

Asalların Sonsuzluğunun Altı Değişik Kanıtı

M. Aigner ve G. M. Ziegler*

Bu yazıda asalların sonsuzluğunun altı değişik kanıtını vereceğiz. Umarız okur bu kanıtlardan bizim kadar hoşlanır. Farklı açılardan bakmalarına karşın şu temel fikir kanıtların hepsinde ortak: Doğal sayılar sınırsızca büyür ve her doğal sayının bir asal bölene vardır. Bu iki olgu her seferinde asal sayıları sonsuz olmaya zorluyor¹.

Asalların sonsuzluğunu ilk olarak Öklid'in kanıtladığı sanılır. Biz de Öklid'in [Öğeler IX, 20] eserinde yer alan bu kanıttan başlayacağız.

1. Birinci Kanıt [Öklid]. Asallardan oluşan sonlu bir $\{p_1, \dots, p_r\}$ kümesi için, $n = p_1 p_2 \dots p_r + 1$ sayısına bakalım. Her sayı gibi bu sayının da asal bir bölene vardır². Bu asal bölenlerden birine p diyelim. p asalı p_i asallarından biri olamaz, çünkü aksi halde, p , hem n 'yi hem de $p_1 p_2 \dots p_n$ çarpımını böldüğünden bu iki sayının farkı olan $n - p_1 p_2 \dots p_r = 1$ sayısını da bölerdi, ki bu olanaksızdır. Yani sonlu bir $\{p_1, \dots, p_r\}$ kümesi tüm asalları içeremez. \square

Diğer kanıtlara geçmeden önce yazıda kullanacağımız bir iki simgeyi açıklayalım.

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

ile pozitif doğal sayılar kümesini,

$$\mathbb{L} = \{\dots, 42, 41, 0, 1, 2, \dots\}$$

ile tamsayılar kümesini, $\mathbb{I} = \{2, 3, 5, 7, \dots\}$ ile de asallar kümesini gösteriyoruz.

Vereceğimiz ikinci kanıt Christian Goldbach'ın (Leonhard Euler'e 1730'da yazılmış bir

* M. Aigner, G.M. Ziegler, *Proofs from the BOOK*, Yayınevi xx, 3'üncü basım (2004), sayfa 3 - 6. Yazı, Galatasaray Üniversitesi Matematik Bölümü öğretim üyesi A. Muhammed Uludağ (muludag@gsu.edu.tr) tarafından "özgürce" çevrilmiştir.

1 MD-200x-xx, sayfa xx'te asalların sonsuzluğunun bir başka kanıtını daha vermiştik. Böylece MD okurları şu anda bu teoremin tam yedi değişik kanıtına sahiptir.

2 Asal sayıların bu temel özelliği için bkz. MD-200x-xx, sayfa xx-xx.

mektubundan), üçüncü kanıt anonim, dördüncüsü Euler'in, beşincisi Harry Fürtenberg'e ait, sonuncusu ise Paul Erdős'ün.

Üçüncü kanıt (çaktırmadan) gruplar kuramı, dördüncü kanıt (çaktırmadan biraz) analiz, beşinci kanıt (çaktırmadan) topoloji kullanacak, ama her biri temel lise düzeyinde bilgi gerektirecek. Ünlü Macar matematikçi Erdős'e ait olan son kanıt hem çok basit hem de asalların sonsuzluğundan daha fazlasını gösteriyor.

2. İkinci Kanıt [Goldbach]. Önce her $n = 0, 1, 2, \dots$ için $F_n = 2^{2^n} + 1$ olarak tanımlanan *Fermat sayılarına* bakalım. İşte ilk birkaç Fermat sayısı:

$$F_0 = 3,$$

$$F_1 = 5,$$

$$F_2 = 17,$$

$$F_3 = 257.$$

Kanıtımızda Fermat sayılarını kullanacağız. Önce Fermat sayıları arasındaki

$$M_{k=0}^{41} F_k = F_n \quad 4 \nmid n$$

tümevarımsal ilişkisini göstereceğiz. Asalların sonsuzluğu bu tümevarımsal ilişkiden kolayca çıkar: Gerçekten de eğer bir p sayısı $k < n$ için F_k ve F_n sayılarını bölüyorsa, birazdan kanıtlayacağımız yukardaki tümevarımsal ilişkiden dolayı, bu p sayısı 2^k 'yi de böler, yani p ya 1 'e ya da 2^k 'ye eşittir. Ama p , 2^k 'ye eşit olamaz çünkü Fermat sayıları tek sayılardır. Demek ki $k \equiv m \pmod{2}$ için F_k ve F_n sayıları birbirlerine asallar.

Dolayısıyla her n için F_n 'yi bölen bir p_n asalı seçersek sonsuz tane asal elde etmiş oluruz.

Tümevarımsal ilişkiyi göstermek için n üzerine tümevarım yapalım.

$n = 1$ için: $F_0 = 3$ ve $F_1 = 5$ olduğundan bu durumda eşitlik sağlanıyor.

Tümevarım adımını göstererek kanıtı tamamlıyoruz. Yani ilişkiyi n için geçerli olduğunu varsayıp aynı ilişkiyi $n + 1$ için kanıtlayacağız. Demek ki

$$M_{k=0}^{41} F_k = F_n \quad 4 \nmid n$$

eşitliğini varsayıp



$$\begin{aligned} \sum_{k=0}^n F_k &= F_{n+1} - 1 \\ \text{eşitliğini kanıtlayacağız. İşte kanıtı:} \\ \sum_{k=0}^n F_k &= (\sum_{k=0}^n F_k) F_n = (F_{n+1} - 1) F_n \\ &= (2^{n+1} - 1)(2^n + 1) \\ &= 2^{2n+1} - 1 = F_{2n+1} - 1 \quad \square \end{aligned}$$

3. Üçüncü Kanıt [Anonim]. n sonlu, p de en büyük asal olsun. *Mersenne sayısı* denen $2^p - 1$ sayısının her böleninin p 'den büyük olduğunu gösterelim, ki bu da istenen sonucu kanıtlar.

q sayısı $2^p - 1$ 'in asal bir böleni olsun ($q, 2$ olmaz), yani $2^p \equiv 1 \pmod{q}$ olsun. Demek ki 2 'nin her gücü, modülo q ,

$$\{2, 2^2, 2^3, \dots, 2^p\}$$

kümesinden bir sayıya denk.

Şimdi $k, 2^k \equiv 1 \pmod{q}$ denkleğini sağlayan en küçük pozitif doğal sayı olsun. $k = p$ eşitliğini kanıtlayacağız. p 'yi k 'ye bölelim; bölüm t , kalan da r olsun; yani bir $0 < r < k$ ve bir t için $p = kt + r$ eşitliği geçerli olsun. Şimdi modülo q hesaplayalım:

$$2^p \equiv 2^{kt+r} = (2^k)^t 2^r \equiv 2^r \pmod{q}.$$

Ama r, k 'den küçük ve k sayısı $2^k \equiv 1 \pmod{q}$ denkleğini sağlayan en küçük pozitif doğal sayı olarak seçilmişti. Demek ki r



Mersenne

sıfır olmak zorunda, yani $p = kt + r = kt$ ve k, p asalını bölüyor! Dolayısıyla ya $k = 1$ ya da $k = p$. Öte yandan $2^k \equiv 1 \pmod{q}$ denkliği yüzünden $k = 1$ olamaz. Demek ki $k = p$ ve $p, 2^p \equiv 1 \pmod{q}$ denkleğini sağlayan en küçük pozitif doğal sayı.

Bundan, yukardaki $\{2, 2^2, 2^3, \dots, 2^p\}$ kümesindeki sayıların modülo q birbirine denk olamayacakları çıkar, çünkü $1 < i < j < p$ için $2^i \not\equiv 2^j \pmod{q}$ ise o zaman, $0 < j - i < p$ ve $2^{j-i} \equiv 1 \pmod{q}$ ve bu bir çelişkidir.

Demek ki 2 'nin her gücü modülo q ,

$$\{2, 2^2, 2^3, \dots, 2^p\}$$

kümesinden tek bir sayıya denk ve bu kümede tam p tane sayı var.

Ayrıca bu kümedeki sayılar modülo q sıfır olmazlar, çünkü $q \nmid 2$. Ama q 'ye bölünmeyen her sayı modülo $q, \{1, 2, \dots, q-1\}$ kümesinden bir sayıya denktir.

Son iki paragraftan $p \mid q - 1 < q$ çıkar.

4. Dördüncü Kanıt [Euler]. Bir n sayısından küçük asalların kümesini S_n olarak yazalım. Şimdi şu toplama bakalım:

$$1 + 1/2 + 1/3 + \dots + 1/n \mid \sum_{m=1}^n 1/m.$$

Burada toplanan $1/m$ terimlerindeki m sayılarının asal bölenleri n 'den küçüktürler (elbette!) yani S_n kümesindedir. Dolayısıyla bu toplam

$$\sum_{m \in S_n} 1/m$$

sayısından küçük, çünkü burada yukardakinden daha fazla sayı topluyoruz. Demek ki,

$$\sum_{m=1}^n 1/m \geq \sum_{m \in S_n} 1/m.$$

Sadece n 'den küçük asallara bölünen her m ,

$$m \in S_n, p^k \mid m$$

çarpımı biçiminde *tam bir* biçimde yazıldığından,

$$\sum_{m=1}^n 1/m \geq \sum_{p \in S_n} (1/p^k).$$

Ama sağdaki terim,

$$\sum_{p \in S_n} (1/p^k)$$

çarpımına eşittir. (Bunu hemen göremeyebilirsiniz.)

Sadece iki değişik p ve q asalı için

$$(1/p^k)(1/q^3)$$

çarpımını üşenmeyip yaparsanız sözünü ettiğimiz eşitliği kavrarsınız.) Ayrıca $\sum_{p \in S_n} 1/p^k$ toplamı $1/p$ oranlı bir geometrik seri olduğundan,

$$\sum_{p \in S_n} 1/p^k \mid \frac{1}{1 - 1/p}.$$

Dolayısıyla,

$$\sum_{m=1}^n 1/m \geq \sum_{p \in S_n} \frac{1}{1 - 1/p}.$$

Eğer sonlu tane asal olsaydı, sağ taraftaki toplam sonlu bir sayı olurdu. Demek ki sol taraftaki $\sum_{m=1}^n 1/m$ toplamının n büyüdükçe her sayıyı geçebileceğini kanıtlarsak sonsuz tane asal sayı olduğunu da kanıtlamış oluruz. Bunu aşağıdaki gri karede gösterdik. \square

$$1 + 1/2 + 1/3 + 1/4 + \dots = \leftarrow$$

$\sum_{m=1}^n 1/m$ toplamının n sonsuza gittiğinde sonsuza gittiğini kanıtlayacağız. Bunu görmek oldukça kolay:

$$1/3 + 1/4 > 1/4 + 1/4 = 1/2$$

$$1/5 + \dots + 1/8 > 1/8 + \dots + 1/8 = 1/2$$

$$1/9 + \dots + 1/16 > 1/16 + \dots + 1/16 = 1/2$$

$$1/17 + \dots + 1/32 > 1/32 + \dots + 1/32 = 1/2$$

ve benzeri eşitsizlikleri (solda ve ortada 2^n tane sayı var) altalta toplarsak, sol tarafta $\sum_{m=3}^n 1/m$ buluruz, sağ taraftaysa sonsuz tane $1/2$ 'nin toplamını. Sağdaki toplam sonsuz olduğundan, daha büyük olan soldaki toplam da sonsuzdur.

Şimdi sıra topolojik kanıtta, ama kanıtı anlamak için topolojinin ne demek olduğunu bilmeye gerek yok! Tamsayılar kümesi \mathbb{L} 'de garip bir topoloji (topoloji ne demekse!) tanımlayacağız.

5. Beşinci Kanıt [Fürstenberg]. $a, b \in \mathbb{L}$ ve $a > 0$ için $a\mathbb{L} + b$ kümesi şöyle tanımlansın:

$$a\mathbb{L} + b = \{an + b : n \in \mathbb{L}\}$$

Şimdi bir $U \subseteq \mathbb{L}$ kümesi boşsa ya da her $b \in U$ için $a\mathbb{L} + b \geq U$ olacak şekilde bir $a > 0$ bulunuyorsa U 'ya *açık küme* diyelim.

Birkaç kolay olguya dikkat çekelim:

(A) *Açık kümelerin bileşimleri de açıktır.* Bu çok bariz.

(B) *İki açık kümenin kesişimi de açıktır.* Eğer U_1, U_2 açıksa ve $b \in U_1 \sim U_2$ ise öyle a_1 ve a_2 vardır ki $a_1\mathbb{L} + b \geq U_1$ ve $a_2\mathbb{L} + b \geq U_2$ sağlanır. Bundan da $a_1a_2\mathbb{L} + b \geq U_1 \sim U_2$ çıkar. Yani açıkların sonlu kesişimleri de açıktır.

(C) *Açık bir küme boş değilse sonsuzdur.* Bu, doğrudan açık kümenin tanımının bir sonucu.

(D) *Her $a\mathbb{L} + b$ ($a > 0$) biçiminde yazılan kümenin tümleyeni açıktır.* Bunun doğruluğu

$$\mathbb{L} \setminus (a\mathbb{L} + b) = \bigcup_{i=1}^{b-1} (a\mathbb{L} + i)$$

eşitliğinden ve (A)'dan çıkar.

(E) *$a\mathbb{L} + b$ biçiminde yazılan sonlu tane kümenin bileşiminin tümleyeni açıktır.* Bileşimin tümleyeni, tümleyenlerin kesişimi olduğundan, bu, yukarıda kanıtlanan (D) ve (B)'den çıkar.

Şu ana kadar asallardan bahsetmedik, ama artık sırası geldi. Eğer n sayısını p asalı bölüyorsa, $n \in p\mathbb{L} + 0 = p\mathbb{L}$ olur, Her $n \in \mathbb{L}$ sayısının asal bir p böleni olduğundan,

$$\mathbb{L} \setminus \{1, 41\} = \bigcup_{p \in \mathbb{L}} p\mathbb{L}$$

bulunur. Şimdi \mathbb{L} sonlu olsaydı, (E)'den dolayı $\bigcup_{p \in \mathbb{L}} p\mathbb{L}$ kümesinin tümleyeni açık olurdu. Ama bu kümenin tümleyeni $\{41, 1\}$ ve bu küme sonlu. Bu da (C) ile çelişkiye yol açıyor. \square

6. Altıncı Kanıt [Erdős]. Son kanıtımızda sadece asalların sonsuzluğunu değil, $\sum_{p \in \mathbb{L}} 1/p$ toplamının ıraksaklığını da göstereceğiz. Bu önemli olgunun ilk kanıtını Euler vermiştir (ve bu kanıt başlı başına ilginçtir) ama bizim burada sunacağımız Erdős'ün kanıtının baştan çıkarıcı bir güzelliği vardır.

Asalları p_1, p_2, p_3, \dots şeklinde küçükten büyüğe dizip $\sum_{p \in \mathbb{L}} 1/p$ toplamını yakınsak varsayalım. O zaman $\prod_{i \in \mathbb{L}} 1/p_i < 1/2$ eşitsizliğini sağlayan bir $r \in \mathbb{L}$ bulunur. p_1, \dots, p_r sayılarına *küçük* asallar

ve diğer p_{r+1}, p_{r+2}, \dots sayılarına da *büyük* asallar diyelim. Her N doğal sayısı için

$$\prod_{i \in \mathbb{L}} 1/p_i < N/2 \quad (1)$$

elbette. En az bir büyük asala bölünüp $0 < n \in \mathbb{L}N$ eşitsizliğini sağlayan n doğal sayılarının sayısını N_b ile, sadece küçük asallara bölünüp $0 < n \in \mathbb{L}N$ eşitsizliğini sağlayan n doğal sayılarının sayısını N_k ile gösterelim. (1'i bölen her asal küçüktür!) Yeterince büyük bir N için $N_b + N_k < N$ eşitsizliğini kanıtlayacağız ki bu bizi aradığımız çelişkiye götürecektir çünkü tanıma göre $N_b + N_k = N$ olmalı.

p 'ye bölünen N 'den küçük bir doğal sayı, $s \in \mathbb{L}N/p$ eşitsizliğini sağlayan bir s doğal sayısı için ps biçiminde yazılır. Demek ki N 'den küçük ve p 'ye bölünen sayılar s 'lerin sayısı kadardır, yani $[N/p]$ 'dir (N/p kesirli sayısının tam kısmı). Dolayısıyla (1)'den ve tanımdan

$$N_b \cdot \prod_{i \in \mathbb{L}} 1/p_i \leq [N/p_i] \leq N/p_i < N/2 \quad (2)$$

elde edilir.

Şimdi N_k 'yi hesaplayacağız. Her n sayısını 1'den büyük bir kareye bölünmeyen bir a_n sayısı için $n = a_n b_n^2$ biçiminde yazabiliriz; örneğin $24 = 6 \cdot 2^2$. Eğer $n \in \mathbb{L}N$, sadece küçük asallara bölünen bir doğal sayıysa, her a_n farklı küçük asalların çarpımı olduğundan karesiz kısım için tam 2^r tane seçeneğimiz vardır. Dahası, $b_n \cdot \prod_{i \in \mathbb{L}} 1/p_i < N$ eşitsizliğinden dolayı b_n için en fazla $\cdot N$ tane seçeneğimiz var. Demek ki $N_k \leq 2^{2r} \cdot N$.



Erdős

(2) eşitsizliği her N için geçerli olduğundan, (1)'le çelişmek için $2^r \cdot N \leq N/2$ eşitsizliğini sağlayan bir N bulmak yeter. Bu koşul da $\cdot N \leq 2^{2r+1}$ eşitsizliğine denk. N 'yi 2^{2r+2} almak işi görür. \blacklozenge

Kaynakça

- [1] B. Artmann, *Euclid, The Creation of Mathematics*, Springer-Verlag, New York, 1999.
- [2] P. Erdős, *Über die Reihe $\sum 1/p$* , *Mathematica*, Zutphen B 7 (1938), 1-2.
- [3] L. Euler, *Introductio in Analysin Infinitorum*, Tomus Primus, Lausanne 1748, Opera Omnia, Ser. 1, Vol. 8.
- [4] H. Fürstenberg, *On the infinitude of primes*, *Amer. Math. Monthly* 62 (1955), 353.