Løsningsforslag Øving 4
TMA4140-MA0302 Diskret matematikk
Høsten 2005

2.2.25
Vi må vise
at $f(x)$ er $\Theta(g(x))$ medfører at $f(x)$ er $O(g(x))$ og at $g(x)$ er $O(f(x))$;
og
at $f(x)$ er $O(g(x))$ og at $g(x)$ er $O(f(x))$ medfører at $f(x)$ er $\Theta(g(x))$.

At $f(x)$ er $\Theta(g(x))$ betyr at $f(x)$ er $O(g(x))$ og at $f(x)$ er $\Omega(g(x))$. At $f(x)$ er $\Omega(g(x))$ betyr at det finnes en konstant k og en konstant $C > 0$ slik at $|f(x)| \geq C|g(x)|$ for alle $x > k$. En annen måte å skrive dette siste på er $|g(x)| \leq \frac{1}{C}|f(x)|$ for alle $x > k$. Dette viser at vi også har at $g(x)$ er $O(f(x))$.

For å bevise den andre delen ser vi på akkurat samme måten som over at $g(x)$ er $O(f(x))$ medfører at $f(x)$ er $\Omega(g(x))$, så at $f(x)$ er $O(g(x))$ og at $g(x)$ er $O(f(x))$ medfører at $f(x)$ er $\Theta(g(x)$.

2.2.36
Dette følger ikke. Et moteksempel: La $f(x) = 2x$ og $g(x) = x$. Da er $f(x)$ $O(g(x))$, $2^{f(x)} = 2^{2x} = 4^x$ og $2^{g(x)} = 2^x$. Men 4^x er ikke $O(2^x)$. Faktisk så er $4^x/2^x = 2^x$, så forholdet blir vilkårlig stort for store x - det er ikke begrenset av en konstant.

2.4.22
La $a \equiv b \pmod{m}$. Dette betyr at $m|(a-b)$, som igjen gir at $a = b + mc$. Men $b = qm + r$ for et ikke-negativt heltall r mindre enn m, altså $r = b \bmod m$. Dette gir $a = qm + r + mc = (q + c)m + r$. Dermed er $a \bmod m = r = b \bmod m$.

2.4.24
Hvis det finnes en ikke-triviell faktor, må vi finne den. Ellers må vi sjekke for alle primtall mindre enn eller lik kvadratroten av det oppgitte tallet.

a)
$2^7 - 1 = 127$. Deling på 2, 3, 5, 7 og 11 viser at disse ikke er faktorer. Siden $\sqrt{127} < 13$ kan vi konkludere at 127 er et primtall.

b)
$2^9 - 1 = 511 = 7 \cdot 73$, så dette er ikke et primtall.

c)

$2^{11} - 1 = 2047 = 23 \cdot 89$, så dette tallet er ikke et primtall.

d)
$2^{13} - 1 = 8191$. Deling på 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83 og 89 (Puh!) viser at disse ikke er faktorer. Siden $\sqrt{8191} < 97$ kan vi konkludere at 8191 er et primtall.

2-4-25
a) Positive heltall mindre enn eller lik 4 som er relativt primiske til 4, er 1 og 3. Altså er $\phi(4) = 2$.

b) Positive heltall mindre enn eller lik 10 som er relativt primiske til 10, er 1, 3, 7 og 9. Altså er $\phi(10) = 4$.

c) Positive heltall mindre enn eller lik 13 som er relativt primiske til 13, er 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Altså er $\phi(13) = 12$.

2-4-26
$\phi(n) = |\{m|\ m \in \mathbf{Z}_+,\ m \leq n,\ (m,n) = 1\}|$.

Vi skal vise et "hvis og bare hvis utsagn", det er med andre ord to ting vi skal vise.

La oss først vise at hvis n er et primtall så har vi at $\phi(n) = n - 1$. Hvis n er et positivt heltall, så er det n positive heltall som er mindre eller lik n. Hvis $n \neq 1$, så er det ikke tilfellet at $(n,n) = 1$ (vi har faktisk at $(n,n) = n$). Dermed vet vi at $\phi(n) \leq n - 1$ (så lenge $n \neq 1$.) Hvis n er et primtall, så er alle tall mindre enn n relativt primiske med n. Hvis ikke dette var sant, ville det være ett tall større enn en, men mindre enn n som hadde felles primtallsfaktor med n. Men da er n et sammensatt tall. Dermed er $\phi(n) = n - 1$.

Hvis $\phi(n) = n - 1$ så har vi at n er et primtall. Hvis ikke så er n et sammensatt tall, og da har n en primtallsfaktor mindre enn seg selv. Men da er n og denne primtallsfaktoren ikke relativt primiske, så $\phi(n) \leq n - 2$.

2-4-27
Et heltall a er relativt primisk med p^k hvis og bare hvis p ikke er en faktor i a. For positive heltall mindre enn eller lik p^k har vi at p er en faktor i $p, 2p, 3p, ..., (p^{k-1})p$. Så $\phi(p^k)$ er antall positive heltall mindre enn eller lik p^k som ikke er delelige med p, $\phi(p^k) = p^k - p^{k-1}$.
2.4.34
Vi har $a = dq + r$ der $0 \leq r < d$ (Teorem 6, kap 2.4). Deler vi denne ligningen på d får vi $a/d = q + (r/d)$, der $0 \leq (r/d) < 1$. Dermed er det klart

fra definisjonen at q er $\lfloor a/d \rfloor$. Ligningen vi startet med viser, naturligvis, at $r = a - dq$, som beviser det andre utsagnet.

2.4.40
Teorem 7, side 161 i boken forteller oss at for positive heltall a, b har vi $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$. Dermed får vi i vårt tilfelle at $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^1 1)/(2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^1 1$.

2.4.42
At $a \equiv b \pmod{m}$ og $c \equiv d \pmod{m}$ betyr at det finnes heltall q_1 og q_2 slik at $a - b = q_1 m$ og $c - d = q_2 m$. Dermed har vi $(a - c) - (b - d) = (a - b) - (c - d) = q_1 m - q_2 m = (q_1 - q_2)m$. Dette gir $a - c = b - d + Cm$, så $a - c \equiv (b - d) \pmod{m}$.

2.4.47
Vi har at $a = b + C_1 m$, og at $a^k = (b + C_1 m)^k = b^k + C_2 m$ (Det eneste leddet som ikke har en faktor av m er b^k, resten av leddene samler vi i konstanten C_2 ganget med m). Det følger at $a^k \equiv b^k \pmod{m}$.

4.2.16
Vi kan anvende "duehullprinsippet" ved å gruppere tallene i de par (delmengder) som adderes til 16, nemlig {1,15}, {3,13}, {5,11} og {7,9}. Dersom vi velger 5 tall fra mengden {1,3,5,7,9,11,13,15}, så må minst to av tallene komme fra samme delmengde, siden det kun er 4 delmengder. Så å velge ut 5 tall er tilstrekkelig for å garantere at summen av to av tallene er 16. Vi ser også at 4 eller færre tall ikke er nok, for da kan vi velge ett tall fra hver gruppe.