Mittuniversitetet
MID SWEDEN UNIVERSITY

MA014G
Algebra och Diskret Matematik A
Svar på uppgifter till Block 4

Referenser utan parenteser är till [J] edition 5, referenser i ()-parenteser är till [J] edition 4, och referenser i []-parenteser är till [J] edition 6.

Uppgifter i läsanvisningen

Uppgift B4.1

1. Sant, 81 - 1 = 80 = 8(10)
2. Sant, 81 - 1 = 8(10)
3. Falskt, 112 - 4 = 108 ≠ k(11) för varje heltal k
4. Sant, 1000 - (-1) = 1001 = 13(77)
5. Falskt, 9 - 90 = -81 ≠ k(5) för alla heltal k.
6. Sant 937-37=900=9(100).
7. Falskt, Med t.ex. a=937, b=37 och m=100 har vi 937≡37 (mod 100) men 937 = 37 är falskt.
8. Sant, Om a≡b (mod m), så finns ett heltal k så att a-b=km. Addera och subtrahera c till vänster led: a+c-(b+c)=km, d.v.s. a+c≡b+c (mod m).
9. Sant. Om a≡b (mod m), så finns ett heltal k så att a-b=km. Multiplicera båda sidor med c: ac-bc=kmc=(kc)m, d.v.s. ac≡bc (mod m).

Uppgift B4.2

$\{x \mid x \equiv 3 \pmod 5\} = \{x \mid x-3 = k(5), k \in \mathbb{Z}\} = \{..., -12, -7, -2, 3, 8, 13, 18, ...\}$.

Uppgift B4.3

Multiplikationstabellen för $\mathbf{Z}_2$ är:

⊙	*[0]*	*[1]*
[0]	[0]	[0]
[1]	[0]	[1]

Multiplikationstabellen för $\mathbf{Z}_3$ är:

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

Multiplikationstabellen för $\mathbf{Z}_6$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*
[0]	[0]	[0]	*[0]*	*[0]*	*[0]*	*[0]*
[1]	[0]	[1]	*[2]*	*[3]*	*[4]*	*[5]*
[2]	[0]	[2]	*[4]*	*[0]*	*[2]*	*[4]*
[3]	[0]	[3]	*[0]*	*[3]*	*[0]*	*[3]*

[4]	[0]	[4]	*[2]*	*[0]*	*[4]*	*[2]*
[5]	[0]	[5]	*[4]*	*[3]*	*[2]*	*[1]*

Multiplikationstabellen för $\mathbf{Z}_7$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Multiplikationstabellen för $\mathbf{Z}_8$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*	*[7]*
[0]	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*
[1]	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*	*[7]*
[2]	*[0]*	*[2]*	*[4]*	*[6]*	*[0]*	*[2]*	*[4]*	*[6]*
[3]	*[0]*	*[3]*	*[6]*	*[1]*	*[4]*	*[7]*	*[2]*	*[5]*
[4]	*[0]*	*[4]*	*[0]*	*[4]*	*[0]*	*[4]*	*[0]*	*[4]*
[5]	*[0]*	*[5]*	*[2]*	*[7]*	*[4]*	*[1]*	*[6]*	*[3]*
[6]	*[0]*	*[6]*	*[4]*	*[2]*	*[0]*	*[6]*	*[4]*	*[2]*
[7]	*[0]*	*[7]*	*[6]*	*[5]*	*[4]*	*[3]*	*[2]*	*[1]*

Multiplikationstabellen för $\mathbf{Z}_9$ är:

⊙	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*	*[7]*	*[8]*
[0]	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*
[1]	[0]	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*	*[7]*	*[8]*
[2]	[0]	*[2]*	*[4]*	*[6]*	*[8]*	*[1]*	*[3]*	*[5]*	*[7]*
[3]	[0]	*[3]*	*[6]*	*[0]*	*[3]*	*[6]*	*[0]*	*[3]*	*[6]*
[4]	[0]	*[4]*	*[8]*	*[3]*	*[7]*	*[2]*	*[6]*	*[1]*	*[5]*
[5]	[0]	*[5]*	*[1]*	*[6]*	*[2]*	*[7]*	*[3]*	*[8]*	*[4]*
[6]	[0]	*[6]*	*[3]*	*[0]*	*[6]*	*[3]*	*[0]*	*[6]*	*[3]*
[7]	[0]	*[7]*	*[5]*	*[3]*	*[1]*	*[8]*	*[6]*	*[4]*	*[2]*
[8]	[0]	*[8]*	*[7]*	*[6]*	*[5]*	*[4]*	*[3]*	*[2]*	*[1]*

Lagen om nolldelare är giltig i $\mathbf{Z}_2$, $\mathbf{Z}_3$ och $\mathbf{Z}_7$, men inte i $\mathbf{Z}_6$, $\mathbf{Z}_8$ eller $\mathbf{Z}_9$.

Uppgift B4.4

De tal $x \in \{0, 1, 2, \ldots , 9\}$ sådana att sgd(x,10) = 1 är 1, 3, 7 och 9.
a och b kan t.ex. väljas enligt 1=(-9)1+(1)10,
1=(-3)3+(1)10,
1=(3)7+(-2)10 och
1=(-1)9+(1)10.

[-9]=[1] så [1] ⊙ [1]= [1].
[-3]=[7] så [3] ⊙ [7]= [1].

Med 1=(3)7+(-2)10 ser vi direkt att [3] ⊙ [7]= [1].
[-1]=[9] så [9] ⊙ [9]= [1].

Uppgift B4.5

(a) Med Euklides algoritm:
12=2(5)+2.
5=2(2)+1, så
1=5-2(2)=5-(12-2(5))(2)=5(5)-2(12).
Det innebär att [5]⊙[5]=[1] och den multiplikativa inversen till [5] är [5] i $\mathbf{Z}_{12}$.
(b) Använd Euklides algoritm:
31=22(1)+9.
22=9(2)+4.
9=4(2)+1 så
1=9-4(2)=9-(22-9(2))(2)=(5)9-(2)22=(5)(31-22)-(2)22=(5)31+(-7)22.

[-7]=[24] så inversen till [22] i $\mathbf{Z}_{31}$ är [24].
(c) Inversen är [7].
(d) Inversen är [9].

Uppgift B4.6

Antag att [x] har en multiplikativ invers [z]. [x] är nolldelare så det finns [y] ≠[0] så att [x]⊙[y]=[0]. Multiplicera båda sidor med inversen [z] till [x]; [z]⊙[x] ⊙[y]=[z]⊙[0]=[0]. [z]⊙[x]=[1] så vi får att [y]=[0]. Det är en motsägelse. Alltså kan inte [x] ha någon invers.

Uppgift B4.7

Antag att det finns två inverser [y] och [z] till [x]. Att de är inverser till [x] innebär att [x]⊙[y]=[1]=[x]⊙[z] och multiplicerar vi denna likhet med [y] från vänster får vi att [y]⊙[x] ⊙[y]= [y]⊙[x] ⊙[z]. [y] är invers till [x] så [y]⊙[x]=[1] så likheten tidigare är [1] ⊙[y]= [1]⊙[z] ur vilken det följer att [y]=[z]. D.v.s. inversen måste vara unik.

Uppgift B4.8

Att $ax \equiv 1 \pmod{n}$ innebär att det finns ett heltal k så att ax-1=kn. Multipliceras båda sidor om likhetstecknet med b får vi att abx-b=bkn. Produkten bk är ett heltal så $a(bx) \equiv b \pmod{n}$.

Uppgift B4.9

Med uppgift B4.5(a) får vi att x=5 är en lösning till kongruensen $5x \equiv 1 \pmod{12}$. Enligt uppgift B4.8 är då x=5(4)=20 en lösning till kongruensen $5x \equiv 4 \pmod{12}$.

Uppgift B4.10

(a) Använd sats B4.9 med a=10, n=12 och b=6.
sgd(10,12)=2 och 2|6 så satsen säger att det finns två lösningar i $\mathbf{Z}_{12}$ och de ges av [x]=[$3x_0$+t6] med t=0,1 och där $x_0 \in$ {0,1,2,3,4,5} är en lösning till $5x \equiv 1 \pmod 6$. x_0=5 fungerar. Med t=0 fås [15] och med t=1 fås [21]. D.v.s. [3] och [9] är lösningarna till [10] ⊙ [x] = [6] i $\mathbf{Z}_{12}$.
(b) Talet $x \in \mathbb{Z}$ är en lösning till kongruensen $10x \equiv 6 \pmod{12}$ om och endast om [10] ⊙ [x] = [6] i $\mathbf{Z}_{12}$ (Varför?). Ur deluppgift a) får vi då att x är en lösning om och endast om x finns i en av kongruensklasserna $[3]_{12}$ eller $[9]_{12}$.

Uppgift B4.11

(a) Använd Euklides algoritm:
37=2(14)+9.
14=1(9)+5.
9=2(5)-1 så

1=2(5)-9=2(14-9)-9=2(14)-3(9)=2(14)-3(37-2(14))=8(14)-3(37).
Inversen till [14] i $\mathbf{Z}_{37}$ är alltså [8].

(b) Med deluppgift (a) kan man komma fram till att $x_0=8$ (varför?).

(c) (i) Observera först att ett heltal x löser kongruensen

$$42x \equiv 15 \pmod{111}$$

om och endast om det löser kongruensen

$$14x \equiv 5 \pmod{37}.$$

(Om x är ett tal sådant att $42x \equiv 15 \pmod{111}$ så finns ett k så att 42x-15=111k. Delar vi båda leden med 3 så blir resultatet likheten 14x-5=37k vilket betyder att $14x \equiv 5 \pmod{37}$. Andra riktningen: om x är ett tal sådant att $14x \equiv 5 \pmod{37}$ så finns ett k så att 14x-5=37k. Multipliceras båda sidor med 3 så har vi att 42x-15=111k vilket innebär att $42x \equiv 15 \pmod{111}$.)

Använd sats B4.10 med a=14, b=5 och n=37:
sgd(14,37)=1 och 1|5 så $[14]\odot[x]=[5]$ har én lösning i $\mathbf{Z}_{37}$. Denna ges av sats B4.10 också, men vi kan hitta den utan:
Vi har

$$[14]\odot[x]=[5].$$

Multiplicera båda sidor med [8] (multiplikativa inversen till [14] enligt (a)), dvs.

$$[8] \odot [14] \odot [x] = [8] \odot [5],$$

varav fås att

$$[1] \odot [x] = [40],$$

och sedan

$$[x] = [3],$$

så [x]=[3] är lösningen till $[14]\odot[x]=[5]$.
Talet x löser då kongruensen $42x \equiv 15 \pmod{111}$ om och endast om $x \in [3]_{37} = \{...,-34, 3, 40, 77, ...\}$.

Observera att $[3]_{37} = [3]_{111} \cup [40]_{111} \cup [77]_{111}$, högersidan är lösningen som ges av sats B4.10.

(ii) sgd(111,42)=3 och 3 delar inte 25 så ekvationen $[42]\odot[x]=[25]$ har enligt sats B4.10 ingen lösning i $\mathbf{Z}_{111}$. Det innebär att det inte finns något heltal x som löser kongruensen $42x \equiv 25 \pmod{111}$.

The author would like to thank the following for their contribution to various updates of the original manuscript:
Pia Heidtmann.

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

Updated 070811