 - 64u^2 - v^4 + 16uv^3 - 4v^5u + v^4u^2)}{u(2 + v)(4 - 2v + v^2)(v - 2)(v^2 + 2v + 4)(2u - v)(2u + v)(-4v + u)}$$

$$b = \frac{16u(-4v+u)v(4v-64u+16uv^2-4u^2v-v^5+4u^2v^3)}{(2+v)(4-2v+v^2)(v-2)(v^2+2v+4)(2u-v)(2u+v)(-v+16u)}$$

$$c = \frac{4(256uv-64u^2-16v^4+64u^2v^2+v^6-16v^5u)(2u-v)(2u+v)}{u(2+v)(4-2v+v^2)(v-2)(v^2+2v+4)(-v+16u)(-4v+u)}$$

değerlerini verir. Bu ise $\mathbb{Q}(u,v)$ üzerinde tanımlı ve rankı ≥ 5 olan bir eliptik eğri tanımlar. Gerçekten de bu eliptik eğri;

$$\begin{aligned}A = v(&256v^{13}-32v^{15}+v^{17}+140288v^9u^2+741888v^7u^4-4096v^{10}u\\&-1167360v^8u^3-21258240v^6u^5-7936v^{12}u+664832v^{10}u^3\\&+11440128v^8u^5+32192v^{11}u^2-2785824v^9u^4-32380416v^7u^6\\&+28747776v^5u^6+6463488v^6u^7+71860224u^7v^4-2205696u^8v^5\\&+1536v^{14}u-24192v^{13}u^2-22528v^{12}u^3+591360v^{11}u^4\\&-3244800u^5v^{10}-128483328v^3u^8-12979200v^8u^7+7816v^{15}u^2\\&-36160v^{14}u^3-8616v^{13}u^4+100992v^{12}u^5-128v^{16}u-2023776v^{11}u^6\\&+4v^{18}u-449v^{17}u^2+7824v^{16}u^3-31368v^{15}u^4+2860032v^{10}u^7\\&+70176v^{14}u^5+112296v^{13}u^6+9461760v^7u^8-2785824v^9u^8\\&-332160v^{12}u^7+128188416v^2u^9-37027840v^4u^9-1441792v^6u^9\\&+2659328v^8u^9+46368v^{11}u^8-6193152u^{10}v^5+515072u^{10}v^7\\&-291840u^9v^{10}+16818240v^9u^6-29425664vu^{10}+32014336u^{10}v^3\\&+140288v^9u^{10}-2097152u^{11}v^2+1572864u^{11}v^4-507904u^{11}v^6\\&-16384u^{11}v^8+65536u^{12}v^5+65536u^{12}v-131072u^{12}v^3\\&+1048576u^{11}),\end{aligned}$$

$$\begin{aligned}B = 4(&8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)\\&\times(-16v^2+64u^2+v^4-16v^3u)(4v-64u+16v^2u-4vu^2-v^5\\&+4v^3u^2)\times(2vu^2-16u^2+2vu+8v^2u-4v^2-v^3)(2vu^2+16u^2-2vu\\&+8v^2u+4v^2-v^3)\times(16vu-4u^2-v^4+4v^2u^2)(16v^2-64u^2-v^4\\&+16v^3u-4v^5u+v^4u^2)\times(-v+16u)^2(-4v+u)^2u^2v^3,\end{aligned}$$

olmak üzere $y^2 = x^3 + Ax^2 + Bx$ formunda olur.

Bu eliptik eğrilerin rankının ≥5 olduğunu görebilmek için bu eğri üzerinde sonsuz mertebeli 5 tane birbiri cinsinden yazılamayan (bağımsız) nokta (Dujella, 2020)'de verilen (P, R, T_1, T_2, T_3) noktalarıdır. Buradaki P noktası $y^2 = (x+ab)(x+ac)(x+bc)$ eğrisi

üzerindeki $[0, abc]$ noktasına karşılık gelir. S noktası yine aynı eğri üzerindeki $[1, rst]$ noktasına karşılık gelmek üzere, R noktası $2R = S$ eşitliğini sağlar. Dikkat edilirse T_1 noktası $t_3(t_3 - t_2) = \square$ koşuluna, T_2 noktası $t_1(t_1 - t_3) = \square$ koşuluna, T_3 noktası $t_2(t_2 - t_1) = \square$ koşuluna karşılık gelir. Özelleşme dönüşümü bir homomorfizm olduğundan (u_0, v_0) özelleşmesini eğri üzerindeki P, R, T_1, T_2 ve T_3 noktalarını sonsuz mertebeli bağımsız nokta olacak şekilde bulmak yeterlidir. (Dujella, 2020)'ye göre

$$[170605, 39532697], [302665, -66247363], [795565, -637321303],$$

$$[-447095, 24260803], \left[\frac{8673115}{4}, -\frac{25165674989}{8}\right]$$

noktaları $y^2 = x^3 + 21361758597x^2 - 28803989016278714304x$ eğrisi üzerinde bağımsız olduğundan $(u_0, v_0) = (2,1)$ bulunur.

Bu bölümün amacı Diophantine üçlüleri tarafından indirgenen ve rankı 12 olan eliptik eğri elde etmek olduğu için bu metod yardımıyla rankı en az 5 olan eliptik eğriden (u, v) nin uygun bir özelleşmesi yardımıyla daha yüksek ranka sahip eliptik eğriler elde edilecektir. Bunu yapabilmek için (Aguirre vd., 2012) ve (Dujella ve Peral, 2019)'da da yer alan eleme metodları kullanılabilir. Deneyimsel matematiğin etkin şekilde kullanıldığı *Pari/GP* ve *Magma* hesaplamalı cebir programlarındaki özellikle Warwick Üniversitesi Öğretim Üyesi Prof. Dr. John Cremona' nın katkı sağladığı kodlar kullanılarak (Dujella, 2020)' de geliştirilen bir elek algoritması yardımıyla $(u, v) = (-\frac{95}{33}, \frac{50}{57})$ için buna karşılık gelen

$$\{a, b, c\} = \left\{\frac{6125241375}{11907531272}, \frac{5535371271425}{14277129995128}, -\frac{273138178560}{153430695649}\right\}$$

rasyonel Diophantine üçlüsü tarafından indirgenen, rankı 12 olan ve aşağıdaki minimal Weierstrass eşitliğine sahip olan eliptik eğri elde edilir.

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 1444491707528591356856089186460491195711268950880x \\ + 559921583779625421248683584939561 7 \\ 624562242901704374615558514820414397 47 \end{aligned}$$

eliptik eğrisi üzerindeki sonsuz mertebeli 12 nokta ise;

$$P_1 = [158850932500649609134809, 57833477581671452461627622170404 2845],$$

$$P_2 = [351104017200784386392209, 30989796694494511619462419833259 3845],$$

$$P_3 = [-427722660290928813983135, -104857664552611152810918562994878672 7],$$

$$P_4 = [954500781939375762742909, 225326008863345220543071618783370945],$$

$$P_5 = [423679598259676591990909, 154829810959547852593332987635966145],$$

$$P_6 = [153580844909581809420790 5,140142144408049838036978553361699951 3],$$

$$P_7 = [444801887422056021535383,735692161486133998173479868597589 45],$$

$$P_8 = [-120600601587104427867875 1, -740210245609217615143269452335454375],$$

$$P_9 = [-192562292438693523617091, -911556889640548767064630159456313855],$$

$$P_{10} = [105088796685273566829212 49,338518000531811689265683628254763856 25],$$

$$P_{11} = [951514410733369555670349,216676520921276805299703311439049825],$$

$$P_{12} = [-\frac{735568009995542671748158 1}{81}, -\frac{605705671933225602690651446390633849125}{729}]$$

şeklinde yazılabilir.

6. RANKI ≥ 7 OLAN ELİPTİK EĞRİLERİN SONSUZ AİLELERİ

Bundan önceki bölümde yüksek ranka sahip ve rasyonel Diophantine üçlülerine indirgenen yalnızca bir eliptik eğrinin elde edilmesi amaçlanmıştı. Bu bölümde problem farklı bir açıdan ele alınacaktır, öyle ki belli bir ranka sahip eliptik eğrilerin 2 parametreli sonsuz aileleri kurulacaktır. Konu ile ilgili yapılan ilk çalışmalardan biri (Aguirre vd., 2012) olup bu çalışmada rankı ≥ 5 olan eliptik eğrilerin 2 parametreli sonsuz ailesi oluşturulmuştur. Daha açık olarak $\mathbb{Q}(m,n)$ üzerinde tanımlı ve rankı ≥ 4 olan eliptik eğrilerin iki parametreli ailesi oluşturulmuştur. Özel olarak $n=\frac{7}{3}$ seçilerek rankı ≥ 5 olan $\mathbb{Q}(m)$ üzerinde tanımlı eliptik eğri aileleri elde edilmiştir. $m=-\frac{20(4u^2-1)}{9u(u+4)}$ alınarak aynı aile elde edilebilir çünkü $v=-1$ alınarak istenen sonuç görülebilir. (Aguirre vd., 2012)'deki tanımlanan eliptik eğri ailelerinde $n=\frac{7}{3}$ alınarak (Dujella ve Peral, 2019)'da $\mathbb{Q}(a,n)$ üzerinde tanımlı ve rankı ≥ 3 olan bir aile ile $\mathbb{Q}(a)$ üzerinde tanımlı ve oldukça basit bir parametrizasyonla oluşan bir eğri ailesi elde edilmiştir. Bu eğri ailesi yardımıyla daha yüksek ranka sahip alt aileler kolaylıkla kurulabilir. Gerçekten de bu aile;

$$A(a) = -2(-51200 + 109440a + 38880a^2 + 55404a^3 + 6561a^4),$$

$$B(a) = 243a^2(20 + 3a)(-4 + 9a)(16 + 9a)(80 + 9a)(320 + 81a^2)$$

olmak üzere;

$$y^2 = x^3 + A(a)x^2 + B(a)x$$

olur.

Örneğin, $a = 2$ alınırsa;

$A(a) = -1742816,\ B(a) = 759204036864$ parametrelerinin bu özel değeri için elde edilen eliptik eğri;

$$y^2 = x^3 - 1742816x^2 + 759204036864x$$

sonucu elde edilir.

Magmadaki rank hesaplama kodu kullanılarak bu eğrinin (gerçek) rankının 3 olduğu görülebilir. Bu eliptik eğrinin torsiyon alt grubu $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ ye izomorf olup bu eğri üzerinde

bulunan bazı noktalar $(0,0), (5616, 64876032), (5616, -64876032), (9828, 85405320), (9828, -85405320)$ şeklindedir.

Farklı değişken dönüşümleri yapılarak rank ≥ 7 olan eliptik eğrilerin sonsuz aileleri elde edilir. Literatürde buna dair (Dujella ve Peral, 2019) gibi birçok makale yer alır.

7. RASYONEL DİOPHANTİNE 4-LÜLERİ TARAFINDAN İNDİRGENEN ELİPTİK EĞRİLER ÜZERİNE

Bu bölümde oldukça güzel bir çalışma olan (Dujella ve Soydan, 2022) de yer alan sonuçlar incelenecektir. $\{a, b, c, d\}$ bir rasyonel Diophantine 4' lüsü olsun. Bu dörtlüyü bir rasyonel Diophantine 5' lisine genişletebilmek için öyle bir rasyonel X sayısı bulunmalıdır ki

$$aX + 1, bX + 1, cX + 1, dX + 1$$

sayıları rasyonel sayıların kareleri olmalıdır. Tıpkı Diophantine 3-lülerinden Diophantine 4-lülerine genişlemedeki gibi bunu 4 koşulla çarpabiliriz.

Böylece bu eğri denklemi $Y^2 = (aX + 1)(bX + 1)(cX + 1)(dX + 1)$ şeklinde elde edilir ki bu denklem cinsi bir olan bir eğriyi belirtir. Cinsi 1 olan cebirsel eğriler (Silverman, 2016) eliptik eğri olduğundan uygun bir değişken değişimi yardımıyla bu eğri bir eliptik eğriye dönüştürülebilir. Gerçekten de $y = \frac{Y(d-a)(d-b)(d-c)}{(dX+1)^2}$, $x = \frac{(aX+1)(d-b)(d-c)}{dX+1}$ değişken değişimi yardımıyla

$$E: y^2 = x(x + (b - a)(d - c))(x + (c - a)(d - b)$$

eğrisi elde edilir. Bu eliptik eğriye, $\{a, b, c, d\}$ rasyonel Diophantine dörtlüsü tarafından indirgenen eliptik eğri adı verilir. Bu özellikteki eliptik eğriler (Dujella, 2020) de incelenmiş olup torsiyon grubu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ve rankı 8 olan birçok eliptik eğri örneği verilmiştir. (Dujella ve Soydan, 2022) makalesinin temel problemi rasyonel Diophantine dörtlüleri tarafından indirgenen eliptik eğriler için hangi torsiyon gruplarının mümkün olabileceği sorusudur. Buradaki temel teknik Mazur'ın meşhur teoremi kullanılarak temel sonuç olan k=2, 4, 6, 8 için bu eliptik eğrilerin $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ olduğu görülmüştür. Bu sonuç sonsuz çokluktaki rasyonel Diophantine 4-lüleri için ispatlanmış olup elde edilen indirgenmiş eliptik eğrilerin rankları oldukça büyüktür. Kolayca görülebilir ki E üzerinde aşikardan farklı tam olarak 3 tane 2-torsiyon noktası vardır. Bu noktalar

$$A = (0,0), \qquad B = (-(b - a)(d - c), 0), C = (-(c - a)(d - b), 0)$$

noktalarıdır. Basit bir hesaplama yardımıyla bu eğri üzerindeki

$$P = \big((b - a)(c - a), (b - a)(c - a)(d - a)\big),$$

$$Q = \left((ad+1)(bc+1), \sqrt{(ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1)}\right)$$

gibi 2 rasyonel nokta bulunmaktadır. Bu iki nokta istenilen özellikteki eliptik eğrilerin elde edilmesinde kritik bir rol oynayacaktır. Bu bölümdeki temel amaç sonlu mertebeli elemanların oluşturduğu torsiyon gruplarının yapısını elde etmek olduğu için ilgili çalışmanın temel sorusu P ve Q hangi şartlarda sonlu mertebeli olduğuna karar vermektir.

7.1 Rasyonel Diophantine 4'lülerinin Parametrik Aileleri

$\{a.b.c\}$ regüler rasyonel Diophantine 3-lüsü olsun. Böylece $ab+1=r^2$ olmak üzere $c=a+b+2r$ olur. O halde $d=b+c+2\sqrt{bc+1}=a+4b+4r$ olmak üzere diğer bir $\{b.c.d\}$ üçlüsü göz önüne alınsın. Bu dört sayıdan Diophantine 4-lüsü elde etmek için sağlanması gereken son koşul $ad+1=\square$ olmasıdır. Bu ise $(a+2r)^2-3=\square$ olması koşulunu gerektirir. Üstelik sıfırdan farklı $t\in\mathbb{Q}'$ lar için $u=\frac{t^2+3}{2t}$ olmak üzere $r=\frac{u-a}{2}$ alınırsa bu koşul sağlanır. O halde $\{a,b,c,d\}$ rasyonel Diophantine 4-lülerinin

$$b=\frac{(t^2-2at-4t+3)(t^2-2at+4t+3)}{16t^2a},$$

$$c=\frac{(t^2+2at+4t+3)(t^2+2at-4t+3)}{16t^2a}, d=\frac{(t-1)(t+3)(t-3)(t+1)}{4t^2a}$$

olmak üzere bir 2-parametrik ailesi elde edilir. Buna karşılık gelen eliptik eğri ailesi ise

$$A_1=6t^8-48t^6a^2+96t^4a^4-120t^6+992t^4a^2+708t^4-432t^2a^2-1080t^2+486$$

$$B_1=(t^2+2at-1)(t^2-6at-9)(3t^2+2at-3)(t^2-2at-9)\times(t^2+6at-9)(t^2-2at-1)(t^2+2at-9)(3t^2-2at-3$$

olmak üzere $y^2=x^3+A_1x^2+B_1x$ eliptik eğri ailesidir.

(Dujella ve Soydan, 2022)'de bu eliptik eğri ailesinde yer alan ve rankı 9 olan eliptik eğri örneği bulunamamıştır ancak Mestre ve Nagao toplamları şeklinde elde edilen bazı elek metotları yardımıyla **mwrank** komutu kullanılarak rankı 10 olan ve yukarıdaki aileye ait iki eliptik eğri bulunmuştur, bunlar

$t=\frac{142}{53}$ ve $v=\frac{142}{23}$ değerlerine karşılık gelen

$$\{a,b,c,d\}=\left\{\frac{19635}{6532},-\frac{46592463}{201832268},\frac{84196064}{50458067},-\frac{1144273}{8775316}\right\}$$

Diophantine 4'lüsü ve

$t = \frac{59}{4}$ ve $v = \frac{59}{34}$ değerlerine karşılık gelen

$$\{a, b, c, d\} = \left\{\frac{2325}{4012}, \frac{187020623}{9949760}, \frac{261411943}{9949760}, \frac{13104399}{146320}\right\}$$

Diophantine 4-lüsüdür.

7.2 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ Torsiyon Grubu

$p_1 = (b-a)(d-c)$ ve $p_2 = (c-a)(d-b)$ olmak üzere $E: y^2 = x(x+p_1)(x+p_2)$ eliptik eğrisi göz önüne alınsın. Bu durumda 2-azalma kullanılarak $\mathbb{Q} = ((ad+1)(bc+1), \sqrt{(ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1)}$ noktası $2E(\mathbb{Q})$ kümesinin bir elemanıdır. Gerçekten de $x_1 = (ad+1)(bc+1)$, $x_1 + p_1 = (ac+1)(bd+1)$, $x_1 + p_2 = (ab+1)(cd+1)$ birer tam kare ifadedir. Dikkat edilirse $ad+1 = 0$ durumunda $\mathbb{Q}$ iki mertebeli bir nokta olur. Bu ise ancak ve ancak $d = -\frac{1}{a}$ durumunda geçerlidir. Böylece $2R = \mathbb{Q}$ özelliğindeki R noktasının mertebesi 4 olur ve böylece $E(\mathbb{Q})$' nun $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ gibi bir alt grubu vardır.

O halde öyle rasyonel Diophantine dörtlüleri bulunmalıdır ki bu dörtlüler $\left\{a, -\frac{1}{a}, b\right\}$ biçimindeki alt üçlüleri bulundurmalıdır. $\alpha = u$, $T = t$ denilirse $a = \frac{ut+1}{t-u}$, b=$((\frac{t+u}{t-u})^2 - 1)/a = \frac{4tu}{(tu+1)(t-u)}$ elde edilir. Geriye dörtlünün dördüncü elemanı olacak olan c yi bulmak kalır. Bu c sayısı $\{a, b, c, d\}$ bir regüler dörtlü olacak şekilde seçilebilir yani bu durumda $(a+b-c-d)^2 = 4(ab+1)(cd+1)$ olur. Bu sayede

$$c = \frac{(u-1)(u+1)(t-1)(t+1)}{(ut+1)(t-u)}$$

elde edilir. O halde $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ torsiyon grubuna sahip indirgenmiş eğrinin karşılık geldiği sonsuz çoklukta rasyonel Diophantine dörtlüsü olduğu gösterilmiş olur.

Diğer bir olasılık ise $c = \frac{8(d-a-b)(a+d-b)(b+d-a)}{(a^2+b^2+d^2-2ab-2ad-2bd)^2}$ olarak seçilmesi halinde

$c = \frac{8(t-u)(ut+1)(-4ut+t^2+u^2+u^2t^2+1)(u-1)(u+1)(t-1)(t+1)(t^2+4ut+u^2+u^2t^2+1)}{(1-8ut-12u^2t^2+2u^2+2t^2-8u^3t^3+u^4t^4+8ut^3+t^4+u^4+8tu^3+2u^2t^4+2u^4t^2)^2}$ elde edilir. Bu dörtlülerin iki parametreli ailesi arasından rankı altı olan iki eğri elde edilir. Bunlar $(t,u) = \left(3,\frac{1}{12}\right)$ ve $(t,u) = (\frac{25}{2},\frac{31}{8})$ durumları olup bunlara karşılık gelen dörtlüler ise sırasıyla

$$\left\{\frac{3}{7},\frac{48}{175},-\frac{625153729200}{363378690481},-\frac{7}{3}\right\}$$

ve

$\left\{\frac{791}{138},\frac{24800}{54579},\frac{14188099227120}{9044268302161},-\frac{138}{791}\right\}$ olur.

7.3 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ Torsiyon Grubu

Uygun parametrizasyon ve değişken değiştirme kullanılarak ve ilk durumdakine benzer metot yardımıyla rankı 3 olan ve bu torsiyon alt grubuna sahip iki eliptik eğri elde edilmiştir. Bu iki eğriye karşılık gelen rasyonel Diophantine 4'lüleri ise sırasıyla

$\left\{-\frac{16051953}{11214104},-\frac{170244712}{1784519841},\frac{914623}{5622936},\frac{5498328}{10310521}\right\}$ ve $\left\{-\frac{18873668}{3382575},\frac{821921100}{5086844387},-\frac{26226421}{4890900},\frac{1090383}{6661892}\right\}$ dir.

7.4 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ Torsiyon Grubu

İlk olarak aşağıda açıkça verilmiş olan $\{a,b,c,d\}$ dörtlüleri ile başlansın.

$$a = \frac{ut+1}{t-u}, b = \frac{4ut}{(ut+1)(t-u)}, c = \frac{(u-1)(u+1)(t-1)(t+1)}{(ut+1)(t-u)}, d = \frac{t-u}{ut+1}$$

Aşikar olarak $\mathbb{Q}(0,0)$ noktasının mertebesi 2 olup bu nokta $2E(\mathbb{Q})$ kümesinin bir elemanıdır. O halde $2R = \mathbb{Q}$ olacak şekilde bir R noktası vardır. Bu bölümde istenen torsiyon grubunu elde etmek için R noktasının, $2E(\mathbb{Q})$ kümesinin bir elemanı olması sağlanmalıdır, bu ise $S \in 2E(\mathbb{Q})$olmak üzere bu S noktası için $R = 2S$ olmasıdır. Bu takdirde S noktasının mertebesi 8 olur. R noktasının koordinatları hesaplanacak olursa $(\frac{(u+t)^2(ut-1)^2}{(ut+1)^2(t-u)^2},\frac{(u^2+1)(t^2+1)(u+t)^2(ut-1)^2}{(ut+1)^3(t-u)^3})$ olur. İstenilen sonucun elde edilebilmesi için $x_1 = \frac{(u+t)^2(ut-1)^2}{(ut+1)^2(t-u)^2}, x_1, x_1+p_1,$ ve x_1+p_2 nin hepsinin tam kare olması gerekir. $x_1+p_1,$ ve x_1+p_2 tam kare iken x_1 zaten tam kare olmak zorunda kalır. Bu iki koşul birlikte düşünüldüğünde istenilen koşul $(u^2+1)(t^2+1)$'in tam kare olmasına denktir. $(u^2+1)(t^2+1) = (u^2+1+(t-u)v^2$ yazılırsa;

$$t = \frac{-2u^2v - 2v + v^2u + u^3 + u}{u^2 + 1 - v^2}$$

olur ve böylece

$a = \frac{(u - v + 1)(u - v - 1)}{2(u - v)}$, $\quad b = -\frac{2(u^2 + 1 - v^2)u(-2u^2v - 2v + v^2u + u^3 + u)}{(u^2 + 1)^2(u - v)(u - v + 1)(u - v - 1)}$,

$c = \frac{(-2u^2v - 2v + v^2u + u^3 + u - u^2 - 1 + v^2)(-2u^2v - 2v + v^2u + u^3 + u + u^2 + 1 - v^2)(u + 1)(u - 1)}{2(u^2 + 1)^2(u - v)(u - v + 1)(u - v - 1)}$,

$d = \frac{2(u-v)}{(u-v+1)(u-v-1)}$ elde edilir. Burada u ve v , $uv(u + 1)(u - 1)(-uv + v + 1 + u^2)(-uv + 1 + u^2)(-uv - v + 1 + u^2)(u - v + 1)(u - v)(u - v - 1) \times (u^2 + 1 - v^2)(-2u^2v - 2v + v^2u + u^3 + u)(-2u^2v - 2v + v^2u + u^3 + u - u^2 - 1 + v^2) \times (-2u^2v - 2v + v^2u + u^3 + u + u^2 + 1 - v^2)$ ifadesi sıfırdan farklı keyfi rasyonel sayılardır. Böylece a, b, c, d birbirinden ve aynı zamanda sıfırdan farklı rasyonel sayılar olur.

(Dujella ve Soydan, 2022:7)'deki tartışma gereği $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ torsiyon grubuna sahip her bir eliptik eğri bir rasyonel Diophantine dörtlüden elde edilebilir. Örneğin:

$\left\{\frac{1804}{1197}, -\frac{226796}{539847}, \frac{303199}{239932}, -\frac{1197}{1804}\right\}$, dörtlüsü $(u, v) = (2, -\frac{25}{19})$ değerlerine karşılık elde edilen dörtlü olup bu dörtlü, torsiyonu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ve rankı 3 olan eliptik eğriye indirger. Dikkat edilirse bu eğri, bu torsiyon grubuna sahip olan bilinen en büyük ranka sahip olan eliptik eğridir.

KAYNAKÇA

Aguirre J., Dujella A. And Peral J. C. (2012). On the rank of elliptic curves coming from rational Diophantine triples, *Rocky Mountain J. Math*. 42, 1759-1776.

Baker A. and Davenport H. (1969). The equations $3x^2 - 2 = y^2 and\ 8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* (2) 20, 129-137.

Cremona J. E. (1997). Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge.

Dujella A. (2000). Irregular Diophantine m-tuples and elliptic curves of high rank, Proc. *Japan Acad. Ser. A Math. Sci*. 76, 66-67.

Dujella A. (2004). There are only finitely many Diophantine quintuples, *J.Reine Angew. Math.* 566, 183-214.

Dujella A. (2007). On Mordell-Weil groups of elliptic curves induced by Diophantine triples, *Glas. Math. Ser. III* 42, 3-18.

Dujella A. and Soydan G. (2022). On elliptic curves induced by rational Diophantine quadruples, *Proc. Japan Acad. Ser. A Math. Sci*. 98, 1-6.

Dujella A., Kazalicki M., Mikic **M. and Szikszai M.** (2017). There are infinitely many rational Diophantine sextuples, *Int. Math. Res. Not. IMRN* 2017 (2), 490-508.

Dujella A. and Mikic M. (2014). On the torsion group of elliptic curves induced by D(4) – triples, An. Stiint. Univ. *"Ovidius" Constanta Ser. Mat*. 22, 79-90.

Dujella A. and Peral J. C. (2014). High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples, *LMS J. Comput. Math*. 17, 282-288.

Dujella A. and Peral J. C. (2019). Elliptic curves induced by Diophantine triples, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM 113, 791-806.

Dujella A. and Peral J. C. (2020). Contruction of high rank elliptic curves, *J. Geom. Anal*., published online.

Gibbs P. (2006). Some rational Diophantine sextuples, Glas. *Math. Ser. III* 41, 195-203.

He B., Togbe **A. and Ziegler V.** (2019). There is no Diophantine quintuble, *Trans. Amer. Math. Soc*. 371, 6665-6709.

Koblitz N.(1984). İntroduction to elliptic curves and modular forms. Springer-Verlag, New York, USA, 248 pp.

Lasic L. (2017) Şahsi yazışmalar.

Mazur B. (1978). Rational isogenies of prime degree, *Invent. Math.* 44, 129-162.

Mestre J.- F. (1982). Construction d'une courbe elliptique de rang ≥ 12, *C. R. Acad. Sci. Paris Ser.* I 295, 643-644.

Nagao K. (1993). An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20, *Proc. Japan Acad. Ser. A Math. Sci.* 69, 291-293.

Silverman J., H. (1986). The arithmetic of elliptic curves. Springer-Verlag, USA, 400 pp.

Washington J., L. (2003). Elliptic curves. Chapman&Hall/CRC, Florida, USA, 429 pp.