T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FERMAT'IN SON TEOREMİNİN UYGULAMA ALANLARI

Musa DEMİRCİ

YÖK TÜRKİYE YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

128481

BURSA 2002

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FERMAT'IN SON TEOREMİNİN UYGULAMA ALANLARI

MUSA DEMİRCİ

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Bu Tez 22.07.2002 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Doç.Dr.İsmail Naci CANGÜL (Danışman)

Doç.Dr.Cengizhan MURATHAN

Yrd.Doç.Dr.İlhan TAPAN

ÖZET

Bu çalışmada Fermat'nın son teoremi ele alınmış ve n = 3, 4, 5 ve 7 özel durumlarında yapılan ispatlar bir araya getirilmiştir. n = 2 durumunda elde edilen Pisagor üçlülerinin bulunuşu ve sayıları ile ilgili yeni sonuçlar elde edilmiştir ve bu sonuçların literatürdeki sonuçlarla karşılaştırılması yapılmıştır.

Anahtar Kelimeler: Fermat'nın son teoremi, Pisagor üçlüleri, Pisagor teoremi

APPLICATIONS OF THE FERMAT'S LAST THEOREM

ABSTRACT

In this work, Fermat's last theorem is considered, and the proofs of the special cases n = 3, 4, 5 and 7 are given. Some results related to the obtaining methods and the total number of Pythagorian triples at the case of n = 2 are obtained and these results are compared with the ones in the literature.

Key Words: Fermat's last theorem, Pythagorian triple, Pythagoras theorem

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
İÇİNDEKİLER iii
TABLOLAR DİZİNİ iv
GİRİŞ v

1. ÖN BİLGİLER
1.1. Pisagor Üçlüleri 1
1.2. Fermat'ın Sonsuz İndirgeme Metodu 19
1.3. Fermat'ın Son Teoremi'nin Tarihsel Gelişimi 20

2. FERMAT'IN SON TEOREMİ'NİN ÖZEL HALLERİ
2.1. n = 4 hali 24
2.2. n = 3 hali 25
2.3. n = 5 ve n = 7 halleri 37

3. FERMAT'IN DİĞER SAYI TEORİK BULUŞLARI 39

Tartışma ve Sonuç 40
Kaynaklar 42
Teşekkür 44
Özgeçmiş 45

TABLOLAR DİZİNİ

Sayfa

Tablo 1.1 5
Tablo 1.2 15

GİRİŞ

$$x^2 + y^2 = z^2$$

denkleminin aşikar olmayan (x, y, z) tamsayı çözümlerine Pisagor üçlüleri denilir. Bu çalışmada öncelikle bu üçlüler ile ilgili bazı problemler ele alınmıştır. Üssün ikiden büyük bir tamsayı olması durumunda Fermat'nın

$$x^n + y^n = z^n$$

denkleminin aşikar olmayan tamsayı çözümlerinin olmadığı yönündeki iddiası 350 yılı aşkın bir süre bir çok matematikçiyi meşgul etmiştir. 1994 de Andrew Wiles birkaç matematikçinin bulduğu yeni sonuçlardan da faydalanarak bu iddianın doğruluğunu ispatlamıştır.

İspatın düzenlenmiş son hali Annals of Mathematics' de 1995 te yayınlanmıştır ve 109 sayfadır, (Wiles, 1995).

Bu çalışma üç bölümden oluşmaktadır. İlk bölümde Pisagor üçlüleri ile ilgili hatırlatmalar yapıldıktan sonra bu üçlüler ile ilgili birkaç problem ele alınmıştır. Daha sonra Fermat'nın Son Teoremi'nin bir çok özel halinin ispatında kullanılan sonsuz indirgeme metodundan bahsedilmiştir. Bu bölümde son olarak Fermat'nın Son Teoremi'nin ispatında kullanılan bazı temel bilgilerden ve tarihsel gelişimden bahsedilmiştir.

İkinci bölümde Fermat'nın Son Teoremi'nin sırasıyla $n = 4$, $n = 3$, $n = 5$ ve $n = 7$ özel hallerindeki ispatıyla ilgili bilgiler verilmiştir.

Üçüncü ve son bölümde ise Fermat'nın Sayılar Teorisi alanında yapmış olduğu diğer çalışmalardan bahsedilmiştir. Bu çalışmaların son teoremin ortaya çıkışıyla ilişkisi ortaya konulmaya çalışılmıştır.

1. ÖN BİLGİLER

Bu bölümde Pisagor teoremini sağlayan tamsayı üçlülerine Pisagor üçlüleri adı verilerek bu üçlülerin bulunuşu ve bazı özellikleri ile ilgili sonuçlar derlenmiştir. Verilen bir pozitif tamsayıyı kenar uzunluğu kabul eden dik üçgenlerin sayısını ve bu dik üçgenlerin diğer kenar uzunluklarını elde etmemize yarayan orjinal sonuçlar elde edilmiştir. Konu ile ilgili temel kavramlar sayılar teorisi kitaplarında bulunabilir.

1.1. Pisagor Üçlüleri

Pisagor üçgeni olarak adlandırılan, kenar uzunlukları tamsayılar olan dik üçgenler Fermat'nın Diophant'ın "Arithmetic" adlı kitabından faydalanarak ortaya koyduğu teorinin $n = 2$ halidir. Yani

$$x^2 + y^2 = z^2$$

durumudur. Bu eşitlik sonsuz çoklukta x, y, z pozitif tamsayı üçlüsü için sağlanır. Daha doğru bir ifade ile Diophant'ın iki tam karenin toplamını başka bir tam kare şeklinde yazabilme probleminin geometrik karşılığı Pisagor üçgenleridir. Bu nedenle Diophant'ın problemini çözmek Pisagor üçgenleri bulmakla özdeştir.

1.1.1. Tanım. Bir Pisagor üçgeninin kenar uzunluklarını oluşturan sayılara, yani $x^2 + y^2 = z^2$ denkleminin (x, y, z) pozitif tamsayı çözümlerine Pisagor üçlüleri denir. x, y, z sayıları aralarında asalsa (x, y, z) üçlüsüne ilkel Pisagor üçlüsü adı verilir.

1.1.2. Tanım. x ve y sayılarından biri tek diğeri çift ise bu sayılara zıt halli sayılar diyeceğiz.

$x^2 + y^2 = z^2$ denklemi her ne kadar Pisagor teoremi olarak bilinse de yapılan araştırmalar bu türde üçlülerin Pisagor'dan çok önceleri Babilliler tarafından da bilindiğini gösteriyor.

$$x^2 + y^2 = z^2$$

denkleminin çözüm metodu eski Yunanlı matematikçiler tarafından bilinen analitik metoddur. Bu metoda göre $x^2 + y^2 = z^2$ denklemini sağlayan bir çözüm verilir ve verilmiş olan çözümün özellikleri bu x, y, z pozitif tamsayıları kullanılarak başka çözümlerin karakterini bulmak için analiz edilir.

İlk olarak d sayısı x, y ve z sayılarını bölüyorsa bu taktirde $x^2 + y^2 = z^2$ denkleminden d^2 sadeleştirilebilir ve $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ tamsayıları da bir Pisagor üçlüsü olur. Eğer d x, y, z nin ortak bölenlerinin en büyüğü ise bu taktirde $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ nin ortak böleni sadece 1 dir ve $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ sayıları da ilkel Pisagor üçlüleridir. Bu yolla her Pisagor üçlüsü en büyük ortak bölen ile bölünerek ilkel Pisagor üçlülerine dönüştürülebilir. Tersine $a^2 + b^2 = c^2$ olacak şekilde bir (a, b, c) ilkel Pisagor üçlüsü verildiğinde her biri aynı sayıyla çarpılarak başka bir Pisagor üçlüsü elde edilebilir. Yani $x = ad$, $y = bd$, $z = cd$ şeklinde başka bir (x, y, z) Pisagor üçlüsü bulunabilir. Buna göre ilkel Pisagor üçgenleri elde etmek için bu indirgeme metodunu kullanmak yeterlidir. Bu nedenle Pisagor üçgenleri ile çalışırken verilen x, y, z Pisagor üçlüsünü ilkel kabul etmek genelliği bozmaz.

Bu tartışma x, y, z sayılarının herhangi ikisinin ortak bir bölene sahip olmadığını belirtir. Örneğin d x ve y nin bir ortak böleni olsaydı bu taktirde

$$x^2 + y^2 = z^2$$

den dolayı d^2 z^2 yi ve böylece d z yi bölerdi. Buna göre d her üçünü de böler ve üçlü ilkel olduğundan d 1 olmalıdır. Aynı şekilde x ve z nin ya da y ve z nin tek ortak böleni de 1 dir.

Özel olarak, x, y, z nin herhangi ikisi çift olamaz. Bu nedenle en az ikisi tektir. Ancak üçünün tek olamayacağı da aşikardır çünkü iki tek sayının toplamı yine tek oluyor demektir ki bu imkansızdır. Dolayısıyla tam olarak bu üç sayıdan biri çifttir. 4 modu dikkate alınarak z nin çift olamayacağı aşağıdaki gibi gösterilebilir. $2n + 1$ tek sayısının karesi, yani $4n^2 + 4n + 1$, 4 ün bir katından 1 fazladır. $2n$ çift sayısının karesi olan $4n^2$ ise 4 ün bir katıdır. Böylece eğer x, y tek ve z çift olsaydı, bu taktirde her biri 4 ün katından bir fazla olan iki sayının toplamı 4 ün bir katına eşit olurdu ki bu imkansızdır. Bundan dolayı z tek ve x ve y zıt hallidir. Yani biri tek

diğeri ise çifttir. Gerekirse x ve y nin değiştirilmesiyle verilen ilkel Pisagor üçlüsünde y ve z tek alındığında x çift olacaktır.

Şimdi $x^2 + y^2 = z^2$ denklemini $x^2 = z^2 - y^2$ formunda tekrar yazalım ve denklemin sağ tarafını

$$x^2 = (z + y)(z - y)$$

şeklinde yazalım. x, z +y ve z – y sayıları çift olduğundan

$$x = 2u$$

$$z + y = 2v$$

$$z - y = 2w$$

olacak şekilde u, v, w pozitif tamsayıları vardır. Ayrıca

$$(2u)^2 = (2v)\,(2w)$$

ya da $u^2 = vw$ dir. Dahası v ve w nun en büyük ortak böleni 1 dir. Aksi halde v ve w yu bölen herhangi bir sayı

$$v + w = \frac{1}{2}(z + y) + \frac{1}{2}(z - y) = z$$

toplamını ve

$$v - w = \frac{1}{2}(z + y) - \frac{1}{2}(z - y) = y$$

farkını da bölerdi ki bu, y ve z sayılarının aralarında asal oluşları ile çelişir. Sonuç olarak v ve w aralarında asaldır.

Tartışmadaki esas adım aşağıdaki gibidir. Aralarında asal v ve w şeklindeki iki sayının çarpımının $vw = u^2$ tam karesine eşit olabilmesi için tek yol v ve w nun kendilerinin de tam kare olmasıdır. Eğer v ve w sayılarının asal çarpanlarına ayrışımı düşünülürse, bunlar aralarında asal olduklarından v ve w nun ayrışımında hiçbir asal çarpanın ortak olmadığı açıkça görülür. Böylece vw nun asal ayrışımı sadece yan yana iki asal çarpımdan oluşur ($vw = p_1 . p_2 . \ldots . p_n . q_1 . q_2 . \ldots . q_r$ ve $(p_i, q_j) = 1$). Eğer vw bir tam kare ise bu taktirde vw nun ayrışımındaki tüm çarpanlar çift kuvvete sahip olmalıdır. Ancak yukarıdaki incelemeden faydalanılarak v ve w nun ayrışımındaki tüm asalların çift kuvvete sahip olduğu elde edilir ve dolayısıyla v ve w birer tam karedir. Bundan dolayı $v = m^2$, $w = n^2$ olacak şekilde m, n pozitif tamsayıları vardır ve v ile w aralarında asal olduğundan m ve n aralarında asaldır. Böylece

$$z = v + w = m^2 + n^2$$

$$y = v - w = m^2 - n^2$$

dir. Bu, m nin n den daha büyük ve m ile n nin zıt halli olmalarının gerektiğini gösterir (çünkü z ve y tek sayıdır). Bununla birlikte x, m ve n cinsinden

$$x^2 = z^2 - y^2 = m^4 + 2m^2n^2 + n^4 - m^4 + 2m^2n^2 - n^4$$
$$= 4m^2n^2$$

biçiminde yazılabilir ve buradan da

$$x = 2mn$$

olarak bulunur. Yani verilmiş herhangi bir ilkel Pisagor üçgeninde aralarında asal, $m > n$ olacak şekilde, zıt halli ve

$$y = m^2 - n^2$$
$$x = 2mn \qquad (1)$$
$$z = m^2 + n^2$$

eşitliklerini sağlayan m ve n pozitif tamsayıları vardır. Bu durumda

$$x^2 + y^2 = z^2$$

olup

1) m ve n aralarında asal
2) $m > n$
3) m, n zıt halli

olduğundan x, y, z bir ilkel Pisagor üçlüsüdür.

$$x^2 + y^2 = z^2 \quad \text{yani} \quad (2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

ifadesi her m, n değeri için doğru olan bir cebirsel özdeşliktir ve m, n üzerindeki şartlar incelendiğinde 2mn ve $m^2 - n^2$ nin aralarında asal olduğu bulunur.

Bu işlem Pisagor üçlüleri oluşturma problemini tümüyle çözer. $m \leq 8$ iken m, n çiftlerine uygun Pisagor üçlüleri aşağıda Tablo 1.1 de gösterilmiştir.

Bir dik üçgende iki dik kenarın karelerinin toplamının hipotenüsün karesine eşit olduğunu ifade eden Pisagor teoreminin en basit örneği olan $3^2 + 4^2 = 5^2$ eşitliğini herkes bilir. Ancak aynı ifadeyi sağlamasına karşın 5, 12 ve 13 sayılarıyla oluşan $5^2 + 12^2 = 13^2$ ifadesini daha az kişi bilir. Dahası bahsedilen bu iki Pisagor üçgeninin dışında bir üçüncüsünü örneğin (7, 24, 25) Pisagor üçlüsünü ise çok daha az insan bilebilir.

EC YÜKSEKÖĞRETİM KURULU DOKÜMANTASYON MERKEZİ

Tablo 1.1 İlkel Pisagor üçlüleri

m	n	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85
8	1	16	63	65
8	3	48	55	73
8	5	80	39	89
8	7	112	15	113

Tamsayı kenarlı dik üçgenler çok eğlenceli problemlerde kullanılabilir. Karelerinin toplamı bir tam kare olacak iki tamsayı bulma problemi bunlardan sadece biridir. 1 ve 2 nin karelerinin dışında her zaman böyle en az bir tam kare bulmak mümkündür. Dikkat edilirse bu düşünce hipotenüs için doğru değildir. Dik üçgende bir sayının hipotenüs olabilmesi için belli bir yapıda olması gerekir.

Yukarıdaki m ve n tamsayıları gelişigüzel bir şekilde seçilebilir. Bu m ve n sayılarına bazen üreteç sayılar denir. Eğer m ve n tamsayıları ardışık sayılar alınırsa bu taktirde y dik kenarı x den daha büyük olur ve y ile z (hipotenüs) ardışık tam sayılar olurlar. m ve n sayıları ardışık sayılar olarak alındığında bunlardan elde edilen dik kenar uzunlukları olan x ve y yi üreteç kabul eden yeni dik üçgenlerde hipotenüs bir tam karedir. Bir Pisagor üçgeninde yalnızca bir kenar uzunluğu tam kare olabilir.

Eğer üreteç sayılar olarak 1 den başlayarak ardışık tam sayıların toplamı olan 1, 3, 6, 10, 15 gibi üçgensel sayılar alınırsa bu taktirde x dik kenarı bir tam küp olur. Buna benzer başka bağıntılar da üretilebilir.

(1) formülünü daha detaylı inceleyelim. Eğer x, y ve z den herhangi ikisinin bir ortak çarpanı varsa bunların çarpımı da, bu sayıların kuvvetlerinin toplamı ve farkında olduğu gibi, bu ortak çarpana sahip olacaktır. Bu şartlar formüle uygulanırsa m ve n nin ortak bir çarpana sahip olması durumunda x, y ve z kenarlarının bu çarpanı bulundurması gerektiği görülür. Dahası, eğer m ve n çift ya da tek ise x, y ve z en azından 2 çarpanına sahiptir. x, y ve z sayılarının bir ortak çarpana sahip olmaması istersek m ve n den biri çift, diğeri tek ve ayrıca ortak çarpana sahip olmayacak şekilde seçeriz. Bu kısıtlamalar ile elde edilen dik üçgenlere ilkel üçgenler demiştik. İlkel olmayan herhangi bir dik üçgen bir ilkel dik üçgendeki kenarların sırasıyla istenilen bir tam sayı ile çarpılmasından bulunabileceğinden yalnızca ilkel dik üçgenleri bulmak için formüle ihtiyaç duyulur. (1) formülü tüm Pisagor üçgenlerini kapsayacak şekilde

$$x = K(m^2 - n^2)$$
$$y = K(2mn) \qquad (1A)$$
$$z = K(m^2 + n^2)$$

olarak yazılmalıdır. K çarpanı olmadan da (1) formülünden ilkel olmayan dik üçgenler elde edilebilir, örneğin (9, 12, 15) Pisagor üçlüsü. Ancak bu üçgen (1A) formülünde $K = 3$, $m = 2$ ve $n = 1$ yazılarak bulunabilir.

(1) formülü dik kenarlarının en büyük ortak böleni bir tam kare, ya da bir tam karenin iki katı olan, ilkel olmayan dik üçgenler dışındaki tüm ilkel dik üçgenleri verir. Formül, özellikle dik kenarlarının ortak çarpanı sadece 2 olan ilkel olmayan dik üçgenleri verir. Kenarların ortak çarpanı bir tam karenin iki katı olduğunda uygun bir dönüşüm yapılır. Bu taktirde (1A) formülü: (1) formülüne benzer bir hale getirilir. Ortak çarpan bir tam kare olduğunda bir dönüşüme gerek kalmaz.

Bir ilkel Pisagor üçgenini oluşturan sayı üçlülerine (kenar uzunluklarına) dikkat edilirse kenarlardan biri daima 3 ile ya da 5 ile bölünür ve dik kenarların çarpımı 12 ile bölünür ve dahası üç kenarın uzunluklarının çarpımı daima 60 ile bölünür.

Bir tam sayı verildiğinde toplamları bir tam kare olacak şekilde ikinci bir tam sayı bulmak verilen tam sayının tek ya da çift oluşuna bağlıdır.

1) Verilen A sayısı tek olduğunda :

A iki sayının çarpımı olarak yazılır (A asal ise bu çarpanlar 1 ve kendisi olur.). Büyük çarpan $m+n$ ye küçüğü $m-n$ ye eşitlenir ve bu lineer denklemlerdeki m ve n bulunur ve x, y ve z yi elde etmek için formülde yerine yazılır. İlkel çözümler istenirse bu iki çarpan aralarında asal seçilmelidir.

Örnek olarak $A = 35$ alalım. $m + n = 7$, $m - n = 5$ olup $m = 6$, $n = 1$ bulunur ki bu değerlerden (35, 12, 37) ilkel Pisagor üçlüsü elde edilir. Eğer $m + n = 35$, $m - n = 1$ seçilirse $m = 18$, $n = 17$ olur ki bu da (35, 612, 613) ilkel Pisagor üçlüsünü verir. Verilen bir A tam sayısına karşılık kaç tane Pisagor üçlüsü elde edileceğini verilen sayının çift olması durumundan sonra göreceğiz.

2) Verilen A sayısı çift olduğunda :

A sayısı $2mn$ ye eşitlenir ve m ve n nin çarpımları tam sayılar olmalıdır. İlkel çözümler istenirse A sayısı 4 ile bölünebilmeli aynı zamanda m ve n aralarında asal ve zıt halli olmalıdır. Eğer A 4 ile bölünmüyorsa ilkel bir çözüm bulmak imkansızdır.

Örnek olarak $A = 12$ alalım. Bu taktirde $mn = 6$ olur eğer $m = 6$, $n = 1$ seçilirse (12, 35, 37) Pisagor üçlüsü elde edilir. Ancak $m = 3$, $n = 2$ alınırsa (5, 12, 13) Pisagor üçlüsü bulunur.

Ayrıca Pisagor üçgenleri ile ilgili aşağıdaki türde problemler de mevcuttur. Alanları oranı verilen, çevresi bir tam kare olan, alanı ile çevresi toplamı bir tam küp olan, alanı hipotenüsüne eşit olan, hipotenüsünün karesi alanına eklendiğinde bir tam kare olan ve çevresi verilen bir sayıya eşit olan Pisagor üçlülerinin varlığı gibi. Böyle problemleri ortaya koyma süreci boyunca Pisagor üçgeninin alanının tam kare olması gibi bazı basit şartlar eklenmesi de doğaldı. Bir çok matematikçi bunun imkansızlığını gösteremedi. Fermat ise $mn(m^2 - n^2)$ ifadesinin bir tam kare olamayacağını ispatladı. Bunun gibi, bazı Diophant denklemleri ile biraz ilgilenen ancak bu alan problemi ile daha önce hiç karşılaşmamış biri er ya da geç biraz ustaca bir hamle ile çözülebileceği düşüncesiyle bunu ispatlamaya çalışabilir.

Tekrar verilen bir A sayısının kaç Pisagor üçgeninde dik kenar ya da hipotenüs olabileceği problemini ele alalım. p ve q tek asal sayılar iken p^3q şeklindeki ya da p bir tek asal sayı iken $16p$ şeklindeki bir sayı tam 10 tane Pisagor üçgeninde kenar olabilir. Böylece $135 = 3^3.5$ ya da $80 = 16.5$ sayıları 10 Pisagor üçgeninde kenar olur.

10 dik üçgende kenar olma durumuna bakılırsa $48 = 16p$ in bunu sağladığı görülür. Ancak 48 sadece 3 tek asal çarpanını bulundurduğundan ve 3, $4x + 1$ formunda olmadığından 48 hiçbir Pisagor üçgeninde hipotenüs olamaz. Bununla birlikte $80 = 16.5$ olup 5, $4x + 1$ formunda olduğundan 80 sadece bir tane Pisagor üçgeninde hipotenüs olur.

Bir A sayısı verildiğinde A yi kenar uzunluğu kabul eden Pisagor üçlülerinin sayısını T ile gösterelim. Genelde A sayısı bir dik kenarı göstermekle birlikte bazen hipotenüsü de gösterebilir. Bütün pozitif tamsayılar hipotenüs olamaz, ancak $4x + 1$ formunda en az bir asal çarpana sahip sayılar hipotenüs olabilir. A sayısını dik kenar kabul eden Pisagor üçgenlerinin sayısının L ile, hipotenüs kabul edilenlerin sayısı ise H ile gösterirsek $T = L + H$ dır. Örneğin tam iki Pisagor üçgeninde kenar olabilen en küçük sayı 5 tir. Yani 5 için $T = 2$ olup 5 bu üçgenlerin birinde dik kenar diğerinde ise hipotenüstür. $T = 29$ için 975 sayısı 22 dik üçgende kenar, 7 dik üçgende hipotenüs olur. 29 üçgende sadece dik kenar olabilen en küçük sayı $2^{30} = 1073741824$ dir.

Örnek olarak 60 sayısı verilsin ve biz bu sayının kaç ilkel Pisagor üçgeninde kenar olabileceğini bulalım. 60' ı asal çarpanlarının çarpımı şeklinde yazarsak $60 = 2^2.3.5$ şeklinde 3 asalın çarpımıdır. Buna göre 60 $2^{3-1} = 4$ tane üçgende kenar olabilir.Yine 5040 sayısı için $5040 = 2^4.3^2.5.7$ olup 4 asalın çarpımı olduğundan $2^{4-1} = 8$ tane dik üçgende kenar olabilir. Genel olarak eğer bir sayı n tane asalı ya da kuvvetlerini bulunduruyorsa bu taktirde 2^{n-1} tane ilkel Pisagor üçgeninin kenarı olabilir. Eğer verilen sayı çift ancak 4 ile bölünmüyorsa hiçbir ilkel Pisagor üçgeninde kenar olamaz. Örneğin $30 = 2.3.5$ olup 4' e bölünmez ayrıca $4x + 2$ şeklindeki sayılar da ilkel Pisagor üçgenlerinde kenar olamaz.

Verilen bir A sayısının kaç tane Pisagor üçgeninde kenar olabileceğini ya da verilen bir pozitif tamsayıyı dik kenar uzunluğu kabul eden ve diğer kenarları da tamsayılar olan dik üçgenlerin sayısını bulmak için oldukça farklı bir formül kullanılır. Bu formül verilmiş olan dik kenar uzunluğunun bir asal sayı, tek sayı ve bir çift sayı oluşuna bağlı olarak aşağıdaki gibi uygulanır.

1.1.1. Teorem. $x > 2$ bir asal sayı olsun. Bir dik kenarı x olan bir tek Pisagor üçgeni vardır ve bu üçgenin diğer dik kenarı $y = (x^2 - 1)/2$, hipotenüs uzunluğu ise $z = (x^2 + 1)/2$ dir.

İspat : Pisagor bağıntısı gereği $x^2 = z^2 - y^2$ yazılabilir. O halde

$$x^2 = (z - y)(z + y)$$

yazabiliriz. $x > 2$ asal olduğundan x^2 sayısını bölen çarpanlar 1, x ve x^2 dir ve hepsi birer tek sayıdır. Burada iki durum söz konusudur. Ya $x^2 = x^2.1$ ya da $x^2 = x.x$ dir. İkinci durumda

$$z - y = x$$

$$z + y = x$$

denklemlerinden $y = 0$ elde edilir ki bu imkansızdır. Yani sadece bir Pisagor üçgeninin varlığı mümkündür. Bu da

$$z - y = 1$$

$$z + y = x^2$$

denklemlerinden elde edilen $z = (x^2 + 1)/2$ ve $y = (x^2 - 1)/2$ kenarlarına sahip olan üçgendir.

1.1.2. Teorem. Yukarıdaki notasyona göre bir dik kenarı, verilen bir x tek sayısı olan $(w - 1)/2$ tane Pisagor üçgeni vardır.

İspat : x herhangi bir tek sayı olsun. x^2 nin çarpanlarının tümü tektir.

$$x^2 = (z - y)(z + y) = m.n$$

diyelim. Bu taktirde

$$z - y = m$$

$$z + y = n$$

denklemlerinden $z = (m + n)/2$ ve $y = (n - m)/2$ bulunur. Burada $m = n$ iken $y = 0$ olacağından $m = n$ olamaz. x' i kenar kabul eden kaç tane Pisagor üçgenin olduğunu bulmak için ise m ve n gibi kaç sayı yazabileceğimizi bulmak gerekir. Bu da x^2 nin pozitif çarpanlarının sayısı yardımıyla bulunur. $p_1, p_2, \ldots, p_r$ farklı tek asallar olmak üzere

$$x^2 = p_1^{2a_1}.p_2^{2a_2}.\ldots.p_r^{2a_r}$$

ise x^2 nin pozitif bölenlerinin sayısı

$$w = (2a_1 + 1)(2a_2 + 1) \ldots (2a_r + 1)$$

ile bulunabilir. Bu sayıların içinde $m = n$ olmasına yol açan bir x sayısı da olacağından w dan 1 çıkarılmalıdır. $m.n = x^2$ iken n.m de x^2 ye eşit olacağından bu sayı ikiye bölünmelidir. Buna göre $(w - 1)/2$ tane Pisagor üçgeni bulunur.

1.1.3. Teorem. x bir çift sayı ise bir dik kenarı x olan Pisagor üçgenlerinin sayısı $[(w-1)/2-v]$ dir.

İspat : x çift olsun. x in bazı çarpanları çift, bazıları tek olacaktır.

$$z-y=m$$

$$z+y=n$$

denilirse $z=(m+n)/2$ nin tamsayı olabilmesi için m ve n nin her ikisi de tek ya da çift olmalıdır. İkisi de tek olsa $m.n=x^2$ de tek olur ki bu bir çelişkidir. O halde m ve n çifttir. Dolayısıyla x in çift çarpanlarının sayısını bulmalıyız. Bunu da Teorem 2 de hesaplanan tüm pozitif çarpanların sayısından tek olanların sayısını çıkararak buluruz.

$$x^2 = 2^{2a_0}.p_1^{2a_1}.p_2^{2a_2}.\ldots.p_r^{2a_r}$$

şeklindeyse x^2 in tek çarpanlarının sayısı

$$v=(2a_1+1)(2a_2+1)\ldots.(2a_r+1)$$

dir. Yani aranan sayı $[(w-1)/2-v]$ dir.

Eğer $N=2^{\alpha_0}\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$ şeklinde çarpanlara ayrılırsa N sayısının kenar olduğu Pisagor üçgenlerinin sayısı

$$L=\frac{(2a_0-1)(2a_1+1)(2a_2+1)\ldots(2a_n+1)-1}{2}$$

şeklindedir.

1.1.1. Örnek. $N=60=2^2.3.5$ olduğundan

$$L=\frac{(2\cdot2-1)(2\cdot1+1)(2\cdot1+1)-1}{2}=\frac{3\cdot3\cdot3-1}{2}=\frac{26}{2}=13$$

tane Pisagor üçgeninde kenar olabilir.

$N=30$ sayısı ise $30=2.3.5$ olarak yazılırsa

$$L=\frac{(2\cdot1-1)(2\cdot1+1)(2\cdot1+1)-1}{2}=\frac{3\cdot3-1}{2}=4$$

tane Pisagor üçgeninde kenar olabilir.

$N=45$ sayısı ise $45=3^2.5$ şeklinde yazılıp

$$L=\frac{(2\cdot2+1)(2\cdot1+1)-1}{2}=\frac{5\cdot3-1}{2}=\frac{14}{2}=7$$

tane Pisagor üçgeninde kenar olabilir.

Yalnızca $K(m^2+n^2)$ formunda yazılabilen sayılar ilkel olan ya da olmayan Pisagor üçgenlerinde hipotenüs olabilir. $4x+1$ formunda en az bir asal çarpan

bulunduran sayılar da (bu sayılar 5, 10, 13, 15, ... şeklindedir) bir Pisagor üçgeninde hipotenüs olur. İlkel Pisagor üçgeninde hipotenüs olmak için K nın değeri 1 ve aynı zamanda m ile n aralarında asal ve zıt halli olmalıdır. İlkel dik üçgenler için asal çarpanların her biri $4x + 1$ formunda karşımıza çıkar ki bu sayılar 5,13, 65, 85 şeklindedir. $4x - 1$ formunda 3, 7, 11, 19 gibi asallardan hiçbiri bu sayının çarpanları olamaz. Eğer N sayısı toplam n farklı asal çarpana sahip ise ve bu asalların her biri $4x + 1$ formunda ise bu taktirde N 2^{n-1} tane ilkel Pisagor üçgeninde hipotenüs olabilir. Örneğin $65 = 5.13$ sayısı $2^{2-1} = 2$ ilkel Pisagor üçgeninin hipotenüsü olabilir. $1105 = 5.13.17$ sayısı $2^{3-1} = 4$ tane üçgende hipotenüs olur. 15, 21 ve 39 gibi sayılar hipotenüs olmayacak çünkü bölenlerinin en az biri 3 olup istenilen formda değildir.

Eğer N sayısı p ler $4x - 1$ formunda asal sayılar ve q lar $4x + 1$ formunda iken

$$N = 2^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_r^{b_r}$$

şeklinde ise N bir tek ilkel üçgenin bile hipotenüsü olamaz ancak ilkel olmayan

$$H = \frac{(2b_1+1)(2b_2+1)\ldots(2b_r+1)-1}{2}$$

tane Pisagor üçgeninde hipotenüs olabilir. Böylece aynı formül tüm asalların yerine yalnızca $4x + 1$ formundakiler alınarak buradaki kenarlar için uygulanır. $N = 2^5.3.5.7^5.11^3.13^2$ olsun. 2, 3, 7 ve 11 asallarını önemsemeyip yalnızca 5 ve 13 ün kuvvetlerinin alınmasıyla

$$H = \frac{(2\cdot 1+1)(2\cdot 2+1)-1}{2} = 7$$

buluruz. Yani N sadece 7 Pisagor üçgeninde hipotenüs olabilir. Bununla birlikte N

$$L = \frac{(2\cdot 5-1)(2\cdot 1+1)(2\cdot 1+1)(2\cdot 5+1)(2\cdot 3+1)(2\cdot 2+1)-1}{2} = 15592$$

tane dik üçgende kenar olabilir. Böylece toplam 15599 tane dik üçgende dik kenar ya da hipotenüs olabilir. Tüm asal çarpanları $4x + 1$ formunda olmadığından N nin hipotenüs olduğu ilkel Pisagor üçgeni yoktur.

Şimdi de $n = 2$ durumu ile ilgili olarak iki kare toplamı hakkında Euler'in görüşünü görelim.

Euler 1747 yılında Fermat'nın, $4n + 1$ formundaki her asal sayının iki kare toplamı olduğuna dair teoremini ispatlamayı başardığında kırk yaşındaydı. 6 Mayıs 1747 de Goldbach'a gönderdiği bir mektupta teoremi sundu ve ispat etti. Ayrıca Euler aslında amacının Fermat'nın bir başka teoremini ispat etmek olduğunu da belirtir. Bu teorem: Her sayının dört ya da daha az sayıda tam karenin toplamı olarak yazılabileceği şeklindedir. Bununla birlikte bu son bahsedilen teorem 1770 de Lagrange tarafından ispatlanana kadar Euler'i meşgul etti. Daha sonraları Euler ispatı kolaylaştırdı. İspatlamış olduğu iki kare toplamı ile ilgili teoremler oldukça önemliydi. Özellikle bu problemle uğraşmak için Euler'in geliştirdiği teknikler, bu çalışmanın 2. bölümünde verilmiş olan, Fermat'nın son teoreminin $n = 3$ durumunu ispatlamak için gereken $x^2 + 3y^2$ şeklindeki tam küpler ile ilgili bazı sonuçları ispatlamada da kullanılabilir.

Euler'in $4n + 1$ formundaki her asalın iki tam karenin toplamı oluşu ile ilgili ispatı uzun değildir ve oldukça basittir.

(1) Her biri iki tam karenin toplamı olan sayıların çarpımı da iki tam karenin toplamıdır. Bu

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

formülünden çıkar.

(2) İki tam karenin toplamı olan bir sayı, iki tam karenin toplamı olan bir asal sayı ile bölünebiliyorsa; bölüm de iki kare toplamıdır. Örneğin $p^2 + q^2$, $a^2 + b^2$ toplamını bölsün ve $p^2 + q^2$ nin asal olduğunu kabul edelim. Bu taktirde $p^2 + q^2$ sayısı

$$\begin{aligned}(pb - aq)(pb + aq) &= p^2b^2 - a^2q^2 \\ &= p^2b^2 + p^2a^2 - p^2a^2 - a^2q^2 \\ &= p^2(a^2 + b^2) - a^2(p^2 + q^2)\end{aligned}$$

sayısını böler. $p^2 + q^2$ asal olduğundan ya $pb - aq$ ya da $pb + aq$ yu böler. İlk olarak $p^2 + q^2$ toplamının $pb + aq$ yu böldüğünü kabul edelim. Bu taktirde

$$(a^2 + b^2)(p^2 + q^2) = (ap - bq)^2 + (aq + bp)^2$$

olduğundan $p^2 + q^2$ nin $ap - bq$ yu da bölmesi gerektiğini görürüz. Bundan dolayı denklem $p^2 + q^2$ nin karesiyle bölünebilir ve sonuç $\frac{a^2+b^2}{p^2+q^2}$ şeklinde istenildiği gibi iki karenin toplamıdır. İkinci hal, $(p^2 + q^2) \mid (pb - aq)$ durumudur ki bu da

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2$$

formülünü kullanarak aynı yöntemle ele alınabilir.

(3) İki tam karenin toplamı olarak yazılabilen bir sayı, iki tam karenin toplamı olmayan bir sayıya bölünebiliyorsa bölüm, iki kare toplamı olmayan bir asal çarpana sahiptir. Buradaki her adım aslında yalnızca (2) nin tersidir. x sayısının $a^2 + b^2$ toplamını böldüğünü kabul edelim. Bölüm $p_1, p_2, \ldots, p_n$ şeklinde asal çarpanlarına ayrılsın. Bu taktirde

$$a + b = x.p_1.p_2. \ldots p_n$$

şeklindedir. Eğer $p_1, p_2, \ldots, p_n$ çarpanlarının tümü iki tam kare toplamı olarak ifade edilebilirse bu taktirde $a^2 + b^2$, $p_1, p_2, \ldots, p_n$ ile ard arda bölünebilir ve (2) den dolayı, her bir bölüm ve bunun sonucunda da x iki tam karenin toplamı olurdu. Bu taktirde eğer x iki kare toplamı değilse $p_1, p_2, \ldots, p_n$ asallarının en az biri iki tam kare toplamı olmamalıdır.

(4) Eğer a ve b aralarında asal ise bu taktirde $a^2 + b^2$ nin her bir çarpanı iki tam karenin toplamıdır. $a^2 + b^2$ nin bir çarpanı x olsun. c ve d nin mutlak değeri en çok $\frac{1}{2}x$ olmak üzere bölme işlemi yapılarak $a = mx \pm c$ ve $b = nx \pm d$ bulunur.

$$a^2 + b^2 = m^2x^2 \pm 2mcx + c^2 + n^2x^2 + 2ndx + d^2 = Ax + (c^2 + d^2)$$

sayısı x ile bölünebildiğinden, $c^2 + d^2$ x ile bölünmelidir. $c^2 + d^2 = xy$ diyelim. Eğer c ve d nin birden büyük herhangi bir ortak böleni varsa, bu bölen x'i bölemez. Eğer bölseydi bu taktirde bu ortak bölen a ve b yi de bölerdi ki bu kabul ile çelişir. Bundan dolayı $c^2 + d^2 = xy$ denklemi c ve d nin en büyük ortak böleninin karesiyle bölünebilir ve $e^2 + f^2 = xz$ formundaki bir denklemi verir. Ayrıca $z \leq \frac{1}{2}x$ dir.

Çünkü

$$zx = e^2 + f^2 \leq c^2 + d^2 \leq \left(\frac{1}{2}x\right)^2 + \left(\frac{1}{2}x\right)^2 = \frac{1}{2}x^2$$

dir. Eğer x iki tam karenin toplamı olmasaydı (3) den dolayı z nin iki tam kare toplamı olarak yazılamayan w gibi bir çarpanı olurdu. Ancak bu sonsuz bir indirgemeye neden olur. Yani her adımda kendisi iki tam karenin toplamı olmayan fakat aralarında asal olan iki tam karenin toplamının bir çarpanı olan bir x sayısıyla

başlayıp daha küçük ve aynı özelliklere sahip bir w sayısını veren bir sonsuz indirgemeye yol açardı. O halde x iki tam karenin toplamı olmalıdır.

(5) $4n + 1$ formundaki her asal iki karenin toplamıdır. Euler, bu sonucun aşağıda verilen ispatını, birkaç tereddüt bulunduran orijinal ispatından 2 yıl sonra 1749 yılında Goldbach'a yolladı. Eğer $4n + 1$ asal sayı ise bu taktirde Fermat'nın teoreminden dolayı $1, 2^{4n}, 3^{4n}, 4^{4n}, \ldots, (4n)^{4n}$ sayılarının her biri p nin bir katından da fazladır. (Sıradaki terim olan p^{4n} p ile bölünebilir ve sonraki $(p + 1)^{4n}, \ldots, (p - p - 1)^{4n}$ terimlerinin hepsi yine p nin bir katından bir fazla olan sayılardır ve bu şekilde devam edilir). Bundan dolayı $2^{4n} - 1, 3^{4n} - 2^{4n}, \ldots, (4n)^{4n} - (4n - 1)^{4n}$ farklarının hepsi p ile bölünebilir. Bu farkların her biri

$$a^{4n} - b^{4n} = (a^{2n} + b^{2n})(a^{2n} - b^{2n})$$

olarak çarpanlarına ayrılabilir ve p asal olduğundan, çarpanlardan birini bölmelidir. Eğer buradaki $4n - 1$ durumdan herhangi birinde p, birinci çarpanı bölebilirse bu taktirde (4) den dolayı ve bir sayı ile ardışığının daima aralarında asal olmasından dolayı, p nin istenildiği gibi iki tam karenin toplamı olduğu görülür. Bundan dolayı, p nin $2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4n)^{2n} - (4n - 1)^{2n}$ şeklindeki tüm $4n - 1$ tane sayıyı bölmeyeceğini göstermek yeterli olacaktır. Bu da aşağıdaki gibi kolayca yapılabilir.
Eğer p, bütün bu sayıları bölerse bu taktirde tüm bu ardışık sayıların $4n - 2$ tane farkını, bunların, tüm $4n - 3$ tane farkını ve sonraki farkları da bölerdi. Ancak $1^k, 2^k, 3^k, 4^k, \ldots$ dizisinin k. farklarının sabit ve k!'e eşit olduğunu ispatlamak basit bir hesaplamadır. x^k için farklar aşağıda Tablo 1.2 de gösterilmiştir.

Tabloya göre $1, 2^{2n}, 3^{2n}, 4^{2n}, \ldots$ dizisinin 2n-inci farkları hep (2n)! dir. Bundan dolayı $p = 4n + 1$ ile bölünemez. Eğer p, $2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4n)^{2n} - (4n - 1)^{2n}$ sayılarının $4n - 1$ tane olan ilk farklarını bölseydi bu taktirde p, $4n - 2n = 2n$ tane 2n-inci farkları bölerdi. Halbuki bu mümkün değildir. Böylece p nin bu $4n - 1$ ilk farkların en az birini bölmemesi gerekir. Bu da istenen sonuçtur.

Tablo 1.2 x^k nın ardışık farkları

k = 1	1	2	3	4	5	6	7	...
1. farklar		1	1	1	1	1	1	...
2. farklar			0	0	0	0	0	0 ...
k = 2	1	4	9	16	25	36	49	...
1. farklar		3	5	7	9	11	13	...
2. farklar			2	2	2	2	2	...
3. farklar				0	0	0	0	0 ...
k = 3	1	8	27	64	125	216	343	512 ...
1. farklar		7	19	37	61	91	127	169 ...
2. farklar			12	18	24	30	36	42 ...
3. farklar				6	6	6	6	6 ...
4. farklar					0	0	0	0 ...
k = 4	1	16	81	256	625	1296	2401	4096 ...
1. farklar		15	65	175	369	671	1105	1695 ...
2. farklar			50	110	194	302	434	590 ...
3. farklar				60	84	108	132	156 ...
4. farklar					24	24	24	24 ...
5. farklar						0	0	0 ....

1658 de Digby'e gönderilen Wallis'in toplanmış çalışmalarından basılmış ve muhtemelen Euler tarafından bilinen önemli bir mektupta, Fermat ;

a) $4n + 1$ formundaki her asalın iki tam karenin toplamı oluşu,

b) $3n + 1$ formundaki her asalın $a^2 + 3b^2$ formunda oluşu ve

c) $8n + 1$ ya da $8n + 3$ formundaki asal sayıların $a^2 + 2b^2$ formunda oluşu ve

d) Her sayının üç ya da daha az üçgensel sayıların, dört ya da daha az tam karenin, beş ya da daha az beşgensel sayıların v.b. toplamı oluşunun reddedilemeyecek birer ispatına sahip olduğunu söylemiştir. Euler bu ifadelerin en sonuncusunu ispatlamaya çok istekliydi. Özellikle de her sayının dört veya daha az sayıda tam karenin toplamı olarak yazılabildiğini ispatlamak istiyordu ve böylece de birincinin ispatında kullandığı yöntemleri diğerlerini ispatlamak için kullanmayı denemesi de doğaldı. Euler (c) ve (d) nin henüz ispatlayabileceği şeyler olmadığını anlamıştı. Ancak b) hemen hemen a) nın ispatlanmasında kullanılan yöntemin aynısıyla ispatlanabilir b) ve a) nın ispatı arasındaki esas fark sadece 2 asalında görülür. Yukarıdaki (4) ifadesi, $a^2 + 3b^2$ formundaki sayı temsilleri için yanlıştır. Çünkü

T.C. YÜKSEKÖĞRETİM KURULU DOKÜMANTASYON MERKEZİ

$1^2 + 3.1^2$ sayısı, 2 nin $a^2 + 3b^2$ formunda olmamasına rağmen, 2 ile bölünebilirdir. Ayrıca eğer (4) ün ispatı $a^2 + 3b^2$ formundaki temsillere uygulanırsa bu taktirde

$$zx \le \left(\frac{1}{2}x\right)^2 + \left(\frac{1}{2}x\right)^2 = \frac{1}{2}x^2$$

eşitsizliği

$$zx \le \left(\frac{1}{2}x\right)^2 + 3\left(\frac{1}{2}x\right)^2 = x^2$$

ile değiştirilebilir ve buradan $z \le x$ olur ve de sonsuz indirgemeyi elde etmede kullanılan kesin eşitsizlik hali kaybolurdu. Bununla birlikte x bir tek sayı ise bu taktirde $|c| \le \frac{1}{2}x$, $|d| \le \frac{1}{2}x$ eşitsizlikleri aslında $|c| < \frac{1}{2}x$, $|d| < \frac{1}{2}x$ kesin eşitsizliklerine dönüşür ve gereken $z < x$ eşitsizliği ortaya çıkar. $a^2 + 3b^2$ formundaki temsiller için (4) ifadesinin bir benzerinin ispatı aşağıdaki gibidir.

(1`) Her biri $a^2 + 3b^2$ formunda yazılabilen iki sayının çarpımı da bu formdadır. Bu ifade

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

eşitliğinden görülür.

(2`) Eğer $a^2 + 3b^2$ formundaki bir sayı 2 ile bölünebiliyorsa bu taktirde 4 ile de bölünmelidir ve 4 ile bölümü de $c^2 + 3d^2$ formunda olmalıdır. Bu taktirde a ve b zıt halli ise $a^2 + 3b^2$, 2^2 ile bölünür ve bölüm $c = \frac{1}{2}a$, $d = \frac{1}{2}b$ olmak üzere $c^2 + 3d^2$ formundadır.

Son olarak a ve b nin tek oluşunu ele alalım. Bu taktirde m, n ve işaretler uygun seçilerek $a = 4m \pm 1$ ve $b = 4n \pm 1$ şeklinde yazılabilir. Böylece ya $a + b$ ya da $a - b$ 4 ile bölünebilir. Eğer $4 \mid (a + b)$ ise bu taktirde

$$4.(a^2 + 3b^2) = (1^2 + 3.1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3(a + b)^2$$

eşitliği 4^2 ile bölünebilirdi çünkü $a - 3b = a + b - 4b$ dir. Bu da gösterir ki $\frac{a^2 + 3b^2}{4}$ sayısı $c^2 + 3d^2$ formundadır. Eğer $a - b$ 4 ile bölünebilirse bu taktirde $4 = 1^2 + 3.1^2$ yerine $4 = (-1)^2 + 3.1^2$ yazılarak aynı sonuca ulaşılır.

(3`) $a^2 + 3b^2$ formunda bir sayı, $p^2 + 3q^2$ formunda bir asal sayı ile bölünebilirse bu taktirde bölüm de $c^2 + 3d^2$ formunda yazılabilir. Bu durumun ispatındaki esas adım tekrar

$$(pb - aq)(pb + aq) = p^2b^2 - a^2q^2 = p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2$$
$$= b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$$

sayısının $p^2 + 3q^2$ ile bölünebilir oluşu ve $p^2 + 3q^2$ asal olduğundan da ya pb - aq ya da pb + aq nun $p^2 + 3q^2$ ile bölünebilir olmasıdır. Bundan dolayı işaret uygun seçilirse

$$(p^2 + 3q^2)(a^2 + 3b^2) = [p^2 + 3(\pm q)^2](a^2 + 3b^2)$$
$$= (ap \pm 3qb)^2 + 3(pb \pm aq)^2$$

eşitliği $(p^2 + 3q^2)^2$ ile bölünebilir ve sonuçta $\frac{(a^2 + 3b^2)}{p^2 + 3q^2}$ istenilen formdadır.

**(4`)** Eğer $a^2 + 3b^2$ formundaki bir sayı aynı formda olmayan bir tek çarpana sahipse bu taktirde bölüm de bu formda olmayan bir tek asal çarpana sahiptir. x tek sayı olmak üzere $xy = a^2 + 3b^2$ olsun. Eğer y bir çift sayı ise bu taktirde (2`) den dolayı 4 ile bölünür ve $x(y/4) = c^2 + 3d^2$ dir. Bu işlem $\frac{y}{4}k$ tek sayı oluncaya dek tekrar edilebilir. Böylece her biri ya 4 ya da tek asal sayı olmak üzere $y = p_1. p_2. \ldots .p_n$ yazılabilir. y nin bu ayrışımdaki tek asal sayıların tümü $c^2 + 3d^2$ formunda yazılabiliyorsa bu taktirde $xy = a^2 + 3b^2$ ard arda p lerin her biriyle bölünebilir. (2') ve (3'), x sayısının $c^2 + 3d^2$ formunda yazılabileceğini gösterir. Bundan dolayı eğer x bu formda değilse bu taktirde y bu formda olmayan bir tek asal çarpana sahip olmalıdır.

(5`) a ve b aralarında asal ise bu taktirde $a^2 + 3b^2$ nin her tek asal çarpanı $c^2 + 3d^2$ formundadır. x, $a^2 + 3b^2$ nin bir tek sayı çarpanı olsun. $|c| < \frac{1}{2}x$, $|d| < \frac{1}{2}x$ iken bölme yaparak $a = mx \pm c$, $b = nx \pm d$ bulunur. Bu yüzden $c^2 + 3d^2$, x ile bölünebilir. $y < x$ olmak üzere $c^2 + 3d^2 = xy$ diyelim. c ve d nin 1 den büyük x i bölebilen bir ortak çarpanı yoktur, çünkü eğer olsaydı bu taktirde a ve b aralarında asal olmazdı. Bundan dolayı $c^2 + 3d^2 = xy$, c ve d nin obebi nin karesiyle bölünebilir ve e ve f aralarında asal olmak üzere $e^2 + 3f^2 = xz$ bulunur. x, $a^2 + 3b^2$ formunda değilse (4`) den dolayı z bir tek çarpana sahiptir. Buna w diyelim.w bu formda değildir.Bundan dolayı (a, b) = 1 iken $a^2 + 3b^2$ formundaki bir sayının çarpanı olan

fakat kendisi $c^2 + 3d^2$ formunda olmayan daha küçük bir x sayısının varlığı aynı formda daha küçük bir w sayısının varlığını gerektirir. İstenilen sonuca sonsuz indirgeme prensibiyle ulaşılır.

3 dışındaki tüm asal sayılar ya $3n + 1$ ya da $3n + 2$ formundadır. $3n + 2$ formundaki bir $a^2 + 3b^2$ sayısı 3 ile bölünmüyorsa bu taktirde a, 3 ile bölünmemelidir. $a = 3m \pm 1$ dir ve $a^2 + 3b^2$ daima 3 ün katlarından 1 fazladır. Böylece (5') den dolayı a ve b aralarında asal iken $a^2 + 3b^2$ formundaki bir sayıyı bölen bir tek asal sayı $3n + 2$ formunda olamaz. Eğer a ve b aralarında asal değillerse e ve f aralarında asal iken ve d, a ile b nin obebi iken $a^2 + 3b^2 = d^2(e^2 + 3f^2)$ dir. Böylece $a^2 + 3b^2$ formundaki bir sayı, $3n + 2$ formunda tek asal çarpana sahip olmayan bir sayı ile bir tam karenin çarpımı olarak yazılabilir. $a^2 + 3b^2$ nin çift asal çarpanları, yani $a^2 + 3b^2$ toplamını bölen 2 lerin sayısı, (2') den dolayı 4 ün bir kuvvetini yani bir tam kareyi bulundurur. Bundan dolayı bir sayının $a^2 + 3b^2$ formunda olması için gerek şart, bulundurduğu en büyük tam kareye bölündüğünde çıkan sonucun $3n + 2$ şeklinde asal çarpan bulundurmasıdır. Bu şartın aynı zamanda yeter bir şartta olduğunu ispatlamak için aşağıdakini ispatlamak yeterlidir.

(6`) $3n + 1$ formundaki her asal $a^2 + 3b^2$ formundadır. Önceki gibi Fermat teoreminden $p = 3n + 1$ asalının $1, 2^{3n}, 3^{3n}, \ldots, (p-1)^{3n}$ sayılarının p–2 tane farklarını böldüğü görülür. Bu farkların her biri

$$a^{3n} - b^{3n} = (a^n - b^n)(a^{2n} + a^n b^n + b^{2n})$$

olarak çarpanlara ayrılabilir ve ikinci çarpan a ya da b çift olduğundan A ve B aralarında asal olmak üzere

$$A^2 + A(2B) + (2B)^2 = (A + B)^2 + 3B^2$$

formunda yazılabilir. Böylece (5') den dolayı p eğer $1, 2^n, 3^n, \ldots, (p-1)^n$ sayılarının $p - 2$ tane farkını bölüyorsa p , $c^2 + 3d^2$ formunda olmalıdır. Önceki gibi bu p nin n!' i bölebileceğini gösterirdi ki bu imkansızdır. Böylece göstermek istediğimiz gibi p $c^2 + 3d^2$ şeklinde olmalıdır.

Eğer bu tartışma $a^2 + 2b^2$ formundaki temsillere uygulanırsa; bir sayının $a^2 + 2b^2$ formunda olması için gerek şart bulundurduğu en büyük tam kareye bölündüğünde çıkan sonucun $8n + 5$ ya da $8n + 7$ formunda asal çarpan bulundurmasıdır. Bu şartın aynı zamanda yeter şart da olduğunu ispatlamak için $8n + 1$ ya da $8n + 3$ formundaki tüm asal sayıların $a^2 + 2b^2$ formunda yazılabildiğini

ispatlamak yeterlidir. (6') ye benzeyen bu son adım, Euler'in ispatlayamadığı bir sonuçtu. Bunun ilk ispatı Lagrange tarafından verilmiştir.

1.2. Fermat'nın Sonsuz İndirgeme Metodu

Fermat'nın bulmakla oldukça övündüğü bir ispat metodudur. Fermat ömrünün sonlarında Sayılar Teorisi ile ilgili buluşlarını özetlediği uzun bir mektupta tüm ispatlarını açık bir şekilde ifade ederken bu metodu kullanmıştır.

Bu metodu anlamak amacıyla örnek olarak şu önermeyi ele alalım: "v ve w aralarında asal ve vw bir tam kare ise bu taktirde v ve w nun her biri birer tam kare olmalıdır". Fermat'nın vurguladığı gibi bu önermeler için en iyi ispat metodu sonsuz indirgeme metodudur. Eldekilere göre,

1) v ve w aralarında asaldır,
2) v.w tam karedir,
3) v ve w her ikisi birden tam kare değildir,

şartlarını sağlayan v ve w sayılarının bulunuşunun imkansızlığı nasıl gösterilebilir ?

Kabul edelim ki böyle v ve w sayıları bulunabilsin. Gerekirse v ve w yer değiştirebileceğinden v nin kare olmadığını kabul edebiliriz. Özellikle v 1 olmasın. Bundan dolayı v nin en az bir asal çarpanı vardır. v nin asal çarpanına P diyelim. O halde $v = P.k$ yazabiliriz. Bu taktirde P, v.w yi de böler. Ancak v.w bir tam kare olarak verilmiştir. O halde $v.w = u^2$ şeklindedir. Asal sayıların temel özelliğinden eğer P u^2 yi bölüyorsa P u yu bölüyor demektir, yani $u = P.m$ demektir. Bu taktirde $v.w = u^2$ yi

$$v.w = P.k.w = (P.m)^2 = P^2.m^2$$

olarak tekrar yazabiliriz. Bu durumda $k.w = P.m^2$ olur. Bu ifadede P sağ tarafı böldüğünden sol tarafı da böler. Yani ya $P \mid k$ ya da $P \mid w$ olmalıdır. v ve w aralarında asal olduğundan P w yu bölemez. Bu durumda $P \mid k$ olmalıdır ve $k = P.v'$ yazabiliriz. O halde $k.w = P.m^2$ ve $P.v'.w = P.m^2$ haline gelir ki $v'.w = m^2$ olur. $v = P.k = P^2.v'$ olduğundan v' nün herhangi bir böleni v nin de bir bölenidir. Böylece v' ve w nin 1 den büyük bir ortak böleni olmadığı görülür. Üstelik v' bir tam kare olsaydı. $v = P^2.v'$ de bir tam kare olurdu. Ancak v bir tam kare değildir. Bundan dolayı v' bir tam kare değildir. Yani v' ve w sayıları 1) , 2) , 3) özelliklerine sahip sayılardır ve $v > v'$ dür.

Aynı mantıkla başka bir v'' sayısının $v'' < v'$ olacak şekilde bulunabileceğini görürüz. v'' ve w aynı özelliklere sahip olur. Aynı yöntem sonsuz çoklukta tekrarlanırsa pozitif sayıların $v > v' > v'' > v''' > ...$ şeklinde azalan sonsuz bir dizisi elde edilir. Pozitif sayılar alttan sıfır ile sınırlandığından böyle bir dizi bulmak imkansızdır. Yani bu üç özelliğe sahip v ve w sayıları bulmak imkansızdır. Böylece önermenin ispatı biter.

Özet olarak, sonsuz indirgeme metodu aşağıdaki düşünceye dayanır.

Kabul edelim ki bir pozitif tamsayı verilen bazı özelliklere sahip olsun. Bu metoda göre aynı özelliklere sahip daha küçük bir (ve dolayısıyla sonsuz çoklukta) pozitif tamsayı vardır. Buradan elde edilecek çelişki yardımıyla hiçbir pozitif tamsayının bu özelliklerin tümünü sağlayacak şekilde bulunamayacağı söylenebilir.

1.3. Fermat'nın Son Teoreminin Tarihsel Gelişimi

Pierre de Fermat 1665 de öldüğünde Avrupa'daki en tanınmış matematikçilerden biriydi. Bugün Fermat'nın adı hemen hemen sayılar teorisi ile özdeşleşmiştir, ancak Fermat'nın kendi döneminde yapmış olduğu çalışmalar oldukça devrimci ve zamanın oldukça ilerisinde olduğu için ne yazık ki onun çalışmalarının değeri anlaşılamamış ve adı daha çok başka alanlardaki çalışmaları ile duyulmuştur. Bu çalışmalar arasında analitik geometrinin bazı konuları, analiz de kare alma, minimum ve maksimum problemleri gibi konular sayılabilir.

Fermat'nın bir matematikçi olarak anılmasında ilginç olan iki durum vardır. Bu durumlardan ilki onun aslında Meclis Yüce Divanında Yüksek Hakim olmasıdır. Fermat hayatının olgunluk döneminde Toulouse'de yargıçlık yaparken bir hobi olarak matematik çalışıyordu. İkincisi ise yapmış olduğu çalışmalarını hiçbir zaman tek başına yayınlamamış olmasıdır. Onun şöhreti diğer bilim adamlarıyla yaptığı yazışmalar sayesinde ve yazdığı müsvedde şeklindeki sayısız yazılarla artmıştır. Fermat birçok defa kendisine çalışmalarını yayınlaması konusunda teklif yapılmasına rağmen hiçbir sebep göstermeksizin sık sık reddetmiş ve yazdıklarının ve keşfettiklerinin çoğunun yazılmasına izin vermemiştir. Bu nedenle Fermat'nın Sayılar Teorisindeki buluşları o hayattayken yayınlanamamıştır.

Fermat'nın çalışmalarının yayınlanmasını reddetmesi ile hayranları, onun çalışmalarının, mektuplarının ve yayınlanmamış el yazmalarının Fermat'nın ölümünden sonra yayınlanmak için biriktirilmezse Fermat'nın kısa sürede unutulabileceği endişesine kapılmışlardır. Bu görev oğlu Samuel tarafından yerine getirilmiştir. Babasının yazıştığı arkadaşlarındaki el yazmalarını ve mektupları bir araya getirmiş olan Samuel de Fermat babasının kendi yazdıklarını ve kitaplarını gözden geçirdi ve Fermat'nın ünlü "Son Teoremi" bu şekilde ortaya çıktı.

Samuel de Fermat, babasının Diophant'ın "Arithmetic" adlı kitabının Bachet tarafından yapılan çevirisinin kenar boşluklarına yazdığı notları buldu. Fermat'nın yazdığı bu notta " $n > 2$ iken $x^n + y^n = z^n$ denklemini sağlayan sıfırdan farklı x,y ve z tamsayılarını bulmak imkansızdır. Bu önermenin gerçekten çok hayret verici bir ispatını biliyorum. Ancak bu boşluk ispatın sığamayacağı kadar küçük." yazılıydı. Bu önerme Fermat'nın Son Teoremi olarak bilinmektedir. Kökleri eski yunan ve Diophant'a dayanan ve bugünkü bilinen hali 1630 lu yıllarda Fermat tarafından ortaya atılmış olan "Son Teorem" in doğruluğunu ispatlamak ya da bu teoremi çürütmek için sayısız matematikçi çaba göstermiştir.Eğer gerçekten de Fermat söylediği gibi önermenin ispatına sahip ise bu ispat gerçekten hayret verici olmalıydı. Çünkü Fermat'dan Andrew Wiles'e kadar yaklaşık 350 yıldır hiç kimse bu önermenin ispatını bulamadı. Bu matematikçilerden bazıları belirli dönemlerde teoremin bazı özel hallerini ispatlamayı başarsa da genel hal bu kişilerin her biri için çok uzak bir hedef olarak kalmıştır. Ancak 20. yüzyıl bu problemin çözümünde en büyük adımların atıldığı dönem olmuştur.

19. yüzyılda Fransız bayan matematikçi Sophie Germain o güne kadar yapılan birkaç özel halden çok daha ileriye götürerek n, $2n + 1$ asal olacak şekilde bir tek asal sayı ise $x^n + y^n = z^n$ denkleminin çözümü oluşunun x, y ve z den en az birinin n ile bölünebileceği gerçeğini kullanan Germain , 100 den küçük n asalları için x, y ve z nin hiçbirisinin n ile bölünemeyeceğini ispatlamıştır. Bu çalışmasından sonra ikisi birden asal olan n ve $2n + 1$ sayı çiftlerine Sophie Germain asalları denilmiştir. Daha sonra Legendre bu yöntemi kullanarak ispatı 197 ye kadar olan tüm asal sayılara genişletti ama hala genel ispat ulaşılmaz görünüyordu. Bu önerme bir çok büyük matematikçinin çözmeyi denediği ancak çözemediği birkaç problemden biridir.

Teoremin, Fermat'nın Son Teoremi olarak adlandırılmasının nedeni; Bu teoremin Fermat'nın en son çalıştığı problem olması değil, Fermat'nın çalıştığı ve

önerdikleri arasında doğruluğu ya da yanlışlığı ispatlanmamış olan en son problem olmasıdır.

Fermat'nın son teoremini sadece asal kuvvetler için ispatlamak yeterlidir. İkiden büyük her n sayısının bir p asalı ile bölünmesi gereklidir. Yani $n = p.m$ olacak şekilde bir $m \in Z^+$ vardır. $x^n + y^n = z^n$ eşitliğinin imkansızlığını ispat etmek için $x^p + y^p = z^p$ nin imkansız olduğunu ispatlamak açıkça yeterli olacaktır. Çünkü, $x^n + y^n = z^n$ eşitliğinin bir çözümünün olması $x^{pm} + y^{pm} = z^{pm}$ eşitliğinin ve dolayısıyla $(x^m)^p + (y^m)^p = (z^m)^p$ eşitliğinin de bir çözümünün olması anlamına gelirdi. Böylece Fermat'nın Son Teoremi $n > 2$ asal iken ispatlanması gereken bir hale dönüşmüştür. Bunu dikkate alan daha sonraki matematikçiler n sayısının sadece asal olduğu durumları incelemişlerdir.

19. yüzyıldaki gelişmelerden sonra problemin çözümüne yönelik en büyük adım 1950 li yıllarda atıldı. Tokyo Üniversitesinde çalışmakta olan Goro Shimura ile meslektaşı Taniyama modüler formlar üzerinde çalışırken bu formların eliptik eğriler ile örtüştüğüne yönelik bir tahmin ortaya attılar. Taniyama ve Shimura bu iddialarının denedikleri her eliptik eğri için doğru çıkmasına rağmen genel ispatı ortaya koyamadılar. Daha sonraki yıllarda tahminin yanlış çıkma ihtimaline rağmen bu alanda yapılan bir çok çalışma dayanak olarak bu tahmini kullanıyordu. 1984 yılında Almanya daki bir matematik sempozyumunda Gerhard Frey, Taniyama-Shimura varsayımının ispatlanması durumunda Fermat'nın Son Teoreminin de bunun sonucu olarak ispatlanabileceğini söyledi.

Frey, Fermat'nın Son Teoremindeki denklem üzerinde bazı değişiklikler yaparak bu denklemi bir eliptik eğri denklemine çevirdi. Frey'e göre eğer Fermat'nın Son Teoremindeki denklemi sağlayan tamsayı çözümler varsa bu böyle bir eliptik eğrinin var olduğu anlamına gelirdi. Frey'in tartışmasında en kritik nokta, Fermat denkleminden çıkarmış olduğu kendi eliptik denkleminin modüler olamayacak kadar tuhaf görünmesiydi. Böyle bir modüler form olmadığı için bu Taniyama-Shimura varsayımının yanlış olması anlamına geliyordu. Demek ki Frey çok çarpıcı bir sonuca ulaşmıştı: Fermat'nın Son Teoremi Taniyama-Shimura varsayımının ispatının doğrudan bir sonucudur. Yani matematikçiler Taniyama-Shimura varsayımını ispat edebilirlerse, Fermat'nın Son Teoremini de otomatikman ispat etmiş olacaklardı. Bu düşünceyi dikkate alarak çalışanlardan biri de bu problemle ilk olarak çocukluğunda karşılamış

olan ve bunu bir gün mutlaka ispatlayacağını düşünen Andrew Wiles'tı. Wiles'ın bu büyük problemi çözmesi 7 yılını aldı ve Wiles bu 7 yıl boyunca Fermat'nın Son Teoremi ile ilgili olmayan hiçbir çalışmayla ilgilenmedi ve bitmek bilmeyen konferans ve toplantı dizilerine katılmayı kesti. Üniversitedeki görevi devam ettiğinden sadece buradaki derslerine ve seminerlere katılmaya devam etti. Wiles bu uzun süre boyunca hangi konuyla ilgilendiğini eşi dışındaki kişilerden gizledi ve sonuca ulaştığını düşündüğü zaman Haziran 1993 te Cambridge'deki konferansta üç günlük bir dizi konuşmayla bunu açıkladı. İspatın duyurulduğu ilk andan sonra incelemeler başladı ve bir süre sonra ispatta bir boşluk olduğu görüldü ve tam herkesin yine umudunu kaybetmeye başladığı anda Wiles bir yıl sonra düzeltilmiş tam ispatı ilan etti. Böylece tarihin en önemli matematik problemi çözülmüş oldu.

2. FERMAT'NIN SON TEOREMİNİN ÖZEL HALLERİ

Bu bölümde Fermat'nın son teoreminin sırasıyla $n = 4, 3, 5$ ve 7 özel hallerinde verilmiş olan ispatları bir araya getirilmiştir.

2.1. n = 4 hali

Fermat'nın Son Teoreminin $n = 4$ halini ispat etmek için Pisagor üçlüleri oluşturma metodunu ve sonsuz azalma metodunu birleştirmek yeterlidir. Kabul edelim ki $x^4 + y^4 = z^4$ olacak şekilde x, y ve z tamsayıları var olsun. Pisagor üçlülerinde olduğu gibi x, y, z sayılarının seçimi, aralarında ikişer ikişer asal olacak şekilde yani 1 den büyük ortak bölenleri olmayacak şekilde yapılabilir. Aksi taktirde herhangi ikisini bölen bir sayı $x^4 + y^4 = z^4$ denkleminden dolayı üçüncüsünü de bölecektir. Bu durumda ise bu sayının dördüncü kuvveti sadeleştirilebilir. Böylece x^2, y^2 ve z^2 ilkel Pisagor üçlüleri haline gelir. Yani

$$(x^2)^2 + (y^2)^2 = (z^2)^2$$

olur. Pisagor üçlülerinde $x^2 + y^2 = z^2$ denkleminin çözümünün p ve q aralarında asal, zıt halli ve $p > q > 0$ iken

$$x = 2pq, \qquad y = p^2 - q^2, \qquad z = p^2 + q^2$$

olduğunu bildiğimize göre Fermat'nın Son Teoreminin $n = 4$ hali için de aynı şartlar altında

$$x^2 = 2pq, \qquad y^2 = p^2 - q^2, \qquad z^2 = p^2 + q^2$$

yazılabilir. Bu üç denklemlerden ikincisi $y^2 + q^2 = p^2$ şeklinde yazılabilir ve p ve q aralarında asal olduklarından y, q, p nin de bir ilkel Pisagor üçlüsü olduğu sonucu çıkar. Buna göre p tektir ve p, q zıt halli olduğundan q çifttir. Böylece a ve b aralarında asal, zıt halli ve $a > b > 0$ iken

$$q = 2ab, \qquad y = a^2 - b^2, \qquad p = a^2 + b^2$$

yazılabilir. Böylece

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

dir. Bu ifade $ab(a^2 + b^2)$ nin bir tam kare olduğunu gösterir. Aslında $ab(a^2 + b^2)$ x çift sayısının yarısının karesi (yani $(x / 2)^2$) dir. Ancak ab ve $a^2 + b^2$ aralarında asaldır. Çünkü ab yi bölen herhangi bir p asalı a ya da b yi bölmelidir. Ayrıca p bu iki sayının her ikisini birden bölemez. Çünkü a ile b aralarında asaldır. Bu durumda p sayısı $a^2 + b^2$ toplamını bölemez. Buna göre ab ve $a^2 + b^2$ nin her ikisi de birer kare olmalıdır. Ancak bu taktirde ab nin bir tam kare ve a ile b nin aralarında asal oluşundan a ve b nin her ikisinin tam kare olması gerekir. $a = X^2$, $b = Y^2$ diyelim. Buna göre

$$X^4 + Y^4 = a^2 + b^2$$

bir tam karedir. Bu ise sonsuz azalma metodunu kullanabilmek için yeterlidir. Başka bir deyişle, eğer x ve y $x^4 + y^4$ bir tam kare olacak şekilde pozitif tamsayılar ise bu taktirde yukarıdaki işlemle $X^4 + Y^4$ bir tam kare olacak şekilde yeni bir X, Y pozitif tamsayı çifti elde edilir. Ayrıca

$$X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$$

tür. Böylece pozitif tamsayıların sonsuz, azalan bir dizisini oluşturmak mümkündür. Bu ise imkansızdır. Buna göre iki tane dördüncü kuvvetin toplamı dördüncü kuvvet olmak bir tarafa bir tam kare bile olamaz. Bu sonuç Fermat'nın Son Teoremini n = 4 hali için ispat eder.

Buna göre m herhangi bir pozitif tamsayı iken

$$X^{4m} + Y^{4m} = Z^{4m}$$

denkleminin çözümünün imkansız olduğu sonucu çıkar. Aksi halde $X = x^m$, $Y = y^m$, $Z = z^m$ sayıları

$$X^4 + Y^4 = Z^4$$

denkleminin bir çözümü olurdu ki bu bir çelişkidir. Böylece Fermat'nın Son Teoremi 4 ile bölünebilen her n kuvveti için doğrudur.

2.2. n = 3 hali

n = 3 durumu, yani

$$x^3 + y^3 = z^3$$

YÜKSEKÖĞRETİM KURULU DOKÜMANTASYON MERKEZİ

denklemi Fermat'nın zamanından yaklaşık yedi yüzyıl önce Arap matematikçiler tarafından biliniyordu ve çözümün imkansızlığının hatalı bir ispatı onlar tarafından verilmişti. Fermat'nın genel teoremi keşfetmeden önce bu özel hali keşfetmiş olması muhtemeldir. Çünkü Fermat bunu bir problem olarak, "Denklemi sağlayan x, y ve z değerlerini bulmak" şeklinde önermişti ve daha sonra da bunun imkansız olduğunu belirtti. Euler bu özel hal için teoremi ispatlayan ilk kişiydi. Ancak Euler'in ispatı sorunun gerçek zorluğunun nerede olduğu konusunda yetersizdi. Bu eksikliğe rağmen Euler'in "Algebra" kitabında vermiş olduğu ispatı Kummer tarafından yıllar sonra oldukça başarılı bir şekilde uygulanacak olan idealler teorisinin gelişimine katkıda bulunmuştu.

Fermat'nın Son Teoreminin $n = 3$ durumunun Euler tarafından yapılan ispatının temel metodu Fermat'nın sonsuz azalma metodudur. Euler eğer

$$x^3 + y^3 = z^3$$

olacak şekilde x, y, z pozitif tamsayıları bulunabilirse bu taktirde aynı özellikte daha küçük pozitif tamsayıların da bulunabileceğini gösterdi. Yani bu metoda göre pozitif tamsayı üçlülerinin sürekli azalan ve asla bitmeyen bir dizisini bulmak mümkün olur. Bu ise açıkça imkansızdır. Böylece bu özellikte x, y ve z sayıları bulunamaz.

$$x^3 + y^3 = z^3$$

olduğunu kabul edelim. x, y ve z sayılarının herhangi ikisini bölen bir sayı, denklemin yapısından dolayı üçüncüyü de böler. Bu nedenle tüm ortak bölenler atılarak bu üç sayının ikişer ikişer aralarında asal olduğu kabul edilebilir.Yani x, y ya da x, z veya y, z nin en büyük ortak böleni 1 dir. O halde x, y, z sayılarından en çok bir tanesi çifttir. Diğer taraftan en az biri çifttir. Örneğin x ve y tek ise z çift olur. Buna göre bu sayılardan tam olarak bir tanesi çifttir.

İlk olarak kabul edelim ki x, y tek ve z çift olsun. Bu taktirde $x + y$ ve $x - y$ çift olur.

$$x + y = 2p \text{ ve } x - y = 2q$$

diyelim. Bu taktirde

$$x = \frac{1}{2}(2p+2q) = p+q \qquad \text{ve} \qquad y = \frac{1}{2}(2p-2q) = p-q$$

bulunur.

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

ifadesi p ve q lar cinsinden yazıldığında

$$(p+q)^3 + (p-q)^3 = 2p[(p+q)^2 - (p+q)(p-q) + (p+q)^2]$$

$$= 2p\,(p^2 + 3q^2)$$

bulunur. Burada p ve q zıt hallidir, çünkü $p+q$ ve $p-q$ tek sayıdır ve bunlar aralarında asaldır çünkü p ve q nun herhangi ortak böleni $x = p+q$ ve $y = p-q$ yu da böler ve böylece bu ortak bölen yalnızca 1 olabilir. Ayrıca p ve q nun her ikisi pozitif kabul edilebilir. (Eğer $x < y$ ise bu taktirde $q > 0$ olması için x ve y yer değiştirilir. $x = y$ olması imkansızdır. Çünkü bu taktirde $x = y = 1$ ve $z^3 = 2$ olur.) Böylece x, y nin ikisi de tek olmak üzere $x^3 + y^3 = z^3$ kabulü;

$$2p(p^2 + 3q^2) = \text{bir küp}$$

olacak şekildeki aralarında asal, zıt halli p, q pozitif tamsayılarının varolduğunu gösterir. Eğer z tek ve x ve y den biri çift alınırsa da aynı sonuca ulaşılır. Bu durumda tek olana y dersek, y denklemin sağ tarafına atılabilir ve

$$x^3 = z^3 - y^3 = (z-y)(z^2 + zy + y^2)$$

olur. Bu taktirde

$$z - y = 2p, \quad z + y = 2q$$

ve böylece de

$$z = q + p, \quad y = q - p$$

dir. Buradan

$$x^3 = 2p\,[(q+p)^2 + (q+p)(q-p) + (q-p)^2]$$

olur ki yine aynı sonuç; yani p ve q aralarında asal, zıt halli pozitif tamsayılar olmak üzere

$$2p(p^2 + 3q^2) = \text{bir küp}$$

sonucu elde edilir.

Tartışmadaki bir sonraki adım kabaca 2p ve $p^2 + 3q^2$ nin aralarında asal olduğunu göstermektir. Buradan 2p ile $p^2 + 3q^2$ nin çarpımlarının bir küp olabilmesinin tek yolunun onların her birinin bir küp olması olduğu elde edilebilir. Buradaki işlemlerin $x^2 + y^2 = z^2$ nin çözümlerinin araştırılmasındaki sonsuz indirgeme metoduna benzerliğine dikkat edelim. Bununla birlikte 2p ve $p^2 + 3q^2$ aralarında asal olduğu ifadesi çok açık değildir. p ve q zıt halli olduğundan $p^2 + 3q^2$ tek sayıdır ve 2p ile $p^2 + 3q^2$ nin herhangi bir ortak böleni p ve $p^2 + 3q^2$ nin de bir ortak böleni

olur. Böylece de bu ortak bölen p ve $3q^2$ nin de bir ortak böleni olurdu. p ve q aralarında asal olduğundan bu mümkün olan tek ortak çarpanın 3 olduğunu gösterir. Ancak eğer 3 p yi bölerse bu taktirde 3 $p^2 + 3q^2$ yi de böler ve 2p ile $p^2 + 3q^2$ aralarında asal olamaz. Buna göre ispat ikiye ayrılır. İlk olarak 3 p yi bölmüyorsa 2p ile $p^2 + 3q^2$ aralarında asaldırlar. İkinci olarak ta $3 \mid p$ olsun. Bu iki durumun birincisini ilk olarak ele alacağız. Bu durumda ikinci durum ilkinin basit bir adaptasyonu olarak düşünülebilir. Buna göre 3 ün p yi bölmediğini kabul edelim. O halde 2p ve $p^2 + 3q^2$ nin her ikisi de birer küptür. Daha önceki bilgilerimizden

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd) + 3(ad + bc)^2$$

formülü kullanılırsa

$$\begin{aligned}(a^2 + 3b^2)^3 &= (a^2 + 3b^2)[\,(a^2 - 3b^2)^2 + 3(2ab)^2] \\ &= [\,a\,(a^2 - 3b^2) - 3b(2ab)\,]^2 + 3[\,a(2ab) + b(a^2 - 3b^2)\,]^2 \\ &= (a^3 - 9ab^2)^2 + 3(3a^2b + 3b^3)^2\end{aligned}$$

yazımıyla $p^2 + 3q^2$ formundaki küpler bulunabilir.

Yani, $p^2 + 3q^2$ formundaki küpleri bulmanın bir yolu rasgele a, b sayıları seçmek ve $p^2 + 3q^2$ = bir küp olacak şekildeki $p = a^3 - 9ab^2$, $q = 3a^2b - 3b^3$ sayılarını almaktır. Euler'in ispatındaki büyük boşluk $p^2 + 3q^2$ nin bir küp olmasının bir tek yolu olduğunun ispatı ile doldurulabilir. Yani eğer $p^2 + 3q^2$ bir küp ise bu taktirde p ve q yukarıdaki denklemlerle verilmiş olacak şekilde a, b sayıları varolmalıdır. Euler aşağıda göreceğimiz tartışmasında bunu esas almıştır. Her durumda, bu sonuç garantilenirse ispatın kalanı daha kolaydır.Bu ifadeler p ve q için

$$p = a(a - 3b)\,(a + 3b), \quad q = 3b(a - b)\,(a + b)$$

olarak çarpanlara ayrılabilir. Elbette a ve b aralarında asaldır. Çünkü onların herhangi bir ortak çarpanı p ve q nun da ortak böleni olurdu ki bu kabul ile çelişir. Ayrıca

$$2p = 2a(a - 3b)\,(a + 3b)$$

sayısı bir küptür. a ve b zıt halli olmalıdır. Çünkü aksi halde p ve q çift olurdu. Böylece $a - 3b$ ve $a + 3b$ sayıları tektir ve 2a ile $a \pm 3b$ nin tek olası ortak çarpanı a ve $a \pm 3b$ nin de ortak çarpanı ve bundan dolayı da a ile $\pm 3b$ nin bir ortak böleni olurdu. Aynı şekilde, $a + 3b$ ve $a - 3b$ nin herhangi bir ortak çarpanı da a nın ve 3b nin bir ortak çarpanı olurdu. Kısaca, mümkün olan tek ortak çarpan 3 tür. Ancak 3 a sayısını bölmez. Çünkü eğer $3 \mid a$ ise $3 \mid p$ olurdu ki bu kabulümüze terstir. Buna göre

$2a$, $a-3b$, $a+3b$ sayıları aralarında asaldır ve bunların her üçü de birer küp olmalıdır. Bunlara $2a=\alpha^3$, $a-3b=\beta^3$, $a+3b=\gamma^3$ diyelim. Bu taktirde

$$\beta^3+\gamma^3=2a=\alpha^3$$

olur ve bu da $x^3+y^3=z^3$ denkleminin orijinal çözümden daha küçük olan bir çözümünü verir. Daha özel olarak;

$$\alpha^3\beta^3\gamma^3=2a(a-3b)(a+3b)=2p$$

olur ki bu pozitiftir ve z çift iken z^3 ün, x çift iken de x^3 ün bir bölenidir. $\alpha^3\beta^3\gamma^3$, z^3 den daha küçüktür. α, β ya da γ nın negatif olmasını engelleyecek bir şey yoktur. Ancak $(-\alpha)^3=-\alpha^3$ olduğundan negatif olan küpler denklemin diğer tarafına taşınarak pozitif küpler haline getirilebilir ve elde edilen denklem X, Y, Z ler pozitif ve $Z^3<z^3$ olmak üzere

$$X^3+Y^3=Z^3$$

formundadır. Böylece sonsuz indirgeme özelliği p 3 e bölünmüyor iken sağlanmış olur.

Son olarak p nin 3 e bölündüğü hali ele alalım. Bu taktirde s bir tamsayı olmak üzere $p=3s$ diyelim. 3 q yu bölemez. Buna göre

$$2p(p^2+3q^2)=3^2.2s(3s^2+q^2)$$

dir. $3^2.2s$ ve $3s^2+q^2$ sayılarının aralarında asal oldukları kolayca görülür. Bu nedenle bunların her ikisi de birer tam küptür.

$3s^2+q^2$ nin sadece a ve b tamsayıları için

$$q=a(a-3b)(a+3b),\qquad s=3b(a-3b)(a+b)$$

iken bir tam küp olabileceği daha sonra bir lemma ile ispatlanacaktır. $3^2.2s$ bir küp olduğundan, $3^3.2b(a-b)(a+b)$ bir küptür. Bu nedenle $2b(a-b)(a+b)$ de bir küptür. Buradaki çarpanların aralarında asal olduğu kolayca görülür. O halde $2b=\alpha^3$, $a-b=\beta^3$, $a+b=\gamma^3$, $\alpha^3=2b=\gamma^3-\beta^3$ olmalıdır. Böylece önceki durumdaki gibi $Z^3<z^3$ olacak şekilde bir $X^3+Y^3=Z^3$ denklemini sağlayan bir üçlü elde edilebilir.

Her iki halde de iki küpün toplamı olan bir küpün varlığı aynı özellikte daha küçük bir küpün varlığı anlamına gelir ki bu imkansızdır. Bu teoremi tamamlamak için geriye kalan tek şey p ve q, p^2+3q^2 bir küp olacak şekilde aralarında asal tamsayılar ise bu taktirde $p=a^3-9ab^2$ ve $q=3a^2b-3b^3$ olacak şekilde a ve b tamsayılarının varolduğunu göstermektir.

Şimdi bundan sonraki kısımda sıkça kullanılacak olan $a + b\sqrt{-3}$ şeklindeki cebirsel sayıların aritmetiğini inceleyelim.

Euler' in $p^2 + 3q^2$ formundaki küpler hakkında gerek duyduğu sonucu bulmak için denediği teknik tamsayıların aritmetiğini, a ve b tamsayı olmak üzere $a + b\sqrt{-3}$ formundaki sayılarla toplama, çıkarma ve çarpma yapmaya genişletme fikrine dayanır. Böyle sayılarla toplama, çıkarma ve çarpmanın nasıl yapılacağı açıktır, sadece çarpma için kuralın

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = ac + ad\sqrt{-3} + bc\sqrt{-3} + bd(-3)$$
$$= (ac - 3bd) + (ad + bc)\sqrt{-3}$$

şeklinde olduğuna dikkat edilmelidir. Değişme, birleşme ve dağılma özellikleri ve

$$1.(a + b\sqrt{-3}) = a + b\sqrt{-3}$$

oluşu geneldeki gibidir.

Modern cebir dilinde $a + b\sqrt{-3}$ sayıları birimli ve değişmeli bir halka oluşturur. $a + b\sqrt{-3}$ şeklindeki sayılarla hesaplama yapma düşüncesi $p^2 + 3q^2$ nin bir küp olabilmesi için yeter şartın elde edilmesini kolaylaştırır.

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

formülünü kullanmak yerine aşağıdaki yol izlenebilir.

$p^2 + 3q^2$ sayısını $(p + q\sqrt{-3})(p + q\sqrt{-3})$ olarak çarpanlarına ayıralım. Eğer bu çarpanlardan biri bir küp ise $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ denilerek bunun eşleniği olan $p - q\sqrt{-3}$ ünde $a + b\sqrt{-3}$ ün eşleniğinin küpü olduğu kolayca kontrol edilebilir. Yani $p - q\sqrt{-3} = (a - b\sqrt{-3})^3$ dür. Böylece çarpmanın değişme özelliğinden

$$(p + q\sqrt{-3})(p - q\sqrt{-3}) = [(a + b\sqrt{-3})(a - b\sqrt{-3})]^3,$$

yani $p^2 + 3q^2 = (a^2 + 3b^2)^3$ bulunur. Başka bir deyişle $p^2 + 3q^2$ formunda bir küp bulmak için $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ yazmak yeterlidir. $(a + b\sqrt{-3})^3$ binom teoremi kullanılarak açılırsa

$$p + q\sqrt{-3} = a^3 + 3a^2b\sqrt{-3} + 3ab^2(-3) + b^3(-3)\sqrt{-3}$$

ifadesi $p^2 + 3q^2$ yi bir küp olarak yazmak için $p = a^3 - 9ab^2$, $q = 3a^2b - 3b^3$ olacak şekilde a ve b tamsayılarını bulmanın yeterli olacağını gösterir. Bu ise bir önceki bölümde bulunmuş olan yeter şarttır.

Euler "Algebra" adlı kitabının bu kısmında gerek ve yeter şartları çok ciddi bir şekilde karıştırmıştır ve ne söylemek istediğini belirlemek çok zordur. Örneklerinde Euler en çok a, b ile başlayıp p ve q yu bulduran yeter şartlarla ilgileniyor gibi görünmektedir.

Ancak Euler bazı hatalı ifadeler kullanmıştır. Örneğin, Euler: " Örnek olarak $x^2 + cy^2$ nin bir küp olması için her iki irrasyonel çarpanın, yani $x + y\sqrt{-c}$ ve $x - y\sqrt{-c}$ nin küp olması gerekir, çünkü x ve y nin hiç ortak böleni olmadığından bunlar aralarında asaldır." demiştir. Ancak $x + y\sqrt{-c}$ ve $x - y\sqrt{-c}$ nin küp olması gerektiğinin bir ispatını vermemiştir. Aynı paragrafın sonunda Euler çok kesin olarak "$ax^2 + cy^2$ iki rasyonel çarpana ayrılamadığı zaman bu durumda burada verilmiş olandan başka çözüm yoktur." diye belirtmiştir. Yani $ax^2 + cy^2$ nin bir küp olması için

$$x\sqrt{a} + y\sqrt{-c} = (p\sqrt{a} + q\sqrt{-c})^3$$

olacak şekilde p ve q tamsayıların bulunabilmesi dışında başka bir yol yoktur. Bu durumun ispatının tek ipucu AB bir küp ve eğer A ve B aralarında asal ise bu taktirde A ve B küp olmalıdır şeklindeki gerçektir. Bu teorem A ve B tamsayıları için ispatlanabilir. Ancak eğer A ve B $p + q\sqrt{-3}$ formunda ya da $x\sqrt{a} + y\sqrt{-c}$ formunda sayılar ise bu taktirde bu ispat artık uygulanamaz. Euler' in ifadesi $a = 1$, $c = 3$ özel halinde doğrudur. Ancak ispatı tamsayılar için olan ispattan oldukça farklıdır. Tabii ki teoremin yanlış olduğu a ve c değerleri de mevcuttur.

Euler'in "$x^2 + cy^2$ = küp" halindeki tartışması "$x^2 + cy^2$ = kare" durumunun tartışmasından daha kapsamlıdır. Bu tartışmada Euler, iki sayının çarpımı bir tam kare ise, buna pq diyerek, ya $p = r^2$ ve $q = s^2$ olacağını yani her bir çarpanın bir tam kare olacağını ya da çarpanların $p = mr^2$ ve $q = ms^2$ gibi bir tam karenin aynı sayı ile çarpılmış hali olacağını belirtmiştir. Bu ifade eğer bahsedilen sayılar tamsayılar ise doğrudur. Bu durum daha önce ispatlanmıştı. Ancak Euler aynı metodu tam sayı olmayan $x + y\sqrt{-c}$ formundaki sayılara da hemen uygulamıştır. Karelerin tartışması küplerin tartışmasından daha kapsamlıdır. Çünkü Euler $x^2 + cy^2$ bir tam kare ve x ve y aralarında asal iken belli a, b tamsayıları için

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

olduğunun alternatif bir ispatını da vermiştir. Bu ispatta Euler, p ve q tam sayıları için $x+\frac{p}{q}y$ olarak yazarak standart Diophant tekniğini kullanmıştır. Bu taktirde

$$\left(x+\frac{p}{q}y\right)^2 = x^2+cy^2$$

$$\frac{2p}{q}xy+\frac{p^2}{q^2}y^2 = cy^2$$

$$\frac{2p}{q}\cdot\frac{x}{y} = \frac{cq^2-p^2}{2pq}$$

$$\frac{x}{y} = \frac{cq^2-p^2}{2pq}$$

Ancak p ve q aralarında asal olduğundan x ve y aralarında asaldır, ve bundan dolayı $x = cq^2 - p^2$ ve $y = 2pq$ " oluşu gereği $-x + y\sqrt{-c} = (p + q\sqrt{-c})^2$ dir. Euler bu alternatif türetmenin, metodun doğruluğunu desteklediğini söylüyor, ancak p ve q nun aralarında asal oluşu şeklindeki kabul $cq^2 - p^2$ ve 2pq nun da aralarında asal olması anlamına gelmez ve bu nedenle de $x = cq^2 - p^2$, $y = 2pq$ şeklindeki Euler'in sonucunu gerektirmez. Aslında $49 = 2^2 + 5.3^2$ örneği sadece ifadenin şüpheli olduğunu göstermekle kalmayıp aynı zamanda sonucunda yanlışlığını gösterir. Çünkü

$$2 = 5q^2 - p^2, \quad 3 = 2pq$$

denklemlerinin p, q tamsayı çözümleri, hatta rasyonel sayı çözümleri bile yoktur.

(Dickson, 1971), $2x^2 - 5$ = bir küp denkleminin bir çözümünü bulmak için

$$x\sqrt{2} + \sqrt{5} = \left(a\sqrt{2}+b\sqrt{5}\right)^3$$

$$= 2a^3\sqrt{2} + 6a^2b\sqrt{5} + 15ab^2\sqrt{5} + 5b^3\sqrt{5}$$

yazmak gerektiğini ve sonuç olarak $x = 2a^3 + 15ab^2$, $1 = 6a^2b + 5b^3$ olacağını belirtmiş ve böylece en son denklemin $b = \pm 1$ ve $6a^2b + 5b^3 = \pm 1$ vereceğini belirtmiştir ki bu açıkça imkansızdır. Bundan dolayı $2x^2 - 5$ ifadesi $x = 4$ halinde bir küp olmasına rağmen bu metoda göre bir küp olamaz. Euler'in bu çelişkiye ilk yorumu bunun sebebinin oldukça önemli temellere dayanabileceği şeklindeydi. Euler'in bu noktada metodunun temel eksikliğini itiraf ettiğini ve bu eksiklik üzerinde çalışılması gerektiğini belirttiği anlaşılmaktadır. Bununla birlikte sonraki bölümde çok açık olarak anlaşılıyor ki Euler zorluğun temelinin $2x^2 - 5y^2$ deki eksi işaretine dayandığına ve $x = \pm 1$, $y = 0$

aşikar çözümünden başka çözümlere sahip olmayan $x^2 - 10y^2 = 1$ Pell denklemiyle bağlantılı olduğuna ikna olmuştu. Euler, işaretin pozitif olduğu hallerde her ne kadar $49 = 2^2 + 5.3^2$ durumunda metot başarısız olsa da genelde aynı zorluğun ortaya çıkmayacağından emin görünüyordu. Buna göre işaret pozitiftir ve $x^2 + 5y^2 = 1$ denkleminin yalnızca aşikar çözümü vardır.

Euler, 1753 yılında Goldbach'a gönderdiği mektubunda Fermat'nın Son Teoreminin $n = 3$ halini ispatlayabildiğini ifade etmiştir. Ancak yayınladığı tek ispat 1770 yılında yazdığı Algebra adlı kitabındakiydi. Bu hatalı ispat için mantıklı bir sebep aranırsa Euler'in orjinal metodunun, "$x^2 + 3y^2$ = küp" olmasının $x = a - 9ab$, $y = 3a^2b - 3b^3$ olmasını gerektirdiğini ispat etmek için daha az hayali bir tartışma kullandığını ve daha sonra bu metodun $(x + y\sqrt{-3})(x - y\sqrt{-3})$ nin bir küp ve $x + y\sqrt{-3}$ ve $x - y\sqrt{-3}$ çarpanları aralarında asal ise bu taktirde çarpanların kendilerinin de asal olmasının gerektiği şeklinde yanlış bir mantığa sahip olduğu görülebilir. Bu hipotez doğru olsun olmasın aslında Euler'in daha önceki çalışmaları $x^2 + 3y^2$ şeklindeki küplerle ilgili Lemmayı ispatlamak için zaten yeterlidir.

Euler'in $a + b\sqrt{-c}$ formundaki sayılar ile hesap yapma düşüncesi yukarıda sık sık kullanılan

$$(x^2 + cy^2)(u^2 + cv^2) = (xu - cyv)^2 + (xv + yu)^2$$

formülünün kullanılması ile yakından ilişkilidir. Bu formüle göre Eğer A tamsayısı B ve C tamsayılarının çarpımı ise ve B ve C sayıları $a^2 + cb^2$ formunda yazılabiliyorsa, $B = x^2 + cy^2$, $C = u^2 + cv^2$ denilerek A sayısı da

$$a + b\sqrt{-c} = (x + y\sqrt{-c})(u + v\sqrt{-c})$$

formülü kullanılarak bu formda yazılabilir ve böylece a, b sayıları belirlenebilir. Fermat'nın Son Teoremi $n = 3$ halinde ispatlamak için gereken Lemma, a ve b aralarında asal ve $a^2 + 3b^2$ bir küp iken belli p ve q tamsayıları için

$$a + b\sqrt{-3} = \left(p + q\sqrt{-3}\right)^3$$

olduğunu söyler. Bunu ispatlamak için $a + b\sqrt{-3}$ ü Euler'in düşüncelerini bir adım ileri götürerek aşağıdaki şekilde çarpanlara ayırmak doğaldır.

(1) Eğer a ve b aralarında asal ve $a^2 + 3b^2$ çift ise bu taktirde $a + b\sqrt{-3}$ sayısı u ve v tamsayılar ve işaret uygun şekilde seçilmek üzere

$$a+b\sqrt{-3} = \left(1 \pm \sqrt{-3}\right)\left(u+v\sqrt{-3}\right)$$

formunda yazılabilir. $a^2 + 3b^2$ çift olduğundan a ve b aynı halli olmalıdır, ve a ile b aralarında asal olduklarından her ikisi de tek sayı olmalıdır. Bundan dolayı her biri $4n \pm 1$ formundadır ve bu nedenle ya $a + b$ ya da $a - b$ 4 ile bölünmelidir. Eğer $4 \mid (a + b)$ ise bu taktirde

$$4(a^2 + 3b^2) = (1^2 + 3.1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3.(a + b)^2$$

sayısı 4^2 ile bölünebilir,

$$u = \frac{a-3b}{4} \quad , \quad v = \frac{a+b}{4}$$

iken

$$\frac{a^2+3b^2}{4} \quad \text{ifadesi} \quad u^2 + 3v^2$$

formunda yazılır. Bu denklemlerdeki a ve b, u ve v ye göre çözülürse bunların

$$u + v\sqrt{-3} = \left(a + b\sqrt{-3}\right)\frac{\left(1+\sqrt{-3}\right)}{4}$$

ifadesine denk olduğuna dikkat edilerek

$$\left(1-\sqrt{-3}\right)\left(u+v\sqrt{-3}\right) = a+b\sqrt{-3}$$

elde edilir. Aynı şekilde eğer $4 \mid (a - b)$ ise uygun u ve v için

$$a+b\sqrt{-3} = \left(1+\sqrt{-3}\right)\left(u+v\sqrt{-3}\right)$$

şeklinde ifade edilir. Dikkat edilirse u ve v aralarında asaldır (aksi halde a ve b aralarında asal olmazdı) ve

$$a^2 + 3b^2 = 4\left(u^2 + 3v^2\right)$$

dir.

(2) Eğer a ve b aralarında asal ve $a^2 + 3b^2$ bir P tek asal sayısı ile bölünebilirse bu taktirde P, p ve q pozitif tamsayı iken $P = p^2 + 3q^2$ formunda yazılabilir ve $a+b\sqrt{-3}$ sayısı u ve v tamsayılar ve işaret uygun şekilde seçilmek üzere

$$a + b\sqrt{-3} = \left(p+q\sqrt{-3}\right)\left(u+v\sqrt{-3}\right)$$

formunda yazılabilir. İlk ifade yani $P = p^2 + 3q^2$ ifadesi, bir önceki bölümde ifade edilen " Eğer a ve b aralarında asal ise bu taktirde $a^2 + 3b^2$ nin her tek çarpanı

$c^2 + 3d^2$ formundadır." İfadesi ile aynıdır. Euler'in ispatındaki gibi ya $pb + aq$ ya da $pb - aq$ P ile bölünebilir. Eğer $P \mid (pb + aq)$ ise bu taktirde

$$P.(a^2 + 3b^2) = (p^2 + 3q^2)(a^2 + 3b^2)\,(pa - 3qb)^2 + 3(pb + aq)^2$$

denklemi P^2 ile bölünebilir.

$$u = \frac{(pa - 3qb)}{P} \quad \text{ve} \quad v = \frac{(pb + aq)}{P}$$

için $\frac{a^2 + 3b^2}{P}$ ifadesi $u^2 + 3v^2$ formunda yazılabilir. Yani

$$u + v\sqrt{-3} = \left(p + q\sqrt{-3}\right).\frac{\left(a + b\sqrt{-3}\right)}{P}$$

şeklindedir. Buna göre $p - q\sqrt{-3}$ ile çarpma, istenildiği gibi

$$\left(p - q\sqrt{-3}\right)\left(u + v\sqrt{-3}\right) = a + b\sqrt{-3}$$

denklemini verir. Aynı şekilde, eğer $P \mid (pb - aq)$ ise bu taktirde

$$a + b\sqrt{-3} = \left(p + q\sqrt{-3}\right)\left(u + v\sqrt{-3}\right)$$

olur. Yine u ve v aralarında asal ve

$$a^2 + 3b^2 = P\,(u^2 + 3v^2)$$

dir.

(3) a ve b aralarında asal olsun. Bu taktirde $a + b\sqrt{-3}$ sayısı, p ler ve q lar pozitif tamsayılar ve $p_i^{\,2} + 3q_i^{\,2}$ ya 4 ya da bir tek asal iken

$$a + b\sqrt{-3} = \left(p_1 \mu q_1\sqrt{-3}\right)\left(p_2 \mu q_2\sqrt{-3}\right)\cdot\ldots\cdot\left(p_n \mu q_n\sqrt{-3}\right)$$

şeklinde yazılabilir. Eğer $a^2 + 3b^2$ çift ise bu taktirde 4 ile bölünebilirdir. Eğer $a^2 + 3b^2$, 1 değilse bu taktirde ya 4 ya da bir tek asal sayı olan bir P çarpanına sahip olur ve de ya (1) ya da (2) den $p^2 + 3q^2 = P$ iken

$$a + b\sqrt{-3} = \left(p \mu q\sqrt{-3}\right)\left(u + v\sqrt{-3}\right)$$

bulunur. Böylece u ve v aralarında asaldır ve $u + v\sqrt{-3}$ ün bir $p \mu q\sqrt{-3}$ çarpanını alma problemi $u^2 + 3v^2 = a^2 + 3b^2$ nin $a^2 + 3b^2$ den küçük oluşu dışında $a + b\sqrt{-3}$ ten bir çarpan almayla aynıdır.

Bu işlemi ardı ardına uygulayarak sonuçta $u^2 + 3v^2 = 1$ olmak üzere

$$a + b\sqrt{-3} = \left(p_1 \mu q_1\sqrt{-3}\right)\left(p_2 \mu q_2\sqrt{-3}\right)\cdot\ldots\cdot\left(p_n \mu q_n\sqrt{-3}\right)\left(u + v\sqrt{-3}\right)$$

aşamasına ulaşılmalıdır. Bu taktirde $u = \pm 1$, $v = 0$ olup , $u+v\sqrt{-3} = \mu 1$ olur ve çarpanlara ayırma işlemi tamamlanır.

(4) a ve b aralarında asal olsun. Bu taktirde $a+b\sqrt{-3}$ ün yukarıdaki ayrışımı

$$\left(p_1^{\,2}+3q_1^{\,2}\right)\left(p_2^{\,2}+3q_2^{\,2}\right)\cdot\ldots\cdot\left(p_n^{\,2}+3q_n^{\,2}\right)=a^2+3b^2$$

ifadesinin 4 lerin ve tek asal sayıların çarpımı oluşu sebebiyle işaretlerin seçimi hariç tamamen belirlidir. Dahası eğer $p+q\sqrt{-3}$ çarpanı bu çarpımda ortaya çıkıyorsa bu taktirde $p-q\sqrt{-3}$ çarpanı ortaya çıkmaz ve tersi de doğrudur. İlk ifadede ispatlanacak şey : $P = 4$ veya bir tek asal sayı ise $p^2 + 3q^2 = P$ nin işarete göre p ve q yu belirttiğidir. Bu $P = 4$ durumunda açıktır. Eğer P bir tek asal ve $a^2 + 3b^2$ de onun farklı bir temsili olsaydı bu taktirde (2) den dolayı

$$a+b\sqrt{-3}=\left(p\,\mu\,q\sqrt{-3}\right)\left(u+v\sqrt{-3}\right)$$

ve

$$P = P\,(u^2 + 3v^2)$$

olurdu. Yani gösterilmek istendiği gibi

$$u^2 + 3v^2 = 1, \quad u = \pm 1, \quad v = 0, \quad a+b\sqrt{-3} = \mu\left(p\,\mu\,q\sqrt{-3}\right)$$

bulunurdu. İkinci ifade ise $p+q\sqrt{-3}$ ve $p-q\sqrt{-3}$ çarpılıp bir $p^2 + 3q^2$ çarpanı elde edileceği yönündedir ki bu eğer a ve b aralarında asal ise imkansızdır.

Fermat'nın son teoreminin $n = 3$ halinin Euler tarafından verilen ispatını tamamlamak için gereken lemma şimdi daha kolay sonuçlandırılabilir.

2.2.1. Lemma : a ve b sayıları, $a^2 + 3b^2$ bir küp olabilecek şekilde aralarında asal sayılar olsun. Bu taktirde $a+b\sqrt{-3} = \left(p+q\sqrt{-3}\right)^3$ olacak şekilde p ve q tamsayıları vardır.

İspat : $a^2 + 3b^2 = P_1.P_2 \ldots P_n$ şeklinde 4 lere ve tek asal çarpanlarına (4) deki gibi ayrılmış olsun, eğer bu ayrışım tam olarak k tane 4 çarpanı bulunduruyorsa bu taktirde 2^{2k} 2 nin $a^2 + 3b^2$ yi bölen en büyük kuvveti olur. $a^2 + 3b^2$ bir küp olduğundan bu, 2k ve buna bağlı olarak ta k nın 3 ün bir katı olması anlamına gelir. Ayrıca ayrışımdaki herhangi bir P tek asalı 3 ün bir katı kez ortaya çıkmalıdır. Böylece n 3 ile bölünebilirdir ve $P_1P_2 \ldots P_n$ çarpanları $P_{3k+1} = P_{3k+2} = P_{3k+3}$ şeklinde düzenlenebilir.

Böylece $a+b\sqrt{-3}$ ün (3) de verilmiş olan ayrışımından her bir üçlü grubuna karşılık gelen çarpanlar özdeştir. Çünkü $p \mu q\sqrt{-3}$ ün işaretinin seçimi önemlidir ve her iki işaret aynı anda ortaya çıkamaz. Bu üç grubun her birinden bir çarpan almak ve onları çarpmakla

$$a+b\sqrt{-3} = \mu\left(c+d\sqrt{-3}\right)^3$$

olacak şekilde bir $c+d\sqrt{-3}$ sayısı bulunur.

$$-\left(c+d\sqrt{-3}\right)^3 = \left(c-d\sqrt{-3}\right)^3$$

olduğundan istenen sonuç görülür.

2.3. n = 5 ve n = 7 halleri

n = 3 ve n = 4 durumlarından sonra ispatlanacak olan iki durum n = 5 ve n = 7 durumlarıdır. İlk durum ile yani n = 5 durumu ile 1825 yılında Legendre ve Dirichlet uğraşmıştır. n = 7 durumu ise 1840 yılında Lame ve Lebesque tarafından ispatlanmıştır. İspatlar n = 3 durumundan çok farklı fikirler bulundurmaz ve iki esasa dayalıdır. İlk olarak eğer p bir asal sayı ve x ile y aralarında asal ise

$$x+y \quad ve \quad \frac{x^p+y^p}{x+y}$$

ifadeleri ya aralarında asal ya da yalnızca p nin birinci kuvveti olan bir ortak çarpana sahip olmaları durumu ele alınır.

$$x + y = s$$

denilirse verilen iki ifade

$$s \quad ve \quad \frac{x^p+(s-x)^p}{s}$$

ya da

$$s \quad ve \quad s^{p-1} - p\cdot s^{p-2}\cdot x + \frac{p.(p-1)}{2}\cdot s^{p-3}\cdot x^2 + \ldots + \frac{p.(p-1)}{2}\cdot s\cdot x^{p-2} + p\cdot x^{p-1}$$

halini alır. Bu ifadelerdeki s ile x inde aralarında asal oluşundan Jaquement (1651-1729) tarafından verilen bu sonuç doğrudur.

İkinci bir gerçek ise $\frac{x^p + y^p}{x+y}$ nin U ve V, x ve y nin polinomları iken

$$\frac{1}{4}\left[u^2 - (-1)^{\frac{p-1}{2}} \cdot p \cdot v^2 \right]$$

formunda yazılabilir olmasıdır. Ancak ispat, ilk durum için olandan çok daha karmaşık olduğundan burada verilmemiştir. n = 5 ya da n = 7 olduğu özel durumlarda basit cebirsel işlemler ile U ve V yi bulmak zor değildir.

n = 5 durumunda

$$z^5 = (x+y)\left(\frac{x^5 + y^5}{x+y}\right)$$

ya da U ve V, x ve y nin ikinci dereceden fonksiyonları olmak üzere

$$z^5 = (x+y)\left(\frac{u^2 - 5v^2}{4}\right)$$

yazarız. Yukarıdakilerden Z^5 için verilen bu eşitlikte sağ taraftaki iki çarpanın ya aralarında asal olduğu ya da $\frac{u^2 - 5v^2}{4}$ ü bir kez bölen bir 5 ortak çarpanına sahip olacağı görülür. Bu taktirde

$$\frac{1}{4}(U^2 - 5V^2) = W^5 \quad ya\ da \quad 5W^5$$

formunda bir denkleme sahip oluruz. n = 3 durumunda ortaya çıkan ve Euler'in gözden kaçırdığı zorluk bu denklemlerin tartışmasında ortaya çıkar. Ancak benzer metotlarla bu zorluktan kaçınılabilir. Böylece n = 5 durumunun da imkansız olduğu sonucu görülür. Benzer bir metot n = 7 durumunda da uygulanır. Ancak bu n = 5 durumundan daha çok cebirsel işlem gerektirir.

3. FERMAT'NIN DİĞER SAYI TEORİK BULUŞLARI

Fermat'nın ispatlanmamış bir çok iddiası ondan sonraki matematikçilere bir meydan okuma olarak kalmıştır. Kendinden hemen sonra gelen jenerasyondan olan Wallis ve diğerlerinin dikkatini çekmemesine rağmen daha sonraları özellikle Euler ile başlayan jenerasyon bu iddiaları ispatlamaya ya da çürütmeye gayret ettiler ve $2^{32} + 1$, $2^{64} + 1$, $2^{128} + 1$, ... sayılarının asal oluşu dışındakilerin hepsinin doğru olduğunu buldular. Bu iddialar yukarıda tartışılanlar dışında direkt olarak Fermat'nın son teoremi ile ilgili değildir ve burada detaylı olarak ele alınmayacaklardır. Ancak burada, yalnızca Fermat'nın çalışma alanı hakkında bir fikir vermek için bazılarından bahsedilecektir. Bu iddialardan Diophant tarafından kapalı olarak verilen ve Bachet'in Diophant ile ilgili açıklamalarında açık olarak ifade edilmiş olanı her sayının dört tane tam karenin toplamı olarak yazılabileceği şeklindedir. Fermat yalnızca bu ifadeyi değil genel hali de ispatlayabildiğini iddia etti. Bu genel hal ise her sayının üçgensel sayıların toplamı ya da dört tane tam karenin ya da beş tane beşgensel sayının ya da altı tane altıgensel sayının toplamı olarak yazılabileceği idi. Burada üçgensel sayılar 0, $0 + 1 = 1$, $1 + 2 = 3$, $3 + 3 = 6$, $6 + 4 = 10$, $10 + 5 = 15$ şeklindedir. Dörtgensel sayılar 0, $0 + 1 = 1$, $1 + 3 = 4$, $4 + 5 = 9$, $9 + 7 = 16$, $16 + 9 = 25$ ve beşgensel sayılar ise 0, $0 + 1 = 1$, $1 + 4 = 5$, $5 + 7 = 12$, $12 + 10 = 22$, $22 + 13 = 35$ gibidir. Genel olarak 0, 1, a_2, a_3, a_4, ... n – gen sayıları 1, n – 1, 2n – 3, 3n – 5, ... aritmetik dizisinin terimlerini ardışık olarak ekleyerek bulunur. Yani $a_0 = 0$, $a_1 = 1$, $a_2 = n$, $a_3 = 3n - 3$, $a_4 = 6n - 8$, $a_5 = 10n - 15$, ... , $a_j = ½\, j(j - 1)n - j(j - 2)$ şeklindedir. Bu güzel teorem daha sonra matematik tarihindeki büyük isimlerin bazılarının dikkatini çekti. Tam kare olan dörtgensel sayılar için ifadeyi ilk ispatlayan Lagrange idi. Gauss üçgensel sayılar için ispat yaptı ve Cauchy genel durumu ispatlayan ilk kişiydi.

Fermat'nın ispatlanmamış ifadelerinden biri de $25 + 2 = 27$ sayısının

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

denkleminin tam sayılardaki tek çözümü olduğu ve benzer olarak $4 + 4 = 8$, $121 + 4 = 125$ ifadelerinin de

$$x^2 + 4 = y^3$$

denkleminin tamsayılardaki tek çözümleri olduğudur. Bu basit ifadeler durup dururken ortaya çıkmış gibidir ve ispatlarını verecek doğal bir yol yok gibi görünebilir. Buna benzer bir başka ifade de $1 + 1 + 1 + 1 = 4$ ve $1 + 7 + 49 + 343 = 400$ sayılarının $1 + x + x^2 + x^3 = y^2$ denkleminin tek çözümleri olduğunu söyler.

Wallis ve diğer İngiliz matematikçilerine Pell denklemini çözme konusundaki meydan okuması aslında Fermat' ın ikinci meydan okumasıydı. Birinci meydan okuma daha zordur ve İngilizlerce pek önemsenmemiştir. Bu, iki problemden meydana gelir: (1) has bölenlerine eklendiğinde tam kare veren bir küp bulma . Örnek olarak 343, kendisinin has bölenleri eklendiğinde $343 + 49 + 7 + 1 = 400$ tam karesini verir. (2) has bölenlerine eklendiğinde bir küp veren bir tam kare bulma. Bu problemlerin çözümleri Dickson'ın History of the Numbers adlı kitabının ikinci cildinde mevcuttur.

Fermat'nın Euler'e esin kaynağı olan bir başka problemi de şudur: İki küpün toplamı olan bir sayı verilsin. O sayıyı iki küpün toplamı olarak bir başka yolla yazabilir miyiz? Bu küpler rasyoneldir. Ancak paydalar sadeleştirilerek problem pozitif tamsayılarda $x^3 + y^3 = u^3 + v^3$ denkleminin tüm çözümlerini bulma problemine dönüştürülür. Fermat'nın meydan okuduğu Frenicle, deneme yanılma yoluyla $1729 = 9^3 + 10^3 = 1^3 + 12^3$ ve $40033 = 16^3 + 33^3 = 9^3 + 34^3$ gibi çeşitli çözümler bulmuştur. İfadesi basit ancak ispatı o kadar da basit olmayan bir başka teorem ise 1 den büyük üçgensel hiçbir sayının aynı zamanda dördüncü kuvvet olamayacağıdır. Diğer bir deyişle $x > 2$ için

$$\frac{1}{2}x(x-1) = y^4$$

denkleminin tam sayılarda çözümü yoktur. Bu durumun ilk yayınlanan ispatı yaklaşık 150 yıl sonra Legendre'in Theorie des Nombres kitabında yer almıştır.

ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu çalışmada Fermat'nın son teoreminin en çok bilinen özel halleri için verilmiş olan ispatlar bir araya getirilmiştir. Ayrıca Fermat'nın son teoreminin $n > 2$ şartı altında ifade edilmesine rağmen çalışmanın 1. bölümünde teoremin ortaya çıkması için temel oluşturan $n = 2$ hali yani Pisagor üçgenleri ile ilgili bazı yeni sonuçlar elde edilmiştir.

Herhangi bir pozitif tamsayı verildiğinde bu sayının asal, tek ya da çift oluşuna bağlı olarak kaç Pisagor üçgeninde dik kenar ya da hipotenüs olabileceğine dair literatürde var olan bir kaç yönteme ek olarak yeni bir sonuç ifade edilmiştir. Bu sonuca göre:

$x > 2$ asal verildiğinde x in dik kenar olduğu bir tek Pisagor üçgeni vardır.Bu dik üçgende hipotenüs, $z = (x^2 + 1) / 2$ diğer dik kenar ise $y = (x^2 - 1) / 2$ dir.

Eğer x bir pozitif tek tamsayı ise w, x in pozitif bölenlerinin sayısını göstermek üzere x in dik kenar olduğu Pisagor üçgenleri $(w-1)/2$ tanedir.

Eğer x bir çift pozitif tamsayı ise v, x in tek sayı bölenlerinin sayısı olmak üzere x in dik kenar olduğu Pisagor üçgenleri $(w-1)/2 - v$ tanedir.

Sonuç olarak bu çalışmada, Fermat'nın son Teoreminin bazı özel hallerinin ispatları bir araya getirilmiştir. Böylece daha sonraki aşamada teoremin genel halinin incelenmesi ve ispatın matematiğin diğer alanları ile ilişkisinin ele alınması amaçlanmıştır.

KAYNAKLAR

ACZEL, A.D. 1997. Fermat's Last Theorem, Delta Boks, New York., 147 p.

BEILER, A.H. 1966. Recreations in The Theory of Numbers, The Queen of Mathematics entertains, Dover, New York, 104-134

DARMON, H., L. MEREL. 1997. Winding quotients and some variants of Fermat's Last Theorem, J. reine angew. Mathematics, 490, 81-100

DICKSON, L. E. 1971. History of the Theory of Numbers, Chelsea Pub. Co., New York.

EDWARDS, H. M. 1977. Fermat's Last Theorem. Springer-Verlag., 410 p.

FIBONACCI, L. P. 1987. The Book of Squares, Academic Pres, Orlando, 124 p.

JONES, G. A., J. M. JONES. 1998. Elementary Number Theory, Springer, London, 191- 237

İNTERNET, 2001. Fermat's Last Theorem
http://www.history.msc.st-and.ac.uk/history/

İNTERNET, 2001. Fermat's Last Theorem
http://www.intipress.com/books/math/fermat5.jpg

KLEINER, I., 2000. From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem. Elem. Math., 55, 19-37

LE,M. 2002. On Cohn's conjecture concerning the diophantine equation $x^2 + 2^m = y^n$. Arch. Math., 78, 26-35

MORDELL, L. J. 1962. Three Lectures On Fermat's Last Theorem, Ders Notları

RIBENBOIM, P. 1999. Fermat's Last Theorem for Amateurs. Springer, New York

SINGH, S. 2001. Fermat'nın Son Teoremi (Çeviri: Yücesoy, S.). Pam Yayıncılık, İstanbul, 328 s.

WILES, A. 1995. Modular Elliptic Curves and Fermat's last Theorem, The Annals of Mathematics, 2nd Ser., Vol. 141, No. 3. 443-551.

TEŞEKKÜR

Bugün Matematik biliminde bir çalışma yapabilecek konuma gelebilmem için imkanlarını zorlayan aileme ve bu çalışmanın ortaya çıkması aşamasında bana karşı destek, güven ve sabrını eksik etmeyen eşime, ayrıca çalışmayı yöneten ve gereken her türlü yardımı sağlayan sayın hocam Doç.Dr. İsmail Naci CANGÜL'e minnet ve teşekkürlerimi sunarım.

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

ÖZGEÇMİŞ

08.01.1978 yılında Sakarya Karasu'da doğdu. İlkokul ve Ortaokulu Sakarya İsmet İnönü İlköğretim Okulunda, liseyi Sakarya Ali Dilmen Lisesinde okudu. 1995 yılında Muğla Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünde Lisans eğitimine başladı. 1997 yılında Uludağ Üniversitesi Fen- Edebiyat Fakültesi Matematik Bölümüne yatay geçiş yaptı ve 2000 yılında mezun oldu. Aynı yıl Uludağ Üniversitesi Fen Bilimleri Enstitüsünde Yüksek Lisansına ve aynı zamanda Uludağ Üniversitesi Fen- Edebiyat Fakültesi Matematik Bölümünde Araştırma Görevliliğine başladı. Halen bu göreve devam etmektedir.