Lösningar till övningar i kapitel 6

6.1.1 Hitta mult. invers av $\overline{p}$ i $\mathbb{Z}_q$ och $\overline{q}$ i $\mathbb{Z}_p$

$p=11, q=13$:

$13 = 1\cdot 11 + 2$

$11 = 2\cdot 5 + 1 \Rightarrow$

$1 = 11 - 2\cdot 5 = 11 - (13 - 1\cdot 11)\cdot 5 \Rightarrow$

$1 = 6\cdot 11 - 5\cdot 13$

Så $1 = 6\cdot 11 - 5\cdot 13 \Rightarrow$

$\overline{11}^{-1} = \overline{6}$ i $\mathbb{Z}_{13}$ respektive

$\overline{13}^{-1} = \overline{-5} = \overline{6}$ i $\mathbb{Z}_{11}$

(Det är verkligen en slump att det blir $\overline{6}$ i båda.)

$p=11, q=17$:

$17 = 1\cdot 11 + 6$

$11 = 1\cdot 6 + 5$

$6 = 1\cdot 5 + 1 \Rightarrow$

$1 = 6 - 1\cdot 5 = 6 - 1\cdot(11 - 1\cdot 6) =$

$= 6 - 1\cdot 11 + 1\cdot 6 = 2\cdot 6 - 1\cdot 11 =$

$= 2\cdot(17 - 1\cdot 11) - 1\cdot 11 =$

$2\cdot 17 - 3\cdot 11$

$\Rightarrow 2\cdot 17 - 3\cdot 11 = 1 \Rightarrow$

$\overline{17}^{-1} = \overline{2}$ i $\mathbb{Z}_{11}$ respektive

$\overline{11}^{-1} = \overline{-3} = \overline{14}$ i $\mathbb{Z}_{17}$

$p,q = 23,29$ resp $p,q = 23,37$, lösning saknas men är exakt analog med ovanstående

6.1.2 $p = 11$, $q = 13$

Sök $\overline{p+q}^{-1}$ i $\mathbb{Z}_q$: $p+q = 24$; $q = 13$

$24 = 1 \cdot 13 + 11$

$13 = 1 \cdot 11 + 2$ } Härifrån är räkningarna exakt

$11 = 5 \cdot 2 + 1$ } överensstämmande med de för

... $p = 11$ & $q = 13$, så

$$\overline{p+q}^{-1} = \overline{24}^{-1} = \overline{6}$$

På samma sätt bottnar $\overline{p+2\cdot q}^{-1} = \overline{37}^{-1}$ i räkningarna kring $\overline{p}^{-1}$. Och även $\overline{p+10\cdot q}^{-1}$. Allmänt: Om vi söker $\overline{p+n\cdot q}^{-1}$ i $\mathbb{Z}_q$ så måste den vara $\overline{p}^{-1}$ eftersom om s som uppfyller $\overline{s} = \overline{p}^{-1}$ uppfyller $s \cdot p \equiv 1 \pmod q$ så gäller förstås även $s \cdot (p+n\cdot q) \equiv 1 \pmod q$. Det betyder precis

$$\overline{p}^{-1} = \overline{s} = \overline{p+n\,q}^{-1}$$

6.2.1 $\mathbb{Z}_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$

$\bar{0}\cdot\bar{0} = \bar{0}$: $\bar{0}$ är inte sin egen invers (självklart)

$\bar{1}\cdot\bar{1} = \bar{1}$; $\bar{1}$ är sin egen mult. invers (självklart)

$\bar{2}\cdot\bar{2} = \overline{2\cdot 2} = \bar{4} \neq \bar{1}$ alltså är $\bar{2}$ inte sin egen mult. inv.

$\bar{3}\cdot\bar{3} = \overline{3\cdot 3} = \bar{9} = \bar{0} \neq \bar{1}$ (inte)

$\bar{4}\cdot\bar{4} = \overline{16} = \bar{7} \neq \bar{1}$ (inte)

$\bar{5}\cdot\bar{5} = \overline{25} = \bar{7} \neq \bar{1}$ (inte)

$\bar{6}\cdot\bar{6} = \overline{36} = \bar{0} \neq \bar{1}$ (inte)

$\bar{7}\cdot\bar{7} = \overline{49} = \bar{4} \neq \bar{1}$ (inte)

$\bar{8}\cdot\bar{8} = \overline{64} = \bar{1}$. är sin egen mult. invers.

Bara $\bar{1}$ och $\bar{8}$ är sina egna multiplikativa inverser, eftersom $\bar{3}\cdot\bar{3} = \bar{0}$ och $\bar{6}\cdot\bar{6} = \bar{0}$ så kan inte $\bar{3}$ eller $\bar{6}$ ha multiplikativa inverser då skulle tex $\underbrace{\bar{3}^{-1}\cdot\bar{3}}_{\bar{1}}\cdot\bar{3} = \bar{3}^{-1}\cdot\bar{0} \Rightarrow \bar{1}\cdot\bar{3} = \bar{0} \Rightarrow \bar{3} = \bar{0}$ som är en motsägelse. Å andra sidan har $\bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}$ multiplikativa inverser eftersom talen 2, 4, 5, 7, 8 är relativt prima 9 så att vi alltid har lösningar till $x\cdot 2 + y\cdot 9 = 1$, $x\cdot 4 + y\cdot 9 = 1$, $x\cdot 5 + y\cdot 9 = 1$, $x\cdot 7 + y\cdot 9 = 1$, $x\cdot 8 + y\cdot 9 = 1$.

(Och hur var det med $\bar{1}$ hade den en multiplikativ invers?)

6.2.2 $a^2b^2 = (ab)^2 = \bar{1}^2 = \bar{1} \Rightarrow a^2$ och b^2 är multiplikativa inverser till varandra.

$ab^2 \cdot a = a^2b^2 = (ab)^2 = \bar{1}^2 = \bar{1} \Rightarrow ab^2$ och a är multiplikativa inverser till varandra.

6.2.3 I $\mathbb{Z}_7$ har alla element multiplikativa inverser så vi kan räkna som vanligt med de fyra räknesätten:

$$\begin{cases} \bar{2}\cdot x + \bar{3}y = \bar{2} \\ \bar{3}x + \bar{2}y = \bar{5} \end{cases} \overset{(-1)}{\Leftrightarrow} \begin{cases} \bar{2}\cdot x + \bar{3}\cdot y = \bar{2} \\ \bar{1}\cdot x - \bar{1}\cdot y = \bar{3} \end{cases} \overset{(-2)}{\Leftrightarrow}$$

$$\begin{cases} (\bar{3}+\bar{2})y = \overline{-4} = \bar{3} \\ \bar{1}\cdot x - \bar{1}\cdot y = \bar{3} \end{cases} \Leftrightarrow \begin{cases} x - y = \bar{3} \\ \bar{5}\cdot y = \bar{3} \end{cases}$$

$\bar{5}^{-1} = \bar{3}$ så detta ger $\bar{5}^{-1}\cdot\bar{5}\cdot y = \bar{5}^{-1}\cdot\bar{3} \Leftrightarrow$

$\bar{1}\cdot y = \bar{3}\cdot\bar{3} \Leftrightarrow y = \bar{9} = \bar{2} \Leftrightarrow$

$$\begin{cases} x = \bar{3} + y = \bar{5} \\ y = \bar{2} \end{cases}$$

Svar: $\begin{cases} y = \bar{5} \\ y = \bar{2} \end{cases}$

Kontroll

$$\begin{cases} \bar{2}\cdot\bar{5} + \bar{3}\cdot\bar{2} = \bar{10} + \bar{6} = \bar{16} = \overline{16-14} = \bar{2} \text{ ok!} \\ \bar{3}\cdot\bar{5} + \bar{2}\cdot\bar{2} = \bar{15} + \bar{4} = \bar{19} = \overline{14+5} = \bar{5} \text{ ok!} \end{cases}$$

6.2.4 Löses på samma sätt som förra uppgiften. Det kan vara bra att veta att i $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ gäller $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$ respektive $\bar{4}^{-1} = 4$.

6.5.1 Visa med matematisk induktion att

$$\forall n \geq 1: \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Bevis: I.f.s. predikatet $A(n) \Leftrightarrow \underbrace{\sum_{k=1}^{n} k}_{VL_n} = \underbrace{\frac{n(n+1)}{2}}_{HL_n}$

Steg 1: Kontrollera att $A(1)$ är sann, dvs att $VL_1 = HL_1$:

$$VL_1 = \sum_{k=1}^{1} k = 1 \qquad HL_1 = \frac{1\cdot(1+1)}{2} = \frac{1\cdot 2}{2} = 1$$

$VL_1 = HL_1$, dvs $A(1)$ gäller.

Steg 2: Visa nu att implikationen

$A(p) \Rightarrow A(p+1)$ gäller för alla $p \geq 1$.

Anlag alltså $A(p)$, dvs $VL_p = \sum_{k=1}^{p} k = \frac{p(p+1)}{2} = HL_p$ och visa med kraft av detta att $A(p+1)$ dvs $VL_{p+1} = HL_{p+1}$ gäller.

Här används $VL_p = HL_p$

$$VL_{p+1} = \sum_{k=1}^{p+1} k = \left(\sum_{k=1}^{p} k\right) + (p+1) \overset{\downarrow}{=} \frac{p(p+1)}{2} + (p+1) = \ldots$$

forts ⇒

6.5.1 (forts)

$$\ldots = \frac{p(p+1)}{2} + \frac{2(p+1)}{2} = \frac{(p+2)(p+1)}{2} = \frac{(p+1)(p+2)}{2}$$

$$HL_{p+1} = \frac{(p+1)\cdot\left((p+1)+1\right)}{2} = \frac{(p+1)(p+2)}{2}$$

Uppenbarligen gäller $VL_{p+1} = HL_{p+1}$ som följd av $VL_p = HL_p$, detta innebär precis $A(p) \Rightarrow A(p+1)$ vilket fullbordar steg 2.

Steg 3.: Steg 1 & Steg 2 och induktionsaxiomet fullbordar beviset.

6.5.2 $\forall n \geq 0: 3 \mid 2^{2n} - 1$. Vi kan skriva om 2^{2n} som 4^n. Visa alltså, med induktion, $\forall n \geq 0: A(n)$, där $A(n) \Leftrightarrow 3 \mid 4^n - 1$.

Bevis:

Steg 1: Kontrollera att $A(0)$ är sann dvs att $3 \mid 4^0 - 1$.

Men eftersom $4^0 - 1 = 1 - 1 = 0$ gäller $A(0) \Leftrightarrow 3 \mid 0$ vilket är sant eftersom 0 är delbart med 3.

Steg 2: Vi ska nu visa implikationen $A(p) \Rightarrow A(p+1)$ för alla $p \geq 0$ så vi antar att $A(p) \Leftrightarrow 3 \mid 4^p - 1$ för godtyckligt $p \geq 0$.

forts ↗

6.5.2 (forts) Med stöd av $3 \mid 4^p - 1$ ska vi visa att även $A(p+1) \Leftrightarrow 3 \mid 4^{p+1} - 1$ gäller. Vi har

$$4^{p+1} - 1 = 4 \cdot 4^p - 1 = \underbrace{3 \cdot 4^p}_{tal_1} + \underbrace{4^p - 1}_{tal_2} = tal_1 + tal_2$$

$tal_1 = 3 \cdot 4^p$ är uppenbart delbart med 3. $tal_2 = 4^p - 1$ är delbart med 3 tack vare induktions-antagandet. Alltså blir summan $tal_1 + tal_2 = 4^{p+1} - 1$ delbar med 3, men detta är precis $3 \mid 4^{p+1} - 1$ varför vi dvar slutsatsen $A(p) \Rightarrow A(p+1)$ och steg 2 är klart.

steg 3: steg 1 & steg 2 och induktionsaxiomet fullbordar beviset.

6.5.3 Visa $\forall n \geq 1: n < 2^n$

Bevis: Inför $A(n) \Leftrightarrow VL_n < HL_n \Leftrightarrow n < 2^n$. Visa $\forall n \geq 1: A(n)$, med matematisk induktion.

steg (1) kontrollera att $A(1)$ stämmer, dvs visa att $VL_1 < HL_1$

$VL_1 = 1 \qquad HL_1 = 2^1 = 2$

Helt klart gäller $VL_1 < HL_1$ dvs $A(1)$ gäller

forts ↗

6.5.3 (forts)

Steg 2: Visa nu att $A(p) \Rightarrow A(p+1)$ för alla $p \geq 1$. Anteg därför att $A(p) \Leftrightarrow VL_p < HL_p$ gäller för ett godt. $p \geq 1$. Det betyder att $p < 2^p$. Visa med stöd av detta att $A(p+1) \Leftrightarrow VL_{p+1} < HL_{p+1} \Leftrightarrow p+1 < 2^{p+1}$. Vi har

$VL_{p+1} = p+1 < 2^p + 1 < 2^p + 2^p$ eftersom $1 < 2^p$ då $p \geq 0$

(enligt $p < 2^p \Leftrightarrow A(p)$)

$= 2 \cdot 2^p = 2^{p+1} = HL_{p+1}$, så tydligen följer

$VL_{p+1} < HL_{p+1}$ av $VL_p < HL_p$ dvs implikationen

$A(p) \Rightarrow A(p+1)$ gäller och steg 2 är klart.

Steg 3: steg 1 & steg 2 och induktionsaxiomet fullbordar beviset.

6.5.4 Visa $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ för alla $n \geq 0$.

Bevis: Vi inför predikatet $A(n) \Leftrightarrow \underbrace{\sum_{k=0}^{n} 2^k}_{VL_n} = \underbrace{2^{n+1}-1}_{HL_n}$ och vi visar $\forall n \geq 0 : A(n)$.

Steg 1: Kolla att $A(0)$ gäller, dvs $VL_0 = HL_0$.

$VL_0 = \sum_{k=0}^{0} 2^k = 2^0 = 1$. $HL_0 = 2^{0+1} - 1 = 2 - 1 = 1$

tydligen gäller $VL_0 = HL_0$, dvs $A(0)$ stämmer.

steg 2: För godt $p \geq 0$ ska vi nu visa implikationen $A(p) \Rightarrow A(p+1)$ så vi antar $A(p) \Leftrightarrow VL_p = HL_p$ dvs att $\sum_{k=0}^{p} 2^k = 2^{p+1} - 1$. (induktions-antagandet.) forts ⇗

6.5.4 (forts.) Med stöd av detta ska vi visa $A(p+1)$ dvs $VL_{p+1} = HL_{p+1}$ dvs $\sum_{k=0}^{p+1} 2^k = 2^{p+2} - 1$.

$$VL_{p+1} = \sum_{k=0}^{p+1} 2^k = \underbrace{\sum_{k=0}^{p} 2^k}_{=2^{p+1}-1 \text{ enligt } A(p) \text{ dvs induktionsantagandet}} + 2^{p+1} = 2^{p+1} - 1 + 2^{p+1} = 2 \cdot 2^{p+1} - 1$$

$= 2^{p+2} - 1$ ← detta är $= HL_{p+1}$, dvs $VL_{p+1} = HL_{p+1}$ följer av $VL_p = HL_p$, dvs vi har $A(p) \Rightarrow A(p+1)$ och steg 2 är klart.

Steg 3: Steg 1 & steg 2 och induktionsaxiomet fullbordar beviset.

6.5.5 Visa att $A^n = \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}$ $\forall n \geq 1$ om $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.

Bevis: Inför predikatet $B(n) \Leftrightarrow A^n = \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}$.

Vi ska visa $\forall n \geq 1 : B(n)$, med induktion.

Här kallar vi också A^n för VL_n och $\begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}$ för HL_n (som vanligt).

Steg 1: Kolla att $B(1)$ gäller, dvs att $VL_1 = HL_1$.

$$VL_1 = A^1 = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

$$HL_1 = \begin{pmatrix} 2^1 & 1 \cdot 2^{1-1} \\ 0 & 2^1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

Lika, alltså gäller $VL_1 = HL_1$ dvs $B(1)$ är sann.

forts ⇒

6.5.5 (forts.)

Steg 2: Vi ska nu visa $B(p) \Rightarrow B(p+1)$ för godt. $p \geq 1$.

Vi gör därför induktionsantagandet $B(p) \Leftrightarrow$ $VL_p = HL_p$, dvs $A^p = \begin{pmatrix} 2^p & p2^{p-1} \\ 0 & 2^p \end{pmatrix}$. Med stöd av detta ska vi nu alltså visa att $B(p+1)$ gäller, dvs $VL_{p+1} = HL_{p+1}$. Vi skriver upp dessa led:

$VL_{p+1} = A^{p+1}$ ← det lämpar sig att börja här.

$HL_{p+1} = \begin{pmatrix} 2^{p+1} & (p+1)2^p \\ 0 & 2^{p+1} \end{pmatrix}$

$VL_{p+1} = A \cdot \underbrace{A^{p+1}}_{= VL_p = HL_p \text{ enligt induktions-antagandet}} = A \cdot \begin{pmatrix} 2^p & p2^{p-1} \\ 0 & 2^p \end{pmatrix} =$

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2^p & p2^{p-1} \\ 0 & 2^p \end{pmatrix} = \begin{pmatrix} 2\cdot 2^p + 1\cdot 0 & 2\cdot p2^{p-1} + 1\cdot 2^p \\ 0\cdot 2^p + 2\cdot 0 & 0\cdot p2^{p-1} + 2\cdot 2^p \end{pmatrix} =$$

$$= \begin{pmatrix} 2^{p+1} & p2^p + 2^p \\ 0+0 & 2^{p+1} \end{pmatrix} = \begin{pmatrix} 2^{p+1} & (p+1)2^p \\ 0 & 2^{p+1} \end{pmatrix}$$ ← detta är HL_{p+1} alltså följer $VL_{p+1} = HL_{p+1}$

av $VL_p = HL_p$, dvs $A(p) \Rightarrow A(p+1)$ gäller. steg 2 ok.

Steg 3: Steg 1 & Steg 2 och induktionsaxiomet fullbordar beviset.

6.6.1 Lösning saknas

6.6.2 Lösning saknas

6.1 Lösning saknas