Fermat Teoreminin Zayıf Bir Şekli

Eldar Hacılarev*

Meşhur Fermat Teoremi'ni herhalde duymuşsunuzdur. Bu teoreme göre $n \geq 3$ için $x^n + y^n = z^n$ eşitliğini sağlayan x, y, z, n doğal sayıları (yani pozitif tamsayılar) yoktur. Her ne kadar teorem diye adlandırılsa da, birçok matematikçinin uğraşlarına rağmen bu önerme şimdiye kadar kanıtlanmış değildir.

$n = 2$ halinin çözümü bilinmektedir; $x^2 + y^2 = z^2$ denkleminin doğal sayılar kümesinde sonsuz sayıda farklı çözümü vardır. Örneğin; $x(u_1, u_2) = u_1^2 - u_2^2$, $y(u_1, u_2) = 2u_1u_2$, $z(u_1, u_2) = u_1^2 + u_2^2$ iki değişkenli polinomları $x^2 + y^2 = z^2$ özdeşliğini sağlarlar; buna göre de u_1, u_2 yerine keyfi $u_1 > u_2$ doğal sayılarını koyarsak, bu denklemin doğal sayılardan oluşan çözümlerini elde ederiz.

Problem 1. Yukarıdaki önermeyi kanıtlamaya çalışınız.

$n \geq 3$ olduğunda $x^n + y^n = z^n$ özdeşliğini sağlayan, tam katsayılı $x(u_1, u_2, \ldots, u_k)$, $y(u_1, u_2, \ldots, u_k)$, $z(u_1, u_2, \ldots, u_k)$ polinomları olsaydı, $u_1, u_2, \ldots, u_k$ değişkenleri yerine belirli doğal sayıları yazarak, denklemin doğal sayı çözümlerini elde ederdik ki, bu da Fermat Teoremi'nin yanlış olduğunu gösterirdi. Ancak bu mümkün değil. Bu yazımızda biz, $n \geq 3$ için, derecelerinden biri en az bir olan (yani sabit olmayan), ikişer ikişer aralarında asal, tam katsayılı ve $x^n + y^n = z^n$ özdeşliğini sağlayan x, y, z polinomları bulunamayacağını göstereceğiz. Okuyucunun karmaşık sayılarla tanışık olduğunu ve polinomların asal çarpanlara, karmaşık sayılarla çarpım dışında, yalnız bir şekilde ayrıldığını bildiğini kabul ediyoruz.

Teorem. *$n \geq 3$ için, $x^n + y^n = z^n$ özdeşliğini sağlayan, çok değişkenli, ikişer ikişer aralarında asal, derecelerinden biri en az bir olan, karmaşık katsayılı üç polinom yoktur.*

Teoremin kanıtına geçmeden bazı noktaları açıklayalım. $x(u_1, u_2, \ldots, u_k)$, $y(u_1, u_2, \ldots, u_k)$, $z(u_1, u_2, \ldots, u_k)$ polinomları ikişer ikişer aralarında asal demekle, bunlardan herhangi ikisinin derecesi en az bir olan $r(u_1, u_2, \ldots, u_k)$ gibi bir ortak çarpanı olmadığını söylüyoruz. Yukarıda tam katsayılı polinomlardan söz etmiştik. Halbuki teorem karmaşık katsayılı polinomlar için geçerli; yani istediğimizden de genel. Kanıtta da göreceğimiz gibi matematikte çoğu kez daha genel bir önermeyi göstermek daha kolaydır.

Olmayana ergi yöntemini kullanacağız. $n \geq 3$ halinde aşağıdaki koşulları sağlayan $x(u_1, u_2, \ldots, u_k)$, $y(u_1, u_2, \ldots, u_k)$, $z(u_1, u_2, \ldots, u_k)$ polinomlarının var olduğunu varsayalım. Yani:

i) $x(u_1, u_2, \ldots, u_k)$, $y(u_1, u_2, \ldots, u_k)$, $z(u_1, u_2, \ldots, u_k)$ polinomları ikişer ikişer aralarında asaldır.

ii) $[x(u_1, u_2, \ldots, u_k)]^n + [y(u_1, u_2, \ldots, u_k)]^n = [z(u_1, u_2, \ldots, u_k)]^n$ özdeşliği sağlanır.

iii) $x(u_1, u_2, \ldots, u_k)$, $y(u_1, u_2, \ldots, u_k)$, $z(u_1, u_2, \ldots, u_k)$ polinomlarından en az biri sabit değildir.

Aşağıda geçen tüm polinomlarda artık $u_1, u_2, \ldots, u_k$ harflerini yazmayacağız.

Kanıt yolumuz şöyle olacaktır: İlk olarak x, y, z polinomlarından i)-iii) koşullarını gerçekleyen yeni x_0, y_0, z_0 polinomları türeteceğiz. Bu x_0, y_0, z_0 polinomlarının dereceleri, x, y, z polinomlarının derecelerinin en büyüğünden daha küçük olacak. Sonra bu işlemleri x, y, z yerine x_0, y_0, z_0 polinomlarına uygulayarak dereceleri tekrar küçülteceğiz ve bu işlemi tekrar tekrar sürdüreceğiz. Öte yandan polinomun derecesi bir doğal sayı olduğundan dereceleri küçültme işlemi sonsuz kere yapılamaz. Bu çelişki ise teoremin doğru olduğunu gösterir.

Kanıtı birkaç adıma ayıralım:

1. $x^n + y^n$ ifadesini çarpanlara ayıracağız. Karmaşık sayıları kullanarak $w^n + 1 = 0$ denkleminin kökleri

$$\epsilon_1 = \cos\frac{\pi}{n} + i\sin\frac{\pi}{n},$$

* Azerbaycan Bilimler Akademisi üyesi

$$\epsilon_2 = \cos\frac{3\pi}{n} + i\sin\frac{3\pi}{n}, \ldots,$$
$$\epsilon_n = \cos\frac{(2n-1)\pi}{n} + i\sin\frac{(2n-1)\pi}{n}$$

olarak bulunur. Bundan $w^n + 1 = (w - \epsilon_1)(w - \epsilon_2)\cdots(w - \epsilon_n)$ bağıntısını elde ederiz. O halde:

$$x^n + y^n = y^n[(\frac{x}{y})^n + 1] = y^n\left(\frac{x}{y} - \epsilon_1\right)$$
$$\left(\frac{x}{y} - \epsilon_2\right)\cdots\left(\frac{x}{y} - \epsilon_n\right)$$
$$= (x - \epsilon_1 y)(x - \epsilon_2 y)\cdots(x - \epsilon_n y)$$

çıkar.

2. Karmaşık sayıları kullanarak, $(\epsilon_1)^n = -1$ olduğundan, $x^n + y^n = z^n$ eşitliği $x^n + y^n + (\epsilon_1 z)^n = 0$ şeklinde yazılabilir. İfade x, y ve $\epsilon_1 z$ terimlerine göre simetriktir; başka bir deyişle Teoremin ifadesinde $x^n + y^n + z^n = 0$ bağıntısını da kullanabilirdik.

i)-iii) koşullarını gerçekleyen x, y, z polinomlarının derecelerinin en büyüğü m olsun. iii) koşuluna göre $m > 0$ dır. Az önce söylediğimiz nedenden m sayısının z polinomunun derecesi olduğunu kabul edebiliriz.

3. $x - \epsilon_k y$ polinomları ikişer ikişer aralarında asaldır. Eğer sabitten farklı bir d polinomu $k \neq m$ için $x - \epsilon_k y$ ve $x - \epsilon_m y$ polinomlarının ortak böleni olsaydı, d iki polinomun farkı $(\epsilon_m - \epsilon_k)y$ yi ve dolayısıyla ($\epsilon_m - \epsilon_k$) sıfırdan farklı bir sabit olduğundan) y polinomunu da bölerdi. Buradan $x = (x - \epsilon_k y) + \epsilon_k y$ polinomunun da d ile bölündüğü çıkardı ki bu ise x ve y aralarında asal olduğundan mümkün değildir.

4. **Problem 2.** İkişer ikişer aralarında asal polinomların çarpımı bir polinomun n-inci kuvvetine eşitse, her bir çarpanın da bir n-inci kuvvet olduğunu kanıtlayınız. Kanıtta asal çarpanlara tek olarak ayrılma teoreminden yararlanınız.

5. $x^n + y^n = (x - \epsilon_1 y)(x - \epsilon_2 y)\cdots(x - \epsilon_n y) = z^n$ ve $x - \epsilon_k y$ çarpanları ikişer ikişer aralarında asal olduğundan, her bir $x - \epsilon_k y$ çarpanı da bir n-inci kuvvettir, yani $x - \epsilon_k y = w_k^n$ şeklindedir; buradaki w_k bir polinomdur. w_k polinomunun derecesini m_k ile gösterelim.

w_k polinomlarının arasından derecesi en büyük olanı seçelim; bunun w_1 polinomu olduğunu kabul edebiliriz.

6. $m_1 < m$.

z polinomunun derecesi m olduğundan $m_1 \leq m$ olduğu açıktır. Eğer $m_1 = m$ olsaydı $k > 1$ için tüm $x - \epsilon_k y$ çarpanları sabit olurdu. $x - \epsilon_2 y$ ve $x - \epsilon_3 y$ çarpanlarını ele alalım. ($n \geq 3$ olduğundan bu mümkündür.) $x - \epsilon_2 y = A$ ve $x - \epsilon_3 y = B$ dersek;

$$(B - A)x - (B\epsilon_2 - A\epsilon_3)y = 0$$

yani $x = \frac{B\epsilon_2 - A\epsilon_3}{B - A} y$ olur. ($A \neq B$ dir.) Bu ise x ve y nin aralarında asal olmasıyla çelişir.

7. x, y, z polinomlarından, ortak çarpanları olmayan, Fermat denklemini sağlayan ve dereceleri m den küçük olan yeni üç polinom oluşturmak istiyorduk. Belli sabitlerle çarpılmış w_1, w_2, w_3 polinomlarının bu koşulları sağlayacağını göstereceğiz.

$$\begin{aligned} x - \epsilon_1 y &= w_1^n \\ x - \epsilon_2 y &= w_2^n \\ x - \epsilon_3 y &= w_3^n \end{aligned}$$

sistemi vardır. Hepsi birden sıfır olmayan öyle c_1, c_2, c_3 sayıları seçelim ki bu sistemdeki eşitlikleri bu sayılarla çarpıp topladığımızda sol taraf sıfır olsun. Bunun için

$$\begin{aligned} c_1 + c_2 + c_3 &= 0 \\ c_1\epsilon_1 + c_2\epsilon_2 + c_3\epsilon_3 &= 0 \end{aligned}$$

sisteminin sağlanmasının yeterli olacağı açıktır. Sıfırdan farklı bir çözüm bulmak kolaydır. $c_3 = 1$ kabul edip, çıkan iki bilinmeyenli iki denklemi çözmek yeter.

Problem 3. Bu hesaplamayı yapınız.

c_1, c_2, c_3 sayılarını bulduktan sonra şunu elde ederiz:

$$\begin{aligned} c_1 w_1^n + c_2 w_2^n + c_3 w_3^n &= 0 \\ (\sqrt[n]{c_1} w_1)^n + (\sqrt[n]{c_2} w_2)^n + (\sqrt[n]{c_3} w_3)^n &= 0 \end{aligned}$$

Bu, yeni üç $\sqrt[n]{c_1} w_1$, $\sqrt[n]{c_2} w_2$, $\sqrt[n]{c_3} w_3$ polinomun da, x, y, z polinomlarının sağladığı i)-iii) koşullarını gerçeklediği kolayca gösterilir. Bununla beraber yeni polinomların dereceleri küçülmüştür.

Kullandığımız kanıt yöntemi Fermat tarafından bulunmuş olup, "sonsuz indirgeme" yöntemi olarak adlandırılır. Bu yöntem Fermat denkleminin doğal sayılar kümesinde çözülemeyeceğini kanıtlamak için kullanılamıyor, zira x, y tamsayılar olmak üzere $x - \epsilon_k y$ şeklindeki sayılar için asal çarpanlara tek olarak ayrılma teoremi doğru değildir. Bu sorunun incelenmesi ile matematikte şimdi gelişmekte olan cebirsel sayılar teorisi ilgilenir.