Unutulmuş Bir Problem: Feit-Thompson Sanısı

Olcay Coşkun / olcaycoskun@gmail.com

Gruplar teorisindeki en derin sonuçlardan biri Feit-Thompson Teoremi, bir diğer ismiyle Tek Mertebe Teoremi'dir. Burnside'ın 1911 tarihli sanısı, abelyen olmayan her bir basit ve sonlu grubun mertebesinin çift olduğunu iddia etmektedir. Bu sanıya denk olan ve mertebesi tek sonlu grupların çözülebilir[1] olduğu önermesi, Burnside'ın sanısından 50 yıl kadar sonra Feit ve Thompson tarafından kanıtlanmıştır [3].

Bu yazıda Feit-Thompson Teoremi'nin ispatından doğan bir sanıdan söz edeceğiz. Önce kısaca teoremden bahsedelim.

Feit-Thompson Teoremi'ni değerli kılan en önemli özellik, yıllarca sürecek ve 12.000 sayfadan daha fazla tutacak olan Basit Sonlu Grupların Sınıflandırılması Teoremi'ne ön ayak olmasıdır. Feit-Thompson'ın çelişki bulma (ya da olmayana ergi) yöntemini kullanan kanıtı 255 sayfa uzunluğundadır. Bu kanıta ulaşabilmek için, temsiller ve gruplar teorilerinden temel ve ileri düzey birçok sonucu yeni yöntemlerle harmanlamak gereklidir.[2,3] Ortaya çıkan yöntemler daha sonra gruplar teorisinin en kullanışlı yöntemleri arasına girecektir.

Feit-Thompson'ın kanıtının son çelişki adımında, o noktaya kadar ortaya çıkmış bazı grupların üreteçleri üzerinden yapılan uzun bir tartışmayla istenilen çelişki elde edilmektedir. Yazarlar, çelişki adımındaki bu tartışmaların verildiği 50 sayfanın, asal sayılara has, simetrisindeki güzellikle dikkat çeken, bir iddianın doğru olması durumunda kısaltılabileceğini öngörmüşlerdir. Yazımızda bu iddiayı ve özel durumlardaki çözümlerini tartışacağız.

Feit-Thompson Sanısı

Sanı 1. *$p < q$ asal sayılar olmak üzere $A = \frac{q^p-1}{q-1}$, $B = \frac{p^q-1}{p-1}$'i bölmez.*

Burada A ve B sayılarının çok hızlı büyüyeceğine dikkat edelim. Örneğin, başlangıç değerleri olan $p = 2, q = 3$ alınırsa, $A = 4$ ve $B = 7$'dir. Öte yandan $p = 5, q = 11$ alındığında, $A = 16.105$ ve $B = 12.207.031$ bulunurken, $p = 11$ ve $q = 13$ olduğunda $A = 149.346.699.503$ ve $B = 3.452.271.214.393$ olur. Bu durum problemi hesaplamayla yanlışlamayı zorlaştırmaktadır.

Feit-Thompson Sanısı'ndan daha güçlü olan ve Stephens Sanısı olarak bilinen bir problem daha vardır.

Sanı 2. *Birbirinden farklı p ve q asal sayıları için A ve B aralarında asaldır.*

Bu iddianın yanlış olduğu yine Stephens tarafından gösterilmiştir [8]. Stephens'ın bilgisayar yardımıyla bulduğu örneğe göre, $p = 17, q = 3.313$ olduğunda 112.643 sayısı A ve B'nin en büyük ortak bölenidir. Yazımızın son bölümünde Stephens'ın bu örneği bulmak için kullandığı yöntemden de bahsedeceğiz.

Her ne kadar yanlışlanmış olsa da Stephens Sanısı da ilginçliğini koruyor. Çünkü yukarıda verilen örnek dışında, bu sanıya karşıt örnek bulunamamıştır. Hatta Dilcher ve Knauer yukarıdaki örneğin biricik karşıt örnek olabileceğini iddia etmişlerdir [2].

Aradan geçen 60 yıla yakın süre içinde, Feit-Thompson Sanısı'nın sadece basit özel durumları kanıtlanabilmiştir. Diğer taraftan Feit-Thompson Teoremi'nin son çelişkisi için gereken basitleştirme, sanının daha teknik bir yorumu yapılarak elde edilmiştir [1]. Böylelikle Feit-Thompson Sanısı, tamamen asal sayılara has bir probleme dönüşmüştür. Bu problemin bugüne kadar çözülememiş olmasının bir sebebi, grup teorisyenlerinin ilgisini çekmemeye başlaması ve sayı teorisyenlerinin ilgisini çekecek kadar ilginç olmaması olabilir.

Sanının Akla Yatkınlığı

Öncelikle $p < q$ olduğunda $A < B$ olduğunu gösterelim. Aslında bunun doğru olması için p ya da q'nun asal sayı olması gerekli değil. Dolayısıyla bu kanıt için p ve q rasgele tamsayılar alınabilir [7].

[1] Yazımızda kullanmayacağımız için grup teoretik tanımlara yer vermiyoruz.

[2] Kanıtın, o güne kadar gruplar teorisinde olmayan, uzun tartışmalarla sonuca ulaşılabileceği fikrini ortaya çıkarması da ayrıca çığır açıcı olmuştur. Kısa süre sonra, bu örneği takip eden ve yüzlerce sayfa uzunluğunda başka sınıflandırma kanıtları da ortaya çıkmıştır.

[3] Teoremin kısa bir kanıtını bulma problemi hâlâ grup teorisyenlerinin ilgisini çeken en önemli problemlerden birisidir.

İlk olarak, $p = 2$ ise,

$$A = \frac{q^2-1}{q-1} = q+1 \quad \text{ve} \quad B = 2^q - 1\text{'dir.}$$

$q \geq 3$ sağlandığında $2^q > q+1$ olacağı aşikârdır.

$p > 2$ ise $p^q > q^p$ eşitsizliği sağlanır. Gerçekten de logaritma fonksiyonu artan olduğundan, bu eşitsizlik $q \ln p > p \ln q$'ya ve dolayısıyla da,

$$\frac{q}{\ln q} > \frac{p}{\ln p} \tag{1}$$

eşitsizliğine denktir. Bu sebeple (1)'i kanıtlamak yeterlidir. Bunun için $f(x) = \frac{x}{\ln x}$ alalım. $f(x)$'in türevi, türevin bölüm kuralını kullanarak,

$$f'(x) = \frac{\ln x - 1}{\ln^2 x}$$

şeklinde hesaplanır. Buradan da $p \geq 3$ ise $\ln p > 1$ bize $f'(p)$'nin pozitif olduğunu verir. Sonuç olarak, $p \geq 3$ olduğunda $f(p)$ artan bir fonksiyondur ve (1) eşitsizliği sağlanır. Bu sayede

$$B = \frac{p^q-1}{p-1} > \frac{p^q-1}{q-1} > \frac{q^p-1}{q-1} = A$$

eşitsizliklerini elde etmiş oluruz.

Feit-Thompson Sanısı, $p = 2$

$p = 2$ olduğunda Feit-Thompson Sanısı aşağıdaki kanıtlanması kolay biçimini alır.

Önerme 1. *$q > 2$ asal sayı olmak üzere,*

$$q+1 \nmid 2^q - 1$$

yani, $q+1$, 2^q-1'i bölmez.

Bu yoruma ulaşmak için iki kare farkı formülünü, yani $a^2 - b^2 = (a-b)(a+b)$'yi kullandık. Önerme aşikârdır çünkü $q+1$ çift sayı iken $2^q - 1$ tek sayıdır.

Feit-Thompson Sanısı, $p = 3$

Sıradaki özel durum için p'yi bir sonraki asal sayı olan 3 alıyoruz. Bu kez elde ettiğimiz yorum aşağıda [5].

Teorem 1. *$q > 3$ asal sayı olmak üzere, $q^2 + q + 1, 3^q - 1$'i bölmez.*

Dikkat edilirse, $q^2 + q + 1$ tek sayı olacağından, $\frac{3^q-1}{2}$ yerine $3^q - 1$ de alabiliriz. Le tarafından verilen bu özel durumun kanıtını özetleyelim [5].

İlk olarak, saçmalığa indirgeyebilmek amacıyla, $n = q^2+q+1$'in 3^q-1'i böldüğünü varsayalım. Bu durumda n'nin asal sayı olması gerektiğini iddia ediyoruz. Gerçekten de eğer n asal değilse, $n < (q+1)^2$ eşitsizliği sağlandığından, n q'dan küçük bir asal bölene sahiptir. Bu asal böleni k ile gösterelim. n'nin tek olması $k > 2$'yi verirken, $3^q - 1$'in n'ye bölünebilmesi $k > 3$'ü verir.

Şimdi Fermat'nın Teoremi'nden $3^{k-1} \equiv 1 \pmod{k}$ denkliğini ve yukarıdaki bölünebilme varsayımından ise $3^q \equiv 1 \pmod{k}$ denkliğini elde ederiz. Ama bu durumda $k - 1 \equiv 0 \pmod{q}$ olmalıdır ki bu sonuç $3 < k < p$ eşitsizlikleriyle çelişir. Dolayısıyla n asal sayı olmalıdır.

Böylece $q > 3$ asal sayısı için $n = q^2 + q + 1$'in $3^q - 1$'in asal böleni olduğu sonucuna ulaştık. Eğer $q \equiv 1 \pmod 3$ olsaydı, bu durumda $n \equiv 1^2+1+1 \equiv 0 \pmod 3$, yani, $3 \mid n$ çıkardı. Ama $n > 3$ bir asal sayı olduğundan bu denklik gerçekleşemez. Öyleyse $q \equiv 2 \pmod 3$ olmalı ki bu bize $n \equiv 1 \pmod 3$ denkliğini de verir. Özetlersek

$$q \equiv 2 \pmod 3 \quad \text{ve} \quad n \equiv 1 \pmod 3$$

denkliklerini bulduk. Kanıtın son bölümü biraz teknik olduğu için ayrıntılardan kaçınacağız. Saçmalığa indirgeme çabası içinde olduğumuzu hatırlayın. Bu amaca ulaşabilmek için iki teoreme daha ihtiyacımız var. İlk olarak, n asal sayısı için,

$$a^2 + 3b^2 = 4n$$

denkleminin doğal sayılar kümesinde, a ve b aralarında asal olma koşulunda, sadece 2 çözümü bulunduğunu iddia ediyoruz. Aslında bu çözümleri bulmak kolay:

$$\begin{aligned} 4n &= 4(q^2+q+1) \\ &= (2q+1)^2 + 3 \\ &= (q+2)^2 + 3q^2. \end{aligned}$$

Ancak, başka bir çözüm bulunamayacağının bu yazıda anlatabileceğimiz bir kanıtını bulamadık. Teknik bir kanıt için [4]'e bakınız.

İhtiyacımız olan ikinci teoremse 3'ün mod n'de bir kübik kalıntı[4] olması durumunda,

$$4n^2 = L^2 + 27M^2$$

eşitliğini ve $3 \mid M$ koşulunu sağlayan, aralarında asal L ve M tamsayılarının varlığını veriyor [6].

Bu teoremin de yazıda yer verebileceğimiz bir kanıtı yok. Ancak, bu teoremi ilkiyle birleştirdiğimizde, 3'ün mod n'de kübik kalıntı olması durumunda, $a^2 + 3b^2 = 4n$ denkleminin, b'nin 9'a bölünebildiği bir çözümü olduğunu buluruz. Ama yukarıda bulduğumuz çözümleri göz önüne alırsanız, çözümlerin ikisinin de bu koşulu sağlamadığını (birincide $b = 1$, ikincide $b = q^2$'dir.) görebilirsiniz. Böylelikle aradığımız çelişkiye ulaşmış oluruz.

[4] Eğer $a \equiv x^3 \bmod n$ denkliğini sağlayan bir x tamsayısı varsa a'ya mod n'de bir kübik kalıntı diyoruz.

Geriye sadece 3'ün mod n'de kübik kalıntı olduğunu göstermek kaldı. İlkin, n asal sayı olduğundan, n'ye bölünmeyen her u, mod n'deki kalan sınıfları için bir üreteç olur. Bir diğer deyişle, her kalan sınıfı m'yi bir $t \in \mathbb{Z}$ için $m \equiv u^t \bmod n$ biçiminde yazabiliriz. Öyleyse, $t \in \mathbb{Z}$ olmak üzere,

$$3 \equiv u^t \pmod{n}$$

yazalım. Her iki tarafın $q+1$'inci kuvvetini alırsak

$$3^{q+1} \equiv u^{t(q+1)} \pmod{n}$$

elde ederiz. Ama $3^p \equiv 1 \bmod n$ denkliğini varsaymıştık, o yüzden,

$$3 \equiv u^{t(q+1)} \pmod{n}$$

buluruz. Son olarak, $q \equiv 2 \bmod 3$ olduğundan $q+1$ 3'e bölünür, yani, 3 mod n'de bir kübik kalıntıdır.

Feit-Thompson Sanısı, $p > 3$

3'ten büyük asallar için de çeşitli özel durumların kanıtları bilinmektedir ancak bu kanıtlar hem sayılar teorisinden hem de temsiller teorisinden sonuçlar kullandığı için burada yer vermeyeceğiz. İlgili okurların [7]'ye bakmasını öneririz.

Stephens Sanısı'na Karşıt Örnek Nasıl Bulunur?

Son bölümde, Stephens Sanısı'yla ilgili hesaplama tekniğine göz atacağız. Yukarıda da belirttiğimiz gibi, $(q^p-1)/(q-1)$ çok hızlı büyüdüğünden doğrudan hesaplamayla karşıt örnek bulmak neredeyse imkansızdır.

Peki, o hâlde nasıl hesap yapacağız? Stephens, hesaplar için kullanacağı iki kilit indirgeme kanıtlamıştır [2]. İlk olarak bu sonuçları inceleyelim.

Önerme 2. *$p \neq q$ asal sayılar olsun.*

(a) $p = 2$ ise A ve B aralarında asaldır.

(b) r A ve B'nin ortak asal çarpanıysa, bir doğal sayı λ için,

$$r = 2\lambda pq + 1$$

eşitliği sağlanır.

Kanıt. a) Yukarıda, $p = 2$'yken, $A = q+1$'in $B = 2^q - 1$'i bölmediğini görmüştük. Şimdiyse ortak bölenleri olamayacağını kanıtlayalım. Öncelikle B'nin her asal çarpanı r için $2^q \equiv 1 \pmod{r}$ sağlanır. Ama bu durumda, Fermat'nın Teoremi'nden dolayı q, $r-1$'i böler. Diğer taraftan, eğer r'nin $A = q+1$'i de bölmesini istersek, $r = q+1$ buluruz ki $q > 2$ koşulunda bu mümkün değildir. Bu sonuç, A ve B'nin ortak böleni olamayacağı anlamına geliyor.

b) Şimdi $r \mid A$ doğruyken, $r \mid p^q - 1$, ya da buna denk olarak, $p^q \equiv 1 \pmod{r}$'de doğrudur. Çünkü $p^q - 1 = (p-1)\cdot A$'dır ve r, $p-1$'i bölemez. Gerçekten, eğer $r \mid p-1$ olsaydı, o zaman

$$A = 1 + p + p^2 + \cdots + p^{q-1} \equiv q \pmod{r}$$

elde edilirdi ve dolayısıyla $r \mid q$, yani $r = q$ çıkardı. Ama q B'yi bölmezken bu mümkün değildir. Sonuç olarak $p^q \equiv 1 \pmod{r}$'dir ve Fermat'nın Teoremi'nden, $q \mid r-1$ buluruz.

Savımız p ve q'ya göre simetrik olduğundan, $q^p \equiv 1 \pmod{r}$ ve $p \mid r-1$ sonuçları da bedavaya elde edilir.

Böylelikle, hem $p \mid r-1$, hem de $q \mid r-1$'i bulmuş olduk. Ayrıca r tek sayı olduğundan $2 \mid r-1$'de doğrudur. Hepsini bir araya getirdiğimizde,

$$r = 2\lambda pq + 1$$

eşitliğini elde ederiz. □

Bu sonuçla birlikte, A ve B'nin ortak çarpanını bulmak için, $r = 2\lambda pq + 1$ asal sayısının

$$p^q \equiv q^p \equiv 1 \pmod{r}$$

denkliklerini sağlayıp sağlamadığını kontrol edebiliriz. Olası r seçeneklerini sınırladığımız için bu hesap kısmen daha kolaydır. Stephens karşıt örneğini, yukarıdakilere ek, $p < 443$, $pq < 200.000$ ve $r < 400.000$ koşulları altında çalışarak bulmuş. Dikkat edilirse, Stephens'ın r'si $2pq+1$'dir, yani $\lambda = 1$'dir.

Kaynaklar

[1] Bender, H., Glauberman, G., Local analysis for the odd order theorem, LMS Lecture Notes Series 188, 1995.

[2] Dilcher, K., Knauer, J., On a conjecture of Feit and Thompson, in High primes and misdemeanours. Fields Institute (2004), 169-178.

[3] Feit, W., Thompson, J., Solvability of groups of odd order, Pacific J. Math. 13 (1963), 775 - 1029.

[4] Hua, L. K., Introduction to number theory, Springer Verlag, 1982.

[5] Le, M., A divisibility problem concerning number theory, Pure and Appl. Math. Quart. 8 (2012), 689-691.

[6] Lemmermeyer, F., Reciprocity laws, Springer Verlag, 2000.

[7] Motose, K., Notes on the Feit-Thompson conjecture, Proc. Japan Acad. 85 (2009), 16-17.

[8] Stephens, N. M., On the Feit-Thompson conjecture, Math. Comp. 25 (1971), 625.