Yrd.Doç.Dr.Nilüfer YURTAY

BSM

Giriş

4. Hafta

Ayrık İşlemsel Yapılar

İletişim :

nyurtay@sakarya.edu.tr
(264) 295 58 98

Tamsayılar

$N \times N$ kümesinde her $(a, b), (c, d) \in N \times N$ için

$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$

şeklinde tanımlanan ~ bağıntısını ele alalım. Bu bağıntının bir denklik bağıntısı olduğu kolaylıkla gösterilebilir. O halde bu bağıntı $N \times N$ kümesini denklik sınıflarına ayırır. (a, b) elemanının denklik sınıfını

$\overline{(a,b)}$

ile gösterelim. Örneğin;

$\overline{(3,1)} = \{ (x, y) \in N \times N : (x, y) \mid (3, 1) \} = \{ (x, y) \in N \times N : x + 1 = y + 3 \} = \{ (2, 0), (3, 1), (4, 2), \ldots \}$.

$\overline{(0,4)} = \{ (x, y) \in N \times N : (x, y) \mid (0, 4) \} = \{ (x, y) \in N \times N : x + 4 = y \} = \{ (0, 4), (1, 5), (2, 6), \ldots \}$.

$(a, b) \in N \times N$ olmak üzere (a, b)'nin ~ bağıntısına göre olan (a,b) denklik sınıfına tamsayı denir ve Z ile gösterilir.

Tamsayılar

Teorem

(a,b) ve $(c,d) \in N \times N$ olsun. $N \times N$ kümesinde

$(a,b) \sim (c,d) \Leftrightarrow a+d=b+c$ biçimden tanımlanan bağıntı bir denklik bağıntısıdır.

ispat:

$N \times N$ kümesinde tanımlanan $\sim$ bağıntısının yansıyan, simetrik ve geçişli olduğunu göstermemiz yeterlidir.

$\forall (a,b) \in N \times N \quad \Rightarrow a+b=b+a$

$\Rightarrow (a,b) \sim (a,b)$ olduğundan $\sim$ bağıntısı yansıyandır.

$\forall (a,b),(c,d) \in N \times N$ olsun.

$(a,b) \sim (c,d) \quad \Leftrightarrow a+d=b+c$

$\Leftrightarrow b+c=a+d$

$\Leftrightarrow c+b=d+a$

$\Leftrightarrow (c,d) \sim (a,b)$ olduğundan bağıntı simetriktir.

$\forall (a,b),(c,d),(e,f) \in N \times N$ olsun.

$[(a,b) \sim (c,d)$ ve $(c,d) \sim (e,f)] \quad \Leftrightarrow [a+d=b+c$ ve $c+f=d+e]$

$\Leftrightarrow a+d+c+f=b+c+d+e$

$\Leftrightarrow a+f=b+e$

$\Leftrightarrow (a,b) \sim (e,f)$ olduğundan $\sim$ bağıntısı geçişlidir.

BSM

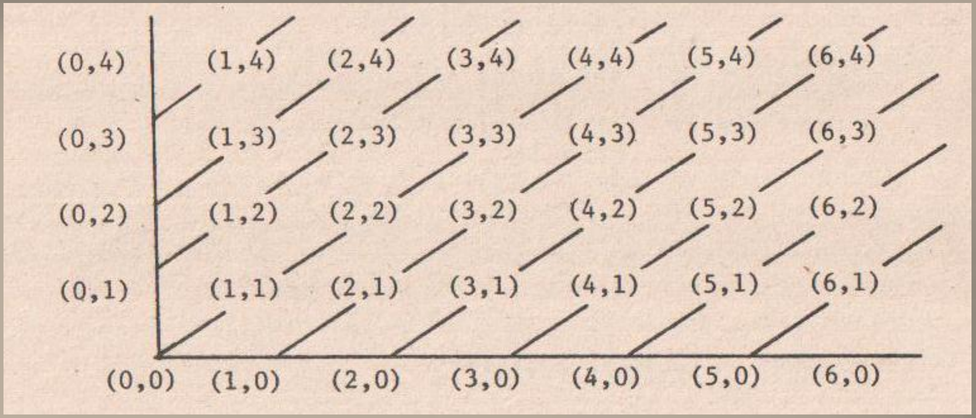
4. Hafta

3. Sayfa

Tamsayılar

(a,b) nin denklik sınıfı

$\overline{(a,b)} = \{(x,y) | (x,y) \in NXN, (x,y) \sim (a,b)]$ olarak tanımlanır.



Tamsayılar

Tamsayılar kümesinde tanımlanan
+: ZXZ→Z

$+:(\overline{(a,b)},\overline{(c,d)}) \to \overline{(a+c,b+d)}$ işlemine $\overline{(a,b)}$ ve $\overline{(c,d)}$

tamsayılarının toplamı denir.

$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}$ olarak gösterilir.

Tamsayılar kümesinde tanımlanan
. : ZXZ→Z
$.:(\overline{(a,b)},\overline{(c,d)}) \to \overline{(ac+bd,ad+bc)}$ işlemine $\overline{(a,b)}$ $\overline{(c,d)}$

tamsayılarının çarpımı denir.

$\overline{(a,b)}.\overline{(c,d)}=\overline{(ac+bd,ad+bc)}$ olarak gösterilir.

Teorem: (Z,+,.) cebirsel yapısı değişmeli ve birikimli bir halkadır. (derste ispatlanacaktır!)

$\overline{(a,b)} \in Z$

olsun.

(a) a > b ise $\overline{(a,b)} = \overline{(a-b,0)} = a-b$

tamsayısına pozitif tamsayı denir.
Pozitif tamsayılar kümesi Z+ ile gösterilir.

(b) a < b ise $\overline{(a,b)} = \overline{(0,b-a)} = -(b-a)$

tamsayısına negatif tamsayı denir.
Negatif tamsayılar kümesi Z- ile gösterilir.

(c) a = b ise

$\overline{(a,b)}$ tamsayısına sıfır denir.

x, y iki tamsayı ise x + (−y) tamsayısına x ile y nin farkı denir ve kısaca x − y ile gösterilir.

Teorem

$x,y,z \in Z$ olsun.
a) $x-y=x+(-1)y$
b) $z(x-y)=(zx)-(zy)$ dir.

Ispat:

$x=\overline{(a,b)}$ ve $y=\overline{(c,d)}$ olsun. $-y=\overline{(d,c)}$ dir.

a) $x-y=x+(-y)=\overline{(a,b)}+\overline{(d,c)}=\overline{(a,b)}+\overline{(0,1)}.\overline{(c,d)}=x+(-1)y$

b) $z(x-y)=z[x+(-y)]=zx+z(-y)=zx+z(-1)y=zx+(-1)zy=zx-zy$

Teorem

$x,y,z,w,t \in Z$ olsun.

(a) $x<y \iff x+z<y+z$

(b) $x<y,\ z<w \Rightarrow x+z<y+w$

(c) $t>0$ ise $xt>yt \iff x>y$

(d) $t<0$ ise $xt>yt \iff x<y$

Tamsayılarda Aritmetik

$a,b \in Z$ için $b=ax$ olacak şekilde bir x tamsayısı varsa, a b yi böler denir ve $a|b$ denir.

Aşağıdaki önermeler doğrudur.

$\forall a \in Z$ için $\pm 1 | a$ ve $\pm a | a$ dır.

$\forall a \in Z$ için $a | \pm 1$ ise $a=\pm 1$ dir.

$\forall a,b \in Z$ için $a|b$ ve $b|a$ ise $a=\pm b$ dir.

$\forall a,b \in Z$ için $a|b$ ise $\pm a | \pm b$ dir.

$\forall a,b,c \in Z$ için $a|b$ ve $b|c$ ise $a|c$

$\forall a,b,c \in Z$ için $a|b$ ve $a|c$ ise $\forall x,y \in Z$ için $a|xb+yc$ dir.

$\forall a,b,c \in Z$ için $a|b$ ise $a|bc$ dir.

$\forall a,b,c \in Z$ için $c \neq 0$ ise $ca|cb \Leftrightarrow a|b$ dir.

$\forall a,b \in Z$ ve $b \neq 0$ için, $a|b$ ise $|a| \leq |b|$ dir. Eğer a has bir bölen ise $1<|a|<|b|$ dir.

BSM

4. Hafta

Tamsayılarda Aritmetik

Z de birimin yani 1 tamsayısının bölenlerine aritmetik birimler denir. Bir tamsayının aritmetik birim olması için gerek ve yeter koşul bütün tamsayıları bölmesidir. Z'de aritmetik birimler ± 1 dir.

$a,b \in Z$ ve $b \neq 0$ olsun. $a=bq+r$ ve $0 \leq r < |b|$ olacak şekilde bir q tamsayısı ve r doğal sayısı bulunabiliyorsa a, b'ye kalanlı olarak bölünüyor denir. a'ya bölünen, b'ye bölen, q'ya bölüm, r'ye kalan denir.

Herhangi bir a tamsayısı için a=0 ise, sıfırdan farklı her tamsayı a'nın bir bölenidir. $a \neq 0$ ise -1,+1,a,-a sayılarından biri a'nın bir bölenidir. A'nın bundan başka bölenleri de bulunabilir. Bir a tamsayısının bölenleri {B(a)} ile gösterilir. Örneğin

{B(8)}={-8,-4,-2,-1,1,2,4,8} dir.

Sıfırdan farklı iki a ve b tamsayısının her ikisini de bölen x tamsayısına bu sayıların ortak böleni denir.

{OB(a,b)} ile gösterilir.

$\{OB(a,b)\}=\{B(a) \cap B(b)\}$
{B(6)}={-6,-3,-2,-1,1,2,3,6}
{B(8)}={-8,-4,-2,-1,1,2,4,8}
$\{OB(6,8)\}=\{B(6) \cap B(8)\}=\{-2,-1,1,2\}$

Tamsayılarda Aritmetik

Teorem
$a,b \in Z$ ve $b \neq 0$ olsun.
$b \mid a \Rightarrow \{OB(a,b)\}=\{B(b)\}$ dir.

Teorem
$a,b \in Z$ ve $b \neq 0$ olsun. $a=bq+r$ ve $0 \leq r < |b|$ ise
$\{OB(a,b)\}=\{OB(b,r)\}$

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. a ve b nin ortak bölenlerinin kümesinin en büyük elemanına OBEB denir.

Örneğin OBEB(36,28)=4 dür.(uygulama1)

Teorem(Öklid Algoritması)

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. $OBEB(a,b)=r_n$ olacak biçimde bir ve yalnız bir tane r_n tamsayısı vardır. Bu sayı a ve b tamsayılarının lineer toplamı olarak yazılabilir. Yani, en az bir m,n tamsayıları için,

$OBEB(a,b)=r_n=ma+nb$ dir.

(uygulama2)

Tamsayılarda Aritmetik

Teorem

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. OBEB(a,b)= OBEB(b,a) dır.

Teorem

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. $m \in Z^+$ ise OBEB(ma,mb)=m[OBEB(a,b)] dir.

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. Bu sayıların ortak bölenlerinin en büyüğü 1 ise bu sayılara aralarında asal sayılar denir. (a,b)=1 ile gösterilir.

(a,b)=1$\Leftrightarrow$ OBEB(a,b)=1

Örneğin OBEB(9,16)=1$\Leftrightarrow$(9,16)=1 dir.

Teorem

En az biri sıfırdan farklı 2 tamsayı a ve b olsun. a ve b nin aralarında asal olması için

ma+nb=1 olacak şekilde m,n tamsayılarının bulunması gerek ve yeter koşuldur.

Teorem

a,b,c tamsayılar olsun. (a,c)=1 ve (b,c)=1 ise (ab,c)=1 dir.

Tamsayılarda Aritmetik

Teorem

a,b,c tamsayılar olsun. $a \mid (bc)$ ve $(a,b)=1$ ise $a \mid c$ dir.

Teorem

a,b,n tamsayılar olsun. $a \mid n$, $b \mid n$ ve $(a,b)=1$ ise $(ab) \mid n$ dir.

Sıfırdan farklı a tamsayısının bütün katlarının kümesi {K(a)} ile gösterilir.
Her ikisi de sıfırdan farklı olan a ve b tamsayılarından her ikisinin katı olan bir tamsayıya bu sayıların ortak bir katı denir. {OK(a,b)} ile gösterilir.

$\{OK(a,b)\}=\{K(a)\cap K(b)\}$ dir.

Örneğin -2 ve 3 sayıları için $\{OK(-2,3)\}=\{K(6)\}$ dır.(uygulama3)

$\{OK(a,b)\}\neq 0$ dır.

BSM

Tamsayılarda Aritmetik

Teorem

$a,b \in Z-\{0\}$ olsun. OBEB(a,b)=d ise

$\{OK(a,b)\}=\{K((ab):d)\}$ dir.

Sıfırdan farklı a ve b tamsayılarının pozitif ortak katlarının en küçüğüne, a ve b nin ortak katlarının en küçüğü denir ve OKEK(a,b) ile gösterilir.

OKEK(a,b)= OKEK(a,-b)= OKEK(-a,b)= OKEK(-a,-b) dir.

Teorem

Sıfırdan farklı a ve b tamsayıları için OKEK(a,b)=k ise

$\{OK(a,b)\}=\{K(k)\}$ dır.

Teorem

Pozitif bir k tamsayısının, a ve b tamsayılarının ortak katlarının en küçüğü olması için

$OKEK(a,b)=k \Leftrightarrow ((k:a),(k:b))=1$ olmalıdır.

BSM

4. Hafta

13. Sayfa

Tamsayılarda Aritmetik

Pozitif bir n tamsayısını ele alalım. a tamsayısının n moduna göre b tamsayına denk olabilmesi için, $a \equiv b \pmod{n}$, n tamsayısının (a-b) tamsayısını bölmesi gerekmektedir.

$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$ dir.

Teorem

Sabit bir n için tanımlanan bir benzeşim tamsayılar kümesi üzerinde bir eşdeğer bağıntıdır, öyleki

a) $a \equiv a \pmod{n}$ her a tamsayısı için doğrudur.

b) Eğer $a \equiv b \pmod{n}$ ise, $b \equiv a \pmod{n}$ benzeşimi a ve b tamsayıları için sağlanır.

c) Eğer $a \equiv b \pmod{n}$ ve $b \equiv c \pmod{n}$ ise $a \equiv c \pmod{n}$ yazılabilir.

Teorem

$x, y, z \in Z$ ve $m \in Z^+$ olsun.

$x \equiv y \pmod{m} \Leftrightarrow r = s$ dir. (r ve s sırasıyla x ve y nin m ile bölünmesi sonucunda kalanlardır)

BSM

4. Hafta

Tamsayılarda Aritmetik

Teorem

$x,y,z,w,u,v \in Z$ ve $m \in Z^+$ olsun.

$x \equiv y (\mathrm{mod}\ m)$ ve $z \equiv w (\mathrm{mod}\ m)$ ise aşağıda önermeler doğrudur:

$x+u \equiv y+u\ (\mathrm{mod}\ m)$

$xu \equiv yu\ (\mathrm{mod}\ m)$

$x+z \equiv y+w\ (\mathrm{mod}\ m)$

$x-z \equiv y-w\ (\mathrm{mod}\ m)$

$xz \equiv yw\ (\mathrm{mod}\ m)$

$ux+vz \equiv uy+vw\ (\mathrm{mod}\ m)$

Algoritmalar

Verilen bir m reel sayısı ve pozitif n sayısı için P=Xn 'i hesaplayan algoritma

Adım1 (KOŞULLAMA)

P=X ve k=1

Adım 2 (SONRAKİ KUVVET)

While k< n

(a) $P \leftarrow P.X$

(b) $k \leftarrow k+1$

EndWhile

Adım 3: (P=Xn olur)

Print P.

BSM

4. Hafta

16. Sayfa

Dikkat edilirse 2.adımda n-1 çarpma n-1 toplama ve k adet karşılaştırma (k=n olduğunda 2.adımdan çıkılıyor) yapılıyor.Buna göre X^n in hesaplanması için toplam (n-1)+(n-1)+n=3n-2 adet elemanter işlem yapılmaktadır.

Algoritmalar

$P(X)=a_n x^n+\ldots\ldots\ldots+a_0$, n pozitif tam sayı , $x, a_0, \ldots\ldots a_n$ reel sayılar

Adım 1: (Koşullama)

$S=a_0$, $k=1$

Adım 2 : (Bir sonraki terimi ekle)

While $k \leq n$

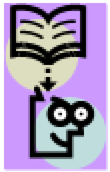
(a) $S \longleftarrow S+a_k x^k$

(b) $\mathbf{k} \longleftarrow k+1$

EndWhile

Adım 3: Print s

2.adımda $k \leq n$ kontrolünü k=1,2.....n+1 için n+1 kere yapıyoruz .Herhangi bir $k \leq n$ için 1 karşılaştırma, 2 toplama ,1 çarpma ve (3k-2) işlem x^k hesabı için yapıyoruz. O halde 3k-2+4=3k+2 işlem yapılmaktadır. k=1,2,...n için $5+8+11+\ldots\ldots+3n+2=(3n^2+7n)/2$ işlem yapılıyor. k=n+1için yapılan karşılaştırmayı da eklersek $((3n^2+7n)+1)/2$ işlem yapılmaktadır . Görüldüğü gibi algoritmanın karmaşıklılığı bir polinomdur , yani $1.5n^2+3.5n+0.5$ dir. Burada polinomun derecesi karmaşıklıkta bizim için çok dalış önemlidir. Bu örnekte n^2 karmaşıklılık etkin olacaktır.



Ödev

1. $\forall a,b,c \in Z$ için $a|b$ ve $a|c$ ise $\forall x,y \in Z$ için $a|xb+yc$ dir. İspatlayınız.
2. $x,y \in Z$ ve $m,n \in Z^+$ olsun.

   $x \equiv y \pmod{m} \Rightarrow x^n \equiv y^n \pmod{m}$ olduğunu ispatlayınız.

3. Öklid algoritmasını yazınız.

Kaynaklar

F.Selçuk,N.Yurtay,N.Yumuşak,Ayrık İşlemsel Yapılar, Sakarya Kitabevi,2005.
İ.Kara, Olasılık, Bilim Teknik Yayınevi, Eskişehir, 2000.
“Soyut Matematik”, S.Aktaş,H.Hacısalihoğlu,Z.Özel,A.Sabuncuoğlu, Gazi Ünv.Yayınları,1984,Ankara.
“Applied Combinatorics”, Alan Tucker, John Wiley&Sons Inc, 1994.
“Applications of Discrete Mathematics”, John G. Michaels, Kenneth H. Rosen, McGraw-Hill International Edition, 1991.
“Discrete Mathematics”, Paul F. Dierker and William L.Voxman, Harcourt Brace Jovanovich International Edition, 1986.
“Discrete Mathematic and Its Applications”, Kenneth H. Rosen, McGraw-Hill International Editions, 5th Edition, 1999.
“Discrete Mathematics”, Richard Johnson Baugh, Prentice Hall, Fifth Edition, 2001.
“Discrete Mathematics with Graph Theory” , Edgar G. Goodaire, Michael M. Parmenter, Prentice Hall, 2nd Edition, 2001.
“Discrete Mathematics Using a Computer”, Cordelia Hall and John O’Donnell, Springer, 2000.
“Discrete Mathematics with Combinatorics”, James A. Anderson, Prentice Hall, 2000.
“Discrete and Combinatorial Mathematics”, Ralph P. Grimaldi, Addison-Wesley, 1998.
“Discrete Mathematics”, John A. Dossey, Albert D. Otto, Lawrence E. Spence, C. Vanden Eynden, Pearson Addison Wesley; 4th edition 2001.
“Essence of Discrete Mathematics”, Neville Dean, Prentice Hall PTR, 1st Edition, 1996.
“Mathematics:A Discrete Introduction”, Edvard R. Schneiderman, Brooks Cole; 1st edition, 2000.
“Mathematics for Computer Science”, A.Arnold and I.Guessarian, Prentice Hall, 1996.
“Theory and Problems of Discrete Mathematics”, Seymour Lipschuts, Marc. L. Lipson, Shaum’s Outline Series, McGraw-Hill Book Company, 1997.
“2000 Solved Problems in Discrete Mathematics”, Seymour Lipschuts, McGraw- Hill Trade, 1991.