MATEMATIK
Chalmers Tekniska Högskola
Tentamen i Diskret matematik IT, TMV200, 2012-12-22.
Lösningar

1. (a) Primtalsfaktoriseringen ges av $450 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$. Alla positiva delare ges av alla möjliga produkter av dessa faktorer och om man successivt tar de som innehåller $0, 1, 2, 3, 4$ respektive 5 faktorer så får man:

$$\{1, 2, 3, 5, 6, 9, 10, 15, 25, 18, 30, 45, 50, 75, 90, 150, 225, 450\}.$$

(b) Euklides algoritm ger:

$$\begin{aligned} 301 &= 3 \cdot 84 + 49 \\ 84 &= 1 \cdot 49 + 35 \\ 49 &= 1 \cdot 35 + 14 \\ 35 &= 2 \cdot 14 + 7 \\ 14 &= 2 \cdot 7. \end{aligned}$$

Alltså är $\text{sgd}(301, 84) = 7$. Vi ersätter successivt de erhållna resterna och får:

$$\begin{aligned} 7 &= 35 - 2 \cdot 14 = 35 - 2 \cdot (49 - 1 \cdot 35) = 3 \cdot 35 - 2 \cdot 49 \\ &= 3 \cdot (84 - 1 \cdot 49) - 2 \cdot 49 = 3 \cdot 84 - 5 \cdot 49 \\ &= 3 \cdot 84 - 5 \cdot (301 - 3 \cdot 84) = 18 \cdot 84 - 5 \cdot 301. \end{aligned}$$

2. Vi gör ett induktionsbevis.

Basfall: $n = 0$

Då gäller att

$$\sum_{i=1}^{0} F(2i - 1) = 0 = F(2 \cdot 0),$$

och alltså gäller likheten för $n = 0$.

Induktionssteget: Antag nu att det gäller för ett fixt naturligt tal n. Visa att då gäller det också för $n + 1$. Vi får

$$\begin{aligned} \sum_{i=1}^{n+1} F(2i - 1) &= \sum_{i=1}^{n} F(2i - 1) + F(2(n + 1) - 1) \\ &= F(2n) + F(2n + 1) = F(2n + 2) = F(2(n + 1)) \end{aligned}$$

och alltså gäller likheten också för $n + 1$.

Enligt induktionsprincipen gäller därmed likheten för alla naturliga tal.

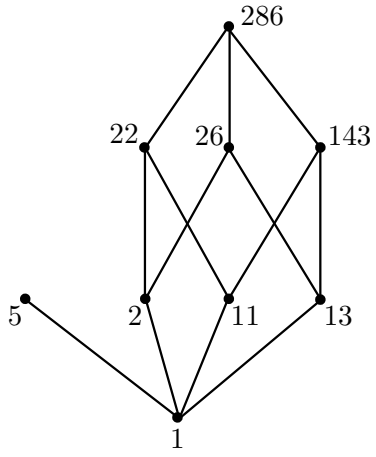
3. (a) Om vi bortser från villkoret så finns det $\binom{14}{5}$ olika arbetsgrupper. Ifrån detta tal får vi sedan subtrahera det antal grupper som innehåller både Herr V och Fru M. En sådan grupp väljs ut genom att de övriga 3 medlemmarna väljs bland de återstående 12. Det finns alltså $\binom{12}{3}$ sådana grupper. Svaret är alltså

$$\binom{14}{5} - \binom{12}{3} = 1782.$$

   (b) Samma resonemang som ovan ger

$$\binom{n}{k} - \binom{n-2}{k-2}.$$

4. Minimalt och minsta element: 1
   Maximala element: 5 och 286
   Största element saknas.



Figur 1: Hasse-diagrammet till mängden M.

5. (a) Låt universum vara de naturliga talen och inför följande två predikat:
   $P(n)$: $5 \mid n$
   $Q(n)$: $n^2 \equiv 1 \pmod 5$.
   Då kan utsagan skrivas som

$$\forall n(\neg P(n) \to Q(n)).$$

   (b) Negationen ges av

$$\begin{aligned} \neg(\forall n(\neg P(n) \to Q(n))) &\Leftrightarrow \exists n\, \neg(P(n) \vee Q(n)) \\ &\Leftrightarrow \exists n(\neg P(n) \wedge \neg Q(n)). \end{aligned}$$

Här använde vi en välkänd ekvivalens för implikation och räkneregeln för negation av kvantorer i det första steget, och deMorgans lag i det andra.

(c) Negationen är sann, för t ex är $P(2)$ och $Q(2)$ båda falska.

6. (a) Vi primtalsfaktoriserar $132 = 2^2 \cdot 3 \cdot 11$ och multiplikativiteten för Φ och formeln för dess värde på primtalspotenser ger att

$$\Phi(132) = \Phi(2^2)\Phi(3)\Phi(11) = 2 \cdot (2-1) \cdot (3-1) \cdot (11-1) = 40.$$

(b) Vi ser direkt att varken 2 eller 3 delar 1121 och eftersom $1122 = 11 \cdot 102$ så gäller också $11 \nmid 1121$. Alltså är $\text{sgd}(1121, 132) = 1$. (Man kunde förstås också visat detta med Euklides algoritm.) Vi får också (första steget i Euklides algoritm, så där hade man lite nytta av om man gjort detta redan) att

$$1121 = 8 \cdot 132 + 65 \text{ så } 1121 \equiv 65 \pmod{132}.$$

Vi utnyttjar Eulers sats, $a^{\Phi(n)} \equiv 1 \pmod{n}$ om $\text{sgd}(a, n) = 1$, med $a = 1121$ och $n = 132$ och får

$$1121^{1121} = 1121^{28 \cdot 40 + 1} = \left(1121^{40}\right)^{28} \cdot 1121^1 \equiv 1^{28} \cdot 65 \equiv 65 \pmod{132}.$$

Svaret är alltså $m = 65$.

7. (a) Reflexiv: Tag $a \in G$. Då har vi att $a \star a^{-1} = e \in H$ så $a \mathcal{R} a$.
Symmetrisk: Antag att $a \mathcal{R} b$, d v s $a \star b^{-1} \in H$. Eftersom H är en grupp så gäller att $(a \star b^{-1})^{-1} \in H$. Men $(a \star b^{-1})^{-1} = b \star a^{-1}$ så alltså har vi att $b \mathcal{R} a$.
Transitiv: Antag att $a \mathcal{R} b$ och $b \mathcal{R} c$, d v s $a \star b^{-1} \in H$ och $b \star c^{-1} \in H$. Men $\star$ är en operator på H så $(a \star b^{-1}) \star (b \star c^{-1}) \in H$. Men från associativiteten hos $\star$ får vi nu att

$$(a \star b^{-1}) \star (b \star c^{-1}) = a \star (b^{-1} \star b) \star c^{-1} = a \star e \star c^{-1} = a \star c^{-1}.$$

Alltså får vi att $a \mathcal{R} c$.

(b) Nollan är identitet och det är välkänt att addition är associativ. Vidare om $n \in \mathbb{Z}$ så är $-n \in \mathbb{Z}$ en invers för addition. Addition är en operator på H_N, ty $N \mid m$ och $N \mid n$ ger $N \mid (m+n)$. Vidare gäller att H_N har en identitet eftersom $0 \in H_N$. Till slut är inversen av ett element i H_N också i H_N, ty $N \mid n$ implicerar att $N \mid -n$.

(c) Definitionen av $\mathcal{R}$ ger i specialfallet $G = \mathbb{Z}$ och $H = H_N$ att $m \mathcal{R} n$ om och endast om $m - n \in H_N$. Men $m - n \in H_N$ om och endast om $N \mid m - n$, d v s om och endast om $m \equiv n \pmod{N}$. I detta specialfall är alltså $\mathcal{R}$ ingenting annat än kongruens modulo N.