DENK SAYILAR VE ELİPTİK EĞRİLER

NAGİHAN KURNAZ

T. C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DENK SAYILAR VE ELİPTİK EĞRİLER

Nagihan KURNAZ

Prof. Dr. Osman BİZİM
(Danışman)

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA–2017

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.

01/06/2017

İmza

Nagihan KURNAZ

TEZ ONAYI

Nagihan KURNAZ tarafından hazırlanan "Denk Sayılar ve Eliptik Eğriler" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimler 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 : Prof. Dr. Ahmet TEKCAN
Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye : Yrd. Doç. Dr. Fırat EVİRGEN
Balıkesir Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Ali BAYRAM
Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

DENK SAYILAR ve ELİPTİK EĞRİLER

Nagihan KURNAZ

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Osman BİZİM

Bu çalışmada çözümü üzerinde oldukça uzun zamandır uğraşıldığı halde henüz çözülememiş en eski sayılar teorisi problemlerinden birisi olan "denk sayı problemi" ele alınmıştır. Denk sayı problemi üzerine günümüze kadar yapılmış olan çalışmaların bir kısmı bir araya getirilmeye çalışılmış ve denk sayı problemi ile eliptik eğriler arasındaki ilişkiler ele alınmıştır. İlk önceleri tamsayılar halkası üzerinde oluşturulan denk sayı problemi önce rasyonel sayılar cismine, daha sonra da rasyonel sayılar cisminden daha genel sayı cisimleri üzerine taşınmıştır. Daha sonra eliptik eğriler ile denk sayı problemi arasındaki ilişki keşfedilmiş ve denk sayı probleminin henüz ispatlanamamış olan Birch ve Swinnerton-Dyer konjektürünün en önemli uygulaması olduğu görülmüştür. Eğer Birch ve Swinnerton-Dyer konjektürü doğru ise bir tamsayının bir denk sayı olup olmadığının belirlenmesi probleminin bir sonlu kümenin kardinalitesinin belirlenmesi problemine indirgendiği sonucu elde edilmiştir.

Anahtar Kelimeler: Denk sayı problemi, denk sayı, eliptik eğri, Birch ve Swinnerton-Dyer konjektürü.
2017, vi + 66 sayfa.

ABSTRACT

MSc Thesis

CONGRUENT NUMBERS and ELLIPTIC CURVES

Nagihan KURNAZ

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

Supervisor: Prof. Dr. Osman BİZİM (Uludag University)

In this work "the congruent number problem" which is the oldest problem of number theory that has not yet been solved despite having studied on the solution for quite long time is discussed. Some of the studies on the congruent number problem have been done until these days is collected. The relation between the congruent number problem and ellliptic curves is given. The congruent number problem was first consider on the ring of integers then field of rational numbers and then the more general number fields than the field of rational numbers. Then the relation between elliptic curves and the congruent number problem is discovered and it is shown that the congruent number problem is one of the important application of Birch and Swinnerton-Dyer Conjecture which has been proved yet. If the Birch and Swinnerton-Dyer Conjecture is true it was derived that the problem of determining whether an integer is a congruent number is reduced to the problem of determining the cardinalty of some finite set.

Key Words: Congruent number problem, congruent number, elliptic curve, Birch and Swinnerton-Dyer Conjecture.
2017, vi + 66 pages.

TEŞEKKÜR

Her ne kadar burada teşekkür etmeye çalıştıysam da burada yazılanlar verilen emeği karşılamayacaktır.

Tanıdığım günden bu yana ilim ve tecrübelerinden en çok istifade ettiğim, iyi insan kimdir denildiğinde aklıma gelen ilk isimlerden birisi olan, insani ve ahlaki olarak daima örnek aldığım ve alacağım, bu çalışma süresince ilgi, hoşgörü, sabır ve bilgisini hiçbir zaman benden esirgemeyen, öğrencisi olmaktan gurur duyduğum çok değerli hocam Prof. Dr. Osman BİZİM'e,

Gerek lisans aşamasında gerekse lisansüstü ders aşamasında ders almış olduğum, bilgi ve tecrübelerinden faydalandığım Prof. Dr. Ahmet TEKCAN ve Doç. Dr. Betül GEZER hocalarıma,

Ayrıca lisans eğitimi süresince emeği geçen tüm hocalarıma,

Ve aileme, özellikle de bu tezin yazımında bana yardımcı olan ablam Tuba KURNAZ'a, sonsuz teşekkürler…

Nagihan KURNAZ

İÇİNDEKİLER

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bu çalışmada, verilen bir doğal sayının bir denk sayı olup olmadığını belirleyen bir algoritmanın veya bir yöntemin bulunması anlamına gelen ve sayılar teorisinin, hatta matematiğin en eski, en büyük çözülememiş problemi olan, "*denk sayı problemi*" olarak adlandırılan problem ele alınacak ve bugüne kadar bu problem üzerine yapılmış olan çalışmalarda elde edilmiş sonuçların sadece bir kısmı bir araya getirilmeye çalışılacaktır.

Denk sayı problemi, antik çağın 200'lü yıllarında yaşamış en büyük matematikçilerinden biri olan Diophant tarafından yazılmış ve 13 kitaptan oluşan "*Arithmetica*" isimli çalışmanın 3. Kitabındaki 19. Problem:

"Öyle dört sayı bulunuz ki bu sayıların toplamlarının karesi ile bu sayılardan sadece birinin toplamı veya farkı herhangi bir sayının karesi olsun, yani

$$(x_1 + x_2 + x_3 + x_4)^2 \pm x_i = \square$$

olacak biçimde x_1, x_2, x_3, x_4 tamsayıları bulunuz."

ve 5. Kitabındaki 7. Problem:

"Öyle üç sayı bulunuz ki bu sayılardan herhangi birinin karesinden bu üç sayının toplamı çıkarıldığında veya toplandığında herhangi bir sayının karesi olsun, yani

$$x_i^2 \pm (x_1 + x_2 + x_3) = \square$$

olacak biçimde x_1, x_2, x_3 tamsayıları bulunuz."

olarak görülmektedir, burada "□" simgesi ile herhangi bir tamsayının karesi gösterilmektedir.

Al-Kazin gibi Arap matematikçilerin bu problem üzerine yapmış oldukları araştırmalardan ve çalışmalardan, bu problem üzerine yapılan ilk sistematik çalışmaların 10. yüzyıla kadar uzandığı görüldüğü halde muhtemelen çok daha eski bir tarihe sahip olduğu düşünülmektedir (L. E. Dickson 1920). 972 yılından daha önce, kimler tarafından yazıldığı bilinmeyen Arap matematik yazılarında denk sayı probleminin orijinal hali;

"Verilen bir N tamsayısı için $x^2 - N$ ve $x^2 + N$ sayıları birer kare olacak biçimde bir x^2 tamsayısı bulunuz" biçiminde görülmekte ve aşağıdaki 29 tamsayının birer denk sayı olduğu belirtilmektedir;

5, 6, 14, 15, 21, 30, 34, 65, 70, 110, 154, 210, 221, 231, 286, 330, 390, 429, 546, 1155, 1254, 1785, 1995, 2730, 3570, 4290, 5610, 7854, 10374.

Daha sonra kim oldukları bilinmeyen Arap matematikçiler tarafından 14 tanesi karesiz olan denk sayıların 52 tanesi listelenmiştir.

Arap matematikçilerden sonra birçok matematikçi de bu problem ile ilgilenmiştir. Denk sayı problemine eşdeğer olduğunu bilmediği halde, Pisagor üçlüleri üzerine çalışmalar yapmış olan Fibonacci, bu matematikçilerden sadece biridir. "Bir kare tamsayının beş fazlası veya 5 eksiği de bir kare tamsayı olabilir mi, yani $y^2 - 5 = x^2$ ve $y^2 + 5 = z^2$ olacak biçimde x, y, z tamsayıları bulunabilir mi?" sorusunu ortaya koymuştur. Daha sonra Fibonacci bu soruyu, 5 sayısı yerine herhangi bir tamsayı alarak genelleştirmiş ve bu soruyu "*Liber Quadratorum*" isimli çalışmasında 14. Önerme olarak "$y^2 - c = x^2$ ve $y^2 + c = z^2$ olacak biçimde x, y, z tamsayıları bulunabilir mi?" biçiminde ifade etmiştir. Bundan başka "denk sayı" kavramından da ilk kez bu çalışmasında söz etmiş,

$$x + y \text{ çarpanı çift ise } xy(x + y)(x - y)$$

ve

$$x + y \text{ çarpanı tek ise } 4xy(x + y)(x - y)$$

biçimindeki sayılara denk sayı adını vermiştir. Üstelik 14. Önermesinde, verilen $y^2 - c = x^2$ ve $y^2 + c = z^2$ eşitliklerinin tamsayı çözümlerinin sadece c sayısının bir denk sayı olması halinde var olduğunu da göstermiştir. Fibonacci tarafından $y^2 - c$, y^2 ve $y^2 + c$ sayılarına, Latincedeki "*congruous*" kelimesinin karşılığı olan ve "*uygun, uyuşma*" anlamına gelen "*denk sayı*" denmesinin nedeni, bu sayının üç kare sayının ortak farkı olmasıdır. Fibonacci, hiçbir tam kare tamsayının bir denk sayı olamayacağı gerçeğinden hareket ile 1 sayısının da bir denk sayı olamayacağını ifade ettiği halde bu sonucu ispat edememiştir.

17. yüzyılda Fermat, (üzerinde oldukça yoğun olarak çalıştığı ve kitabın üzerine birçok notlar yazdığı bilinen) "*Arithmetica*" isimli çalışmanın ekindeki 20. Problem, yani

"Alanı verilen bir tamsayı olan, tamsayı kenar uzunluklarına sahip bir dik üçgen bulunabilir mi?" problemi ile ilgili çalışmalar yapmış ve kendisinin geliştirdiği "*sonsuz azalma*" yöntemini kullanarak, 1 sayısının bir denk sayı olmadığını ispat etmiştir. Fermat, daha sonra kenar uzunlukları rasyonel sayı olan bir dik üçgenin alanının bir kare sayı olamayacağını da ifade ve ispat etmiştir. Üstelik 1 sayısının denk sayı olmamasının $xy \neq 0$ olmak üzere $x^4 + y^4 = 1$ olacak biçimde x, y rasyonel sayılarının olamayacağını gerektirdiğini de belirtmiştir. Bazı kaynaklar, ilk ispatı A. Wiles tarafından 1994 yılında verilen ve "Fermat'nın Son Teoremi" olarak adlandırılan, her $n \geq 3$ tamsayısı için $xy \neq 0$ olmak üzere $x^n + y^n = 1$ olacak biçimde x, y rasyonel sayılarının olamayacağını ifade eden bu teoreme de Fermat'yı denk sayı probleminin yönlendirdiğini belirtmektedir (Coates 2012). Wiles tarafından verilen ispat, özellikle 19. ve 20. yüzyıl-larda doğan ve gelişen cebirsel sayılar teorisi ile otomorf formlar teorisinin önemli bir uygulamasıdır.

1922 yılında Mordell, Fermat'nın 1 sayısının bir denk sayı olmadığını gösteren ispatını genelleştirerek, rasyonel katsayılara sahip her eliptik eğri için, bu eğri üzerindeki rasyonel koordinatlara sahip noktaların grubunun bir sonlu üreteçli abelyen grup olduğunu ispat etmiş ve bu harika sonuç modern aritmetik geometrinin başlangıç noktası olmuştur.

K. Heegner, 1952 yılında yayınlamış olduğu makalesinde, n bir doğal sayı olmak üzere $p = 8n + 5$ biçimindeki her p asal sayısının bir denk sayı olduğunu ispatlamış ve böylece sonsuz çoklukta denk sayı olduğunu gösteren ilk matematikçi olmuştur. Heegner'in bu ispatının ne kadar önemli olduğu ancak 1960'lı yılların sonunda Birch ve Swinnerton-Dyer konjektürünün ifade edilmesi ile anlaşılmıştır. Henüz ispatlanamamış olan bu konjektür, bir E eliptik eğrisi üzerinde sonsuz çoklukta rasyonel koordinatlara sahip nokta olması için gerek ve yeter koşulun E eliptik eğrisinin $L(E, s)$ serisinin $s = 1$ noktasında sıfır olması, olduğunu ifade eder. Eğer $L(E, s)$ serisi $s = 1$ noktasında sıfır olmuyor ise E eliptik eğrisi üzerinde sadece sonlu sayıda rasyonel koordinatlı nokta vardır ve üstelik bu sonuç, birçok denk olmayan sayının varlığının ispatlanmasında da kullanılmaktadır (işte bu nedenle denk sayı probleminin, Birch ve Swinnerton-Dyer konjektürünün en can alıcı uygulaması olduğu da söylenebilir). Konjektür, eğer doğru ise $n = 0, 1, 2, \ldots$ için $8n + 5$, $8n + 6$, $8n + 7$ formundaki sayılarının birer denk sayı (her denk sayı bu formda olmasa da, örneğin 34 sayısı bir denk sayı olduğu halde bu formda

değildir, bu formdaki sayıların birer denk sayı) oldukları öngörüsünde bulunur. Bununla birlikte, Y. Tian tarafından 2012 yılında yapılan çalışma, bu formda oldukça fazla asal olmayan denk sayı olduğunu belirtmekte, özellikle her bir $k \geq 1$ için k farklı tek asal çarpana sahip olan $8n + 5$, $8n + 6$, $8n + 7$ formunda sonsuz çoklukta karesiz denk sayı olduğunu ve üstelik bu denk sayıların nasıl oluşturulacaklarını da göstermektedir.

Yukarıdaki açıklamalar dikkate alındığında denk sayı problemi ile eliptik eğriler arasında oldukça sıkı bir ilişki olduğu açıktır. Özellikle "*Fermat'nın Son Teoremi*"nin ispatında aldığı rol ile son yıllarda oldukça popüler olan ve hatta bazı kaynaklarda denk sayı probleminin ele alınmasıyla ortaya çıkmış olduğu belirtilen eliptik eğriler teorisi, denk sayı probleminin çözüm yolunda büyük bir yol göstericidir.

2. DENK SAYILAR VE ELİPTİK EĞRİLER

Bu bölümde denk sayılar ve eliptik eğriler ile ilgili temel kavramlar verilecektir. Kısım 2.1'de denk sayı kavramının nasıl ortaya çıktığı üzerinde durulacak ve denk sayı kavramı tanımlanacaktır. Kısım 2.2'de denk sayı problemi ile eliptik eğriler arasında nasıl bir ilişki olduğu ele alınacaktır. Kısım 2.3'de E_N eliptik eğrileri ile çalışmalar yapabilmek için "sonsuzdaki nokta" olarak isimlendirilen özel noktaya ulaşabilmek için kısaca projektif düzlemden bahsedilecektir. Kısım 2.4'te genel olarak eliptik eğri kavramı ve bir cisim üzerinde tanımlanmış olan bir E_N eliptik eğrisinin noktalarının oluşturmuş olduğu küme üzerinde toplama işlemi tanımlanacak, bu kümenin toplama işlemi ile bir abelyen grup yapısına sahip olduğu gösterilecek ve eliptik eğriler ile ilgili bazı özellikler, temel sonuçlar bir araya getirilecektir. Kısım 2.5'de sonlu mertebeli nokta kavramı tanımlanacak, E_N eliptik eğrisi üzerindeki sonlu mertebeli noktalar, yani büküm noktaları ele alınacak ve daha sonra iki mertebeli, daha genel olarak *n* mertebeli noktaların grup yapısı ve $E(\mathbb{Q})$ gruplarının $E(\mathbb{Q})_{\text{tors}}$ alt grubuna bağlı olarak tam yapısını ortaya koyan Mordell Teoremi ifade edilecektir. Kısım 2.6'da singüler eğriler, bir eliptik eğrinin indirgenmişi ve bunlarla ilgili bazı temel sonuç ve teoremler verilecektir.

2.1. Denk Sayılar

Sayılar teorisini matematiğin birçok dalından ayıran en önemli özelliklerinden biri, çözümleri (ispatları) oldukça zor olan problemlerinin birçoğunun ifadelerinin oldukça basit olmasıdır. Bu çalışmada ele alınacak olan "*denk sayı problemi*" de oldukça basit bir ifadeye sahip olduğu halde henüz çözülemeyen en eski sayılar teorisi problemlerinden birisidir. Hangi doğal sayıların birer denk sayı olduğunun belirlenmesi olarak ifade edilebilecek olan denk sayı probleminin kolayca çözülebilecek bir problem olmadığı, çözümü üzerinde oldukça uzun zamandır birçok matematikçi uğraştığı halde henüz çözülememiş olmasından da açıktır.

6 tamsayısının, tüm kenar uzunlukları tamsayı olan bir dik üçgenin alanı olan en küçük doğal sayı olduğu antik zamanlardan beri bilinmektedir. Bundan başka alanı 6 ve kenar uzunlukları da birer **doğal sayı** olan tek dik üçgen 3-4-5 dik üçgenidir. Denk sayı

problemi üzerine yapılan çalışmalar, daha sonra üçgenin kenar uzunluklarının rasyonel sayı olmasına genişletilmiş ve Fibonacci tarafından 1225 yılında, alanı 5 ve kenar uzunlukları 3/2, 20/3 ve 41/6 rasyonel sayıları olan dik üçgen bulunmuştur. 5 sayısı bir doğal sayıdır ve üstelik 6 sayısından da küçüktür. Bu durum akıllara, hemen "Acaba her N doğal sayısı, kenar uzunlukları rasyonel sayılar olan bir dik üçgenin alanı olarak ifade edilebilir mi?" sorusunu getirmiştir. Yaklaşık 350 yıl önce, Fermat, N = 1, 2, 3, 4 sayılarına karşılık böyle dik üçgenlerin olmadığını, yani 1, 2, 3, 4 sayılarının birer denk sayı olmadığını ispatlamıştır. Dolayısıyla kenar uzunlukları rasyonel sayı olan bir dik üçgenin alanı olan doğal sayı anlamına gelen, denk sayıların en küçük olanı, yani 5 denk sayısı Fibonacci tarafından çoktan bulunmuştur.

İlk olarak tamsayılar halkası üzerinde oluşturulmuş olan denk sayı problemi, rasyonel sayılar cismine ve daha sonra rasyonel sayılar cisminden de daha genel sayı cisimleri üzerine taşınmış, kenar uzunlukları belli bir sayı cismine ait olan dik üçgenler dikkate alınmış ve denk sayı problemi daha genel olan bu sayı cisimleri üzerinde ele alınmıştır. Örneğin 1 sayısı, $\mathbb{Q}$ cismi üzerinde bir denk sayı olmadığı halde 1 sayısı, kenar uzunlukları $\sqrt{2}$, $\sqrt{2}$ ve 2 olan dik üçgenin alanı olduğundan $\mathbb{Q}(\sqrt{2})$ cismi üzerinde bir denk sayıdır. Bu çalışmanın amaçlarından birisi de denk sayı probleminin m, 1 sayısından farklı bir karesiz pozitif tamsayı olmak üzere $\mathbb{Q}(\sqrt{m})$ sayı cismi üzerinde ele alınmasıyla elde edilmiş olan sonuçları bir araya getirmektir.

Verilen bir N doğal sayısının bir denk sayı olup olmadığını belirlemek için sonlu sayıda adımdan oluşan koşulsuz bir algoritma henüz ortaya konulamamıştır. N sayısının bir denk sayı olduğunu göstermenin en doğal yolu, alanı N olan bir rasyonel dik üçgen elde etmek olduğu halde bu özellikteki bir dik üçgenin bulunması da öyle çok kolay değildir. Örneğin, D. Zagier (Zagier 1987) alanı 157 olan dik üçgenin dik kenar uzunluklarının

$$X = \frac{6803298487826435051217540}{411340519227716149383203},\ Y = \frac{41134051922771614938320 3}{2166655569371476130961 0}$$

olduğunu, oldukça uzun çalışmalar sonrası gösterebilmiştir. Alanı 157 olan bu üçgenin, yukarıda belirtilen kenar uzunluklarının, denemeler yapılarak kolayca bulunamayacağı açıktır.

2.1.1. Tanım. Kenar uzunlukları rasyonel ve alanı N doğal sayısına eşit olan bir dik üçgen varsa N doğal sayısına bir ***denk sayı*** denir.

Yukarıda verilmiş olan denk sayı tanımının, eğer N doğal sayısı için

$$a^2 + b^2 = c^2 \text{ ve } \frac{1}{2}ab = N$$

olacak biçimde $a, b, c \in \mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ sayıları varsa N sayısına bir *denk sayı* denir, biçiminde ifade edilebileceği açıktır. Pisagor üçlülerinin Euclid karakterizasyonu kullanılarak, alanı ve kenar uzunlukları tamsayılar olan bir dik üçgenin var olup olmadığına karar vermek çok kolay olduğu halde dik üçgenin kenar uzunluklarının tamsayı olmaması halinde bu yöntem kullanılamaz.

2.1.2. Örnek. $N = 6$, kenar uzunlukları 3, 4, 5 ve alanı 6 olan dik üçgene karşılık gelen bir denk sayıdır. $N = 5$ sayısı da kenar uzunlukları $\frac{3}{2}$, $\frac{20}{3}$, $\frac{41}{6}$ ve alanı 5 olan dik üçgene karşılık gelen bir denk sayıdır.

İki üçgen benzer ise bu üçgenlerin kenarları orantılıdır ve üstelik eğer bu orantı sabiti α ise üçgenlerin alanlarının oranın da α^2 olacağı açıktır. Bu nedenle denk sayı problemi, 1 sayısından büyük kare bulundurmayan (karesiz) doğal sayılara, yani tekrar eden asal çarpanları olmayan sayılara indirgenebilir. Dolayısıyla 2 ve 3 sayıları birer denk sayı olmadıklarından $4 = 2^2 \cdot 1$, $9 = 3^2 \cdot 1$ ve $8 = 2^2 \cdot 2$ sayıları da birer denk sayı olamaz. 10 sayısından küçük olan altı karesiz doğal sayı arasından üç tanesi (5, 6, 7 sayıları) birer denk sayı olduğu halde diğer üç tanesi birer denk sayı değildir. Bu bilgi "N sayısı, $N \equiv 5, 6, 7 \pmod 8$ olacak biçimdeki bir karesiz doğal sayı ise N, kenar uzunlukları rasyonel olan bir dik üçgenin alanıdır, yani bir denk sayıdır" konjektürünün ifade edilmesine neden olmuştur. Bu konjektür dikkate alındığında, 8 modülüne göre 1, 2, 3 sayılarına denk olan karesiz sayıların birer denk sayı olmadıkları tahmin edilebilir, ancak bu tahminin yanlış olduğu görülmüştür.

Denk sayı problemi, denk sayı olabilecek olan tüm denk sayıların belirlenmesidir, bu nedenle başlangıç olarak kenar uzunlukları tamsayı olan tüm dik üçgenler sınıflandırılacaktır.

2.1.3. Teorem. X, Y, Z tamsayıları, bir dik üçgenin obeb$(X, Y, Z) = 1$ özelliğindeki kenar uzunlukları olsun. O halde $X = 2mn$, $Y = m^2 - n^2$ ve $Z = m^2 + n^2$ olacak biçimde $m, n \in \mathbb{N}$ vardır. Tersine, herhangi $m, n \in \mathbb{N}$ için obeb$(X, Y, Z) = 1$ ve kenar uzunlukları $X = 2mn$ $Y = m^2 - n^2$ ve $Z = m^2 + n^2$ olacak biçimde bir dik üçgen vardır (Brown 2003).

İspat. Verilen herhangi $m, n \in \mathbb{N}$ için verilen formüller kullanılarak kenar uzunlukları tamsayı olan bir dik üçgen elde edileceği açıktır. O halde obeb(X, Y, Z) = 1 olmak üzere kenar uzunlukları $X, Y, Z \in \mathbb{Z}$ olarak verilen bir dik üçgenden böyle m ve n sayılarının elde edilebileceğini gösterelim. $X^2 + Y^2 = Z^2$ olduğundan X ve Y tek sayı ise $Z^2 \equiv 2 \pmod 4$ olur. Ancak 4 modülüne göre kare sayıların 0 ve 1 oldukları dikkate alınırsa X ve Y tamsayılarının tek olmadığı sonucu elde edilir. Dolayısıyla X veya Y mutlaka çift olmalıdır. Genelliği bozmadan, X çift sayı olarak alınırsa $\frac{X}{2}$ bir tamsayı olur.

$$\left(\frac{X}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - \left(\frac{Y}{2}\right)^2 = \left(\frac{Z-Y}{2}\right)\left(\frac{Z+Y}{2}\right)$$

eşitliğini dikkate alalım. Eğer p, $\frac{X}{2}$ sayısını bölen bir asal sayı ise $p^2 \mid \left(\frac{X}{2}\right)^2$ dir. p bir asal sayı olduğundan $p \mid \left(\frac{Z-Y}{2}\right)$ ya da $p \mid \left(\frac{Z+Y}{2}\right)$ dir. obeb(X, Y, Z) = 1 olduğundan p asal sayısı bu sayıların her ikisini de bölmez, yani $p^2 \mid \left(\frac{Z-Y}{2}\right)^2$ ya da $p^2 \mid \left(\frac{Z+Y}{2}\right)^2$ dir. $\frac{X}{2}$ sayısını bölen tüm asal sayılar dikkate alınarak, m ve n sayıları, sırasıyla, bu asal sayılardan $\frac{Z-Y}{2}$ ve $\frac{Z+Y}{2}$ sayılarını bölenlerden oluşmak üzere $\left(\frac{X}{2}\right)^2 = m^2n^2$ biçiminde yazılabilir. Genelliği bozmadan, $m > n$ olmak üzere $X = 2mn$, $Y = m^2 - n^2$ ve $Z = m^2 + n^2$ olarak alınabilir.■

Bu teorem, kenar uzunlukları tamsayı olan dik üçgenlerden elde edilen tüm denk sayıların üretilmesine olanak verir. Aşağıda bu denk sayılardan bazıları yer almaktadır.

Çizelge 2.1. Pisagor Üçlülerinden Elde Edilen Denk Sayılar

m	***n***	***X***	***Y***	***Z***	***N***
2	1	4	3	5	6
3	1	6	8	10	24
3	2	12	5	13	30
4	1	8	15	17	60
4	3	24	7	25	84
4	2	16	12	20	96
5	1	10	24	26	120
5	4	40	9	41	180

Doğal olarak sadece tamsayı kenar uzunluklara sahip dik üçgenlerin ele alınması yerine rasyonel kenar uzunluklara sahip olan dik üçgenler de ele alınabilir. N bir denk sayı olmak üzere kenar uzunlukları $X, Y, Z \in \mathbb{Q}$ olan bir dik üçgene sahip olduğumuzu varsayalım. a, X ve Y sayılarının paydalarının en küçük ortak katı olmak üzere X ve Y sayılarının a sayısı ile çarpılmasıyla kenar uzunlukları tamsayı olan bir dik üçgen ve aN^2 denk sayısının elde edilebileceği görülebilir. Dolayısıyla kenar uzunlukları rasyonel olan bir dik üçgenden, kenar uzunlukları tamsayı olan bir dik üçgen ve bir kare sayı ile bölünebilen yeni bir denk sayı elde edilebilir. Tersine, kenar uzunlukları $X, Y, Z \in \mathbb{Z}$ olan bir dik üçgen ve $N = a^2N_0$ denk sayısı verildiğinde X ve Y, a ile bölünerek kenar uzunlukları rasyonel olan bir dik üçgen ve bu dik üçgenden de N_0 denk sayısı elde edilir.

2.1.4. Örnek. $m = 5$ ve $n = 4$ olmak üzere kenar uzunlukları 40, 9 ve 41 olan dik üçgeni göz önüne alalım. Bu üçgenin alanı $180 = 6^2 \cdot 5$ dir. Böylece 5 sayısı, kenar uzunlukları $\frac{3}{2}$, $\frac{20}{3}$ ve $\frac{41}{6}$ olan bir dik üçgen ile elde edilen bir denk sayıdır.

Çizelge 2.2. Rasyonel Dik Üçgenlerden Elde Edilen Denk Sayılar

X	***Y***	***Z***	***N***
3/2	20/3	41/6	5
4/9	7/4	65/36	14
4	15/2	17/2	15
7/2	12	25/2	21
4	17/36	145/36	34
28/9	5	53/9	70

Bu yöntem, kenar uzunlukları rasyonel olan dik üçgenlerden elde edilen denk sayıları üretmek için Teorem 2.1.3. de verilen Pisagor üçlülerinin kullanılmasına olanak verir. Gerçekte denk sayıların sayısı sonsuz çoklukta olduğundan asıl amaç çok sayıda denk sayı üretmek değil verilen bir doğal sayının bir denk sayı olup olmadığının belirlenmesi veya belirlenmesinde kullanılacak bir algoritmanın oluşturulmasıdır. Yukarıda verilmiş olan yöntem kullanılarak, alanı N olan bir dik üçgen bulunamaz ise N sayısının bir denk sayı olmadığı sonucu elde edilir. Bununla birlikte böyle bir üçgenin olmadığını

göstermek zor değilmiş gibi de görünebilir. Örneğin, 157 bir denk sayı olduğu halde, alanı 157 olan en basit dik üçgenin kenar uzunlukları

$$X = \frac{680329848782643505121754 0}{411340519227716149383203}\ ,\ Y = \frac{411340519227716149383203}{21666555693714761309610}$$

dir. Dolayısıyla bu problemi çözmek için yeni bir yönteme ihtiyaç olduğu açıktır. Bu yönteme geçmeden önce böyle bir N sayısına neden bir denk sayı denildiğini açıklamaya öncelik verelim. Aşağıdaki teorem bu soruya bir cevap oluşturmaktadır, eğer N sayısı bir denk sayı ise N modülüne göre birbirine denk olan üç kare rasyonel sayı elde edilebilir.

2.1.5. Teorem. N, bir karesiz pozitif tamsayı ve $X < Y < Z$ olmak üzere X, Y ve Z birer pozitif rasyonel sayı olsun. Kenar uzunlukları X, Y, Z ve alanı N olan dik üçgenler ile her biri bir rasyonel sayının karesi olan $x - N$, x, $x + N$ rasyonel sayıları arasında bir birebir eşleme vardır. Bu eşleme X, Y, Z sayıları için

$$x = (Z/2)^2$$

ve x rasyonel sayısı için

$$X = \sqrt{x+N} - \sqrt{x-N},\ Y = \sqrt{x+N} + \sqrt{x-N},\ Z = 2\sqrt{x}$$

biçimindedir. Özel olarak, N sayısının bir denk sayı olması için gerek ve yeter koşul $x - N$, x ve $x + N$ sayılarının her birisinin rasyonel sayıların kareleri olacak biçimde bir x rasyonel sayısının var olmasıdır (Koblitz 1993, Brown 2003).

İspat. İlk olarak X, Y ve Z sayılarının istenilen özellikteki bir üçlü olduğunu varsayalım, yani $X^2 + Y^2 = Z^2$ ve $\frac{XY}{2} = N$ olsun. Eğer birinci eşitlikten ikinci eşitliğin dört katı çıkarılır ya da birinci eşitliğe ikinci eşitliğin dört katı eklenirse $(X \pm Y)^2 = Z^2 \pm 4N$ ve daha sonra bu eşitliğin her iki tarafı dört ile bölünürse $\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm N$ eşitliği elde edilir. Böylece $x \pm N$ sayılarının $\left(\frac{X \pm Y}{2}\right)^2$ biçimindeki bir rasyonel sayının karesi ve x sayısının da $\left(\frac{Z}{2}\right)^2$ özelliğindeki kare sayılar oldukları sonucu elde edilmiş olur.

Tersine istenilen özellikteki x sayısı verilmiş olsun. Bu durumda $X < Y < Z$ pozitif rasyonel sayılar olmak üzere x ve N sayıları için

$$X^2 + Y^2 = \left(\sqrt{x+N} - \sqrt{x-N}\right)^2 + \left(\sqrt{x+N} + \sqrt{x-N}\right)^2 = 4x = Z^2$$

$$XY = \left(\sqrt{x+N} - \sqrt{x-N}\right)\left(\sqrt{x+N} + \sqrt{x-N}\right) = (x+N) - (x-N) = 2N$$

eşitliklerinin gerçeklendiği açıktır. Son olarak X, Y, Z rasyonel sayıları ve x, N sayıları arasında bir birebir eşleme olduğu da görülebilir.■

Aşağıdaki teorem kullanılarak, denk sayı problemi, Diophant denklemler teorisinin bir problemine dönüştürülür. Bu teorem kullanılarak teoremin ifadesinde yer alan iki Diophant denklemi ile tanımlanan uzay eğrisinin $y^2 = x^3 - a^2x$ düzlem eğrisine eşit olduğu sonucu elde edilir.

2.1.6. Teorem. a doğal sayısının bir denk sayı olması için gerek ve yeter koşul dört bilinmeyenli

$$x^2 + ay^2 = z^2$$

$$x^2 - ay^2 = t^2 \tag{2.1}$$

denklem sisteminin aşikar olmayan tamsayı çözümüne sahip olmasıdır (Chahal 2006).

İspat. Verilen denklem sisteminin aşikar olmayan tamsayı çözümleri var ve $y > 0$ olmak üzere (2.1) eşitliğinin tamsayı çözümlerinin x, y, z ve t olduğunu varsayalım. Bundan başka x, y, z ve t sayılarının pozitif oldukları da varsayılabilir. Bu durumda z sayısının x, y, z ve t sayılarının en büyüğü olduğu açıktır. Yukarıdaki denklem sisteminde ilk eşitlikten ikinci eşitlik çıkarıldığında

$$a = \frac{1}{2}\left(\frac{z+t}{y}\right)\left(\frac{z-t}{y}\right)$$

olarak bulunur. Şimdi $r = \frac{z+t}{y}$ ve $s = \frac{z-t}{y}$ sayılarının bir dik üçgenin kenar uzunluklarını temsil ettiği ve aynı zamanda hipotenüs uzunluğu olan h sayısının da bir rasyonel sayı olduğunu görelim. (2.1) ile verilen eşitlikler taraf tarafa toplandığında

$$z^2 + t^2 = 2x^2$$

elde edilir. Bu eşitlik kullanılarak

$$r^2 + s^2 = \left(\frac{z+t}{y}\right)^2 + \left(\frac{z-t}{y}\right)^2 = \frac{2(z^2+t^2)}{y^2} = \left(\frac{2x}{y}\right)^2 = h^2$$

ve $x, y \in \mathbb{Q}$ olduğundan $h = \frac{2x}{y} \in \mathbb{Q}$ olduğu sonucu elde edilir. Tersine r, s ve h pozitif rasyonel sayılar olmak üzere

$$a = \frac{1}{2}rs,\ r^2 + s^2 = h^2 \tag{2.2}$$

ve $h > r > s$ olduğunu varsayalım ($\sqrt{2}$ rasyonel olmadığından $r = s$ olması mümkün değildir). (2.2) eşitliği kullanılarak

$$(r \pm s)^2 = r^2 + s^2 \pm 2rs = h^2 \pm 4a$$

veya

$$\left(\frac{h}{2}\right)^2 \pm a = \left(\frac{r \pm s}{2}\right)^2 \tag{2.3}$$

eşitlikleri elde edilir. (2.3) eşitliğindeki paydalar yok edildiğinde $y > 0$ olmak üzere (2.1) eşitliğinin bir tamsayı çözümü elde edilir. ■

Fibonacci, yukarıdaki (2.1) eşitliğinde x =41, y = 12, z = 49 ve t = 31 olarak alındığında

$$41^2 + 5 \cdot 12^2 = 49^2 \text{ ve } 41^2 - 5 \cdot 12^2 = 31^2,$$

dolayısıyla 5 sayısının bir denk sayı olduğu sonucunu elde etmiştir.

2.1.7. Teorem. Sekiz modülüne göre her kabul edilebilir kalan sınıfı sonsuz çoklukta denk sayı bulundurur (Chahal 2006).

Bu teoremin ispatı aşağıdaki teoremler ifade edildikten sonra ele alınacaktır. Denk sayı problemi ile ilgili çalışmalar yapılırken sadece karesiz sayılar dikkate alındığından $a \equiv 0$ veya 4 (mod 8) özelliğindeki a tamsayıları kabul edilebilir sayılar olamaz. Ancak a sayısının 4 ile bölünebilen bir sayı olması halinde teoremdeki "kabul edilebilir" kelimesi kaldırılabilir. Aşağıdaki teorem denk sayılar ve eliptik eğriler arasındaki ilişkiyi ortaya koymaktadır.

2.1.8. Teorem. $a > 0$ olmak üzere a karesiz tamsayısının bir denk sayı olması için gerek ve yeter koşul

$$y^2 = x^3 - a^2x \tag{2.4}$$

eşitliği ile tanımlanan E eliptik eğrisinin sonsuz çoklukta rasyonel noktaya sahip olmasıdır (Chahal 2006).

Bu teoremin ispatı da daha sonra 2.5 kısmında Lutz-Nagell teoremi ifade edildikten sonra ele alınacaktır. Fermat'nın en bilinen sonuçlarından birisi, Fermat'nın Son Teoreminin $X^4 + Y^4 = Z^4$ haline karşılık gelen aşağıdaki teoremdir.

2.1.9. Teorem (Fermat). $x^4 + y^4 = z^2$ (2.5)

Diophant denkleminin tamsayılarda aşikar olmayan (yani, $xyz \neq 0$) çözümü yoktur (Chahal 2006).

d sıfırdan farklı bir tamsayı olmak üzere,

$$x^4 + dy^4 = z^2 \tag{2.6}$$

eşitliğine (2.5) eşitliğinin bir ***kıvrılması*** (twist) denir. (2.6) eşitliğinin $t > 0$ olmak üzere aşikar olmayan s, t, u çözümünden

$$y^2 = x^3 + dx \tag{2.7}$$

eşitliği ile tanımlanan E eliptik eğrisi üzerinde

$$x = s^2/t^2,\ y = su/t^3 \tag{2.8}$$

olmak üzere bir rasyonel $P = (x, y)$ noktası elde edilir. 1878'de Fransız matematikçi Desboves (Desboves 1879),

$$(y^2 + 2xy - x^2)^4 + (2x^3 + x^2y^2)(2x + 2y)^4 = (x^4 + y^4 + 10x^2y^2 + 4xy^3 + 12x^3y)^2 \tag{2.9}$$

özdeşliğini (Chahal 1984) kullanarak d sayısının belli değerleri için (2.6) eşitliğinin bir aşikar olmayan çözümünün varlığını ispatlamıştır.

Eğer (2.9) eşitliğinde $x = 1 - 2\lambda$ ve $y = 4\lambda$ olarak alınırsa

$$(1 - 12\lambda + 4\lambda^2)^4 + 8\lambda(2\lambda - 1)^2\,(2(1 + 2\lambda))^4 = (1 + 40\lambda - 104\lambda^2 + 160\,\lambda^3 + 16\lambda^4)^2$$

ve $d = d(\lambda) = 8\lambda(2\lambda - 1)^2$ için

$$x = x(\lambda) = \frac{(1-2\lambda+4\lambda^2)^2}{4(1+2\lambda)^2} \text{ ve } y = y(\lambda) = \frac{(1-12\lambda+4\lambda^2)(1+40\lambda-104\lambda^2+160\lambda^3+16\lambda^4)}{8(1+2\lambda)^3}$$

olmak üzere (2.8) eşitliği ile verilen E eliptik eğrisi üzerinde bir $P = (x, y)$ rasyonel noktası elde edilir. Böylece $r_{\mathbb{Q}}(E)$, 2.5 Kısmında tanımlanacak olan, eliptik eğrinin rankı olmak üzere, yukarıda ifadesi verilmiş ve 2.5 Kısmında ele alınacak olan Lutz-Nagell Teoremi gereği, aşağıdaki sonuç elde edilir.

2.1.10. Teorem. λ sıfırdan farklı bir tamsayı olmak üzere $d = d(\lambda) = 8\lambda(2\lambda - 1)^2$ için

$$E : y^2 = x^3 + dx$$

ise $r_{\mathbb{Q}}(E) > 0$ dır (Chahal 2006).

Böylece Lutz-Nagell Teoremi, Teorem 2.1.8. ve Teorem 2.1.10. birlikte ele alındığında aşağıdaki sonuç elde edilir.

2.1.11. Sonuç. Her bir m pozitif tamsayısı için $a = m(4m^2 + 1)$ tamsayısı bir denk sayıdır (Chahal 2006).

İspat. Teorem 2.1.10. da $\lambda = -2m^2$ olarak alınırsa

$$d(\lambda) = -(2^2 m(4m^2 + 1))^2$$

dir. O halde Teorem 2.1.7. gereği, $2^2 m(4m^2 + 1)$ sayısı bir denk sayıdır. Bu sayıdaki kare çarpan yok edildiğinde $m(4m^2 + 1)$ sayısının da bir denk sayı olduğu görülür. ■

Teorem 2.1.7.'nin İspatı. Sonuç 2.1.11. de $m = 2s + t$ olarak alınırsa

$$a = m(4m^2 + 1) = (2s + t)\cdot(4(2s + t)^2 + 1) \equiv 4t^3 + 2s + t \pmod 8$$

elde edilir. $0 \leq r < 8$ özelliğindeki r sayıları için $t = 0$ veya 1 olarak alınırsa $4t^3 + 2s + t \equiv r \pmod 8$ denkliğini gerçekleyen sonsuz çoklukta s sayısının bulunacağı açıktır. ■

Yukarıdaki tartışma herhangi $m > 0$ tamsayısı ve işaretin herhangi seçimi için

$$(1 + 24m^2 + 16m^4)^2 \pm m(4m^2 + 1)(2(4m^2 - 1))^2$$

sayısının bir mükemmel kare sayı olduğunu da gösterir. $a \geq 1$ karesiz ve $y = 2c(4m^2 - 1)$ olmak üzere $m(4m^2 + 1) = ac^2$ olarak alınırsa, u ve v tamsayıları için

$$(1 + 24m^2 + 16m^4)^2 + ay^2 = u^2$$

$$(1 + 24m^2 + 16m^4)^2 - ay^2 = v^2 \qquad (2.10)$$

olarak ifade edilebilir. Bu iki eşitlikten, kenar uzunlukları $\frac{u+v}{y}$ ve $\frac{u-v}{y}$ olan dik üçgenin alanı

$$a = \frac{1}{2}\left(\frac{u+v}{y}\right)\left(\frac{u-v}{y}\right)$$

ve hipotenüs uzunluğu da

$$h = \left(\left(\frac{u+v}{y}\right)^2 + \left(\frac{u-v}{y}\right)^2\right)^{1/2} = \frac{2(1+24m^2+16m^4)}{y}$$

olarak bulunur, *h* sayısının bir rasyonel sayı olduğu açıktır.

2.1.12. Örnek 1. *m* = 1 için (2.10) eşitliği

$$41^2 + 5\cdot 12^2 = 49^2, \quad 41^2 - 5\cdot 12^2 = 31^2$$

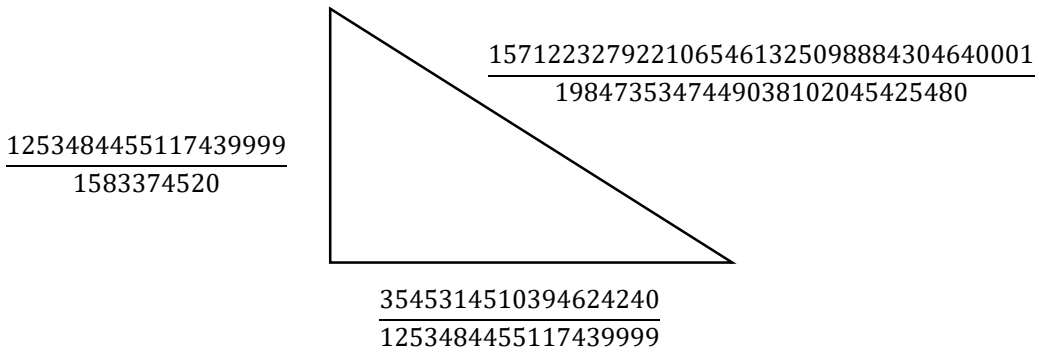
halini alır. Dolayısıyla, Fibonacci tarafından bulunmuş olan ve alanı da 5 olan dik üçgenin kenar uzunlukları

$$\frac{49+31}{12} = \frac{20}{3}, \quad \frac{49-31}{12} = \frac{3}{2}, \quad \frac{2\cdot 41}{12} = \frac{41}{6}$$

biçimindedir.

2. *m* = 6 olarak alınırsa, dört farklı asal sayının çarpımı olan *a* = 2·3·5·29 denk sayısı elde edilir. Alanı *a* = 2·3·5·29 olan rasyonel dik üçgenin kenar uzunlukları 143/2, 3480/143 ve 21601/286 dır.

3. *m* = 23660^2 olsun. Bu durumda *a* = 1 119 543 881 denk sayısı bir asal sayıdır. Alanı *a* olan rasyonel dik üçgenin kenar uzunlukları Şekil 2.1 de gösterildiği gibidir.



Şekil 2.1. Alanı *a* = 1 119 543 881 asal sayısı olan bir rasyonel dik üçgen

2.2. Denk Sayılardan Eliptik Eğrilere

Bu kısımda "Kenar uzunlukları $X, Y, Z \in \mathbb{Q}$ ve alanı N olacak biçimde bir dik üçgen bulunabilir mi?" sorusu ele alınacak, başka bir deyişle

$$X^2 + Y^2 = Z^2 \quad \text{ve} \quad \frac{1}{2}XY = N$$

eşitliklerinden yola çıkarak, bu eşitliği gerçekleyen $X, Y, Z \in \mathbb{Q}$ sayılarının belirlenmesi probleminin belli bir eliptik eğri üzerindeki rasyonel koordinatlı noktaların problemine dönüştürülebileceği gösterilecektir.

N, kenar uzunlukları $X, Y, Z \in \mathbb{Q}$ olan bir dik üçgen ile elde edilen bir denk sayı yani,

$$X^2 + Y^2 = Z^2 \tag{2.11}$$

ve

$$\frac{1}{2}XY = N \tag{2.12}$$

olsun. (2.12) eşitliğinin her iki tarafı 4 ile çarpılır ve elde edilen yeni eşitlik (2.11) eşitliği ile toplanır ve çıkarılırsa

$$(X + Y)^2 = Z^2 + 4N \quad \text{ve} \quad (X - Y)^2 = Z^2 - 4N$$

eşitlikleri ve dolayısıyla

$$\left(\frac{X+Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 + N \tag{2.13}$$

ve

$$\left(\frac{X-Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - N \tag{2.14}$$

eşitlikleri elde edilir. (2.13) ve (2.14) eşitlikleri birlikte çarpıldığında

$$\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 + N^2$$

eşitliği elde edilir. Dolayısıyla N denk sayısına karşılık gelen bir rasyonel dik üçgen,

$$v^2 = u^4 - N^2 \tag{2.15}$$

eşitliği için $u = \left(\frac{Z}{2}\right)$ ve $v = \left(\frac{X^2-Y^2}{4}\right)$ biçiminde bir rasyonel çözüm üretir. (2.15) eşitliği u^2 ile çarpılarak

$$(uv)^2 = u^6 - N^2u^2$$

eşitliği elde edilir. $x = u^2 = \left(\frac{Z}{2}\right)^2$ ve $y = uv = \frac{Z(X^2-Y^2)}{8}$ olarak alınırsa N denk sayısına karşılık gelen bir rasyonel dik üçgenin

$$E_N : y^2 = x^3 - N^2x \tag{2.16}$$

eşitliği için bir rasyonel çözüm ürettiği elde edilir. Bu eğri, bir eliptik eğri belirtir, bu eğriler daha detaylı bir şekilde daha sonraki bölümlerde ele alınacak olmasına karşılık bu sürecin tersine çevrilebileceğini ve N sayısının bir denk sayı olduğunu göstermek için E_N eliptik eğrileri üzerindeki noktaların kullanılabileceğini belirtmekte fayda vardır.

2.2.1. Önerme. (x_0, y_0), $E_N : y_0^2 = x_0^3 - N^2x_0$ eliptik eğrisi üzerinde rasyonel koordinatlı bir nokta ve x_0 rasyonel sayısı,

i. x_0, bir rasyonel sayının karesidir,

ii. x_0 sayısının paydası çifttir,

iii. x_0 sayısının payı ile N aralarında asaldır,

koşullarını gerçeklesin. Bu durumda

$$X = \sqrt{x_0 + N} - \sqrt{x_0 - N},\ Y = \sqrt{x_0 + N} + \sqrt{x_0 - N} \text{ ve } Z = 2\sqrt{x_0}$$

olmak üzere kenar uzunlukları $X, Y, Z \in \mathbb{Q}$ ve alanı N olan bir dik üçgen vardır (Brown 2003).

İspat. $u \in \mathbb{Q}$ olmak üzere $x_0 = u^2$ ve $v = \frac{y_0}{u}$ olsun. Dolayısıyla

$$v^2 = \frac{{y_0}^2}{u^2} = \frac{{x_0}^3 - N^2x_0}{x_0} = x_0^2 - N^2$$

ve böylece

$$x_0^2 = N^2 + v^2 \tag{2.17}$$

olur. u sayısının paydası t olsun. $u^2 = x_0$ ve varsayım gereği, x_0 sayısının paydası çift olduğundan $2|t$ olmalıdır. Üstelik N bir tamsayı ve $x_0{}^2 = N^2 + v^2$ olduğundan v^2 ve x_0^2 sayılarının paydaları aynıdır ve t^4 dir. (2.17) eşitliği t^2 ile çarpılarak t^2N, t^2v, $t^2x_0 \in \mathbb{Z}$ olmak üzere t^2N, t^2v ve t^2x_0 biçiminde bir Pisagor üçlüsü elde edilir. (*iii*) koşulu gereği, x_0 ve N sayısı aralarında asal olduklarından obeb(t^2N, t^2v, t^2x_0) = 1 dir. Böylece Teorem 2.1.3. gereği, $t^2N = 2mn$, $t^2v = m^2 - n^2$ ve $t^2x_0 = m^2 + n^2$ olacak biçimde m ve n doğal sayıları vardır. $X = \frac{2m}{t}$, $Y = \frac{2n}{t}$, $Z = 2u$ üçlüsünü göz önüne alınırsa,

$$X^2 + Y^2 = \frac{4}{t^2}(m^2 + n^2) = \frac{4}{t^2}(t^2x_0) = 4x_0 = (2u)^2 = Z^2,$$

yani bu üçlü bir dik üçgen belirtir ve bu üçgenin alanı

$$\frac{1}{2}XY = \frac{1}{2}\frac{4mn}{t^2} = \frac{2mn}{t^2} = N$$

dir. Böylece iddia edildiği gibi, kenar uzunlukları rasyonel ve alanı N olan bir dik üçgenin var olduğu sonucu elde edilir. ■

2.2.2. Uyarı. A ve B kümeleri

$$A = \{(X, Y, Z) \in \mathbb{Q}^3 \mid \frac{1}{2}XY = N, X^2 + Y^2 = Z^2\}$$

$$B = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - N^2x, y \neq 0\}$$

biçiminde olmak üzere A ve B kümeleri arasında

$$f(X, Y, Z) = \left(-\frac{NY}{X+Z}, \frac{2N^2}{X+Z}\right) \text{ ve } g(x, y) = \left(\frac{N^2-x^2}{y}, -\frac{2xN}{y}, \frac{N^2+x^2}{y}\right)$$

dönüşümleri ile verilen bir birebir ve örten dönüşüm vardır (Brown 2003).

2.3. Projektif Düzlem

Bu kısımda, E_N eliptik eğrileri ile çalışmalar yapabilmek için "sonsuzdaki nokta" olarak isimlendirilen özel noktaya ulaşabilmek için kısaca projektif düzlemden bahsedilecektir.

$x, y, z \in \mathbb{C}$ olmak üzere $(x, y, z) \neq (0, 0, 0)$ biçimindeki (x, y, z) sıralı üçlülerini göz önüne alalım. Belli $\lambda \in \mathbb{C}\backslash\{0\}$ için $x = \lambda a$, $y = \lambda b$ ve $z = \lambda c$ ise (x, y, z) ve (a, b, c) sıralı üçlülerine ***denk üçlüler*** denir ve bu durum $(x, y, z) \sim (a, b, c)$ ile gösterilir, yani

$$(x, y, z) \sim (a, b, c) \Leftrightarrow (x, y, z) = (\lambda a, \lambda b, \lambda c),\ \lambda \in \mathbb{C}\backslash\{0\}$$

dir. "∼" bağıntısının bir denklik bağıntısı olduğu kolayca görülebilir, (x, y, z) sıralı üçlüsünün denklik sınıfı $(x : y : z)$ ile gösterilir. Bu şekilde elde edilen sıralı üçlülerin denklik sınıflarının oluşturduğu kümeye ***projektif düzlem*** denir ve $\mathbb{P}^2_{\mathbb{C}}$ ile gösterilir, yani

$$\mathbb{P}^2_{\mathbb{C}} = \{(x : y : z) \mid x, y, z \in \mathbb{C}, (x, y, z) \neq (0, 0, 0)\}$$

dir. Projektif düzlemler $\mathbb{C}$ cisminden başka cisimler üzerine de kurulabilir. Örneğin, $\mathbb{K}$ bir cisim olmak üzere $\mathbb{P}^2_{\mathbb{K}}$, $\mathbb{P}^2_{\mathbb{R}}$ ve $\mathbb{P}^2_{\mathbb{Q}}$ projektif düzlemleri de $\mathbb{P}^2_{\mathbb{C}}$ projektif düzlemine benzer şekilde tanımlanır.

$z \neq 0$ olmak üzere $(x : y : z) \in \mathbb{P}^2_{\mathbb{C}}$ denklik sınıfı $(x/z : y/z : 1)$ biçiminde ifade edilir, genellikle $(x : y : z) = (x/z : y/z : 1)$ olarak alınır. Bu şekildeki noktalara, $\mathbb{P}^2_{\mathbb{C}}$ ***projektif düzlemindeki sonlu noktalar*** denir. $z = 0$ olmak üzere $(x : y : 0)$ biçimindeki noktalara da $\mathbb{P}^2_{\mathbb{C}}$ ***projektif düzlemindeki sonsuzdaki noktalar*** denir.

Projektif düzlem üzerinde bileşen bileşene toplama ve çarpma işlemleri tanımlanabilir, $(x_1 : y_1 : z_1), (x_2 : y_2 : z_2) \in \mathbb{P}^2_{\mathbb{C}}$ olmak üzere, bu işlemler, sırasıyla,

$$(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_1 + x_2 : y_1 + y_2 : z_1 + z_2)$$

ve

$$(x_1 : y_1 : z_1)\cdot(x_2 : y_2 : z_2) = (x_1 \cdot x_2 : y_1 \cdot y_2 : z_1 \cdot z_2)$$

olarak tanımlanır. Bu işlemlerin iyi tanımlı, yani toplama ve çarpma işlemlerinin denklik sınıflarından seçilen temsilcilerden bağımsız oldukları görülebilir.

Projektif düzlem, alışılmış xy-düzleminin bir genellemesinden başka bir şey değildir, özel olarak $z = 1$ olarak alınırsa, alışılmış xy-düzlemindeki noktalara dönülmüş olur. Bu durum $z \neq 0$ olmak üzere her denklik sınıfında z^{-1} ile çarpıldığında bir tek $(x, y, 1)$ noktasını veren (x, y, z) noktasının olması gerçeğinden ortaya çıkmaktadır. $z = 0$ olması halinde elde edilen noktalar ise sonsuzdaki doğru üzerindeki noktalar olarak adlandırılırlar. $(0 : 1 : 0)$ noktası da bu doğru üzerindeki noktalardan birisidir ve üstelik $(0 : 1 : 0)$ noktası, E_N eliptik eğrisi üzerindeki noktalardan bu doğru üzerinde bulunan tek nokta olacaktır.

Verilen herhangi $f(x, y) = 0$ eğrisi, projektif düzlemdeki bir eğri ile ilişkilendirilebilir. Bir $x^i y^j$ monomunun derecesi $i + j$ olmak üzere $f(x, y)$ polinomunun derecesi, bu polinomu oluşturan monomların en yüksek dereceli olanının derecesi olarak tanımlanır. $f(x, y)$ polinomunun derecesi n olmak üzere bu polinomun her bir $x^i y^j$ monomunun z^{n-i-j} ile çarpılmasıyla elde edilen $F(x, y, z)$ polinomuna ***n.dereceden homojen polinom*** denir. Örneğin $F(x, y, z) = 2x^4 - 5xy^2z + 7y^3z$ dördüncü dereceden bir homojen polinomdur. Bundan başka, n dereceli bir homojen $F(x, y, z)$ polinomundan $z = 1$ alınarak bir $f(x, y)$ polinomu elde edilebilir. Örneğin $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$ üçüncü dereceden bir homojen polinomdur ve $F(x, y, z) = z^3 f\left(\frac{x}{z}, \frac{y}{z}\right)$ dir, eğer $z = 1$ olarak alınırsa $F(x, y, 1) = f(x, y)$ olarak elde edilir. Özel olarak $f(x, y) = y^2 - x^3 + N^2x$ polinomundan elde edilen homojen polinom da $F(x, y, z) = y^2z - x^3 + N^2xz^2$ dir.

Homojen polinomlar, projektif düzlem üzerindeki fonksiyonlar olarak düşünülebilir. Dikkat edilirse $\lambda \neq 0, 1$ olması halinde $(x : y : z) = (\lambda x : \lambda y : \lambda z)$ olmasına karşılık

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z) \neq F(x, y, z)$$

dir. Bununla birlikte $F(x, y, z) = 0$ olması için gerek ve yeter koşul $F(\lambda x, \lambda y, \lambda z) = 0$ olmasıdır, dolayısıyla $F(x, y, z) = 0$ biçimindeki eğriler, projektif düzlemdeki eğriler olarak düşünülebilir.

2.3.1. Tanım. $P = (x_0, y_0, z_0)$ olmak üzere $F(x_0, y_0, z_0) = 0$ ise P noktasına $F(x, y, z) = 0$ ***eğrisi üzerindeki bir nokta***, $x_0, y_0, z_0 \in \mathbb{Q}$ olmak üzere P noktası eğri üzerindeki bir nokta ise P noktasına $F(x, y, z) = 0$ eğrisi üzerindeki bir ***rasyonel nokta*** denir.

$F(x, y, z) = 0$ eğrisi C olmak üzere C eğrisi üzerindeki tüm rasyonel noktaların oluşturduğu küme $C(\mathbb{Q})$ ile gösterilir.

2.3.2. Örnek. $(0 : 0 : 1)$ ve $(0 : 1 : 0)$ noktaları, $E_N : y^2z - x^3 + N^2xz^2 = 0$ eğrisi üzerindeki rasyonel noktalardır.

2.4. Eliptik Eğriler

Bu kısımda, genel olarak eliptik eğri kavramı tanımlanacak, bir cisim üzerinde tanımlanmış olan bir E_N eliptik eğrisinin noktalarının oluşturmuş olduğu küme üzerinde

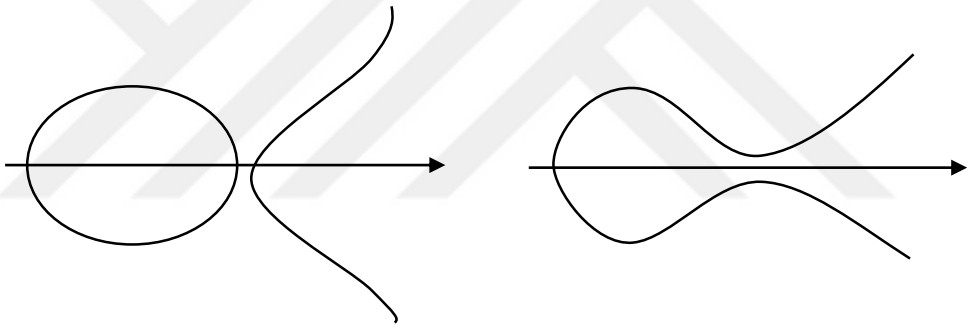
toplama işlemi tanımlanacak ve bu kümenin bir grup yapısına sahip olduğu gösterilecek, eliptik eğriler ile ilgili bazı özellikler ve temel sonuçlar bir araya getirilecektir.

2.4.1. Tanım. $a, b \in \mathbb{Z}$ ve $\Delta = 4a^3 + 27b^2 \neq 0$ olmak üzere

$$y^2 = x^3 + ax + b$$

biçimindeki bir kübik eşitlik ile tanımlanan bir E cebirsel eğrisine bir ***eliptik eğri*** ve Δ sayısına da $f(x) = x^3 + ax + b$ kübiğinin ***diskriminantı*** denir.

Tanıma dikkat edilirse $\Delta \neq 0$ koşulu, $f(x)$ kübiğinin $\mathbb{C}$ cisminde katlı kökünün olmamasına denktir. $y^2 = f(x)$ kübiğinin ya üç gerçel kökü ya da tek gerçel kökü vardır. Buna göre, gerçel koordinatlı bu eğri üzerindeki noktaların kümesi Şekil 2.2. de gösterildiği gibi ya tek bileşenlidir ya da iki bileşenlidir.



(a) (b)

Şekil 2.2. Eliptik eğriler

$\mathcal{O}$, düzlemde x eksenine dik olan her dik doğrunun iki ucunda da bulunan bir nokta olarak kabul edilmek üzere $E(\mathbb{Q})$, E eliptik eğrisi üzerindeki rasyonel noktaların kümesi

$$E(\mathbb{Q}) = \{(x,\ y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

dir. Bir eliptik eğri sonsuz çoklukta rasyonel noktaya sahip olabileceği gibi olmayabilir de. Hangi eliptik eğrilerin sadece sonlu çoklukta rasyonel noktaya sahip olduğu, henüz cevaplanamamış bir sorudur.

Eliptik eğriler ile ilgili çalışmalar yapılırken, özellikle uygulamalarda paket yazılımlardan da faydalanılır. SAGE ve MAGMA programları en çok kullanılan yazılımlardır. Örneğin, $y^2z = x^3 - N^2xz^2$ eliptik eğrisi SAGE programında

sage: E = EllipticCurve([$-N^2$, 0]); E

Elliptic Curve defined by $y^2 = x^3 - N^2x$ over Rational Field.

biçiminde ve p asal sayı, $a, b \in \mathbb{F}_p$ olmak üzere sonlu $\mathbb{F}_p$ cismi üzerinde tanımlı $y^2 = x^3 + ax + b$ eliptik eğrisi de MAGMA programında

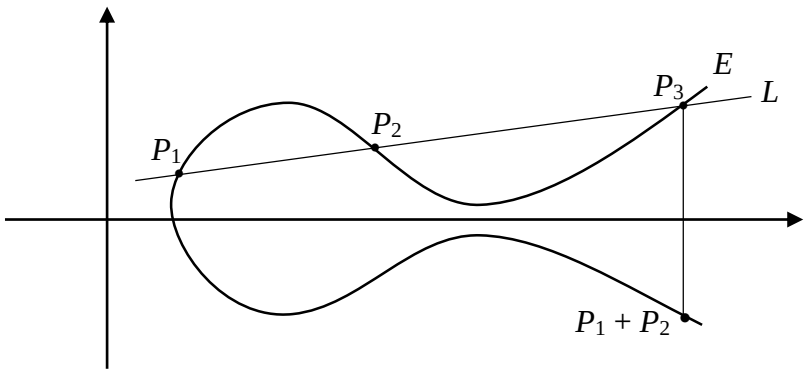
E = EllipticCurve([a, b]);

EllipticCurve defined by $y\text{^}2 = x\text{^}3 + a * x + b$ over $\mathbb{F}_p$

biçiminde tanımlanır.

Eliptik eğrileri özel yapan, herhangi $P, Q \in E(\mathbb{Q})$ noktaları için $P + Q \in E(\mathbb{Q})$ olacak biçimde $E(\mathbb{Q})$ üzerinde bir "+" işleminin tanımlanabilir olmasıdır. Gerçekte, E eliptik eğrisinin rasyonel koordinatlı noktalarının oluşturduğu $E(\mathbb{Q})$ kümesi üzerindeki bu toplama işlemi, $E(\mathbb{Q})$ kümesinin bir grup yapısına sahip olduğunu gösterir. Bu toplama işlemi, teğet ve kesen yöntemi ile geometrik olarak şu şekilde tanımlanabilir:

Eliptik eğri üzerindeki $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktalarının toplamını bulmak için bu noktalardan geçen L doğrusu çizilir ($P_1 = P_2 = P$ olması halinde E eğrisinin P noktasındaki teğeti dikkate alınır) ve bu doğrunun eliptik eğriyi kestiği üçüncü $P_3 = (x_3, y_3)$ noktası belirlenir. P_3 noktasının x-eksenine göre simetriği alınarak $P_1 + P_2 = (x_3, -y_3)$ olarak bulunur. Eliptik eğrinin bir dikey doğru üzerinde bulunan herhangi iki noktası $\mathcal{O}$ noktası ile doğrusal olduğundan, $\mathcal{O}$ noktası bu toplama işleminin etkisiz elemanıdır.



Şekil 2.3. $E(\mathbb{Q})$ üzerinde toplama işlemi

Eliptik eğri üzerindeki P_1 ve P_2 noktalarının koordinatları kullanılarak $P_1 + P_2$ noktasının daha kolay hesaplanması için bazı formüller oluşturulabilir. $P_1 + P_2$ noktasının x ve y koordinatları, sırasıyla, $x(P_1 + P_2)$ ve $y(P_1 + P_2)$ ile gösterilirse, $P_1 \neq P_2$ ise $m =$

$\frac{y(P_1)-y(P_2)}{x(P_1)-x(P_2)}$ ve $P_1 = P_2$ ise $f(x) = x^3 + ax^2 + bx + c$, $m = \frac{f'(x(P1))}{2y(P1)}$ olmak üzere P_1 ve P_2 noktalarından geçen doğru $y = mx + n$ biçiminde yazılabilir. Bu durumda $x(P_1 + P_2)$ değeri,

$$f(x) - (mx + n)^2$$

kübiğinin $x(P_1)$ ve $x(P_2)$ den farklı olan üçüncü köküdür. Bundan başka kübiğin kökleri toplamı da kübiğin x^2 teriminin katsayısının negatifine eşit olduğundan

$$x(P_1) + x(P_2) + x(P_1 + P_2) = -(a - m^2)$$

ve dolayısıyla

$$x(P_1 + P_2) = -x(P_1) - x(P_2) - a + m^2$$

olarak bulunur. $y(P_1 + P_2)$ değeri de eğrinin doğru ile kesiştiği üçüncü P_3 noktasının y değerinin negatifidir, yani

$$y(P_1 + P_2) = m(x(P_1) - x(P_3)) - y(P_1)$$

dir. Bu toplama işleminin, düzlemdeki noktaların bilinen, bileşen bileşene toplama işleminden farklı bir işlem olduğu açıktır.

2.4.2. Örnek. $y^2 = x^3 - 36x$ kübik eğrisi verilsin. Eğri üzerindeki $P_1 = (-3, 9)$ ve $P_2 = (0, 0)$ noktalarını toplayalım. Dikkat edilirse P_1 ve P_2 noktalarından geçen doğru denklemi

$$y = -3x$$

dir. O halde bu doğru ile kübik eğrinin kesişiminden

$$x^3 - 9x^2 - 36x = 0$$

eşitliği elde edilir. Bu eşitliğin iki kökü $x_1 = -3$ ve $x_2 = 0$ olduğundan

$$(-3) + 0 + x_3 = 9$$

$x_3 = 12$ ve dolayısıyla $y_3 = -36$ olarak bulunur. Bu durumda $P_3 = (x_3, y_3) = (12, -36)$ dır ve bu noktanın x-eksenine göre simetriği olan nokta, yani $P_1 + P_2$ noktası $P_1 + P_2 = (x_3, -y_3) = (12, 36)$ olarak bulunur. Bu nokta yukarıdaki formüller kullanılarak da bulunabilir. Burada

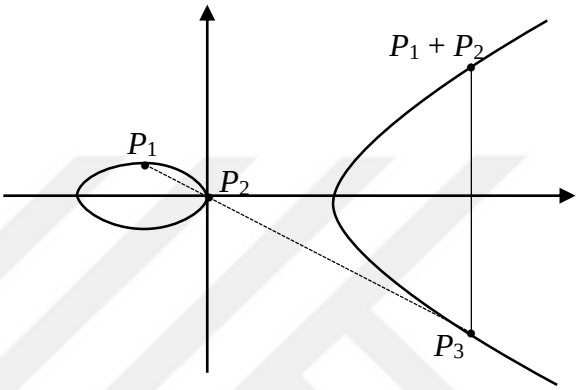
$$m = \frac{9-0}{-3-0} = -3,\ a = 0,\ x(P_1) = -3,\ x(P_2) = 0,\ y(P_1) = 9$$

olduğundan

$$x(P_1 + P_2) = -x(P_1) - x(P_2) - a + m^2 = 3 - 0 - 0 + 9 = 12$$

$$y(P_1 + P_2) = m(x(P_1) - x(P_3)) - y(P_1) = -3(-3 - 12) - 9 = 36$$

dir. Böylece $P_1 + P_2 = (12, 36)$ olarak bulunur.



Şekil 2.4. E_6 eğrisi üzerindeki $P_1 = (-3, 9)$, $P_2 = (0, 0)$ noktalarının toplamı

2.4.3. Örnek. $y^2 = x^3 + 17$ eğrisi verilsin. İlk olarak bu eğri üzerindeki $P_1 = (-1, 4)$ noktası ile kendisini toplayalım. $P_1 + P_1 = 2P_1$ noktasını bulmak için öncelikle eğrinin P_1 noktasındaki teğetinin denklemini bulalım. $m = \frac{f'(x(P1))}{2y(P1)} = \frac{f'(-1)}{2\cdot 4} = \frac{3}{8}$ olduğundan teğet doğru denklemi $y = \frac{3x+35}{8}$ dir. Bu doğru ile eğrinin kesişiminden

$$x^3 - \frac{9}{64}x^2 - \ldots = 0$$

eşitliği elde edilir. (–1) çift katlı kök olduğundan

$$(-1) + (-1) + x_3 = \frac{9}{64},$$

yani $x_3 = \frac{137}{64}$ ve dolayısıyla $y_3 = \frac{2651}{512}$ dir. Bu durumda $P_3 = (x_3, y_3) = \left(\frac{137}{64}, \frac{2651}{512}\right)$ ve böylece $P_1 + P_1 = 2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$ olarak elde edilir. Şimdi de bu eğri üzerindeki $P_1 = (-1, 4)$ ve $P_2 = (2, 5)$ noktalarını toplayalım. P_1 ve P_2 noktalarından geçen doğru denklemi

$$y = \frac{1}{3}x + \frac{13}{3}$$

dir. Bu doğru ile kübik eğrinin kesişiminden

$$x^3 - \frac{1}{9}x^2 - \frac{26}{9}x - \frac{16}{9} = 0$$

eşitliği elde edilir. Bu eşitliğin iki kökü $x_1 = -1$ ve $x_2 = 2$ olduğundan

$$(-1) + 2 + x_3 = \frac{1}{9},$$

yani $x_3 = -\frac{8}{9}$ ve dolayısıyla $y_3 = \frac{109}{27}$ olarak elde edilir. Bu durumda $P_3 = (x_3, y_3) = \left(-\frac{8}{9}, \frac{109}{27}\right)$ ve bu noktanın x-eksenine göre simetriği olan nokta, yani $P_1 + P_2$ noktası $P_1 + P_2 = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ olarak bulunur.

Yukarıda SAGE yazılım programında tanıtılan eliptik eğri üzerindeki noktalar, SAGE ile belirlenebilir ve tekrar SAGE yazılım programı kullanılarak bu noktaların toplamları hesaplanabilir. Bunun için önce

```
sage: E.point_search(20)
```

komutu ile eliptik eğri üzerinde 20 tane nokta aranır, doğal olarak bu eliptik eğri üzerinde henüz kaç tane nokta olduğu bilinmemektedir, bu nedenle bu sayı eğri üzerindeki noktaların sayısından fazla olabileceği gibi az da olabilir. Bununla birlikte aranan nokta sayısının arttırılması halinde noktaların belirlenmesi süresinin de uzayacağı açıktır.

Magma yazılımı kullanılarak da bir eliptik eğri üzerindeki noktalar belirlenebilir. Örneğin $\mathbb{F}_{13}$ üzerinde tanımlı $E : y^2 + xy = x^3 + x^2 + 10x + 9$ eliptik eğrisi üzerindeki rasyonel noktalar

```
>E:=EllipticCurve([GF(13) | 1, 1, 0, 10, 9]);
>A:=RationalPoints;
>#E;
>#A;
```

komutları ile bulunur.

2.4.4. Örnek. $E_6 : y^2 = x^3 - 36x$ eliptik eğrisini göz önüne alalım. Yukarıdaki Sage komutu kullanılarak eğri üzerindeki $P = (-2, 8)$, $Q = (12, 36)$ noktalarının belirlendiğini varsayalım. Buna göre, Sage kullanılarak

sage: $P = E([-2, 8])$; $Q = E([12, 36])$

sage: $P + Q$

$(-6 : 0 : 1)$

yani $P + Q = (-6, 0)$ olarak bulunur. Benzer şekilde, Sage yardımıyla P noktasının kendisiyle 5 defa toplamı, yani $(P + P + P + P + P) = 5P$ noktası da

sage: $5P$

komutu ile $5P = \left(-\frac{1074902978}{2015740609}, \frac{394955797978644}{90500706122273}\right)$ olarak bulunur (Brown 2003).

Belli $n \in \mathbb{Z}$ için $nP = \mathcal{O}$ olacak biçimdeki $P \in E(\mathbb{Q})$ noktalarının hangi noktalar olduğu ve bu noktaların kaç tane olduğu bilinmek istenir. Örneğin, yukarıdaki eğri üzerinde olan $R = (6, 0)$ noktası dikkate alındığında $2R = \mathcal{O}$ eşitliğinin gerçeklendiği görülür.

2.5. Eliptik Eğriler Üzerindeki Sonlu Mertebeli Noktalar

Bu kısımda, E_N eliptik eğrisi üzerindeki sonlu mertebeli noktalar, yani büküm noktaları ele alınacaktır. Öncelikle sonlu mertebeli nokta kavramı tanımlanacak ve daha sonra iki mertebeli ve daha genel olarak n mertebeli noktaların grup yapısı ve $E(\mathbb{Q})$ gruplarının $E(\mathbb{Q})_{tors}$ alt grubuna bağlı olarak tam yapısını ortaya koyan Mordell Teoremi ifade edilecektir.

2.5.1. Tanım. E, bir $\mathbb{K}$ cismi üzerinde tanımlı bir eliptik eğri ve P noktası eliptik eğri üzerinde bir nokta olmak üzere

$$nP = P + P + \cdots + P = \mathcal{O}$$

olacak biçimde bir $n \in \mathbb{N}$ var ise $P \in E(\mathbb{K})$ noktasına ***sonlu mertebeli nokta*** veya ***büküm (torsiyon) noktası*** denir. Eğer P noktası bir büküm noktası değil ise bu nokta ***sonsuz mertebeli nokta*** olarak adlandırılır. Tüm büküm noktalarının kümesi $E(\mathbb{K})_{tors}$ ile gösterilir. Eğer P noktası E eliptik eğrisinin bir büküm noktası ve üstelik her $1 \leq n' \leq n$

tamsayısı için $n'P \neq \mathcal{O}$ olmak üzere $nP = \mathcal{O}$ ise P noktasına ***n mertebeli nokta*** denir (Silverman ve Tate 1992).

Belli bir $n \in \mathbb{N}$ için ***n-büküm noktaların kümesi*** $E(\mathbb{K})[n]$ ile gösterilir, yani

$$E(\mathbb{K})[n] = \{P \in E(\mathbb{K}) \mid nP = \mathcal{O}\}$$

dir ve üstelik $E(\mathbb{K})[n]$ ve $E(\mathbb{K})_{\text{tors}}$ kümelerinin her ikisinin de $E(\mathbb{K})$ grubunun birer alt grubu olduğu açıktır. Eğer kar$(\mathbb{K}) \neq 2$ ise

$$E(\mathbb{K})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

ve kar$(\mathbb{K}) = 2$ ise

$$E(\mathbb{K})[2] \cong \{0\} \text{ veya } \mathbb{Z}/2\mathbb{Z}$$

olduğu kolayca görülebilir. Daha genel olarak,

i. n bir pozitif tamsayı olmak üzere kar$(\mathbb{K}) \nmid n$ veya 0 ise

$$E(\mathbb{K})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

ii. kar$(\mathbb{K}) = p \mid n$ ise $(p, n^*) = 1$ ve $n = p^r n^*$ olmak üzere

$$E(\mathbb{K})[n] \cong \mathbb{Z}/n^*\mathbb{Z} \times \mathbb{Z}/n^*\mathbb{Z} \text{ veya } \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n^*\mathbb{Z}$$

dir (Washington 2008).

$\mathbb{K} = \mathbb{Q}$ olması hali oldukça ilginçtir, bu halde $E(\mathbb{Q})_{\text{tors}}$ grubu için sadece 15 ihtimal söz konusudur:

$$1 \leq n \leq 10 \text{ veya } n = 12 \text{ için } \mathbb{Z}/n\mathbb{Z} \text{ veya } 1 \leq n \leq 4 \text{ için } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$$

dir. Mazur (Mazur 1977, 1978) tarafından verilmiş olan bu sonuç oldukça önemlidir, dikkat edilirse bu sonuç $E(\mathbb{Q})_{\text{tors}}$ grubunun sonlu bir grup olduğunu ortaya koymaktadır.

Mordell tarafından verilen aşağıdaki sonuç, $E(\mathbb{Q})$ grubunun, $E(\mathbb{Q})_{\text{tors}}$ alt grubuna bağlı olarak tam yapısını ortaya koyar.

2.5.2. Teorem (Mordell Teoremi). r bir pozitif tamsayı olmak üzere

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

dir (Silverman ve Tate 1992, Chahal 2006).

Burada $E(\mathbb{Q})_{tors}$ grubuna, $E(\mathbb{Q})$ grubunun ***torsiyon alt grubu*** ve negatif olmayan $r = r_{\mathbb{Q}}(E)$ tamsayısına da $\mathbb{Q}$ üzerinde E eğrisinin (Mordell-Weil) ***rankı*** denir. $r_{\mathbb{Q}}(E) > 0$ olması için gerek ve yeter koşul E eğrisinin sonsuz çoklukta rasyonel noktaya sahip olmasıdır. Özellikle $a > 0$ olmak üzere bir karesiz a tamsayısının bir denk sayı olması için gerek ve yeter koşul (2.4) eşitliği ile tanımlanmış olan eliptik eğrinin bir pozitif ranka sahip olmasıdır.

$r_{\mathbb{Q}}(E)$ hakkındaki bilinenler tam olmasa da $E(\mathbb{Q})_{tors}$ alt grubu iyi bilinmektedir ve 1937'de Lutz ve Nagell tarafından bağımsız olarak ifade edilen aşağıdaki teorem, keyfi bir E eliptik eğrisi için $E(\mathbb{Q})_{tors}$ alt grubunun belirlenmesi için bir algoritma vermektedir.

2.5.3. Teorem (Lutz-Nagell). $a, b \in \mathbb{Z}$ ve $\Delta = 4a^3 + 27b^2 \neq 0$ olmak üzere E eliptik eğrisi

$$y^2 = x^3 + ax + b$$

eşitliği ile verilmiş olsun. $P = (x, y)$, $E(\mathbb{Q})_{tors}$ alt grubunun $\mathcal{O}$ noktasından farklı bir noktası ise x ve y tamsayıdır. Üstelik $y = 0$ ya da $y^2|\Delta$ dir (Silverman ve Tate 1992, Chahal 2006).

Lutz-Nagell teoremi, $y^2 = x^3 - a^2x$ eşitliği ile verilmiş olan pozitif ranklı eliptik eğriler ile kenar uzunlukları rasyonel ve alanı N olan dik üçgenin varlığı arasında bir köprüdür. Bundan başka, eliptik eğriler üzerindeki rasyonel noktaların koordinatlarının aşağıdaki özelliklerine de ihtiyaç duyulacaktır.

2.5.4. Önerme. x ve y, $y^2 = x^3 + ax + b$ eşitliği ile verilmiş olan eliptik eğri üzerindeki noktanın sıfırdan farklı rasyonel koordinatları ise, en sade halde

$$x = \frac{s}{t^2}, y = \frac{u}{t^3}$$

biçimindedir (Chahal 2006).

İspat. $S, U \geq 1$ ve obeb(s, S) = 1 olmak üzere x ve y rasyonel sayılarını $x = s/S$ ve $y = u/U$ olarak alalım. Bu durumda

$$u^2S^3 = U^2s^3 + asU^2S^2 + bU^2S^3$$

dir. Bu eşitlikten S^3 ve U^2 sayılarının birbirini böldüğü kolayca görülebilir. Dolayısıyla $S^3 = U^2$ dir. Dolayısıyla belli $t \geq 1$ için $S = t^2$ ve $U = t^3$ dir. ■

Şimdi Kısım 2.1 de "$a > 0$ olmak üzere a karesiz tamsayısının bir denk sayı olması için gerek ve yeter koşul

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

eşitliği ile tanımlanan E eliptik eğrisinin sonsuz çoklukta rasyonel noktaya sahip olmasıdır." biçiminde ifade edilmiş olan teoremin ispatını verelim.

Teorem 2.1.8.'in İspatı. a sayısının bir denk sayı olduğunu (yani, x, y, z ve $t \in \mathbb{N}$ olmak üzere (2.1) eşitliğinin bir x, y, z ve t çözümüne sahip olduğunu ve üstelik bu sayıların ikişer ikişer aralarında asal olduğunu) varsayalım. $y > 1$ olduğu kolayca görülebilir. (2.1) eşitliğinde verilen iki eşitlik çarpılır ve daha sonra elde edilen eşitliğin her iki tarafı x^2/y^6 çarpanı ile çarpılır ve gerekli düzenlemeler yapılırsa

$$\left(\frac{ztx}{y^3}\right)^2 = \left(\frac{x^2}{y^2}\right)^2 - a^2\left(\frac{x^2}{y^2}\right)$$

eşitliği elde edilir. x ve y aralarında asal ve $y > 1$ olduğundan, Lutz-Nagell Teoremi gereği $P = (x^2/y^2, ztx/y^3)$ noktası (2.4) eşitliği ile tanımlanmış olan E eliptik eğrisi üzerindeki sonsuz mertebeli bir noktadır. Dolayısıyla $r_{\mathbb{Q}}(E) > 0$ dır. Tersine $P = (x, y)$ noktasının E eğrisi üzerinde sonsuz mertebeli bir nokta olduğunu varsayalım. $x \neq 0$ ve $y \neq 0$ olduğu açıktır. O halde obeb(s, t) = obeb$(u, t) = 1$ olmak üzere $x = s/t^2$ ve $y = u/t^3$ ve dolayısıyla

$$\left(\frac{u}{t^3}\right)^2 = \left(\frac{s}{t^2}\right)^3 - a^2\left(\frac{s}{t^2}\right)$$

dir. Bu ise

$$u^2 = s(s + at^2)(s - at^2)$$

olduğunu gösterir. Böylece s, $s + at^2$ ve $s - at^2$ sayılarının ikişer ikişer aralarında asal olduğu görülür. Dolayısıyla bu sayıların her biri bir mükemmel kare sayıdır. $s = v^2$ ise

$$v^2 + at^2 = m^2,\ v^2 - at^2 = n^2$$

ve böylece $y = t \geq 1$ olacak biçimde (2.1) eşitliğinin bir çözümü elde edilmiş olur. ■

Dikkat edilirse, $y^2 = x^3 - a^2x$ eşitliği ile tanımlanmış olan eliptik eğri üzerindeki her bir rasyonel nokta (2.1) eşitliğinin bir aşikar olmayan çözümünü verir ve böylece alanı a

olan bir rasyonel dik üçgenin kenar uzunlukları elde edilir. Böylece aşağıdaki sonuca ulaşılmış olur.

2.5.5. Sonuç. Her bir a denk sayısı için, alanı a olan sonsuz çoklukta (benzer olmayan) rasyonel dik üçgen vardır (Chahal 2006).

Bu benzer olmayan dik üçgenler, $y^2 = x^3 - a^2x$ eşitliği ile tanımlanmış olan eliptik eğri üzerindeki rasyonel noktaların toplanması ile elde edilen noktalar ile bulunurlar.

2.6. Singüler Eğriler ve Bir Eliptik Eğrinin İndirgenmişi

Bu kısımda singüler eğri ve bir eliptik eğrinin indirgenmesi kavramları ele alınacaktır.

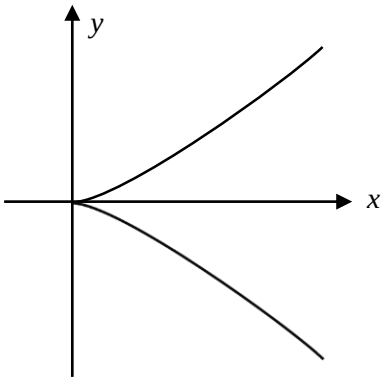
2.6.1. Tanım. $P = (x_0 : y_0 : z_0)$ noktası $F(x, y, z) = 0$ eğrisi üzerindeki bir nokta ve

$$\frac{\partial F}{\partial x}(x_0, y_0, z_0) = 0, \quad \frac{\partial F}{\partial y}(x_0, y_0, z_0) = 0 \text{ ve } \frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0$$

ise bir $F(x, y, z) = 0$ eğrisine P noktasında ***singüler eğri*** denir. P noktası eğri üzerindeki bir nokta ancak eğri P noktasında singüler değil ise $F(x, y, z) = 0$ eğrisine ***P noktasında singüler olmayan eğri*** ve eğri, üzerindeki tüm noktalarda singüler olmayan bir eğri ise eğriye ***singüler olmayan eğri*** denir.

Tanım dikkate alındığında, eğrinin bir noktada singüler olmaması, eğrinin singüler olmayan noktada iyi tanımlı bir teğetinin olmasına karşılık geldiği görülür.

2.6.2. Örnek. $F(x, y, z) = y^2z - x^3 = 0$ eğrisini göz önüne alalım. Bu eğrinin xy-düzlemindeki grafiği aşağıdaki gibidir.



Şekil 2.5. $y^2 = x^3$ eğrisi

Bu eğrinin (0 : 0 : 1) noktasında iyi tanımlı teğetinin olmadığı, dolayısıyla eğrinin (0 : 0 : 1) noktasında bir singüler eğri ve eğrinin diğer tüm noktalarında bir singüler olmayan eğri olduğu kolayca görülebilir. Gerçekten de,

$$\frac{\partial F}{\partial x} = -3x^2 \text{ ve } \frac{\partial F}{\partial y} = 2yz$$

ve dolayısıyla *xy*-düzleminde eğri üzerinde kısmi türevlerin her ikisinin de sıfır olduğu tek noktanın (0 : 0 : 1) noktası olduğu açıktır. Bundan başka $z = 0$ olması halinde *xy*-düzlemindeki noktaların hiçbirisi eğri üzerinde değildir. Dolayısıyla eğri üzerinde sadece (0 : 1 : 0) projektif noktası vardır ve bu durumda $\frac{\partial F}{\partial z} = y^2$ dir. O halde bu eğri, (0 : 1 : 0) noktasında da singüler olmayan bir eğridir. Dolayısıyla $F(x, y, z) = y^2z - x^3 = 0$ eğrisi (0 : 0 : 1) noktasından başka her noktada singüler olmayan eğridir.

Şimdi $E_N(\mathbb{Q})_{\text{tors}}$ grubunun yapısını tam olarak belirlemeye çalışalım, bunun için ilk olarak aşağıdaki teorem ele alınacaktır.

2.6.3. Teorem. Herhangi *N* karesiz pozitif tamsayısı için

$$E_N(\mathbb{Q})_{\text{tors}} = \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}$$

ve bundan başka

$$E_N(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

dir (Brown 2003).

Bu teorem ve denk sayılar üzerindeki sonuçlar, sadece $\mathbb{Q}$ üzerinde tanımlı eliptik eğrileri değil, aynı zamanda $\mathbb{F}_p$ cismi üzerinde tanımlı eliptik eğrilerin de dikkate alınmasını gerektirir. Bunun için, E_N eliptik eğrisinin *p* modülüne göre ***indirgenmişi*** olan

$$\bar{E}_N : y^2 = x^3 - \bar{N}^2 x$$

biçimindeki eğri dikkate alınacaktır. Bu nedenle bu teoremin ispatı bazı hazırlıklar yapıldıktan sonra verilecektir.

2.6.4. Örnek. E_7 eliptik eğrisini göz önüne alalım. Bu eğri 3 modülüne göre indirgendiğinde $\bar{E}_7 : y^2 = x^3 - x$ eliptik eğrisi elde edilir. $0 \le i, j \le 2$ için $(\bar{\imath} : \bar{\jmath} : \bar{1})$ ve $(\bar{\imath} : \bar{\jmath} : \bar{0})$ noktalarının tümü kontrol edilerek

$$\bar{E}_7 = \{(\bar{0} : \bar{1} : \bar{0}), (\bar{0} : \bar{0} : \bar{1}), (\bar{1} : \bar{0} : \bar{1}), (\bar{2} : \bar{0} : \bar{1})\}$$

olarak bulunur (Brown 2003).

Belli p asalları için $\bar{E}_N$ eliptik eğrisi singüler noktalara sahip olabileceğinden dikkatli olunmalıdır. Bununla birlikte $\bar{E}_N$ eğrisinin singüler olmayan bir eğri olması için gerek ve yeter koşulun $p \nmid 2N$ olduğu da açıktır.

$\bar{E}_N$ eliptik eğrisini, $\mathbb{F}_p$ cismi üzerinde tanımlı bir eliptik eğri olarak düşünmek için, $\bar{E}_N$ eğrisi üzerinde bir toplama işlemi yapılabildiğinden emin olunması gerekir. $p \nmid 2N$ özelliğindeki bir p asal sayısı için $P = (x(P), y(P))$ ve $Q = (x(Q), y(Q))$, $\bar{E}_N(\mathbb{F}_p)$ eliptik eğrisi üzerindeki noktalar olsun. $P + Q = (x(P + Q), y(P + Q))$ noktası, $x(P) \neq x(Q)$ için $m = \frac{y(P)-y(Q)}{x(P)-x(Q)}$ olmak üzere,

$$x(P + Q) = m^2 - x(P) - x(Q), y(P + Q) = m(x(P) - x(P + Q)) + y(P)$$

ve $x(P) = x(Q)$ ise

$$P + Q = (\bar{0} : \bar{1} : \bar{0})$$

olarak elde edilir.

$E_N(\mathbb{Q})$ grubunun yapısının belirlenebilmesi için, $\bar{E}_N(\mathbb{F}_p)$ grubunu ele almak anlamsız görülebilir. Ancak $E_N(\mathbb{Q})$ grubundaki noktaların sayısı kolayca hesaplanamadığı halde $\bar{E}_N(\mathbb{F}_p)$ grubundaki noktaların sayısı kolayca hesaplanabilir. Dolayısıyla $\bar{E}_N(\mathbb{F}_p)$ grubunu incelemek daha kolaydır ve elde edilen bu bilgi, $E_N(\mathbb{Q})$ grubu hakkındaki bilinenleri bir araya getirmek için $p \nmid 2N$ özelliğindeki asallar için kullanılabilir.

$(x : y : z) \in \mathbb{P}^2_{\mathbb{Q}}$ olsun. Uygun bir tamsayı ile çarpılarak paydalar yok edilebilir ve bu nokta x, y, z birer tamsayı ve obeb$(x, y, z) = 1$ olacak biçimde yeniden düzenlenebilir, dolayısıyla $(x_1 : y_1 : z_1) = (x : y : z)$ ve obeb$(x_1, y_1, z_1) = 1$ olacak biçimde $x_1, y_1, z_1 \in \mathbb{Z}$ vardır. Böylece $\epsilon : \mathbb{P}^2_{\mathbb{Q}} \longrightarrow \mathbb{P}^2_{\mathbb{F}_p}$, $(x : y : z) \longmapsto (\bar{x} : \bar{y} : \bar{z})$ biçiminde tanımlanan ϵ dönüşümü, obeb$(x, y, z) = 1$ olduğu için $\bar{x}$, $\bar{y}$ ve $\bar{z}$ değerlerinin hepsi birden $\bar{0}$ olamayacağından iyi tanımlıdır. Böylece $\bar{E}_N(\mathbb{F}_p)$ grubu üzerinde yapılan toplama işlemi ϵ dönüşümünün $E_N(\mathbb{Q}) \longrightarrow \bar{E}_N(\mathbb{F}_p)$ grup homorfizmine kısıtlaması olur. Genellikle ϵ dönüşümü birebir

değildir, aşağıda bu dönüşüm altında hangi noktaların aynı nokta ile eşlendiği belirtilmektedir.

2.6.5. Önerme. $P = (x_1 : y_1 : z_1)$ ve $Q = (x_2 : y_2 : z_2)$ olmak üzere P ve Q noktalarının $\mathbb{P}^2_{\mathbb{F}_p}$de aynı noktaya karşılık gelmeleri için gerek ve yeter koşul $p|x_1y_2 - x_2y_1$, $p|x_2z_1 - x_1z_2$ ve $p|y_1z_2 - y_2z_1$ olmasıdır (Brown 2003).

İspat. İlk olarak P ve Q noktalarının $\mathbb{P}^2_{\mathbb{F}_p}$de aynı noktaya karşılık geldiğini, yani

$$\bar{P} = (\overline{x_1} : \overline{y_1} : \overline{z_1}) = (\overline{x_2} : \overline{y_2} : \overline{z_2}) = \bar{Q}$$

olduğunu varsayalım. Bu durumda p asal sayısı x_1, y_1 ve z_1 sayılarını bölmez. Genelliği bozmadan $p \nmid x_1$ olduğu varsayılabilir. $\bar{P} = \bar{Q}$ olduğundan aynı zamanda $p \nmid x_2$ dir. Bu durumda

$$(\overline{x_1}\,\overline{x_2} : \overline{x_1}\,\overline{y_2} : \overline{x_1}\overline{z_2}) = (\overline{x_2} : \overline{y_2} : \overline{z_2}) = \bar{Q} = \bar{P} = (\overline{x_1} : \overline{y_1} : \overline{z_1}) = (\overline{x_2}\,\overline{x_1} : \overline{x_2}\,\overline{y_1} : \overline{x_2}\overline{z_1})$$

dir. Bu eşitliğin x-koordinatları eşit olduğundan y ve z-koordinatları da eşit olmalıdır. O halde $p|(x_1y_2 - x_2y_1)$ ve $p|(x_1z_2 - x_2z_1)$ dir. $p|y_1$ ise $p \nmid y_2$ dir, dolayısıyla $p|(y_1z_2 - y_2z_1)$ dir. $p \nmid y_1$ ise $p|(y_1z_2 - y_2z_1)$ olduğunu elde etmek için yukarıda yapılanlarda x_1 ile y_1 sayılarının rollerini değiştirmek yeterlidir.

Şimdi de $p|(x_1y_2 - x_2y_1)$, $p|(x_2z_1 - x_1z_2)$ ve $p|(y_1z_2 - y_2z_1)$ olduğunu varsayalım. $p \nmid x_1$ ise, örneğin, $\overline{x_1}\,\overline{y_2} = \overline{x_2}\,\overline{y_1}$ varsayımı kullanıldığında

$$\bar{Q} = (\overline{x_2} : \overline{y_2} : \overline{z_2}) = (\overline{x_1}\,\overline{x_2} : \overline{x_1}\,\overline{y_2} : \overline{x_1}\overline{z_2}) = (\overline{x_2}\,\overline{x_1} : \overline{x_2}\,\overline{y_1} : \overline{x_2}\overline{z_1}) = \bar{P}$$

dir. Şimdi $p|x_1$ olduğunu varsayalım. Bu durumda $p \nmid y_1$ veya $p \nmid z_1$ olmalıdır. Fakat varsayım gereği $x_2z_1 \equiv 0 \pmod{p}$ ve $x_2y_1 \equiv 0 \pmod{p}$ dir. y_1 veya z_1, p modülüne göre sıfırdan farklı olduğundan $x_2 \equiv 0 \pmod{p}$ olmalıdır. Genelliği bozmadan $y_1 \not\equiv 0 \pmod{p}$ olduğunu varsayalım. Bu durumda $\overline{y_1}\,\overline{z_2} = \overline{y_2}\,\overline{z_1}$ olduğu kullanılarak

$$\bar{Q} = (\bar{0} : \overline{y_1}\,\overline{y_2} : \overline{y_1}\,\overline{z_2}) = (\bar{0} : \overline{y_1}\,\overline{y_2} : \overline{y_2}\,\overline{z_1}) = \bar{P}$$

olarak elde edilir. ■

Genelde, $E_N(\mathbb{Q}) \longrightarrow \bar{E}_N(\mathbb{F}_p)$ dönüşümünün bir örten dönüşüm olduğu doğru değildir. E_{21} eliptik eğrisinin 5 modülüne göre indirgenmişi dikkate alındığında $(\bar{2}, \bar{4}) \in \bar{E}_{21}$ olduğu halde $(2, 24) \notin E_{21}(\mathbb{Q})$ dir.

p sayısı $p \nmid 2N$ özelliğinde bir asal sayı olmak üzere $\bar{E}_N(\mathbb{F}_p)$ grubundaki 2-büküm noktalar sadece $(0 : 1 : 0)$, $(0 : 0 : 1)$ ve $(\pm N : 0 : 1)$ noktalarıdır.

$p \nmid 2N$ için $a_{E_N}(p)$ Frobenius endomorfizminin izi olmak üzere,

$$a_{E_N}(p) = p + 1 - \#\bar{E}_N(\mathbb{F}_p)$$

dir. Aşağıdaki kurallar kullanılarak, bu tanım genişletilebilir. $r \geq 2$ ve $p \nmid 2N$ özelliğindeki bir p asalı için

$$a_{E_N}(p^r) = a_{E_N}(p^{r-1})a_{E_N}(p) - pa_{E_N}(p^{r-2})$$

ve obeb$(mn, 2N) = 1$ olmak üzere aralarında asal m ve n sayıları için

$$a_{E_N}(mn) = a_{E_N}(m)a_{E_N}(n)$$

dir.

2.6.6. Lemma. p sayısı $p \nmid 2N$ ve $p \equiv 3 \pmod 4$ özelliğindeki bir asal sayı ise $a_{E_N}(p) = 0$ dır (Brown 2003).

İspat. Yukarıda $\bar{E}_N(\mathbb{F}_p)$ grubundaki 2-büküm noktaların sadece $(\bar{0} : \bar{1} : \bar{0})$, $(\bar{0} : \bar{0} : \bar{1})$ ve $(\pm\bar{N} : \bar{0} : \bar{1})$ noktaları olduğu belirtilmişti. $p \nmid 2N$ olduğundan bu noktaların her biri birbirinden farklıdır. Şimdi $x \neq \bar{0}, \pm\bar{N}$ olmak üzere $(x, y) \in \bar{E}_N(\mathbb{F}_p)$ noktalarını belirleyelim. Dikkat edilirse $\bar{E}_N(\mathbb{F}_p)$ grubunda $z = \bar{0}$ özelliğindeki tek nokta $(\bar{0} : \bar{1} : \bar{0})$ noktasıdır. Dolayısıyla, x bileşeni için $p - 3$ tane ihtimal vardır. x bileşeninin kalan ihtimallerini $\{x, -x\}$ biçiminde eşleyelim. $x \neq -x$ olduğunu görelim. Eğer $x = -x$ olsaydı $\bar{2}x = \bar{0}$, böylece x bir 2-büküm noktası ve dolayısıyla $x \neq \bar{0}, \pm\bar{N}$ olurdu. $\bar{E}_N(\mathbb{F}_p)$ grubundaki 2-büküm noktaları dikkate alındığında $x = \bar{0}, \pm\bar{N}$ olduğu sonucu elde edilir. Dolayısıyla her bir $\{x, -x\}$ kümesinin kardinalitesi ikidir. $f(x) = x^3 - \bar{N}^2x$ olmak üzere $f(x)$ fonksiyonunun tek, yani her x için $f(-x) = -f(x)$ olduğu açıktır. $p \equiv 3 \pmod 4$ olduğundan $\left(\frac{-1}{p}\right) = -1$, yani -1 sayısı p modülüne göre bir ikinci dereceden kalan değildir. $f(x)$ fonksiyonunun p modülüne göre ikinci dereceden kalan olmadığını, yani $\left(\frac{f(x)}{p}\right) = -1$ olduğunu varsayalım. Dolayısıyla $\left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right) = 1$, yani $-f(x)$ fonksiyonu p modülüne göre bir ikinci dereceden kalandır. Benzer şekilde $f(x)$ fonksiyonu p modülüne göre bir ikinci dereceden kalan ise $-f(x)$ fonksiyonunun p modülüne göre bir

ikinci dereceden kalan olmadığı da görülebilir. Böylece her bir $\{x, -x\}$ çifti için, $f(x)$ veya $-f(x)$ fonksiyonunun p modülüne göre bir ikinci dereceden kalan olup olmadığına bağlı olarak $\bar{E}_N(\mathbb{F}_p)$ grubunda ya $(x, \pm\sqrt{f(x)})$ veya $(x, \pm\sqrt{-f(x)})$ noktası elde edilir. Böylece x bileşeninin $p - 3$ farklı değerine karşılık $\bar{E}_N(\mathbb{F}_p)$ grubunda $p - 3$ tane farklı nokta belirten $(p - 3)/2$ tane $\{x, -x\}$ çifti elde edilmiş olur. Bu noktalar yukarıda belirlenmiş olan dört büküm noktası ile bir araya getirilerek

$$a_{E_N}(p) = (p + 1) - (p + 1) = 0$$

olduğu sonucu elde edilir. ■

Bu lemma ve Önerme 2.6.5., Teorem 2.6.3.'ün ispatı için temel iki bileşendir. Ayrıca, aritmetik dizilerdeki asal sayılar üzerinde Dirichlet Teoremi olarak bilinen aşağıdaki teoreme de ihtiyacımız vardır.

2.6.7. Teorem. obeb$(a, b) = 1$ olmak üzere $a, b \in \mathbb{Z}$ olsun.

$$a, a + b, a + 2b, \ldots$$

aritmetik dizisi sonsuz çoklukta asal sayı bulundurur (Brown 2003).

Şimdi Teorem 2.6.3.'ün ispatı verilebilir:

Teorem 2.6.3.'ün İspatı. P noktası, $E_N(\mathbb{Q})_{\text{tors}}$ grubunun $(0 : 1 : 0)$, $(0 : 0 : 1)$ ve $(\pm N : 0 : 1)$ noktalarından farklı bir noktası olsun. $\bar{E}_N(\mathbb{F}_p)$ grubundaki 2-büküm noktalar sadece $(0 : 1 : 0)$, $(0 : 0 : 1)$ ve $(\pm N : 0 : 1)$ noktaları olduğundan P noktasının mertebesi 2 olamaz. P noktasının mertebesi m olsun. $E_N(\mathbb{Q})_{\text{tors}}$ grubunun, ya tek mertebeli ya da sekiz mertebeli bir alt gruba sahip olduğunu görelim. İlk olarak, m tek ise $\langle P \rangle$ grubunun $E_N(\mathbb{Q})_{\text{tors}}$ grubunun tek mertebeli bir alt grubu olduğu açıktır. Dolayısıyla m çift olsun. Eğer m, ikinin bir kuvveti değil ise, $a, b \in \mathbb{Z}$, b tek sayı ve $b > 1$ olmak üzere $m = 2^a b$ olarak yazılabilir. Bu durumda $\langle aP \rangle$ grubu, $E_N(\mathbb{Q})_{\text{tors}}$ grubunun b (yani tek) mertebeli bir alt grubudur. Dolayısıyla, m sayısının ikinin bir kuvveti olduğu varsayılabilir. P noktası iki mertebeli olmadığından, $j \geq 2$ olmak üzere $m = 2^j$ dir. P noktasının mertebesi dört ve $Q = (N : 0 : 1)$ olsun. $\{(0 : 1 : 0), Q, P, 2P, 3P, P + Q, 2P + Q, 3P + Q\}$ kümesinin $E_N(\mathbb{Q})_{\text{tors}}$ grubunun sekiz mertebeli bir alt grubu olduğu görülebilir. $j \geq 3$ ise, $b \geq 1$ olmak üzere $m = 8b$ olarak yazılabilir. Bu durumda, $\langle bP \rangle$ grubunun $E_N(\mathbb{Q})_{\text{tors}}$ grubunun sekiz mertebeli bir alt grubu olduğu görülür. Dolayısıyla tüm durumlar dikkate

alındığında, $E_N(\mathbb{Q})_{\text{tors}}$ grubunun ya tek mertebeli bir alt grup ya da sekiz mertebeli bir alt grubu içerdiği sonucu elde edilir. Bu alt grubu $\mathcal{S}$ ile gösterelim ve bu grubu $\mathcal{S} = \{P_1, \dots, P_{\#\mathcal{S}}\}$ biçiminde ifade edelim. Şimdi $\mathcal{S}$ kümesinin, sonlu çoklukta p asal sayısı hariç, tüm asallar için $\bar{E}_N(\mathbb{F}_p)$ grubunun içinde kaldığını gösterelim. $\langle P \rangle$ grubunun noktaları, $1 \leq i \leq \#\mathcal{S}$ için $P_i = (x_i : y_i : z_i)$ olarak yazılabilir. $i \neq j$ olmak üzere $\langle P \rangle$ grubundaki P_i ve P_j noktalarını ele alalım. $\mathcal{S}$ kümesinin ne zaman $\bar{E}_N(\mathbb{F}_p)$ grubunun içinde kaldığını belirlemek için, ne zaman $\bar{P}_i = \bar{P}_j$ olduğunun belirlenmesi gerekir. Önerme 2.6.5. gereği, $\bar{P}_i = \bar{P}_j$ olması için gerek ve yeter koşul $p | x_i y_j - x_j y_i$, $p | x_j z_i - x_i z_j$ ve $p | y_i z_j - y_j z_i$ dir. P_i ve P_j noktalarının farklı noktalar olması (bu noktalar $\mathbb{R}^3$ de vektör olarak düşünülürse), P_i ve P_j noktalarının orantılı olmadıklarını gösterir. Dolayısıyla, bu vektörlerin vektörel çarpımı sıfır vektörü değildir, yani $(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i)$ noktası sıfır vektörü değildir.

$$d_{i,j} = \text{obeb}(x_i y_j - x_j y_i, x_j z_i - x_i z_j, y_i z_j - y_j z_i)$$

olsun. Dolayısıyla $\bar{P}_i = \bar{P}_j$ olması için gerek ve yeter koşul $p | d_{i,j}$ olmasıdır. $D = \text{ekok}(d_{i,j})$ olarak alınırsa, $p > D$ olmak üzere her $i \neq j$ için $\bar{P}_i \neq \bar{P}_j$ dir. Bu ise, sonlu çoklukta asal sayı hariç tüm asallar için (yani, D sayısından büyük olan tüm asallar için) $\mathcal{S}$ kümesinin $E_N(\mathbb{Q})_{\text{tors}}$ grubunun içinde kaldığını göstermektedir. Dolayısıyla, sonlu çoklukta asal sayı hariç tüm asallar için $\#\mathcal{S} | \#\bar{E}_N(\mathbb{F}_p)$ olmalıdır. Şimdi bir çelişki elde etmek için bu özelliği kullanacağız.

$\#\mathcal{S} | \#\bar{E}_N(\mathbb{F}_p)$ olduğu gerçeği Lemma 2.6.6. ile birlikte düşünüldüğünde, sonlu sayıda p asal sayısı hariç tüm asallar için $p \equiv 3 (\text{mod } 4)$ özelliğindeki sonlu sayıda p asalı hariç tüm asal sayılar için $p \equiv -1 (\text{mod } \mathcal{S})$ olmasını gerektirir. $\#\mathcal{S} = 8$ ise $3 + 8k$ formunda sadece sonlu çoklukta asal sayı vardır, ki bu Teorem 2.6.7 ile çelişir. $\#\mathcal{S}$ tek ve $3 \nmid \#\mathcal{S}$ ise $4(\#\mathcal{S})k + 3$ formunda sadece sonlu çoklukta asal sayı vardır, ki bu tekrar Teorem 2.6.7. ile çelişir. Son olarak $3 | \#\mathcal{S}$ olması halinde de $12k + 7$ formunda sadece sonlu çoklukta asal sayı vardır ve bu da Teorem 2.6.7. ile çelişir. Olası tüm durumlarda bir çelişki elde edildiğinden, belirtilen özellikte bir P noktasının var olamayacağı sonucu elde edilmiş olur. ■

Teorem 2.6.3. dikkate alındığında verilen bir $P \in E_N(\mathbb{Q}) \setminus \{(0 : 1 : 0), (0 : 0 : 1), (\pm N : 0 : 1)\}$ noktasının sonsuz mertebeli olduğu sonucu elde edilir.

2.6.8. Sonuç. $P \in E_N(\mathbb{Q})\backslash\{(0:1:0), (0:0:1), (\pm N:0:1)\}$ olmak üzere

$$\langle P\rangle = \{nP \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$$

dir (Brown 2003).

İspat. $\varphi : \mathbb{Z} \longrightarrow \langle P\rangle$, $\varphi(n) = nP$ biçiminde tanımlanan φ dönüşümünü dikkate alalım. $\langle P\rangle$ grubunun tanımı gereği φ dönüşümü örtendir. Eğer $\varphi(m) = \varphi(n)$ ise $mP = nP$ yani $(m - n)P = \mathcal{O}$ dir. P noktası bir büküm noktası olmadığından $m - n = 0$ yani $m = n$ dir. Dolayısıyla φ dönüşümü birebirdir. Bundan başka

$$\varphi(m + n) = (m + n)P = mP + nP = \varphi(m) + \varphi(n)$$

dir.■

Eğer $P \notin E_N(\mathbb{Q})_{\text{tors}}$ özelliğinde böyle bir P noktası varsa, $E_N(\mathbb{Q})$ grubunun rankının pozitif olduğu söylenir. Gerçekte bir eliptik eğrinin rankı, kaç tane belirtilen özellikte "bağımsız" nokta olduğunu ölçer (eğer Q noktası $Q \notin E_N(\mathbb{Q})_{\text{tors}}$ ve $Q \notin \langle P\rangle$ özelliğindeki başka bir nokta ise Q noktasına P noktasından bağımsız nokta denir). Dolayısıyla eliptik eğrinin rankı, $E_N(\mathbb{Q})_{\text{tors}}$ grubunda olmayan bağımsız noktaların sayısıdır. Rank, daha cebirsel olarak, önceden vermiş olan Mordell-Weil Teoremi ile ifade edilmektedir.

Nihayet aşağıdaki teorem ile, bu teori denk sayılar ile ilişkilendirilebilir.

2.6.9. Teorem. N bir karesiz pozitif tamsayı olsun. Bu durumda N sayısının bir denk sayı olması için gerek ve yeter koşul E_N eğrisinin rankının pozitif olmasıdır (Brown 2003).

İspat. N bir denk sayı olsun. Bu durumda N sayısı, $E_N(\mathbb{Q})$ grubunda x-koordinatı sıfırdan farklı bir kare sayı olan bir nokta, yani $x(P) \in (\mathbb{Q}_{>0})^2$ olacak biçimde bir $P \in E_N(\mathbb{Q})$ noktası verir. N sayısı karesiz olduğundan $x(P) \neq 0, \pm N$ dir. Dolayısıyla bu şekilde elde edilen P noktası $E_N(\mathbb{Q})_{\text{tors}}$ grubunda olamaz, yani P noktası sonsuz mertebelidir. Dolayısıyla E_N eğrisinin rankı pozitiftir.

Tersine, E_N eğrisinin rankı pozitif olsun. O halde $y(P) \neq 0$ olacak biçimde bir $P \in E_N(\mathbb{Q})$ noktası vardır. Bu ise $P \in \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - N^2x, y \neq 0\}$ ve dolayısıyla P noktasının alanı N olan bir dik üçgene karşılık geldiğini gösterir.■

Bu teorem dikkate alınarak, verilen bir N sayısının ne zaman bir denk sayı olduğu problemi E_N eliptik eğrisinin rankının belirlenmesi problemine indirgenmiş olur.

3. SAYI CİSİMLERİ ÜZERİNDEKİ DENK SAYILAR

Cebirsel genişlemeler üzerinde denk sayı problemini çalışma fikri, gerçel kuadratik cisimleri ele alan Tada'ya kadar uzanır (Tada 2001). Denk sayı problemine konu olan dik üçgenin kenar uzunluklarının bir cebirsel sayı cisminden seçilmesi ile denk sayı probleminin doğal bir genellemesi elde edilir. Bu bölümde denk sayı problemi sayı cisimleri üzerinde ele alınacaktır.

m sayısı 1'den farklı bir karesiz pozitif tamsayı olsun. N sayısı bir pozitif tamsayı olmak üzere eğer N sayısı kenar uzunlukları $\mathbb{Q}(\sqrt{m})$ cismine ait olan bir dik üçgenin alanı ise N sayısına $\mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayıdır denir. $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ olmak üzere $E_N(\mathbb{K})$, $y^2 = x^3 - N^2x$ eşitliği ile tanımlanmış olan E_N eliptik eğrisi üzerindeki $\mathbb{K}$-rasyonel noktaların oluşturduğu grup olsun. Bu bölümde "$m \neq 2$ olmak üzere N sayısının $\mathbb{K}$ cismi üzerinde bir denk sayı olması için gerek ve yeter koşul $E_N(\mathbb{K})$ grubunun bir pozitif ranka sahip olmasıdır." olduğu sonucu elde edilecek ve ayrıca alanı N ve tüm kenar uzunlukları $\mathbb{K}$ cismine ait olan dik üçgenler sınıflandırılacaktır.

N sayısının bir denk olmayan sayı olması halinde N sayısının kenar uzunlukları bir gerçel kuadratik cisme ait olan bir dik üçgenin alanını verip vermediği sorulabilir. Bu bölümdeki amacımız, gerçel kuadratik cisimler üzerindeki denk sayıları dikkate almaktır. Karışıklığı önlemek için N sayısı kenar uzunlukları rasyonel olan bir dik üçgenin alanı olduğunda N sayısının $\mathbb{Q}$ cismi üzerinde bir denk sayı olduğu belirtilecektir. Tada (Tada 2001), $A, B \in \mathbb{Z}$ olmak üzere $E : y^2 = x(x + A)(x + B)$ eğrisinin torsiyon alt gruplarını sınıflandırmıştır, Tada tarafından verilen bu sonuçlar kullanılarak $E_N(\mathbb{K})$ grubunun torsiyon alt grubu belirlenebilir.

3.1. Sayı Cisimleri Üzerindeki Denk Sayılar

Denk sayı probleminin doğrudan eliptik eğriler teorisinin bir problemine dönüştürülebildiği daha önce de gösterilmişti. N sayısının bir denk sayı olduğunu kabul edelim. $a^2 + b^2 = c^2$ ve $\frac{1}{2}ab = N$ eşitliğinden, $x = c^2/4$ olmak üzere aralarındaki fark N olan üç kare sayının oluşturduğu $x - N$, x, $x + N$ aritmetik dizisi için $(x - N)x(x + N)$ sayısı da

bir rasyonel kare sayıdır. Başka bir deyişle, alanı N ve rasyonel kenar uzunlukları $a,\ b,\ c$ olan bir dik üçgen

$$E_N : Y^2 = X^3 - N^2X$$

eliptik eğrisi üzerindeki $(c^2/4,\ c(a^2 + b^2)/8)$ rasyonel noktaya karşılık gelir. Tersine, $y \neq 0$ olacak biçimde E_N eğrisi üzerinde verilen bir (x, y) rasyonel noktası için alanı N ve kenar uzunlukları $a,\ b,\ c$ olan bir dik üçgen elde etmek için

$$a = \left|\frac{y}{x}\right|,\ b = 2N\left|\frac{x}{y}\right|,\ c = \frac{x^2+y^2}{|y|} \tag{3.1}$$

olarak alınabilir.

Daha önce belirtildiği gibi, N sayısının bir denk sayı olması için gerek ve yeter koşul E_N eliptik eğrisinin $y \neq 0$ olacak biçimde bir rasyonel noktaya sahip olmasıdır.

3.1.1. Tanım. $\mathbb{K}$ bir sayı cismi ve N pozitif bir tamsayı olsun. Eğer $a^2 + b^2 = c^2$ ve $\frac{1}{2}ab = N$ eşitliğini gerçekleyen $a, b, c \in \mathbb{K}$ var ise N sayısına bir $\mathbb{K}$-***denk sayı*** denir.

Dikkat edilirse $\mathbb{Q}$-denk sayıları alışılmış denk sayılardır. $\mathbb{K}$-denk sayı olan bir N sayısı, alanı N ve kenar uzunlukları $\mathbb{K}$ cisminin elemanlarından olan bir dik üçgenin varlığını gerektirir.

3.1.2. Tanım. E bir cisim ve $F \subset E$ olsun. Eğer F, E cisminin işlemlerine göre bir cisim ise F cismine E cisminin bir ***alt cismi*** denir ve $F < E$ ile gösterilir. Eğer $F < E$ ise E cismine F cisminin bir ***cisim genişlemesi*** denir.

Herhangi bir N pozitif tamsayısının, $\mathbb{Q}$ cisminin belli kuadratik genişlemesinde bir denk sayı olduğunu görmek kolaydır. Örneğin $a = b = \sqrt{2}$ olarak alınırsa alanı $N = 1$ olan bir dik üçgen elde edilir. Ancak (3.1) eşitliğinde x ve y değerleri a, b ve c değerlerine bağlı olarak çözüldüğünde elde edilen $x = \frac{1}{2}a(a \pm c)$ ve $y = ax$ eşitlikleri, $(1 \pm \sqrt{2},\ \sqrt{2} \pm 2)$ noktalarının E_1 eğrisi üzerinde olduğunu gösterir ve bu noktalar $\mathbb{Q}(\sqrt{2})$ cismi üzerindeki tüm torsiyon noktalardır. Dolayısıyla bu noktalarla sonsuz çoklukta farklı dik üçgen elde edilemez. Bu örnek bizi aşağıdaki tanıma yönlendirir.

3.1.3. Tanım. N bir $\mathbb{K}$-denk olan sayı olsun. Eğer $a^2 + b^2 = c^2$ ve $\frac{1}{2}ab = N$ eşitliklerini gerçekleyen sonsuz çoklukta $a, b, c \in \mathbb{K}$ çözümü var ise N sayısına ***has*** $\mathbb{K}$***-denk sayı*** denir.

Tüm $\mathbb{Q}$-denk sayılar birer has $\mathbb{Q}$-denk sayı olduğundan $\mathbb{K} = \mathbb{Q}$ olması halinde yukarıda verilen tanım pek ilgi çekici değildir. Ancak yukarıdaki örnek, bu durumun farklı sayı cisimleri üzerinde değişebileceğini göstermektedir.

3.1.4. Teorem. Her N pozitif tamsayısı belli bir gerçel kuadratik $\mathbb{K}$ cismi üzerinde has $\mathbb{K}$-denk sayıdır (Girondo ve ark. 2009).

İspat. $a, b, c \in \mathbb{K}$ olmak üzere

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2N \end{cases}$$

sistemindeki ilk eşitlikte a yerine $\frac{2N}{b}$ yazılırsa

$$4N^2 + b^4 = c^2b^2$$

eşitliği elde edilir. Dolayısıyla,

$$c = \frac{\sqrt{4N^2+b^4}}{b}$$

dir. b seçilen herhangi bir rasyonel sayı ve $m = 4n^2 + b^4$ olmak üzere N sayısı $\mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayıdır. Böylece verilen bir $(a, b, c) \in \mathbb{Q}(\sqrt{m})^3$ üçlüsü için (2.19) eşitliği kullanılarak E_N eğrisi üzerindeki bir P $\mathbb{Q}(\sqrt{m})$-rasyonel noktası elde edilir. $E_N(\mathbb{Q}(\sqrt{m}))$ grubunun torsiyon alt grubu, 2-torsiyon alt grubuna, yani $(N, m) = (1, 2)$ ya da $(N,m) = (2, 2)$ durumları hariç olmak üzere $\{\mathcal{O}, (0, 0), (\pm N, 0)\}$ grubuna indirgenir. $b \in \mathbb{Q}$ sayısı $m \neq 2$ olacak biçimde seçilebilir ve bu halde P noktası bir torsiyon olmayan nokta haline gelir. ■

3.1.5. Uyarı. Tada (Tada 2001), eğer N sayısı bir $\mathbb{Q}$-denk sayı değil ise N sayısının $\mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayı olması için gerek ve yeter koşulun Nm sayısının bir $\mathbb{Q}$-denk sayı olması olduğunu göstermiştir. Bu gerçekten hareket ile aşağıdaki sonuçlar ifade edilebilir.

1 ve 11 sayılarının $\mathbb{Q}$-denk sayılar olmadığı bilindiği için 1 sayısı $\mathbb{Q}(\sqrt{11})$-denk sayı değildir. Yukarıdaki ispata göre $4N^2 + b^4 = 4 + b^4$ eşitliği, seçilen herhangi $b \in \mathbb{Q}$ sayısı, $d \in \mathbb{Q}$ olmak üzere $11 \cdot d^2$ biçiminde ifade edilemez, yani cinsi 1 olan

$$11y^2 = x^4 + 4$$

eğrisi $\mathbb{Q}$ üzerinde bir eliptik eğri değildir. Dolayısıyla bu eğri singüler olmayan $\mathbb{Q}$-rasyonel noktaya sahip değildir.

Benzer şekilde yukarıda verilen sonuç herhangi $n, m \in \mathbb{Z}^*$ çiftine uygulandığında aşağıdaki genellemeye ulaşılır: Cinsi 1 olan $C_{n,m} : my^2 = x^4 + 4$ eğrisini $C_{n,m}$ ile gösterelim. Bu durumda $C_{n,m}$ eğrisinin bir $\mathbb{Q}$-rasyonel noktaya sahip olması için gerek ve yeter koşul n sayısının bir $\mathbb{Q}(\sqrt{m}\,)$-denk sayı olmasıdır, veya denk olarak $C_{n,m}$ eğrisinin bir $\mathbb{Q}$-rasyonel noktaya sahip olması için gerek ve yeter koşul nm sayısının bir $\mathbb{Q}$-denk sayı olmasıdır.

3.1.6. Teorem. Her N pozitif tamsayısı, belli gerçel kübik cisim üzerinde has denk sayıdır. Daha kesin olarak, bir N pozitif tamsayısı için $\lambda = \lambda(N)$ olmak üzere

$$32\lambda^3 - 32\lambda^2 + 8\lambda + N^2 = 0$$

kübik eşitliğinin tek gerçel çözümü olsun, bu durumda koordinatları aşağıda (3.4) ve (3.5) eşitlikleri ile verilen $P_\lambda = (x_\lambda, y_\lambda)$ noktası, $\mathbb{Q}(\sqrt{\lambda})$ üzerindeki $Y^2 = X^3 - N^2X$ eliptik eğrisinin Mordell-Weil grubundaki sonsuz mertebeli noktadır (Girondo ve ark. 2009).

İspat. İspatta Chahal (Chahal 2006)'ın yöntemi takip edilecektir.

$$(Y^2 + 2XY - X^2)^4 + (2X^3Y + X^2Y^2) = (X^4 + Y^4 + 10X^2Y^2 + 4XY^3 + 12X^3Y)^2,$$

eşitliğinde $X = 1 - 20\lambda$ ve $Y = 4\lambda$ olarak alınırsa

$$(1 - 12\lambda + 4\lambda^2)^4 + 8\lambda(2\lambda - 1)^2 = (1 + 40\lambda - 104\lambda^2 + 160\lambda^3 + 16\lambda^4)^2$$

eşitliği elde edilir. Bu ise $d = d(\lambda) = 8\lambda(2\lambda - 1)^2$ olmak üzere $y^2 = x^3 + dx$ eliptik eğrisi üzerinde koordinatları

$$x = x(\lambda) = \frac{(1-12\lambda+4\lambda^2)^2}{4(1+2\lambda)^2} \tag{3.2}$$

$$y = y(\lambda) = \frac{(1-12\lambda+4\lambda^2)(1+40\lambda-104\lambda^2+160\lambda^3+16\lambda^4)}{8(1+2\lambda)^2} \tag{3.3}$$

olan (x, y) noktasını verir. N pozitif bir tamsayı olmak üzere $-N^2 = 8\lambda(2\lambda - 1)^2$ eşitliğini göz önüne alalım. Bu eşitliğin, $\kappa = \kappa(N) = \sqrt[3]{-8 - 27N + 3\sqrt{48N^2 + 81N^4}}$ olmak üzere

$$\lambda = \lambda(N) = \frac{1}{3} + \frac{1}{12}\kappa + \frac{1}{3\kappa}$$

ile verilen bir tek gerçel çözümü vardır. Buradaki κ, tüm N pozitif tamsayıları için negatif olacak biçimdeki tek gerçel küp kök olarak seçilmiştir. Gerekli hesaplamaların yapılması ile $E_N(\mathbb{Q}(\lambda))$ eğrisi üzerinde koordinatları

$$x = x(\lambda) = \frac{1}{4(N^2-16)^2}\{256 + 992N^2 + 65N^4 + (1024 - 2688N^2 - 28N^4)\lambda + (1024 + 1920N^2 + 4N^4)\lambda^2\} \quad (3.4)$$

$$y = y(\lambda) = \frac{1}{32(N^2-16)^3}\{-16384 + 72704N^2 + 80960N^4 + 2868N^6 - N^8 + (196608 - 462848N^2 - 145152N^4 - 1456N^6)\lambda + (196608 + 421888N^2 + 100608N^4 + 208N^6)\lambda^2\} \quad (3.5)$$

olan bir $P_\lambda = (x_\lambda, y_\lambda)$ noktası elde edilir. Bu değerler, aşağıdaki gibi el ile hesaplanarak ya da bir cebir programı kullanılarak kontrol edilebilir. Öncelikle (3.2) ve (3.3) eşitlikleri ile verilen koordinatların pay ve paydası sırasıyla $(1 + 2\lambda)^2$ ve $(1 + 2\lambda)^3$ ifadelerinin eşlenikleri ile çarpıldığında bu koordinatlar λ değişkenine bağlı rasyonel polinomlar olarak elde edilir. $\mathbb{Q}(\lambda)$ bir cisim olduğundan, bu polinomların derecesi en fazla ikidir, ki buradan (3.4) ve (3.5) eşitlikleri elde edilir. Geriye P_λ noktasının $E_N(\mathbb{Q}(\lambda))$ eğrisi üzerinde bir sonlu mertebeli nokta olduğunu göstermek kalır. Dikkat edilirse (x, y) noktasını $(-x, \sqrt{-1}y)$ noktasına gönderen dönüşüm E_N eliptik eğrisi üzerinde bir endomorfizmdir. Dolayısıyla E_N eliptik eğrisi $\mathbb{Z}[\sqrt{-1}]$ ile karmaşık çarpım işlemine sahiptir. Bu sonuçlar, $\mathbb{Q}(\lambda)$ kübik cismi üzerindeki E_N eliptik eğrisine uygulandığında,

"M, $E_N(\mathbb{Q}(\lambda))$ eğrisinin bir torsiyon noktasının mertebesi ise, bu durumda ϕ, Euler ϕ-fonksiyonu olmak üzere $\phi(M) \leq 6$"

sonucu elde edilir. Dolayısıyla $M \in \mathcal{B} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18\}$ dir. Dolayısıyla P_λ noktasının mertebesinin $\mathcal{B}$ kümesinde olmadığını ispatlamak yeterlidir. Bunun için E_N eliptik eğrisi ile ilişkilendirilmiş $\Psi_m(x)$ *m-bölüm* polinomu kullanılır. x_λ

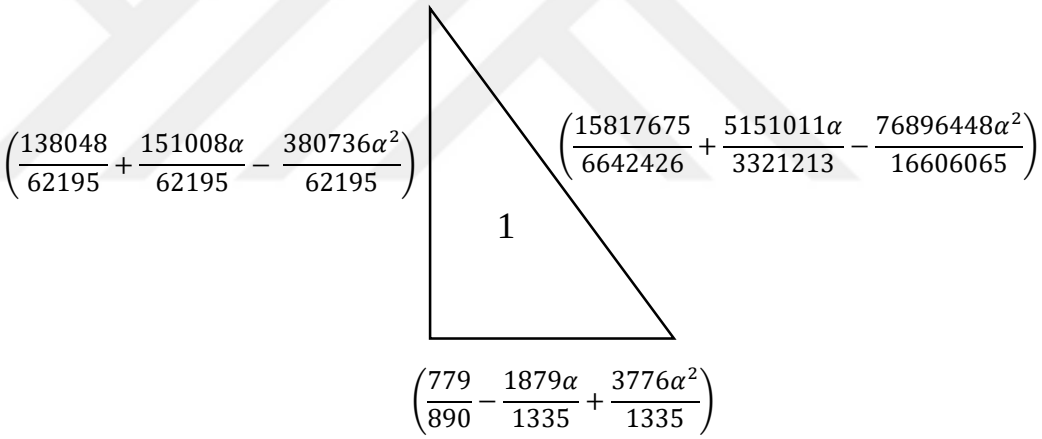
noktasının, $\mathbb{Q}(\lambda)$ üzerinde $m \in \mathcal{B}$ için $\Psi_m(x)$ polinomunun bir kökü olmadığının kontrol edilmesi yeterlidir. $P_{k,\,m} \in \mathbb{Q}[n]$, $k = 0, 1, 2$ için kökleri tamsayı olmayan polinomlar ve $m \in \mathcal{B}$ olmak üzere,

$$\Psi_m(x_\lambda) = P_{0,\,m}(N) + P_{1,\,m}(N)\lambda + P_{2,\,m}(N)\lambda^2$$

dir. Dolayısıyla $m \in \mathcal{B}$ ve herhangi $N \in \mathbb{Z}$ için $\Psi_m(x_\lambda) \neq 0$ dır. Bu ise $P_{\lambda(N)}$ noktasının sonsuz mertebeli ve dolayısıyla $E_N(\mathbb{Q}(\lambda))$ eğrisinin Mordell-Weil grubunun rankının pozitif olduğunu ispatlar.

3.1.7. Örnek. $\alpha = \frac{1}{3} + \frac{1}{12} \cdot \sqrt[3]{-35 + 3\sqrt{129}} + \frac{1}{3\sqrt[3]{-35+3\sqrt{129}}}$ olmak üzere $N = 1$ tamsayısı $\mathbb{Q}(\alpha)$ kübik cismi üzerinde bir denk sayıdır (Girondo ve ark. 2009).

Aşağıdaki şekil, alanı 1 ve kenar uzunlukları $\mathbb{Q}(\alpha)$ cisminin elemanlarından olan bir dik üçgeni göstermektedir.



Şekil 3.1. Alanı 1 ve kenar uzunlukları $\mathbb{Q}(\alpha)$ cisminin elemanlarından olan bir dik üçgen

Verilen bir $\mathbb{K}$ cismi için, $\mathbb{K}$ cismi üzerindeki denk sayılar hangileridir?

Her N pozitif tamsayısı için E_N, $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - N^2x$ eşitliği ile tanımlanan eliptik eğri ve k bir sayı cismi olmak üzere $E_N(k)$, E_N eliptik eğrisi üzerindeki k-rasyonel noktaların oluşturduğu grup olmak üzere aşağıdaki teoremde N sayısının $E_N(\mathbb{Q})$ grubuna bağlı olarak bir denk sayı olması için gerek ve yeter koşul belirtilmektedir.

3.1.8. Teorem. Bir N pozitif tamsayısının bir denk sayı olması için gerek ve yeter koşul $E_N(\mathbb{Q})$ grubunun bir sonsuz mertebeli noktaya sahip olmasıdır (Koblitz 1993).

$\mathcal{O}$ noktası, E_N eliptik eğrisi üzerindeki grup yapısı için birim eleman olan $E_N(\mathbb{Q})$ grubunun sonsuzdaki noktası olsun. Teorem 3.1.8.'in ispatında, $E_N(\mathbb{Q})$ grubunun torsiyon alt grubunun $\mathcal{O}$, (0, 0) ve 1 ya da 2 mertebeli ($\pm N$, 0) elemanlarından oluştuğunun kullanıldığına dikkat ediniz.

Herhangi N pozitif tamsayısı için, N sayısının bir denk sayı olup olmadığının belirlenmesi problemi oldukça eski bir problemdir. Teorem 3.1.8. ile ilgili olarak bazı önemli sonuçlar bilinmektedir. J. Coates ve A. Wiles (Coates ve Wiles 1977) tarafından yapılan çalışmalardan, karmaşık çarpım işlemi ile $\mathbb{Q}$ cismi üzerindeki E eliptik eğrileri için $E_N(\mathbb{Q})$ grubunun rankı pozitif ise bu durumda $L(E_N, s)$, Hasse-Weil L-fonksiyonu olmak üzere $L(E_N, 1) = 0$ olduğu sonucu elde edilir. Zayıf Birch and Swinnerton-Dyer (Birch ve Swinnerton-Dyer 1963, 1965) konjektürünün doğru olduğu varsayıldığında $L(E_N, 1) = 0$ ise $E_N(\mathbb{Q})$ grubunun rankı pozitiftir. F. R. Nemenzo (Nemenzo 1998), $N < 42553$ için BSD konjektürünün E_N eliptik eğrisi için gerçeklendiğini yani, $E_N(\mathbb{Q})$ grubunun rankının pozitif olması için gerek ve yeter koşulun $L(E_N, 1) = 0$ olması gerektiğini göstermiştir. Üstelik J. B. Tunnell (Tunnell 1983) tarafından $L(E_N, 1) = 0$ olacak biçimdeki N tamsayısı için bir gerek ve yeter koşul vermiştir. Böylece Tunnell tarafından, zayıf BSD konjektürünün doğru olduğu kabul edilerek, N sayısının bir denk sayı olup olmadığının belirlenmesi için basit bir kriter elde edilmiştir.

3.1.9. Teorem. N sayısı bir pozitif tamsayı olsun ve $m \neq 2$ olduğunu kabul edelim. Bu durumda N sayısının $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayı olması için gerek ve yeter koşul $E_N(\mathbb{K})$ grubunun bir sonsuz mertebeli noktaya sahip olmasıdır (Tada 2001).

$m = 2$ olması halinde Teorem 3.1.9. gerçeklenmez. Örneğin, $m = 2$ ve $N = 1$ olması halinde kenar uzunlukları ($\sqrt{2}$, $\sqrt{2}$, 2) ve alanı 1 olan bir dik üçgen elde edilir. Ancak, aşağıda ele alınacak olan Teorem 3.1.14. kullanılarak, $E_1(\mathbb{Q}(\sqrt{m}))$ grubunun rankının sıfır olduğu görülebilir. Teorem 3.1.9. ve Teorem 3.1.14. bir araya getirilerek aşağıdaki sonuç elde edilir.

3.1.10. Sonuç. N bir pozitif tamsayı olmak üzere $m \neq 2$ olduğunu kabul edelim. Bu durumda N sayısının $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayı olması için gerek ve yeter koşul N ya da Nm sayılarının $\mathbb{Q}$ üzerinde bir denk sayı olmasıdır (Tada 2001).

N sayısının $\mathbb{Q}$ cismi üzerinde bir denk olmayan sayı olduğunu kabul edelim. Bu bölümdeki bir başka amaç kenar uzunlukları $\mathbb{K}$ cismine ait ve alanı N olan dik üçgenleri sınıflandırmaktır. $2P \in 2E_N(\mathbb{K})\backslash\{\mathcal{O}\}$ noktalarının oluşturduğu küme ile alanı N ve kenar uzunlukları $(X, Y, Z) \in \mathbb{K}^3$ olan dik üçgenlerin kümesi arasındaki eşleme ve σ, $Gal(\mathbb{K}/\mathbb{Q})$ grubunun üreteci olmak üzere $P + \sigma(P)$ noktaları dikkate alınarak, kenar uzunlukları $\mathbb{K}$ cismine ait ve alanı N olan dik üçgenler aşağıdaki gibi sınıflandırılabilir.

3.1.11. Teorem. N sayısı $\mathbb{Q}$ cismi üzerinde bir denk olmayan sayı olsun. Bu durumda,

1. $X \leq Y < Z$ olmak üzere alanı N ve kenar uzunlukları $X, Y, Z \in \mathbb{K} = \mathbb{Q}(\sqrt{m})$ olan herhangi dik üçgen aşağıda verilen tipteki dik üçgenlerden biridir: σ, $Gal(\mathbb{K}/\mathbb{Q})$ grubunun üreteci olmak üzere,

1. Tip. $X\sqrt{m}, Y\sqrt{m}, Z\sqrt{m} \in \mathbb{Q}$,

2. Tip. $X, Y, Z\sqrt{m} \in \mathbb{Q}$,

3.Tip. $\sigma(X) = Y, Z \in \mathbb{Q}$ olmak üzere $X, Y \in \mathbb{K}\backslash\mathbb{Q}$,

4. Tip. $\sigma(X) = -Y, Z \in \mathbb{Q}$ olmak üzere $X, Y \in \mathbb{K}\backslash\mathbb{Q}$ dir.

2. $m \equiv 3, 6, 7 \pmod 8$ veya m sayısı $q \equiv 3 \pmod 4$ biçiminde bir asal çarpana sahip ise, 2. tipte bir dik üçgen yoktur, üstelik bu durumda 3. ve 4. tipte de bir dik üçgen yoktur.

3. $m \equiv 3, 5, 6, 10, 11, 13 \pmod{16}$ veya m sayısı $q \equiv 3, 5 \pmod 8$ biçiminde bir asal çarpana sahip ise 3. ve 4. tipte bir dik üçgen yoktur (Tada 2001).

3.1.12. Uyarı. $m = 2$ olsun. Belli $c \in \mathbb{N}$ için $N = c^2$ ise, kenar uzunlukları $X = Y = c\sqrt{2}$ ve alanı N olan 4. tip bir dik üçgen vardır. Belli $c' \in \mathbb{N}$ için $N = 2c'^2$ ise kenar uzunlukları $X = Y = 2c'$ ve alanı N olan bir 2.tip dik üçgen vardır (Tada 2001).

Buradaki bir diğer amaç, alanı N ve kenar uzunlukları $\mathbb{Q}(\sqrt{m})$ cismine ait olan dik üçgenlerin tipleri üzerine, N ve Nm sayılarının $\mathbb{Q}$ cismi üzerinde birer denk sayı olmasına denk olan bir koşul vermektir.

3.1.13. Teorem. Bir N pozitif tamsayısının, $X \leq Y < Z$, $Z \notin \mathbb{Q}$ ve $Z\sqrt{m} \notin \mathbb{Q}$ olacak biçimde $X, Y, Z \in \mathbb{Q}(\sqrt{m})$ kenar uzunluklarına sahip bir dik üçgenin alanı olması için

gerek ve yeter koşul N ve Nm sayılarının $\mathbb{Q}$ cismi üzerinde birer denk sayı olmasıdır (Tada 2001).

Herhangi $\mathbb{K}$ gerçel kuadratik cismi için, Teorem 3.1.9., Teorem 3.1.11. ve Sonuç 3.1.10.'un ispatlanması için $E_N(\mathbb{K})$ grubunun rankının bilinmesi gerekir.

3.1.14. Teorem. $E, a, b, c \in k$ olmak üzere k sayı cismi üzerinde

$$E : y^2 = x^3 + ax^2 + bx + c$$

biçiminde tanımlanan bir eliptik eğri ve D, $k\backslash\{\alpha^2 \mid \alpha \in k\}$ kümesinin bir elemanı olsun. Bu durumda E^D, E eğrisinin $k(\sqrt{D})$ cismi üzerinde

$$E^D: y^2 = x^3 + aDx^2 + bD^2x + cD^3$$

biçiminde tanımlanan tivisti (kıvrılması) olmak üzere

$$\text{rank}\,(E(k(\sqrt{D}))) = \text{rank}\,(E(k)) + \text{rank}\,(E^D(k))$$

dır (Tada 2001).

Aşağıdaki teorem $2E_N(\mathbb{K})$ grubunun elemanlarının tanınmasına olanak verir.

3.1.15. Teorem. k, karakteristiği 2 ve 3'ten farklı bir cisim ve E, k cismi üzerinde bir eliptik eğri olsun. $\alpha, \beta, \gamma \in k$ olmak üzere E eliptik eğrisinin

$$E_N : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

biçiminde tanımlandığını varsayalım. (x_0, y_0) noktası, $E\backslash\{\mathcal{O}\}$ kümesinin bir k-rasyonel noktası olsun. Bu durumda, E eliptik eğrisinin $2(x_1, y_1) = (x_0, y_0)$ olacak biçimde bir k-rasyonel (x_1, y_1) noktasının var olması için gerek ve yeter koşul $x_0 - \alpha$, $x_0 - \beta$ ve $x_0 - \gamma$ sayılarının k cisminde birer kare sayı olmasıdır (Tada 2001).

Yukarıdaki Teorem 3.1.9'un ispatını vermek için ilk olarak aşağıdaki önermeyi kullanarak $E_N(\mathbb{Q}(\sqrt{m}))$ grubunun torsiyon alt grubunu belirleyelim.

3.1.16. Önerme. N, 1 veya karesiz pozitif tamsayı olmak üzere $T(E_N, k)$, k sayı cismi üzerinde $E_N(k)$ grubunun torsiyon alt grubu ve $E_N[2]$, E_N grubunun 2-torsiyon alt grubu olsun.

i. $N = 1$, $m = 2$ ise

$$T(E_1, \mathbb{Q}(\sqrt{2})) = \{\mathcal{O}, (0, 0), (\pm 1, 0), (1 + \sqrt{2}, \pm(2 + \sqrt{2})), (1 - \sqrt{2}, \pm(2 - \sqrt{2}))\},$$

ii. $N = 2$, $m = 2$ ise

$$T(E_2, \mathbb{Q}(\sqrt{2})) = \{\mathcal{O}, (0, 0), (\pm 2, 0), (2 + 2\sqrt{2}, \pm 4(1 + \sqrt{2})), (2 - 2\sqrt{2}, \pm 4(1 - \sqrt{2}))\},$$

iii. Diğer hallerde,

$$T(E_N, \mathbb{Q}(\sqrt{m})) = E_N[2] = \{\mathcal{O}, (0, 0), (\pm N, 0)\}$$

dır (Tada 2001).

İspat. E_N grubunun 2-torsiyon alt grubu $E_N[2]$, $\mathcal{O}$, $(0, 0)$ ve $(\pm N, 0)$ olmak üzere dört noktadan oluşur, yani

$$T(E_N, \mathbb{Q}(\sqrt{m})) \supset E_N[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

dir. E_N^m, $\mathbb{Q}(\sqrt{m})$ üzerinde $y^2 = x^3 - (Nm)^2 x$ ile tanımlanan E_N eğrisinin kıvrılması olmak üzere $E_N^m = E_{Nm}$ ve böylece $T(E_N^m, \mathbb{Q}) = T(E_{Nm}, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ dir. $T(E_N, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ olduğundan, Kwon'un (Kwon 1997) vermiş olduğu sonuç kullanılarak

$$T(E_N, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ veya } T(E_N, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

elde edilir.

$T(E_N, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ olduğunu varsayalım. Bu durumda $T(E_N, \mathbb{Q}(\sqrt{m}))$ grubunda dört mertebeli bir P noktası vardır. Dolayısıyla, $2P = (0, 0)$ veya $2P = (\pm N, 0)$ olmalıdır. Teorem 3.1.15. gereği, eğer $2P = (0, 0)$ veya $2P = (-N, 0)$ ise $-N$ sayısı $\mathbb{Q}(\sqrt{m})$ cisminde bir kare sayıdır, ki bu bir çelişkidir. Eğer $2P = (N, 0)$ ise Teorem 3.1.15. gereği N ve $2N$ sayıları $\mathbb{Q}(\sqrt{m})$ de birer kare sayı olmalıdır. N sayısı bir karesiz tamsayı olduğundan, $N = 1$, $m = 2$ ya da $N = m = 2$ olduğu sonucu elde edilir. Eliptik eğriler üzerindeki duplikasyon formülü ile elde edilen denklemler çözülerek $T(E_N, \mathbb{Q}(\sqrt{m}))$ grubu tam olarak tanımlanabilir. Diğer hallerde ise $T(E_N, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ dir.■

Teorem 3.1.9.'un İspatı. k cismi, $\mathbb{R}$ cisminin bir alt cismi olmak üzere N pozitif tamsayısı için,

$$S = \{(X, Y, Z) \in k^3 \mid 0 < X \leq Y < Z, X^2 + Y^2 = Z^2 \text{ ve } XY = 2N\}$$

ve

$$T = \{(u, v) \in 2E_N(k)\backslash\{\mathcal{O}\} \mid v \geq 0\}$$

olsun. Bu durumda $(X, Y, Z) \in S$ için $\varphi : S \longrightarrow T$,

$$\varphi(X, Y, Z) = \left(\left(\frac{Z}{2}\right)^2, \frac{Z(Y^2 - X^2)}{8}\right)$$

ve Teorem 3.1.15. gereği, $(u, v) \in T$ için $\psi : T \longrightarrow S$,

$$\psi(u, v) = (\sqrt{u+n} - \sqrt{u-n},\ \sqrt{u+n} + \sqrt{u-n},\ 2\sqrt{u})$$

olarak tanımlanan φ ve ψ dönüşümleri dikkate alındığında ψ dönüşümünün, φ dönüşümünün tersi olduğu kolayca görülebilir.

Şimdi $S \neq \emptyset$ olması için gerek ve yeter koşulun $E_N(k)\backslash E_N[2] \neq \emptyset$ olduğunu görelim. İlk olarak $S \neq \emptyset$ olduğunu varsayalım. $(X, Y, Z) \in S$ için $Q = \varphi(X, Y, Z)$ olsun. Q noktası T üzerinde olduğundan $Q = 2P$ olacak biçimde bir $P \in E_N(k)\backslash E_N[2]$ noktası vardır, o halde $E_N(k)\backslash E_N[2] \neq \emptyset$ dir. Tersine $E_N(k)\backslash E_N[2] \neq \emptyset$ olduğunu varsayalım. $P \in E_N(k)\backslash E_N[2]$ olmak üzere $2P = (x_0, y_0)$ olarak alalım. Teorem 3.1.15. gereği $x_0 - N$, x_0 ve $x_0 + N$ sayıları k cisminde birer kare sayıdır. Dolayısıyla ψ dönüşümü kullanılarak kenar uzunlukları k cismine ait olan bir dik üçgen elde edilir.

k cismini $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ kuadratik cismi olarak alalım ve $m \neq 2$ olsun. Bu durumda Önerme 3.1.16. gereği $T(E_N, \mathbb{K}) = E_N[2]$ dir. Dolayısıyla $E_N(\mathbb{K})$ grubunun rankının pozitif olması için gerek ve yeter koşul $E_N(\mathbb{K})\backslash E_N[2] \neq \emptyset$ olmasıdır. Böylece ispat tamamlanmış olur.■

Sonuç 3.1.10.'un İspatı. Teorem 3.1.14. gereği, rank $(E_N(\mathbb{K})) > 0$ olması için gerek ve yeter koşul rank $(E_N(\mathbb{Q})) > 0$ ya da rank $(E_N^m(\mathbb{Q})) > 0$ olmasıdır. Burada E_N^m, $\mathbb{K}$ cismi üzerinde tanımlı $E_N : y^2 = x^3 - (Nm)^2x$ eliptik eğrisinin kıvrılmasıdır. Dolayısıyla $E_N^m = E_{Nm}$ ve böylece rank $(E_N^m(\mathbb{Q})) > 0$ olması için gerek ve yeter koşul Nm sayısının bir denk sayı olmasıdır.■

Şimdi Teorem 3.1.11'in (1) şıkkını ispatlayalım. N sayısı $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ cismi üzerinde bir denk sayı ve $0 < X \leq Y < Z$, $X, Y, Z \in \mathbb{K}$ olmak üzere X, Y, Z sayıları alanı N olan bir dik üçgenin kenar uzunlukları olsun. Bu durumda, Teorem 3.1.9.'un ispatında

görüldüğü gibi $\psi(2P) = (X, Y, Z)$ olacak biçimde bir $P \in E_N(\mathbb{K})\backslash E_N[2]$ noktası vardır. $E_N(\mathbb{R})$ üzerindeki grup işleminin geometrik yorumlanmasıyla, gerekli olması halinde $P = (x, y)$ noktasının yerine, $P + (0, 0)$, $P + (N, 0)$ veya $P + (-N, 0)$ noktaları alınarak $x \geq (1 + \sqrt{2})N$ eşitsizliğinin gerçeklendiği varsayılabilir. $2P = (u, v)$ ve $|\cdot|$, $\iota(\sqrt{m})$ pozitif olacak biçimde $\iota : \mathbb{K} \hookrightarrow \mathbb{R}$ gömme dönüşümünden indirgenen alışılmış mutlak değer olsun. Yukarıda verilen duplikasyon formülü ile

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

ve böylece,

$$\sqrt{u+N} = \frac{x^2+2Nx-N^2}{2|y|},\ \sqrt{u-N} = \frac{x^2-2Nx-N^2}{2|y|},\ \sqrt{u} = \frac{x^2+N^2}{2|y|}$$

olarak bulunur. Dolayısıyla, ψ dönüşümü kullanılarak,

$$X = \frac{2Nx}{|y|},\ Y = \frac{x^2-N^2}{|y|},\ Z = \frac{x^2+N^2}{|y|}$$

olarak elde edilir. σ, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ grubunun üreteci ve $\sigma(P) = (\sigma(x), \sigma(y))$ olsun. $P + \sigma(P)$, $E_N(\mathbb{Q})$ grubunun bir elemanı ve N sayısı $\mathbb{Q}$ cismi üzerinde bir denk olmayan sayı olduğundan

$$P + \sigma(P) \in T(E_N, \mathbb{Q}) = \{\mathcal{O}, (0, 0), (\pm N, 0)\}$$

dir. Dolayısıyla aşağıdaki durumlardan biri elde edilir:

1. Durum. $P + \sigma(P) = \mathcal{O}$ dır. $E_N(\mathbb{R})$ grubu üzerindeki toplama işleminin geometrik yorumu ile $\sigma(x) = x$ ve $\sigma(y) = -y$ olarak bulunur. Dolayısıyla x ve $y\sqrt{m}$ sayıları birer rasyonel sayıdır. Dolayısıyla $X\sqrt{m}$, $Y\sqrt{m}$ ve $Z\sqrt{m}$ sayıları birer rasyonel sayıdır ve böylece 1.tip bir dik üçgen elde edilmiş olur.

2. Durum. $P + \sigma(P) = (0, 0)$ dır. $E_N(\mathbb{R})$ grubu üzerindeki toplama işleminin geometrik yorumu ile $\frac{\sigma(x)}{x} = \frac{\sigma(y)}{y} = \alpha$ olarak bulunur. O halde,

$$\sigma(y)^2 = \alpha^2 y^2 = \alpha^2 x^3 - \alpha^2 N^2 x$$

ve $\sigma(P)$, E_N eğrisi üzerindeki bir nokta olduğundan

$$\sigma(y)^2 = \sigma(x)^3 - N^2\,\sigma(x) = \alpha^3 x^3 - N^2 \alpha x$$

elde edilir. $\alpha \neq 0, 1$ ve $x \neq 0$ olduğu kolayca görülebilir, dolayısıyla bu eşitliklerden

$$\alpha x^2 = -N^2$$

elde edilir. Bu eşitlik yardımıyla

$$Y = x(x + \sigma(x))/|y| \text{ ve } Z\sqrt{m} = x(x - \sigma(x))\sqrt{m}/|y|$$

olarak elde edilir. $x/y = \sigma(x/y)$ ve $x \geq (1 + \sqrt{2})N > 0$ olduğundan $x/|y|$ sayısı rasyoneldir. Dolayısıyla, $X = 2Nx/|y|$, Y ve $Z\sqrt{m}$ sayıları birer rasyonel sayıdır, böylece dik kenar uzunlukları rasyonel olan 2.tip bir dik üçgen elde edilmiş olur.

3. Durum. $P + \sigma(P) = (N, 0)$ dir. $E_N(\mathbb{R})$ grubu üzerindeki toplama işleminin geometrik yorumu ile $\sigma(x - N)/(x - N) = \sigma(y)/y = \beta$ elde edilir. $z = x - N$ olsun. O halde

$$\sigma(y)^2 = \beta^2 z^3 + 3\beta^2 z^2 N + 2\beta^2 z N^2$$

ve $\sigma(P)$, E_N eğrisi üzerinde bir nokta olduğundan,

$$\sigma(y)^2 = \beta^3 z^3 + 3\beta^2 z^2 N + 2\beta z N^2$$

elde edilir. $\beta \neq 0, 1$ ve $z \neq 0$ olduğu kolayca görülebilir, dolayısıyla bu iki eşitlikten

$$\beta z^2 = 2N^2$$

elde edilir. Bu eşitlik ve $x = z + N$ eşitliği X, Y ve Z değerlerinde yerine yazıldığında

$$X = z(\sigma(z) + 2N)/|y|,\ Y = z(z + 2N)/|y| \text{ ve } Z = z(z + 2N + \sigma(z))/|y|$$

olarak elde edilir. $z/y = \sigma(z/y)$ ve $z > 0$ olduğundan, $z/|y|$ rasyoneldir. Dolayısıyla Z rasyonel ve $\sigma(X) = Y$ dir. Böylece iki kenar uzunluğu birbirinin eşleniği ve bir kenar uzunluğu da rasyonel sayı olan 3.tip bir dik üçgen elde edilmiş olur.

4. Durum. $P + \sigma(P) = (-N, 0)$ dır. $w = x + N$ olarak alınırsa 3.tip bir dik üçgen elde edilen durumda olduğu gibi $w/|y|$ ve Z sayılarının birer rasyonel sayı ve

$$X = w(-\sigma(w) + 2N)/|y| \text{ ve } Y = w(w - 2N)/|y|$$

olduğu gösterilebilir, bu ise $\sigma(X) = -Y$ olmasını gerektirir. Böylece, $\sigma(X) = -Y$ olmak üzere iki kenar uzunluğu X, Y ve bir kenar uzunluğu da $Z \in \mathbb{Q}$ biçimindeki 4.tip bir dik üçgen elde edilmiş olur.■

Şimdi de, Teorem 3.1.11.'in (3) ü ispatlanacaktır. 3.tip (ve 4.tip) bir dik üçgenin var olduğunu kabul edelim ve a, b, c sayıları pozitif rasyonel sayılar olmak üzere bu dik üçgenin dik kenar uzunlukları $a - b\sqrt{m}$ (ve $-a + b\sqrt{m}$), $a + b\sqrt{m}$ ve hipotenüs uzunluğu c olsun. Bu durumda $(x, y, z) = (a, b, c)$,

$$2x^2 + 2my^2 = z^2$$

eşitliğinin sıfırdan farklı bir çözümüdür. Hasse teoremi gereği, yukarıdaki eşitliğin rasyonel sayılarda bir çözümünün olması için gerek ve yeter koşul $\mathbb{Q}_p$, p-adic sayıların oluşturduğu cisim olmak üzere bu eşitliğin her p asal sayısı için $\mathbb{Q}_p$ cisminde bir çözüme sahip olmasıdır. Hilbert sembolleri kullanılarak, bu eşitliğin $\mathbb{Q}_2$ cisminde bir çözümünün olması için gerek ve yeter koşulun $m \equiv 1, 2, 7, 9, 14, 15 \pmod{16}$ olduğu ve m sayısının $q \neq 2$ asal çarpanı için $p = q$ olması halinde yukarıdaki eşitliğin $\mathbb{Q}_p$ cisminde bir çözümünün olması için gerek ve yeter koşulun 2 sayısının q modülüne göre bir ikinci dereceden kalan yani, $q \equiv 1, 7 \pmod{8}$ olduğu görülebilir.

Son olarak Teorem 3.1.11.'in (2) si ispatlanacaktır. Tıpkı Teorem 3.1.11'in (3) durumunda olduğu gibi Hilbert sembolleri kullanılarak, $m \equiv 3, 6, 7 \pmod{8}$ ya da m sayısının $q \equiv 3 \pmod{4}$ biçiminde bir asal çarpanı varsa, bu durumda 2.tip dik üçgen elde edilemez. Bundan başka $\{P + \sigma(P)\}$ kümesi, $E_N[2]$ grubunun bir alt grubu olduğundan alanı N olan farklı tipteki dik üçgenlerin sayısı üç olamaz. Dolayısıyla, eğer 2.tip dik üçgen yoksa, bu durumda 3.tip ya da 4.tip dik üçgenlerin olmadığı sonucu elde edilir. ■

Yukarıda verilen Teorem 3.1.13'ün ispatı için N ve Nm sayılarının $\mathbb{Q}$ üzerinde birer denk sayı olduğunu kabul edelim. Denk sayı tanımı gereği, $a^2 + b^2 = c^2$, $ab = 2N$ ve $a < b < c$ olacak biçimde a, b, c rasyonel sayıları vardır. Benzer şekilde $d^2 + e^2 = f^2$, $de = 2mn$ ve $d < e < f$ olacak biçimde d, e, f rasyonel sayıları vardır. Dolayısıyla n sayısı aynı zamanda

$$\left(\frac{d}{\sqrt{m}}, \frac{e}{\sqrt{m}}, \frac{f}{\sqrt{m}}\right)$$

biçimindeki bir dik üçgenin alanı olur.

$\varphi : S \longrightarrow T$ ve $\psi : T \longrightarrow S$ dönüşümleri yukarıda belirtilmiş olan dönüşümler olmak üzere $P = (u, v) = \varphi(a, b, c) + \psi\left(\frac{d}{\sqrt{m}}, \frac{e}{\sqrt{m}}, \frac{f}{\sqrt{m}}\right)$ olsun. Bu durumda

$$u = \frac{f^2(e^2 - d^2)^2 + m^3c^2(b^2 - a^2)^2 - (f^2 + mc^2)(f^2 - mc^2)^2}{4m(f^2 - mc^2)^2}$$
$$- \frac{cf(b^2 - a^2)(e^2 - d^2)\sqrt{m}}{2(f^2 - mc^2)^2}$$

dir. Gerekli olması halinde P noktasının yerine $-P$ noktası alınarak $P = (u, v)$ noktasının $v \geq 0$ özelliğindeki bir nokta olduğu varsayılabilir. $(u, v) \in T$ olduğundan $\psi(u, v) \in S$ dir. (X, Y, Z), yukarıda elde edilen alanı N olan dik üçgenin üç kenar uzunluğunun oluşturduğu sistem olsun. Teorem 3.1.15. ve eliptik eğri üzerindeki noktalar için toplama kuralı kullanılarak $X, Y, Z \in \mathbb{Q}(\sqrt{m})$, $Z \notin \mathbb{Q}$ ve $Z\sqrt{m} \notin \mathbb{Q}$ olduğu görülebilir.

Tersine, N veya Nm sayıları $\mathbb{Q}$ üzerinde denk olmayan sayı olsun. N sayısının $\mathbb{Q}$ üzerinde bir denk olmayan sayı ve Nm sayısının da $\mathbb{Q}$ üzerinde bir denk sayı olduğunu varsayalım. Teorem 3.1.11. (1) gereği N sayısı, $X \leq Y < Z$, $Z \notin \mathbb{Q}$ ve $Z\sqrt{m} \notin \mathbb{Q}$ olacak biçimde üç kenar uzunluğu $X, Y, Z \in \mathbb{Q}(\sqrt{m})$ olan bir dik üçgenin alanı değildir. Şimdi de Nm sayısının $\mathbb{Q}$ üzerinde bir denk olmayan sayı ve N sayısının $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ üzerinde bir denk sayı olduğunu varsayalım. $(a, b, c) \in \mathbb{K}^3$, alanı N olan dik üçgenlerin kenar uzunluklarının oluşturduğu bir sistem olsun. Üçgenin tüm kenar uzunlukları $\sqrt{m}$ ile çarpılarak, alanı Nm ve üç kenar uzunluğu $(a\sqrt{m}, b\sqrt{m}, c\sqrt{m}) \in \mathbb{K}^3$ olan bir dik üçgen elde edilir. Nm pozitif tamsayısı için, φ' dönüşümünü φ dönüşümüne benzer şekilde tanımlayalım. Bu durumda, bir $P' \in E_{Nm}(\mathbb{K})$ noktası için $2P' = \varphi'((a\sqrt{m}, b\sqrt{m}, c\sqrt{m}))$ olarak alınabilir. $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ grubunun σ üreteci için, $P' + \sigma(P') \in E_{Nm}(\mathbb{Q})$ ve Nm sayısı $\mathbb{Q}$ üzerinde bir denk olmayan sayı olduğundan

$$P' + \sigma(P') \in T(E_{Nm}, \mathbb{Q}) = \{\mathcal{O}, (0, 0), (\pm Nm, 0)\}$$

dir. O halde Teorem 3.1.11. (1) in ispatında olduğu gibi aşağıdaki durumlardan birinin gerçekleştiği görülür:

1. Durum. $a, b, c \in \mathbb{Q}$

2. Durum. $a\sqrt{m},\ b\sqrt{m},\ c \in \mathbb{Q}$

3. Durum. $\sigma(a) = -b$, $c\sqrt{m} \in \mathbb{Q}$ olmak üzere $a, b \in \mathbb{K}\backslash\mathbb{Q}$

4. Durum. $\sigma(a) = b$, $c\sqrt{m} \in \mathbb{Q}$ olmak üzere $a, b \in \mathbb{K}\backslash\mathbb{Q}$.

Dolayısıyla N sayısı, $Z \notin \mathbb{Q}$ ve $Z\sqrt{m} \notin \mathbb{Q}$ olmak üzere $Z = c$ hipotenüs uzunluğuna sahip bir dik üçgenin alanı değildir. Son olarak N ve Nm sayılarının $\mathbb{Q}$ üzerinde birer denk olmayan sayılar olduklarını varsayalım. $m \neq 2$ olması halinde Sonuç 3.1.10. gereği, N sayısı $\mathbb{K}$ üzerinde bir denk sayı değildir. $m = 2$ ve N sayısının $\mathbb{K}$ üzerinde bir denk sayı olması halinde, alanı N olan dik üçgen dik kenar uzunlukları eşit, yani $X = Y$ özelliğinde bir dik üçgendir. Böylece N sayısının, $Z \notin \mathbb{Q}$ ve $Z\sqrt{m} \notin \mathbb{Q}$ olmak üzere Z hipotenüs uzunluğuna sahip bir dik üçgenin alanı olmadığı sonucu elde edilmiş olur. ■

3.1.17. Örnek. Burada bazı dik üçgen örnekleri verilecektir. N bir pozitif tamsayı, m bir karesiz pozitif tamsayı ve $X \leq Y < Z$ olmak üzere $X, Y, Z \in \mathbb{K} = \mathbb{Q}(\sqrt{m})$ sayıları, alanı N olan bir dik üçgenin kenar uzunlukları olsun. Yukarıda ele alınmış olan φ dönüşümü kullanılarak $Q = \varphi(X, Y, Z) \in 2E_N(\mathbb{K})\backslash\{\mathcal{O}\}$ olarak alalım.

1. $N = 2$, $m = 17$ için 1., 2., 3.tip ve Teorem 3.1.11. (1) de verilen 4.tip dik üçgenleri ve $2E_N(\mathbb{K})\backslash\{\mathcal{O}\}$ kümesine karşılık gelen noktaları oluşturalım (Tada 2001).

1.Tip. 34 (= 2·17) sayısı $\mathbb{Q}$ üzerinde bir denk sayıdır ve rasyonel kenar uzunlukları (15/2, 136/15, 353/30) ve alanı 34 olan bir dik üçgen vardır. Bu üçgenin tüm kenar uzunlukları $\sqrt{17}$ ile bölünerek

$$(X, Y, Z) = \left(\frac{15\sqrt{17}}{34},\ \frac{8\sqrt{17}}{15},\ \frac{353\sqrt{17}}{510}\right)$$

biçimindeki dik üçgen ve

$$Q = \left(\frac{2118353}{1040400},\ \pm\frac{8245727\sqrt{17}}{62424000}\right) \in 2E_2(\mathbb{Q}(\sqrt{17}))\backslash\{\mathcal{O}\}$$

noktası elde edilir.

2. Tip. Dik kenar uzunlukları rasyonel olan

$$(X, Y, Z) = (1, 4, \sqrt{17})$$

biçiminde bir dik üçgen vardır ve bu üçgene karşılık

$$Q = \left(\frac{17}{4},\ \pm\frac{15\sqrt{17}}{8}\right) \in 2E_2(\mathbb{Q}(\sqrt{17}))\backslash\{\mathcal{O}\}$$

dir.

3.Tip. $x, y, z \in \mathbb{Q}\backslash\{0\}$ olmak üzere $X = x - y\sqrt{17}$, $Y = x + y\sqrt{17}$ ve $Z = z$ olsun. Bu durumda (x, y) noktası $x^2 - 17y^2 = 4$ eşitliğini gerçekler. Örneğin, (13/2, 3/2) noktası bu eşitliğin bir çözümüdür. Yukarıdaki çözüm kullanılarak, $t \in \mathbb{Q}$ parametresine bağlı olarak tüm x ve y çözümleri

$$x = \frac{13-102t+221t^2}{2(-1+17t^2)},\ y = \frac{-3+26t-51t^2}{2(-1+17t^2)}$$

olarak elde edilir. $t = 1$ olması halinde x ve y değerleri $2x^2 + 34y^2$ ifadesinde yerine yazıldığında $2x^2 + 34y^2$ sayısının $\mathbb{Q}$ cisminde bir kare sayı olduğu görülür. Böylece,

$$(X, Y, Z) = \left(\frac{33+7\sqrt{17}}{8},\ \frac{33-7\sqrt{17}}{8},\ \frac{31}{4}\right)$$

biçimindeki dik üçgen ve

$$Q = \left(\frac{961}{64},\ \pm\frac{7161\sqrt{17}}{512}\right) \in 2E_2(\mathbb{Q}(\sqrt{17}))\backslash\{\mathcal{O}\}$$

noktası elde edilir.

4. Tip. Benzer şekilde 3.tip dik üçgen elde etme durumuna benzer şekilde

$$(X, Y, Z) = \left(\frac{-1+\sqrt{17}}{2},\ \frac{1+\sqrt{17}}{2},\ 3\right)$$

biçimindeki dik üçgen ve

$$Q = \left(\frac{9}{4},\ \pm\frac{3\sqrt{17}}{8}\right) \in 2E_2(\mathbb{Q}(\sqrt{17}))\backslash\{\mathcal{O}\}$$

noktası elde edilir.

$\mathbb{K} = \mathbb{Q}(\sqrt{17})$ olarak alınırsa $E_{34}(\mathbb{Q})$ grubunun rankının ikiden daha küçük olmadığı görülebilir. σ, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ grubunun üreteci ve $P \in E_2(\mathbb{K})$ olmak üzere $\varphi : E_2(\mathbb{K}) \longrightarrow E_2(\mathbb{Q})$, $\varphi(P) = P + \sigma(P)$ olarak tanımlanan φ homomorfizmini dikkate alalım. 2, $\mathbb{Q}$ üzerinde bir denk olmayan sayı olduğundan, $E_2(\mathbb{Q}) = E_2[2]$ dir. Alanı 2 olan dört tip dik üçgenin var olduğundan φ dönüşümü örtendir yani,

$$E_2(\mathbb{K})/\mathrm{Ker}(\varphi) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

dir.

Dikkat edilirse $\mathrm{Ker}(\varphi) \supset 2E_2(\mathbb{K})$ dır. $P_1, P_2 \in E_2(\mathbb{K})$ noktaları $2P_1 = (17/4, 15\sqrt{17}/8)$, $2P_2 = (961/64, 7161\sqrt{17}/512)$ olacak biçimde noktalar olsun. Bu durumda, Teorem 3.1.11. (1) in ispatı gereği $\varphi(P_1) = (0, 0)$, $\varphi(P_2) = (2, 0)$ dır. Böylece, $P_1, P_2 \notin 2E_2(\mathbb{K})$ ve $P_1 + P_2 \notin 2E_2(\mathbb{K})$ dır. $E_2(\mathbb{K})$ grubunun rankının 1 olduğu varsayılırsa, $P_1 + P_2 \in 2E_2(\mathbb{K})$ dır, ki bu bir çelişkidir. O halde Teorem 3.1.14. gereği $E_{34}(\mathbb{Q})$ grubunun rankının 1 den büyük olduğu sonucu elde edilir (gerçekte $E_{34}(\mathbb{Q})$ grubunun rankı 2 dir).

2. $N = 3$, $m = 7$ olmak üzere 1.tip ve Teorem 3.1.11. (1) de verilen 4.tip dik üçgen ve $2E_2(K)\backslash\{\mathcal{O}\}$ grubuna karşılık gelen noktalar elde edilebilir. Teorem 3.1.11. (2) gereği, 2.tip ve 3.tip dik üçgen elde edilemeyeceği açıktır (Tada 2001).

1. Tip. 21 (= 3·7) sayısı $\mathbb{Q}$ üzerinde bir denk sayıdır, dolayısıyla alanı 21 ve rasyonel kenar uzunlukları (7/2, 12, 25/12) olan bir dik üçgen vardır. Bu dik üçgenin tüm kenar uzunlukları $\sqrt{7}$ ile bölünerek

$$(X, Y, Z) = \left(\frac{\sqrt{7}}{2}, \frac{12\sqrt{7}}{7}, \frac{25\sqrt{7}}{14}\right)$$

biçimindeki 1.tip dik üçgen ve

$$Q = \left(\frac{4375}{784}, \pm\frac{13175\sqrt{7}}{3136}\right) \in 2E_3(\mathbb{Q}(\sqrt{7}))\backslash\{\mathcal{O}\}$$

noktası elde edilir.

4. Tip. Yukarıdaki Örnek 1'de 3.tip dik üçgen elde edilişine benzer şekilde

$$(X, Y, Z) = (-1 + \sqrt{7}, 1 + \sqrt{7}, 4)$$

dik üçgeni ve

$$Q = (4, \pm 2\sqrt{7}) \in 2E_3(\mathbb{Q}(\sqrt{7}))\backslash\{\mathcal{O}\}$$

noktası elde edilir.

3. $N = 2$, $m = 3$ olmak üzere Teorem 3.1.11 (1) de verilen 1.tip dik üçgen ve $2E_2(\mathbb{K})\backslash\{\mathcal{O}\}$ grubuna karşılık gelen nokta elde edilebilir. Teorem 3.1.11. (2) ve Teorem 3.1.11. (3) gereği, 2., 3. ve 4.tip dik üçgenlerin elde edilemeyeceği açıktır (Tada 2001).

1.Tip. 6 (= 2·3) sayısı $\mathbb{Q}$ üzerinde bir denk sayıdır, alanı 6 ve rasyonel kenar uzunlukları (3, 4, 5) olan bir dik üçgen vardır. Bu dik üçgenin kenar uzunlukları $\sqrt{3}$ ile bölündüğünde

$$(X, Y, Z) = \left(\sqrt{3},\ \frac{4\sqrt{3}}{3}, \frac{5\sqrt{3}}{3}\right)$$

biçiminde dik üçgen ve

$$Q = \left(\frac{25}{12},\ \pm\frac{35\sqrt{3}}{72}\right) \in 2E_2(\mathbb{Q}(\sqrt{3}))\backslash\{\mathcal{O}\}$$

elde edilir.

4. $N = 6$, $m = 5$ olmak üzere 6 sayısı $\mathbb{Q}$ üzerinde bir denk sayıdır. Alanı 6 ve rasyonel kenar uzunlukları (3, 4, 5) olan bir dik üçgen vardır. Üstelik 30 (= 6·5) sayısı da $\mathbb{Q}$ üzerinde bir denk sayıdır, alanı 30 ve rasyonel kenar uzunlukları (5, 12, 13) olan bir dik üçgen vardır. Bu dik üçgenin kenar uzunlukları $\sqrt{5}$ ile bölündüğünde

$$\left(\sqrt{5},\ \frac{12\sqrt{5}}{5},\ \frac{13\sqrt{5}}{5}\right)$$

dik üçgeni elde edilir. Teorem 3.1.13.'ün ispatındaki hesaplamalar ile alanı 6 olan

$$(X, Y, Z) = \left(\frac{33(13-5\sqrt{5})}{44},\ \frac{4(13+5\sqrt{5})}{11},\ \frac{7(85-13\sqrt{5})}{44}\right)$$

biçimindeki dik üçgen elde edilir (Tada 2001).

4. BİR MİLYON DOLARLIK PROBLEM

N sayısının bir denk sayı olup olmadığının belirlenmesi problemi E_N eğrisinin rankının pozitif olup olmadığının belirlenmesi problemine indirgendiğinden E_N eğrisinin rankının kolayca belirlenebileceği bir yol bulmak gerekir. Ne yazık ki, bir eliptik eğrinin rankının belirlenebilmesi sanıldığı kadar kolay bir problem değildir. Bunun için ilk olarak, E_N eğrisinin rankı ile eliptik eğrinin L-fonksiyonunun 1 noktasındaki değeri arasında nasıl bir ilişki olduğu ele alınacaktır.

4.1. Bir Milyon Dolarlık Problem

Hatırlanırsa, $p \nmid 2N$ özelliğindeki tüm p asalları için,

$$a_{E_N}(p) = p + 1 - \#\bar{E}_N(\mathbb{F}_p)$$

biçiminde tanımlanmıştı. E_N eğrisinin L-fonksiyonu ise s, gerçel kısmı uygun büyüklükte olan bir karmaşık sayı olmak üzere

$$L(s, E_N) = \prod_{p \nmid 2N}(1 - a_{E_N}(p)p^{-s} + p^{1-2s})^{-1}$$

biçiminde tanımlanır. Bu fonksiyon, karmaşık düzlemin tamamına analitik olarak devam ettirilebileceğinden, dolayısıyla fonksiyonun hangi fonksiyona yakınsadığı konusunda endişelenmeye gerek yoktur. L-fonksiyonuna olan ilgimiz, aşağıda verilecek olan, Birch ve Swinnerton-Dyer konjektüründen gelmektedir. Bu konjektür, Amerika'daki Clay Matematik Enstitüsü'nün Milenyum problemlerinden birisidir, yani enstitü bu konjektürü ispatlayabilecek ya da konjektürün aksini ispatlayabilecek olan herkese bir milyon dolar teklif etmektedir (konjektürün doğru olduğuna inanılmaktadır).

4.1.1. Birch ve Swinnerton-Dyer (BSD) Konjektürü. E_N eliptik eğrisi üzerinde sonsuz çoklukta rasyonel nokta olması için gerek ve yeter koşul $L(1, E_N) = 0$ olmasıdır (Birch ve Swinnerton-Dyer 1963, 1965).

Bu konjektür, daha sonra daha genel olarak ifade edileceği halde bu hali ile $s = 1$ noktasında L-fonksiyonu hakkında daha fazla bilgi vermektedir ve üstelik konjektürün

bu hali bizim için yeterlidir. Yukarıda verilen sonuçlar dikkate alındığında aşağıdaki önerme verilebilir.

4.1.2. Önerme (BSD konjektürü varsayımı altında). N tamsayısının bir denk sayı olması için gerek ve yeter koşul $L(1, E_N) = 0$ olmasıdır (Birch ve Swinnerton-Dyer 1963, 1965).

Bazı kaynaklarda yapılan çalışmalar dikkate alındığında E_N eliptik eğrisi için $r > 0$ olması halinde $L(1, E_N) = 0$ olduğu görülmektedir (gerçekte bu sonuç karmaşık çarpım özelliğine sahip olan herhangi eliptik eğri için de doğrudur). Bu ifadenin tersi, yani "$L(1, E_N) = 0$ ise $r > 0$ olduğu" hala açık bir problemdir. $L(1, E_N) = 0$ olması halinde problem kolay bir problem olmasa da $L(1, E_N) = 0$ olup olmadığı hakkında bir fikir elde etmek için en azından bazı sayısal yaklaşımlar yapılabilir.

Önceki bölümde olduğu gibi, $a_{E_N}(n)$ sayısının tanımı da asal olmayan tüm n değerlerini kapsayacak şekilde genişletilebilir. $p \nmid 2N$ ve $r \geq 2$ için

$$a_{E_N}(p^r) = a_{E_N}(p^{r-1})\, a_{E_N}(p) - p a_{E_N}(p^{r-2})$$

ve obeb(mn, $2N$) = 1 olmak üzere aralarında asal m ve n sayıları için

$$a_{E_N}(mn) = a_{E_N}(m) a_{E_N}(n)$$

dir.

Son eşitlik, $L(s, E_N)$ fonksiyonunun çarpım yerine,

$$L(s, E_N) = \sum_{\substack{n \geq 0 \\ obeb(n,2N)=1}} a_{E_N}(n) n^{-s}$$

biçiminde bir ile ifade edilebilmesine olanak verir. Böylece istenildiği kadar büyük $a_{E_N}(n)$ değerleri, daha küçük olanlar kullanılarak hesaplanabilir ve böylece sonuçta elde edilen sonlu toplam kullanılarak, $s = 1$ için $L(1, E_N)$ değeri için yaklaşık bir değer elde edilmiş olur. Bu hesaplamalar SAGE programı kullanılarak yapılabilir. Eliptik eğri E olarak tanımlanmak üzere q asal sayısı için $a_{E_N}(q)$ değeri

```
sage: E.ap(q)
```

komutu ile bulunur. Eğer 2 ve 100 arasındaki asal sayılar için, $a_{E_N}(q)$ değerlerinin bir listesi istenirse yukarıdaki komut yerine,

sage: for q in primes(2, 100):

print q, E.ap(q)

komutu kullanılır. $a_{E_N}(n)$'nin ilk 100 değeri için komut,

sage: E.anlist(100)

biçimindedir. Bu komutlar, $L(1, E_N)$ değerinin sonlu toplam yaklaşımlarını oluşturmak için kullanılabileceği gibi SAGE programında $L(1, E_N)$ değeri doğrudan

sage: E.Lseries(1)

biçimindeki komut ile de bulunabilir.

4.1.3. Örnek. 56 sayısı bir denk sayı mıdır? 56 sayısı bir denk sayı ise kenar uzunlukları rasyonel ve alanı 56 olan bir dik üçgen bulunuz. Eğer 56 sayısı bir denk sayı değil ise, bunu ispatlayınız (BSD konjektürünün doğru olduğu varsayılabilir).

Diophant-Pisagor yöntemi kullanılarak 56 sayısının bir denk sayı olduğunu gösterilebilir. Kenar uzunlukları $a, b, c \in \mathbb{Q}$ ve alanı 56 olan dik üçgeni göz önüne alalım. Bu durumda $\frac{ab}{2} = 56$ olduğundan

$$a^2 + b^2 = c^2 \text{ ve } ab = 112$$

dir. Şimdi

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \frac{c^2 - 224}{4} = \left(\frac{c}{2}\right)^2 - 56$$

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2 + 224}{4} = \left(\frac{c}{2}\right)^2 + 56$$

eşitliklerinde $x = \left(\frac{c}{2}\right)^2$ olarak alınırsa

$$x - 56 = \left(\frac{a-b}{2}\right)^2 \text{ ve } x + 56 = \left(\frac{a+b}{2}\right)^2$$

elde edilir. O halde problemin çözümü için aritmetik farkları 56 olan ardışık

$$x - 56, x, x + 56$$

sayılarının belirlenmesi gerekir. Dikkat edilirse bu sayıların her biri birer kare sayıdır, dolayısıyla bu sayıların çarpımı olan

$$(x - 56)\cdot x\cdot(x + 56) = x^3 - 3136x$$

sayısı da bir kare sayıdır. Dolayısıyla bu eşitlik

$$y^2 = x^3 - 3136x$$

biçiminde yazılabilir. Dikkat edilirse bu eşitlik bir eliptik eğri belirtir. Bu eşitliği gerçekleyen her bir rasyonel çözüme karşılık, istenen özellikte bir dik üçgen elde edilemeyeceği açıktır. Bu nedenle bir rasyonel çözümden başlanarak bu eğri üzerindeki yeni noktalar elde edilerek istenilen uzunluklara sahip olan dik üçgen elde edilir. Yukarıdaki eşitliklerden

$$x = \left(\frac{c}{2}\right)^2,$$

$$y = \sqrt{(x - 56)\cdot x\cdot(x + 56)} = \frac{(a-b)\cdot c\cdot(a+b)}{8} = \frac{(a^2-b^2)\cdot c}{8}$$

olarak elde edilir. $(-56, 0)$, $(0, 0)$, $(56, 0)$ noktaları eliptik eğri üzerindeki aşikar noktalardır fakat bu noktalar ile bir dik üçgen elde edilemez. $(-7, 147)$ noktası da eliptik eğri üzerindeki bir noktadır ve bu durumda $(-7, 147)$ noktası ve yukarıdaki aşikar noktalar ile eliptik eğri üzerinde yeni noktalar elde etmek mümkün değildir. Bu nedenle, bu nokta ve kendisinden geçen, yani bu noktada eğriye teğet olan doğruyu dikkate alalım.

$$2yy' = 3x^2 - 3136$$

olduğundan

$$y' = \left.\frac{3x^2 - 3136}{2y}\right|_{(-7,147)} = -\frac{2989}{294}$$

ve dolayısıyla eliptik eğrinin $(-7, 147)$ noktasından geçen teğetinin denklemi

$$y = -\frac{2989}{294}x + \frac{22295}{294}$$

olarak bulunur. Bu doğru ile eliptik eğrinin kesişimi dikkate alınırsa

$$\left(-\frac{2989}{294}x + \frac{22295}{294}\right)^2 = x^3 - 3136x$$

ve dolayısıyla

$$x^3 - \frac{8934121}{86436}x^2 + \cdots = 0$$

eşitliği elde edilir. Doğru eliptik eğriye $(-7, 147)$ noktasında teğet olduğundan $x = -7$ noktası son eşitliğin çift katlı köküdür. Son eşitliğin köklerinin toplamının $\frac{8934121}{86436}$ olduğu hatırlanırsa

$$(-7) + (-7) + x = \frac{8934121}{86436}$$

eşitliği ve bu eşitlikten de $x = \frac{10144225}{86436} = \left(\frac{3185}{294}\right)^2$ olarak bulunur. Bu değer teğet doğru denkleminde yerine yazılırsa $y = -\frac{28393997905}{25412184}$ olarak bulunur. $x = \left(\frac{c}{2}\right)^2$ olduğundan $c = \frac{6370}{294}$ ve dolayısıyla

$$-\frac{28393997905}{25412184} = y = \frac{(a^2 - b^2)\cdot c}{8} = \frac{6370(a^2 - b^2)}{2352}$$

dir. Bu eşitlikten de

$$a^2 - b^2 = -\frac{35659652}{86436}$$

olarak bulunur. Diğer yandan $a^2 + b^2 = c^2 = \left(\frac{6370}{294}\right)^2$ olduğundan $a^2 = \frac{614656}{21609}$, $b^2 = 441$ ve böylece alanı 56 olan dik üçgenin kenar uzunlukları

$$a = \frac{16}{3},\ b = 21 \text{ ve } c = \frac{65}{3}$$

olarak bulunur. Dikkat edilirse bu üçgen (16, 63, 65) üçgeninin her bir kenarının 3 ile bölünmesiyle elde edilmiş olan üçgendir. Bundan başka bu yöntem kullanılarak $y^2 = x^3 - 3136x$ eliptik eğrisi üzerinde sonsuz çoklukta çözüm bulunabilir.

Eliptik eğrileri kullanmadan, verilen N sayısının bir denk sayı olup olmadığını belirleyebilmek için bir yöntem belirlemek, bir kritere sahip olmak istiyoruz. BSD konjektürünün geçerli olduğunu varsayarak, Tunnell (Tunnell 1983), N sayısının bir denk sayı olup olmadığını belirleme problemini sonlu kümelerin mertebelerini karşılaştırma problemine dönüştürmüştür. Bu teoremde, bu çalışmada yer almayacak olan modüler formları kullanılmaktadır. Nispeten küçük ve sonlu kümeler olmaları

nedeniyle eliptik eğriler ile hesaplama yapmanın çok fazla zaman aldığı durumlarda bu kümelerin mertebelerinin hesaplanması oldukça akıllıcadır.

4.1.4. Teorem. *N*, karesiz, tek (veya çift) sayı ve bir rasyonel dik üçgenin alanı ise,

$$\#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + 2y^2 + 32z^2\} = \frac{1}{2}\#\{ x, y, z \in \mathbb{Z} \mid N = 2x^2 + 2y^2 + 8z^2\}$$

$$(\text{veya } \#\{x, y, z \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{ x, y, z \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 8z^2\})$$

dir (Tunnell 1983).

Eğer BSD konjektürü E_N eliptik eğrisi için doğru ise, bu durumda bu eşitlik *N* sayısının bir denk sayı olmasını gerektirir.

BSD konjektürünün doğru olduğu varsayılarak 2006 ve 2007 sayılarının da birer denk sayı oldukları belirlenebilir.

Böylece denk sayılar hakkındaki tartışmadaki döngü tamamlanmış oldu. Kenar uzunlukları rasyonel olan üçgenlerin alanları hakkındaki masum bir problemle başladıktan sonra eliptik eğrilerin, bu problemdeki yerini görmüş olduk. Daha sonra bir milyon dolarlık konjektürün aslında denk sayıların incelenmesinde ortaya çıktığını ve eğer bu milyon dolarlık konjektür doğru ise bir sayının denk sayı olup olmadığını belirlenmesi probleminin, sonlu bir kümenin kardinalitesinin belirlenmesine indirgendiği sonucunu elde etmiş olduk.

KAYNAKLAR

Birch, B., Swinnerton-Dyer, P. 1963. Notes on elliptic curves I and II. *J. Reine Angew. Math.*, 212: 7–25.

Birch, B., Swinnerton-Dyer, P. 1965. Notes on elliptic curves I and II. *J. Reine Angew. Math.*, 218: 79–108.

Brown, J. 2003. Congruent Numbers and Elliptic Curves. Second Edition, University of Princeton, U.S.A, 184 pp.

Chahal, J. S. 1984. On a identity of Desboves. *Proc. Japan Acad.*, 60: 105-108.

Chahal, J. S. 2006. Congruent numbers and elliptic curves. *American Mathematical Monthly*, 113: 308-317.

Coates, J. H. 2012. Congruent numbers. *Proc. Natl. Acad. Sci.*, 109: 21182–21183.

Coates, J., Wiles, A. 1977. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39: 223-251.

Desboves, A. 1879. Sur l'emploi des identités algébriques dans la résolution, en nombres entiers, des équations d'un degré supérieur au second. *C. R. Acad. Sci*., 87: 159–161.

Dickson, L. E. 1920. History of the theory of numbers, Vol. 2, Carnegie Institution of Washington, Washington, 462 pp.

Girondo, E., González-Diez, G., González-Jiménez, E., Steuding, R., Steuding, J. 2009. Right Triangles with algebraic sides and Elliptic Curves over Number Fields**.** *Mathematica Slovaca*., 3: 299-306**.**

Heegner, K. 1952. Diophantische analysis und modulfunktionen. *Math. Z.*, 56: 227–253.

Koblitz, N. 1993. Introduction to Elliptic Curves and Modular Forms. Second Edition, Springer-Verlag, New York Berlin Heidelberg, Tokyo, U.S.A, 248 pp.

Kwon, S. 1997. Torsion subgroups of elliptic curves over quadratic extensions. *Journal of Number Theory*., 62: 144 –162.

Mazur, B. 1977. Modular curves and the Eisenstein ideal. *IHES Publ. Math*., 47: 33-186.

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

Mordell, L. 1922. On the rational solutions of the indeterminate equations of the third and fourth degree. *Math. Proc. Camb. Phil. Soc.*, 21: 179–192.

Nemenzo, F. R. 1998. All congruent numbers less than 40000. *Proc. Japan. Ser. A Math. Sci.*, 74: 29-31.

Silverman, J. H., Tate, J. T. 1992. Rational Points on Elliptic Curves. Second Edition, Springer Verlag, New York, 332 pp.

Tada, M. 2001. Congruent number over real quadratic fields. *Hiroshima Math. J.*, 31: 331-343.

Tian, Y. 2012. Congruent numbers with many prime factors. *Proc. Natl. Acad. Sci.*, 109: 21256–21258.

Tunnell, J. B. 1983. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math*., 72: 323-334.

Washington, L. C. 2008. Elliptic Curves Number Theory and Cryptography. Second Edition, University of Maryland College Park, Mayland, U.S.A., 513 pp.

Wiles, A. 1995. Modular elliptic curves and Fermat's last theorem. *Ann Math*., 141: 443-551.

Zagier, D. 1987. Large integral points on elliptic curves. *Math. Comput*.,48: 425– 436.

ÖZGEÇMİŞ

Adı Soyadı	: Nagihan KURNAZ
Doğum Yeri ve Tarihi	: Osmangazi/BURSA, 20/10/1992
Yabancı Dili	: İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise	: Bursa Hürriyet Anadolu Lisesi, 2006-2010
Lisans	: Uludağ Üniversitesi, 2010-2014
Yüksek Lisans	: Uludağ Üniversitesi, 2014-2017

İletişim (e–posta) : nkurnaz99@gmail.com