5.18 Lös följande ekvationer i $\mathbb{Z}_{10}$.

b) $[2]x - [1] = [7]$.

Lös ut x, som vanligt, om det går.

$\Leftrightarrow [2]x = [7] + [1] = [8]$

$x = [4]$ ger

$[2]x = [2][4] = [2 \cdot 4] = [8]$.

Så vi har en lösning.

c) $[7]x - [5] = [8]$.

$\Leftrightarrow [7]x = [13]$.

$[-3]x = [3] \Rightarrow x = [-1]$ är en lösning. Notera: $[-1] = [9]$.

$\mathbb{Z}_{10}/\sim$, där

$x \sim y$ om $10 \mid (x-y)$.

$[x]$ är ekvivalensklassen som innehåller x. Add/mult ges av $[x]+[y] := [x+y]$. $[x][y] = [x \cdot y]$.

Tex $[x] = [x + k \cdot 10]$, $k \in \mathbb{Z}$.

Alternativ lösning till c).

$[7]x = [13]$

$\Leftrightarrow [7 - 10 \cdot 2]x = [13]$.

$\Leftrightarrow [-13]x = [13]$

$\Rightarrow x = [-1]$.

d) $[6]x + [3]\cdot[4]x + [6] = 0$

$\Leftrightarrow [6]x + [12]x + [6] = 0$

$\Leftrightarrow ([6] + [12])x + [6] = 0$

$\Leftrightarrow [18]x + [6] = 0$

$\Leftrightarrow [18]x = [-6]$

$[18]x = [-6 - 10\cdot 3] = [-36]$

$\Rightarrow x = [-2]$.

Alternativ i sista steget.

$[18]x = [-6]$.

Detta är ekvivalent med att $\exists n, m \in \mathbb{Z}$ så att

$(18 + 10n)x = -6 + 10m$

För $n = 0$, $m = -3$ så är $x = -2$ en lösn, så $[-2]$ löser alla kongruenser i uppgiften.

d) $[6]x + [3]\cdot[4]x + [6] = 0$

$\Leftrightarrow [6]x + [12]x + [6] = 0$

$\Leftrightarrow ([6] + [12])x + [6] = 0$

$\Leftrightarrow [18]x + [6] = 0$

$\Leftrightarrow [18]x = [-6]$

$[18]x = [-6 - [0 \cdot 3]] = [-36]$

$\Rightarrow x = [-2]$.

varför funkar det inte att göra -10 * 2 på [18]x så att vi får [-2]x = [-6]

$[18]x = [-6]$

$[-2]x = [-6]$

$x = [3]$

$3 - (-2) = 5$

$10 \not\equiv 5$.

So $[3] \neq [-2]$.

Finns två olika lösningar.

a) $[5]x + [3] = [2]$

$[5]x = [-1]$

Ekvivalent att hitta $m, n, x \in \mathbb{Z}$ så att

$(5 + 10m)x = -1 + 10n$

Notera att VL är delbart med 5. Eftersom

$\frac{(5+10m)x}{5} = (1 + 2m)x \in \mathbb{Z}$.

men $\frac{-1+10n}{5} = \frac{-1}{5} + 2n \notin \mathbb{Z}$.

Så det finns ingen lösning.

Allmänt:

$[A]x = [B]$ i $\mathbb{Z}_d$. $d \in \mathbb{N}$ d>0.

Om $A \mid d$, så kommer det finnas 0 eller fler än en lösning.

a) $[5]x + [3] = [2]$

$[5]x = [-1]$

Ekvivalent att hitta $m, n, x \in \mathbb{Z}$ så att

$(5 + 10m)x = -1 + 10n$

Notera att VL är delbart med 5. Eftersom

$\frac{(5+10m)x}{5} = (1 + 2m)x \in \mathbb{Z}$.

men $\frac{-1+10n}{5} = \frac{-1}{5} + 2n \notin \mathbb{Z}$.

Så det finns ingen lösning.

5.21 Visa att om $a \equiv b \bmod mn$ så gäller $a \equiv b \bmod n$ och $a \equiv b \bmod m$.

$a \equiv b \bmod n$ $\Leftrightarrow$ $n \mid (a-b)$ alltså $[a] = [b]$ i $\mathbb{Z}_n$.

Antag för $a, b, m, n \in \mathbb{Z}$ att $a \equiv b \bmod mn$.

$\Rightarrow$ $mn \mid a-b$. $\overset{\text{definition}}{\Rightarrow}$ $\exists k \in \mathbb{Z}$ $a - b = mnk$

$\Rightarrow (m \mid a-b) \wedge (n \mid a-b)$

$\Leftrightarrow a \equiv b \bmod m \wedge a \equiv b \bmod n$. ∎

5.22 Visa att om $ac \equiv bc \bmod n$ och $\gcd(c,n)=1$, då gäller att $a \equiv b \bmod n$.

Vad betyder egentligen $\gcd(c,n)=1$.

"Intuitivt" perspektiv: primtals faktorisering av c och n

$c = p_1 \cdot p_2 \cdot p_3 \cdots p_M \qquad n = q_1 \cdot q_2 \cdot q_3 \cdots q_K$.

Då ger $\gcd(c,n)=1 \Rightarrow p_i \neq q_j \quad \forall i=1 \ldots M, \forall j=1 \ldots K$.

Ett annat, ibland mycket använd bart perspektiv:

$\gcd(c,n)=1 \iff$ Existerar lösning, $(\exists l,k \in \mathbb{Z})\ cl+nk=1$.

Bevis ett: Antag för $a,c,b,n \in \mathbb{Z}$ att $ac \equiv bc \bmod n$ och $\gcd(c,n)=1$. $\Rightarrow n \mid ac-bc \wedge \exists l,k \in \mathbb{Z}: cl+nk=1$

$\Rightarrow \exists m \in \mathbb{Z}: ac-bc = m \cdot n \wedge \exists l,k \in \mathbb{Z}: cl = 1-nk$

$\Rightarrow \exists m,l,k \in \mathbb{Z}\ acl - bcl = mnl \wedge cl = 1-nk \Rightarrow \exists m,l,k \in \mathbb{Z}: a(1-nk) - b(1-nk) = mnl$

$\exists m,l,k \in \mathbb{Z}: a-b = mnl + ank - bnk = n(ml+ak-bk)$

$\Rightarrow n \mid a-b \Rightarrow a \equiv b \bmod n$. ∎