Asallar, Spiraller ve Cebir

Ayberk Zeytin / ayberkz@gmail.com
Begüm Gülşah Çaktı / begumcakti@gmail.com

1 Goldbach ve İkiz Asallar Sanısı

İlkokul sıralarında hepimiz defterimize yazmışızdır. Asal sayılar, "sadece 1'e ve kendisine bölünebilen doğal sayılar"dır. Ders dışında yüzüne bakmadığımız bu "basit" tanımının aksine günlük hayatımızda çok önemli bir yeri vardır asalların. Özünde bilgisayarsız, tabletsiz, telefonsuz (aslında internetsiz) yaşayamayan birçoğumuzun minnet duyması gereken sayılar denilebilir. Bulunduğumuz teknoloji çağında haberleşmelerimizin (e-posta, vs.) veya bankaların internet şubelerinde yaptığımız işlemlerin gizliliğini, çevrimiçi yapılan alışverişlerin güvenliğini, en azından şimdilik, onlara borçluyuz. Buna karşılık, bu özel sayılarla ilgili bildiklerimiz; buzdağının sadece görünen kısmıdır. Görünmeyen kısmında ise çok büyük soru işaretleri ve bolca gizem vardır.

Akla gelen ilk sorulardan bir tanesi şu gözlemler dizisinde yatmaktadır:

$$6 = 2 + 2 + 2$$
$$7 = 2 + 2 + 3$$
$$8 = 2 + 3 + 3$$
$$9 = 3 + 3 + 3$$
$$10 = 2 + 3 + 5$$
$$11 = 3 + 3 + 5$$
$$12 = 2 + 3 + 7$$

Goldbach, Euler'e yazdığı mektupta aşağıdaki sanıyı (Zayıf Goldbach sanısı) ortaya koyar:

Beşten büyük her doğal sayı üç tane asal sayının toplamı biçiminde yazılabilir.

Bunun ardından Euler iddianın daha güçlü bir hali olan şu sanıyı ortaya koyar: İkiden büyük veya ikiye eşit her çift doğal sayı iki tane asal sayının toplamı formunda yazılabilir. Günümüzde 1'i asal sayı olarak kabul etmediğimiz için bu sanıyı literatürde aşağıdaki hali ile yer almaktadır:
Goldbach Sanısı: İkiden büyük her çift doğal sayı iki tane asal sayının toplamı formunda yazılabilir.

Sanıyı desteklemesi için yine birkaç örnek verelim:

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 3 + 5$$
$$10 = 3 + 7$$
$$12 = 5 + 7$$
$$14 = 7 + 7$$

Goldbach ve Euler'in iddialarını "zayıf" ve "güçlü" olarak sınıflandırmamızın sebebi, Güçlü Sanı'nın Zayıf Sanı'yı gerektirmesidir. Bunun nedenine bakalım:

5'ten büyük bir n doğal sayısı alalım ve bu sayıdan 3 çıkararak 2'den büyük bir doğal sayı, m, elde etmiş olalım. Eğer güçlü sanı doğru ise şayet m doğal sayısı iki tane asal sayının toplamı şeklinde yazılabilir. Bu asallar p_1 ve p_2 olsun. Dolayısıyla $n = (n-3)+3$ sayısı p_1, p_2 ve 3'ün toplamı; yani üç tane asalın toplamı şeklinde yazılabilir. Bu yüzden Güçlü Sanı doğru ise Zayıf Sanı da doğrudur.

Harald Andrés Helfgott zayıf sanıyı ispatladığını 2013 yılının sonunda, "The ternary Goldbach conjecture is true" başlıklı makalesi ile ilan etmiştir. Bu makale yazıldığı esnada ispatın doğruluğu halen kontrol edilmekteydi. Bu tabii ki güçlü sanıyı desteklemesi açısından çok önemli bir adım olsa bile güçlü sanı halen çözünü beklemektedir.

Asal sayılarla ilgili diğer bir problem ise ikiz asallar sanısıdır. Bu sanıyı ifade edebilmek için bir tanımla başlayalım:

Tanım 1.1. *Bir n doğal sayısı için hem n hem de $n+2$ bir asal sayı oluyorsa $(n, n+2)$ ikilisine* ikiz asallar *denir.*

$(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$ ikiz asallara örnektir. Adı her ne kadar geometri ile özdeşleşmiş olda da "Sonsuz tane ikiz asal vardır."şeklinde ifade edilen *İkiz Asallar Sanısı*'nı ilk ortaya atanın Öklid olduğu düşülmektedir. Probleme yaklaşım asal sayıların arasındaki mesafelerin anlaşılması üzerine odaklanmaktadır. Cem Yalçın Yıldırım ve çalışma arkadaşları henüz ispatlanmamış olan Elliot-Halberstam sanısının doğruluğunu kabul ederek aralarındaki fark 16 olan sonsuz tane asal sayının varlığını ispatlamışlar ve bu çalışmalarıyla Frank Nelson Cole Ödülüne layık görülmüşlerdir. Konu üzerinde makale yazıldığı esnadaki en güncel sonuç Yitang Zhang'in çalışmaları

kullanılarak elde edilmiştir. Buna göre aralarında 246 fark olan sonsuz tane asal vardır.

2 İkinci Dereceden Tek Değişkenli Polinomlar ve Asallar

Genel sonuçları an için bir kenara bırakalım. Cahil cesareti ile kendimize ilk olarak şu soruyu soralım: öyle bir tamsayı katsayılı p polinomu var mıdır ki her n doğal sayısı için $f(n)$ bir asal sayı olsun*? Bu araştırma için polinomları derecelerine göre sınıflayalım. Derecesi 0 olan polinomlar elbette ki hemen elenecekler. Derecesi 1 olan bir p polinomu $p(x) = ax + b$ şeklinde yazılabilir. Polinomun değerlerinin pozitif kalması için $a > 0$ olmalıdır. Her n doğal sayısı için $p(n) = p_n$'in asal sayı olduğunu varsayarsak tüm asal sayılar a modunda birbirine (ve dolayısıyla b'ye) denk olmalıdır. Bu $p(0) = p_0 = b$'ninde asal sayı olmasını gerektirir. $f(b) = ab+b = (a+1)b$ de varsayımımız gereği asal olmalıdır. Çelişki!

Dolayısıyla böyle bir polinomun derecesi ikiden büyük veya eşit olmalıdır. Tamsayı katsayılı polinomların kümesini $\mathbb{Z}[x]$ ile gösterelim. Genel durumu incelerken kullanacağımız bir kaç tanıma ihtiyacımız var:

Tanım 2.1. *$p(x)$ tamsayı katsayılı bir polinom olsun, yani $p(x) \in \mathbb{Z}[x]$ olsun. Her x tamsayısı için $p(x + k) = p(x)$ eşitliğini sağlayan sıfırdan farklı bir k tamsayısı var ise $p(x)$ polinomuna* periyodik polinom *denir.*

Lemma 2.2. *Hiçbir tamsayı katsayılı ve sabit olmayan polinom periyodik değildir.*

Kanıt. $p(x) \in \mathbb{Z}[x]$ sabit olmayan ve periyodik bir polinom olsun. a_i'ler gerçel sayı olmak üzere $p(x) := \sum_{i=0}^{n} a_i x^i$ şeklinde yazalım. $p(x)$ periyodik olduğu için öyle bir k tamsayısı bulabiliriz ki her x tamsayısı için $p(x + k) = p(x)$ olur. Dolayısıyla her m doğal sayısı için:

$$\begin{aligned} 0 &= p(0 + m \cdot k) - p(0) \\ &= a_1(m-1)(x) + a_2(m^2-1)x^2 + ... \\ &+ a_n(m^n - 1)x^n \end{aligned}$$

eşitliğini elde ederiz. Yukarıdaki polinomu x yerine m'nin bir polinomu olarak görecek olursak, her m doğal sayısı ve her x için 0 olan bir polinom elde etmiş oluruz; başka bir deyişle her ν doğal sayısı için $p(\nu) = 0$ olur, i.e. $m-\nu$ polinomu $p(m)$ polinomunu böler. Bu da p polinomunun m değişkenine göre derecesinin sonsuz olduğu anlamında gelir ki bir polinomun derecesi en fazla sonlu olabilir. Çelişki! □

Lemma 2.3. *$p(x)$ tamsayı katsayılı bir polinom, q ve ν birer doğal sayı olsun. Eğer $p(\nu) \equiv 0 \pmod q$ ise her k doğal sayısı için $p(\nu + kq) \equiv 0 \pmod q$ olur.*

Kanıt. $p(x)$ polinomunu $p(x) := \sum_{i=0}^{n} a_i x^i$ şeklinde yazalım. O halde

$$\begin{aligned} p(\nu + kq) &= \sum_{i=0}^{n} a_i(\nu + kq)^i \\ &= a_0 + a_1(\nu + kq) + a_2(\nu + kq)^2 + \dots \\ &+ a_n(\nu + kq)^n \\ &= a_0 + a_1(\nu + kq) \\ &+ a_2(\nu^2 + 2\nu kq + k^2q^2) + \dots \\ &+ a_n[\nu^n + \binom{n}{1}\nu^{n-1}kq + \dots \\ &+ \binom{n}{n-1}\nu(kq)^{n-1} + k^n q^n] \\ &= a_0 + a_1\nu + a_2\nu^2 + \dots + a_n\nu^n \\ &+ q\left(a_1 k + a_2(2k + k^2 q) + \dots +\right) \\ &+ q\left(\binom{n}{1}\nu^{n-1}k + \dots\right) \\ &+ q\left(\binom{n}{n-1}\nu k^{n-1}q^{n-2} + k^n q^{n-1}\right) \\ &= p(\nu) + qM \end{aligned}$$

olur. Yani $p(\nu + kq) \equiv p(\nu) \pmod q$. □

Yukarıdaki gözlemlerimizin direkt sonucunu vermeye artık hazırız:

Teorem 2.4. *Hiçbir tamsayı katsayılı ve sabit olmayan polinom her n doğal sayısı için asal sayı üretemez.*

Kanıt. Böyle bir $p(x)$ polinomunun varlığını kabul edelim. Herhangibir ν doğal sayısı için $p(\nu) = p_o$ bir asal sayı olsun. Lemma 2.3 bize her k tamsayısı için p_o asal sayısının $f(\nu + kp_o)$ sayısını böldüğünü söyler. Öte yandan $p(x)$ polinomu sabit olmadığı için Lemma 2.2 bize $p(x)$'in periyodik de olamayacağı sonucunu verir. Dolayısıyla $p(\nu + kp_o)$ bir asal sayıya eşit olamaz. Çelişki! □

Teorem elbette ki yapılan araştırmaların sonunu değil sadece yeni bir başlangıcı işaret ediyor. Örneğin okuyucuyu Teorem 2.4'i rasyonel fonksiyonlar yani iki tamsayı katsayılı polinomun

*Katsayıların gerçel olmasına müsaade edersek elde edilecek polinomun değerlerinin bırakın asal sayı olmayı tamsayı olmasını bile beklemek hayalperestlik olurdu.

bölümü şeklinde yazılan fonksiyonlar için de genellemeye davet ediyoruz. Bu gerçekler bizi asal üreten fonksiyon aramaktan oldukça uzaklaştırıyor. Yine de umuyoruz aşağıdaki gözlemleri siz de bizim kadar şaşırtıcı bulursunuz:

- $p(x) = 2x^2 + 11$ polinomu için $p(0) = 11, p(1) = 13, \ldots, p(10) = 211$ sayılarının hepsi asaldır.
- $p(x) = -66x^3 - 3485x^2 - 60897x + 251831$ polinomu için $p(0) = 251831, p(1) = 194713, \ldots, p(45) = -716659$ sayılarının hepsi asaldır.
- $p(x) = x^4 + 29x^2 + 101$ polinomu için $p(0) = 101, p(1) = 131, \ldots, p(19) = 140891$ sayılarının hepsi asaldır.

Yukarıdaki listeyi uzatmak elbette ki mümkün. Meraklı okuyucuyu:
`http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html`
sitesini ziyaret etmeye davet ediyoruz. Polinomları tekrar ziyaret etmek üzere bırakıyoruz. Sizlerle birlikte şimdi başka tesadüfleri incelemeye koyulalım.

3 Ulam Spirali

Bu ve önümüzdeki bölümde doğal sayıları alışageldiğimiz sayı doğrusu ve koordinat sisteminin dışındaki sistemlere -spirallere- oturtaca ğız ve asal sayıları işaretleyerek gözlemler yapacağız. Şimdiden söylemeliyiz ki şaşırtıcı sonuçlara şahit olacağız.

İlk olarak *Ulam Spirali*'ni ele alalım. 1963 yılında "modelleyicisi" matematikçi Stanislaw Ulam'ın katıldığı sıkıcı bir toplantıda defterinde yaptığı karalamalar sonucu ortaya çıktığı rivayet edilen spirali elde etmek için kareli bir sayfa alalım. Sayfanın tam ortasındaki kareye 1, bunun hemen yanındaki (buradaki seçim tamamen bize ait, biz soldan sağa doğru yazmaya alıştığımız için Resim **??**'de 1'in sağına yazdık) kareye 2, 2'nin üstündeki kareye 3, 3'ün solundaki kareye 4, 4'ün yine solundaki kareye 5, 5'in altındaki kareye 6 yazıp bu şekilde devam ederek Ulam Spirali'ni elde edebiliriz.

Şimdi ise asallara daha geniş çerçeveden bakma zamanı. Aynı spirali çok daha büyük doğal sayılara kadar ilerletip asal sayıları işaretlediğimizde Resim **??** karşımıza çıkıyor. Siyahlar asalları, boşluklar ise asal olmayan doğal sayıları temsil ediyor.

Makalemizin başından beri amacımız, asal sayıları anlamak ve bu sayıların davranış biçimlerini -dağılımlarını- incelemek. Tabloya baktığımızda, milattan önceye dayanan tarihsel sürece rağmen matematikçilerin bugün bile tam olarak anlamlandıramadığı asal sayılar arasındaki ilişki ve düzen aslında bu kadar net. Spirale bakıp etkilenmemek geometriye çok büyük bir haksızlık olur diye düşünüyoruz.

Birazdan gözlemlerimize başlayacağız ama öncelikle akıllara şu soru gelmiş olabilir: Spirali neden 1'den başlatıyoruz? Örneğin negatif tamsayılardan başlatamaz mıydık? Elbette ki başlatabilirdik ama ilkokuldan beri öğrendiğimiz o "malum" tanımda asal sayıları doğal sayıların bir alt kümesi olarak tanımladığımız için negatif tamsayıları spiralde gözlemlemek pek de mantıklı bir hareket olmazdı. Spirali 0'dan değil de 1'den başlatmak ise Ulam için tercihten öte bir durum değildi. Yeri gelmişken belirtelim, 0'ın bir doğal sayı olup olmadığı matematikçiler açısından ciddi bir tartışma konusudur. İlgili okuyucuların bu soruya felsefi açıdan ve matematik açısından bakması, bu sorunun üzerine düşünmesi matematiksel olgunluk kazanımı açısından güzel bir alıştırma olabilir. Biz de ileride spirali farklı doğal sayılardan başlatıp asalların çizdiği düzenin tutarlı olup olmadığını inceleyeceğiz.

Söz verdiğimiz gibi gözlemlerimize başlayalım ve asal sayıların yoğunlukta olduğu bölgelere daha yakından bakalım. Gördüğümüz üzere asal sayıların yoğunlukta olduğu bölgeler doğrular/yarı doğrular şeklinde temsil edilebiliyor. Lise bilgilerimize dönersek, doğrular şu ana kadar bizim için "1. dereceden tek değişkenli polinom ve fonksiyonlar"ın geometriye yansımalarıydı. Öncelikle şunu not etmeliyiz ki spiralde şu an doğrular gözlemliyor olmamız, asal sayıları lineer; yani 1. dereceden polinomlarla rahatlıkla ifade edebileceğimiz anlamına gelmez. Doğal sayıların dizilimini tamamen farklı bir şekilde yaptığımız için doğrular elde ettik; aslında bu doğrular kuadratik, yani 2. dereceden polinomlarla elde edilebilir. Bunun nedenini makalemizin son bölümünde açıklayacağız. Daha spesifik bir bilinenden bahsetmek gerekirse bu doğrular:

$$4x^2 + bx + c, \quad b, c \in \mathbb{Z}$$

formundaki polinomlara karsılık gelirler. Spiral üzerinden birkaç örnek verecek olursak: $\{3, 13, 31, 57, ...\}$ sayılarını barındıran doğru $4x^2 - 10x + 7$ polinomunun, $\{5, 17, 37, 65, 101, ...\}$ doğrusu da $4x^2 + 1$ polinomunun değerlerindendir.

Lineer yapıları gözlemledikten sonra ikinci gözlemimize geçelim: Spirali daha dikkatli incelersek fark edeceğiz ki bu doğruları iki partisyona ayırmak mümkün çünkü bu doğruların eğimleri ya +1 ya da -1 olabiliyor. Bunun nedenine gelince, ne yazık ki fazla matematiksel bir açıklaması yok; spiralin tasarımından dolayı böyle bir sonuç elde ediyoruz.

Ulam Spirali'nin orijinal halini analiz ettikten sonra bu bölümün başında da bahsettiğimiz bir diğer aşamaya geçelim: Acaba spirali 1'den değil de başka bir doğal sayıdan başlatsaydık asalların arasındaki düzen yine bu kadar görünür olur muydu? Bu konudaki merakımızı gidermek için spirali aynı düzende oluşturmak şartıyla önce 5'ten, sonra da 12'den başlatalım ve asal sayıları işaretleyelim. Sırasıyla aşağıdaki tablolar karşımıza çıkar:

Görüldüğü üzere her iki durumda da asalların çizdiği doğrular, en az spiralin orijinal halinde olduğu kadar belirgin. Okuyucunun aynı spirali başka doğal sayılarla başlatarak incelemesi çizilen düzenin tutarlılığını gözlemleyebilmesi açısından bizce iyi bir deneyim olur. İpucu vermek gerekirse, sonuç her seferinde aynı şaşırtıcılıkta olacaktır. Bu konuda dikkatinizi son bir noktaya çekmek istiyoruz, spirali özel bir sayı olan 41'den başlatacağız. Bundan önce, 41'in neden özel olduğunu anlayabilmek için aşağıdaki tanıma ihtiyacımız var:

Tanım 3.1. *x^2+x+41 ve x^2-x+41 polinomlarına "Euler'in Asal Üreten Polinomları" denir.*

1772 yılında İsviçreli matematikçi Leonhard Euler'in keşfi olan Euler'in Asal Üreten Polinomları'nı bu kadar özel olmalarının sebebi, sırasıyla $x \in [0, 39]$, $x \in \mathbb{Z}$ ve $x \in [0, 40]$, $x \in \mathbb{Z}$ şartlarını sağlayan x değerleri için; yani 0'dan itibaren x'in ilk 40 ve 41 doğal sayı değeri için 40 farklı asal sayı üretmesidir.

Euler'in Asal Üreten Polinomları'nı tanıdıktan sonra Ulam Spirali'ni 41'den başlatarak çizmeye başlayabiliriz:

Sonuç bizce görsel olarak çok etkileyici. Gördüğünüz üzere $x^2 + x + 41$ polinomunun yukarıdaki şartları sağlayan ilk 40 değeri spiralde "köşegen" olarak adlandırabileceğimiz doğruda yer alıyor.

Başta söz verdigimiz gibi, şimdi de biz karesel bir spiral olusturalım ve asalların yoğun oldugu doğruların eğimlerini farkli bulup bulamayacağımıza bakalım. Biz de Ulam Spirali'nin orijinal halini koruyalım ve doğal sayıları ayni şekilde konumlandıralım. Tek bir değişiklik yapalım, o da spirale çift sayıları dahil etmemek olsun. Aşağıdaki spiral karşımıza çıkıyor:

Şekle baktıgımızda $\{11, 37, 79, 137, 211, ...\}$ doğrusu asal sayıların yoğun oldugu bölgelerden biri ve spirali xy düzleminde düşünürsek x aksisine paralel bir doğru bulmuş oluyoruz. $\{43, 89, 151, ...\}$ doğrusu ise y aksisine paralel bir doğru olmuş oluyor. Böylece farkli bir spiral inşaası yaparak eğimleri +1 veya -1 olmayan asalca yoğun iki doğru bulmuş olduk ve başta söylediğimiz, spiralin şeklinden kaynaklı sebebimizi örneklendirerek destekledik.

4 Sacks Spirali

Asal sayıların dizilimlerini, birbirleri arasındaki mesafeyi görmemize yardımcı bir diğer spiral de Sacks Spirali'dir. Sürpriz olmayan bir şekilde Sacks Spirali, adını yaratıcısı Robert Sacks'ten alır. Yazılım mühendisi olan Robert Sacks, spirali 1994 yılında inşa etmiştir. Bu, aslında Ulam Spirali'ni bir nevi geliştirerek asalların dağılımını görsel olarak daha düzenli hale getirme çabasıdır. Gerçekten de Ulam Spirali ile karşılaştırdığımızda göreceğiz ki birazdan analiz etmeye başlayacağımız bu spiralde asallar daha belirgin ve tabiri caizse daha "düzenli" desenler çizecekler.

Peki bu spiral nasıl çizilir? Karışık görünse de Sacks Spirali, kutupsal koordinatları

$$r = \sqrt{n}$$
$$\theta = \sqrt{n}.2\pi, \quad \forall n \in \mathbb{R}_{\geq 0}$$

olan spiraldir. En temelde bu spirali, doğal sayıları 0'dan başlayarak bir yarı doğru üzerinde aralarındaki mesafe eşit olacak ve 1'er birim şekilde işaretleyip bu yarı doğruyu $\mathbb{R}^2$ düzleminde döndürdüğümüz bir spiral gibi düşünebiliriz.

İleride faydalanacağımız için eklemek gerek, burada θ'yı rotasyon cinsinden de ifade edebilirdik.

Biraz daha açıklayıcı olmak için bir örnek verelim: 9 doğal sayısına ulaşabilmek için orijinden başlayarak x eksenine 3 defa uğrarız; bu da 3 rotasyona denk gelir. Genelleme yapmak ve kutupsal koordinatların bize ne dediklerini sözlü olarak açıklamak gerekirse, spiralin herhangi bir noktasına kaç rotasyon yaparak ulaşıyorsak; o noktadaki reel sayı yapılan rotasyonun karesine eşittir. Reel sayıllardan söz ettiğimiz için bu noktada akıllara irrasyonel sayıllar gelebilir ve irrasyonel rotasyonun geometrik olarak neye karşılık geldiği kafamızı karıştırabilir. Bu noktada itiraf etmeliyiz ki Sacks Spirali, asal sayılarla ortak bir soruna sahiptir: İyi tanımlı olmamak! Ne yazık ki spiralin arkasındaki matematiği anlamak ve spiral üzerinde ilerleyebilmek için az önce yaptığımız genellemeyi kabul etmek zorundayız.

Sacks Spirali'nin genişletilmiş hali aşağıdaki gibidir:

Şekle çok dikkatli bakmasak bile spiralin içerdiği eğrileri gözlemlemek mümkün. Bu eğriler bize spiralin üzerindeki her bir doğal sayının hangi faktorizasyona yakın olduğu konusunda fikir sahibi olmamızı sağlayacaklar. Öyleyse artık spirali daha yakından tanımaya hazırız.

Tanım 4.1. *Herhangi bir n doğal sayısı için n^2 formundaki doğal sayılları içeren eğriye "S eğrisi" denir.*

Tanımdan da anlaşılacağı üzere S eğrisi,

$$\{0, 1, 4, 9, 16, 25, ...\}$$

kümesine eşittir. Aslında bu eğri, spiralin inşaasında temel rol oynayan, en başından beri adı geçen $y = 0$ doğrusunun $x \geq 0$ alanındaki kısıtıdır ve Sacks'in spiralde çizmeyi tercih ettiği eğri olarak kabul edilen tek doğrusudur.

Tanım 4.2. *Bir n doğal sayısı için $n.(n+1)$ formundaki doğal sayıları içeren eğriye "P eğrisi" denir.*

P eğrisinin elemanları sırasıyla

$$\{0, 2, 6, 12, 20, 30, 42, ...\}$$

kümesini oluşturur.

İleride göreceğiz ki spiralde gözlemlediğimiz eğrilerin büyük bir çoğunluğunu S ve P eğrileri cinsinden yazmak mümkün; bu yüzden bu iki tanım bizim için önemliydi. Ancak bunu yapabilmek için son bir tanıma daha ihtiyacımız var:

Tanım 4.3. *S eğrisinin eğimi 0'dır.*

Şimdi de spiralde "mesafe" kavramından bahsedelim. Makalemizin bu bölümünün başında spiralin inşaasından bahsetmiştik ve orada doğal sayıları bir yarı doğru üzerinde birbirlerine "eşit" mesafede ve ardışık iki doğal sayı arasındaki fark 1 olacak şekilde işaretleyip spirali oluşturduğumuzu söylemiştik. Buradan varacağımız sonuç, spiral üzerindeki iki sayı arasındaki fark, yarı doğru üzerindeki farkları kadardır. Mesafe kavramını ayrıca konuşmamızın sebebi, spiralin şeklinin bizi yanıltma ihtimalidir. Örnek verecek olursak, 48 ve 49 sayıları spiralde farklı eğriler üzerinde yer alıyorlar. Bulundukları bu iki eğri de gittikçe birbirlerinden uzaklaşıyor gibi görünüyor. Ancak 48 ve 49'u sayı doğrusu üzerinde düşündüğümüzde aralarındaki fark 1 birim olduğundan spiralde de bu fark değişmemektedir. Aynı durum 3 ve 4 sayıları için de geçerlidir.

Artık S ve P eğrilerinden bahsetmeye devam edebiliriz. Sıfır açısını referans alarak S eğrisine pozitif veya negatif yönde ve sabit mesafede olacak şekilde doğrular çizmek mümkündür. Bir önceki cümlede "sabit açıda" demek yerine "sabit mesafede" diye belirtmemizin sebebi, açıları rotasyon cinsinden ifade ederek eğrilerin üzerindeki noktaları kolayca belirleyebiliyor olmamızdır. Yine bu bölümün başında belirttiğimiz, rotasyon ve sayı arasılndaki ilişkiyi hatılrlayarak bir örnek yapalılm: Pozitif yönde 120° ile çizilen doğrunun elemanlarını bulalım. 120° 'nin $\frac{1}{3}$ rotasyona karşılık geldiği çıkarımını yaparak bu doğrunun 0'dan sonraki ilk elemanını bulalım. Kutupsal koordinatlardan yola çıkarak bu doğrunun ikinci elemanı $(\frac{1}{3})^2 = \frac{1}{9}$'dur. Üçüncü eleman ise $(1 + \frac{1}{3})$ rotasyondan sonra elde edilen $(\frac{4}{3})^2 = \frac{16}{9}$'dur. Özetle bu doğrunun elemanları

$$\{0, {}^{1}/_{9}, {}^{16}/_{9}, {}^{49}/_{9}, {}^{100}/_{9}, ...\}$$

kümesini verir. Aynı akıl yürütmeyle 180°; yani $\frac{1}{2}$ rotasyona karşılık gelen doğrunun elemanları ise

$$\{0, {}^{1}/_{4}, {}^{9}/_{4}, {}^{25}/_{4}, {}^{49}/_{4}, ...\}$$

kümesindedir.

$\frac{1}{2}$ doğrusunu spiralde çizdiğimizde dikkatimizi çekmesi gereken olgu, P eğrisindeki herhangi bir sayının $\frac{1}{2}$ doğrusunda kendisinden sonra gelen sayıya hep sabit mesafede duracak şekilde konumlanmış olmasıdır. Örneğin P eğrisi üzerindeki 2

ve 6 doğal sayılarından sonra $\frac{1}{2}$ doğrusu üzerinde sırasıyla $\frac{9}{4}$ ve $\frac{25}{4}$ rasyonel sayıları gelmektedir. Aralarındaki mesafeye bakacak olursak:

- $\frac{9}{4} - 2 = \frac{1}{4}$
- $\frac{25}{4} - 6 = \frac{1}{4}$.

Bu eşitliği aynı eğri ve doğru üzerindeki her nokta için görmek mümkündür.

Sınıflandırmayı tamamlayabilmek için son bir adımımız kaldı. Şimdi de S ve P eğrilerine eşit mesafede duran eğrileri bulmaya çalışalım. P eğrisiyle başlayalım. Örneğin $\{0, 1, 5, 11, 19, 29, ...\}$ doğal sayılarını barındıran eğri P eğrisine hep aynı mesafededir. Bu sayıları 0'ı dahil etmeden incelediğimizde:

- $1 = 2 \times 1 - 1$
- $5 = 2 \times 3 - 1$
- $11 = 3 \times 4 - 1$
- $19 = 4 \times 5 - 1$ ...

düzeni dikkat çeker; yani bir n doğal sayısı için **"n.(n+1)-1"** düzeni. Bu yüzden bu eğriyi "P-1" eğrisi olarak adlandıralım. Aynı şekilde $\{0, 8, 14, 22, 32, ...\}$ doğal sayılarını barındıran eğri ile P eğrisi arasındaki mesafe her zaman 2 birimdir. Yine 0 dışındaki elemanlara baktığımızda

- $8 = 2 \times 3 + 2$
- $14 = 3 \times 4 + 2$
- $22 = 4 \times 5 + 2$ ...

düzenini görüyoruz. Bu düzenden dolayı bu eğriye de "P+2" eğrisi diyelim.

Benzer aşamalarla spiralin sağ tarafında konumlanmış eğrilerin S eğrisine olan uzaklıklarını gözlemleyerek spiralin sağ tarafını da büyük çoğunlukla S eğrisi cinsinden yazabiliriz. Böylece spiraldeki çoğu eğriyi S ve P eğrilerine benzetebilir hale geldik.

Spiraldeki açı ve mesafe kavramlarını tanımladıktan sonra söyleyebiliriz ki spiralin ilk halinde görünür olmamasına rağmen $\frac{1}{2}$ rotasyona karşılık gelen doğruyu örnek olarak incelememizin sebebi, P eğrisi ve onun cinsinden yazabileceğimiz eğriler hakkında yorum yapabilmekti. Daha geniş bir çerçeveden baktığımızda spiral iki temel doğru üzerinden şekilleniyor. 0 ve $\frac{1}{2}$ açılarına karşılık gelen doğruları bir küme gibi düşündüğümüzde S ve P eğrileri ile "$S\pm$" ve "$P\pm$ " eğrilerini sırasıyla 0 ve $\frac{1}{2}$ doğrularının birer alt kümesi gibi tasvir etmek de bize farklı bir bakış açısı kazandıracaktır.

Spirali iyice anladıktan sonra faktorizasyon hakkında konuşabiliriz. Şu ana kadar yaptığımız örneklerden de anlayacağınız gibi Sacks Spirali, sayıların "ifade ediliş şekline" göre tasarlanmıştır ve bu ifade şekline göre de eğriler meydana gelmiştir. "Bazı" doğal sayılar birden fazla şekilde çarpanlara ayrılabildiğine göre bu doğal sayılar birden fazla eğride gözlemlenebilir. Bir örnekle açıklamak gerekirse, 4 doğal sayısını 4×1 ve 2×2 şeklinde ifade edebileceğimizi ilkokuldan beri biliyoruz. Önceki tanımlardan yola çıkarak $4 \times 1 = 2 \times 3 - 2$ formu bize 4'ün P-2 eğrisinde bulunduğunu, $2 \times 2 = 2^2$ tasviri de yine 4'ün S eğrisinde gözlemlenebildiğini söyler. Artık ulaşmak istediğimiz o malum sonucu sizlerle paylaşmak için hazırız:

Sonuç 4.4. *1'den büyük bir p doğal sayısı asaldır ancak ve ancak bu sayı sadece tek bir eğride gözlemlenebiliyorsa.*

Artık asalları bu spiral üzerinde de işaretleyebiliriz:

Yukarıda görüldüğü üzere tıpku Ulam Spirali'nde olduğu gibi Sacks Spirali'nde de asalların oluşturduğu düzen inkar edilemez bir hal almıştır. Hatırlayacağınız gibi Ulam Spirali'nde Euler'in Asal Üreten Polinomu'nu tek bir doğru üzerinde gözlemleyebilmek için spiralin başlangıç noktasını değiştirmemiz gerekiyordu. Ulam Spirali'nin aksine, burada Euler'in Asal Üreten Polinomları'ndan $x^2 + x + 41$ polinomu hiçbir oynama yapmadan P+41 eğrisi üzerinde rahatlıkla gözlemlenebilir.

5 Kuadratik Sayı Cisimleri

Bu bölümde yukarıda bahsi geçen kuadratik polinomların neden *beklenenden fazla* asal sayı ürettiğini açıklamaya çalışacağız. Amacımıza ulaşmak için bir miktar öncalışma yapmamız gerekiyor.

5.1 Cebirsel Tamsayılar

İlk olarak tamsayıları genellemeye çalışarak başlayalım. Bunun için öncelikle rasyonel sayılar kümesi, $\mathbb{Q}$, içindeki tamsayıları, $\mathbb{Z}$, (literatürde rasyonel tamsayı olarak de yer alır ancak biz bu terminolojiyi kullanmayacağız) sınıflamaya çalışalım[†]. Verilen bir α rasyonel sayısı için öyle p ve q tamsayıları vardır ki $\alpha = p/q$ şeklinde yazılır yani α $qx - p = 0$ eşitliğinin çözümüdür. Başka bir deyişle $x \in \mathbb{Q}$ $q\alpha - p$ tamsayı katsayılı polinomun[‡] bir köküdür. Tersine, verilen her derecesi 1 olan herhangi tamsayı katsayılı polinomunun, $p(x) = ax+b$, kökü bir rasyonel sayıdır. Özetle:

Önerme 5.1. *Rasyonel sayılar kümesi, $\mathbb{Q}$, ile derecesi* 1 *olan tamsayı katsayılı polinomların köklerinin kümesi arasında birebir ve örten bir eşleme vardır.*

Tamsayı katsayılı bir polinomun kökünün yine bir tamsayı olması için polinomun başkatsayısının 1 olması gerek ve yeterli koşuldur. Önerme 5.1'in direk sonucu olarak aşağıdaki sonucu elde ederiz:

Sonuç 5.2. *Tamsayılar kümesi, $\mathbb{Z}$, ile başkatsayısı ve derecesi* 1 *olan polinomların köklerinin kümesi arasında birebir ve örten bir eşleme vardır.*

Yukarıdaki tanımın ilk akla gelen genellemelerinden bir tanesi kullanılan polinomların dereceleri üzerinden elde edilendir:

Tanım 5.3. *Verilen bir x karmaşık sayısı başkatsayısı* 1 *olan tamsayı katsayılı bir polinomun kökü ise x'e* cebirsel tamsayı *denir.*

İlk gözlemimiz her tamsayının bir cebirsel tamsayı olduğu, zira her n tamsayısı $p(\alpha) = \alpha - n$ polinomumun kökü. Tamsayı olmayan cebirsel tamsayılar da var. Örneğin, $\sqrt{2}$ sayısı cebirsel bir tamsayıdır, çünkü $p(\alpha) = \alpha^2 - 2$ tamsayı katsayılı polinomunun köküdür. $p(\alpha) = \alpha^7 - 3$ polinomunun kökü olan $\sqrt[7]{3}$ sayısı da bir cebirsel tamsayıdır.

Birkaç deneyden sonra okuyucunun da farkına varacağı üzere bir x cebirsel sayısını kök olarak kabul eden polinom biricik değildir; mesela $\sqrt{2}$ hem $\alpha^2 - 2$, hem de $\alpha^3 - 2\alpha$ polinomunun köküdür. Bu karmaşayı önlemek için, verilen bir x cebirsel tamsayısı için x'i kök olarak kabul eden başkatsayısı 1 olan tamsayı katsayılı polinomların kümesini P_x ile gösterelim. Bu kümede yer alan polinomları derecelerine göre sıralayalım. Dereceler birer doğal sayı olduğundan bu kümede derecesi en küçük olan bir polinom bulunur[§]. Bu polinomun derecesine x cebirsel tamsayısının derecesi denir. Tamsayıların derecesi 1'dir. Derecesi 2 olan cebirsel tamsayılar *kuadratik*, üç olanlar kübik, ... olarak adlandırılır. Örneğin $\sqrt{2}$ ve $-1/2 + \sqrt{-3}/2$ kuadratik bir tamsayı, $\sqrt[3]{3}$ kübik bir tamsayıdır. Bu üç iddiayı ispatlamayı okura bırakıyoruz. Derecesi en küçük olan bu polinomlara bir de katsayıların ortak böleninin olmaması koşulunu eklediğimizde geriye biricik bir polinom kalır[¶]. Bu polinoma cebirsel sayının *minimal polinomu* denir. Örneğin $\sqrt{2}$'nin minimal polinomu $p(\alpha) = \alpha^2 - 2$, $i = \sqrt{-1}$'in minimal polinomu $x^2 + 1$'dir.

Karmaşık sayılar kümesinde tanımlı toplama ve çarpma işlemleri cebirsel tamsayılar kümesine, CT, miras kalır. Ancak CT haddinden fazla büyük. Buna ek olarak ileride açıklığa kavuşacak nedenlerden ötürü nihai hedefimize ulaşmak için kümenin hepsini ele almamıza gerek yok. Dolayısıyla ilk olarak cebirsel tamsayılar kümesini tamsayıların derecelerine göre ayrık alt-kümelere ayıralım. Kuadratik cebirsel tamsayılar kümesini CT_2 ile gösterelim. $\sqrt{2}$ ve $\sqrt{3}$ CT_2'nin bir elemanı olsa bile $\sqrt{2} + \sqrt{3}$ maalesef derecesi 4 olan bir cebirsel sayıdır[‖], yani CT_2'in bir elemanı değildir. Bu da demek oluyor ki CT_2 toplama işlemi altında kapalı değil. Benzer bir fikirle CT_2'nin çarpma işlemi altında kapalı olmadığı da kolaylıkla gösterilebilir.

[†] Okuyucuyu tamsayıları karakterize eden başka özellik bulmaya davet ediyoruz.

[‡] Makale boyunca polinomları, aksi belirtilmediği sürece, tek değişkenli ve sıfırdan farklı olarak varsayacağız.

[§] Bu sonuca doğal sayılar kümesi üzerinde iyi sıralama prensibini kullanarak ulaşabiliriz. İlgili okuyucuyu konu hakkındaki wikipedia makalesine başvurmaya davet ediyoruz.

[¶] Bu ispatı bizi maksadımızdan uzaklaştıracağı için buraya dahil etmiyoruz.

[‖] Bu iddiayı şu aşamada göstermesi oldukça zordur. Okuyucu $\sqrt{2} + \sqrt{3}$'ün $p(\alpha) = \alpha^4 - 10\alpha^2 + 1$ polinomunun kökü olduğunu görmesi kafidir.

5.2 Kuadratik Tamsayı Halkaları

Yukarıdaki gözlem bizi dereceler kullanarak yapılan sınıflamanın da cebirsel açıdan uygun olmadığını söylüyor. Okuyucunun da hemen farkına varacağı gibi bunun temel nedeninin de karekök içindeki sayıların, yani 2 ve 3'ün, birbirinden farklı olmasıdır. Bunu aşmak için öncelikle bir tanımla başlayalım:

Tanım 5.4. *d karesiz bir tamsayı olsun*[**]*.*

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \colon a, b \in \mathbb{Q}\}$$

kümesine kuadratik sayı cismi *denir.*

Okuyucuyu $\mathbb{Q}(\sqrt{d})$ kümesinin gerçekten bir cismi olduğunu, yani $\mathbb{Q}(\sqrt{d})$

- $\mathbb{Q}(\sqrt{d})$ toplama işlemine göre abelyen grup olduğunu,
- $\mathbb{Q}(\sqrt{d}) \setminus \{0\}$ çarpma işlemine göre abelyen grup olduğunu, ve
- çarpma işlemi toplama işlemi üzerine dağılma özelliğini sağladığını

kontrol etmeye davet ediyoruz. Şimdi $\mathbb{Q}(\sqrt{d})$ içindeki cebirsel tamsayıları bulmaya çalışalım. Herhangi bir $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ sayısı için $\overline{x}$ ile $a - b\sqrt{d}$ sayısını gösterelim. α'nın

$$p(\alpha) = \alpha^2 - (x + \overline{x})\alpha + (x \cdot \overline{x})$$

polinomunun bir kökü olduğunu okuyucu kolayca kontrol edebilir. Minimal polinmun biricik olmasını kullanarak x'in bir cebirsel tamsayı olması için $x+\overline{x} = 2a$'in ve $x \cdot \overline{x} = a^2 - db^2$ rasyonel sayılarının birer tamsayı olmasının gerek ve yeter koşul olduğu sonucuna ulaşırız. a'nın paydasında en *kötü ihtimalle* 2 olabilir, başka bir deyişle $\frac{1}{2} \cdot \mathbb{Z}$'nin elemanı olmalıdır. O halde öyle bir $a' \in \mathbb{Z}$ vardır ki $a = \frac{a'}{2}$. d'nin karesiz bir tamsayı olduğunu biliyoruz. Dolayısıyla $a^2 - db^2$ farkının bir tamsayı olabilmesi için $b \in \frac{1}{2} \cdot \mathbb{Z}$ olmalı. b rasyonel sayısı için de yine öyle bir $b' \in \mathbb{Z}$ vardır ki $b = \frac{b'}{2}$'dir. O zaman

$$\begin{aligned} a^2 - db^2 \in \mathbb{Z} &\leftrightarrow \frac{1}{4}(a'^2 - db'^2) \in \mathbb{Z} \qquad (5.1) \\ &\leftrightarrow (a')^2 - d(b')^2 \equiv 0 \mod 4 \end{aligned}$$

olmalı. Şu iki gözlemi not edelim:

- $(a')^2$ ve $(b')^2$, 4 modunda 0 ve 1 olabilir; ve
- d, 4 modunda 0'dan farklı bir sayıya denk olmak zorundır.

Yani $(a')^2 \equiv 0 \mod 4$ ise, yani a' çift bir tamsayı ise, yani a bir tamsayı ise x'in bir cebirsel tamsayı olabilmesi için b de mutlaka bir tamsayı olmalıdır. $(a')^2 \equiv 1$ ise, yani a' tek bir tamsayı ise $(b')^2 \equiv 1$ olmalı, yani b' de tek bir sayı olmalıdır. Bu durumda x'in bir cebirsel tamsayı olması için $d \equiv 1$ olmak zorunda! $\mathbb{Q}(\sqrt{d})$'deki cebirsel tamsayılar kümesini $\mathcal{O}_d$ ile gösterirsek şunu ispatlamış olduk:

Teorem 5.5. *a ve b birer tamsayı olmak üzere*

$$\mathcal{O}_d = \begin{cases} \{a + b\sqrt{d}\} & d \equiv 2, 3 \mod 4, \\ \{a + b\left(\frac{1+\sqrt{d}}{2}\right)\} & d \equiv 1 \mod 4. \end{cases}$$

Yukarıdaki tariften ötürü tüm karesiz d tamsayıları için aşağıdaki iddiaları göstermek artık zor değil:

- $\mathcal{O}_d$ bir değişmeli halkadır.
- $\mathcal{O}_d$ hiç sıfır böleni içermez, yani $\mathcal{O}_d$ bir tamlık bölgesidir.
- $\mathcal{O}_d$ bir cisim değildir.

$\mathcal{O}_d$ halkaları tamsayıların bir genellemesi olduğundan ilk sorumuz $\mathbb{Z}$'nin hangi özelliklerinin $\mathcal{O}_d$ halkaları için de geçerli olduğunu bulmak. Bu sorunun aritmetikte en önemli sorulardan bir tanesi olduğunu ve halen daha çözülememiş bir sürü kısmı olduğunu bu noktada vurgulamak isteriz.

5.3 Çarpanlara Ayırma

Yukarıdaki liste üç ortak özelliği listeliyor. Halbuki $\mathbb{Z}$ ile $\mathcal{O}_d$ arasıda belirli bazı karesiz d tamsayıları için farklılıklar var. Bunlardan ilki çarpanlara

[**]Bir d tamsayısına $n^2|d$, $n = \pm 1$ olmasını gerektiriyorsa *karesiz* denir.

ayırma. Hepimizin uzun süredir bildiği gibi herhangi bir tamsayıyı asal sayıların çarpımı şeklinde yazabiliriz, yani rastgele verilen n tamsayısı için öyle sonlu tane farklı asal sayılar, $p_1, \ldots, p_k$ ve doğal sayılar $n_1, \ldots, n_k$, $k \geq 1$ vardır ki

$$n = \pm p_1^{n_1} \ldots p_k^{n_k}$$

eşitliği sağlanır. Üstüne üstlük, bu asal sayıların sıralanması ve ± 1 ile çarpma göz ardı edilecek olursa bu çarpmanın tek türlü yapılabileceğini görürüz. Ancak bu durum bir çok $\mathcal{O}_d$ için geçerli değildir. Bundan bahsedebilmek için biraz terminolojiye ihtiyacımız var.

5.3.1 Kuadratik tamsayı halkalarındaki birim elemanlar

Bu bölümde $\mathcal{O}_d$'deki birim elemanları inceleyeceğiz. İlk olarak $\{\pm 1\}$ kümesi tam olarak $\mathbb{Z}$'de çarpma işlemine tersi olan elemanların kümesi olduğunu not edelim. Biz de $\mathcal{O}_d$'de tersi olan elemanlara *birim elemanlar* diyeceğiz. Yani bir $\alpha \in \mathcal{O}_d$ elemanı için yine $\mathcal{O}_d$'nin içinde $\alpha \cdot \beta = 1$ eşitliğini sağlayan bir β elemanı varsa α'ya birim eleman diyeceğiz. Çarpmaya göre etkisiz elemanı barındıran herhangibir R halkası için, halkanın içindeki birim elemanların oluşturduğu küme $R^\times$ ile gösterilir. Bizim ihtiyacımız olmayacak ama ilgili okuyucu $\mathcal{O}_d^\times$'ın bir grup olduğunu göstermeyi deneyebilir. Verilen her $\alpha = \in \mathcal{O}_d$ için α elemanının normu, $N(\alpha)$ şu şekilde tanımlanır:

$$N(\alpha) = \alpha \cdot \overline{\alpha}.$$

Şayet $d \equiv 2, 3 \mod 4$ olursa $\alpha = a + b\sqrt{d}$ şeklinde yazılabilir ve $N(\alpha) = a^2 - db^2$ formunu alır, $d \equiv 1 \mod 4$ olursa $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$ şeklinde yazılır ve $N(\alpha) = \left(a + \frac{b}{2}\right)^2 - d\frac{b^2}{2}$ formunu alır. Okuyucuyu bu noktada normun çarpımsal olduğunu ispatlamaya davet ediyoruz, yani verilen her $\alpha, \beta \in \mathcal{O}_d$ için $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ eşitliği sağlanır. Norm ile ilgili bir kaçgözlemimiz var:

- kuadratik tamsayı halkalarının inşasında görüğümüz üzere (bkz. Eşitlik 5.1) her $\alpha \in \mathcal{O}_d$ için $N(\alpha)$ bir tamsayıdır,
- $\alpha, \beta, \gamma \in \mathcal{O}_d$ için $\alpha\beta = \gamma$ eşitliğinde her iki tarafın normu alınırsa $N(\alpha)$ ve $N(\beta)$'nın $N(\gamma)$'yı bölmesi gerektiği elde edilir, ve
- $N(0) = 0$, $N(1) = 1$ olur.

Bir $\alpha \in \mathcal{O}_d$ alalım. $\alpha \in \mathcal{O}_d^\times$ ise $\alpha\beta = 1$ eşitliğini sağlayan bir β vardır. Her iki tarafın normu alınırsa

$$N(\alpha)N(\beta) = 1$$

olur. Eşitliğin solundaki her iki çarpan da yukarıdaki gözlemimizden dolayı 1'in bir böleni olmak, yani ± 1'e eşit olmak, zorundadır. Tersine, bize normu 1 olan bir $\alpha = a + b\sqrt{d}$ elemanı verilirse, $\beta = a - b\sqrt{d}$ elemanı için $\alpha \cdot \beta = 1$ olur. β'nın aslında $\overline{\alpha}$ olduğunu ve $\mathcal{O}_d$'nin bir elemanı olduğunu kontrol etmeyi okuyucuya bırakıyoruz. Şunu ispatlamış olduk:

Önerme 5.6.

$$\mathcal{O}_d^\times = \{\alpha = a + b_d \in \mathcal{O}_d \colon N(\alpha) = \pm 1\}.$$

Gelin şimdi bir kaç farklı d için $\mathcal{O}_d^\times$'yı belirlemeye çalışalım.

Örnek 1. *İlk olarak $d = -1$ alalım. $d \equiv 3 \mod 4$ olduğundan Teorem 5.5 bize*

$$\mathcal{O}_d = \{a + b\sqrt{-1} \colon a, b \in \mathbb{Z}\}$$

olduğunu söyler. $\mathcal{O}_d^\times$'ın hesabı için

$$a^2 + b^2 = 1 \text{ ve } a^2 + b^2 = -1$$

denklemlerini çözmeliyiz. İkinci denklemin çözümü olmadığı aşikar. İlk denklemin çözüm kümesi ise $(\pm 1, 0)$ ve $(0, \pm 1)$ şeklindeki (a, b) ikililerinden oluşmakta. Dolayısıyla:

$$\mathcal{O}_{-1} = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$$

$d = -3$ durumunda $\mathcal{O}_d^\times$'nın 6 elemanı olduğu ipucunu verip detayları okuyucuya bırakalım ve $\mathcal{O}_d$ hesabını $d < -3$ olan tüm karesiz ve $d \equiv 2, 3 \mod 4$ olan d tamsayıları için hesabı yapmaya çalışalım. Bu kez çözülmesi gereken denklem:

$$a^2 - db^2 = 1 \text{ ve } a^2 - db^2 = -1$$

olacak. $a^2 \geq 0$ ve $-db^2 \geq 0$ olduğundan bu iki büyüklüğün toplamı da ≥ 0 olmak zorunda, yani sağdaki eşitliğin çözümü yok. Soldakine gelecek olursak, $d < -3$ olduğundan $d^2 > 9$. Dolayısıyla, $b \neq 0$ olduğu durumda $a^2 \geq 0$ olduğundan soldaki denklem çözümsüz. Geriye kalan tek durum olan $b = 0$'da ise $a = \pm 1$ tek çözüm. Benzer bir nedenleme ile $d \equiv 3 \mod 4$ durumunun çözüm kümesinin de aynı olduğu sonucu elde edilebilir. Dolayısıyla:

Önerme 5.7. *$d < -3$ karesiz bir tamsayı olsun. O halde*

$$\mathcal{O}_d^\times = \{1, -1\}$$

olur.

Bunun ardından hemen "Peki $d > 0$ olursa?" sorusunu sormalıyız. Bu kez $d > 0$ olduğundan benzer nedenlemeler sonuç vermiyor. Ve kuramın bu kısmı Pell denkleri ile alakalı ve başka bir yazının konusu olmaya aday.

Bu bölümü kapatmadan önce normu sınırlamamıza yarayan ve daha sonra kullanacağımız bir sonucu ispatlayalım:

Önerme 5.8. *$\alpha \in \mathcal{O}_d \setminus \mathbb{Z}$ alalım. O halde α'nın normu*

- *$d \equiv 2, 3 \mod 4$ ise $N(\alpha) \geq -d$*
- *$d \equiv 1 \mod 4$ ise $N(\alpha) \geq \frac{1-d}{4}$*

eşitsizliklerini sağlar.

Kanıt. $d \equiv 2, 3 \mod 4$ ise $\alpha = a + b\sqrt{d}$ şeklinde yazılır ve $N(\alpha) = a^2 - db^2$ olur. $\alpha \notin \mathbb{Z}$ olduğundan $b \neq 0$ olmalıdır. $a^2 \geq 0$ olduğundan

$$N(\alpha) = a^2 - db^2 \geq -db^2 \geq -d;$$

zira $b^2 \geq 1$.

$d \equiv 1 \mod 4$ ise $\alpha = a + b\frac{1+\sqrt{d}}{2}$ şeklinde yazılır ve $N(\alpha) = \left(a + \frac{b}{2}\right)^2 - d\frac{b^2}{4}$ olur. Yine $b \neq 0$ olmalıdır, yani $b^2 \geq 1$ olmalıdır. Öte yandan $\left(a + \frac{b}{2}\right)^2 \geq \frac{1}{4}$ olmalıdır. Bunlar kullanılarak

$$N(\alpha) = \left(a + \frac{b}{2}\right)^2 - d\frac{b^2}{2} \geq \frac{1}{4} - \frac{d}{4} = \frac{1-d}{4}$$

hemen elde edilir. □

5.3.2 Kuadratik Asallar

Çarpanlara ayırma için kullandığımız başka bir kavram ise asallık. Bir $\alpha \in \mathcal{O}_d$ elemanı alalım. $\alpha = \beta \cdot \gamma$ eşitliğini sağlayan her β ve γ için ya β ya da γ birim oluyorsa α'ya asal eleman denir. Verilen herhangibir $\alpha \in \mathcal{O}_d$ elemanının çarpanlara ayrılabildiğini, yani asal elemanların çarpımı şeklinde yazılabildiğini, varsayalım, yani $u \in \mathcal{O}_d^\times$, $\alpha_i \in \mathcal{O}_d$ her $i \in \{1, \ldots, k\}$ için asal olmak üzere

$$\alpha = u \cdot \alpha_1^{n_1} \ldots \alpha_k^{n_k}$$

olsun. $\mathcal{O}_d$ içerisinde elde edilen her farklı çarpanlara ayırma yukarıda verilen çarpanlara ayırmada sadece ve sadece ya asalların sıralaması ya da birim eleman ile çarpma olarak ayrışıyor ise $\mathcal{O}_d$'de çarpanlara ayırma tek türlü yapılır diyeceğiz. Bu koşulu sağlayan halkalara tek türlü çarpanlarına ayrılma bölgesi (TTÇAB) denir. Bazı d'ler için $\mathcal{O}_d$ TTÇAB iken bazıları için değildir. An itibariyle bir $\mathcal{O}_d$'nin TTÇAB olduğunu göstermek zor olsa da olmadığını göstermek oldukça kolaydır. Örneğin $\mathcal{O}_{-5}$ içinde

$$9 = 3 \cdot 3 = \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right)$$

şeklinde yazılabilir ve bu iki çarpanlara ayırma bir birim eleman kadar fark edemez, zira $\mathcal{O}_{-5}$'teki birim elemanlar sadece 1 ve -1'dir. Dolayısıyla $\mathcal{O}_{-5}$ bir TTÇAB değildir. Buna karşın göstermesi her ne kadar zor olsa da $\mathcal{O}_{-1}$ bir TTÇAB'dir.

5.3.3 Antrakt: Asallık İndirgenemezliğe Karşı

Okuyucunın aklına hemen şu soru gelmesi doğaldır: Asal sayılar aynı zamanda "bir p doğal sayısı asal ise ve p, ab çarpımını bölüyorsa p, a'yı veya b'yi böler" ile de tanımlanabilir. Niye böyle tanımlamadık? Genel bir R halkasında bu özelliği sağlayan elemanlar *indirgenemez* olarak tanımlanır. Asallık ve indirgenemezlik tamsayılar halkasında birbirine denk olsa da genelde (örneğin bazı d'ler için $\mathcal{O}_d$'lerde) bu denklik doğru değildir:

Örnek 2. *$\alpha = 2 + \sqrt{-5} \in \mathcal{O}_{-5}$ elemanını alalım. $N(\alpha) = 4 + 5 = 9$ olur. Varsayalım ki $\alpha = \beta \cdot \gamma$ eşitliğini sağlayan β ve γ elemanları olsun. O halde $9 = N(\beta)N(\gamma)$ eşitliği sağlanmalıdır. β ve γ elemanlarının ikisinin birden birim eleman olmaması demek hem $N(\beta) > 1$ hem de $N(\gamma) > 1$ olması demektir. Bu da*

$$N(\beta) = \pm 3 \text{ ve } N(\gamma) = \pm 3$$

olması anlamına gelir. Ancak $\mathcal{O}_{-5}$ içinden normu 3 eleman bulunamaz, çünkü

$$a^2 + 5b^2 = 3 \text{ ve } a^2 + 5b^2 = -3$$

denklemlerinin çözümü yoktur. Dolayısıyla $\alpha \in \mathcal{O}_{-5}$ indirgenemez bir elemandır.

Ancak, $N(\alpha) = 9$ olduğundan α elemanı 9'u yani $3 \cdot 3$'ü böler, ancak $2 + \sqrt{-5}$, 3'ü bölemez (bölseydi, yani $\alpha \cdot \beta = 3$ özelliğini sağlayan $\beta \in \mathcal{O}_{-5}$ olsaydı, o zaman $N(\beta) = \pm 1$ olması yani β'nın birim olması gerekirdi ancak Önerme 5.7 bize $\mathcal{O}_d$'nin birim elemanlarının 1 ve -1'den ibaret olduğunu söylüyor.).

Bu iki tanım TTÇAB'ler için (ve dolayısıyla, tek üreteçli ideal bölgeleri (TÜİB) ve öklid bölgeleri (ÖB) için) birbirine denktir.

6 Asal Üreten Kuadratik Polinomlar

Bu bölümde evvelce makalede ele alınan asal üreten kuadratik polinomların neden bu kadar fazla asal sayı ürettiğini kuramsal olarak açıklamaya çalışacağız. Bunun için bir önceki bölümde geçen kavramlara ve önermelere sıklıkla başvuracağız. Bu bölümde makalenin başından beri karesiz olan d tamsayısının aynı zamanda negatif olduğunu da varsayıyoruz.

6.1 Ön Hazırlık

Önerme 5.8'yi kullanarak aşağıdaki sonucu elde etmek mümkün:

Önerme 6.1. *$p \in \mathbb{Z}$ bir asal sayı olsun.*

$$\begin{cases} d \equiv 2,3 \mod 4 & \text{iken } p < -d \text{ ise, veya} \\ d \equiv 1 \mod 4 & \text{iken } p < \frac{1-d}{4} \text{ ise} \end{cases}$$

p indirgenemez olmak zorundadır.

Kanıt. $p = \alpha_1\alpha_2$ şeklinde yazalım, öyle ki $|N(\alpha_1)| > 1$ ve $|N(\alpha_2)| > 1$ olsun. O halde $N(p) = p^2 = N(\alpha_1)N(\alpha_2)$ eşitliğinden $i = 1, 2$ için $N(\alpha_i) = \pm p$ olacaktır. α_1 ve α_2 birer tamsayı olamazlar, yani $\mathcal{O}_d \setminus \mathbb{Z}$'nin elemanıdır. Önerme 5.8 bize

$$N(\alpha_i) \geq \begin{cases} -d, & d \equiv 2,3 \mod 4 \text{ iken, ve} \\ \frac{1-d}{4}, & d \equiv 1 \mod 4 \text{ iken} \end{cases}$$

olduğunu söyler; çelişki!. □

Yukarıdaki önermeden direk olarak şu sonucu elde ederiz:

Sonuç 6.2. *$\mathcal{O}_d$ bir TTÇAB ve p Önerme 6.1'daki gibi bir asal sayı olsun. Her a tamsayısı için*

$$\begin{cases} a + \sqrt{-d}, & d \equiv 2,3 \mod 4 \text{ iken, ve} \\ a + \frac{1+\sqrt{-d}}{2}, & d \equiv 1 \mod 4 \text{ iken} \end{cases}$$

sayısının normu p asal sayısına bölünemez. Başka bir deyişle bu sayının normunun $\frac{1-d}{4}$'den küçük asal böleni yoktur.

Kanıt. İspatı $d \equiv 1 \mod 4$ için yapalım, diğer durumun ispatı aynı tekniğin tekrarlanması ile elde edilebilir. Önerme 6.1 p'nin indirgenemez olduğunu söyler. p, $N(a+\sqrt{-d})$ tamsayısını bölmesi, $a+\sqrt{-d}$ veya $a-\sqrt{-d}$ sayılarından en az bir tanesini bölmesini gerektirir. □

6.2 $x^2 + x + D$ ve $\mathcal{O}_d$.

Bu bölüme şunu not ederek başlayalım: $d \equiv 2,3 \mod 4$ olduğunda $\mathcal{O}_d$ TTÇAB olamaz. Bunu görmek için x bir tamsayı olmak üzere

$$N(x + \sqrt{-d}) = x^2 - d$$

polinomunu düşünelim. Nu polinomun d'deki değeri, yani $d^2 - d$, d tek de olsa çift de olsa $2 < -d$ ile bölünebilir. $\mathcal{O}_d$ bir TTÇAB olsaydı Sonuç 6.2 ile çelişirdi.

Bu noktadan itibaren $d \equiv 1 \mod 4$ varsayabiliriz. Bu durumda $D = \frac{1-d}{4}$ olmak üzere, tekrar

$$\begin{aligned} N\left(x + \frac{1-\sqrt{d}}{2}\right) &= (x + \frac{1}{2})^2 - \frac{d}{4} \\ &= x^2 + x + D \end{aligned} \tag{6.1}$$

polinomunu düşünelim. Göstereceğimiz sonuç şu:

Theorem 6.3. *$\mathcal{O}_d$ bir TTÇAB ise $0 \leq x \leq \frac{-d-7}{4}$ eşitsizliğini sağlayan her x tamsayısında eşitlik 6.1'de verilen $x^2 + x + D$ polinomu asal değer alır.*

Kanıt. x^2+x+D polinomunun asal olmadığını varsayalım. $0 \leq x \leq \frac{-d-7}{4}$ eşitsizliğini sağlayan her x için

$$\begin{aligned} x^2+x+D &\leq \frac{d^2+14d+49}{16} + \frac{-d-7}{4} + \frac{1-d}{4} \\ &= \frac{d^2+14d+49-8d-24}{16} \\ &= \frac{d^2-2d+1}{16} + \frac{8d+24}{16} \\ &\leq \left(\frac{1-d}{4}\right)^2, \end{aligned}$$

çünkü $d<0$ ve $d \equiv 1 \mod 4$ olduğundan $d \leq -3$ olmalı, yani $\frac{8d+24}{16} \leq 0$ olmalıdır. Ancak herhangi n doğal sayısının eğer kendisi asal bir sayı değilse $\sqrt{n}$'den küçük bir asal böleni mutlaka vardır. Dolayısıyla x^2+x+D'nin $\frac{1-d}{4}$'ten küçük bir asal böleni olmalıdır, Sonuç 6.2 ile çelişki!!! □

Dolayısıyla polinomların asal sayı üretmesi kuadratik tamsayı halkalarının TTÇAB olması ile açıklanabilmektedir. Bir sonraki soru ise hangi negatif d tamsayıları için ele aldığımız $\mathcal{O}_d$ halkalarının TTÇAB olduklarıdır. Bu sorunun kökleri 200 yıl öncesine, Gauß'un meşhur "Disquisitiones Arithmeticae" kitabına dayanmaktadır. Geçtiğimiz yüzyıl içinde Siegel ve Stark gibi parlak matematikçilerin katkısı ile soru tam olarak çözülebilmiştir. Buna göre listemiz tam olarak şu tamsayılardan oluşur:

$$-3, -7, -11, -19, -43, -67, -163$$

Bu listeden elde edilen x^2+x+D formundaki polinomların D değerleri şunlardır:

$$1, 2, 3, 5, 11, 17, 41$$

Yukarıdaki kuram ile tek tek kontrol etmeden x^2+x+41 polinomunun ilk 39 değer için asal olacağı sonucuna varabiliriz. Elbetteki hangisinin daha verimli olduğu okuyucunun tercihine kalmıştır.