

$$a_2 = \frac{1}{6 \cdot 2^{k-1}} \left[ 2 \binom{k+1}{2} + \binom{k+1}{3} \right],$$

$$a_3 = \frac{1}{6 \cdot 2^{k-1}} \left[ 2 \binom{k+1}{4} + \binom{k+1}{5} \right]$$

$$a_j = \frac{1}{6 \cdot 2^{k-1}} \left[ 2 \binom{k+1}{1} + \binom{k+1}{0} \right]$$

biçiminde tayin edilebilir.  $k+1$ 'in tek olma durumu da benzer biçimde ele alınabilir.

Son olarak şu sonucu göstermeyi de okuyucuya bırakıyoruz. Her  $k$  çift sayısı için  $S_k(n)/S_2(n)$  ifadesi  $S_1(n)$ 'in rasyonel katsayılı bir polinomu olarak ifade edilebilir.

#### KAYNAKÇA

- [1] N.Çalışkan, Gauss Formülünün Genelleştirilmesi Matematik Dünyası Cilt: 5, Sayı: 1
- [2] T.Terzioğlu, Gauss Formülünün Genelleştirilmesi Matematik Dünyası Cilt: 2, Sayı: 3
- [3] D.Allison, Problem 10290, American Mathematical Monthly, 100, 290 (1993)
- [4] G.H.Hardy, E.M.Wright, An Introduction to the Theory of Numbers, 1979

## KUADRATİK REZİDÜLER

Aytek Erdil \*

Bu yazıda, Sayılar Kuramı'nın çok ünlü bir teoreminin kanıtını vereceğiz. Bu teorem 1783 de Euler tarafından ifade edilmiş ve ilk kez 1796'da Gauss tarafından kanıtlanmıştır.

İlgilenenler, teoremin bazı basit uygulamalarını 96/2 Problem Semineri'nin çözümlerinden inceleyebilirler.

### Kuadratik Rezidü ve Legendre Simgesi

$a$  ve  $n$ ,  $(a, n) = 1$  ve  $n > 0$  olacak biçimde tamsayılar olsunlar  $y^2 \equiv a \pmod{n}$  denkleğinin bir çözümlü varsa  $a \pmod{n}$  de kuadratik rezidüdür denir.  $P$  bir asal ve  $(a, p) = 1$  olmak üzere  $\left(\frac{a}{p}\right)$  Legendre simgesi,  $a \pmod{p}$  de bir kuadratik rezidüyse 1'e değilse  $-1$ 'e eşit olarak tanımlanır.

**Lagrange Teoremi:**  $(a_0, p) = 1$   $P$  bir asal sayı olmak üzere  $P(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{p}$  denkleğinin,  $\pmod{p}$ 'de herhangi ikisi birbirine denk olmayan en çok  $n$  çözümlü vardır.

**Kanıt:** Teoremi  $n$  üzerinde tümevarımla kanıtlayacağız.  $(a_0, p) = 1$  olduğundan  $n = 1$

için tek çözümlü vardır. Şimdi teoremin  $n - 1$  dereceli polinom için doğru olduğunu kabul edelim. Herhangi bir  $a$  tamsayısı için  $P(x) - P(a) = a_0(x^n - a^n) + a_1(x^{n-1} - a^{n-1}) + \dots + a_{n-1}(x - a) = (x - a)Q(x)$  olacak biçimde tamsayı katsayılı, başkatsayısı  $a_0$  olan ve  $(n - 1)$ 'inci dereceden bir  $Q(x)$  polinomunun bulunduğu görülmektedir.  $P(x) \equiv 0 \pmod{p}$  denkleğinin bir  $a$  çözümlü varsa diğer tüm çözümler  $(x - a)Q(x) \equiv 0 \pmod{p}$  denkleğini sağlar. Tümevarım varsayımımızdan  $Q(x)$ 'in en çok  $n - 1$  çözümlü vardır ve bu  $n - 1$  çözümlü tümü  $a$ 'dan farklı bile olsa  $P$  sayısının asallığı nedeniyle  $P(x)$ 'in en fazla  $n$  çözümlü vardır. Bu da teoremin kanıtını tamamlar.

**Euler Ölçütü:**  $p$ , çift olmayan bir alsalsa  $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$  dir.

**Kanıt:** Yazım kolaylığı sağlamak için  $r = \frac{1}{2}(p - 1)$  diyelim  $a \pmod{n}$  de bir kuadratik rezidüyse  $x^2 \equiv a \pmod{p}$  olacak biçimde bir  $x$  tamsayısı vardır, ve Fermat'ın küçük teoreminden  $a^r \equiv x^{p-1} \equiv 1 \pmod{p}$  iken öte yandan  $a$  bir kuadratik rezidü, tanımdan  $\left(\frac{a}{p}\right) = 1$

\* Bilkent Üniversitesi Matematik Bölümü Öğrencisi

Önsavından  $\left(\frac{p}{q}\right) = (-1)^n$  olduğunu gözlemleriz. Bu eşitsizliklerden  $y < (pxq) + \frac{1}{2} < \frac{1}{2}(p+1)$  elde ederiz. Buradan,  $y$  bir tamsayı olduğu için  $n$ 'nin,  $0 < x < \frac{1}{2}q$  ve  $0 < y < \frac{1}{2}p$  ile tanımlanan  $D$  dikdörtgenin içinde  $\frac{1}{2}q < px - qy < 0$  koşulunu sağlayan tamsayı koordinatlı noktaların sayısına eşit olduğunu gözlemleriz (Şekle bkz.) Benzer biçimde,  $m$   $D$  dikdörtgeni içinde  $-\frac{1}{2}p]qy - px < 0$  koşulunu sağlayan tamsayı koordinatlı noktaların sayısını göstermek üzere,  $\left(\frac{q}{p}\right) = (-1)^m$  dir. Şimdi  $\frac{1}{4}(p-1)(q-1) - (n+m)$  nin çift olduğunu kanıtlamak yeterlidir.  $\frac{1}{4}(p-1)(q-1)$ ,  $D$  dikdörtgeni içindeki tamsayı koordinatlı noktaların sayısına eşittir, ve  $\frac{1}{4}(p-1)(q-1) - (n+m)$ ,  $D$  dikdörtgeni içinde  $px - qy \leq -\frac{1}{2}q$  ya da  $qy - px \leq -\frac{1}{2}p$  koşulunu sağlayan noktaların ayrıştır ve eşit sayıda tamsayı koordinatlı nokta içerirler, çünkü  $x = \frac{1}{2}(q+1) - x'$  ve  $y = \frac{1}{2}(p+1) - y'$  biçiminde bir değişken değiştirme, iki ayrık alan arasında bir, bire-bir eşleme kurar. Buradan da bu iki ayrık alanda bulunan tamsayı koordinatlı nokta sayısının çift olduğunu elde ederiz ve kanıt tamamlanır.

**Gauss Önsavı:**  $p$  çift olmayan bir asal ve  $(a, p) = 1$  olsun.  $\frac{p-1}{2} = r$  diyelim ve  $j = 1, 2, \dots, r$  için  $a_j \equiv a \cdot j \pmod{p}$  ve  $-r < a_j \leq r$  olsun.  $n$  sayısı  $a_j < 0$  koşulunu sağlayan  $j$ 'lerin sayısını gösteriyorsa  $\left(\frac{a}{p}\right)^n = (-1)^n$  dir.

**Kanıt:**  $|a_j|$  sayıları birbirinden farklıdır. Eğer öyle olmasalardı,  $a_j = -a_k$  olacak biçimde  $j$  ve  $k$  olurdu. Buradan  $a(j+k) \equiv 0 \pmod{p}$  ve  $(a, p) = 1$  olduğundan  $p|(j+k)$  elde ederiz. Ama  $0 < j+k < p-1$  olduğundan bu olanaksızdır. Ayrıca  $1 \leq |a_j| \leq r$  olduğundan  $|a_j|$  sayılarıyla,  $1, 2, \dots, r$  sayıları arasında bire-bir bir eşleme vardır. Buradan  $a_1, a_2, \dots, a_r = (-1)^n r!$  olduğunu ve  $a_j \equiv a, j \pmod{p}$  olduğundan  $a^r r! \equiv (-1)^n r! \pmod{p}$  denkleğini elde ederiz.  $(p, r!) = 1$  olduğu için  $a^r \equiv (-1)^n \pmod{p}$  dir. Euler ölçütünden  $\left(\frac{a}{p}\right) \equiv a^r \pmod{p}$  dir ve buradan da  $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$  ve  $\left(\frac{a}{p}\right) = (-1)^n$  elde edilir. Böylece kanıt tanımlanır.

Artık başlangıçta sözünü ettiğimiz ünlü teoremi kanıtlayabiliriz.

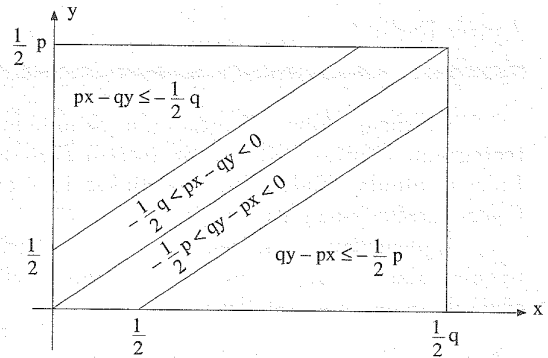
**Karesel Karşıklık Kuralı:** (Law of Quadratic Reciprocity)

$p$  ve  $q$  çift olmayan ve birbirinden farklı asallarsa

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)} \text{ dir.}$$

**Kanıt:** İlk önce,  $n, 0 < x < \frac{1}{2}q < px - qy < 0$  koşullarını sağlayan  $(x, y)$  tamsayı ikililerinin sayısını göstermek üzere, Gauss'un

önsavından  $\left(\frac{p}{q}\right) = (-1)^n$  olduğunu gözlemleriz. Bu eşitsizliklerden  $y < (pxq) + \frac{1}{2} < \frac{1}{2}(p+1)$  elde ederiz. Buradan,  $y$  bir tamsayı olduğu için  $n$ 'nin,  $0 < x < \frac{1}{2}q$  ve  $0 < y < \frac{1}{2}p$  ile tanımlanan  $D$  dikdörtgenin içinde  $\frac{1}{2}q < px - qy < 0$  koşulunu sağlayan tamsayı koordinatlı noktaların sayısına eşit olduğunu gözlemleriz (Şekle bkz.) Benzer biçimde,  $m$   $D$  dikdörtgeni içinde  $-\frac{1}{2}p]qy - px < 0$  koşulunu sağlayan tamsayı koordinatlı noktaların sayısını göstermek üzere,  $\left(\frac{q}{p}\right) = (-1)^m$  dir. Şimdi  $\frac{1}{4}(p-1)(q-1) - (n+m)$  nin çift olduğunu kanıtlamak yeterlidir.  $\frac{1}{4}(p-1)(q-1)$ ,  $D$  dikdörtgeni içindeki tamsayı koordinatlı noktaların sayısına eşittir, ve  $\frac{1}{4}(p-1)(q-1) - (n+m)$ ,  $D$  dikdörtgeni içinde  $px - qy \leq -\frac{1}{2}q$  ya da  $qy - px \leq -\frac{1}{2}p$  koşulunu sağlayan noktaların ayrıştır ve eşit sayıda tamsayı koordinatlı nokta içerirler, çünkü  $x = \frac{1}{2}(q+1) - x'$  ve  $y = \frac{1}{2}(p+1) - y'$  biçiminde bir değişken değiştirme, iki ayrık alan arasında bir, bire-bir eşleme kurar. Buradan da bu iki ayrık alanda bulunan tamsayı koordinatlı nokta sayısının çift olduğunu elde ederiz ve kanıt tamamlanır.



#### KAYNAKÇA

1. Baker, Alan. A concise intuduction to the theory of numbers, Birinci Baskı, Combredge University Press, New York, 1984.
2. Chandrasekharan, K. Introduction to analytic number thery, Sprigner-Verlag, Almanya, 1968.