Lösningar till tentamensskrivningen
i MAL 200 del 4, 2000-01-08

1. **Ge exempel på**
(a) en relation som är symmetrisk, men inte transitiv,
(b) en operation på heltalsmängden $\mathbb{Z}$ som inte är kommutativ,
(c) en restring $\mathbb{Z}_n$ som inte är en kropp.
Motivera dina svar!

(a) Låt M vara mängden av alla människor. Låt $x, y \in M$ och definiera $x \sim y$ om x och y känner varandra. Relationen är symmetrisk, men inte transitiv: det kan vara så att $x \sim y$ och $y \sim z$, medan $x \not\sim z$.
(b) Subtraktion är en operation på heltalsmängden $\mathbb{Z}$ som inte är kommutativ: t ex $2-1=1$, medan $1-2=-1$.
(c) Restringen $\mathbb{Z}_n$ är en kropp omm p är ett primtal. Det enklaste exemplet som inte är en kropp är därför $\mathbb{Z}_4$. Elementet $2 \in \mathbb{Z}_4$ saknar en multiplikativ invers, ty $2 \cdot x = 0$ eller 2 för alla $x \in \mathbb{Z}_4$.

2. **Faktoruppdela polynomet $X^4 + 2X^2 - 8$ i produkt av irreducibla polynom med koefficienter i $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ (d v s i $\mathbb{Q}[X]$, $\mathbb{R}[X]$ och $\mathbb{C}[X]$).**

Låt $X^2 = Y$. Då är $X^4 + 2X^2 - 8 = Y^2 + 2Y - 8 = (Y+4)(Y-2) = (X^2+4)(X^2-2)$. Polynomen X^2+4 och X^2-2 är irreducibla i $\mathbb{Q}[X]$ eftersom de saknar rationella nollställen, så $(X^2+4)(X^2-2)$ är faktoruppdelningen i $\mathbb{Q}[X]$. Polynomet X^2+4 saknar reella nollställen och är därmed irreducibelt i $\mathbb{R}[X]$, medan $(X^2-2) = (X+\sqrt{2})(X-\sqrt{2})$; detta ger faktoruppdelningen $(X^2+4)(X+\sqrt{2})(X-\sqrt{2})$. Slutligen kan man i $\mathbb{C}[X]$ skriva polynomet som produkt av linjärfaktorer: $X^4+2X^2-8 = (X+2i)(X-2i)(X+\sqrt{2})(X-\sqrt{2})$.

3. **Som bekant kan heltal definieras som ekvivalensklasser av relationen**

$$(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$$

på mängden av alla par (a,b), där a,b,c,d är naturliga tal.
(a) Kontrollera att relationen $\sim$ verkligen är en ekvivalensrelation.
(b) Ge exempel på två representanter för ekvivalensklassen av -2 och två representanter för ekvivalensklassen av 4. Utnyttja dina exempel för att förklara att multiplikation av heltal kan utföras med helt godtyckliga representanter för dessa klasser.
(c) Visa att multiplikation av heltal är en kommutativ operation. (4p)

(a) Vi kollar de tre kraven i definitionen av en ekvivalensrelation:
reflexiv: $(a,b) \sim (a,b)$. Detta stämmer ty $a+b = b+a$.
symmetrisk: om $(a,b) \sim (c,d)$, så är $(c,d) \sim (a,b)$. Ty $a+d = b+c$ omm $c+b = d+a$ stämmer detta också.
transitiv: om $(a,b) \sim (c,d)$ och $(c,d) \sim (e,f)$, så är $(a,b) \sim (e,f)$. Givet är alltså $a+d = b+c$ och $c+f = d+e$. Då är $a+d+f = b+c+f = b+d+e$ och nu kan vi subtrahera d på båda sidor, så $a+f = b+e$, d v s $(a,b) \sim (e,f)$.

(b) Representanter för -2 är t ex $(0, 2)$ och $(1, 3)$, och för 4 kan man ta $(4, 0)$ och $(5, 1)$. Heltal multipliceras via $[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$ (ty $(a - b)(c - d) = ac - ad - bc + bd$). Vi får $(0, 2) \cdot (4, 0) = (0, 8)$ och $(1, 3) \cdot (5, 1) = (5 + 3, 1 + 15)$ och både $(0, 8)$ och $(8, 16)$ representerar -8.
(c) Multiplikation är definierad genom $[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$. Vi beräknar $[(c, d)] \cdot [(a, b)] = [(ca + db, cb + da)]$. Eftersom $ac + bd = ca + db$ och $ad + bc = cb + da$ för naturliga tal är $[(a, b)] \cdot [(c, d)] = [(c, d)] \cdot [(a, b)]$, d v s multiplikation av heltal är kommutativ.

4. På hur många sätt kan 13 personer delas in i 1 grupp om 4 och 3 grupper om 3 personer?

Man kan välja 4 personer ur 13 på $\binom{13}{4}$ olika sätt. Sen har man 9 personer kvar, ur vilka man kan välja tre på $\binom{9}{3}$ sätt; sen har man $\binom{6}{3}$ sätt att välja en grupp av tre. Slutligen är tre personer kvar (observera att $\binom{3}{3} = 1$). Man kan inte skilja mellan de tre grupperna av tre personer, så vi delar produkten av binomialkoefficienter med $3! = 6$. Svaret blir alltså

$$\binom{13}{4} \cdot \binom{9}{3} \cdot \binom{6}{3} \cdot \binom{3}{3} \cdot \frac{1}{3!} = \frac{13!}{4! \cdot 3! \cdot 3! \cdot 3! \cdot 3!}$$
$$= \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5}{6 \cdot 6 \cdot 6 \cdot 6} = 13 \cdot 4 \cdot 11 \cdot 10 \cdot 7 \cdot 5 = 200200$$

Man kan också välja de tre grupperna av tre först, så att de kvarstående bildar gruppen av 4 personer. Då får man $\binom{13}{3} \cdot \binom{10}{3} \cdot \binom{7}{3} \cdot \frac{1}{3!} = 200200$.

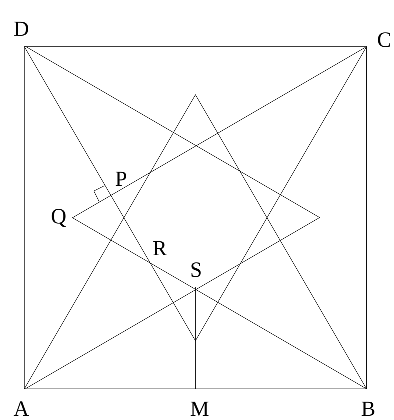
5. Formulera och bevisa Pythagoras' sats.

Se kompendiet om Euklidisk geometri och övningarna.

6. (a) Visa att de tre höjderna i en triangel skär varandra i en punkt.
(b) När ligger skärningspunkten utanför triangeln? Motivera ditt svar.

(a) Se kompendiet om euklidisk geometri.
(b) Skärningspunkten ligger utanför triangeln i en trubbvinklig triangel. Då ligger höjderna genom de två spetsa vinklarna utanför triangeln, och därmed deras skärningspunkt.

7. På sidorna i en kvadrat med sidan 2 ritas liksidiga trianglar, alla inåt. De fyra triangelytornas snitt är en liksidig (men ej regelbunden) 8-hörning. Beräkna dess sida.



Triangeln ΔPDC är rätvinklig med $\angle PDC = 60^\circ$ så $|CP| = \sqrt{3}$ och $|QP| = 2 - \sqrt{3}$. Triangeln ΔPQR är av samma typ, så $|QR| = 2|QP| = 4 - 2\sqrt{3}$. Hypotenusan BS i triangeln ΔMSB har längd $2/\sqrt{3} = \frac{2}{3}\sqrt{3}$. Den sökta sträckans längd är nu $|RS| = |BQ| - |BS| - |QR| = 2 - 4 + 2\sqrt{3} - \frac{2}{3}\sqrt{3} = \frac{4}{3}\sqrt{3} - 2$.

8. (a) Lös, om möjligt, ekvationen

$$X^2 + 1 = 0$$

i $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ och $\mathbb{Z}_{13}$.

(b) Visa att ekvationen inte har några lösningar i $\mathbb{Z}_p$ om p är ett primtal på formen $p = 4k - 1$.

Ledning: antag att x är en lösning och beräkna $(x^2)^{\frac{p-1}{2}}$ på två sätt.

(a) Det räcker att kolla tal $1, \ldots, \frac{p-1}{2}$ i $\mathbb{Z}_p$. I $\mathbb{Z}_3$ har vi $1^1 + 1 = 2$. I $\mathbb{Z}_5$ hittar vi en lösning: $2^2 + 1 \equiv 0 \pmod 5$; därmed är $3 \equiv -2$ också en lösning och eftersom en andragradsekvation har högst två lösningar har vi hitta alla. Genom att beräkna $3^2 + 1 = 10$, $4^2 + 1 = 17$ och $5^2 + 1 = 26$ ser vi att ekvationen saknar lösningar i $\mathbb{Z}_7$ och $\mathbb{Z}_{11}$. Däremot finns två lösningar, 5 och $-5 \equiv 8$ i $\mathbb{Z}_{13}$.

(b) Låt $p = 4k - 1$. Enligt beviset för Fermats lilla sats är $(x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$ för alla $x \neq 0 \in \mathbb{Z}_p$. Om nu $x^2 = -1$, är $(x^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = (-1)^{2k-1} = -1$ ty $2k - 1$ är udda. Denna motsägelse beviser att ekvationen inte har några lösningar i $\mathbb{Z}_p$ om p är ett primtal på formen $p = 4k - 1$.