Mittuniversitetet
MID SWEDEN UNIVERSITY

Block 4
Algebra och Diskret Matematik A

BLOCK INNEHÅLL

Modulär aritmetik, relationer och funktioner

Referenser

[J] Edition 5: Nedanstående text + [J] 2.4, 2.5, 2.8
[J] Edition 4: Nedanstående text + [J] (2.4), (2.5), (2.8)
[J] Edition 6: Nedanstående text + [J] [3.1], [3.2], [2.2]

Bemärk, referenser i texten utan parenteser är till [J]ohnsonbaugh Edition 5, referenser i ()-parenteser är till [J] Edition 4, och referenser i []-parenteser är till [J] Edition 6.

Inledning

I detta block skall vi titta på modulär aritmetik, som är ett viktigt redskap när man studerar heltal. Vi skall också studera relationer på mängder, och vi skall se hur några speciella relationer kan användas för att dela upp, partitionera, en mängd i delmängder, så att man kan urskilja några strukturella egenskaper hos mängden. Slutligen skall vi se på funktioner, ett område som du känner igen från gymnasietiden.

1. Kongruens modulo n

Vi börjar med en viktig definition:

Definition
Låt n vara ett *positivt* heltal. Heltalen a och b sägs vara **kongruenta modulo n** om n är en faktor i a-b eller med andra ord om

$$n \mid (a-b).$$

Om a och b är kongruenta modulo n skriver vi

$$a \equiv b \pmod{n},$$

vilket utläses som 'a är kongruent med b modulo n'.

Exempel
$12 \equiv 22 \equiv 42 \equiv 2 \pmod{10}$

$-18 \equiv -38 \equiv -8 \equiv 2 \pmod{10}$

$12 \equiv 19 \equiv -9 \equiv 5 \pmod{7}$

$7 \equiv 5 \equiv 3 \equiv 1 \pmod 2$

$6 \equiv 4 \equiv 2 \equiv 0 \pmod 2$

Notera till att börja med, att n | (a-b) om och endast om vi kan finna en kvot k i $\mathbb{Z}$ sådan att a - b = kn.

Vidare, när a - b =kn för något heltal k så ger a och b samma rest vid division med n:
Antag att $a=q_1n + r_1$ och $b=q_2n + r_2$ med $0 \leq r_1 < n$ och $0 \leq r_2 < n$. Då är

$$a - b = (q_1 - q_2)n + (r_1 - r_2),$$

som omskrivas till

$$r_1 - r_2 = (a - b) - (q_1 - q_2)n = kn - (q_1 - q_2)n = (k - q_1 + q_2)n.$$

Höger sida av detta uttryck innehåller en faktor n, så n måste också vara en faktor i vänster sida, så $n \mid r_1-r_2$.
Men $-n < r_1 - r_2 < n$, så det följer att $r_1 - r_2 = 0$, så $r_1=r_2$.

Omvänt gäller också att om a och b ger samma rest vid division med n, så följer att n | (a-b):
Om $a=q_1n + r$ och $b=q_2n + r$, så är $a - b =(q_1 - q_2)n + (r - r) = (q_1 - q_2)n$. Vi har alltså följande tre resultat:

Sats B4.1
$a \equiv b \pmod n$ om och endast om det finns ett heltal k så att a-b =kn.

Sats B4.2
$a \equiv b \pmod n$ om och endast om det finns ett heltal k så att a = b + kn.

Sats B4.3
$a \equiv b \pmod n$ om och endast om a och b ger samma rest vid division med n.

Dessa tre resultat bygger alla på en av de viktigaste satser vi har lärt oss (i block 2):

Divisionsalgoritmen
Givet ett godtyckligt heltal a och ett positivt heltal n, så existerar det entydigt bestämda heltal k och r sådana att

$$a=kn + r \quad \text{och} \quad 0 \leq r \leq n-1.$$

Översatt till kongruenser mellan heltal så betyder denna sats att det finns ett *entydigt* bestämt heltal r i mängden {0, 1, 2, 3, 4, . . . , n-1} sådan att $a \equiv r \pmod n$. En del programmeringsspråk, t.ex. Pascal har en standard funktion MOD som beräknar denna entydigt bestämda rest. I Java finns funktionen också, men betecknas '%'.

Exempel
Låt oss beräkna det entydigt bestämda heltal r så att
$a \equiv r \pmod n$ och $0 \leq r \leq n-1$, när

(a) n = 5 och a = 448;
(b) n = 5 och a= - 63;
(c) n = 4 och a=17, -17;
(d) n = 2 och a är ett jämnt/udda heltal.

Svar:
(a) När vi dividerar 448 med 5 får vi kvoten 89 och resten 3, d.v.s. 448= 5(89) +3
så r=3 och $448 \equiv 3 \pmod 5$ med $0 \leq 3 \leq 4$ som vi vill.

(b) När vi dividerar -63 med 5 får vi kvoten -13 och resten 2, d.v.s. -63= 5(-13) +2
så r=2 och $-63 \equiv 2 \pmod 5$ med $0 \leq 2 \leq 4$.

(c) När vi dividerar 17 med 4 får vi kvoten 4 och resten 1, d.v.s. 17= 4(4) +1
så r=1 och $17 \equiv 1 \pmod 4$ med $0 \leq 1 \leq 3$.

När vi dividerar -17 med 4 får vi kvoten -5 och resten 3, d.v.s -17= 4(-5) +3
så r=3 och $-17 \equiv 3 \pmod 4$ med $0 \leq 3 \leq 3$.

(d) När vi dividerer ett jämnt tal 2k med 2 får vi kvoten k och resten 0, d.v.s. 2k= 2(k) +0,
så r=0 och $2k \equiv 0 \pmod 2$ med $0 \leq 0 \leq 1$.

När vi dividerar ett udda tal 2k+1 med 2 får vi kvoten k och resten 1, d.v.s. 2k+1= 2(k) +1
så r=1 och $2k+1 \equiv 1 \pmod 2$ med $0 \leq 1 \leq 1$.

Exempel
Låt oss nu göra det motsatta och bestämma mängden av alla heltal som är kongruenta modulo 5 med vart och ett av talen 0, 1, 2, 3 och 4:

- Mängden av heltal a sådana att $a \equiv 0 \pmod 5$ är

  $\{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} = \{x \mid x=5z, z \in \mathbb{Z}\}$

- Mängden av heltal a sådana att $a \equiv 1 \pmod 5$ är

  $\{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} = \{x \mid x=5z+1, z \in \mathbb{Z}\}$

- Mängden av heltal a sådana att $a \equiv 2 \pmod 5$ är

  $\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} = \{x \mid x=5z+2, z \in \mathbb{Z}\}$

- Mängden av heltal a sådana att $a \equiv 3 \pmod 5$ är

  $\{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} = \{x \mid x=5z+3, z \in \mathbb{Z}\}$

- Mängden av heltal a sådana att $a \equiv 4 \pmod 5$ är

  $\{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\} = \{x \mid x=5z+4, z \in \mathbb{Z}\}$

Notera att alla heltal i var och en av de fem mängderna ger samma rest vid division med 5, så i en och samma mängd är varje par av element därför kongruenta modulo 5. Notera också att varje heltal är i en och endast en av dessa mängder. Dvs. de fem mängderna partitionerar $\mathbb{Z}$.

Mängden av heltal a sådana att $a \equiv b \pmod n$ kallas för **kongruensklassen modulo n med representanten** b.
Vi använder beteckningen $[b]_n$ för kongruensklassen som innehåller alla a sådana att $a \equiv b \pmod n$. När det av sammanhanget klart framgår vad n är, kan vi bortse från indexet n i denna notation och endast skriva [b] för kongruensklassen modulo n med representanten b.

Exempel
Låt oss bestämma några kongruensklasser modulo 10 med diverse representanter:

$[3]_{10} = \{\ldots, -27, -17, -7, 3, 13, 23, 33, \ldots\}$,

$[5]_{10} = \{\ldots, -25, -15, -5, 5, 15, 25, 35, \ldots\}$,

$[12]_{10} = \{\ldots, -28, -18, -8, 2, 12, 22, 32, \ldots\}$,

$[43]_{10}$ = {. . ., -27, -17, -7, 3, 13, 23, 33, 43, . . .}.

$[-2]_{10}$ = {. . . , -32, -22, -12, -2, 8, 18, 28, 38, . . .}

Vid en snabb blick verkar det finnas oändligt många kongruensklasser modulo n (en för varje representant ur $\mathbb{Z}$). Detta är inte fallet, för många av dem är lika. Till exempel är $[43]_{10} = [3]_{10}$. För n=5 vet vi också från det föregående exemplet, att eftersom alla heltal är i en av de fem mängderna vi beräknade, är det precis fem kongruensklasser modulo 5, en svarande till var och en de fem möjliga resterna vid division med 5.

Allmänt finns det precis n kongruensklasser modulo n, nämligen en klass svarande mot var och en av de n möjliga resterna 0,1, ... n-1 som kan uppkomma vid division med n. Det vanliga är att ett av talen 0,1,2, . . . , n-1 används som representant för kongruensklassen, men det är inte absolut nödvändigt: ett *godtyckligt* element i kongruensklassen kan användas som representant. Till exempel så skrivs mängden {. . ., -28, -18, -8, 2, 12, 22, 32, . . .} vanligen med $[2]_{10}$ för 2 är den entydigt bestämda resten i divisionsalgoritmen, men som du såg i exemplet ovan är $[12]_{10}$ precis samma mängd.

Exempel
Tidigare beräknade vi för n = 5:

$[0] = \{x \mid x=5z, z \in \mathbb{Z}\}$,

$[1] = \{x \mid x=5z+1, z \in \mathbb{Z}\}$,

$[2] = \{x \mid x=5z+2, z \in \mathbb{Z}\}$,

$[3] = \{x \mid x=5z+3, z \in \mathbb{Z}\}$,

$[4] = \{x \mid x=5z+4, z \in \mathbb{Z}\}$,

men vi skulle också kunna representera t.ex. kongruensklassen $\{x \mid x=5z+2, z \in \mathbb{Z}\}$ med [7]
och klassen $\{x \mid x=5z+1, z \in \mathbb{Z}\}$ med [6] eller [-4] eller [-9] eller . . .

Uppgift B4.1
Sant eller falskt?

1. $81 \equiv 1 \pmod 8$;
2. $81 \equiv 1 \pmod{10}$;
3. $112 \equiv 4 \pmod{11}$;
4. $1000 \equiv -1 \pmod{13}$;
5. $9 \equiv 90 \pmod 5$;
6. $937 \equiv 37 \pmod{100}$;
7. För godtyckliga heltal a, b, c och m; om $a \equiv b \pmod m$, så är a = b;
8. Om $a \equiv b \pmod m$, så är $a+c \equiv b+c \pmod m$;
9. Om $a \equiv b \pmod m$, så är $ac \equiv bc \pmod m$.

Uppgift B4.2
Bestäm alla heltal x sådana att $x \equiv 3 \pmod 5$.

2. $\mathbf{Z}_n$ -- heltalen modulo n

Vi såg i avsnitt 1 ovan att kongruens modulo n ger n kongruensklasser [0], [1], [2], . . . , [n-1] sådana att varje heltal finns i precis en av dessa klasser. Vi definierar nu mängden $\mathbf{Z}_n$, som läses **heltalen modulo n**, till att vara mängden bestående av dessa n kongruensklasser, d.v.s.

$$\mathbf{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}.$$

Om det klart framgår av sammanhanget vilket talet n är kommer vi endast att skriva [x] för ekvivalensklassen $[x]_n$. Heltalen modulo n skrivs då

$$\mathbf{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Vi kan definiera en slags addition, som vi betecknar med $\oplus$, och en slags multiplikation, som vi betecknar med $\odot$, på $\mathbf{Z}_n$:

$$[x] \oplus [y] := [x+y],$$
$$[x] \odot [y] := [xy].$$

Notera att resultatet vid utförande av operationerna $\oplus$ eller $\odot$ på två element i $\mathbf{Z}_n$ är ett element i $\mathbf{Z}_n$ för vi visade i avsnitt 1, att for varje heltal x är klassen $[x]_n$ ett av de n elementen i $\mathbf{Z}_n$. Vi har också följande viktiga resultat:

Sats B4.4
Låt x, y, s och t vara heltal och låt n vara ett positivt heltal. Om $s \in [x]_n$ och $t \in [y]_n$, så är $s+t \in [x+y]_n$ och $st \in [xy]_n$.

Bevis.
Om $s \in [x]_n$ och $t \in [y]_n$, så är $s \equiv x \pmod n$ och $t \equiv y \pmod n$. Det vill säga $n \mid (s-x)$ och $n \mid (t-y)$, så det existerar alltså heltal k och m sådana att s-x=kn och t-y=mn. Men då är

$$(s - x) + (t - y) = kn + mn,$$

och detta kan skrivas om till

$$(s + t) - (x + y) = (k+m)n,$$

varav det inses att

$$(s + t) \equiv (x + y) \pmod n,$$

eller med andra ord

$$s+t \in [x+y]_n .$$

Vi får också

$$(s - x)(t - y) = (kn)(mn),$$

som ger att

$$(kn)(mn) = st + xy - xt - ys = st + xy - x(y + mn) - y(x + kn) = st - xy - (xm + yk)n,$$

vilket kan skrivas om till

$$st - xy = (knm + xm + yk)n.$$

Det följer att

$$st \equiv xy \pmod n,$$

så $st \in [xy]_n$. □

Sats B4.4 säger att om $s \in [x]_n$ och $t \in [y]_n$, så är $[s+t]_n = [x+y]_n$, och $[st]_n = [xy]_n$, vilket betyder att inte bara klasserna, utan också definitionerna av $\oplus$ och $\odot$ är oberoende av valet av klassrepresentant.

Det finns många grundläggande lagar som gäller för de två operationerna $\oplus$ och $\odot$. Du känner säkert igen de flesta av dem som har motsvarigheter i liknande räknelagar för heltal.

Sats B4.5
Om $\mathbf{Z}_n$ är mängden av kongruensklasser modulo n och $\oplus$ och $\odot$ är definierade som ovan, så uppfyller $\mathbf{Z}_n$ följande:

1. *Slutenhet*. För alla $[x], [y] \in \mathbf{Z}_n$ gäller att
   $[x] \oplus [y] \in \mathbf{Z}_n$ och
   $[x] \odot [y] \in \mathbf{Z}_n$.
2. *Associativa lagar*. För alla $[x], [y], [z] \in \mathbf{Z}_n$ gäller att
   $[x] \oplus ([y] \oplus [z]) = ([x] \oplus [y]) \oplus [z]$ och
   $[x] \odot ([y] \odot [z]) = ([x] \odot [y]) \odot [z]$.

3. *Identiteter existerar*.
   Det existerar ett element $[0] \in \mathbf{Z}_n$ sådant att för alla $[x] \in \mathbf{Z}_n$ har vi att
   $[x] \oplus [0] = [0] \oplus [x] = [x]$.

   Det existerar också ett element $[1] \in \mathbf{Z}_n$, med $[1] \neq [0]$, sådant att för alla $[x] \in \mathbf{Z}_n$ har vi att
   $[x] \odot [1] = [1] \odot [x] = [x]$.

4. *Additiva inverser existerar*. För alla $[x] \in \mathbf{Z}_n$ har vi att
   det existerar en additiv invers $[-x] \in \mathbf{Z}_n$ som uppfyller att
   $[x] \oplus [-x] = [-x] \oplus [x] = [0]$.

5. *Kommutativa lagar*. För alla $[x],[y] \in \mathbf{Z}_n$ så gäller att
   $[x] \oplus [y] = [y] \oplus [x]$ och
   $[x] \odot [y] = [y] \odot [x]$.

6. *Distributiva lagar*. För alla $[x],[y],[z] \in \mathbf{Z}_n$ gäller att
   $[x] \odot ([y] \oplus [z]) = ([x] \odot [y]) \oplus ([x] \odot [z])$ och

   $([y] \oplus [z]) \odot [x] = ([y] \odot [x]) \oplus ([z] \odot [x])$.

Bevis.
Vi resonerade tidigare om varför den första lagen gäller. Vi visar nu de associativa lagarna (lag 2) och lagen om existens av additiv invers (lag 4). De andra bevisen överlåter vi till läsaren.

Först visar vi att $\oplus$ är associativ:

$$\begin{aligned}
([x] \oplus [y]) \oplus [z] &= [x+y] \oplus [z] && \text{(från definitionen av } \oplus) \\
&= [(x+y) + z] && \text{(igen med definitionen av } \oplus) \\
&= [x+ (y+z)] && \text{(för att + är associativ på } \mathbb{Z}) \\
&= [x] \oplus [y+z] && \text{(från definitionen av } \oplus) \\
&= [x] \oplus ([y] \oplus [z]) && \text{(igen med definitionen av } \oplus)
\end{aligned}$$

Därnäst visar vi att $\odot$ är associativ:

$$\begin{aligned}
([x] \odot [y]) \odot [z] &= [xy] \odot [z] && \text{(från definitionen av } \odot) \\
&= [(xy)z] && \text{(igen med definitionen av } \odot) \\
&= [x(yz)] && \text{(för att + är associativ på } \mathbb{Z}) \\
&= [x] \odot [yz] && \text{(från definitionen av } \odot) \\
&= [x] \odot ([y] \odot [z]) && \text{(igen med definitionen av } \odot)
\end{aligned}$$

Med lag 4 har vi från definitionen av $\oplus$, att det för alla $[x] \in \mathbf{Z}_n$ gäller att

$$[x] \oplus [n-x] = [n-x] \oplus [x] = [n] = [0].$$

Det innebär att klassen [n-x] är en additiv invers till [x]. □

Låt oss nu konstruera additions- och multiplikationstabeller för $\mathbf{Z}_n$ för några värden på n:

Exempel
Additionstabellen för $\mathbf{Z}_4$ är:

⊕	*[0]*	*[1]*	*[2]*	*[3]*
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Multiplikationstabellen för $\mathbf{Z}_4$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Exempel
Additionstabellen för $\mathbf{Z}_5$ är:

⊕	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Multiplikationstabellen för $\mathbf{Z}_5$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Många av räknelagarna i sats B4.5 kan lätt läsas av i dessa tabeller. Till exempel visas de kommutativa lagarna av att tabellerna är symmetriska omkring huvuddiagonalen. Man ser också att [0] är en additiv identitet och att [1] är en multiplikativ identitet, ty raden för [0] i additionstabellen och raden för [1] i multiplikationstabellen har alla element i naturlig ordningsföljd. Vidare är det precis ett element [0] i varje rad i additionstabellen svarendes mot att det för en godtycklig klass [x] finns precis en klass [y] sådan att $[x] \oplus [y] = [0]$ - detta är lagen om existens av additiv invers.

Vi noterar också att $\mathbf{Z}_5$ har några egenskaper som $\mathbf{Z}_4$ inte har:

I multiplikationstabellen för $\mathbf{Z}_5$ är det precis en [1] och precis en [0] i varje rad och varje kolonn. Detta är inte fallet i multiplikationstabellen för $\mathbf{Z}_4$, i vilken det inte finns någon [1] i raden eller kolonnen för [2], medan det finns två [0] i denna rad/kolonn. Elementet $[2] \in \mathbf{Z}_4$ kallas en nolldelare.

Definition
Vi definerar en **nolldelare** i $\mathbf{Z}_n$ till att vara ett element $[z] \in \mathbf{Z}_n$ med $[z] \neq [0]$
för vilket det existerer ett element $[m] \in \mathbf{Z}_n$ med $[m] \neq [0]$ sådant att $[z] \odot [m] = [0]$.

Exempel
Om man sätter z=2 och m=2 i denna definition ser man att [2] är en nolldelare i $\mathbf{Z}_4$.

De reella talen $\mathbb{R}$, de rationella talen $\mathbb{Q}$ och heltalen $\mathbb{Z}$ uppfyller en mycket viktig lag som kallas **lagen om nolldelare**. Den säger att dessa talmängder *inte* innehåller nolldelare. Om man t. ex. har två reella tal r och s sådana att rs=0, så är antingen r=0 eller s=0 (eller de är bägge 0). För de reella talen $\mathbb{R}$ är det därför inte möjligt att ha två tal båda skilda från noll med produkten noll. Vi använder ofta denna lag vid lösning av ekvationer. Resonemang i stil med följande exempel känner du säkert igen:

$$(x-2)(x-4)=0 \quad \Rightarrow \quad (x-2)=0 \text{ eller } (x-4)=0 \quad \Rightarrow \quad x=2 \text{ eller } x=4.$$

Ur multiplikationstabellen för $\mathbf{Z}_5$ ser vi att $\mathbf{Z}_5$ också uppfyller lagen om nolldelare. Det är ingen produkt av element i $\mathbf{Z}_5$ som är [0] utan att minst en av faktorerna är [0]. Vi noterade ovan att $\mathbf{Z}_4$ har en nolldelare, för

$$[2]_4 \odot [2]_4 = [0]_4,$$

det vill säga $\mathbf{Z}_4$ uppfyller *inte* lagen om nolldelare.

Uppgift B4.3
Beräkna multiplikationstabellerna för $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_6$, $\mathbf{Z}_7$, $\mathbf{Z}_8$ och $\mathbf{Z}_9$. I vilka av dessa är lagen om nolldelare giltig och i vilka håller den inte? Kan du gissa för vilka n lagen on nolldelare gäller i $\mathbf{Z}_n$?

Vi hoppas att ditt svar till uppgift B4.3 stämmer överens med följande sats:

Sats B4.6
Låt n vara ett heltal sådant att $n \geq 2$ och låt $\mathbf{Z}_n$ vara mängden av kongruensklasser (mod n).
Då finns det ingen nolldelare i $\mathbf{Z}_n$ om och endast om n är ett primtal.

Bevis
Antag först att n=p där p är ett positivt primtal och att $[x] \odot [y] = [0]$ i $\mathbf{Z}_p$. Eftersom $[x] \odot [y] = [xy]$ har vi att $[xy] = [0]$, dvs. $xy \equiv 0 \pmod{p}$, och därför gäller att $p \mid xy$. Men då följer det av sats B3.8 från läsanvisningen till block 3 att $p \mid x$ eller $p \mid y$, dvs. $[x] = [0]$ eller $[y] = [0]$. Så när n är ett positivt primtal, då finns det ingen nolldelare i $\mathbf{Z}_n$.

När n däremot *inte* är ett primtal så är n ett sammansatt tal och vi kan därför uttrycka n som en produkt av två äkta faktorer a och b, dvs.

$$n=ab,$$

med $2 \leq a \leq n-1$ och $2 \leq b \leq n-1$. Då är

$$[a]_n \odot [b]_n = [ab]_n = [n]_n = [0]_n,$$

och både $[a]_n \neq [0]_n$ och $[b]_n \neq [0]_n$, så $[a]_n$ (och också $[b]_n$) är en nolldelare i $\mathbf{Z}_n$. □

Vid lösning av ekvationer med reella tal användes ofta möjligheten att det är tillåtet att förkorta med en faktor skild från 0 på båda sidor av likhetstecknet. Har vi till exempel för $x \in \mathbb{R}$ att $3x = 3 \cdot 2$ så kan vi dra följande slutsats:

$$3x = 3 \cdot 2 \quad \Rightarrow \quad x=2,$$

dvs. vi delar med en faktor 3 på båda sidor av likhetstecknet.

Om p är ett primtal fungerar en motsvarande förkortningslag i $\mathbf{Z}_p$:

Följdsats B4.7 [Förkortningsregeln]
Låt p vara ett positivt primtal och anta att klassen $[a] \in \mathbf{Z}_p$ är sådan att $[a] \neq [0]$.
För alla klasser $[x], [y] \in \mathbf{Z}_p$ gäller att, om $[a] \odot [x] = [a] \odot [y]$ så är $[x] = [y]$.

Bevis.
Om $[a] \odot [x] = [a] \odot [y]$, så har vi att $[ax]=[ay]$. Det följer att $ax \equiv ay \pmod p$, så $p \mid (ax-ay)$.
Dvs. $[0] = [ax-ay] = [a] \odot [x-y]$ och sats B4.6 säger då att $[a]=[0]$ eller $[x-y]=[0]$. Med antagandet att $[a] \neq [0]$ så måste $[x-y]=[0]$ vilket medför att $p \mid (x-y)$. Dette ger nu att $x \equiv y \pmod p$ vilket är detsamma som att $[x] = [y]$. □

Var aktsam på att förkortningsregeln *inte* gäller i $\mathbf{Z}_n$ om n är ett sammansatt tal:
Låt n=ab vara en faktorisering av n i två äkta faktorer, så är $[a] \odot [b] = [0]$; men även $[a] \odot [0] = [0]$, så vi har alltså att

$$[a] \odot [b] = [a] \odot [0].$$

Trots detta är det *inte* så att $[b] = [0]$ ty b är en äkta faktor i n, så $1 < b < n$.

De reella talen $\mathbb{R}$ och de rationella talen $\mathbb{Q}$ har en annan viktig egenskap som vi också ofta använder när vi löser ekvationer. Det är egenskapen att varje tal skilt från 0 har en såkallad multiplikativ invers. En *multiplikativ invers* till ett tal r är ett tal s sådant att rs = sr = 1. Det reella talet 0,5 är en multiplikativ invers till 2 eftersom $(0,5)\cdot 2 = 2\cdot(0,5) =1$, och vi kan till exempel använda detta vid lösning av ekvationen $2x =6$ på följande sätt:

$$2x = 6 \quad => \quad (0,5)\cdot(2x) = (0,5)\cdot 6 \quad => \quad ((0,5)\cdot 2)x = (0,5)\cdot 6 \quad => \quad 1\cdot x = 3 \quad => \quad x=3.$$

På liknande sätt definierar vi:

Definition
En **multiplikativ invers** till $[x] \in \mathbf{Z}_n$, där $[x] \neq [0]$, är ett element $[m] \in \mathbf{Z}_n$ med egenskapen att

$$[x] \odot [m] = [m] \odot [x] = [1].$$

Vi såg i multiplikationstabellen för $\mathbf{Z}_4$ tidigare att $[2]_4$ inte har en multiplikativ invers, ty det finns inte något element i $\mathbf{Z}_4$ som ger $[1]_4$ när vi multiplicerar det med $[2]_4$. I $\mathbf{Z}_5$ däremot har varje element som inte är $[0]_5$ en multiplikativ invers, ty i multiplikationstabellen för $\mathbf{Z}_5$ ser vi att varje rad utom för $[0]_5$ innehåller $[1]_5$. Allmänt gäller det följande:

Sats B4.8
Låt n vara ett positivt heltal med $n \geq 2$ och låt $[x] \in \mathbf{Z}_n$ vara skilt från [0].
Då har [x] en multiplikativ invers i $\mathbf{Z}_n$ om och endast om sgd(x,n) = 1.
Det gäller ytterligare att om det existerar en multiplikativ invers till [x], så är denna invers unik.

Bevis.
Om sgd(x,n) = 1 så finns det (enligt sats B3.7 från läsanvisningen till block 3) heltal a och b
sådana att ax+bn=1. Det vill säga bn = 1 - ax och vi har därför att $ax \equiv 1 \pmod n$.
Detta betyder att i $\mathbf{Z}_n$ har vi $[a] \odot [x] = [1]$. Alltså är [a] en multiplikativ invers till [x] i $\mathbf{Z}_n$.

Omvänt, om det existerar ett element $[m] \in \mathbf{Z}_n$ sådant att $[x] \odot [m] = [m] \odot [x] = [1]$, då är
$xm \equiv 1 \pmod n$ och därför har vi att $n \mid (xm - 1)$. Dvs. det finns ett heltal r sådant att $rn = xm - 1$ och alltså är

$$1 = xm - nr.$$

Eftersom sgd(x,n) delar både x och n, är högra sidan av detta uttryck delbart med sgd(x,n). Det följer att

sgd(x,n) också delar vänstra sidan av utrycket, det vill säga att sgd(x,n) delar 1. Men största gemensamma delaren är alltid ett positivt tal, och 1 har endast delarna -1 och 1, alltså kan vi dra slutsatsen att sgd(x,n)=1.

Att visa att inversen är unik är uppgift B4.7 nedan. □

Exempel
Bestäm den multiplikativa inversen till [1753] i $\mathbf{Z}_{3571}$.
Lösning:
(a) Använd först Euklides algoritme för att visa att sgd(1753, 3571)=1:

3571 = 1753(2) + 65
1753 = 65(26) + 63
65 = 63(1) + 2
63 = 2(31) + 1
2 = 1(2) + 0

Så sgd(1753, 3571) = 1.

(b) Använd sedan Euklides algoritme baklänges för at hitta heltal s och t sådana att 1753s + 3571t=1:
1 = 63 + 2(-31)
= 63 + (65-63)(-31)
= 63(32) + 65(-31)
= (1753 - 65(26))(32) + 65(-31)
= 1753(32) + 65(-863)
= 1753(32) + (3571-1753(2))(-863)
= 1753(**1758**) + 3571(-863)

(c) Av beviset för Sats B4.8 fås då att [s] = [1758] är den multiplikativa inversen till [1753] i $\mathbf{Z}_{3571}$.

(d) Koll: (1753)(1758) = 3081774 = 1 + 3571(863), så [1753] $\odot$ [1758]= [1] i $\mathbf{Z}_{3571}$. □

Uppgift B4.4
Låt n=10. Bestäm alla tal $x \in \{0,1,2, \ldots ,9\}$ sådana att sgd(x,10) = 1. För vart och ett av dessa tal använd Euklides algoritm för att bestämma tal $a, b \in \mathbb{Z}$ sådana att 1=ax + b(10), och sedan $[y] \in \mathbf{Z}_{10}$ sådant att [x] $\odot$ [y]= [1].

Uppgift B4.5
Bestäm den multiplikativa inversen till
(a) [5] i $\mathbf{Z}_{12}$;
(b) [22] i $\mathbf{Z}_{31}$;
(c) [10] i $\mathbf{Z}_{23}$;
(d) [14] i $\mathbf{Z}_{25}$.

Uppgift B4.6
Visa för varje heltal $n \geq 2$ att om [x] är en nolldelare i $\mathbf{Z}_n$, så har [x] inte någon multiplikativ invers.

Uppgift B4.7
Visa m.h.a. Förkortningsregeln, att den multiplikativa inversen i Sats B4.8 är unik.

3. Ekvationer modulo n

I detta avsnitt skall vi lära oss bestämma alla möjliga lösningar $x \in \mathbb{Z}$ till kongruenser på formen

$$ax \equiv b \pmod{n}$$

och alla möjliga lösningar $[x] \in \mathbf{Z}_n$ till ekvationer

$$[a] \odot [x] = [b],$$

där a,b och n är heltal och $n \geq 2$.

Det är värt att notera att element $[x] \in \mathbf{Z}_n$, som uppfyller $[a] \odot [x] = [1]$, motsvarar element $x \in \{1, \ldots, n-1\}$, som löser kongruensen $ax \equiv 1 \pmod{n}$. Detta används mycket ofta i bevisen för satserna som följer.

Sats B4.9
Kongruensen $ax \equiv 1 \pmod{n}$ har lösningar $x \in \mathbb{Z}$ om och endast om sgd(a,n) = 1.
Det gäller ytterligare, att alla lösningar är kongruenta modulo n.

Bevis.
Om sgd(a,n) =1 så finns heltal s och t sådana att sa + tn = 1. Av beviset till sats B4.8 ser vi att lösningarna till kongruensen $ax \equiv 1 \pmod{n}$ är alla element x i klassen [s].
Om däremot $\text{sgd}(a,n) \neq 1$, så har kongruensen inga lösningar, för en lösning skulle betyda, att det existerar en multiplikativ invers till [a] i $\mathbf{Z}_n$, vilket är omöjligt enligt sats B4.8.□

Uppgift B4.8
Antag att a, b och n är heltal sådana att $n \geq 2$ och sgd(a,n) =1. Visa att om $ax \equiv 1 \pmod{n}$, så är $a(bx) \equiv b \pmod{n}$, dvs. visa att om y = x löser kongruensen $ay \equiv 1 \pmod{n}$, så löser bx kongruensen $ay \equiv b \pmod{n}$.

Uppgift B4.9
Använd din lösning till uppgift B4.5(a) för att bestämma en lösning till kongruensen $5x \equiv 1 \pmod{12}$ och bestäm sedan en lösning till kongruensen $5x \equiv 4 \pmod{12}$.

Om $\text{sgd}(a,n) \neq 1$, så har kongruensen $ax \equiv b \pmod{n}$ antingen ingen lösning eller också så löser alla tal i en eller flera kongruensklasser modulo n kongruensen. Följande sats talar om när det finns lösningar och vilka de i sådant fall är.

Sats B4.10
Låt a, b och n vara heltal sådana att $n \geq 2$ och sgd(a,n) =s.
Om $s \mid b$, så har ekvationen

$$[a] \odot [x] = [b]$$

s lösningar i $\mathbf{Z}_n$, nämligen

$$[x] = [(b/s)\, x_0 + t(n/s)],$$

där $t = 0, 1, \ldots, s-1$, och $x_0 \in \{0, 1, \ldots, (n/s) -1\}$ är en lösning till den reducerade kongruensen $(a/s)x \equiv 1 \pmod{(n/s)}$.
Om $s \nmid b$, så har ekvationen inga lösningar.

Bevis.
Om $[a]_n \odot [x]_n = [b]_n$ har en lösning $[x]_n \in \mathbf{Z}_n$, så har vi att $n \mid (ax-b)$, och genom att $s \mid n$ och $s \mid ax$, följer det att att $s \mid b$. Så om $s \nmid b$ kan det inte finnas någon lösning.

Antag nu att $s \mid b$.
Vid insättning ser man genast att om x_0 löser kongruensen $(a/s)x \equiv 1 \pmod{(n/s)}$, så är de s kongruensklasserna $[x]_n = [(b/s)x_0 + t(n/s)]_n$ där t = 0, 1, ..., s-1 lösningar till ekvationen

$$[a]_n \odot [x]_n = [b]_n. \qquad (*)$$

Vi behöver då bara visa två saker:
(i) Varje lösning till ekvationen (*) kan skrivas på formen $[x]_n = [(b/s)x_0 + t(n/s)]_n$ för något $t \in \mathbb{Z}$.
(ii) Ekvationen (*) har precis s lösningar.

För (i): Antag att $[x]_n$ är en lösning till (*). Det finns då ett heltal k sådant att ax=b+kn, och eftersom s | a, s | b och s | n, har vi vidare att

$$(a/s)x \equiv (b/s) \pmod{(n/s)}.$$

Detta betyder att i $\mathbf{Z}_{n/s}$ har vi likheten

$$[a/s] \odot [x] = [b/s]. \qquad (**)$$

Enligt sats B4.8 har [a/s] en entydigt bestämd multiplikativ invers $[x_0]$ i $\mathbf{Z}_{n/s}$. Om vi då multiplicerar med $[x_0]$ på båda sidor av likheten (**), får vi att i $\mathbf{Z}_{n/s}$ gäller det att

$$[x] = [(b/s)x_0].$$

Detta innebär att för något $t \in \mathbb{Z}$ är

$$x = (b/s)x_0 + t(n/s),$$

vilket är x skriven i den önskade formen.

För (ii): Det finns som mest s kongruensklasser $[(b/s)x_0 + r(n/s)]_n$, nämligen en för varje r = 0,1,2, ... , s-1, för om $r \notin \{0,1, \ldots, s-1\}$, så kan man med divisionsalgoritmen få fram ett $r_0 \in \{0,1, \ldots, s-1\}$ sådant att $r = qs + r_0$. Men $[(b/s)x_0 + r(n/s)]_n = [(b/s)x_0 + r_0(n/s)]_n$, så r_0 ger precis samma kongruensklass som r.

Det är också minst s kongruensklasser $[(b/s)x_0 + r(n/s)]_n$:
Antag att $[(b/s)x_0 + r(n/s)]_n = [(b/s)x_0 + t(n/s)]_n$, med $r, t \in \mathbb{Z}$ och $s-1 \geq t > r \geq 0$, då är

$$(t-r)(n/s) = zn, \text{ för något } z \in \mathbb{Z},$$

vilket strider mot att $0 < t-r < s$.
Det finns alltså precis s sådana kongruensklasser. □

Exempel
Bestäm alla lösningar i $\mathbf{Z}_7$ till ekvationen $[5] \odot [x] = [2]$.

Lösning:

1. sgd(5,7)=1.
   Det finns alltså precis 1 kongruensklass i $\mathbf{Z}_7$ som är lösning till ekvationen.

2. Den reducerade kongruensen är
   $$(5/1)x \equiv 2/1 \pmod{(7/1)},$$
   som i $\mathbf{Z}_{7/1}$ motsvaras av ekvationen
   $$[5/1] \odot [x] = [2/1].$$
   (Denna ekvationen var alltså redan reducerad!)

3. Bestäm nu den multiplikativa inversen till [5/1] i $\mathbf{Z}_7$ med Euklides algoritm:
   7=5(1) +2
   5=2(2)+1.
   Så 1 = 5 + 2(-2) = 5 + [7 - 5](-2) = 5(**3**) + 7(-2),
   och [3] är då den multiplikativa inversen till [5] i $\mathbf{Z}_7$.

4. Lösningen till den reducerade ekvationen fås nu genom att multiplicera ekvationen med multiplikativa inversen:
   $$[3] \odot [5] \odot [x] = [3] \odot [2].$$
   Men $[3] \odot [5] = [1]$, så detta ger
   $$[1] \odot [x] = [6],$$
   så [x] = [6] är lösningen till den reducerade ekvationen.

5. Eftersom ekvationen i detta exempel var samma som reducerade ekvationen är lösningen till ekvationen också [x] = [6].

(Lösningen till ekvationen fås i vanliga fall av Sats B4.10:
[x] = [(2/1)3 + t(7/1)] där t=0, så [x] = [6].) □

Exempel
Bestäm alla lösningar i $\mathbf{Z}_{14}$ till ekvationen $[10] \odot [x] = [4]$.

Lösning:

1. sgd(10,14)=2.
   Det finns alltså precis 2 kongruensklasser i $\mathbf{Z}_{14}$ som är lösning till ekvationen.

2. Den reducerade kongruensen är
   $$(10/2)x \equiv 4/2 \pmod{(14/2)},$$
   som i $\mathbf{Z}_7$ motsvaras av den reducerade ekvationen
   $$[5] \odot [x] = [2].$$

3. Bestäm nu den multiplikativa inversen till $[5]$ i $\mathbf{Z}_7$ med Euklides algoritm:
   7=5(1) +2
   5=2(2)+1.
   Så 1 = 5 + 2(-2) = 5 + [7 - 5](-2) = 5(**3**) + 7(-2),
   och [3] är då den multiplikativa inversen till $[5]$ i $\mathbf{Z}_7$.

4. Lösningen till den reducerade ekvationen fås nu genom att multiplicera ekvationen med multiplikativa inversen:
   $$[3] \odot [5] \odot [x] = [3] \odot [2].$$
   Men $[3] \odot [5] = [1]$, så detta ger
   $$[1] \odot [x] = [6],$$
   så [x] = [6] är lösningen till den reducerade ekvationen.

5. Lösningen till ekvationen fås nu av Sats B4.10, nämligen

   [x] = [6 + t(7)] där t=0, 1, så
   lösningen är [x] = [6] eller [13] i $\mathbf{Z}_{14}$. □

Exempel
Bestäm alla lösningar $x \in \mathbb{Z}$ till kongruensen $10x \equiv 4 \pmod{14}$.

Lösning:
Kongruensen motsvaras av ekvationen $[10] \odot [x] = [4]$ i $\mathbf{Z}_{14}$, så av exemplet ovan fås att lösningen är alla heltal i de två kongruensklasserna [6] och [13] i $\mathbf{Z}_{14}$. Dvs. att kongruensen har lösningarn

$$x = 14k+6 \text{ eller } 14k+13 = 7k+6, \text{ där } k \in \mathbb{Z}.$$

Uppgift B4.10
(a) Bestäm alla lösningar i $\mathbf{Z}_{12}$ till ekvationen $[10] \odot [x] = [6]$.
(b) Bestäm alla lösningar $x \in \mathbb{Z}$ till kongruensen $10x \equiv 6 \pmod{12}$.

Uppgift B4.11
(a) Bestäm den multiplikativa inversen till $[14]$ i $\mathbf{Z}_{37}$.
(b) Bestäm x_0 med $0 \leq x_0 \leq 36$ och $14x_0 \equiv 1 \pmod{37}$.
(c) Bestäm alla heltalslösningar x till kongruenserna
   (i) $42x \equiv 15 \pmod{111}$;
   (ii) $42x \equiv 25 \pmod{111}$.

4. Relationer

Vi skall nu studera relationer på mängder. I princip kan man säga att en relation på en mängd X, är ett sätt att beskriva ett samband mellan elementen i X.

Exempel
Låt M vara mängden av alla personer i världen, då kan vi definiera relationen R på M genom att låta person x vara relaterad till person y om och endast om x är född samma månad som y.

Om x är relaterad till y under relationen R skriver vi

$$xRy$$

Exempel
Låt M vara mängden av alla personer i världen, då kan vi definiera andra relationer på M. T.ex.

- xR_1y om och endast om x har samma kön som y.
- xR_2y om och endast om x är yngre än y.
- xR_3y om och endast om x är syster till y.
- xR_4y om och endast om x känner y.
- xR_5y om och endast om x förstår det språk som y talar.

Exempel
Låt $\mathbb{Z}$ vara mängden av heltalen, då är följande relationer på $\mathbb{Z}$:

- xR_1y om och endast om $x < y$.
- xR_2y om och endast om y är en faktor i x.
- xR_3y om och endast om $x \equiv y \pmod 5$.

Mer formellt, definierar vi en **relation** R på en mängd S att vara en delmängd till den kartesiska produkten $X \times X$. Det ordnade paret $(x,y) \in R$ om och endast om xRy.

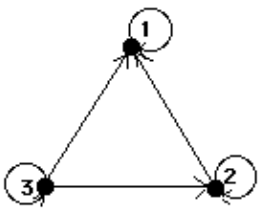
Exempel
Betrakta relationen R på S={1,2,3} definierad genom xRy om och endast om $x \geq y$.

Då har vi att 1R1, 2R1, 3R1, 2R2, 3R2 och 3R3 eftersom $1 \geq 1$, $2 \geq 1$, $3 \geq 1$, $2 \geq 2$, $3 \geq 2$ och $3 \geq 3$.

R kan också beskrivas som en delmängd av $S \times S$, nämligen

$$R=\{(1,1), (2,1), (3,1), (2,2), (3,2), (3,3)\}.$$

Man kan ochså rita en bild som beskriver relationen:



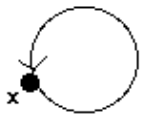
Detta kallas för **digrafen för relationen** $\geq$ på S={1,2,3}.

Nu skall du läsa [J] Kapitel 2.4 (2.4)[3.1] börja med Exempel 2.4.4 på s. 78 (93) [Exempel 3.1.4 på s. 118] fram till och med Exempel 2.4.21 på sida 81 - 82 (97 - 98) [Exempel 3.1.21 på s. 121].
En relations **digraf** beskrivas på sidan 78 (93) [118].

Vi kan klassificera relationer utifrån egenskaper. En relation R på X sägs vara

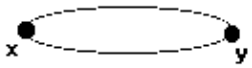
- **reflexiv** om för alla $x \in X$ det gäller att $(x,x) \in R$;
- **symmetrisk** om för alla $x, y \in X$ det gäller att om $(x,y) \in R$ så är även $(y,x) \in R$;
- **antisymmetrisk** om för alla $x, y \in X$ det gäller att om $(x,y) \in R$ och $x \neq y$ så är $(y,x) \notin R$;
- **transitiv** om för alla $x, y, z \in X$ det gäller att om $(x,y) \in R$ och $(y,z) \in R$ så är även $(x,z) \in R$.

Var och en av dessa egenskaper kan kontrolleras genom att studera relationens digraf:
Om relationen är reflexiv, finns det en loop vid varje hörn i digrafen.



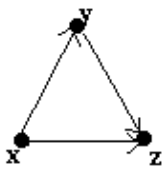
Notera att relationen $\geq$ på S={1,2,3} är reflexiv eftersom det finns en loop vid alla hörn 1, 2 and 3 i digrafen vi ritade ovan.

Om relationen är symmetrisk, så gäller att *om* det finns en pil från hörn x till hörn y i relationens digraf, så skall det också finnas en pil från y tillbaka till x.



Notera att relationen $\geq$ på S={1,2,3} *inte* är symmetrisk, eftersom det finns en pil från hörn 2 till hörn 1 i relationens digraf, men ingen pil från hörn 1 till hörn 2.

Om relationen är transitiv, gäller att om det går en pil mellan x och y i relationens digraf och en pil mellan y och z, så skall det finnas en pil mellan x och z.



Notera därmed att relationen $\geq$ på S={1,2,3} är transitiv.

Om relationen är anti-symmetrisk, gäller att om det finns en pil mellan x och y i relationens digraf, så skall det *inte* finnas någon pil från y tillbaka till x, såvida inte x=y. Notera därför att relationen $\geq$ på S={1,2,3} från ovan är antisymmetrisk.

Observera att för att kontrollera om någon av dessa egenskaper gäller för en relation, räcker det inte att kontrollera att egenskapen uppfylls för några speciella val av x, y och z, utan egenskapen måste gälla för alla möjliga val av x, y och z. Tag till exempel, relationen $\geq$ på S={1,2,3} från ovan, vi ser klart att det går en pil från x=1 till y=1, så naturligtvis går samma pil tillbaka från y=1 till x=1, men relationen är inte symmetrisk för det, eftersom vi upptäckte att det går en pil från hörn x=2 till hörn y=1, men det finns ingen pil från hörn y=1 tillbaka till hörn x=2.

Relationer på en mängd X kan användas vid försök att ordna elementen på rad. En **partialordning** på en mängd X är en relation på X som är reflexiv, antisymmetrisk och transitiv. Relationen $\geq$ på S={1,2,3} ovan är därför en partialordning. Av namnet finns en antydan om att man bara delvis (partiellt) lyckas ordna elementen på en rad med en partialordning och detta kan vara fallet. Två element i X behöver inte vara "jämförbara" med en partialordning.

En **fullständig ordning** på en mängd X är en partialordning i vilken varje par av element i X är jämförbara. Relationen $\geq$ on S={1,2,3} ovan är därför även en fullständig ordning. Ett annat namn på en fullständig ordning som också används är linjär ordning vilket belyser att elementen ordnas på linje med denna relation. Läs sidan 81 (97) [121] i [J] där begreppet jämförbar förklaras tillsammans med exempel på partialordningar. Läs nu avsnitt 2.5 (2.5) [3.2] i [J]. En relation R på en mängd X som är reflexiv, symmetrisk och transitiv kallas en **ekvivalensrelation**.

Exempel
Relationen R på $\mathbb{Z}$ definierad som (x,y)$\in$R om x$\equiv$ y (mod n) är en ekvivalensrelation (Kontrollera detta! Dvs. kontrollera att R är reflexiv, symmetrisk och transitiv).

Tidigare såg vi att tal som är kongruenta bildar kongruensklasser och att mängden av kongruensklasser är en partition av $\mathbb{Z}$. Mer allmänt bildar element i X som är ekvivalenta (d.v.s. de element som är relaterade med ekvivalensrelationen R) **ekvivalensklasser** och mängden av dessa ekvivalensklasser är en partition av X. Detta är innehållet i sats 2.5.9 (2.5.9) [3.2.8] på sidan 87 (106) [127] i [J].

Exempel
Låt oss definiera en relation R på $\mathbb{Z}$ genom (x,y) $\in$ R om $x^2=y^2$. Våra uppgifter är (a) att visa att R är en ekvivalensrelation och (b) att beskriva ekvivalensklasserna.

För (a): För alla heltal x så gäller att $x^2 = x^2$ och (x,x) $\in$ R så R är reflexiv.
Antag att x och y är heltal och (x,y) $\in$ R. Att paret tillhör R betyder att $x^2 = y^2$. Detta är detsamma som att $y^2 = x^2$ vilket betyder att (y,x) $\in$ R. Talen x och y valdes godtyckligt med egenskapen att (x,y) $\in$ R så vi kan dra slutsatsen att R är symmetrisk.
Om x, y och z är heltal sådana att $x^2 = y^2$ och $y^2 = z^2$ så innebär det att $x^2 = z^2$. Detta uttalande är precis det samma som att säga att relation R är transitiv.

För (b): Ekvivalensklassen med elementet n$\in\mathbb{Z}$ är
[n]={x$\in\mathbb{Z}$ | (x,n) $\in$ R} = {x$\in\mathbb{Z}$ | $x^2 = n^2$} = {x$\in\mathbb{Z}$ | (x+n)(x-n) = 0} = {n, -n}.
Den sista likheten av det faktum att produkten (x+n)(x-n) är 0 precis då faktorn (x+n) eller (x-n) är 0. Partitionen av $\mathbb{Z}$ med ekvivalensklasserna till denna ekvivalensrelation R blir alltså {{0}, {-1,1}, {-2,2}, {-3,3}, {-4,4}, ...}.

5. Funktioner

Fram till nu har vi bara studerat relationer på én mängd. Det är också möjligt att definiera en relation som beskriver sammanhang mellan element som tillhör två olika mängder X och Y. Minns att en relation på en mängd formellt definierades som en delmängd till den kartesiska produkten X × X. På samma sätt kommer en relation från en mängd X till en mängd Y att vara en delmängd till den kartesiska produkten X × Y. Läs nu Kapitel 2.4 (2.4) [3.1] i [J] fram till Exempel 2.4.4 (2.4.4) [3.1.4], som beskriver relationer mellan två mängder istället för relationer på én mängd.

Läs nu avsnitt 2.8 2.8 [2.2] i [J].

En **funktion** f från X till Y är en relation från X till Y med egenskaperna att

1. **definitionsmängden** (engelska: domain) är hela X,
2. om $(x,y) \in f$ och $(x,z) \in f$ så är $y = z$.

Y är funktionens **bildmängd** (engelska: codomain). Egenskaperna tillåter oss att prata om värdet $y \in Y$ av funktionen i $x \in X$. Det vill säga att varje $x \in X$ återfinns som förstakoordinat i precis ett ordnat par i relationen. Vanligt är att skriva $y = f(x)$ istället för $(x,y) \in f$ för att ytterliggare illustrera att funktionen f har värdet y i x. Man kan tänka på en funktion f från X till Y som en maskin som har "x-värden" som indata och "y-värden" som utdata. För varje indatavärde kastar maskinen ut precis ett utdatavärde. Mängden av alla utdatavärden kallas för funktionens **värdemängd** (engelska: range).

Exempel
Med X={1, 2, 3} och Y={a, b, c} är

$$f = \{(1,a), (2,b), (3,b)\}$$

en funktion från definitionsmängden X till bildmängden Y, f:s värdemängd är {a, b}.

Däremot är inte $g = \{(1,a), (2,b), (3,b), (3,c)\}$ en funktion från X till Y. Relationen g har som definitionsmängd hela X men andra egenskapen ovan är inte uppfylld eftersom båda $(3,b) \in g$ och $(3,c) \in g$.

Exempel
Regeln att till varje reellt tal multiplicera detta med 5 och sedan addera 2 kan ses som en funktion f från $\mathbb{R}$ till $\mathbb{R}$ definierad med $y = f(x) = 5x + 2$. Istället för att ge sig på att rita denna relations digraf kan man som illustration ange denna funktions graf i det kartesiska koordinatsystemet av $\mathbb{R}$ och $\mathbb{R}$. Denna uppgift skulle också kunna formuleras som "rita funktionen y = 5x+2 i xy-planet" där namnet på funktionen har uteslutits och där det är underförstått att xy-planet är det kartesiska koordinatplanet av $\mathbb{R}$ och $\mathbb{R}$.

I avsnitt 2.8 (2.8) [2.2] i [J] finns en ny definition 2.8.9 (2.8.6) [2.2.10] med namnet *mod* inblandat. För naturliga tal x och y med $y > 0$ så är x mod y resten vid heltalsdivision av x med y. Varje värde på y ger upphov till en funktion.

Exempel
Med y=7 ser funktionen ut som f(x) = x mod 7. I exempel 2.8.11 (2.8.8) [2.2.12] i [J] används denna funktion till att räkna ut vilken veckodag det är 365 dagar från onsdag.

Exempel 2.8.12 (2.8.9) [2.2.13] om ISBN kod och 2.8.13 (2.8.10) [2.2.14] i [J] är andra goda exempel på hur funktioner av detta slag kan användas.

Golv och tak funktionerna

Håller du med om att antalet heltal *i* sådana att $10 \leq i \leq 20$ är 11? Mer allmänt, med m och n heltal, finns det m+n-1 stycken heltal *i* sådana att $m \leq i \leq n$. Men hur många jämna heltal i sådana att $m \leq i \leq n$ finns det? Om vi låter f vara golvfunktionen, definierad i 2.8.15 (2.8.11) [2.2.16], så är antalet jämna heltal mellan m och n precis f(n/2) - f((m-1)/2) stycken. Kontrollera att detta stämmer för några specifika värden på n och m och försök sedan resonera dig fram till varför detta är allmänt sant.

Begreppen injektiv och surjektiv

Att räkna de femton kakorna på ett brödfat är detsamma som att definiera en funktion f från mängden {1, 2, 3,...,15} till mängden {x | x är en kaka på brödfatet} som är injektiv (varje kaka räknas bara en gång) och surjektiv (varje kaka räknas). Även om detta exempel illustrerar betydelsen av orden injektiv och surjektiv kan detta exempel kanske missförstås. Definitionen av begreppen "ett till ett" eller injektiv och "på" eller surjektiv för en funktion hittar man på sidan 107 (129) [92 och 94]. En funktion som är både injektiv och surjektiv sägs vara **bijektiv**.

I avsnitt 2.4 (2.4) [3.1] nämns att varje relation från X till Y har en invers relation från Y till X. Är det så att varje funktion från X till Y har en invers relation som också är en funktion (som kallas en invers funktion till funktionen)? Följande sats ger svar på den frågan.

Sats B4.11
En funktion f från X till Y har en invers funktion g om och endast om f är bijektiv.

Bevis.
Antag först att f har en invers funktion g från Y till X, dvs. g är en *funktion* sådan att om $(x,y) \in f$, så är $(y,x) \in g$.
Vi måste bevisa att f är bijektiv, dvs. att
(i) f är injektiv; och
(ii) f är surjektiv.

För (i): Om $f(a) = f(b)$ för ett godtyckligt par element a och b i X, så är $(f(b),b) \in g$ och $(f(a),a) \in g$. Eftersom $f(a)=f(b)$ har vi då att $(f(a),b) \in g$ och $(f(a),a) \in g$, men g är en funktion så av detta följer att a=b. Dvs. f är injektiv.
För (ii): Låt $y \in Y$ vara godtyckligt vald. Funktionen g har definitionsmängden Y, så det existerar ett element $g(y) \in X$ sådant att $(y,g(y)) \in g$. Av att g också är invers relation till f får vi att $(g(y),y) \in f$ och vi ser att y finns i värdemängden till f. Så f är surjektiv.

Antag nu att f är bijektiv. Definiera en relation g från Y till X sådan att om $(x,y) \in f$, så är $(y,x) \in g$. Vi måste bevisa att g är en funktion:
Funktionen f är surjektiv så för varje $y \in Y$ finns det ett $x \in X$ sådant att $(x,y) \in f$. För relationen g betyder detta att för varje $y \in Y$ finns ett $x \in X$ sådant att $(y,x) \in g$. Dvs. definitionsmängden till g är hela Y.
Antag att för något $y \in Y$ är $(y,x_1) \in g$ och $(y,x_2) \in g$ för ett godtyckligt par element x_1 och x_2. För relationen f betyder detta att $(x_1,y) \in f$ och $(x_2,y) \in f$, men av att f är injektiv följer då att $x_1 = x_2$. Elementen $y \in Y$ och $x_1, x_2 \in X$ valdes godtyckligt så g uppfyller alltså också andra egenskapen i definitionen för en funktion. □

6. Förslag till övningsuppgifter

Uppgifterna i texten ovan.

Övningsuppgifter från [J]:

[J] sida 83-84:
Uppg. 4, 7, 9, 12, 13, 14, 16, 19, 29, 32, 34, 38, 41.
(sida 99-101: 4, 7, 9, 12, 13, 14, 16, 19, 29, 32, 34, 38, 41.)
[sida 123-124: 4, 7, 9, 12, 13, 14, 16, 19, 29, 32, 35, 39, 42.]

[J] sida 89-90:
Uppg. 1, 4, 7, 9, 12, 15, 18, 24, 27, 30(b).
(sida 108-110: 1, 4, 7, finns ej, finns ej, 9, 12, 18, 21, 24(b))
[sida 129-130: 1, 4, 7, 9, 12, 15, 18, 24, 27, 30(b).]

[J] sida 111-114:
Uppg. 1, 4, 6, 16, 17, 18, 25, 37(a), 38, 39, 89.
(sida 131-136: 1, 4, finns ej, 6, 7, 8, 9, 12(a), 13, 14, 64)
[sida 99-101: 1, 4, 6, 16, 17, 18, 25, 37(a), 38, 39, 78.]

This is the 3rd Edition of the study guide for Block 4 of Algebra and Discrete Mathematics most of which was written by Pia Heidtmann and Andreas Brodin in 2000 and revised in 2002. It was translated in part from Danish and English to the Swedish by Sam Lodin.

The authors welcome comments and corrections via email. All contributions incorporated in updates of the manuscript will be acknowledged.

The author would like to thank the following for their contribution to various updates of the original manuscript:
Sam Lodin, Katharina Huber and Fredrik Engström.

Current lecturers:
Pia Heidtmann, Sam Lodin.

MID SWEDEN UNIVERSITY
Department of Engineering, Physics and Mathematics
Mid Sweden University
S-851 70 SUNDSVALL
Sweden

Updated 070811