

# WILSON TEOREMİ

SAFAK ALPAY †

$p$  verilen bir tamsayı olsun.  $p|(x-y)$  ise  $x$  ve  $y$  tamsayıları  $\text{mod } p$  de denktir denir ve  $x \equiv y \pmod{p}$  yazılır. Bu şekilde tam sayılar kümesi  $\mathbb{Z}$  de daha öncede çalışılan bir bağıntı elde edilir [1]. Sıfır her sayıyı böldüğünden her  $x \in \mathbb{Z}$  için  $x \equiv x \pmod{p}$  vardır (yansıma özelliği).  $p|(x-y)$  ise  $p|(y-x)$  olacağından  $x \equiv y \pmod{p} \Rightarrow y \equiv x \pmod{p}$  (simetri özelliği).  $x \equiv y \pmod{p}$  ve  $y \equiv z \pmod{p}$ ,  $x \equiv z \pmod{p}$  gerektirir (geçişme özelliği). Yansıma, simetri ve geçişme özelliklerini taşıyan bağıntılara kısaca denklik bağıntısı dendiğinden,  $x \equiv y \pmod{p}$  bağıntısı denklik bağıntısıdır.  $p = 2$  alırsa,  $x \in \mathbb{Z}$  çift veya tek oluşuna göre ya  $x = 0 \pmod{2}$  veya  $x = 1 \pmod{2}$  olacaktır.  $n$  ögeli bir küme üzerinde tanımlı birebir ve örten fonksiyonlar kümesinde tanımlı bir denklik bağıntısı önümüzdeki sayıda ele alınacaktır [2].  $[x]$  ile  $x$ 'e denk olan tamsayıları gösterirsek, yansıma özelliğinden  $[x] \neq \emptyset$  ve  $[0] \cup [1] = \mathbb{Z}$  ve  $[0] \cap [1] = \emptyset$ . [3]'te verilen bölme algoritmasını kullanarak,  $p = 3$  için herhangi bir  $x$  tam sayısının 0, 1 veya 2 ye denk olduğunu görürüz.  $p = 3$  için,

$$\begin{aligned} [0] &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}, \\ [1] &= \{\dots, -4, -1, 1, 4, 7, 10, \dots\} \text{ ve} \\ [2] &= \{\dots, -5, -2, 2, 5, 8, 11, \dots\} \end{aligned}$$

bölme algoritması ile kolayca görülür. Yani  $[0] \cup [1] \cup [2] = \mathbb{Z}$  ve bu kümelerin ortak elemanları yoktur.

$[x]$ 'e  $x$  elemanın denklik sınıfı denir. Bölme algoritması verilen  $p$  sayısı için  $\mathbb{Z}$  nin  $p$  tane denklik sınıftan oluştuğunu söyler.  $\mathbb{Z}$  nin  $p = 2$  ve 3 için denklik sınıflarına ayrışması her denklik bağıntısı için doğrudur. Yani bir denklik bağıntısı tanımlandığı kümeyi bileşimleri tüm küme olan ve kesişmeyen parçalara böler.

$R$  bağıntısı  $A$  kümesi üzerinde tanımlı bir denklik bağıntısı olsun.  $[x]$  ile  $x$ 'in denklik sınıfını, yani,  $\{y \in A : yRx\}$  gösterelim.  $xRy$  için gerekli ve yeterli koşul  $[x] = [y]$  dir.  $xRy$  ise  $[x] = [y]$  önermesini ele alalım.  $[x], [y]$   $A$ 'nın

alt kümeleri olduğundan  $[x] \subseteq [y]$  ve  $[y] \subseteq [x]$  gösterilmelidir.  $z \in [x]$  olsun. Kabul gereği  $xRy$  ve  $zRx$  bize,  $R$ 'nin geçişme ve simetri özelliğinden,  $zRy$  veya  $z \in [y]$  verir.  $z$  keyfi alındığından  $[x] \subseteq [y]$  elde edilir.  $[y] \subseteq [x]$  benzer şekilde gösterilir. Öte yandan  $[x] = [y]$  ise  $xRy$  olduğu aşikardır. Şimdide denklik sınıflarının ya aynı ya da ortak öğeleri olmayacağını görelim.  $z \in [x] \cap [y]$  ise  $zRx, zRy$  bağıntıları vardır.  $R$ 'nin simetri ve geçişme özelliği  $xRy$  verir. Önceki gözlemden  $[x] = [y]$  elde edilir.  $p$  için,  $x = y \pmod{p}$  bağıntısına göre elde edilen denklik sınıflarının kümesini  $\mathbb{Z}_p$  ile göstereceğiz. Bölme algoritması ile  $\mathbb{Z}$  nin aritmetik yapısı kullanılarak  $\mathbb{Z}_p$  içinde de aritmetik yapabiliriz.  $\mathbb{Z}_p$  de aritmetik  $[x] + [y] = [x + y]$  ve  $[x][y] = [xy]$  ile tanımlanır.  $\mathbb{Z}_4$  için toplama tablosu şöyledir:

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Tablodan görüleceği gibi  $\mathbb{Z}_4$  Abelian bir gruptur. Genelde her  $n \geq 2$  için  $\mathbb{Z}_n$  Abelian bir gruptur [4].

$\mathbb{Z}_4$  çarpma tablosu aşağıdadır.  $\mathbb{Z}_4$ 'ün çarpma altında grup olmadığı tablodan kolayca görülebilir! Genelde her  $n$  asal sayısı için  $\mathbb{Z}_n \setminus \{0\}$  çarpma altında gruptur [4].

•	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Şimdi bölme algoritması ve yukarıdaki önbilgiler ve cebimizdeki 5100 TL ile çarşıya çıkalım. Bu para ile 200 ve 500 liralık sakızlardan kaçar tane alabiliriz?  $x$  ile 200 liralıkların sayısını,  $y$  ile 500 liralıkların sayısını gösterirsek, sorunun yanıtı  $200x + 500y = 5100$  denkleminin çözümleri kadar olacaktır.

†ODTÜ, Matematik Bölümü öğretim üyesi

$a, b$  ve  $c$  pozitif tamsayılar olmak üzere  $ax + by = c$  şeklindeki denklemlere iki değişkenli (doğrusal) diofantin denklem denir [5].

Kanıtında sadece bölme algoritmasının kullanıldığı ilk teorem böyle denklemlerin çözülebilirliği hakkında.

**Teorem 1.**  $a, b \in \mathbb{Z}, d = (a, b)$  olsun.  $d \nmid c$  ise  $ax + by = c$  denkleminin tam sayılar kümesinde çözümü yoktur.  $d|c$  ise sonsuz tane çözüm vardır.  $(x_0, y_0)$  bir çözüm ise, tüm çözümler  $x = x_0 + (b/d)n$ ,  $y = y_0 - (a/d)n$  ( $n \in \mathbb{Z}$ ) şeklindedir.

**Kanıt.**  $x, y \in \mathbb{Z}$  olmak üzere  $ax + by = c$  olsun.  $d|a$  ve  $d|b \Rightarrow d|c$ . Bu nedenle  $d \nmid c$  ise denklemin çözümü yoktur.  $d|c$  ise bir  $e \in \mathbb{Z}$  için  $de = c$  ve  $d = (a, b)$  olduğundan  $s, t \in \mathbb{Z}$  için

$$d = as + bt \quad (5)$$

yazılabilir.

(1)'in her iki tarafını  $e$  ile çarparak  $c = de = (as + bt)e = a(se) + b(te)$  elde edilir ki bu  $x_0 = se$ ,  $y_0 = te$  çiftinin çözüm olduğunu gösterir:  $n \in \mathbb{Z}$  için

$$x = x_0 + (b/d)n, \quad y = y_0 - (a/d)n \quad (6)$$

çiftlerinin çözüm olduğu kolayca görülür.

Şimdi her çözümün bir  $n \in \mathbb{Z}$  için (2)'deki gibi olduğunu görelim.  $(x, y)$  bir çözüm olsun.  $ax + by = c$  ve  $ax_0 + by_0 = c$  olduğundan  $(ax + by) - (ax_0 + by_0) = 0$  veya  $a(x - x_0) + b(y - y_0) = 0$  veya

$$a(x - x_0) = b(y_0 - y) \quad (7)$$

vardır. Her iki taraf  $d$  ile bölünerek

$$(a/d)(x - x_0) = (b/d)(y_0 - y)$$

elde edilir.

$$(a/d, b/d) = 1 \quad \text{ve} \quad (a/d)|(b/d)(y_0 - y)$$

olduğundan  $(a/d)|(y_0 - y)$ . Yani, bir  $n \in \mathbb{Z}$  için  $(a/d)n = y_0 - y$  veya  $y = y_0 - (a/d)n$  elde edilir. Bu (3)'de yerine konarak  $x = x_0 + (b/d)n$  bulunur.

**Örnek:**  $(15, 6) = 3, 3 \nmid 7$  den ötürü  $15x + 6y = 7$  denkleminin tamsayı çözümü yoktur.  $(21, 14) = 7, 7|70$  den ötürü  $21x + 14y = 70$  denkleminin sonsuz çözümü vardır. Bölme algoritması ile  $x_0 = 10, y_0 = -10$  çözüm olduğu kolayca görülür. Diğer çözümler  $x = 10 + 2n, y = -10 - 3n$  şeklindedir.

$x$  bilinmeyen tam sayıları göstermek üzere  $ax = b(\text{mod } p)$   $a, b, p \in \mathbb{Z}$  denklemine tek

değişkenli doğrusal kongürans denklemi denir.  $x_0$  bir çözüm ise,  $x = x_0(\text{mod } p)$  bağıntısını sağlayan her  $x$  de çözümdür. Amacımız denklik sınıflarından çözüm bulmak olacaktır.

**Teorem 2.**  $0 < p$  olmak üzere  $a, b, p \in \mathbb{Z}$  ve  $(a, p) = d$  olsun.  $d \nmid b$  için  $ax = b(\text{mod } p)$  denkleminin çözümü yoktur.  $d|b$  için bu denklemin  $\mathbb{Z}_p$  de  $d$  tane çözümü vardır.

**Kanıt:**  $x$  tamsayısının  $ax = b(\text{mod } p)$  denkleminin çözümü olması için gerekli ve yeterli koşul bir  $y \in \mathbb{Z}$  için  $ax - py = b$  diophantin denkleminin sağlanmasıdır. (Niye?)  $d \nmid b$  iken çözüm olmadığını,  $d|b$  ise bu denklemin  $(x_0, y_0)$  herhangi bir çözüm olmak üzere her  $t \in \mathbb{Z}$  için

$$x = x_0 + (p/d)t, \quad y = y_0 + (a/d)t$$

şeklinde sonsuz tane çözüm olduğunu Teorem 1'den biliyoruz.

Şimdi  $(\text{mod } p)$  ye göre kaç tane denklik sınıfının çözüm olabileceğini arayalım.

$$x_1 = x_0 + (p/d)t_1, \quad \text{ve} \quad x_2 = x_0 + (p/d)t_2$$

şeklindeki iki çözümün  $(\text{mod } p)$  bağıntısında denk olması için  $(p/d)t_1 \equiv (p/d)t_2 (\text{mod } p)$  olması gerekir.  $m/d \mid m$  den  $(m, m/d) = m/d$  elde edilir ki, bu yukarıdaki eşitliğinin sağlanması için  $t_1 = t_2(\text{mod } d)$  verir. Dolayısı ile  $(\text{mod } p)$  bağıntısına göre farklı çözümler  $x = x_0 + (p/d)t$  de  $t$  yi  $(\text{mod } d)$  bağıntısında farklı denklik sınıflarından alınarak elde edilir. Yani,  $x = x_0 + (p/d)t$ ,  $t = 0, 1, \dots, d - 1$  tüm çözümleri betimler.

**Örnek:**  $(9, 15) = 3$  ve  $3|12$  olduğundan  $9x = 12(\text{mod } 15)$  denkleminin çözümü vardır. Bir çözümü  $9x - 15y = 12$  diophantin denklemini çözümler bulabiliriz. Bölme algoritmasından  $15 = 9 \cdot 1 + 6, 9 = 6 \cdot 1 + 3, 6 = 3 \cdot 2$  buradan da  $3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15$  elde ederiz. Dolayısı ile  $x_0 = 8, y_0 = 4$  çifti  $9x - 15y = 12$  denkleminin çözümüdür. Buradan da  $9x = 12(\text{mod } 15)$  denkleminin tüm çözümlerini  $x_1 = 8(\text{mod } 15), x_2 = x_1 + 5 = 13(\text{mod } 15)$  ve  $x_3 = x_0 + 2 \cdot 5 = 18(\text{mod } 15)$  olarak elde ederiz.

$(a, p) = 1$  ise  $ax = 1(\text{mod } p)$  denkleminin çözümüne  $a$  nın  $(\text{mod } p)$  bağıntısına göre tersi denir. Örneğin  $7x = 1(\text{mod } 31)$  denkleminde 9 ve mod 31 bağıntısında 9'un denklik sınıfındaki tüm sayılar 7'nin tersidir. mod  $p$  bağıntısında  $a$  nın tersi varsa  $ax = b(\text{mod } p)$  denklemini kolayca çözülür.  $ax = b(\text{mod } p)$  de her iki tarafı  $a$  nın tersi  $\bar{a}$  ile çarparak,

$\bar{a}(ax) = \bar{a}b(\text{mod } p)$  veya  $x = \bar{a}b(\text{mod } p)$  elde edilir. Örneğin,  $7x = 22(\text{mod } 31)$  denkleminde her iki tarafı 9 ile çarparak

$$\begin{aligned} 9.(7x) &= (9.7).x = x = 9.22(\text{mod } 31) \\ &= 198 = 12(\text{mod } 31) \end{aligned}$$

elde ederiz.

$(a, p) = 1$  ise  $ax = b(\text{mod } p)$  denkleminin  $\text{mod } p$  de tek çözümü vardır.  $7x = 4(\text{mod } 12)$  de tek çözüm vardır. Bunu  $7x - 12y = 4$  diophantın denklemini çözerek  $x_0 = -20, y_0 = 12$  buluruz. Öyle ise  $7x = 4(\text{mod } 12)$  denkleminin tek çözümü  $x = -20 = 4(\text{mod } 12)$  dir.

Daha sonra kullanacağımız aşağıdaki teorem  $p$  asal iken hangi sayıların  $(\text{mod } p)$  bağıntısında terslerinin kendileri olduğunu söyler.

**Teorem 3.**  $p$  asal olsun.  $a$  pozitif tam sayısının  $(\text{mod } p)$  bağıntısında tersinin kendisi olması için gerekli ve yeterli koşul  $a \equiv 1(\text{mod } p)$  veya  $a \equiv -1(\text{mod } p)$  olmasıdır.

**Kanıt:**  $a \equiv \mp 1(\text{mod } p)$  ise  $a^2 = 1(\text{mod } p)$  olacağından  $a$  nın  $(\text{mod } p)$  de tersi kendisidir.

$a$  nın tersi kendisi ise  $a^2 = a.a = 1(\text{mod } p)$  olur. Dolayısı ile  $p|a^2 - 1 = (a + 1)(a - 1)$  den  $p|a - 1$  veya  $p|a + 1$  elde edilir. Bu ise  $a \equiv 1(\text{mod } p)$  veya  $a \equiv -1(\text{mod } p)$  demektir.

Aşağıdaki teoremin kanıt yöntemini daha iyi anlamak için  $p = 7$  alalım ve  $(p - 1)!$  hesaplayalım.  $2.4 \equiv 1(\text{mod } 7), 3.5 \equiv 1(\text{mod } 7)$  olduğunu göz önüne alalım.  $(p - 1)! = 6! = 1.2.3.4.5.6$  uygun şekilde parantezlere alınarak  $(p - 1)! = 1.(2.4).(3.5).6 = 1.6 \equiv -1(\text{mod } 7)$  bulunabilir.

**Wilson Teoremi.** Asal  $p$  sayısı için  $(p - 1)! \equiv -1(\text{mod } p)$ .

**Kanıt:**  $p = 2$  için  $(p - 1)! \equiv 1 \equiv -1(\text{mod } 2)$  olduğundan teorem  $p = 2$  için doğrudur.  $2 < p$  alalım. Teorem 2'den  $1 \leq a \leq p - 1$  koşulunu sağlayan her  $a$  tamsayısı için  $a.\bar{a} \equiv 1(\text{mod } p), 1 \leq \bar{a} \leq p - 1$  olan  $\bar{a}$  sayısı vardır.

Teorem 3'e göre  $p$  den küçük sayılar içinde tersi kendisine eşit olan sayılar  $1$  ve  $p - 1$  dir. Örnekteki yöntemi izleyerek  $2$  ile  $p - 2$  arasındaki sayıları tersleri ile eşleyerek  $(p - 3)/2$  tane çift oluşturalım. Böylelikle elde edeceğimiz

$$2.3 \cdots (p - 4)(p - 3)(p - 2) \equiv 1(\text{mod } p)$$

eşitliğinde her iki tarafı  $(p - 1)$  ile çarparak

$$\begin{aligned} (p - 1)! &= 1.2 \cdots (p - 3)(p - 2)(p - 1) \\ &= 1.(p - 1) \equiv -1(\text{mod } p) \end{aligned}$$

elde edilir.

Wilson Teoremi'nin terside doğrudur.

**Teorem 4.**  $(n - 1)! \equiv -1(\text{mod } n)$  ise  $n$  asal bir sayıdır.

**Kanıt:**  $n$  asal değilse,  $1 < a < n, 1 < b < n$  olmak üzere  $n = ab$  yazılabilir.  $a < n$  olduğundan  $a|(n - 1)!$  Varsayım gereği  $(n - 1)! \equiv -1(\text{mod } n)$  olduğundan  $n|((n - 1)! + 1)$  vardır.  $a|((n - 1)! + 1)$  ve  $a|((n - 1)! + 1) - (n - 1)! = 1$  elde edilir.  $1 < a$  olduğundan bu bir çelişkidir.

#### KAYNAKÇA

- [1] İsmail Güloğlu: Çinlilerin Kalan Teoremi, Matematik Dünyası, Cilt 3, Sayı 1.
- [2] Mahmut Kuzucuoğlu, Şule Durdaş: Simetrik Grup  $S_4$  ve Bazı Grup Özellikleri, Matematik Dünyası, Cilt 3, Sayı 5.
- [3] Cemal Koç: Tam Sayılar ve Polinomlar: Matematik Dünyası, Cilt 3, Sayı 3.
- [4] Kenneth H. Rosen: Elementary Number Theory and its Applications, Addison-Wesley, 1993.
- [5] Şafak Alpay, Halil İ. Karakaş: An Introduction to Modern Mathematics, ODTÜ Yayını, 1979 Ankara.