Sayılar Kuramına Giriş

Özet

David Pierce

26 Aralık 2017
Matematik Bölümü, MSGSÜ
dpierce@msgsu.edu.tr
http://mat.msgsu.edu.tr/~dpierce/

1 Toplama ve sıralama

Sınırsız bir doğruda, bir nokta 0 olarak seçilirse, o zaman Öklid'in 3. önermesi ile iki noktanın **toplamı** ve bir noktanın **negatifi** tanımlanabilir. Sonuç olarak doğrunun herhangi a, b, ve c noktaları için

$$\begin{aligned} a+(b+c)&=(a+b)+c,\\ a+b&=b+a,\\ a+0&=a,\\ a+(-a)&=0. \end{aligned}$$

Tanıma göre

$$a-b=a+(-b).$$

Eğer bir b noktası bir a noktasının sağındaysa, o zaman a, b'den **küçük** ve b, a'dan **büyük** olarak sayılır, ve

$$a<b, \qquad\qquad b>a$$

yazılır. Tanıma göre

$$\begin{gathered} a\leqslant a,\\ a<b \implies a\leqslant b,\\ a\leqslant b \iff b\geqslant a. \end{gathered}$$

O halde

$$\left.\begin{gathered} a<b \implies a\neq b,\\ a\leqslant b\ \&\ b\leqslant a \implies a=b,\\ a\leqslant b\ \&\ b\leqslant c \implies a\leqslant c. \end{gathered}\right\} \tag{$*$}$$

Ayrıca

$$a<b \implies a+c<b+c,$$

dolayısıyla

$$a<b \iff b-a>0.$$

2 Sayma sayıları

0'ın sağında olan bir nokta 1 olarak seçilsin. **Sayma sayılarının** özyineli tanımına göre

(i) 1 bir sayma sayısıdır, ve
(ii) eğer n bir sayma sayısı ise, o zaman $n+1$ de bir sayma sayısıdır.

Burada $n+1$, n'nin **ardılıdır.** Sayma sayıları kümesi $\mathbb{N}$ olarak yazılır. O halde

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

Tanımdan $\mathbb{N}$'nin herhangi A altkümesi için, eğer

(i) $1 \in A$ ise ve
(ii) A her elemanının ardılını da içerirse,
o zaman $A = \mathbb{N}$. Bu sonuç, **Tümevarım İlkesidir.**

- Tümevarım,
- $\mathbb{N}$'nın sıralanmasının $(*)$ özellikleri ve
- $n < n + 1$ kuralından

$\mathbb{N}$'nin bütün özellikleri elde edilebilir.

Özellikle **Özyineleme Teoremi** kanıtlanabilir (ama kanıtlamadık). Bu teoreme göre, eğer B bir küme ise, $c \in B$ ise, ve f, B'nin tek konumlu bir işlemi (yani $f\colon B \to B$) ise, o zaman $\mathbb{N}$'den B'ye giden bir ve tek bir h göndermesi için

(i) $h(1) = c$,
(ii) her n sayma sayısı için $h(n+1) = f(h(n))$.

Örneğin $\mathbb{N}$'de toplama

$$m + 1 = (m\text{'nin ardılı}), \quad m + (n+1) = (m+n) + 1$$

kuralları ile tanımlanabilir. Tümevarım ile, toplamanın gördüğümüz özellikleri kanıtlanabilir.

Alıştırmalar I'deki gibi doğrumuzun noktalarının, sayma sayıları ile **katları** (yani çoğaltılmaları) ve **kuvvetleri** tanımlanır, ve bunların özellikleri tümevarım ile kanıtlanır.

Eğer doğrunun $0 < a < b$ eşitsizliğini sağlayan herhangi a ve b noktaları için, bir n sayma sayısı için, $b < a \cdot n$ ise, o zaman doğrunun **Arşimet Özelliği** vardır, ve bu durumda doğrunun noktaları **gerçel sayılar** olarak sayılabilir. Aslında Arşimet Özelliği'ni kullanmayacağız.

Çoğaltma ile $\mathbb{N}$'de iki konumlu **çarpma** işlemini elde ederiz, ve $\mathbb{N}$'de

$$k \cdot m = m \cdot k$$

özelliği, tümevarım ile kanıtlanır.

Özyineli tanıma göre

$$\sum_{k=1}^{1} a_k = a_1, \qquad \sum_{k=1}^{n+1} = \sum_{k=1}^{n} a_k + a_{n+1}.$$

Benzer şekilde

$$\prod_{k=1}^{1} a_k = a_1, \qquad \prod_{k=1}^{n+1} = \prod_{k=1}^{n} a_k \cdot a_{n+1}.$$

Sayma sayıları ve 0, **doğal sayılardır.** Tanıma göre ω (omega), doğal sayıların kümesidir:

$$\omega = \{0\} \cup \mathbb{N} = \{0, 1, 2, \dots\}.$$

Bazen

$$\sum_{k=1}^{0} a_k = 0, \qquad \prod_{k=1}^{0} a_k = 1$$

kurallarına ihtiyacımız vardır. Örneğin tanıma göre $n \in \omega$ ise

$$n! = \prod_{k=1}^{n} k.$$

Daha fazla örnekler için, Alıştırmalar I ve V'e bakın.

3 Bölme

$\mathbb{N}$'de $a \cdot b = c$ ise a ve b, c'nin **çarpanı** veya **bölenidir,** ve her biri c'yi **böler.** $\mathbb{N}$'de $p > 1$ ise ve p'nin 1'den ve kendisinden farklı olan hiç çarpanı yoksa, p **asaldır.**

İyisıralama Teoremine göre, herhangi verilen sayma sayılarından biri, onların en küçüğüdür. Sonuç olarak 1'den büyük olan her sayma sayısının asal bir çarpanı vardır. Aslında verilen sayının 1'den büyük olan çarpanlarının en küçüğü asaldır. Alıştırma I'e bakın.

Güçlü Tümevarım Teoremine göre, $\mathbb{N}$'nin herhangi A altkümesi için, eğer her n sayma sayısı için

$$\{x \in \mathbb{N} \colon x < n\} \subseteq A \implies n \in A$$

ise, o zaman $A = \mathbb{N}$. Örneğin her sayma sayısının **asal çarpanlara ayrılışı** vardır. Bu ayrılış, $p_1 \leqslant \cdots \leqslant p_m$ ve her biri asal olmak üzere

$$\prod_{k=1}^{m} p_k$$

şeklinde yazılabilir. Zira bir n için n'den küçük olan her sayma sayısı için iddia doğru olsun. Eğer n asal veya 1'e eşit ise, o zaman aşikâr bir şekilde n'nin asal çarpanlara ayrılışı vardır. Eğer $n > 1$ ise ama n asal değilse, 1'e eşit olmayan bazı a ve b için

$$n = a \cdot b.$$

Varsayıma göre a ve b'den her birinin asal çarpanlara ayrılışı vardır, ve bunlardan n'nin asal çarpanlara ayrılışı elde edilir. (Aynı sonuç, Alıştırma I'deki gibi iyisıralama ile kanıtlanabilir.)

Bölme Teoremine göre $\mathbb{N}$'de herhangi a ve b için ya

$$a = bx$$

denklemi ya da

$$a = bx + y \ \ \& \ \ y < b$$

sistemi çözülebilir. Bu teoremden (ve $\mathbb{N}$'nin iyisıralı olduğundan) **Öklid Algoritması** ile iki sayının **en büyük ortak böleni** bulunur. Alıştırma II'ye bakın. Başka bir teoreme göre a ve b'nin **en küçük ortak katı** vardır ve

$$a \cdot b = \operatorname{ebob}(a, b) \cdot \operatorname{ekok}(a, b).$$

4 Tamsayılar

Sayma sayıları, negatifleri ve 0, **tamsayılardır.** Bunların kümesi $\mathbb{Z}$ olarak yazılır. Buradaki toplama ve çarpmanın temel kuralları, Alıştırma II'nin Alıştırma 1'indedir. **Bézout Lemması'na** göre

$$ax + by = \operatorname{ebob}(a, b)$$

denklemi $\mathbb{Z}$'de çözülebilir. Bir çözüm, Öklid Algoritması'nın adımlarından elde edilebilir.

Bézout Lemması'ndan **Öklid Lemması** ve Alıştırmalar III'teki genelleştirilmesi elde edilir. Öklid Lemması sayesinde her sayma sayısının asal çarpanlara ayrılışı tektir; bu sonuç, **Temel Aritmetik Teoremidir.**

$\mathbb{Z}$'de tanıma göre

$$a \mid b \iff \text{bir } x \text{ için } ax = b.$$

O zaman **Fermat Teoremine** göre her p asalı için

$$p \mid a^p - a, \tag{$\dagger$}$$

ve ayrıca

$$p \nmid a \implies p \mid a^{p-1} - 1. \tag{$\ddagger$}$$

Aynı teorem, **kalandaşlıklar** ile ifade edilebilir:

$$a^p \equiv a \pmod p,$$
$$p \nmid a \implies a^{p-1} \equiv 1 \pmod p.$$

Şimdi $p \nmid a$ olsun. O zaman $\mathbb{N}$'de

$$a^x \equiv 1 \pmod p$$

kalandaşlığının çözümü vardır. En küçük çözüm, a'nın p'ye göre **mertebesidir** (İngilizce *order*). Bu mertebe m ise, o zaman $m \mid p-1$, ve ayrıca, $p-1 = mn$ olmak üzere bazı b_1, $\dots$, b_{n-1} sayıları için her tamsayı, aşağıdaki matrisin bir ve tek bir girdisine p'ye göre denktir:

$$\begin{bmatrix} 1 & a & a^2 & \cdots & a^{m-1} \\ b_1 & b_1a & b_1a^2 & \cdots & b_1a^{m-1} \\ \hdotsfor{5} \\ b_{n-1} & b_{n-1}a & b_{n-1}a^2 & \cdots & b_{n-1}a^{m-1} \end{bmatrix}$$

(Bu sonuca **Lagrange Teoremi** diyebiliriz ama derste demedik.) Örneğin $p = 13$ durumunda

$$\begin{bmatrix} 1 & 3 & 9 \\ 2 & 6 & 18 \\ 4 & 12 & 36 \\ 7 & 21 & 63 \end{bmatrix}$$

matrisi çıkar. Bunu daha iyi anlamak için, girdilerin yerine ya $\{1, \dots, 12\}$ ya da $\{-6, \dots, -1\} \cup \{1, \dots, 6\}$ kümesinde olan, 13'e göre denk olan sayıları koyabiliriz:

$$\begin{bmatrix} 1 & 3 & 9 \\ 2 & 6 & 5 \\ 4 & 12 & 10 \\ 7 & 8 & 11 \end{bmatrix} \qquad \begin{bmatrix} 1 & 3 & -4 \\ 2 & 6 & 5 \\ 4 & -1 & -3 \\ -6 & -5 & -2 \end{bmatrix}$$

Verilen bir modüle göre denklik, bir **denklik bağıntısıdır,** çünkü yansımalı, simetrik, ve geçişlidir. Öklid için sınırlı doğruların eşitliği bir denklik bağıntısıdır. Bizim için tanıma göre

$$(a, b) \sim (c, d) \iff ad = bc$$

ise, o zaman $\mathbb{N} \times \mathbb{N}$'de $\sim$ bağıntısı bir denklik bağıntısıdır.

Bir A kümesinde E bir denklik bağıntısı ise, o zaman A'nın her b elemanının (E'ye göre) **denklik sınıfı**

$$\{x \in A \colon b \mathrel{E} x\}$$

kümesidir. Bu küme için $[b]$ yazılsın. O zaman

$$[b] = [c] \iff b \mathrel{E} c.$$

Örneğin $\sim$ bağıntısı yukarıdaki gibi ise, $[(a, b)]$ sınıfı a/b kesirli sayısı olarak anlaşılabilir.

Genelde A'nın elemanlarının denklik sınıfları bir A/E kümesini oluşturur. Eğer $A = \mathbb{Z}$ ise ve E, bir n modülüne göre denklik ise, o zaman A/E,

$$\mathbb{Z}_n$$

olarak yazılabilir. Bu küme $\{1, \dots, n\}$, $\{0, \dots, n-1\}$ veya ($n = 2m+1$ durumunda) $\{-m, \dots, m\}$ olarak anlaşılabilir. O zaman tanıma göre

$${\mathbb{Z}_n}^{\times} = \{x \in \mathbb{Z}_n \colon \operatorname{ebob}(n, x) = 1\}.$$

Bézout Lemması ile bu kümenin her elemanının tersi bulunabilir. Bu nedenle Fermat Teoreminin (‡) parçası, (†) parçasından çıkar.

Tanıma göre $\phi(n)$, $\mathbb{Z}_n^{\times}$ kümesinin elemanlarının sayısıdır. O zaman **Gauss Teoremine** göre

$$\sum_{d\mid n} \phi(d) = n.$$

Euler Teoremine göre $\operatorname{ebob}(n,a) = 1$ ise $a^{\phi(n)} \equiv 1 \pmod{n}$, ama bunu göstermedik; çoğunlukla asal modüller ile çalışmayı tercih ederiz.

Eğer tekrar p asal ise, o zaman $\mathbb{Z}_p^{\times}$ kümesinde a^n kuvvetlerini hesaplamak için bir yöntem vardır:

(a) Öyle m'yi bulun ki $m \equiv n \pmod{p-1}$ ve $\frac{1}{2}(p-1) < m \leqslant \frac{1}{2}(p-1)$ olsun. O zaman $a^n \equiv a^m \pmod{p}$.

(b) Eğer $m < 0$ ise m'nin yerine $-m$'yi, a'nin yerine a^{-1}'i kullanın.

(c) 2'nin farklı kuvvetlerinin bir toplamı olarak m'yi yazın.

(d) Buradaki 2'nin en yüksek kuvveti 2^{ℓ} ise adım adım a^2, a^{2^2}, …, $a^{2^{\ell}}$ kuvvetlerini p'ye göre hesaplayın.

(e) Gereken çarpımları çarparak a^m'yi elde edin.

Şimdi p'ye göre bir a'nın mertebesi

$$\operatorname{mer}_p(a)$$

olarak yazılsın. Bu mertebe m ise

$$\operatorname{mer}_p(a^k) = \frac{\operatorname{ekok}(m,k)}{k} = \frac{m}{\operatorname{ebob}(m,k)}.$$

Eğer $\operatorname{mer}_p(a) = p-1$ ise, o zaman a'ya p'nin **ilkel bir kökü** denir. Kanıtladığımız bir teoreme göre her asal sayının ilkel bir kökü vardır. Aslında $d \mid p-1$ ise $\phi(d)$, $\mathbb{Z}_p^{\times}$ kümesinin mertebesi n olan elemanlarının sayısıdır.

Eğer a, p'nin ilkel bir kökü ise, o zaman p'ye göre

$$\begin{aligned}(p-1)! \equiv \prod_{k=1}^{p-1} k \equiv \prod_{k\in\mathbb{Z}_p^{\times}} k \equiv \prod_{j\in\mathbb{Z}_{p-1}} a^j \equiv \prod_{j=1}^{p-1} a^j \\ \equiv a^{\sum_{j=1}^{p-1} j} \equiv a^{p\cdot(p-1)/2} \equiv (a^p)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv -1.\end{aligned}$$

Bu sonuç, **Wilson Teoremidir.**

Şimdi $\operatorname{ebob}(k,m) = 1$ olsun. Eğer $mx + ky = 1$ ise, o zaman $amx + bky$,

$$t \equiv a \pmod{k}, \qquad t \equiv b \pmod{m}.$$

sistemini çözer. Eğer tersine d ve e bu sistemi çözerse, o zaman (Alıştırma V'ten) $d \equiv e \pmod{km}$. Bu sonuç, **Çin Kalan Teoremidir.** Eğer ayrıca $\operatorname{ebob}(km,n) = 1$ ve

$$\begin{aligned} mnx &\equiv 1 \pmod{k},\\ kny &\equiv 1 \pmod{m},\\ kmz &\equiv 1 \pmod{n}\end{aligned}$$

ise, o zaman

$$t \equiv a \pmod{k}, \quad t \equiv b \pmod{m}, \quad t \equiv c \pmod{n}$$

sisteminin çözümleri,

$$t \equiv amnx + bkny + ckmz \pmod{kmn}$$

kalandaşlığının çözümleridir.