Kontrollskrivning 2

2. Mängdlära. Låt A, B, C vara tre godtyckliga mängder. Vad kan du säga om mängden

$$(A - (B \cup C)) \cap ((A \cap B) \cup (A \cap C))?$$

Bevisa ditt påstående utan att använda Venndiagram. (Men ett Venndiagram kan vara bra för att komma fram till vad den här mängden är för en mängd.)

Lösning: Vi kan genom att studera ett Venndiagram övertyga oss om att mängden är tomma mängden. Vi visar detta genom omskrivningen

$$(A-(B\cup C))\cap((A\cap B)\cup(A\cap C)) = A\cap(B\cup C)^c\cap(A\cap(B\cup C)) = A\cap A\cap(B\cup C)\cap(B\cup C)^c = A\cap\emptyset = \emptyset.$$

4. Inledande talteori.

KS2. Använd Euklides utvidgade algoritm för att finna alla heltal x som uppfyller

$$38x \equiv 56 \pmod{101}.$$

(Reducera ditt svar modulo 101.)

Lösning: Euklides algoritm ger $101 = 2\cdot 38 + 25, 38 = 1\cdot 25 + 13, 25 = 1\cdot 13 + 12, 13 = 1\cdot 12 + 1$ $\Rightarrow 1 = 13 - 1\cdot 12 = 13 - 1\cdot(25 - 1\cdot 13) = 2\cdot 13 - 1\cdot 25 = 2\cdot(38 - 1\cdot 25) - 1\cdot 25 = 2\cdot 28 - 3\cdot 25 = 2\cdot 38 - 3\cdot(101 - 2\cdot 38) = 8\cdot 38 - 3\cdot 101$. Så $8\cdot 38 \equiv 1 (\mathrm{mod}\ 101)$, dvs 8 är den multiplikativa inversen för 38 modulo 101. Det ger oss

$$38x \equiv 56 \pmod{101} \Leftrightarrow 8\cdot 38x \equiv 8\cdot 56 \pmod{101} \Leftrightarrow x \equiv 8\cdot 56 \pmod{101}$$

vilket reduceras till

$$x \equiv 44 \pmod{101}.$$

5. Relationer. Definiera relationen $\mathcal{R}$ på $\mathbb{Z}$ genom

$$x\mathcal{R}y \Leftrightarrow (x+1)^2 \equiv (y-1)^2 \pmod 2.$$

Är denna relation en ekvivalensrelation? I såfall, bevisa det. Om den inte är en ekvivalensrelation bevisa det.

Lösning – alternativ 1: Den är en ekvivalensrelation eftersom

$$x\mathcal{R}y \Leftrightarrow (x+1)^2 \equiv (y-1) \pmod 2 \Leftrightarrow x^2+2x+1 \equiv y^2-2y+1 \pmod 2 \Leftrightarrow x^2 \equiv y^2 \pmod 2 \Leftrightarrow$$
$$x^2 - y^2 \equiv 0 \pmod 2 \Leftrightarrow (x-y)(x+y) \equiv 0 \pmod 2 \Leftrightarrow 2|(x-y) \vee 2|(x+y)$$

eftersom 2 är ett primtal och eftersom $y \equiv -y (\mathrm{mod}\ 2)$ blir detta ekvivalent med $2|(x-y) \vee 2|(x-y)$ det vill säga $2|(x-y)$ som är $x \equiv y (\mathrm{mod}\ 2)$. Så i själva verket gäller $x\mathcal{R}y \Leftrightarrow x \equiv y (\mathrm{mod}\ 2)$, det vill säga $\mathcal{R}$ *är* kongruensrelationen som är en ekvivalensrelation.

Lösning – alternativ 2: Vi kan även skriva

$$x\mathcal{R}y \Leftrightarrow (x+1)^2 \equiv (y-1)^2 \pmod 2 \Leftrightarrow x^2+2x+1 \equiv y^2-2y+1 \pmod 2 \Leftrightarrow$$
$$x^2+2x \equiv y^2-2y \pmod 2 \Leftrightarrow x^2 \equiv y^2 \pmod 2$$

(minns att $2 \equiv 0 \equiv -2 (\mathrm{mod}\ 2) \Rightarrow 2x \equiv 0 \equiv -2y (\mathrm{mod}\ 2)$) och det är väldigt lätt att visa att relationen $x^2 \equiv y^2 (\mathrm{mod}\ 2)$ är reflexiv, symmetrisk och transitiv, beviset ser precis likadant ut som det för att kongruensrelationen är reflexiv, symmetrisk och transitiv. Vi kan dessutom sätta upp en tabell som visar att i $\mathbb{Z}_2$ gäller

$\overline{x}$	$\overline{y}$	$\overline{x}^2$	$\overline{y}^2$
$\overline{0}$	$\overline{0}$	$\overline{0}^2 = \overline{0}$	$\overline{0}^2 = \overline{0}$
$\overline{0}$	$\overline{1}$	$\overline{0}^2 = \overline{0}$	$\overline{1}^2 = \overline{1}$
$\overline{1}$	$\overline{0}$	$\overline{1}^2 = \overline{1}$	$\overline{0}^2 = \overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{1}^2 = \overline{1}$	$\overline{1}^2 = \overline{1}$

Eftersom tabellen visar att i $\mathbb{Z}_2$ gäller $x^2 = x$ så kan vi i $\mathbb{Z}^2$ skriva $x^2 = y^2 \Leftrightarrow x = y$ vilket, tillsammans med ovanstående ger

$$x\mathcal{R}y \Leftrightarrow x^2 \equiv y^2 \pmod 2 \Leftrightarrow x \equiv y \pmod 2$$

dvs den studerade relationen är en kongruensrelationen modulo 2 som är en ekvivalensrelation.

Lösning – alternativ 3: Vi ger även en lösning som kanske är mer intressant för er att studera eftersom tekniken som används i den här lösningen har en större allmängiltighet. Vi visar reflexivitet, symmetri och transitivitet utgående från relationens definition.

Reflexivitet. Vi ska visa att för alla $x \in \mathbb{Z}$ gäller $x\mathcal{R}x$ det vill säga att

$$(x+1)^2 \equiv (x-1) \pmod 2$$

för alla $x \in \mathbb{Z}$. Vi låter därför x vara ett godtyckligt heltal. Vi har då

$$(x+1)^2 \equiv (x-1) \pmod 2 \Leftrightarrow x^2 + 2x + 1 \equiv x^2 - 2x + 1 \pmod 2 \Leftrightarrow x^2 \equiv x^2 \pmod 2$$

som alltid är sant. (Ett tal – x^2 – är alltid kongruent med sig själv.) Eftersom x var godtyckligt valt är relationen reflexiv.

Symmetri. Vi ska nu visa att för alla $x, y \in \mathbb{Z}$ gäller implikationen $x\mathcal{R}y \Rightarrow y\mathcal{R}x$. För den skull antar vi att x, y är godtyckligt valda i $\mathbb{Z}$ men med $x\mathcal{R}y$ och vi ska, utgående från detta visa att $y\mathcal{R}x$. Vi kan uttrycka det så här:

Vi **HAR**: $x\mathcal{R}y \Leftrightarrow (x+1)^2 \equiv (y-1)^2 \pmod 2 \Leftrightarrow \exists k_1 \in \mathbb{Z} : x^2 + 2x + 1 = y^2 - 2y + 1 + 2k_1$
Vi **VILL HA**: $y\mathcal{R}x \Leftrightarrow (y+1)^2 \equiv (x-1)^2 \pmod 2 \Leftrightarrow \exists k_2 \in \mathbb{Z} : y^2 + 2y + 1 = x^2 - 2x + 1 + 2k_2$

Ekvationen med k_1 är alltså given och vi vill finna k_2 som löser den andra ekvationen. Vi kan därför skriva dem som ett ekvationssystem:

$$\begin{cases} x^2 + 2x + 1 = y^2 - 2y + 1 + 2k_1 \\ y^2 + 2y + 1 = x^2 - 2x + 1 + 2k_2 \end{cases} \Leftrightarrow \begin{cases} x^2 + 2x + 1 - y^2 + 2y - 1 = 2k_1 \\ y^2 + 2y + 1 - x^2 + 2x - 1 = 2k_2 \end{cases}$$

Om dessa ekvationer adderas tar alla kvadrater ut varandra och vi får

$$2x + 2y + 2y + 2x = 2k_1 + 2k_2 \Leftrightarrow k_2 = 2x + 2y - k_1$$

(vi har släppt den andra ekvationen eftersom detta tydligen ger oss vad k_2 måste vara). Att k_2 nu existerar i $\mathbb{Z}$ – $2x + 2y - k_1$ är ju ett *heltal* – innebär att $y\mathcal{R}x$ måste vara uppfyllt och, återigen, eftersom x, y var godtyckligt valda visar detta reflexiviteten.

Transitivitet. Vi ska nu visa att för alla $x, y, z \in \mathbb{R}$ har vi

$$x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$$

och detta är en utmärkt övningsuppgift, så vi ger inte detaljerna här annat än översiktligt: ni antar $x\mathcal{R}y$, det leder till existensen av ett k_1 samt $y\mathcal{R}z$ som leder till existensen av ett k_2 och ni ska visa $x\mathcal{R}z$ som kan uttryckas som existensen av ett k_3, ni tar fram det explicita uttrycket för k_3 (det kommer att bero på y, k_1, k_2) och konstaterar att det finns och ger upphov till att $x\mathcal{R}z$ gäller, så implikationen $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$ gäller och eftersom x, y, z var godtyckligt valda så är relationen transitiv.

6. Fördjupad talteori. Visa med matematisk induktion att

$$\sum_{k=1}^{n} (k+1)(k+5) = \frac{1}{6} n(n+7)(2n+7)$$

för alla $n = 1, 2, 3, \ldots$.

Lösning: Vi inför predikatet $A(n) \Leftrightarrow \sum_{k=1}^{n}(k+1)(k+5) = \frac{1}{6}n(n+7)(2n+7)$ och vi ska visa $\forall n \in \mathbb{N} : A(n)$. Inför också beteckningarna $VL_n = \sum_{k=1}^{n}(k+1)(k+5)$ respektive $HL_n = \frac{1}{6}n(n+7)(2n+7)$. Vi har då $A(n) \Leftrightarrow VL_n = HL_n$. Vi tar nu de tre stegen i ett induktionsbevis.

Steg 1. Visa att $A(1)$ är sann, det vill säga visa att $VL_1 = HL_1$. Vi studerar dessa var för sig:

$$VL_1 = \sum_{k=1}^{1}(k+1)(k+5) = (1+1)(1+5) = 12. \qquad HL_1 = \frac{1}{6} \cdot 1 \cdot (1+7) \cdot (2 \cdot 1 + 7) = \frac{8 \cdot 9}{6} = 12.$$

Eftersom tydligen $VL_1 = 12 = HL_1$ så måste $A(1)$ vara sann vilket fullbordar första steget.

Steg 2. Vi ska nu visa implikationen $A(p) \Rightarrow A(p+1)$ för alla positiva heltal p och vi antar därför att $A(p)$ är sant för ett visst p. Då har vi alltså $A(p) \Leftrightarrow VL_p = HL_p \Leftrightarrow$

$$\sum_{k=1}^{p}(k+1)(k+5) = \frac{1}{6}p(p+7)(2p+7).$$

Med kraft av detta ska vi visa att även $A(p+1)$ dvs $VL_{p+1} = HL_{p+1}$ gäller så vi studerar VL_{p+1} :

$$VL_{p+1} = \sum_{k=1}^{p+1}(k+1)(k+5) = \sum_{k=1}^{p}(k+1)(k+5) + (p+1+1)(p+1+5) = \sum_{k=1}^{p}(k+1)(k+5) + (p+2)(p+6).$$

Men nu vet vi att $VL_p = VL_p = \sum_{k=1}^{p}(k+1)(k+5) = \frac{1}{6}p(p+7)(2p+7)$ enligt induktionsantagandet så vi sätter in det och får

$$VL_{p+1} = \frac{1}{6}p(p+7)(2p+7)+(p+2)(p+6) = \frac{p(p+7)(2p+7) + 6(p+2)(p+6)}{6} = \frac{(p^2+7p)(2p+7) + 6(p^2+8p+12)}{6} =$$

$$\frac{2p^3 + 7p^2 + 14p^2 + 49p + 6p^2 + 48p + 72}{6} = \frac{1}{6}(2p^3 + 27p^2 + 97p + 72).$$

Vi är klara om vi kan visa att detta också är HL_{p+1} så vi berk̈nar:

$$HL_{p+1} = \frac{1}{6}(p+1)(p+1+7)(2(p+1)+7) = \frac{1}{6}(p+1)(p+8)(2p+9) = \frac{1}{6}(p^2+9p+8)(2p+9) =$$

$$\frac{1}{6}(2p^3 + 9p^2 + 18p^2 + 81p + 16p + 72) = \frac{1}{6}(2p^3 + 27p^2 + 97p + 72)$$

vilket mycket riktigt överensstämmer med uttrycket för VL_{p+1}. Alltså har vi med stöd av induktionsantagandet $VL_p = HL_p$ visat att $VL_{p+1} = HL_{p+1}$, det vill säga vi har visat implikationen $A(p) \Rightarrow A(p+1)$. Eftersom p var ett godtyckligt positivt heltal är andra steget klart.

Steg 3. Steg 1 och steg 2 samt induktionsaxiomet fullbordar beviset.